(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2010-533344
(P2010-533344A)
(43)公表日　平成22年10月21日(2010.10.21)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330F	5B017
H04L 9/32	(2006.01)	H04L	9/00	673D	5B285
G06F 21/24	(2006.01)	H04L	9/00	675A	5J104
		G06F	15/00	330G	
		G06F	12/14	530P	

審査請求 未請求　予備審査請求 未請求　（全 46 頁）

(21)出願番号　特願2010-516295 (P2010-516295)
(86)(22)出願日　平成20年7月14日 (2008.7.14)
(85)翻訳文提出日　平成22年3月12日 (2010.3.12)
(86)国際出願番号　PCT/US2008/069958
(87)国際公開番号　WO2009/009788
(87)国際公開日　平成21年1月15日 (2009.1.15)
(31)優先権主張番号　60/949,282
(32)優先日　平成19年7月12日 (2007.7.12)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　60/987,312
(32)優先日　平成19年11月12日 (2007.11.12)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/049,613
(32)優先日　平成20年5月1日 (2008.5.1)
(33)優先権主張国　米国 (US)

(71)出願人　510010311
イノベーション　インベストメンツ、エルエルシー
アメリカ合衆国、３００１０　ジョージア州、ノークロス、ポスト　オフィス　ボックス　９２１２３４
(74)代理人　100104411
弁理士　矢口　太郎
(74)代理人　100158621
弁理士　佐々木　義行
(74)代理人　100133503
弁理士　関口　一哉

最終頁に続く

(54)【発明の名称】識別認証および保護アクセスシステム、構成要素、および方法

(57)【要約】
【解決手段】　セキュリティートークンは、そのトークンの利用許可されたユーザーに対する固有のバイオメトリック識別子に基づいて各々に固有に暗号化されたデータを含む。デコーダーは、前記トークンおよび前記ユーザーのバイオメトリック識別子を受け取り、前記バイオメトリック識別子をバイオメトリックキーに変換し、前記バイオメトリックキーを適用して前記トークンを解読する。このようにすれば、前記デコーダーは、バイオメトリック識別子の比較を実行せずに前記ユーザーを認証する。幾つかの実施形態において、前記データの片または組は指定されたデータ区画内に格納され、前記指定されたデータ区画は利用許可キーに基づいて個別に暗号化され、前記暗号化されたデータ区画の全ては前記バイオメトリックキーに基づいて集合的に暗号化されて前記トークンが生成される。前記デコーダーは、前記デコーダーが開く許可を有する前記データ区画に対応する前記利用許可キーのみを格納する。さらに、幾つかの実施形態において、前記トークンおよび前記バイオメトリック識別子は暗号化され、リモート認証サーバーに送られて

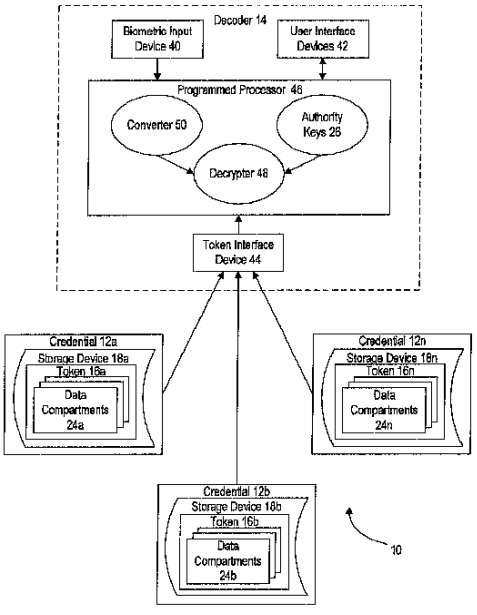

FIG. 1

【特許請求の範囲】
【請求項１】
１若しくはそれ以上のユーザーのための識別認証システムであって、このシステムは、
前記ユーザーのうちの１人に発行された少なくとも１つのクレデンシャルであって、このクレデンシャルは暗号化アルゴリズムを用いた暗号化ソフトウェアによって暗号化され且つ前記ユーザーのバイオメトリック識別子から生成されたバイオメトリックキーに基づいて暗号化されたデータを有するセキュリティートークンを含むものである、前記クレデンシャルと、
トークンインターフェース装置とバイオメトリック入力装置とを含み、前記暗号化アルゴリズムを用いた解読ソフトウェアおよび変換ソフトウェアへのアクセスを有する少なくとも１つのデコーダーであって、前記バイオメトリック入力装置は前記ユーザーからのバイオメトリック識別子を受け取り、前記変換ソフトウェアは前記バイオメトリック識別子を前記バイオメトリックキーに変換し、前記トークンインターフェース装置は前記ユーザーのクレデンシャルから前記トークンを受け取り、前記解読ソフトウェアは前記トークンに前記暗号化アルゴリズムおよび前記バイオメトリックキーを適用して、前記トークンを解読することにより前記トークンを開くものであって、当該トークンは、前記ユーザーが前記トークンを暗号化するために使用した前記バイオメトリック識別子を提示することによってのみ開放可能であり、これにより前記トークンが開くことによって前記ユーザーが認証されるものである、前記デコーダーと
を有するシステム。
【請求項２】
請求項１記載のシステムにおいて、前記トークンは、前記データを格納する少なくとも１つのデータ区画を含むものであって、このデータ区画は同一または異なる暗号化ソフトウェアによって暗号化され且つ少なくとも１つの利用許可キー（オーソリティキー）に基づいて暗号化されるものである。
【請求項３】
請求項２記載のシステムにおいて、前記デコーダーは前記少なくとも１つの利用許可キーへアクセスし、当該デコーダーは、前記トークンを開いた後、前記解読ソフトウェアおよび前記少なくとも１つの利用許可キーを適用して前記データ区画を開くものである。
【請求項４】
請求項２記載のシステムにおいて、前記トークンの暗号化および前記データ区画の暗号化は、前記ユーザーの前記同一または異なるバイオメトリック識別子から生成された少なくとも２つのバイオメトリックキーに基づいているものである。
【請求項５】
請求項４記載のシステムにおいて、前記デコーダーは、前記同一のバイオメトリック識別子または前記異なるバイオメトリック識別子から前記少なくとも２つのバイオメトリックキーを生成するものであって、当該デコーダーは前記少なくとも１つの利用許可キーへアクセスし、前記バイオメトリックキーのうちの第１のものを用いて前記トークンを開いた後、前記デコーダーは前記解読ソフトウェア、前記少なくとも１つの利用許可キー、および前記バイオメトリックキーのうちの第２のものを適用して前記データ区画を開くものである。
【請求項６】
請求項１記載のシステムにおいて、前記トークンは複数のデータ区画を含むものであって、各々のデータ区画は１片または１組の前記データを格納することができ、当該各々のデータ区画が前記同一または異なる暗号化ソフトウェアによって暗号化され且つ複数の利用許可キーのうちの少なくとも１つに基づいて暗号化されるものであり、当該利用許可キーに基づいて暗号化されたデータ区画は前記バイオメトリックキーに基づいて集合的に暗号化されて前記トークンを形成するものである。
【請求項７】
請求項６記載のシステムにおいて、前記デコーダーは前記利用許可キーのうちの少なく

とも１つへアクセスし、前記デコーダーは、前記トークンを開いた後、前記同一または異なる解読ソフトウェアおよびその少なくとも１つの利用許可キーを適用してその少なくとも１つの利用許可キーに対応した前記データ区画を開くものであって、当該デコーダーは、対応する利用許可キーへのアクセスを有さない前記データ区画については何れも開くことができないものである。

【請求項８】

請求項１記載のシステムにおいて、このシステムは、さらに、

少なくとも１つのバイオメトリック入力装置と、少なくとも１つのトークンインターフェース装置と、変換ソフトウェアと、前記暗号化アルゴリズムを用いた暗号化ソフトウェアとを備えた設定ワークステーションを有するものであって、当該バイオメトリック入力装置は前記ユーザーから前記バイオメトリック識別子を受け取り、当該変換ソフトウェアは前記バイオメトリック識別子を前記バイオメトリックキーに変換し、当該暗号化ソフトウェアは前記暗号化アルゴリズムおよび前記バイオメトリックキーを適用して前記データを暗号化して前記トークンを形成し、当該トークンインターフェース装置は前記トークンを前記クレデンシャルに転送するものである。

【請求項９】

請求項８記載のシステムにおいて、前記設定ワークステーションは少なくとも１つの利用許可キーへアクセスし、前記利用許可キーに基づいてデータ区画内の前記データの少なくとも一部を暗号化し、次に、前記バイオメトリックキーに基づいて前記データ区画を暗号化するものである。

【請求項１０】

請求項１記載のシステムにおいて、前記クレデンシャルはデジタル財布のクレデンシャルであり、前記トークンはバンクカード情報を含むものである。

【請求項１１】

請求項１記載のシステムにおいて、前記クレデンシャルは保険カードのクレデンシャルであり、前記トークンは保険情報を含むものである。

【請求項１２】

請求項１記載のシステムにおいて、前記クレデンシャルは医療パスポートのクレデンシャルであり、前記トークンは医療サービス情報を含むものである。

【請求項１３】

請求項１記載のシステムにおいて、前記クレデンシャルは政府発行の身分証明クレデンシャルであり、前記トークンはユーザーの身分証明情報を含むものである。

【請求項１４】

請求項１記載のシステムにおいて、前記クレデンシャルは境界アクセスのクレデンシャルであり、前記デコーダーが前記トークンを認証することによって、前記ユーザーは保護された境界領域内への進入を許可されるものである。

【請求項１５】

請求項１記載のシステムにおいて、前記クレデンシャルはＡＴＩ従事者のクレデンシャルであり、前記デコーダーはＡＴＩシステムに動作可能に接続されており、前記デコーダーが前記トークンを認証することによって、前記ユーザーは空港の保護された境界領域内への進入を許可されるものである。

【請求項１６】

請求項１記載のシステムにおいて、前記クレデンシャルはＡＴＩの乗客のクレデンシャルであり、前記トークンは、前記ユーザーのバイオメトリック識別子に基づいて生成された公開バイオメトリックキーに基づいて暗号化され、そして、前記ユーザーのバイオメトリック識別子に基づいて生成された非公開バイオメトリックキーによって解読され、前記デコーダーが前記トークンを認証することによって、前記ユーザーは空港の保護された境界領域内への進入を許可されるものである。

【請求項１７】

請求項１記載のシステムにおいて、前記クレデンシャルはＡＴＩの手荷物クレデンシャ

ルであり、前記トークンは空港のＡＴＩ搭乗手続き装置で生成され、前記クレデンシャルは前記ユーザーが前記空港で預ける手荷物に取り付けられるものである。
【請求項１８】
ユーザーのためのセキュリティークレデンシャルを生成する設定ワークステーションであって、
少なくとも１つのバイオメトリック入力装置と、
少なくとも１つのトークンインターフェース装置と、
バイオメトリック識別子をバイオメトリックキーに変換するように動作可能な変換ソフトウェアと、
暗号化アルゴリズムを用いた暗号化ソフトウェアと
を有し、
前記バイオメトリック入力装置はユーザーからバイオメトリック識別子を受け取り、前記変換ソフトウェアは前記バイオメトリック識別子をバイオメトリックキーに変換し、前記暗号化ソフトウェアは前記暗号化アルゴリズムおよび前記バイオメトリックキーを適用してデータを暗号化してトークンを形成し、前記トークンインターフェース装置は前記トークンを前記クレデンシャルに転送するものである
設定ワークステーション。
【請求項１９】
請求項１８記載のワークステーションにおいて、前記ワークステーションは少なくとも１つの利用許可キーへアクセスし、前記暗号化ソフトウェアは前記暗号化アルゴリズムおよび前記利用許可キーを適用してデータ区画内の前記データの少なくとも一部を暗号化し、次に、前記暗号化アルゴリズムおよび前記バイオメトリックキーを適用して前記利用許可キーによって暗号化されたデータ区画を暗号化するものである。
【請求項２０】
ユーザーのためのセキュリティークレデンシャルを生成する方法であって、
前記ユーザーからバイオメトリック識別子を受け取る工程と、
前記バイオメトリック識別子をバイオメトリックキーに変換する工程と、
前記バイオメトリックキーに基づいてデータを暗号化してトークンを形成する工程と、
前記トークンを前記クレデンシャルに転送する工程と
を有する方法。
【請求項２１】
請求項２０記載の方法において、この方法は、さらに、
少なくとも１つの利用許可キーにアクセスする工程と、
前記バイオメトリックキーに基づいて前記データを暗号化する前に、前記利用許可キーに基づいてデータ区画内の前記データの少なくとも一部を暗号化する工程と
を有するものである。
【請求項２２】
ユーザーのクレデンシャルのセキュリティートークンを開くデコーダーであって、
トークンインターフェース装置と、
バイオメトリック入力装置と、
暗号化アルゴリズムを用いた解読ソフトウェアと
バイオメトリック識別子をバイオメトリックキーに変換するように動作可能な変換ソフトウェアと
を有し、
前記バイオメトリック入力装置は前記ユーザーからバイオメトリック識別子を受け取り、前記変換ソフトウェアは前記バイオメトリック識別子をバイオメトリックキーに変換し、前記トークンインターフェース装置は前記ユーザーのクレデンシャルから前記トークンを受け取り、前記解読ソフトウェアは前記暗号化アルゴリズムおよび前記バイオメトリックキーを前記トークンに適用して前記トークンを解読することで前記トークンを開くものであって、当該トークンは、前記ユーザーが前記トークンを暗号化するのに使用した前記

バイオメトリック識別子を提示することによってのみ開放可能であり、これにより前記トークンが開くことによって前記ユーザーが認証されるものである
デコーダー。
【請求項２３】
請求項２２記載のデコーダーにおいて、前記トークンは前記データを格納する少なくとも１つのデータ区画を含み、前記データ区画は前記同一または異なる暗号化ソフトウェアによって暗号化され且つ少なくとも１つの利用許可キーに基づいて暗号化されるものであり、前記デコーダーは前記少なくとも１つの利用許可キーへアクセスし、当該デコーダーは、前記トークンを開いた後、前記解読ソフトウェアおよび前記少なくとも１つの利用許可キーを適用して前記データ区画を開くものである。
【請求項２４】
請求項２３記載のデコーダーにおいて、前記トークンの暗号化および前記データ区画の暗号化は前記ユーザーの前記同一または異なるバイオメトリック識別子から生成された少なくとも２つのバイオメトリックキーに基づいており、前記デコーダーは前記同一バイオメトリック識別子または前記異なるバイオメトリック識別子から前記少なくとも２つのバイオメトリックキーを生成するものであって、当該デコーダーは、前記少なくとも１つの利用許可キーへのアクセスを有するものであって、当該デコーダーは、前記バイオメトリックキーのうちの第１のものを用いて前記トークンを開いた後、前記解読ソフトウェア、前記少なくとも１つの利用許可キー、および前記バイオメトリックキーのうちの第２のものを適用して前記データ区画を開くものである。
【請求項２５】
請求項２２記載のデコーダーにおいて、前記トークンは複数のデータ区画を含むものであって、各々のデータ区画は１片または１組の前記データを格納することができ、当該各々のデータ区画が前記同一または異なる暗号化ソフトウェアによって暗号化され且つ複数の利用許可キーのうちの少なくとも１つに基づいて暗号化されるものであり、前記利用許可キーに基づいて暗号化されたデータ区画は前記バイオメトリックキーに基づいて集合的に暗号化されて前記トークンを形成するものである。
【請求項２６】
請求項２２記載のデコーダーにおいて、前記デコーダーは前記利用許可キーのうちの少なくとも１つへアクセスし、当該デコーダーは、前記トークンを開いた後、前記同一または異なる解読ソフトウェアおよびその少なくとも１つの利用許可キーを適用してその少なくとも１つの利用許可キーに対応した前記データ区画を開き、当該デコーダーは、対応する利用許可キーへのアクセスを有さない前記データ区画については何れも開くことができないものである。
【請求項２７】
ユーザーのバイオメトリック識別子に基づいたバイオメトリックキーに基づいて暗号化されたデータを有するセキュリティートークンを用いて前記ユーザーの識別情報を認証する方法であって、
前記ユーザーから前記バイオメトリック識別子を受け取る工程と、
前記バイオメトリック識別子をバイオメトリックキーに変換する工程と、
前記ユーザーのクレデンシャルから前記トークンを受け取る工程と、
前記バイオメトリックキーを使用して前記トークンを解読して前記トークンを開く工程であって、前記トークンは、が前記トークンの暗号化に使用された前記バイオメトリック識別子を提示するユーザーによってのみ開放可能であり、これにより前記トークンを開くことで前記ユーザーが認証されるものである、前記解読し、開く工程と
を有する方法。
【請求項２８】
請求項２７記載の方法において、前記トークンは前記データを格納する少なくとも１つのデータ区画を含み、さらに少なくとも１つの利用許可キーに基づいて暗号化されるものであって、

前記少なくとも１つの利用許可キーにアクセスする工程と、
前記バイオメトリックキーを使用して前記トークンを解読した後、前記少なくとも１つの利用許可キーを使用して前記データ区画を解読する工程と
をさらに有するものである。
【請求項２９】
請求項２８記載の方法において、前記データ区画を解読する工程は、前記少なくとも１つの利用許可キーを使用し、前記ユーザーの前記同一または異なるバイオメトリック識別子から生成された第２のバイオメトリックキーを使用して前記データ区画を解読する工程を含むものである。
【請求項３０】
請求項２７記載の方法において、前記トークンは複数のデータ区画を含むものであって、各々のデータ区画は前記データの一部を格納し、当該各々のデータ区画が複数の利用許可キーの少なくとも１つに基づいて暗号化されているものであって、
前記利用許可キーにアクセスする工程と、
前記バイオメトリックキーを使用して前記トークンを解読した後、前記利用許可キーを使用して前記データ区画を解読する工程と
をさらに有するものである。
【請求項３１】
１若しくはそれ以上のユーザーのための識別認証システムであって、このシステムは、
前記ユーザーのうちの１人に発行された少なくとも１つのクレデンシャルであって、このクレデンシャルは、暗号化アルゴリズムを用いた暗号化ソフトウェアによって暗号化され、さらに前記ユーザーのバイオメトリック識別子から生成されたバイオメトリックキーに基づいて暗号化されたデータを有するセキュリティートークンを含むものである、前記クレデンシャルと、
トークンインターフェース装置と、バイオメトリック入力装置と、ネットワークインターフェース装置とを備え、前記暗号化アルゴリズムを用いた暗号化ソフトウェアへアクセスする少なくとも１つのデコーダーであって、当該バイオメトリック入力装置は前記ユーザーから前記バイオメトリック識別子を受け取り、当該トークンインターフェース装置は前記ユーザーのクレデンシャルから前記トークンを受け取り、当該ネットワークインターフェース装置はＯＴＫを要求してこれを受け取り、当該暗号化ソフトウェアは前記暗号化アルゴリズムおよび前記ＯＴＫを適用して前記トークンおよび前記バイオメトリックキーをパッケージに暗号化し、当該ネットワークインターフェース装置は前記暗号化されたパッケージを送信するものである、前記デコーダーと、
ネットワークインターフェース装置と、ＯＴＫ生成ソフトウェアと、変換ソフトウェアと、暗号化アルゴリズムを用いた解読ソフトウェアとを備えた認証サーバーであって、当該ネットワークインターフェース装置は前記ＯＴＫ要求を受け取り、当該ＯＴＫ生成ソフトウェアは前記ＯＴＫを生成し、当該ネットワークインターフェース装置は前記ＯＴＫを前記デコーダーに送り、前記デコーダーから前記暗号化されたパッケージを受け取り、当該変換ソフトウェアは前記バイオメトリック識別子を前記バイオメトリックキーに変換し、当該解読ソフトウェアは前記暗号化アルゴリズムおよび前記バイオメトリックキーを前記トークンに適用して前記トークンを解読することで前記トークンを開くものであって、当該トークンは、前記ユーザーが前記トークンを暗号化するのに使用した前記バイオメトリック識別子を提示することによってのみ開放可能であり、これにより前記トークンが開くことによって前記ユーザーが認証されるものである、前記認証サーバーと
を有するシステム。
【請求項３２】
請求項３１記載のシステムにおいて、前記トークンは前記データを格納する少なくとも１つのデータ区画を含み、前記データ区画は前記同一または異なる暗号化ソフトウェアによって暗号化され且つ少なくとも１つの利用許可キーに基づいて暗号化されるものであり、前記認証サーバーは前記少なくとも１つの利用許可キーへアクセスし、当該認証サーバ

ーは、前記トークンを開いた後、前記解読ソフトウェアおよび前記少なくとも１つの利用許可キーを適用して前記データ区画を開くものである。
【請求項３３】
請求項３２記載のシステムにおいて、前記トークンの暗号化および前記データ区画の暗号化は前記ユーザーの前記同一または異なるバイオメトリック識別子から生成された少なくとも２つのバイオメトリックキーに基づくものであり、前記認証サーバーは前記同一のバイオメトリック識別子または前記異なるバイオメトリック識別子から前記少なくとも２つのバイオメトリックキーを生成し、前記認証サーバーは前記少なくとも１つの利用許可キーへアクセスし、当該認証サーバーは、前記バイオメトリックキーのうちの第１のものを用いて前記トークンを開いた後、前記解読ソフトウェア、前記少なくとも１つの利用許可キー、および前記バイオメトリックキーのうちの第２のものを適用して前記データ区画を開くものである。
【請求項３４】
請求項３１記載のシステムにおいて、前記トークンは複数のデータ区画を含むものであって、各々のデータ区画は前記データの１片または１組を格納することができ、当該各々のデータ区画が前記同一または異なる暗号化ソフトウェアによって暗号化され且つ複数の利用許可キーのうちの少なくとも１つに基づいて暗号化されるものであり、前記利用許可キーに基づいて暗号化されたデータ区画は前記バイオメトリックキーに基づいて集合的に暗号化されて前記トークンを形成し、前記認証サーバーは前記利用許可キーのうちの少なくとも１つへアクセスし、当該認証サーバーは、前記トークンを開いた後、前記同一または異なる解読ソフトウェアおよびその少なくとも１つの利用許可キーを適用してその少なくとも１つの利用許可キーに対応した前記データ区画を開くものであって、当該認証サーバーは、前記認証サーバーがそれに対応する利用許可キーへのアクセスを有さない前記データ区画については何れも開くことができないものである。
【請求項３５】
請求項３１記載のシステムにおいて、前記クレデンシャルはゲーム用のクレデンシャルでり、前記トークンはユーザーの身分証明およびバンクカード情報を含むものである。
【請求項３６】
請求項３１記載のシステムにおいて、前記クレデンシャルはネットワークアクセスのクレデンシャルであり、前記トークンはユーザーの身分証明情報を含むものである。
【請求項３７】
ユーザーのクレデンシャルのセキュリティートークンを開く認証サーバーであって、
ネットワークインターフェース装置と、
ＯＴＫを生成するように動作可能な生成ソフトウェアと、
バイオメトリック識別子をバイオメトリックキーに変換するように動作可能な変換ソフトウェアと、
暗号化アルゴリズムを用いた解読ソフトウェアと
を有し、
前記ＯＴＫ生成ソフトウェアはＯＴＫを生成し、前記ネットワークインターフェース装置は前記ＯＴＫをデコーダーに送り、前記デコーダーから暗号化されたパッケージを受け取り、前記変換ソフトウェアは前記バイオメトリック識別子を前記バイオメトリックキーに変換し、前記解読ソフトウェアは前記暗号化アルゴリズムおよび前記バイオメトリックキーを前記トークンに適用して前記トークンを解読することで前記トークンを開くものであって、当該トークンは、前記ユーザーが前記トークンを暗号化するために使用した前記バイオメトリック識別子を提示することによってのみ開放可能であり、これにより前記トークンが開くことによって前記ユーザーが認証されるものである
認証サーバー。
【請求項３８】
請求項３７記載のデコーダーにおいて、前記トークンは前記データを格納する少なくとも１つのデータ区画を含み、前記データ区画は前記同一または異なる暗号化ソフトウェア

によって暗号化され且つ少なくとも１つの利用許可キーに基づいて暗号化されるものであり、前記認証サーバーは前記少なくとも１つの利用許可キーへのアクセスを有するものであって、当該認証サーバーは、前記トークンを開いた後、前記解読ソフトウェアおよび前記少なくとも１つの利用許可キーを適用して前記データ区画を開くものである。

【請求項３９】

ユーザーのバイオメトリック識別子に基づいたバイオメトリックキーに基づいて暗号化されたデータを有するセキュリティートークンを用いて前記ユーザーの個人情報を認証する方法であって、

デコーダーからＯＴＫの要求を受け取る工程と、

前記ＯＴＫを生成し、それを前記デコーダーに送る工程と、

前記デコーダーから前記トークンと前記バイオメトリックキーとを含んだ、前記ＯＴＫに基づいて暗号化されたパッケージを受け取る工程と、

前記ＯＴＫを使用して前記暗号化されたパッケージを解読して前記トークンおよび前記バイオメトリック識別子にアクセスする工程と、

前記バイオメトリック識別子を前記バイオメトリックキーに変換する工程と、

前記バイオメトリックキーを使用して前記トークンを解読して前記トークンを開く工程であって、当該トークンは、前記ユーザーが前記トークンを暗号化するために使用した前記バイオメトリック識別子を提示することによってのみ開放可能であり、これにより前記トークンが開くことによって前記ユーザーが認証されるものである、前記開く工程と

を有する方法。

【請求項４０】

請求項３９記載の方法において、前記トークンは、前記データが格納された、少なくとも１つの利用許可キーに基づいて暗号化された少なくとも１つのデータ区画を含むものであって、

前記少なくとも１つの利用許可キーにアクセスする工程と、

前記バイオメトリックキーを使用して前記トークンを解読した後、前記少なくとも１つの利用許可キーを使用して前記データ区画を解読する工程と

をさらに有する方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本願は、２００８年５月１日付けで出願された米国特許仮出願第６１／０４９，６１３号、２００７年１１月１２日付で出願された米国特許仮出願第６０／９８７，３１２号、および２００７年７月１２日付で出願された米国特許仮出願第６０／９４９，２８２号に対して優先権を主張するものであり、この参照によりその範囲および内容の全てが本明細書内に組み込まれるものである。

【０００２】

本発明は識別認証システムに関し、特に、ユーザーの識別情報を認証し、認証されたユーザーに保護された情報および／または領域へアクセスすることを許可するシステムおよび方法に関する。

【背景技術】

【０００３】

現在、なりすまし犯罪が非常に大きな問題となっている。ほとんどの人がなりすまし犯罪を金融関連のなりすまし犯罪、例えば、クレジットカードの口座番号および／または社会保障番号を盗んで不当な購入を行うこととして捉えている。これがなりすまし犯罪事件全体のかなりの部分を占めるものの、医療、保険、境界、およびネットワーク（またはコンピューター／電子）に関するなりすまし犯罪を含む、その他多くの種類のなりすまし犯罪が存在する。医療および保険に関するなりすまし犯罪では、ある人物の医療および保険情報がそれぞれアクセスされ、利用許可のない者によって悪用されることがある。境界に関するなりすまし犯罪では、制限区域へのアクセスを得る目的で個人識別情報が盗まれる

（空港、原子力発電所、自治体の給水設備などについては特に重要な問題である）。そして、ネットワークに関するなりすまし犯罪は、軍または企業のコンピューターネットワークなどのコンピューターシステムへの不当なアクセスを得る目的でのユーザーの識別情報の盗難にかかわる。

【０００４】

現存の識別情報セキュリティーの技術は、識別認証の欠如という重大な問題に悩まされている。米国政府は、識別認証システムのセキュリティーの強健性の格付けとして「厳密認証」という言葉を使用している。識別認証システムが以下の認証記号のうちの少なくとも２つを使用する場合、厳密認証システムとして格付けされる：（１）前記ユーザーが有するもの（セキュリティートークン、運転免許証、クレジットカード、デビット／キャッシュカード、スマートカード、許可証、キーフォブなど）、（２）前記ユーザーが知っていること（パスワード、ＰＩＮ、郵便番号など）、および（３）前記ユーザーであること（署名、指紋、ＤＮＡなど）。これら認証記号の２つ、または、さらには３つ全てを有することは認証を強健にするように思えるが、現実には、これら全てまたはほとんどの認証記号はセキュリティー侵害されることがある。そして実際には、これらの１若しくはそれ以上は往々にして全く使用されていないことさえある。例えば、クレジット・カード・サービスは前記ユーザーが有するクレジットカード（認証記号１）および前記ユーザーの署名（認証記号３）を使用していたので、初めのうちは厳密認証の必要条件を満たしていた。しかし現在の実用上、クレジットカード決済中に前記ユーザーの署名を確認することは稀であり、クレジットカード会社は、実際に、これによって彼らのカードの使用の迅速性および利便性が向上することを宣伝している。

【０００５】

識別情報セキュリティーの向上を提供する目的でバイオメトリック識別子を使用した識別認証システムが開発されている。しかし、最新かつ最良のバイオメトリック識別認証システムでさえセキュリティー侵害を受けやすい。これらのセキュリティーは、中央に位置するデータベースまたは個別のトークン上に格納されたバイオメトリック識別子のファイルへのアクセスの制限に依存する。前記中央のデータベース上のバイオメトリック識別子のファイルの格納は、前記データベースが窃盗犯（即ちハッカー）にとって重要な標的となるなどの明らかな問題をもたらす。そして、前記バイオメトリック識別子のファイルが前記トークン上に格納される場合、前記バイオメトリック識別子のファイルが多数の個別のトークンの間に分散されていても、前記トークンはやはりハッキングされやすい。これは、従来のトークン式システムが、トークン上のバイオメトリック識別子のファイルをアクセスし、ユーザーによって入力されたバイオメトリック識別子を受け取り、比較を実行して前記ユーザーの識別情報を認証するトークンリーダーを含むからである。前記リーダーは前記トークン上のバイオメトリック識別子のファイルにアクセスする機能を有する必要があるので、前記窃盗犯はそこを攻撃する。１つのリーダーをハッキングして１つのトークンへのアクセスを得ることで全てのトークンへのアクセスを得る。単に前記トークン上に格納されたバイオメトリック識別子のファイルを前記窃盗犯のそれと取り替えるだけで、前記ユーザーの識別情報の窃盗が完了する。

【０００６】

従って、機密情報および保護区域へのアクセスの保護の改善、特に前記機密情報または前記アクセスが制限された場所へのアクセスを得ようとしている個人の識別情報の認証の改善が必要であることが分かる。本発明は、主に、これらおよびその他の必要性に合致する解決策を提供することを目的とする。

【発明の概要】

【課題を解決するための手段】

【０００７】

概述すれば、本発明は、ユーザーの識別情報を認証し、場合によっては認証されたユーザーに保護されたデータまたは区域へのアクセスを許可するシステム、構成要素、および方法を提供する。前記識別認証システムは、セキュリティートークンとデコーダーとを含

む。前記トークンは、そのトークンの利用許可されたユーザーに固有のバイオメトリック識別子に基づいて暗号化されたデータを含む。この暗号化の設定ワークステーションおよび方法が提供される。ユーザーは、ローカルまたはリモート復号化用の前記デコーダーのうちの１つにトークンおよびバイオメトリック識別子を提示する。変換ソフトウェアを使用して前記バイオメトリック識別子を固有のバイオメトリックキーに変換し、解読ソフトウェアを使用して前記バイオメトリックキーを前記トークンに適用して前記トークンを開く。このようにすれば、前記利用許可されたユーザーのみが前記トークン上のデータをアクセスできる。そして、前記ユーザーおよび前記トークンは中央またはローカルに格納されたバイオメトリック識別子のファイルへのアクセス、および／または前記入力されたバイオメトリック識別子との比較の実行を必要とせずに認証される。

【０００８】

第１の例のシステムおよび方法において、前記デコーダーは前記変換ソフトウェアおよび前記解読ソフトウェアを格納し、前記解読／認証は前記デコーダー上でローカルに行われる。第２の例のリモート認証のためのシステムおよび方法において、前記システムは、さらに、認証サーバーを含む。この実施形態において、前記デコーダーは前記サーバーからワン・タイム・キーを検索し、前記トークンおよび前記バイオメトリック識別子を収集し、それらを一緒にパッケージとして暗号化し、前記暗号化されたパッケージを前記サーバーに送って前記認証処理を実行する。および第３の実施例において、前記トークンは第１のＯＴＫに基づいて暗号化され、前記トークンおよびバイオメトリック識別子は第２のＯＴＫに基づいてパッケージに暗号化され、前記認証サーバーに送られて認証処理される。認証が無事に完了すると、前記認証サーバーが前記第１のＯＴＫを前記装置に送って前記トークンを開く。

【０００９】

幾つかの「認証のみ」の実施形態において、前記トークンを開く目的は単に前記ユーザーおよび前記トークンを認証することである。従って、前記トークンに格納されたデータは特に重要ではないかもしれない。他の「認証のみ」の実施形態において、前記データは、前記ユーザーが認証された後で使用されるユーザー情報、セキュリティー許可レベル情報（または認証データ）などを含む。および幾つかの「保護されたデータ」の実施形態において、前記トークンを開く目的は、前記ユーザーおよび前記トークンを認証することであり、さらに前記トークン内で保護されたデータにアクセスすることである。

【００１０】

さらに、幾つかの実施形態において、データ片またはデータのセットは、利用許可キー（オーソリティキー）に基づいて暗号化され解読される指定されたデータ区画内に格納される。前記利用許可キーは、デコーダーまたは認証サーバーが開くことを許可された前記データ区画に対応した利用許可キーのみにアクセスを有するデコーダーまたは認証サーバー上に格納される。データ区画のセットは、単一の利用許可キーに基づいて集合的に暗号化／解読できるが、通常、各データ区画はその独自の利用許可キーに基づいて暗号化／解読される。このようにすれば、各データ片は、そのデータ区画が利用許可キーに基づいて暗号化されるときに１度、および前記データ区画の全て（前記トークン全体）が前記トークンを生成するバイオメトリックキーに基づいて集合的に暗号化されるときに１度の２度暗号化される。

【００１１】

さらに、幾つかの実施形態において、前記トークンは、同一のまたは異なるバイオメトリック識別子に基づいてもよい２若しくはそれ以上のバイオメトリックキーに基づいて暗号化される。これらの実施形態のいくつかにおいて、前記トークンは、各工程が異なるバイオメトリックキーを使用する複数工程の処理において暗号化／解読される。さらに他の幾つかの実施形態において、前記トークンは１つのバイオメトリックキーに基づいて暗号化／解読され、前記データ区画は、（前記利用許可キーによる暗号化／解読に加えて、またはその代わりに）同一のまたは異なるバイオメトリックキーに基づいて暗号化／解読される。および他の幾つかの実施形態において、前記トークンの暗号化／解読アルゴリズム

は、バイオメトリック識別子に基づいて選択される。

【００１２】

本発明によって用いられる、従来のシステムおよび方法の欠点を改善し、本明細書内に説明した利点を達成する特定の技術および構造は、以下の本発明の実施例の詳細な説明および添付の図面および請求項から明白となるであろう。

【図面の簡単な説明】

【００１３】

【図１】図１は、デコーダーおよび３つのクレデンシャルを示す、本発明の第１の実施例による識別認証システムのブロック図である。

【図２】図２は、図１のクレデンシャルのうちの１つおよびデコーダーの概念ブロック図であって、クレデンシャルのトークンの１つのデータ区画のみを開く利用許可キーを有するデコーダーを示す。

【図３】図３は、図２のクレデンシャルおよびデコーダーの概念ブロック図であって、クレデンシャルのトークンの全てのデータ区画を開く別の利用許可キーを有するデコーダーを示す。

【図４】図４は、図１の識別認証システムのトークン設定ワークステーションのブロック図である。

【図５】図５は、図４のトークン設定ワークステーションを使用した、トークン設定方法のフロー図である。

【図６】図６は、図５の設定方法のトークン生成方法のフロー図である。

【図７】図７は、図１のデコーダーを使用したローカルトークン開放方法のフロー図である。

【図８】図８は、デコーダーと、クレデンシャルと、リモート認証サーバーとを示す、本発明の第２の実施例による識別認証システムのブロック図である。

【図９】図９は、図８のデコーダーを使用したリモートトークン開放方法のフロー図である。

【図１０】図１０は、図８の認証サーバーを使用したリモートトークン開放方法のフロー図である。

【発明を実施するための形態】

【００１４】

本発明は、セキュリティートークンおよびトークンデコーダーを使用した識別認証システムおよび方法を提供する。前記トークンの各々は、そのトークンの利用許可されたユーザーのバイオメトリック識別子に基づいて固有に暗号化されている。本明細書内で使用されるとき、「ユーザー」という語は認証過程にある個人を意味する。前記デコーダーは前記トークンおよび前記ユーザーのバイオメトリック識別子を入力として受け取る。次に、前記デコーダーは前記ユーザーのバイオメトリック識別子をバイオメトリックキーに変換し、前記バイオメトリックキーを適用して前記固有に暗号化されたトークンを解読することで前記トークンを開く。このようにすれば、前記システムは、前記ユーザーが有するもの（トークン）および前記ユーザーであること（バイオメトリック識別子）を使用することによって厳密認証の基本的な基準を満たす。さらに、前記システムは、前記ユーザーによって提示されたバイオメトリック識別子を前記ユーザーのトークンまたは中央に位置するデータベース内に格納されたバイオメトリック識別子と比較することによって識別情報を認証する従来のバイオメトリック識別認証システムからの根本的な離脱を提示する。しかし、本発明によるシステムは、このような比較を実行せず、従ってそもそも前記ユーザーのバイオメトリック識別子を格納する必要がない。その代わりに、前記ユーザーによって提示されたバイオメトリック識別子は、前記トークンを解読／開放するバイオメトリックキーに変換される。このようにすれば、前記システムは、現存の識別認証システムが有する潜在的な攻撃点を含まないので、真に安全である。

【００１５】

ここで図面の図を参照して、本発明によるシステム、その構成要素、および方法の実施

例を説明する。図１～４は、本発明の第１の実施例による識別認証システム１０を示す。図１に示すように、前記システム１０は、少なくとも１つのクレデンシャルと少なくとも１つのデコーダーとの、少なくとも２つの構成要素を含む。明瞭性および図示のために、図示した前記システム１０は、１つのデコーダー１４と、３つのクレデンシャル１２ａ～ｎ（時によって、個別に「クレデンシャル１２」として、および集合的に「クレデンシャル１２」として参照する）とを含む。通常の商用の実施形態において、前記システム１０は、例えば一人に１つの複数の前記クレデンシャル１２と、例えば識別認証が所望される各特定の場所に１つの複数の前記デコーダー１４とを含む。含まれる構成要素の数に拘らず、この実施形態の前記システム１０は、前記ユーザーが物理的に前記デコーダー１４のうちの１つと同一の場所にいる用途において使用するように設計されている。これらの用途において、前記識別認証は、例えば店頭（ｐｏｉｎｔ－ｏｆ－ｓａｌｅ：ＰＯＳ）の場所、保護された境界のアクセスポイント、航空会社の乗客搭乗ゲートなどで「ローカルに」行われると表現される。

【００１６】

前記クレデンシャル１２ａ～ｎは、セキュリティートークン１６ａ～１６ｎ（時によって、個別に「トークン１６」として、および集合的に「トークン１６」として参照する）をそれぞれ格納する。本明細書内で使用されるとき、「トークン１６」という語は暗号化されたデータファイルを意味する。前記クレデンシャル１２は、任意数の異なる形態で提供することのできる物理的対象である。例えば通常の商用の実施形態において、前記クレデンシャル１２はプラスティック（例えば塩化ビニル（ｐｏｌｙｖｉｎｙｌ ｃｈｌｏｒｉｄｅ：ＰＶＣ））カード、航空会社の搭乗券、セキュリティーパス、スマートカード、携帯電話、携帯情報端末（ｐｅｒｓｏｎａｌ ｄｉｇｉｔａｌ ａｓｓｉｓｔａｎｔｓ：ＰＤＡｓ）、ユニバーサル・シリアル・バス（ｕｎｉｖｅｒｓａｌ ｓｅｒｉａｌ ｂｕｓ：ＵＳＢ）サムドライブ、メモリースティック、電子キーフォブ、１回書き込み装置、書換え可能装置、および／またはその他の携帯型電子装置である。

【００１７】

前記クレデンシャル１２ａ～ｎは、それぞれ、前記トークン１６ａ～ｎを格納するデータ記憶装置１８ａ～ｎ（時によって、個別に「記憶装置１８」として、および集合的に「記憶装置１８」として参照する）を含む。例えば航空会社の搭乗券または何らかのプラスティックカード（キーフォブのサイズのカードなど）によって提供されるクレデンシャル１２について、前記記憶装置１８は、印刷されたバーコードなどの光学的に走査可能な媒体であってもよい。例えばクレデンシャル１２はその他何らかのプラスティックカード（財布に収納可能なサイズのカードなど）により提供され、前記記憶装置１８は磁気ストライプなどの磁気的に走査可能な媒体であってもよい。そして、例えば携帯電話、ＰＤＡ、電子キーフォブ、スマートカード、ＵＳＢサムドライブ、およびメモリースティックなどの携帯型電子装置によって提供されるクレデンシャル１２について、前記記憶装置１８は、メモリーチップ、フラッシュメモリー装置、磁気または光ドライブなどのプロセッサー可読メモリー装置であってもよい。

【００１８】

また、このような携帯型電子装置のクレデンシャル１２は、前記デコーダー１４と通信する従来の短距離無線通信の構成要素を含んでもよい。例えば、前記クレデンシャル１２は各々、前記トークン１６をデコーダー１４に送信する送信機と、アンテナと、コントローラーとを含んでもよい。または、前記クレデンシャル１２は、送信機の代わりに、前記クレデンシャルの設定時の前記トークン１６の受信、前記認証後の更新されたトークンの受信などもする送受信機を含んでもよい。

【００１９】

前記クレデンシャル１２が携帯電話、ＰＤＡ、またはその他の携帯無線通信装置である実施形態において、前記クレデンシャルの既存の無線通信構成要素を使用して前記デコーダー１４と通信してもよく、または前記クレデンシャルは、前記デコーダーと通信する別個の専用無線通信構成要素を含んでもよい。さらに、前記デコーダー１４と通信する無線

通信構成要素を有する前記クレデンシャル１２は、ブルートゥース、ジグビー、無線ＬＡＮ、近距離無線通信（Ｎｅａｒ Ｆｉｅｌｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎ：ＮＦＣ）、ＴＣＩＰなどの通信プロトコル、または別の無線通信技術を用いて設定してもよい。

【００２０】

上述のように、前記クレデンシャル１２の記憶装置１８によって格納された前記トークン１６は、暗号化されたデータファイルである。前記データファイルは、バイオメトリックキーに基づいて固有に暗号化され、次に前記クレデンシャル１２のユーザーに固有のバイオメトリック識別子に基づいて暗号化される。前記システム１０は、指紋、手形、光彩、顔の特徴、声紋、ＤＮＡ、それらの組み合わせ、および／またはその他任意の固有な物理的または行動的な人間的特性を含むバイオメトリック識別子を使用するようにできる。具体的には、前記システム１０は、そのための入力装置２０を提供可能な任意のバイオメトリック識別子と、入力された前記バイオメトリック識別子をバイオメトリックキーに変換する変換ソフトウェア２２とを使用するようにできる。下記の通り、前記バイオメトリック識別子入力装置２０および前記変換ソフトウェア２２は、前記デコーダー１４に動作可能に接続され、または一体化している。本明細書内で使用されるとき、「バイオメトリックキー」という語は、バイオメトリック識別子から生成され、前記データファイルを暗号化して前記トークン１６を形成し、前記トークンを解読することで前記トークンを開くように使用できる、固有の反復文字列（例えば、数字、文字、英数字の組み合わせ、その他の記号、特徴、または特殊記号の列、またはそれらの組み合わせ）を意味する。即ち、バイオメトリックキーは、固有のバイオメトリック識別子の固有なデジタル表現である。

【００２１】

指紋スキャナー、手形スキャナー、光彩スキャナー、顔スキャナー、音声レコーダー、およびＤＮＡサンプリング装置などの市販のバイオメトリック入力装置を使用して、それぞれ指紋、手形、光彩、顔の特徴、声紋、およびＤＮＡサンプルなどのバイオメトリック識別子を入力することができる。さらに、走査入力した指紋を前記バイオメトリックキーとして使用できる固有の反復数字列に変換する市販（例えば、カリフォルニア州Ｍｏｕｎｔａｉｎ Ｖｉｅｗ市のＧＥＮＫＥＹ社から）の変換ソフトウェアが存在する。当業者であれば、この変換ソフトウェアを、光彩、顔の特徴、および声紋など、その他の入力されたバイオメトリック識別子を前記バイオメトリックキーとして使用できる固有の反復文字列に変換するようにでき、またはそのようにする他の変換ソフトウェアを提供できることを理解するであろう。従って、現存する技術を使用して、前記システム１０を少なくとも入力した指紋、光彩、顔の特徴、および／または声紋を前記バイオメトリック識別子として使用するように構成することができる。さらに、現存の技術を使用して、前記システム１０がその他の入力されたバイオメトリック識別子（ＤＮＡおよびその他固有の物理的または行動的な人間的特性など）のバイオメトリックキーへの変換を提供するようにすることは、十分に当業者の能力の範囲内であると考えられる。

【００２２】

前記トークン１６内の暗号化されたデータは、前記特定の用途に関連する任意の種類の情報であってよい。例えば、前記暗号化されたデータには、前記クレデンシャル１２がデジタル化された運転免許証である用途での特定ユーザーの情報と、前記クレデンシャルが保護された境界へのアクセスカードである場合の特定用途情報と、前記トークンがユニバーサルＩＤカードである用途での特定ユーザーおよび特定用途の情報とが含まれる。もしくは、前記暗号化されたデータは、認証のみの用途において前記ユーザーまたは前記用途に特定ではない情報（例えばランダムなデータ片）を含んでもよい。認証のみの用途においては、前記クレデンシャル１２の提示者が前記クレデンシャルに登録された人であることを証明することだけが所望される（その他一切の目的では、前記データへのアクセスを保護し、または使用する必要がない）。さらに、前記トークン１６内の暗号化されていない追加のデータは保護されていないにも拘らず、前記記憶装置１８は、このような追加のデータを格納することができる。前記全ての情報を中央のデータベースではなく前記クレデンシャル１２上に格納することによって、各個別のクレデンシャルの価値が低減し、単

一攻撃点（中央のデータベース）が排除される。

【００２３】

前記クレデンシャル１２上で１片または１組のデータのみが保護されている用途において、前記トークン１６を暗号化されたその１片または１組のデータで構成してもよい。この構成は、前記保護されたデータのセットが前記ユーザーの個人情報（名前、住所、誕生日（ｄａｔｅ　ｏｆ　ｂｉｒｔｈ：ＤＯＢ）、社会保障番号（ｓｏｃｉａｌ　ｓｅｃｕｒｉｔｙ　ｎｕｍｂｅｒ：ＳＳＮ）など）および金融情報（前記クレジットカード口座番号、有効期限など）を含む、クレジットカードなどの用途に好適である。

【００２４】

複数のデータ片または複数組のデータが保護されている用途において、前記トークン１６ａ～ｎは、複数のデータ区画２４ａ～ｎ（時によって、個別に「データ区画２４」として、および集合的に「データ区画２４」として参照する）を含む。本明細書内で使用するとき、「データ区画」２４は、前記トークンの暗号化に加えて追加的に暗号化されたデータを収容する、前記トークン１６内のデジタル記憶場所を意味する。各データ区画２４は、相互のデータ区画から独立して固有に暗号化される。これによって、特定のデコーダー１４（下記の通りに正しく認証されたもの）のみが特定のデータ区画２４にアクセスすることができる。この構成は、前記保護されたデータが前記ユーザーの個人情報と、金融情報と、医療履歴とを含む、ユニバーサルＩＤカードなどの用途に好適である。

【００２５】

前記データ区画２４の各々は利用許可キー（オーソリティキー）２６に基づいて固有に暗号化され、前記トークン１６全体（即ち、前記データ区画の全て）は前記バイオメトリックキーに基づいて暗号化される。本明細書内で使用されるとき、「利用許可キー」という語は、固有の利用許可レベルに対応し、前記データ区画２４を暗号化し解読することに使用できる固有の文字列（例えば、数字、文字、英数字の組み合わせ、その他の記号、特徴、または特殊記号の列、またはそれらの組み合わせ）を意味する。下記の通り、前記利用許可キー２６は前記デコーダー１４に格納される。

【００２６】

前記利用許可レベルは、特定の用途における特定のデコーダー１４によってアクセスする必要のある前記トークン１６内の前記特定のデータに基づき、これらは実際には必ずしも階層的ではない。各データ区画２４は少なくとも２つのキーで暗号化されるので（そのデータ区画のための少なくとも１つの利用許可キー２６および全ての前記データ区画のための少なくとも１つのバイオメトリックキー）、たとえデコーダー１４をハッキングしてその中に格納された利用許可キーを取得しても、前記ハッカーは一切のトークン１６の一切のデータ区画を開くことはできない。このようにすれば、各データ区画２４は、完全に固有に暗号化され、（正しい前記利用許可キー２６を有する）利用許可されたデコーダー１４を使用する（前記正しいバイオメトリックキーを有する）前記利用許可されたユーザーによってのみアクセスできる。

【００２７】

例えば、図２および図３は前記クレデンシャル１２が運転免許証の情報を格納するＰＤＡ型携帯電話であるデジタル化された運転免許証の用途を示している。各データ片はその独自のデータ区画２４ａ～ｎ内に格納され、各データ区画はその独自に固有の利用許可キー２６に基づいて暗号化され、前記データ区画の全て（即ちトークン１６）は前記利用許可されたユーザーに固有のバイオメトリックキーに基づいて集合的に暗号化される。前記データ区画２４ａ～ｎ内に格納されたデータは、従来の運転免許証のデータと同一であり、例えば、前記ユーザーの名前、住所、性別、誕生日、年齢、身長、および体重、その運転免許証番号、免許交付の州などである。前記ユーザーの写真さえも前記データ区画２４のうちの１つに格納できるが、前記クレデンシャル１２が異なる種類の認証記号３（前記ユーザーであること）即ちバイオメトリック識別子を提示する前記ユーザーによって認証されているので、これは不要である。

【００２８】

図２に示すように、前記ユーザーが前記デジタル化された運転免許証のクレデンシャル１２を小売店のデコーダー１４に提示し、事前に選択されたバイオメトリック識別子を前記デコーダーのバイオメトリック入力装置４０に提示して制限された購入（例えばアルコール飲料の購入）のために年齢を確認するとき、３つのことが起こる。前記クレデンシャル１２が認証される。前記バイオメトリックキーが前記トークン１６を開くと、前記トークンが前記正しい暗号アルゴリズムを使用して生成されたことが示されているので、次に前記クレデンシャルが認証される。（前記トークン１６の生成および前記デコーダー１４の構成の詳細は下記に提供する。）前記ユーザーが前記クレデンシャル１２上のデータをアクセスする権利が認証される。前記固有のバイオメトリックキーは前記固有のユーザーに由来するので、前記トークン１６を開く前記バイオメトリックキーもまた前記ユーザーを認証する。そしてこれら両方に間違いがない場合、次に前記ユーザーの年齢が確認される。前記クレデンシャル１２および前記バイオメトリック識別子の提示によって厳密認証が達成されると、次に前記小売店のデコーダー１４がその利用許可キーおよび（入力された前記バイオメトリック識別子に基づいて前記小売店のデコーダー１４が生成した）前記バイオメトリックキーを使用して前記トークン１６の誕生日のデータ区画を開き、これを読む。前記データ区画２４のうちの１つ（前記誕生日を格納したもの）のみが開く。この小売店のデコーダー１４では、その他のデータ区画２４、即ち前記ユーザーの名前、住所などを格納したものはアクセスできない。このデコーダー１４の許可された用途は年齢の確認であってそれ以外の目的ではないので、このデコーダー１４は前記誕生日のデータ区画のみを開きそれ以外を開かない利用許可キーで設定されている。

【００２９】

しかし、図３に示すように、警察官によって使用されるデコーダー１４は、図示された１２個のデータ区画２４の全てにアクセスするように複数の（例えば１２個の）利用許可キーで設定される。従って、同一の運転免許証のクレデンシャル１２が警察官に提示されたとき、彼のデコーダー１４は前記運転免許証のデータの全てを格納する前記データ区画２４の全てにアクセスする利用許可を有する。

【００３０】

その他の用途において、前記クレデンシャル１２は、個別のデータ区画２４内に前記ユーザーの名前および住所、前記クレジットカード番号、前記クレジットカードの有効期限などを格納したクレジットカードとして設定される。この用途のデコーダー１４は、クレジットカードの支払いを処理する用途に設定される。これらデコーダー１４は、前記クレジットカードの決済を処理するために必要なデータを格納するデータ区画２４にアクセスするために必要な利用許可キーを格納し、それ以外の利用許可キーは格納しない。

【００３１】

そしてクレデンシャル１２が複数の用途向けに設定された用途（例えば、個人の身分証明、クレジットカードによる購入、医療履歴など用のユニバーサル個人認証カード）において、格納された各データ片またはデータのセットは固有の利用許可レベルによって暗号化される。従って、前記警察官のデコーダーおよび前記小売店のデコーダーは前記医療履歴のデータ区画を開く利用許可キーを有さない。

【００３２】

通常の商用の実施形態において、各データ区画２４は１片のデータを格納し、利用許可キーで固有に暗号化される。特定のデータ片にアクセスすることを許可された前記デコーダー１４は、それに対応した、その１片のデータを格納する前記データ区画２４を開く利用許可キーを格納する。従って、１片のデータのみへのアクセスを必要とする用途において、前記許可されたデコーダー１４は、それに対応した、その必要な１片のデータを格納する前記データ区画２４を開く利用許可キーのみを格納する。そして、複数のデータ片にアクセスする必要のある用途において、前記許可されたデコーダー１４は、それに対応する、必要な前記データ片の全てを格納する前記データ区画２４の全てを開く利用許可キーの全てを格納する。

【００３３】

複数のデータ片にアクセスする必要のある用途の別の実施形態において、各データ区画２４は、複数のデータ片（即ち１組のデータ）を格納し、利用許可キーで固有に暗号化される。従って、例えば、前記データ区画２４のうちの１つが運転免許証のデータを格納し、別の１つがクレジットカードのデータを格納し、もう１つが医療データを格納する。クレジットカードのデータにアクセスする必要のある前記デコーダー１４は、それに対応した、そのデータ区画２４を開く利用許可キーを有するが、前記ユーザーの全ての医療履歴を格納するデータ区画を開く前記利用許可キーを有さないこととなる。この実施形態において、同一のデータ片（例えば前記ユーザーの名前および住所）を複数のデータ区画２４内に格納できる。

【００３４】

複数のデータ片にアクセスする必要のある用途のもう１つの別の実施形態において、各データ区画２４は、単一のデータ片を格納し、（特定の用途のために必要な前記データの全てを集合的に格納する）前記データ区画のうちの１組は、単一の利用許可キーで一緒に暗号化される。前記利用許可キーは、その用途のために利用許可されたデコーダー１４に格納される。勿論、前記データ区画２４は、当業者によって理解されるその他の方法で構成して複数のデータ片を格納し、それらへのアクセスを提供することができる。

【００３５】

前記デコーダー１４の詳細に至る前に、トークン設定装置および前記トークン１６の設定方法について説明する。前記設定装置は、専用ワークステーションまたはその他のプロセッサーを用いた電子装置によって提供でき、またはその構成要素を前記デコーダー１４の幾つかまたは全ての中に組み込んで１種類の装置のみを提供すればよいようにすることができる。

【００３６】

図４に、前記識別認証システム１０のトークン設定ワークステーション２８を示す。前記ワークステーション２８は、少なくとも１つのバイオメトリック入力装置２０と、少なくとも１つのユーザーインターフェース装置３２と、少なくとも１つのトークンインターフェース装置３４と、プログラムされたプロセッサー３０とを含む。通常の商用の実施形態において、前記ワークステーション２８は、固定媒体データ記憶装置（例えば磁気ディスク装置）と、交換型媒体データ記憶装置（例えばＣＤ－ＲＯＭまたはＤＶＤドライブ）と、および／またはコンピューターワークステーション内で一般的に使用されるその他の構成要素（明瞭性の目的で図示せず）とを含む。本明細書内では、「ワークステーション」という語は、広義で使用され、汎用コンピューター、コンピューターキオスクなどを含む。前記設定装置２８に動作可能に（例えば無線でまたは配線によって）接続される周辺装置として、前記バイオメトリック入力装置２０と、前記ユーザーインターフェース装置３２と、前記トークンインターフェース装置３４とを提供してもよく、またはそれらを前記設定装置に一体化した構成要素としてもよい。

【００３７】

上述の通り、前記バイオメトリック入力装置２０は、指紋スキャナー、手形スキャナー、光彩スキャナー、顔の特徴スキャナー、音声レコーダー、ＤＮＡサンプリング装置、または別の従来の装置（例えばカメラ、ソナー、または赤外線装置）によって提供して、バイオメトリック識別子を収集してもよい。具体的には、前記バイオメトリック装置２０は、前記バイオメトリック識別子のデジタルテンプレートを生成することによって前記バイオメトリック識別子を受け取る。本明細書内で使用される「デジタルテンプレート」という語は、前記バイオメトリック識別子に由来し、前記バイオメトリック識別子に固有のデジタル表現を意味する。幾つかのバイオメトリック入力装置２０について、前記デジタルテンプレートは前記バイオメトリック識別子に視覚的に（または別の点で）似ているが、これは前記システム１０が正常に機能するためには必要ではない。好適な指紋スキャナー、手形スキャナー、光彩スキャナー、顔の特徴スキャナー、音声レコーダー、およびＤＮＡサンプリング装置が多くの業者から市販されている。前記設定ワークステーション２８を使用して１より以上の種類のバイオメトリック識別子に基づいて前記トークン１６を暗

号化する用途について、前記ワークステーションには、例えば指紋スキャナーと光彩スキャナーとのような１より以上の種類のバイオメトリック入力装置２０を提供してもよい。

【００３８】

前記ユーザーインターフェース装置３２には、通常、１若しくはそれ以上の入力装置と１若しくはそれ以上の出力装置とが提供される。前記入力装置は、例えばタッチスクリーン、手書き入力画面、キーパッド、キーボード、データ入力ボタン、ポインティング装置（例えばマウス）、磁気ストライプリーダー、および／または光学式スキャナーであってもよい。そして、出力装置は、例えば、タッチスクリーン、表示画面、スピーカー、および／または表示灯であってもよい。

【００３９】

前記ワークステーション２８を設定するために選択された前記トークンインターフェース装置３４は、特定の用途で使用されるクレデンシャル１２およびトークン記憶装置１８の種類に基づく。例えば、前記記憶媒体が印刷されたバーコードなどの光学的に走査可能な媒体である航空会社の搭乗券または何らかのプラスティックカード（キーフォブのサイズのカードなど）によって提供されるクレデンシャル１２について、前記トークンインターフェース装置３４は、前記トークン１６を前記クレデンシャル上に印刷するプリンターによって提供してもよい。磁気ストライプなどの磁気的に走査可能な媒体である前記記憶装置１８を含むその他の何らかのプラスティックカード（財布サイズのカードなど)によって提供されるクレデンシャル１２について、前記トークンインターフェース装置３４は、前記トークン１６を前記クレデンシャル上に書き込む磁気ストライプエンコーダーによって提供してもよい。

【００４０】

内部の前記記憶装置１８がクレデンシャル上に搭載された無線通信構成要素（例えば、アンテナ、送信機／送受信機、およびコントローラー）に結線されたプロセッサー可読のメモリー装置である、携帯電話およびＰＤＡなどの携帯型電子通信装置によって提供される前記クレデンシャル１２について、前記トークンインターフェース装置３４は、前記トークン１６を前記クレデンシャルに無線送信する、アンテナ、送信機、およびコントローラーなどの無線通信構成要素を含んでもよい。同様に、内部の前記記憶装置１８がクレデンシャル上に搭載された無線通信構成要素（例えばＲＦＩＤ構成要素）に結線されたプロセッサー可読のメモリー装置である、電子キーフォブおよびプロセッサー搭載型のスマートカード（別名非接触型チップカード）などの携帯型電子装置によって提供されるクレデンシャル１２について、前記トークンインターフェース装置３４は、前記トークン１６を前記クレデンシャルに無線送信するアンテナ、送信機、およびコントローラーなどの無線通信構成要素を含んでもよい。そして、内部の前記記憶装置１８がクレデンシャルのコネクターに結線されたプロセッサー可読のメモリー装置である、ＵＳＢサムドライブ、メモリースティック、およびメモリー・スマート・カード（別名接触型チップカード）などの携帯型メモリーオンリー装置によって提供される前記クレデンシャル１２について、前記トークンインターフェース装置３４は、前記トークン１６を前記クレデンシャルに電子的に送信する前記クレデンシャルのコネクターと接触して結合するコネクターによって提供してもよい。

【００４１】

前記設定ワークステーション２８が無線クレデンシャル１２と通信する無線通信構成要素を有する用途において、前記ワークステーションは、ブルートゥース、ジグビー、無線ＬＡＮ、近距離無線通信（Ｎｅａｒ　Ｆｉｅｌｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ：ＮＦＣ）、ＴＣＩＰなどの通信プロトコル、または別の無線通信技術で設定してもよい。そして、前記ワークステーション２８を使用して１より以上の種類のクレデンシャル１２を設定する用途について、前記ワークステーションに、例えばプラスティックカードのクレデンシャル上にバーコードをマーキングするプリンターおよび前記トークンを携帯電話のクレデンシャルに送信する通信構成要素などの、１より以上の種類のトークンインターフェース装置３４を提供してもよい。

【００４２】
別の実施形態において、前記設定ワークステーションは、その初期設定過程において前記トークン１６を前記クレデンシャル１２に送信するようにのみ設定されているのではない。このような別の実施形態は、以前に発行されたクレデンシャル１２からトークン１６を受け取り、前記トークンを変更または更新し、それらを前記クレデンシャルに送り返すこともするように構成された設定ワークステーションを含む。このようなワークステーションは、解読ソフトウェア（暗号化ソフトウェアだけではなく）と、前記トークンインターフェース装置の構成要素としての受信機または送受信機（送信機だけの代わりに）と、トークンインターフェース装置としてのスキャナー（プリンターだけの代わりに）となどを含んでもよい。

【００４３】
前記プログラムされたプロセッサーシステム３０は、前記変換ソフトウェア２２と、前記利用許可キー２６と、暗号化ソフトウェア３６とを含むソフトウェア構成要素を格納し、および／またはこれをアクセスできる。明瞭性のために個別には示していないものの、プログラムされたプロセッサーシステム３０は、前記ワークステーション２８の総合的な処理能力を一体的に定義する、１若しくはそれ以上のプロセッサーと、メモリーと、および／またはその他の論理回路とを含む。当業者であれば理解できるように、前記ソフトウェア要素は図示の目的で概念的に示されており、メモリー内に同時に存在しないかもしれず、またはその全体が存在しないかもしれない。むしろ、既知のコンピューターの動作方法によって、前記ソフトウェア要素またはその部分は、メモリーチップ、固定媒体のローカルドライブ、交換型媒体のローカルドライブ、および／またはネットワークに接続されたリモートコンピューターまたは記憶装置から必要に応じて取り込むことができる。さらに、前記ソフトウェア要素の機能は、より多くのソフトウェア要素に分散でき、またはより少ない要素に統合／集約できる。オペレーティングシステム、グラフィック・ユーザー・インターフェース、ユーティリティー、インターフェース・デバイス・ドライバーなどのコンピューティングシステムに一般的に含まれる追加のソフトウェア要素を含んでもよいが、明瞭性のためにこれらは図示しない。本明細書内の説明を考慮して、当業者であれば好適なソフトウェアを提供し、あるいはワークステーション２８をプログラムし、または構成して下記のトークン設定方法を容易に実行できるであろう。

【００４４】
上述のように、前記変換ソフトウェア２２は、前記バイオメトリック入力装置２０からのバイオメトリック識別子のデジタルテンプレートを前記バイオメトリックキーに変換する。前記変換ソフトウェア２２は、市販のバージョン（例えばカリフォルニア州Ｍｏｕｎｔａｉｎ　Ｖｉｅｗ市のＧＥＮＫＥＹ社の前記指紋変換ソフトウェア）または市販のソフトウェアの適合バージョンであってもよい。

【００４５】
前記格納された利用許可キー２６には、前記特定の用途の全ての利用許可レベルの全ての利用許可キーが含まれる。前記トークン１６が１片または１組のデータのみを含み、利用許可レベルが設定されていない用途において、前記トークン１６は前記専用のデータ区画２４が設定されていない。このような用途において、前記ワークステーション２８は前記利用許可キー２６を格納し、または前記利用許可キー２６へのアクセスを有する必要はない。

【００４６】
前記暗号化ソフトウェア３６は、暗号化アルゴリズムを使用して前記データ区画２４の各々をそれに対応した利用許可キーに基づいて個別に暗号化し、前記データ区画の全て（即ち前記トークン１６全体）を前記利用許可されたユーザーの選択されたバイオメトリックキーに基づいて集合的に暗号化する。前記暗号化ソフトウェア３６は、次世代暗号化標準（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ：ＡＥＳ）、シャーク（ＳＨＡＲＫ）、トゥーフィッシュ（ＴＷＯＦＩＳＨ）、ブローフィッシュ（ＢＬＯＷＦＩＳＨ）などの暗号化アルゴリズム、または別の公開暗号化アルゴリズムまたは所有権を

主張できる暗号化アルゴリズムを使用する暗号化ソフトウェアによって提供してもよい。好適な暗号化ソフトウェアが、ＲＳＡセキュリティ株式会社（ＲＳＡ　Ｓｅｃｕｒｉｔｙ　Ｉｎｃ．）（マサチューセッツ州Ｂｅｄｆｏｒｄ市）およびＰＧＰ　Ｃｏｒｐｏｒａｔｉｏｎ（カリフォルニア州Ｍｅｎｌｏ　Ｐａｒｋ市）を含む多くの業者から市販されている。図示の実施形態において、前記暗号化ソフトウェア３６は、同一の暗号化アルゴリズムを使用して前記データ区画２４を個別に暗号化し、前記データ区画を集合的に暗号化して前記トークン１６を形成する。別の実施形態において、前記プログラムされたプロセッサーシステム３０は、前記個別および集合的暗号化に異なる暗号化アルゴリズムを使用し、および／または前記データ区画の暗号化の一部または全部に異なる暗号化アルゴリズムを使用する。

【００４７】

さらに、前記プログラムされたプロセッサー３０上に格納された、および／またはそれによってアクセス可能な前記ソフトウェア要素は、利用者許可ソフトウェア３８を含んでもよい。前記利用者許可ソフトウェア３８は、前記ユーザーインターフェース装置３２を使用して前記ユーザーおよびインターネットインターフェース（図示せず）とインターフェースしてリモート格納されたデータをアクセスして、新しい（利用許可を得るべき）ユーザーに入力（例えば、真正の本人のみが知りうる質問への回答）を提供するように促し、前記入力を分析して前記個人が実際に彼／彼女が名乗る人物であるか否かを決定する。前記利用者許可ソフトウェア３８は、市販のプログラム（例えば、信用調査会社によって提供される、ペンシルバニア州Ｗａｙｎｅ市のサンガード・データ・システムズ社（ＳＵＮＧＡＲＤ　ＤＡＴＡ　ＳＹＳＴＥＭＳ　ＩＮＣ．）からＳＩＧＮＩＸというブランド名で、またはその他のデジタル署名ソフトウェア）によって提供してもよい。このような利用者許可ソフトウェア３８は、人間の介入または補助を必要とせず、前記新しいユーザーを利用許可されたユーザーとして認証するように自動化されている。前記利用者許可ソフトウェア３８を含む実施形態において、前記ワークステーションは前記利用許可およびトークン発行機関の現場でのセルフサービスキオスクとして、または遠隔地に分散して提供してもよい。前記利用者許可ソフトウェア３８を用いない実施形態において、前記利用者許可は、当該技術分野で既知の従来の方法で行うことができる。

【００４８】

別の実施形態において、設定ワークステーションは、前記データを暗号化して前記トークンを形成するように構成され、プログラムされているが、最初に一切のデータ区画を暗号化するようには構成されていない。この実施形態の設定ワークステーションは、保護すべきデータが１片または１組だけ存在し、前記データまたはデータセットがバイオメトリックキーに基づいて暗号化されて前記トークンが形成される用途での使用に好適である。従って、前記設定ワークステーションは、利用許可キーを有さず、データ区画を設定しない。それでも勿論、保護すべきデータが１片または１組のみ存在する用途において、利用許可キーに基づいてデータ区画内のそのデータの１片または１組を最初に暗号化し、次にそのデータ区画をバイオメトリックキーに基づいて暗号化するように前記ワークステーションを構成することは可能である。

【００４９】

さらに別の実施形態において、設定ワークステーションは１より以上のバイオメトリック識別子に基づいてトークンを暗号化するように構成され、プログラムされている。例えば、ワークステーションには、例えば指紋スキャナーと光彩スキャナーとの２つ（若しくはそれ以上）の異なるバイオメトリック入力装置を提供してもよい。幾つかのこのような用途において、前記設定ワークステーションは、第１のユーザーが彼のバイオメトリック識別子を入力する１つのバイオメトリック入力装置を（例えば、ユーザーインターフェース表示装置上に表示されたメニューから）選択でき、第２のユーザーが彼のバイオメトリック識別子を入力する異なるバイオメトリック入力装置を選択できるように設定されている。他の幾つかのこのような用途において、前記ワークステーションは、１ユーザーが２つの所望のバイオメトリック識別子を入力する２つのバイオメトリック入力装置を（例え

ば、ユーザーインターフェース表示装置上に表示されたメニューから）選択できるように設定されている。前記ワークステーションは、前記第２のバイオメトリック識別子を第２のバイオメトリックキーに変換し、２段階の工程で前記第２のバイオメトリックキーおよび前記利用許可キーに基づいて前記データ区画を暗号化し、次に前記第１のバイオメトリックキーに基づいて全ての前記データ区画を暗号化する。そして、同様の別の実施形態において、ワークステーションは、２段階の工程で前記利用許可キーおよび前記トークンの生成に使用した同一のバイオメトリックキーに基づいて前記データ区画を暗号化するように設定されている。

【００５０】

従って、前記ワークステーションは、１若しくはそれ以上のバイオメトリックキーを使用して前記トークンを設定して、少なくとも３つの異なるモードで前記データ区画を暗号化するように構成できる。３つ全てのモードにおいて、１つのバイオメトリックキーを使用して前記トークン（前記データ区画全てを集合的に）暗号化し、１若しくはそれ以上の利用許可キーを使用して前記データ区画を暗号化する。バイオメトリックキーで前記データ区画を追加的に暗号化する前記３つの方法は、（１）前記データ区画の各々を前記トークンの暗号化に使用したのと同一のバイオメトリックキーで暗号化、（２）前記データ区画の各々を前記トークンの暗号化に使用した前記バイオメトリックキーとは異なるバイオメトリックキーで暗号化、（３）前記データ区画の各々をその独自の専用バイオメトリックキーで暗号化、である。例えば、モード(２)において、右の人差し指の指紋を使用して前記トークンを暗号化でき、左の人差し指の指紋を使用して前記データ区画の全てを暗号化でき、モード(３)の例としては、右の人差し指の指紋を使用して前記トークンを暗号化し、左の人差し指の指紋を使用して前記「名前」データ区画を暗号化し、右の薬指の指紋を使用して前記「社会保障番号」データ区画を暗号化し、および左の薬指の指紋を使用して前記「運転免許証」データ区画を暗号化できる。

【００５１】

トークン設定ワークステーション２８の実施例を説明したので、ここで前記トークン１６を設定する方法について説明する。概述すれば、前記設定方法は、データ区画２４内にデータを入力する工程と、前記データ区画をそれに対応する利用許可キーに基づいて暗号化する工程と、ユーザーによって入力されたバイオメトリック識別子を受け取る工程と、前記入力されたバイオメトリック識別子からバイオメトリックキーを生成する工程と、前記データ区画の全てを前記バイオメトリックキーに基づいて暗号化して前記トークン１６を生成する工程と、前記トークンを前記クレデンシャル１２に転送する工程とを含む。前記設定方法は、前記必要な構成要素を含み、前記トークンの設定をプログラムするようになっているデコーダー１４を使用する、前述した前記設定ワークステーション２８を使用して、または列挙した工程を実行する同様の構成要素を有するその他同様の装置を使用して実行できることが理解されるであろう。便宜上、前記設定方法を、図４の設定ワークステーション２８を使用し、プログラムしてトークン１６を設定する説明と関連して説明する。

【００５２】

本発明のトークンの設定方法５００の例を図５に示す。前記方法５００は、トークン１６を所望する新しいユーザーからの要求を受けて、工程５０２から開始する。前記新しいユーザーは、通常、前記ユーザーインターフェース装置３２を使用して前記要求を前記設定ワークステーション２８内に入力する。前記要求は、通常、前記新しいユーザーの１若しくはそれ以上の識別データ片（正式氏名、ニックネーム／別名、社会保障番号、誕生日、現住所など）を含む。前記要求は、前記新しいユーザーを登録するために有用かもしれないその他の情報をさらに含むことができる。

【００５３】

これに応答して、工程５０４で、新しいユーザーの利用許可処理が行われる。（例えばサンガード・データ・システムズ社（ＳＵＮＧＡＲＤ　ＤＡＴＡ　ＳＹＳＴＥＭＳ　ＩＮＣ．）がＳＩＧＮＩＸブランドで提供するような）利用者許可ソフトウェア３８を含む設

定ワークステーション２８を使用するとき、前記ワークステーションは、前記ユーザーインターフェース装置３２を介して前記新しいユーザーに識別情報入力を提供するように促す。例えば、前記ワークステーション２８は、前記ユーザーインターフェース装置３２を介して前記新しいユーザーに、真正の本人のみが正しい答えを知っていると思われるという理由で選択された、一連の質問を問うことができる。このような質問は、「１０年前のあなたの住所は？」、「あなたの最初の犬の名前は？」、「あなたの高校の校長の名前は？」などを含むことができる。通常の商用の実施形態において、前記ワークステーション２８は、ネットワークインターフェースを介してインターネット（または別のグローバル通信ネットワーク）をアクセスして前記入力された識別情報データに基づいて前記新しいユーザーに関連したよく知られていないデータを検索し、見つけた前記よく知られていないデータに基づいて質問を組み立てる。いずれにしても、前記ワークステーション２８は、次に、前記ユーザーインターフェース装置３２を介して前記ユーザー識別情報入力（例えば、問われた質問に対する答え）を受け取り、前記入力を解析して（例えば、それらを前記見つけたよく知られていないデータと比較して）前記個人が実際に名乗るとおりの人物であるか否かを決定する。さらに、またはその代わりに、前記ワークステーション２８は、前記ユーザーインターフェース装置３２を介して前記新しいユーザーに、州発行の運転免許証、パスポート、公共料金の請求書などの特定のユーザーを識別する証拠を、前記ユーザーインターフェース装置３２（例えばスキャナー）を介して入力するように要求することができる。前記ワークステーション２８に前記利用者許可ソフトウェア３８を提供することによって、前記新しいユーザーの認証処理が自動化され、人間の介入または補助を必要とせずに（または最小限の人間の介入または補助で）それを行うことができる。

【００５４】

利用者許可ソフトウェア３８を用いずに設定ワークステーション２８を使用するときは、当該技術分野で既知の従来の方法によって利用者許可処理を実施できる。このような従来の方法には、前記新しいユーザーから受け取ったユーザーを識別する証拠を手作業で（即ち人間によって）検査する方法が含まれる。このようなユーザーを識別する証拠は、運転免許証、社会保障カード、パスポート、または就労許可証を含む政府またはその他の公的機関によって交付された書類であってもよい。または、バイオメトリック識別子が政府またはその他の公的機関によって既に保持されている場合、このようなユーザーを識別する証拠は、前記バイオメトリック識別子であってもよい。

【００５５】

前記新しいユーザーの利用許可処理の完了時に、前記新しいユーザーが認証されないと、次に工程５０６において前記方法５００が終了し、トークンは生成されない。前記新しいユーザーが認証された場合、次に工程５０８において、前記ワークステーション２８が、前記ユーザーインターフェース装置３２を介してこの時点で利用許可されたユーザーに、少なくとも１つのバイオメトリック識別子を入力するように問い、前記バイオメトリックインターフェース装置２０を介して前記バイオメトリック識別子を受け取る。前記バイオメトリックインターフェース装置２０が、前記バイオメトリック識別子に固有のデジタルテンプレートを生成する。好ましくは、前記バイオメトリック識別子のデジタルテンプレートは、前記ワークステーション２８上に一時的にのみ格納され（または一切格納されず）、プライバシーに関する懸念を回避する。上述のように、前記バイオメトリック識別子は、指紋、手形、光彩紋／スキャン、声紋、ＤＮＡサンプル、および／またはそれらの組み合わせ、および／またはその個人に特有のその他任意の固有の物理的または行動的な人間的特性であってよい。

【００５６】

次に、工程５１０において、前記ワークステーション２８が前記トークン１２内で保護されるべきデータを受け取る。例えば、前記ワークステーション２８は、前記ユーザーインターフェース装置３２を介して前記ユーザーに照会し、前記ユーザーインターフェース装置を介して前記ユーザーから前記データを受け取るように構成できる。追加として、またはその代わりに、前記ワークステーション２８は、工程５０２の前記トークン要求工程

で前記ユーザーから受け取った、（その一部または全てが保護されるべきデータである）前記識別データをアクセスできる。上述のように、前記データは、ユーザーに特定の情報、用途に特定の情報、またはその他の情報を含む、前記特定の用途に関連する任意の種類のデータであってよい。前記利用許可工程５０４、前記バイオメトリック識別子入力工程５０８、および前記データ入力工程５１０は、説明した順序で実行しなくてもよいことに注意すべきである。

【００５７】

工程５１２において、前記ワークステーション２８が、前記ユーザーインターフェース装置３２を介して前記ユーザーに照会して前記データが正確であることを確認する。例えば、前記ワークステーション２８が受け取った通りにリストされた前記データを前記ユーザーに表示することができ、前記ユーザーには、全てのタイプミスを修正し、全ての不完全なデータ欄を完全なものにし、などの機会が与えられる。前記データが完全で正しくない場合、前記方法５００は、次に工程５０８に戻り、前記ワークステーション２８が前記ユーザーインターフェース装置３２を介して前記ユーザーから前記修正された情報を受け取る。

【００５８】

前記情報が正しく完全である場合、次に工程５１４において、トークン１６が生成される。前記トークン生成工程５１４の詳細については、図６に関して以下に提供する。最後に、前記ワークステーション２８は、前記トークンインターフェース装置３４を介して前記トークン１６をクレデンシャル１２に転送し、前記方法５００が完了する。その結果、トークンおよび前記利用許可されたユーザーのバイオメトリック識別子の提示を受けたデコーダー１４によってのみアクセス可能なデータを収容した前記トークン１６を有するクレデンシャル１２が得られる。

【００５９】

図６に、前記トークン生成工程５１４の詳細を示す。前記方法５１４は、そのデータの種類に対応したデータ区画２４内のデータの各片または各組を格納することによって、工程６０２から開始する。上述のように、各データ区画２４は、選択的に一まとめにして特定の用途に使用する１片のデータまたは１組のデータ（例えばユーザーの金融データまたは医療データ）を格納することができる。

【００６０】

工程６０４において、前記ワークステーション２８が、前記暗号化ソフトウェア３６を使用して、そのデータ区画の所定の利用許可キー２６に基づいて前記データ区画２４のうちの１つを暗号化する。上述のように、前記利用許可キー２６の各々は利用許可レベルに対応し、用途によっては、多数の異なる利用許可レベルがあってもよい。例えば、１つの利用許可レベル（およびそれに対応した利用許可キー２６）は（例えばクレジットカード口座のデータを格納する）所定の金融データ区画２４のアクセス用であってもよく、別の利用許可レベル（およびそれに対応した利用許可キー）は所定の医療履歴のデータ区画のアクセス用であってもよい。別の例として、第１の利用許可レベル（およびそれに対応した利用許可キー２６）は、前記ユーザーが第１の保護区域に入ることを許可されたことを示す、所定の第１のセキュリティー許可の（例えばランダムデータを格納する）データ区画２４の開放用であってもよい。そして、第２の利用許可レベル（およびそれに対応した利用許可キー）は、ユーザーが前記第２の保護区域に入ることを許可されたことを示す、所定の第２のセキュリティー許可の（例えばランダムデータを格納する）データ区画の開放用であってもよい。

【００６１】

他にも暗号化すべきデータ区画２４が存在する場合、次に工程６０６において、前記方法５１４は前記データ区画暗号化工程６０４に戻り、これを繰り返す。前記データ区画２４の全てがそれぞれ対応する利用許可キー２６に基づいて個別に暗号化されると、前記方法５１４は工程６０８に進む。

【００６２】

工程６０８において、前記ワークステーション２８が、前記変換ソフトウェア２２を使用して工程５０８からの前記バイオメトリック識別子のデジタルテンプレートをバイオメトリックキーに変換する。そして工程６１０において、前記ワークステーション２８が、前記暗号化ソフトウェア３６を使用して前記バイオメトリックキーに基づいて前記データ区画２４の全てを集合的に暗号化することでトークン１２を生成する。

【００６３】

ここで説明したトークン生成の方法の例５１４において、前記入力データは初期的に（そして好ましくは一時的にのみ）前記設定ワークステーション２８のデータ記憶装置のデータ区画２４内に格納される。前記データ区画２４が個別におよび集合的に暗号化されて前記トークン１６が生成された後、前記トークンが前記クレデンシャル１２にロードされる。別の方法において、前記入力データは、初期的に前記クレデンシャル１２の記憶装置１８のデータ区画２４に転送され、格納される。前記データ区画２４は、次に、個別に暗号化され、前記クレデンシャル１２の暗号化されていないデータ区画に保存される。そして次に、前記暗号化されたデータ区画２４が集合的に暗号化されて前記トークン１６が生成され、次に前記クレデンシャル１２上の前記個別に暗号化されたデータ区画２４に保存される。

【００６４】

保護されるべきデータが１片または１組しかない別のトークン生成方法において、データ区画または利用許可キーは使用されない。具体的には、データ区画が存在しないので、工程６０２において前記データはデータ区画２４に格納されず、工程６０４および６０６は削除され、工程６１０において、前記データは前記バイオメトリックキーに基づいて暗号化される。この別の方法は、前記データにアクセスする利用許可キーが必要ないので、セキュリティーがそれほど堅固でなくより公開されたトークン１２が望まれる用途への使用に好適である。この別の方法でさえも、前記生成されたトークン１６は完全に自律的であり、中央のサーバーまたはデータベースに接続せずに利用者許可およびデータ転送を可能とする。

【００６５】

さらに別の方法は、第２のバイオメトリック識別子を受け取る工程と、前記第２のバイオメトリック識別子を第２のバイオメトリックキーに変換する工程と、前記第２のバイオメトリックキーを使用して前記トークン１６をさらに追加的に暗号化する工程とを含む。例えば、前記第２のバイオメトリックキーおよび第１の利用許可キー２６を使用して第１のデータ区画２４を逐次暗号化し、前記第２のバイオメトリックキーおよび第２の利用許可キーを使用して第２のデータ区画を逐次暗号化し、次に前記第１のバイオメトリックキーを使用して前記データ区画の両方を暗号化して前記トークン１６を形成することができる。この別の方法は、前記データのアクセスに２つ（若しくはそれ以上の）（同一のまたは異なる種類の）バイオメトリック識別子が必要なので、セキュリティーがより堅固でより非公開なトークン１６が望まれる用途への使用に好適である。

【００６６】

図１に戻って、ここで前記デコーダー１４を詳細に説明する。前記デコーダー１４は、少なくとも１つのバイオメトリック入力装置４０と、少なくとも１つのユーザーインターフェース装置４２と、少なくとも１つのトークンインターフェース装置４４と、プログラムされたプロセッサーシステム４６とを含む。通常の商用の実施形態において、前記デコーダー１４は、ランダム・アクセス・メモリー（ｒａｎｄｏｍ　ａｃｃｅｓｓ　ｍｅｍｏｒｙ：ＲＡＭ）データ記憶装置と、および／または、プロセッサーを用いた装置に一般的に使用されるその他の構成要素（明瞭性のために図示せず）とを含む。前記バイオメトリック入力装置４０、前記ユーザーインターフェース装置４２、および前記トークンインターフェース装置４４は、前記デコーダー１４に動作可能に（例えば無線でまたは配線によって）接続される周辺装置として提供してもよく、またはこれらを前記デコーダーに一体化した構成要素としてもよい。

【００６７】

前記バイオメトリック入力装置４０は、前記設定ワークステーション２８のバイオメトリック入力装置２０と同一または類似の種類のものであってよい。従って、前記バイオメトリック入力装置４０は、指紋または手形スキャナー、光彩スキャナー、顔の特徴スキャナー、音声レコーダー、ＤＮＡサンプリング装置、または上述のような前記バイオメトリック識別子のデジタルテンプレートを収集する別の従来の装置（例えば、カメラ、ソナー、または赤外線装置）であってよい。１より以上の種類のバイオメトリック識別子に基づいて暗号化されたトークン１６を解読するために前記デコーダー１４を使用する用途について、前記デコーダーには、１より以上の種類のバイオメトリック入力装置４０、例えば、指紋スキャナーと光彩スキャナーとを提供してもよい。このような用途の幾つかにおいて、１つのトークン１６は１つのバイオメトリック識別子に基づいて暗号化され、別のトークンは異なるバイオメトリック識別子に基づいて暗号化され、前記デコーダー１４は、前記ユーザーがその特定のバイオメトリック識別子を前記解読のために入力する前記バイオメトリック入力装置４０のうちの適切な１つを（例えば、ユーザーインターフェース表示装置４２上に表示されたメニューから）選択できるように構成され、プログラムされている。そして、他のこのような用途において、１つのトークン１６は２つの異なるバイオメトリック識別子に基づいて暗号化され、前記デコーダー１４は、前記バイオメトリック入力装置４０のうちの１つからの１つのバイオメトリック識別子に基づいて前記トークンを解読する第１の工程、および、次に、前記バイオメトリック入力装置４０のうちの他の１つからの他のバイオメトリック識別子に基づいて前記一度解読されたトークンを解読する工程のために構成され、プログラムされている。前記デコーダー１４は、前記トークン設定ワークステーション２８に関する上述の３つのモードの何れかにおいて、例えば２若しくはそれ以上のバイオメトリックキーで暗号化されたトークン１６およびデータ区画２４を解読するように構成され、プログラムできることが理解されるであろう。

【００６８】

前記ユーザーインターフェース装置４２には、通常、１若しくはそれ以上の入力装置と、１若しくはそれ以上の出力装置とが提供されている。前記入力装置は、例えば、タッチスクリーン、手書き入力画面、キーパッド、キーボード、データ入力ボタン、ポインティング装置（例えばマウス）、磁気ストライプリーダー、および／または光学スキャナーであってよい。そして、前記出力装置は、例えば、タッチスクリーン、表示画面、スピーカー、および／または表示灯であってよい。例えば、図２および図３に図示した実施形態において、前記デコーダー１４は、前記ユーザー入力装置としてデータ入力ボタンと、前記ユーザー出力装置としてＬＣＤまたはＬＥＤ表示画面とを含む。

【００６９】

前記デコーダー１４用に選択された前記トークンインターフェース装置４４は、特定の用途に使用される種類のクレデンシャル１２およびトークン記憶装置１８に基づく。また、通常、前記トークンインターフェース装置４４は、前記設定ワークステーション２８のトークンインターフェース装置３４に対応するように選択される。このように、前記記憶媒体１８が印刷されたバーコードなどの光学的に走査可能な媒体である搭乗券または幾つかのプラスティックカード（キーフォブのサイズのカードなど）によって提供されるクレデンシャル１２について、前記トークンインターフェース装置４４は、前記バーコードまたはその他の光学的に走査可能な媒体を読む光学スキャナーによって提供してもよい。前記記憶装置１８が磁気ストライプなどの磁気的に走査可能な媒体であるその他の幾つかのプラスティックカード（財布サイズのカードなど）によって提供されるクレデンシャル１２について、前記トークンインターフェース装置４４は、前記磁気ストライプを読む磁気リーダー、またはその他の磁気的に走査可能な媒体によって（即ち前記カードを「リーダーに通す」ことによって）提供してもよい。

【００７０】

前記記憶装置１８がクレデンシャル上に搭載された無線通信構成要素（例えばアンテナ、送信機／送受信機、およびコントローラー）に配線されたプロセッサー可読のメモリー装置である携帯電話およびＰＤＡなどの携帯型電子通信装置によって提供される前記クレ

デンシャル１２について、前記トークンインターフェース装置４４は、前記クレデンシャルから前記トークン１６を無線で受信するアンテナ、受信機、コントローラーなどの無線通信構成要素を含んでもよい。同様に、前記記憶装置１８がクレデンシャル上に搭載された無線通信構成要素（例えばＲＦＩＤ構成要素）に配線されたプロセッサー可読のメモリー装置である電子キーフォブおよびプロセッサー搭載型のスマートカード（別名非接触型チップカード）などの携帯型電子装置によって提供される前記クレデンシャル１２について、前記トークンインターフェース装置４４は、前記クレデンシャルから前記トークン１６を無線で受信するアンテナ、受信機、およびコントローラーなどの無線通信構成要素を含んでもよい。そして前記記憶装置１８がクレデンシャルのコネクターに配線されたプロセッサー可読のメモリー装置であるＵＳＢサムドライブ、メモリースティック、およびメモリー・スマート・カード（別名接触型チップカード）などの携帯型メモリーオンリー装置によって提供される前記クレデンシャル１２について、前記トークンインターフェース装置４４は、前記クレデンシャルから前記トークン１６を電子的に受け取る前記クレデンシャルのコネクターと接触して結合するコネクターによって提供してもよい。

【００７１】

前記デコーダー１４が無線クレデンシャル１２と通信する無線構成要素を有する用途について、前記デコーダーは、ブルートゥース、ジグビー、無線ＬＡＮ、近距離無線通信（Ｎｅａｒ Ｆｉｅｌｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎ：ＮＦＣ）、ＴＣＩＰなどの通信プロトコル、または別の無線通信技術を用いて設定してもよい。そして前記デコーダー１４を使用して１より以上の種類のクレデンシャル１２を開く用途において、前記デコーダーには、１より以上の種類のトークンインターフェース装置４４、例えば、プラスティックカードのクレデンシャル上のバーコードを読む光学スキャナーと、前記携帯電話のクレデンシャルから前記トークンを無線で受信する通信構成要素とを提供してもよい。

【００７２】

前記プログラムされたプロセッサーシステム４６は、前記変換ソフトウェア５０、前記利用許可キー２６、および解読ソフトウェア４８を含むソフトウェア要素を格納し、および／またはこれをアクセスできる。明瞭性のために個別には図示しないが、プログラムされたプロセッサーシステム４６は、前記デコーダー１４の総合的な処理能力を一体となって定義する、１若しくはそれ以上のプロセッサーと、メモリーと、および／またはその他の論理回路とを含む。当業者であれば理解できるように、前記ソフトウェア要素は図示の目的で概念的に示されており、同時に、またはその全体がメモリー内に存在しないかもしれない。むしろ、コンピューターの動作として知られる方法において、前記ソフトウェア要素またはその部分は、データ記憶装置（例えば、ボード上に搭載されたＲＡＭチップ、固定媒体のローカルドライブまたは交換型媒体のローカルドライブ、および／またはネットワークを介して接続されたリモートコンピューターまたは記憶装置）から必要に応じて取り込むことができる。さらに、前記ソフトウェア要素の機能は、より多くのソフトウェア要素に分散でき、またはより少ない要素に統合／集約できる。オペレーティングシステム、グラフィック・ユーザー・インターフェース、ユーティリティー、インターフェース・デバイス・ドライバーなどのコンピューティングシステムに一般的に含まれる追加のソフトウェア要素を含んでもよいが、明瞭性の目的で図示しない。本明細書内の説明を鑑みて、当業者であれば、好適なソフトウェアを提供し、あるいは以下に説明するトークンを開く方法を実行するように前記デコーダー１４をプログラムし、または構成することが容易にできる。

【００７３】

上述のように、前記変換ソフトウェア５０は、前記バイオメトリック入力装置４０からのバイオメトリック識別子デジタルテンプレートを前記バイオメトリックキーに変換する。前記変換ソフトウェア５０は、前記設定ワークステーション２８の変換ソフトウェア２２と同一または類似の種類のものであってよい。従って、前記変換ソフトウェア５０は、市販のバージョン（例えばカリフォルニア州Ｍｏｕｎｔａｉｎ Ｖｉｅｗ市のＧＥＮＫＥＹの指紋変換ソフトウェア）または市販のソフトウェアの適合バージョンであってよい。

【００７４】
前記デコーダー１４に格納した利用許可キー２６には、その特定のデコーダーに割り当てられた利用許可レベルに対応した利用許可キーのみが含まれる。前記利用許可レベル２６は各々、異なる用途の一定のデコーダーのユーザーが必要とするデータを格納した異なる所定のデータ区画２４（またはデータ区画の組）に関連づけられ、それらは実際には必ずしも階層的ではない。このように、各デコーダー１４は、少なくとも１つの利用許可キー２６を有し、それに提示されたトークン１２を適用して、その特定のデコーダーのユーザーが必要とするデータを格納したデータ区画２４を開く。
【００７５】
用途によっては、前記デコーダー１４は、１より以上の利用許可キー２６を格納する。例えば、２つのデコーダー１４が、各デコーダーが前記トークン１６の両方の第１の特定のデータ区画２４（例えば、前記ユーザーの名前のうちの対応した１つを格納した各第１のデータ区画）にアクセスすることを許可する第１の利用許可キー２６を各々格納するかもしれない。そしてこれら２つのデコーダーは、幾つかの異なる利用許可キー２６をさらに有するかもしれない。従って、前記デコーダーのうちの第１のそれは、それが（例えばクレジットカード情報を格納した）第２のデータ区画にアクセスすることを許可する第２の利用許可キー２６をも格納し、前記デコーダーの前記第２のそれは、その利用許可キーを有さないかもしれない。しかし、前記第２のデコーダー１４は、それが（例えば医療情報を格納した）第３のデータ区画にアクセスすることを許可する第３の利用許可キー２６をも格納し、前記第１のデコーダーはその利用許可キーを有さないかもしれない。
【００７６】
さらに、前記トークン１６が１片または１組のデータのみを含み、利用許可レベルが設定されていない幾つかの用途について、前記トークン１６には、前記専用のデータ区画２４が設定されていない。その代わりに、利用許可キーに基づいて前記データまたはデータセットを最初に暗号化せずに、バイオメトリックキーに基づいて前記１片または１組のデータが暗号化され、前記トークン１６が形成される。このような用途において、前記デコーダー１４は、前記利用許可キー２６を一切格納する必要がなく、またはそれらへのアクセスを有する必要がない。
【００７７】
その他の幾つかの用途において、１つのデコーダー１４を複数の目的に使用してもよい。例えば、診療所が患者の医療記録をアクセスして医療サービスを提供し、また前記患者のクレジットカード口座の情報をアクセスして提供した医療サービスの対価の支払いを受ける必要があるかもしれない。このような用途について、前記デコーダー１４には、複数の利用許可キーまたはキーセット２６が提供され、アクセスすべきデータを選択するメニューが（例えばユーザーインターフェース表示装置を介して）表示される。前記デコーダー１４は、次に、前記選択されたデータに対応した利用許可キーまたはキーセット２６のみを受け取り、それを対応したデータ区画に適用して前記選択されたデータにアクセスする。
【００７８】
前記解読ソフトウェア４８は、暗号化アルゴリズムを使用して、前記利用許可されたユーザーの前記選択されたバイオメトリックキーに基づいて前記データ区画２４の全て（即ち前記トークン１６全体）を集合的に暗号化し、前記デコーダーが対応した利用許可キーを有する前記データ区画の各々を個別に解読する。前記解読ソフトウェア４８は、前記設定ワークステーション２８の解読ソフトウェア３６と同じまたは類似の種類のものであってよい。従って、前記解読ソフトウェア４８は、次世代暗号化標準（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ：ＡＥＳ）、シャーク（ＳＨＡＲＫ）、トゥーフィッシュ（ＴＷＯＦＩＳＨ）、ブローフィッシュ（ＢＬＯＷＦＩＳＨ）などの暗号化アルゴリズム、または別の公開された、または所有権を主張できる暗号化アルゴリズムを使用する暗号化ソフトウェアによって提供してもよい。好適な暗号化ソフトウェアは、ＲＳＡセキュリティ株式会社（ＲＳＡ Ｓｅｃｕｒｉｔｙ Ｉｎｃ．）（マサチューセッツ州

Ｂｅｄｆｏｒｄ市）およびＰＧＰ　Ｃｏｒｐｏｒａｔｉｏｎ（カリフォルニア州Ｍｅｎｌｏ　Ｐａｒｋ市）を含む多くの業者から市販されている。別の実施形態において、前記解読ソフトウェア４８並びに前記暗号化ソフトウェア５０は、前記データ区画２４を個別に暗号化するものと、前記データ区画の全てを集合的に暗号化して前記トークン１６を形成するものとの２つの異なる暗号化アルゴリズムを有する。さらに別の実施形態において、前記解読ソフトウェア４８および前記暗号化ソフトウェア５０は各々、前記データ区画２４の一部または全てを保護し、開く複数の暗号化アルゴリズムを有する。

【００７９】

図示した実施形態において、前記データ区画２４は、前記正しいデコーダーの利用許可キー２６および前記正しいユーザーのバイオメトリックキーの両方がないと開くことができない。従って、例えば警察官のデコーダーのようなデコーダー１４をハッキングしても、データは一切露出することはない。前記デコーダー１４は１つのキー（前記利用許可キー）のアクセスしか有さないので、前記デコーダーはそれ自体によって前記データ区画２４の何れも開く機能を有さない。前記デコーダー１４は、（それに入力された前記バイオメトリック識別子に基づいてそれが生成する）前記固有のバイオメトリックキーおよびそれが保持する前記利用許可キー２６を適用して前記データ区画２４を開き、それらに格納されたデータにアクセスすることのみが可能である。これは、前記認証を実行する必要のある前およびその時に、スマート・カード・リーダーが読むトークン上に、またはそれがアクセスするデータベース上に前記データが格納されているか否かに拘らず、前記保護されているデータにアクセスする能力を有し、これによってハッカーに前記データを盗む機会を提示する従来の（例えばクレジットカードの決済用の）スマート・カード・リーダーとは異なる。

【００８０】

さらに、ハッカーは、前記デコーダーに「偽りの外見」を装わせてユーザーの入力したバイオメトリック識別子を取り込み、次に、それを前記バイオメトリックキーに変換することができない。何故なら、前記ハッカーは、前記バイオメトリック識別子を前記バイオメトリックキーに変換する正しい変換ソフトウェアを有さず、前記ハッカーは前記キーに適用する前記正しい解読ソフトウェアを有さないからである。従って、前記利用許可キー２６、または前記バイオメトリック識別子、またはその両方を盗むだけでは、前記トークン１６または一切の前記データ区画２４を開くには不十分である。

【００８１】

別の実施形態において、前記デコーダー１４が前記トークン１６を解読するのに必要な前記解読ソフトウェアにアクセスするために、前記デコーダーがバイオメトリック識別子を受け取ることを要求することによって、前記デコーダー１４はハッカーからさらに保護されている。上述のように、前記トークン設定ワークステーション２８は、暗号化アルゴリズムを使用した暗号化ソフトウェア４８、およびそれが前記ユーザーから受け取ったバイオメトリック識別子から生成するバイオメトリックキーを用いて各トークン１６を固有に暗号化する。そして、前記デコーダー１４は、同一の暗号化アルゴリズムを使用した解読ソフトウェア５０を用いて前記トークン１６を解読する。しかし、この別の実施形態において、前記デコーダー１４に格納された前記解読ソフトウェア５０は、前記デコーダーが前記ユーザーの所定のバイオメトリック識別子を受け取ることによってのみアクセス可能である。前記デコーダー１４は、前記解読ソフトウェア５０が前記トークン１６を開くために使用するのと同一のバイオメトリック識別子を入力することでアクセスされ、または異なるバイオメトリック識別子を入力することでのみアクセス可能であるように構成できる。異なる種類のバイオメトリック識別子を入力する実施形態について、前記デコーダー１４は、２つの異なる種類のバイオメトリック入力装置４０（各バイオメトリック識別子の種類に１つ）を含んでもよい。要求されるバイオメトリック識別子の両方が、前記ユーザーが複数有する種類のもの（例えば１０個の指紋、左右の手形、左右の光彩紋など）である場合、同一のバイオメトリック入力装置４０を使用してそれら両方を入力できる。このようにすれば、前記デコーダー１４は、１つの入力されたバイオメトリック識別子を

使用して前記トークン１６を開くのに必要な前記解読ソフトウェアにアクセスする。次に、前記デコーダー１４は、前記同一または追加で入力されたバイオメトリック識別子を使用して前記解読ソフトウェアを適用する前記バイオメトリックキーを生成する。これにより、ハッキングすべきものがないので、非常に高いレベルのセキュリティーが提供される。ある実施例において、前記バイオメトリック識別子を固有の反復数字に変換し、次にそれを「シード」として使用して前記暗号化処理に使用する実際のアルゴリズムを決定することができる。別の実施例において、前記デコーダーはその中に格納した複数の暗号化アルゴリズムを有することができ、前記バイオメトリック識別子をどのアルゴリズムを使用するかを選択するための固有の反復数字に変換することができる。例えば、どのアルゴリズムを使用するかを選択する数字が偶数か基数かを決定することによって前記バイオメトリックキーを使用することができる。または、前記バイオメトリックキーに別の数字を掛け、またはそれを式に挿入してその結果を計算することによって、および前記トークンを暗号化するために使用する前記アルゴリズムを決定した結果に基づいて前記バイオメトリックキーを使用することができる。

【００８２】

さらに別の実施形態において、前記変換および解読ソフトウェア並びに前記オペレーティングシステム、および演算処理ソフトウェアを含む前記ソフトウェアの全ては、前記デコーダーのハッキングをさらに防止する単一チップ内に統合されている。即ち、前記ソフトウェアがどのように機能するかを学ぶためにハッキングし、または監視することが潜在的に可能なディスク上に存在する前記ソフトウェア要素の一部または全部の代わりに、前記ソフトウェア要素が全て前記デコーダー内の単一チップ上に存在する。このようにすれば、前記ソフトウェアの演算処理、前記バイオメトリックキーの演算処理、前記トークンの演算処理など、全てが、何が起こっているかを外部から監視する機会がないまま単一チップ上で発生する。従って、ハッカーはただ単に前記演算処理を「見て」それがどのように機能するのかを学ぶことができない（単一チップ上では前記チップに入るデータおよび前記チップから出るデータしかないので、見るべきものが存在しない）。

【００８３】

そして、さらに別の実施形態において、前記セキュリティーは、前記トークンを暗号化／解読する１つと、（前記利用許可キーと共に）前記データ区画を暗号化／解読する他方との２つのバイオメトリックキーで階層化されている。２つの異なる暗号化アルゴリズムを使用することによって、同一のバイオメトリック識別子（および同一のバイオメトリック入力装置）を使用して２つの固有のバイオメトリックキーを生成して前記トークンおよび前記データ区画を保護することができる。本発明は、その他の同様の方法によって前記セキュリティーを階層化して前記システムをより安全にするその他の実施形態を含むことを考慮し、そのように意図するものであることが理解されるであろう。

【００８４】

図示の実施形態において、前記デコーダー１４は、前記トークン１６をローカルに開く構成要素のみで構築され構成されている。別の実施形態において、デコーダーは、前記トークン１６をローカルに開き、前記トークンの初期設定もし、および／または前記トークンの更新もするように構成要素で構築され、構成されている。前記デコーダーが前記トークン１６の初期設定をもする別の実施形態において、前記デコーダーは前記トークンを暗号化し、それらを前記クレデンシャル１２にロードする。そして前記デコーダーが前記トークンの更新もする別の実施形態において、前記デコーダーは、前記データを更新し、前記トークンを再度暗号化し、それらを前記クレデンシャル１２にロードし直す。このような代替のデコーダーは、暗号化ソフトウェア（解読ソフトウェアだけではなく）と、前記トークンインターフェース装置の構成要素としての送信機または送受信機（受信機だけの代わりに）と、トークンインターフェース装置としてのプリンター（スキャナーだけの代わりに）となどを含んでもよい。

【００８５】

さらに別の実施形態において、前記デコーダー１４は、インターネットなどのネットワ

ークに接続するネットワークインターフェース装置（図示せず）を含む。前記ネットワークインターフェース装置は、前記デコーダー１４と一体化した構成要素であってもよく、または前記デコーダーに動作可能に（無線でまたは配線によって）接続した別個の構成要素であってもよい。前記ネットワークインターフェース装置は、前記デコーダー１４がローカルまたはリモートＰＯＳ装置、例えば扉またはゲートを含む境界アクセス制御装置、リモートサーバーなどのその他の装置と通信することを可能とする。

【００８６】

デコーダー１４の実施例を説明したので、ここで、前記デコーダーを使用して前記トークン１６を開く方法を説明する。概述すると、前記トークンを開く方法は、ユーザーからトークン１６およびバイオメトリック識別子を受け取る工程を含む。次に、前記デコーダー１４は、前記ユーザーのバイオメトリック識別子をバイオメトリックキーに変換し、前記バイオメトリックキーを適用して前記固有に暗号化されたトークン１６を解読することでそれを開く。前記トークンを開く方法は、今説明した前記デコーダー１４を使用し、前記必要な構成要素を含むようになっているワークステーション２８を使用し、前記トークンを開くようにプログラムし、または列挙した工程を実行する同様の構成要素を有するその他の同様の装置を使用して実行できることが理解されるであろう。便宜上、前記トークンを開く方法は、図１のデコーダー１４を使用し、プログラムしてトークン１６を開く工程の説明と共に説明する。

【００８７】

図７に、本発明のリモートにトークンを開く方法の例７００を示す。前記方法７００は、前記デコーダー１４がユーザーからトークン１６を受け取る工程７０２から開始する。前記トークン１６は、前記クレデンシャル１２の記憶装置１８上に格納され、前記トークンインターフェース装置４４を介して受け取られる。例えば図２に示す実施形態において、前記ＰＤＡのクレデンシャル１２は、前記トークン１６を前記デコーダー１４の無線通信の構成要素（例えば、アンテナ、送受信機、およびコントローラー）に無線で送信する。このようにすれば、前記クレデンシャル１２は前記トークン１６を前記デコーダー１４に動的に伝達する。別の実施形態において、前記クレデンシャル１２は、前記トークン１２を前記デコーダー１４に静的に伝達する。このような別の実施形態には、前記トークンインターフェース装置４４が光学スキャナー、磁気リーダー、または電気的コネクターによって提供される実施形態が含まれ、またはその他幾つかの無線用途では、例えばスマートカードのクレデンシャル１２を使用する実施形態が含まれる。

【００８８】

工程７０４において、前記デコーダー１４が、前記ユーザーからのバイオメトリック識別子を受け取る。前記バイオメトリック識別子は、前記バイオメトリックインターフェース装置４０を介して受け取られる。例えば、図２に示す実施形態では、指紋スキャナー４０を使用して前記ユーザーの指紋をデジタルテンプレートとして走査する。前記バイオメトリックインターフェース装置４０に光彩スキャナーと、顔の特徴スキャナーと、音声レコーダーと、ＤＮＡサンプリング装置と、などが提供されている別の実施形態において、前記デコーダー１４は、それぞれの前記バイオメトリックインターフェース装置からそれぞれの前記バイオメトリック識別子のデジタルテンプレートを同様に受け取る。説明した順序において、前記トークン入力工程７０２、および前記バイオメトリック識別子入力／変換工程７０４／７０６は実行する必要がないことに注目すべきである。

【００８９】

工程７０６において、前記デコーダー１４が、前記変換ソフトウェア５０を使用して前記バイオメトリック識別子のデジタルテンプレートをバイオメトリックキーに変換する。次に工程７０８において、前記デコーダー１４が、前記解読ソフトウェア４８を使用して前記バイオメトリックキーを前記トークン１６に適用して前記トークンを開こうとする。工程７１０において、前記トークン１６が開かなければ、次に工程７１２において、前記デコーダー１４が、前記認証が失敗したことの表示を提供する。前記失敗の表示は例えば赤い表示灯、ブザー音、および／またはメッセージを表示した画面によって前記ユーザー

インターフェース装置４２を介して提供される。この時点で、前記デコーダー１４は、前記ユーザー、前記トークン１６、またはその両方が真正ではないと決定しており、前記方法７００は前記トークンを開かずに終了する。

【００９０】

しかし、工程７１０において、前記トークン１６が前記バイオメトリックキーによって開いたならば、次に前記デコーダー１４は前記ユーザーが真正であると決定している。前記利用許可されたユーザー以外には誰も、前記バイオメトリックキーが基づく前記ユーザーのバイオメトリック識別子を提示できないので、このとき、前記クレデンシャル１２の提示者は、前記利用許可されたユーザーとして認証されたことになる。前記トークン１６の解読（即ち前記ユーザーの認証）は前記受け取られたトークンおよびバイオメトリック識別子のみに基づいて前記デコーダー１４によってなされるので、その他全ての既知のバイオメトリック識別子の認証システムでなされるように、バイオメトリック識別子のファイルを（例えば中央のサーバーまたは前記トークン上に）格納し、それをアクセスし、それを前記入力されたバイオメトリック識別子と比較する必要はない。

【００９１】

工程７１４に進んで、前記トークン１６はここで開くが、前記個別のデータ区画２４は開かないままで安全に暗号化されたままである。工程７１６において、前記デコーダー１４が、前記解読ソフトウェア４８を使用してその利用許可キー２６の１つを適用して対応した前記トークン１６のデータ区画２４を開こうとする。上述のように、所定のトークン１６は、１つのデータ区画２４を有してもよく、所定のデコーダー１４はその１つのデータ区画を開く１つの利用許可キー２６を有してもよい。または、所定のトークン１６は、複数のデータ区画２４を有してもよく、所定のデコーダー１４は前記データ区画の１つ、幾つか、または全てを開く１つの利用許可キー２６、または前記データ区画の幾つかまたは全てを開く複数の利用許可キー２６を有してもよい。例えば図２のデコーダー１４は、前記トークン１６の１２個のデータ区画２４のうちの１つのみを開くただ１つの利用許可キー２６を有する。そして、図３のデコーダー１４は、前記トークン１６のデータ区画２４の１２個全てを開くのに必要な利用許可キー２６の全て（またはただ１つ）を有する。

【００９２】

工程７１８において、その利用許可キー２６によって一切のデータ区画２４が開かなければ、次に工程７２０において、前記デコーダー１４が、正しくないクレデンシャルであるという表示を提供する。前記正しくないクレデンシャルであるという表示は、例えば赤い表示灯および／またはメッセージを表示した画面によって、前記ユーザーインターフェース装置４２を介して提供される。この時点で、前記ユーザーがその用途には誤ったクレデンシャル１２を提示した（即ち、アクセスされるべきデータの全てが提示されたトークン１６上に存在しない）と決定されているので、一切のデータ区画２４は開かない。

【００９３】

次に、工程７２２において、前記デコーダー１４が何らかの追加の利用許可キー２６を有する場合、前記方法７００は次に工程７１６に戻る。前記デコーダー１４がその利用許可キー２６の全てを適用し、一切のデータ区画２４が開かない場合、次に工程７２４において、前記デコーダー１４が利用許可不十分という表示を提供する。前記利用許可不十分という表示は、例えば赤い表示灯および／またはメッセージを表示した画面によって、前記ユーザーインターフェース装置４２を介して提供される。この時点で、前記デコーダー１４は前記データ区画２４の一切にアクセスする利用許可レベルを有さないことが決定されており、前記方法７００は前記データ区画の一切を開かずに終了する。

【００９４】

しかし、工程７１８において、前記適用された利用許可キー２６に対応したデータ区画２４が開いた場合、次に前記方法７００は、工程７２６に進む。前記デコーダー１４が何らかの追加の利用許可キー２６を有する場合、前記方法７００は、次に工程７１６に戻り、前記デコーダー上の前記利用許可キーの全てが適用されるまで、対応したデータ区画２４の全てを開こうと試み続ける。

【００９５】
前記デコーダー１４で開くことが可能な前記データ区画２４の全てが開かれると、前記方法７００は、工程７２８に進む。そこで、前記デコーダー１４は、前記特定の用途に適切な何らかの次の動作を起こし、次に前記方法７００が終了する。例えば、認証のみの境界アクセスの用途において、前記デコーダー１４は、信号を送って、前記アクセスされたデータで何もせずに扉、ゲート、またはその他の境界アクセス遮蔽装置を開けることができる。デジタル運転免許証の用途において、前記デコーダー１４は、前記ユーザーインターフェース装置４２を介して（例えば表示画面を介して）、前記アクセスされたデータを表示することができる。そしてデジタル財布の用途において、前記デコーダー１４は、一体型の、または周辺装置の従来のクレジットカード認証装置と通信して前記トークン１６からの前記クレジットカードのデータを使用して購入の承認を得ることができる。これらの任意の用途において、前記デコーダー１４は、例えば前記ユーザーインターフェース装置４２を介して（例えば緑色灯または表示画面上のメッセージによって）、認証が無事に行われたという表示をも提供するように設定してもよい。

【００９６】
別の方法において、工程７１０において前記トークン１６が開かれた後、前記方法は工程７２８に直接進んで、次に終了する。この別の方法は、例えば、前記トークン１６を開く目的が、前記クレデンシャル１２の提示者が、前記クレデンシャルに登録された利用許可されたユーザーであることを証明する事であり、前記トークンのデータにアクセスすることではない認証のみの用途において使用することができる。または、この別の方法は、前記トークン１６が、前記バイオメトリックキーに基づいてのみ暗号化された１片または１組のデータのみを含む用途に使用できる。いずれにしても、前記データまたはデータセットが利用許可キーに基づいて追加的に暗号化されていないこれらのような用途において、前記別の方法は、個別のデータ区画を開く工程に関連した工程（工程７１４～７２６）を含まない。

【００９７】
さらに別の方法は、前記同一または異なる種類の１より以上のバイオメトリック識別子に基づいて、追加的なセキュリティーの階層のために暗号化されたトークン１６を開くようにデコーダー１４を設定する用途に好適である。例えば、同種の２つのバイオメトリック識別子に基づいて暗号化されたトークン１６を認証するために、前記デコーダー１４は第１の事前選択されたバイオメトリック識別子（例えば右の人差し指の指紋）を前記バイオメトリック入力装置４０に入力するように前記ユーザーを促す。前記デコーダー１４は前記第１の事前選択されたバイオメトリック識別子を受け取り、前記変換ソフトウェア５０を使用して前記第１のバイオメトリック識別子を第１のバイオメトリックキーに変換し、前記解読ソフトウェア４８を使用して前記トークン１６を解読することで前記トークンを開く。また、前記デコーダー１４は、第２の事前選択されたバイオメトリック識別子（例えば左の人差し指の指紋）を前記バイオメトリック入力装置４０に入力するように前記ユーザーを促す。前記デコーダー１４は、前記第２の事前選択されたバイオメトリック識別子を受け取り、前記変換ソフトウェア５０を使用して前記第２のバイオメトリック識別子を第２のバイオメトリックキーに変換する。ここで、前記デコーダー１４は、利用許可キー２６および前記第２のバイオメトリックキーを用いた前記解読ソフトウェア４８を使用して、その前記利用許可されたデータ区画２４を２段階の工程で開く。このようにすれば、前記トークン１６が第１のバイオメトリック識別子を用いて開いた（即ち認証された）後、前記利用許可されたデータ区画２４は、次に、各々それに対応した利用許可キー２６（前記データ区画開放工程の第１段階）および前記第２のバイオメトリックキー（前記データ区画開放工程の第２段階）を順次適用することによって開かれる。勿論、前記２段階のデータ区画開放工程の順序は入れ替え可能である（即ち、前記第２のバイオメトリックキーを適用し、次に前記利用許可キーを適用することによって）。さらに、この別の方法は、（単一のバイオメトリック識別子に基づいた）単一のバイオメトリックキーを使用して前記トークン１６を解読し、前記データ区画２４を（前記利用許可キーと共に）解読

することができる。

【００９８】

別の例において、異なる種類の２つ（若しくはそれ以上）のバイオメトリック入力装置４０を有するデコーダー１４を使用することによって、異なる種類の２つ（若しくはそれ以上）のバイオメトリック識別子に基づいて暗号化したトークン１６を認証する別の方法が提供されている。前記方法は、第１の事前選択されたバイオメトリック識別子（例えば右の人差し指の指紋）を前記バイオメトリック入力装置４０のうちの第１のものに入力し、第２の事前選択されたバイオメトリック識別子（例えば光彩紋）を前記バイオメトリック入力装置のうちの第２のものに入力するように、前記デコーダー１４が前記ユーザーに促すことを除けば、前述したものと類似している。その後、前記デコーダー１４が前記解読ソフトウェア４８を使用して、その利用許可キー２６および前記第２のバイオメトリックキーの両方で前記利用許可されたデータ区画２４を２段階工程で開こうとする点において、前記方法は同様である。デコーダー１４が（同一または異なる種類の）１より以上のバイオメトリック入力装置４０を有する用途において、前記方法は、前記バイオメトリック識別子を順次または同時に受け取る工程を含むことが理解されるであろう。

【００９９】

さらに別の方法において、第１の利用許可キーは、前記バイオメトリックキーと統合されて、前記データ区画を１工程で暗号化／解読するために使用される第２の利用許可キーが生成される。例えば、当業者であればその方法を知っているように、前記第１の利用許可キーおよび前記バイオメトリックキーは、幾つかの構成のうちの何れかで連結することができる。このようにすれば、前記第１の利用許可キーまたは前記バイオメトリックキーに何らかのセキュリティー侵害が発生しても、前記第２の利用許可キーの一部のみをセキュリティー侵害し、全てを侵害しないので、それに対応したデータ区画は依然開くことができない。

前記認証システム１０を説明したので、ここで、その構成要素、前記システムおよびその構成要素の使用法、および幾つかの用途の例を説明する。上述のように、これらは全て、前記ユーザーが前記デコーダーの１つと同じ場所に物理的に存在し、そのデコーダーによって前記識別認証がなされる、「現実の所在」の用途である。これらの用途において、前記データは、１若しくはそれ以上のバイオメトリックキーによってのみ保護でき、または前記データは、１若しくはそれ以上の利用許可キーによって個別に保護され、次に１若しくはそれ以上のバイオメトリックキーによって集合的に保護されたデータ区画内に格納できる。

【実施例１】

【０１００】

例１：デジタル財布の用途

通常の商用の実施形態において、デジタル財布のクレデンシャルは携帯電話の形態であるが、スマートカードまたはその他の対象の形態であることもできる。前記携帯電話のクレデンシャルは、クレジットカードおよびその他のバンクカード（小切手保証カード、デビットカード、キャッシュカードなど）の口座情報を含む前記トークンを格納する。所望ならば、前記トークンは、運転免許証、社員証またはバッジ、保険証、ガソリンスタンドのカードまたは小売店のカード、航空会社のポイントカード、小売店のアフィニティーカード、および／またはレンタルビデオカード上のデータ、並びに家族および友人の写真など、通常、前記ユーザーが従来の財布に入れて持ち歩く追加情報を含むことができる。このように、これは、通常、前記トークンが前記金融データをより高度のセキュリティーで格納する１若しくはそれ以上のデータ区画を含む「保護されたデータ」の用途である。

【０１０１】

使用に際して、前記デコーダーが保護されたデータをアクセスした後、前記デコーダーは、前記ユーザーのバンクカード口座のメニューを（例えば表示画面またはタッチスクリーンのユーザーインターフェース装置を介して）表示し、前記ユーザーはそれから支払い方法を選択できる。一旦前記ユーザーがバンクカード口座を（例えばキーパッドまたはタ

ッチスクリーンのユーザーインターフェース装置を介して）選択すると、前記支払いの決済は従来のバンクカードの決済と同様の方法で行われる。前記デコーダーはユーザーの自宅または事務所にあることもでき、または前記デコーダーはユーザーが商品およびサービスを購入する小売店およびその他の場所にあってもよい。

【実施例２】

【０１０２】

例２：医療保険カードの用途

この用途では、前記クレデンシャルは、保険の適用を申請している患者が実際に保険に加入している本人であることの保証を保険会社に提供する。通常の商用の実施形態において、前記クレデンシャルは磁気ストライプまたはバーコードを用いたチップまたはプラスティックカードからなるスマートカードの形態であって、前記トークンは前記ユーザーの保険情報を保護する。このように、これは、通常、前記トークンが前記保険データをより高度のセキュリティーで格納する１若しくはそれ以上のデータ区画を含む「保護されたデータ」の用途である。

【０１０３】

使用に際して、ユーザーは、保険カードのクレデンシャルおよびバイオメトリック識別子を彼の医院のデコーダーに提示する。前記デコーダーが前記トークンおよび前記ユーザーを認証して前記保護されたデータをアクセスした後、前記患者の保険情報が前記医院の記録に転送される。前記保険データを前記医院の記録に電子的に転送するように前記デコーダーを前記医院のローカルネットワークに（無線または配線で）接続でき、または前記データを人手で転送できる。さらに、所望であれば、デジタル署名を確認できる。この認証工程は患者の訪問毎になされ、前記デコーダーを前記保険会社のサーバーに接続する必要がない。

【実施例３】

【０１０４】

例３：医療パスポートの用途

この用途では、前記クレデンシャルは、医療サービスを提供するときの間違いを低減するのに役立つ。通常の商用の実施形態において、前記クレデンシャルは、磁気ストライプまたはフラッシュ（サム）ドライブを伴うチップまたはプラスティックカードからなるスマートカードの形態であって、前記トークンは、前記ユーザーのために処方された医療サービスに関連した指示を保護する。このように、これは通常、前記トークンが前記医療の指示データをより高度のセキュリティーで格納する１若しくはそれ以上のデータ区画を含む「保護されたデータ」の用途である。

【０１０５】

医療サービスを処方するとき、前記医師は、設定ワークステーションまたはデコーダーを使用して前記クレデンシャルを発行し、前記処方した指示の全てを前記クレデンシャルのトークンに入力する。各指示は、通常、前記トークンの個別のデータ区画に保護されているので、例えば臨床検査部門は前記医師の前記臨床検査部門に対する指示にアクセスする利用許可レベルをそのデコーダー上に有するのみで、前記臨床検査部門は前記トークン上のその他一切の情報へのアクセスは有さない。前記クレデンシャルは、例えば前記臨床検査部門のデコーダー（データ更新構成要素が提供されていれば）または前記医師の設定ワークステーションまたはデコーダーによって、前記臨床検査の結果で更新できる。前記患者が実際の前記処置のために移動するとき、前記クレデンシャルはそれらと共に移動し、前記患者および前記クレデンシャルは前記手術室（ｏｐｅｒａｔｉｏｎ　ｒｏｏｍ：ＯＲ）内のデコーダーによって認証される。次に前記ＯＲのデコーダーが前記患者の前記処置に関する情報の全てをアクセスし、前記情報を前記ＯＲ内に（例えばユーザーインターフェース表示装置を介して）表示するので、前記情報は容易に見落とすことがない。

【実施例４】

【０１０６】

例４：政府発行の身分証明の用途

この用途では、前記クレデンシャルは、安全で認証可能な政府発行の身分証明である。このような身分証明には、運転免許証、パスポート、査証、グリーンカード、社会保障／給付カード、生活保護カード、およびその他政府発行の身分証明が含まれる。これら政府発行のクレデンシャルは、州の車両管理局または連邦政府の社会保障庁などの政府関係機関によって発行され、これらの機関は前記クレデンシャルを発行する設定ワークステーションを有する。通常の商用の実施形態において、前記クレデンシャルは、磁気ストライプを用いたチップまたはプラスティックカードからなるスマートカードの形態であって、前記トークンは、通常これらの身分証明上にあるデータを保護する。このように、これらは通常、前記トークンが前記身分証明のデータをより高度のセキュリティーで格納する１若しくはそれ以上のデータ区画を含む「保護されたデータ」の用途である。

【実施例５】

【０１０７】

例５：境界アクセスの用途

典型的な境界アクセスの用途は、建物および駐車場ガレージ（例えば政府、軍、産業用）、基地（例えば軍施設）、その他施設（例えば水処理施設、原子力発電所）、およびこれら任意の場所内の保護された区域／区画（例えば生物学研究所、コンピューター室）への進入を保護するためのものである。これらの用途では、前記クレデンシャルは通常、保護されている区域の従業員、訪問者、業者、または住民に交付された携帯電話、キーフォブ、スマートカード、またはＩＤバッジの形態である。このように、これは通常、前記トークンを開くことで前記ユーザーが認証され、前記トークン内に保護されたデータはそれ以上一切使用されない「認証のみ」の用途である。従って、前記トークン内のデータはランダムであることができ、データ区画内に保護される必要もない。追加的なセキュリティーのため、および／またはユーザーを識別するデータ（例えばユーザーの名前）を格納するために、前記データを１若しくはそれ以上のデータ区画内に保護することもできる。

【０１０８】

使用に際して、前記デコーダーが前記トークンを開いた後、前記デコーダーは、（例えば点灯した表示灯またはユーザーインターフェース装置の表示画面上のメッセージを介して）「ユーザーが認証されました」という表示を提供する。この時点で、警備担当者は、前記ユーザーの前記保護された区域内への進入を手動で許可することができる。用途によっては、前記デコーダーは作動装置または遮蔽装置と（例えば無線でまたは配線によって）通信して扉、ゲート、またはその他の遮蔽対象を開けることで、前記ユーザーの前記保護された区域への進入を自動的に許可する。さらに、用途によっては、前記保護されたデータ（トークンのデータ区画内またはデータ区画のないトークン内に拘らず）は、前記ユーザーの一定のセキュリティーレベルに対応する。従って、前記システムは、複数の保護された区画を有する施設内で異なるセキュリティーレベル（例えば低、中、高、極秘）で使用し、前記デコーダーはユーザーを認証しても、その要求されるセキュリティー許可レベルが前記トークン上に格納されていなければ一定の保護された区域へのアクセスを拒否することができる。このようにすれば、前記システムを使用してユーザーを認証し、また認証されたユーザーが保護された区域に進入することを（前記必要なセキュリティー許可によって）許可されているかを決定することができる。

【実施例６】

【０１０９】

例６：航空運輸産業（Ａｉｒ　Ｔｒａｎｓｐｏｒｔ　Ｉｎｄｕｃｔｒｙ：ＡＴＩ）従事者の用途

この用途は、前記航空運輸産業内の従業員および業者に交付されるＩＤクレデンシャルを提供する。前記クレデンシャルは通常、パイロット、客室乗務員、荷物係、ターミナルの売店員などに交付されるスマートカードまたはＩＤバッジの形態である。このように、これは通常、「認証のみ」の用途であるが、追加的セキュリティーのために、ユーザーを識別するデータ（例えばユーザーの名前）またはセキュリティー許可レベルデータを前記トークン内または前記トークンのデータ区画内に格納することが望ましいかもしれない。

【０１１０】
この用途では、前記システムは前記境界アクセスの用途と同様に機能する。しかし、この用途では、前記システムは、ＡＴＩの所在地相互間の、または中央に位置するデータベースとの接続なしで、複数の所在地に亘るＡＴＩシステム（例えば、従業員アクセスシステム、搭乗客アクセスシステムなど）の相互運用性を提供する。例えば、任意の航空会社の設定ワークステーションが任意のパイロットのために発行したＩＤクレデンシャルは、前記ＡＴＩシステム内の任意の空港のデコーダーで機能する。前記ＡＴＩシステムに接続されたＡＴＩ制御サーバーが前記デコーダーに取り消し信号を送ると、前記ＩＤクレデンシャルは、前記ＡＴＩシステム内の任意の空港の任意のデコーダーによって取り消すことができる。しかし、ユーザー認証（取り消しは除外して）は、中央のデータベースまたはサーバーに接続する必要なく前記デコーダーでローカルに行われる。

【実施例７】

【０１１１】
例７：航空運輸産業（Ａｉｒ　Ｔｒａｎｓｐｏｒｔ　Ｉｎｄｕｓｔｒｙ：ＡＴＩ）乗客の用途

この用途は、航空会社の乗客が前記ＡＴＩ内を旅行する際の認証用である。前記クレデンシャルは通常、前記航空会社の乗客に発行される、暗号化されたデータを各々格納した印刷されたバーコードを含む従来の紙の搭乗券、または携帯電話のクレデンシャルに格納された搭乗券トークンなどの搭乗券の形態である。このように、これは、通常、「認証のみ」の用途であるが、追加的なセキュリティーのために、ユーザーを識別するデータ（例えば、ユーザーの名前、フライト情報など）を前記トークン内または前記トークンのデータ区画内に格納することが望ましいかもしれない。

【０１１２】
乗客であるユーザーが一度（例えば、上述したような設定ワークステーション、航空会社のウェブサーバー、家庭のデスクトップまたはラップトップコンピューターなどから）登録をし、ネットワークに接続されたＡＴＩサーバー（またはその他のコンピューター装置）が前記ユーザーによって入力されたバイオメトリック識別子から公開バイオメトリックキーを生成する。次に、前記公開バイオメトリックキーは、各個別の航空会社またはそれ以外の場所の中央のＡＴＩデータベース内に保存され、後に（例えば前記航空会社の、またはＡＴＩのウェブサイトのサーバーによって）アクセスされて前記搭乗券のトークンを生成する。前記ユーザーが航空会社の搭乗券を受け取る（例えば、家庭のコンピューター、空港のキオスク、携帯電話などで印刷またはダウンロードする）準備ができているとき、前記公開バイオメトリックキーをアクセスし、それを使用して前記データを暗号化して前記搭乗券のトークンを形成する。従って、前記ユーザーは、前記公開バイオメトリックキーに基づいて暗号化された搭乗券のトークンを受け取る。

【０１１３】
前記初期のユーザー登録は、ほとんど何処でも、普通郵便などによって人手でさえ行えることに注目すべきである。しかし、それがＡＴＩネットワークに接続されたコンピューター（例えば、設定ワークステーション、キオスクなど）でない場合、前記バイオメトリック識別子を入力することは（少なくとも絶対的な安全性を伴っては）できず、前記公開バイオメトリックキーを生成することはできない。従って、安全性のために、前記公開バイオメトリックキーを生成する前記バイオメトリック識別子は、ＡＴＩネットワークに接続されたコンピューターからのみ前記ユーザーによって入力できる。従って、前記初期のユーザー登録がＡＴＩネットワークに接続されたコンピューターからなされた場合、前記ユーザーはその場でバイオメトリック識別子を入力する。しかし、前記初期の登録がＡＴＩネットワークに接続されたコンピューターからなされない場合（例えば、航空会社のウェブサーバーから家庭のコンピューターまたはラップトップコンピューターを介して、または郵送で、など）、前記ユーザーは、初回は、ＡＴＩネットワークに接続されたコンピューターから搭乗券トークンを受け取らなければ（例えば、印刷、ダウンロードなどをしなければ）ならない。前記ＡＴＩシステムは、将来の用途のために前記バイオメトリック

識別子をこの時点で有するので、前記ユーザーは、将来の搭乗券のトークンをＡＴＩネットワークに接続されたコンピューター以外から（例えば、航空会社のウェブサイトのサーバーから家庭のデスクトップまたはラップトップコンピューターなどを介して）受け取ることができる。

【０１１４】

前記認証は、前記ユーザーが前記空港で（紙の搭乗券上、携帯電話上などの）前記搭乗券のトークンおよび前記正しいバイオメトリック識別子をデコーダーに提示するときに、なされる。前記空港で前記バイオメトリック識別子に基づいて前記デコーダーが生成した、前記非公開のバイオメトリックキーのみが、前記搭乗券のトークンを開くことができる。このようにすれば、前記ユーザー（前記非公開のバイオメトリックキーを生成するために必要な前記バイオメトリック識別子を有する個人のみ）以外は、前記搭乗券のトークンを使用できない。従って、前記空港内の前記デコーダーを使用して、前記乗客／ユーザーが前記空港内を移動する際に彼ら全員を正確に認証でき、従って、これらデコーダーは、従来のシステムよりもはるかに少ない費用で、乗客の遅延をはるかに小さくし、はるかにより安全な空港を提供できる。

【０１１５】

さらに、前記搭乗券のクレデンシャル上のトークンは、金融支払い情報（例えばバンクカード口座のデータ）を格納できる。手荷物で両手の塞がった乗客は財布を探るための手が空かないが、彼らは普通、その片方の手に搭乗券を持っている。従って、彼らは、彼らがその状態でもアクセスできる前記搭乗券のクレデンシャルおよびバイオメトリック識別子の両方を提示することによって、そのコンコースでの（例えば食べ物、雑誌などの）購入を行うことができる。

【実施例８】

【０１１６】

例８：航空運輸産業（Ａｉｒ　Ｔｒａｎｓｐｏｒｔ　Ｉｎｄｕｓｔｒｙ：ＡＴＩ）の手荷物の用途

この用途は、空港で乗客が手荷物を取り上げ、その手荷物受取所から持ち去るとき、そのバッグが実際にその乗客のものであることを保証する。この用途では、前記ＩＤクレデンシャルは、通常、バーコードの付いたチップまたはプラスティックまたは紙のタグからなるスマートカードの形態である。これは、通常、「認証のみ」の用途であるが、追加的なセキュリティーのために、前記トークン内または前記トークンのデータ区画内にユーザーを識別するデータ（例えばユーザーの名前）を格納することが望ましいかもしれない。

【０１１７】

乗客であるユーザーが、空港の搭乗手続き装置（例えばそのターミナル内のメイン搭乗手続きカウンターまたは前記ターミナルの外のカーブサイド搭乗手続きカウンターのネットワークに接続されたコンピューター）でフライトのチェックインを行うとき、（例えば任意の搭乗手続きの場所で）その上にトークンが印刷されたバッグタグのクレデンシャルが生成され、前記バッグタグのクレデンシャルは預けたバッグに取り付けられる。前記乗客が前記フライトの後で前記バッグを回収し、前記手荷物受取所の出口に移動するとき、デコーダーが前記バッグタグのクレデンシャル上のトークンを走査し、前記乗客が前記デコーダーにバイオメトリック識別子を提示する。前記デコーダーが、認証が行われたと表示すれば、前記手荷物はその乗客のものである。

【０１１８】

ここで図８を参照して、本発明の第２の実施例による識別認証システム１１０が示されている。前記システムは、少なくとも１つのクレデンシャル１１２と、少なくとも１つのデコーダー１１４と、少なくとも１つのリモート認証サーバー１５２とを含む。この実施形態のシステム１１０は、例えばネットワークのアクセス、ウェブ上の決済などのために前記ユーザーが「リモートに」認証される、リモートな所在または仮想アプリケーションの用途のために設計されている。

【０１１９】

前記クレデンシャル１１２は、前記第１の例のシステム１０で説明したものと同一または類似のクレデンシャルによって提供される。例えば、前記クレデンシャル１１２は各々、１若しくはそれ以上のデータ区画１２４を含むことができるトークン１１６を格納し、これら構成要素の各々が上述のものと同一または類似のものである、少なくとも１つのデータ記憶装置１１８を含む。さらに、前記デコーダー１１４は、前記第１の例のシステム１０で説明したそれらと同様である。例えば、前記デコーダー１１４は各々、その構成要素の各々が上述のものと同一または類似している、少なくとも１つのバイオメトリック入力装置１４０と、少なくとも１つのユーザーインターフェース装置１４２と、少なくとも１つのトークンインターフェース装置１４４と、少なくとも１つのプログラムされたプロセッサーシステム１４６とを含む（またはこれらに動作可能に接続されている）。

【０１２０】

この実施形態において、上述のシステム１０および方法７００でなされたように、バイオメトリック識別子をバイオメトリックキーに変換し、前記バイオメトリックキーを適用して前記トークン１６を解読し、利用許可キー１２６を適用して前記データ区画１２４を解読する。しかし、この実施形態では、前記バイオメトリック識別子の前記バイオメトリックキーへの変換、および前記バイオメトリックキーおよび前記利用許可キー１２６を適用した前記トークン１１６および前記データ区画１２４の解読は、前記デコーダー１１４上でローカルに行う代わりに、リモート認証サーバー１５２上でリモートに行う。

【０１２１】

従って、前記デコーダー１１４がネットワークインターフェース装置１５４を有し、前記認証サーバー１５２がネットワークインターフェース装置１５６を有することで、前記デコーダーおよび前記認証サーバーが、通信ネットワーク１５８に接続され、相互に通信することが可能となる。前記ネットワークインターフェース装置１５４および１５６は、それぞれ前記デコーダー１１４および前記認証サーバー１５２と一体化した構成要素であってもよく、またはそれらに動作可能に（無線でまたは配線によって）接続された別個の構成要素であってもよい。前記通信ネットワーク１５８は、グローバル通信ネットワーク（例えばインターネット）、ローカル・エリア・ネットワーク（ｌｏｃａｌ　ａｒｅａ　ｎｅｔｗｏｒｋ：ＬＡＮ）、セルラーネットワークなどであってよい。

【０１２２】

さらに、前記デコーダー１１４は、前記プログラムされたプロセッサー１４６用の暗号化ソフトウェア１５０（上述のデコーダー１４が解読ソフトウェア４８を含むのに対して）を含む。そして、前記デコーダー１１４は、解読ソフトウェアと、変換ソフトウェアと、および／または前記利用許可キー１２６とを有さない。（従って、前記デコーダー１１４は、前記バイオメトリックキーおよび前記利用許可キー１２６を適用して前記トークン１１６および前記データ区画１２６を復号／解読することでそれらを開く機能を有さず、前記リモート認証サーバー１５２の収集装置として機能する。いずれにしろ、一貫性のために、本明細書内ではこのデータ収集装置のために「デコーダー」という用語を使用する。）その代わり、前記認証サーバー１５２は、その構成要素の各々が上述のものと同一である、または類似している、解読ソフトウェア１４８と、変換ソフトウェア１５０と、利用許可キー１２６とを含むソフトウェア要素を格納し、および／またはアクセスするプログラムされたプロセッサーシステム１６０を有する。さらに、前記プログラムされたプロセッサーシステム１６０は、当該技術分野で既知の従来の種類のワン・タイム・キー（ｏｎｅ－ｔｉｍｅ　ｋｅｙ：ＯＴＫ）生成器１６２を格納し、および／またはアクセスする。例えば、前記ＯＴＫ生成器１６２は、固有のワンタイム暗号化キーを生成する既知の公開キー／非公開キー解読技術に基づくことができる。

【０１２３】

明瞭性のために個別には図示しないが、前記プログラムされたプロセッサーシステム１６０は、前記認証サーバー１５２の総合的な処理能力を一体となって定義する、１若しくはそれ以上のプロセッサーと、メモリーと、および／またはその他の論理回路とを含む。当業者であれば理解できるように、前記ソフトウェア要素は、図示の目的で概念的に示さ

れており、メモリー内に同時に存在しないかもしれず、またはその全体が存在しないかもしれない。むしろ、既知のコンピューターの動作として、前記ソフトウェア要素またはその部分は、メモリーチップ、固定媒体のローカルドライブ、交換型媒体のローカルドライブ、および／またはネットワークに接続されたリモートコンピューターまたは記憶装置から必要に応じて取り込むことができる。さらに、前記ソフトウェア要素の機能は、より多くのソフトウェア要素に分散でき、またはより少ない要素に統合／集約できる。オペレーティングシステム、グラフィック・ユーザー・インターフェース、ユーティリティー、インターフェース・デバイス・ドライバーなどのコンピューティングシステムに一般的に含まれる追加のソフトウェア要素を含んでもよいが、明瞭性のためにこれらは図示しない。本明細書内の説明を考慮して、当業者であれば好適なソフトウェアを提供し、あるいはプログラムし、または前記認証サーバー１５２を構成して下記のリモート認証方法を容易に実行できるであろう。さらに、保守の機能のために、インターフェース装置（キーボード、マウス、モニターなど）を前記サーバー１５２に接続してもよい。

【０１２４】

この実施形態において、前記デコーダー１１４は、前記バイオメトリック識別子および前記トークン１１６を受け取り、前記リモート認証サーバー１５２からＯＴＫを受け取り、前記ＯＴＫを使用して前記トークンおよび前記バイオメトリック識別子をパッケージに暗号化し、前記暗号化されたパッケージを前記認証サーバーに転送する。次に、前記認証サーバー１５２は、（そもそも前記サーバーが生成した）前記ＯＴＫを使用して前記暗号化されたパッケージを開くことで、前記トークン１１６および前記バイオメトリック識別子にアクセスする。この時点で、前記認証サーバー１５２は、上述のローカル認証システム１０で前記デコーダー１４が行うのと同様に、前記変換ソフトウェア１５０を使用して前記バイオメトリック識別子を前記バイオメトリックキーに変換し、前記解読ソフトウェア１４８を使用して前記バイオメトリックキーを前記トークン１１６に適用し、前記解読ソフトウェアを使用して前記利用許可キー１２６を前記データ区画１２４に適用することができる。

【０１２５】

別の実施形態において、前記デコーダーは、また、前記解読ソフトウェア、変換ソフトウェア、および前記利用許可キーのコピーをも含む。この実施形態では、前記デコーダーは、（前記第１の実施例のデコーダーのように）ローカル認証に使用でき、また（前記第２の実施例のデコーダーのように）リモート認証にも使用できる。

【０１２６】

リモート認証システム１１０で使用するデコーダー１１４および認証サーバー１５２の実施例を説明したので、ここで、前記デコーダーおよび認証サーバーを使用して前記トークン１１６を開く方法を説明する。前記リモートトークン開放方法は、今説明したデコーダー１１４、または前記必要な構成要素を含むようになっている前記第１の実施形態のデコーダー１４と共に前記認証サーバー１５２を使用し、この方法のためにプログラムをして実行できることが理解されるであろう。または、前記リモートトークン開放方法は、列挙した工程を実行する同様の構成要素を有するその他類似の装置を使用して実行できる。便宜上、前記リモートトークン開放方法については、図８のデコーダー１１４および認証サーバー１５２を使用し、プログラムしてトークン１１６を開く工程の説明と共に説明する。

【０１２７】

図９は、図８のデコーダー１１４を使用したリモートトークン開放方法の例９００を示す。前記リモートトークン開放方法９００は、前記デコーダー１１４が前記ユーザーから前記トークン１１６および前記バイオメトリック識別子を受け取る工程９０２から開始する。この工程は、前述のローカル認証方法７００の中で集合的に９０２として示された工程と同様であり、簡潔性のために、ここでは詳細を繰り返さない。

【０１２８】

次に、工程９０４において、前記デコーダー１１４が前記認証サーバー１５２からＯＴ

Ｋを取り込む。前記デコーダー１１４は、前記ＯＴＫの要求をそのネットワークインターフェース装置１５４を介して前記認証サーバー１５２に送り、次に前記認証サーバーからそのネットワークインターフェース装置を介して前記ＯＴＫを受け取ることによってこれを行う。次に、工程９０６において、前記デコーダー１１４が前記暗号化ソフトウェア１５０を使用して前記トークン１１６および前記バイオメトリック識別子をパッケージに暗号化する。そして、次に工程９０８において、前記デコーダー１１４が、前記暗号化されたパッケージを前記認証サーバー１５２に送って前記認証サーバーによって前記トークン１１６をリモートに開く。

【０１２９】

図８の認証サーバー１５２を使用したリモートトークン開放方法の例１０００を図１０に示す。前記リモートトークン開放方法１０００は、前記認証サーバー１５２が前記デコーダー１１４から前記ＯＴＫの要求を受け取る工程１００２から開始する。前記認証サーバー１５２は、そのネットワークインターフェース装置１５６を介して前記ＯＴＫの要求を受け取る。次に、工程１００２において、前記認証サーバー１５２が、前記ＯＴＫ生成器１６２を使用して前記固有のＯＴＫを生成し、そのネットワークインターフェース装置１５６を使用して前記ＯＴＫを前記デコーダー１１４に送る。さらに、前記認証サーバー１５２は、前記ＯＴＫを、少なくとも一時的に、メモリー内に格納する。

【０１３０】

次に、工程１００６において、前記認証サーバー１５２が、前記デコーダー１１４から前記暗号化されたパッケージを受け取る。前記認証サーバー１５２は、そのネットワークインターフェース装置１５６を介して前記暗号化されたパッケージを受け取る。次に、工程１００８において、前記認証サーバー１５２が、前記解読ソフトウェア１４８を使用して前記ＯＴＫを適用して前記暗号化されたパッケージを開く。前記暗号化されたパッケージが開いたので、前記認証サーバー１５２はこの時点で、前記トークン１１６および前記バイオメトリック識別子へのアクセスを有する。

【０１３１】

前記トークン開放方法１０００は、ローカルデコーダーのように、前記認証サーバー１５２が前記トークン１１６を処理する工程１０１０で終了する。このように、前記認証サーバー１５２は、前記変換ソフトウェア１５０を使用して前記バイオメトリック識別子をバイオトリックキーに変換し、前記解読ソフトウェア１４８を使用して前記バイオメトリックキーを適用して前記トークン１１６を開き、前記解読ソフトウェアを使用して前記利用許可キー１２６を適用して前記データ区画１２４を開き、この時点で認証された前記ユーザーに関する次の動作を開始する。この工程は、前述したローカル認証方法７００内に集合的に１０１０として示した工程と同様であり、簡潔性のために、ここではその詳細は繰り返さない。

【０１３２】

用途によっては、前記次の動作とは、前記認証サーバー１５２がそのネットワークインターフェース装置１５６を介して前記トークン１１６からのデータをネットワークに接続された別のサーバーに送ってさらに先の処理を行うことである。例えば、前記クレデンシャル１１６が、クレジットカード情報を格納するトークン１１６を有するデジタル財布である用途において、前記認証サーバー１５２は、前記クレジットカード情報を、支払い処理を行う前記クレジットカード会社の決済サーバーに直接送る。このようにすれば、この時点で保護されていない前記クレジットカードデータは、前記ローカルデコーダー１１４に送り返されない。これによってリモート認証が可能となり、かつ、前記システム（従って前記ユーザーおよび前記データ）をセキュリティー侵害から保護する厳格な管理が維持される。

【０１３３】

今説明したリモート認証システム１１０、および方法９００および１０００は、本発明の例示である。従って、前記リモート認証システム１１０、および方法９００および１０００は、例えば、本明細書内で説明した前記ローカル認証システム１０および方法７００

のための別の実施形態および方法、並びに当業者であれば容易に識別できるその他の変形の適合を含むようになっていてもよいことは、理解されるであろう。

【０１３４】

前記認証システム１１０、その構成要素、および前記システムおよびその構成要素の使用方法を説明したので、ここで幾つかの用途の例を説明する。上述のように、これらは全て、前記ユーザーが前記デコーダーから「リモート」に認証される、リモートな所在または仮想アプリケーションである。これらの用途では、前記データは１若しくはそれ以上のバイオメトリックキーによってのみ保護でき、または前記データは１若しくはそれ以上の利用許可キーによって個別に保護され、次に１若しくはそれ以上のバイオメトリックキーによって集合的に保護されたデータ区画内に格納できる。

【実施例９】

【０１３５】

例９：ゲームの用途

この用途は、オンラインゲームおよび携帯ゲーム（即ち賭博又はギャンブル）を提供する。具体的には、この用途は、賭博産業、公共（未成年および不正賭博の観点から）、および税務当局にとって重要な、賭博会社が賭けの相手側のユーザーが誰であるかを知る方法を提供する。通常の商用の実施形態において、賭博クレデンシャルは、携帯電話、ラップトップ、ＰＤＡ、またはその他の携帯型電子装置の形態であるが、前記クレデンシャルは、スマートカードまたはその他のプラスティックカードによって提供することもできる。前記賭博クレデンシャルは、ユーザーの口座および支払い情報（例えばバンクカードのデータ、当座預金口座のデータ）を含む前記トークンを格納する。このように、これは、通常、前記トークンがより高度のセキュリティーで前記金融データを格納する１若しくはそれ以上のデータ区画を含む「保護されたデータ」の用途である。

【０１３６】

使用に際して、ユーザーは、携帯電話、ラップトップ、ＰＤＡなどを使用して賭博ウェブサイトに接続し、（例えば前記ユーザーの自宅の）デコーダーに彼のクレデンシャルのトークンおよびバイオメトリック識別子を入力する。前記デコーダーは、前記認証を実行する認証サーバーに接続する。前記認証サーバーは、前記賭博ウェブサイト会社によって、または前記賭博会社のために前記支払いを処理する第三者によって、所有／管理できる。前記クレデンシャルが賭博を行うために使用できる携帯型電子装置（例えば携帯電話、ラップトップ、ＰＤＡ）である実施形態において、前記クレデンシャルは前記トークンを含むことができ、また前記デコーダーの構成要素をも含むことができる。このようにすれば、前記ユーザーは、ネットワークアクセスのある所であれば何処でも賭博を行うことができる。さらに、この用途は、オンライン賭博ウェブサイトだけではなく、賭博場でも使用できる。

【実施例１０】

【０１３７】

例１０：ネットワークアクセスの用途

この用途は、コンピューターネットワーク上のユーザー認証を提供する。具体的には、この用途は、ネットワーク管理者が、誰が彼らのネットワーク上にいるかを確実に知ることを可能とし、ウェブマスターが、誰が彼らのウェブサイトに接続しているかを確実に知ることを可能とする。これは、オンラインバンキング、マイスペースまたはフェイスブックのような会員制ウェブサイト、またはそのサイトに誰が実際に接続しているかを確実に知ることが重要なその他任意のウェブサイトにとって特に有用である。この用途は、また、アダルトなどのウェブサイトまたは未成年者に合法的に販売することのできないその他のウェブサイト上で誰が購入しているかを確実に決定するためにも使用できる。前記クレデンシャルは、本明細書内で説明したほとんど任意の形態であることができ、前記デコーダーは、前記ユーザーのいる場所（例えば、事務所のコンピューター、家庭のコンピューター、携帯電話など）に位置できる。このように、これは、通常、「認証のみ」の用途であるが、追加的なセキュリティーのために、前記トークンまたは前記トーク内のデータ区

画にユーザーを識別するデータ（例えばユーザーの名前）を格納することが望ましいかもしれない。

【０１３８】

第３の実施形態において、前記トークンは、ＰＤＡ、携帯電話、またはラップトップのクレデンシャルなどの携帯型電子装置上に格納され、企業またはユーザーの機密情報などのデータを含む。この実施形態において、前記トークンは、前記認証サーバーによって格納またはアクセス可能な第１のＯＴＫに基づいて（バイオメトリックキーに基づく代わりに）暗号化される。前記ユーザーが前記データをアクセスしたいとき、彼らは、認証される必要がある。この認証は携帯型電子装置上で行われず、前記認証サーバー上で行われる。前記装置は、前記ユーザーから前記バイオメトリック識別子を収集し、前記認証サーバーから第２のＯＴＫを取得し、前記第２のＯＴＫに基づいて前記トークンおよび前記バイオメトリック識別子をパッケージに暗号化し、前記暗号化されたパッケージを前記認証サーバーに送って前記認証処理を実施させる。前記認証処理が完了すると、前記認証サーバーは、前記データの暗号化のための前記第１のＯＴＫおよび前記データの再暗号化のための第３のＯＴＫを前記装置に送る。前記装置は、次に、前記第１のＯＴＫを使用して前記データを解読する。前記データは常に暗号化されているので、前記第１のＯＴＫは１度だけ使用され、前記第１のＯＴＫを取得できる個人のみが利用許可されたユーザーであり、たとえ前記装置を紛失しても、前記装置上のデータは常に安全である。前記データを使用した後、もしくは時間切れ後に、前記第３のＯＴＫは前記データを再暗号化する。

【０１３９】

本発明は、本明細書内に説明し、および／または図示した特定の装置、方法、条件、またはパラメーターに限定されず、本明細書内で使用される用語は、例としてのみの特定の実施形態を説明する目的のものであることを理解すべきである。従って、前記用語は、広義に解釈すべく意図したもので、請求の発明を不必要に限定すべく意図したものではない。例えば、添付の請求項を含む本明細書内で使用されるとき、その文脈が明らかに別段の定めをした場合を除き、「ａ」、「ａｎ」、「ｏｎｅ」という単数形はその複数形を含み、「または」は「および／または」を意味し、特定の数値への参照は少なくともその特定の値を含む。さらに、本明細書内で説明した任意の方法は、説明の工程順に限定されるべく意図したものではなく、本明細書内で明示的に別段の定めをした場合を除き、その他の順序で実行できる。

【０１４０】

本発明を例示的な形態で図示し、説明したが、当業者であれば、以下の請求項に定義した通りの本発明の趣旨および範囲から逸脱することなく、これらに多くの変更、追加、および削除を施すことができることは明白である。

【図１】

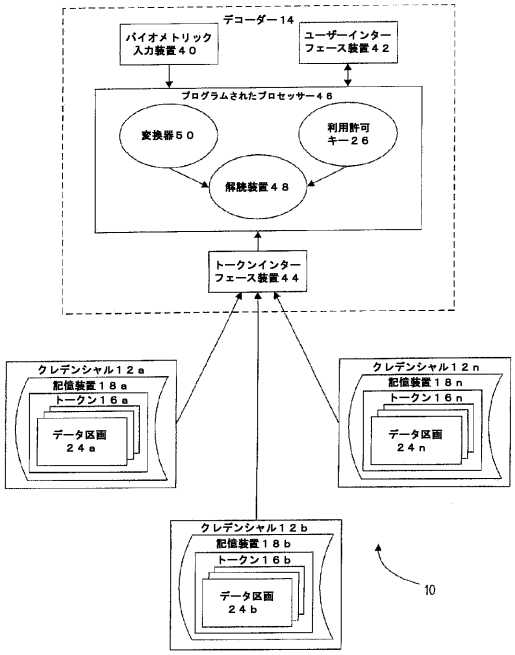

図１

【図２】

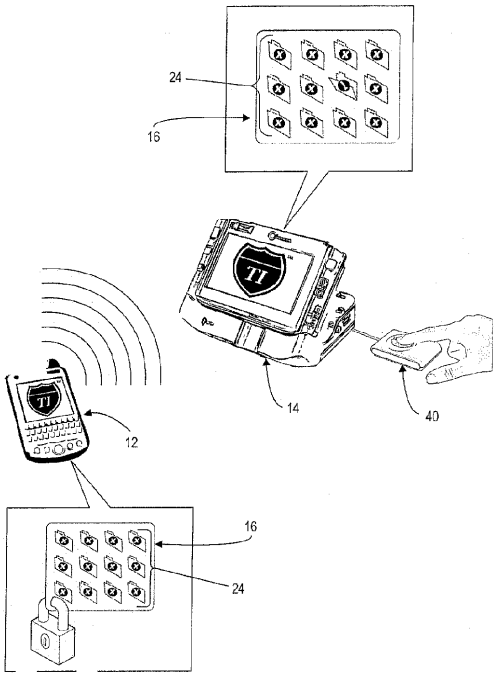

図２

【図３】

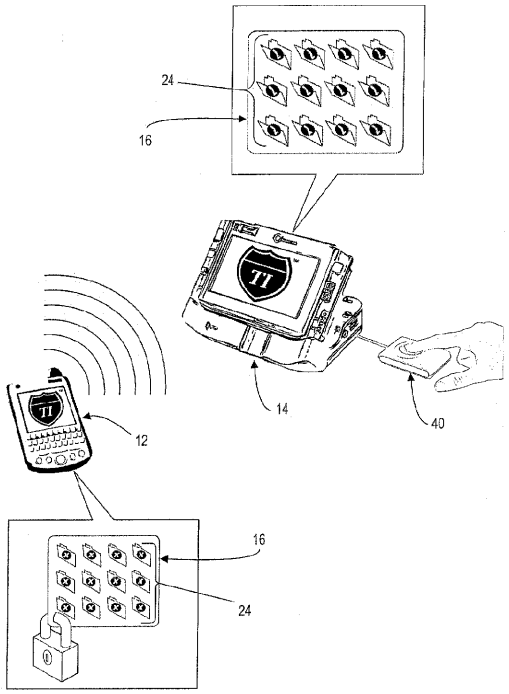

図３

【図４】

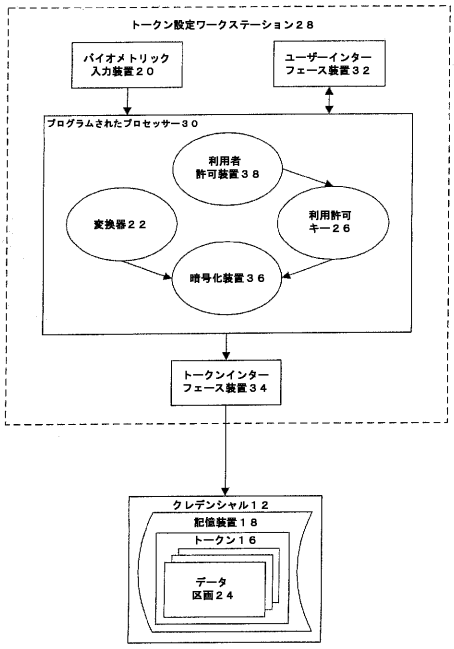

図４

【図５】

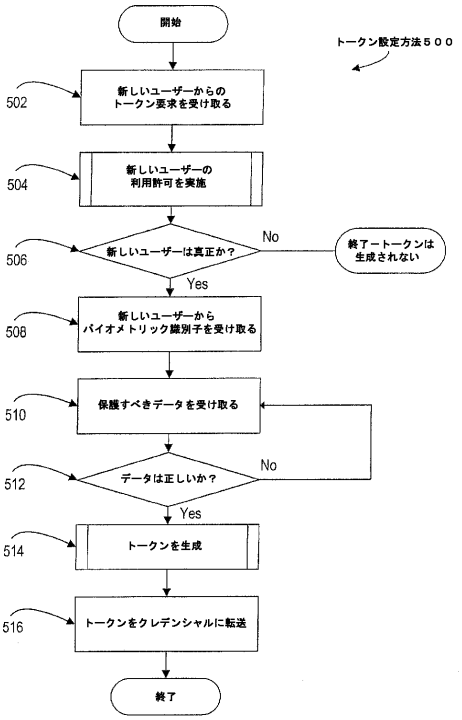

図５

【図６】

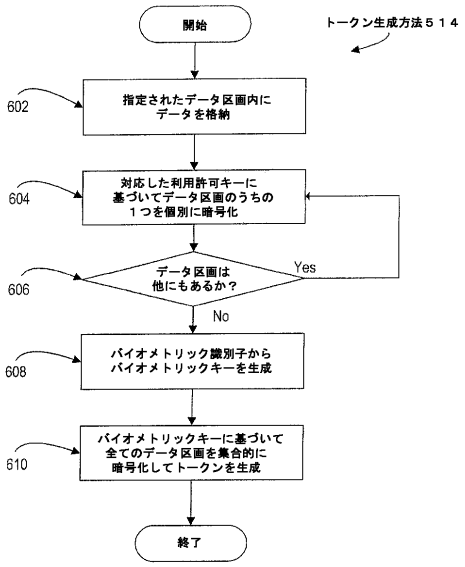

図６

【図７】

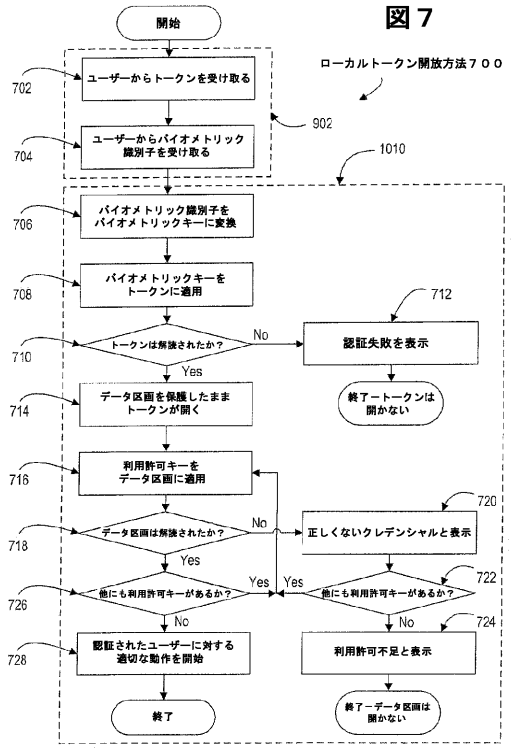

図７

【図８】

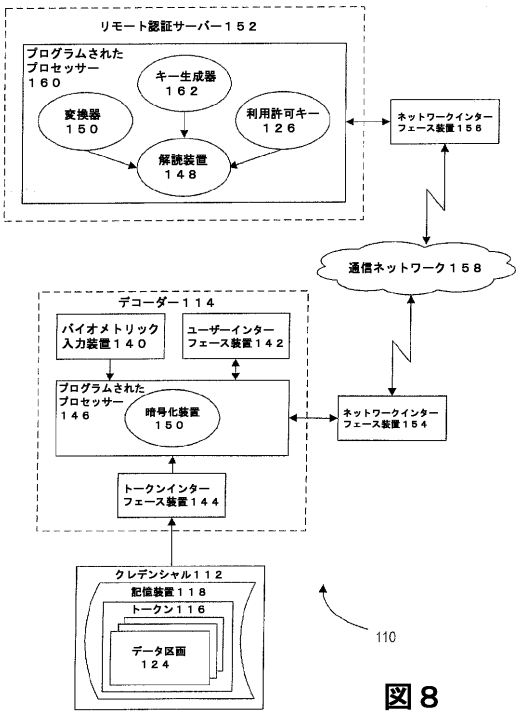

図８

【図９】

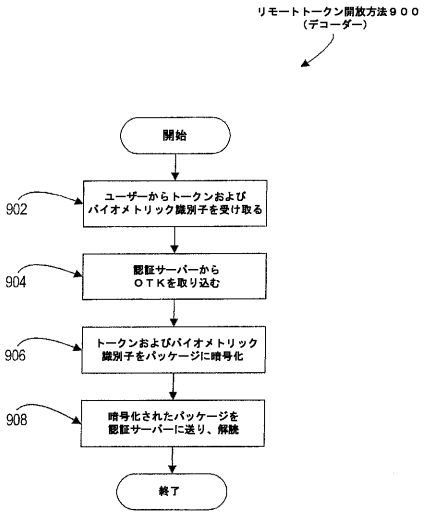
リモートトークン開放方法９００
（デコーダー）
開始
902
ユーザーからトークンおよび
バイオメトリック識別子を受け取る
904
認証サーバーから
ＯＴＫを取り込む
906
トークンおよびバイオメトリック
識別子をパッケージに暗号化
908
暗号化されたパッケージを
認証サーバーに送り、解読
終了

図９

【図１０】

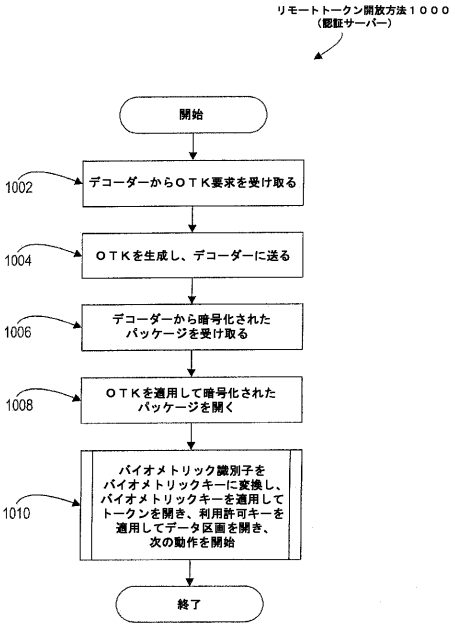
リモートトークン開放方法１０００
（認証サーバー）
開始
1002
デコーダーからＯＴＫ要求を受け取る
1004
ＯＴＫを生成し、デコーダーに送る
1006
デコーダーから暗号化された
パッケージを受け取る
1008
ＯＴＫを適用して暗号化された
パッケージを開く
1010
バイオメトリック識別子を
バイオメトリックキーに変換し、
バイオメトリックキーを適用して
トークンを開き、利用許可キーを
適用してデータ区画を開き、
次の動作を開始
終了

図１０

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 08/69958

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04K 1/00 (2008.04)
USPC - 713/182
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC (8): H04K 1/00 (2008.04)
USPC: 713/182

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 713/159, 168, 185, 186; 726/2, 4, 5, 17-19 (See keywords below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Pub WEST (USPT, PGPB, JPAB, EPAB), Google Scholar.
Search Terms Used: user, identity authentication, token, encrypt, decrypt, biometric key, sensor, storage, token identifier, one time, wallet, security device, baggage check-in, insurance card.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2002/0124176 A1 (EPSTEIN), 05 September 2002 (05.09.2002), entire document, especially abstract; FIGS. 2-4; para [0018]-[0019]; [0026]-[0029]; [0030]-[0031] and[0032]-[0035].	1-9, 14-16 and 18-30 --- 10-13, 17 and 31-40
Y	US 2007/0024551 A1 (GELBMAN), 01 February 2007 (01.02.2007), entire document, especially para [0112]-[0113]; [0115]; [0118]; [0125] and [0130]-[0133].	10-13, 17 and 35
Y	US 2003/0070101 A1 (BUSCEMI), 10 April 2003 (10.04.2003), entire document, especially para [0013]-[0016]; [0019]-[0021]; [0023]-[0025] and [0030].	31-40

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 September 2008 (30.09.2008)	07 OCT 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2007)

フロントページの続き

(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,HR,HU,IE,IS,IT,LT,LU,LV,MC,MT,NL,NO,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,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 ジョブマン、ブライアン、シー.
アメリカ合衆国、３０００４ ジョージア州、アルファレッタ、１４４４５ ウィンダム ファームズ ドライブ

Ｆターム(参考) 5B017 AA03 BA07 BB02 CA16
5B285 AA01 BA01 BA08 CA16 CA41 CA44 CB12 CB14 CB15 CB17
CB18 CB23 CB52 CB57 CB64 CB73 CB74 DA10
5J104 AA07 AA16 AA32 DA04 EA03 EA04 EA17 JA03 KA01 KA16
NA02 NA05 NA37 NA38 PA07

【要約の続き】
前記トークンが解読される。
【選択図】 図１