

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4792405号
(P4792405)

(45) 発行日 平成23年10月12日(2011.10.12)

(24) 登録日 平成23年7月29日(2011.7.29)

(51) Int. Cl. F I
G06K 19/10 (2006.01) G O 6 K 19/00 S
G06K 17/00 (2006.01) G O 6 K 17/00 V

請求項の数 45 (全 22 頁)

(21) 出願番号	特願2006-553085 (P2006-553085)	(73) 特許権者	505318994
(86) (22) 出願日	平成17年2月7日(2005.2.7)		ブリサイス バイオメトリクス アクチボ
(65) 公表番号	特表2007-522580 (P2007-522580A)		ラゲット
(43) 公表日	平成19年8月9日(2007.8.9)		スウェーデン国 2 2 3 8 0 ルンド、
(86) 国際出願番号	PCT/SE2005/000141		シェーレヴェーゲン 1 9 シー
(87) 国際公開番号	W02005/078647	(74) 代理人	100066692
(87) 国際公開日	平成17年8月25日(2005.8.25)		弁理士 浅村 皓
審査請求日	平成20年1月25日(2008.1.25)	(74) 代理人	100072040
(31) 優先権主張番号	0400308-3		弁理士 浅村 肇
(32) 優先日	平成16年2月12日(2004.2.12)	(74) 代理人	100091339
(33) 優先権主張国	スウェーデン(SE)		弁理士 清水 邦明
(31) 優先権主張番号	60/543,545	(74) 代理人	100094673
(32) 優先日	平成16年2月12日(2004.2.12)		弁理士 林 拓三
(33) 優先権主張国	米国(US)		

最終頁に続く

(54) 【発明の名称】 無線データ転送をするためのポータブルデータキャリア、外部装置、システムおよび方法

(57) 【特許請求の範囲】

【請求項 1】

バイオメトリックテンプレート(13)およびアプリケーション固有の機能(15)を含むデータを記憶するためのキャリアの記憶装置(12)と、データを無接触で送受信するためのキャリアの通信手段(11)とを備えたポータブルデータキャリア(10)において、

バイオメトリックテンプレートと外部装置(20)から受信されたバイオメトリックサンプル(23)とを比較するためのキャリアの処理手段(16)を更に備え、外部装置によりハンドシェイクプロセスを完了すると共に、アプリケーション固有の機能を実行し、バイオメトリックサンプルがバイオメトリックテンプレートと一致した場合に限り、アプリケーション固有の機能の結果を前記外部装置に送信するようになっており、バイオメトリックテンプレートとバイオメトリックサンプルとが一致していることを見なされるまで、ポータブルデータキャリア(10)からのデータのすべての送信を防止するようになってい

【請求項 2】

前記アプリケーション固有の機能(15)が、前記キャリアの記憶装置(12)内に記憶されているアプリケーション固有の情報(14)を、前記キャリアの記憶装置(12)から検出することを含み、前記機能の結果が、前記アプリケーション固有の情報を含む、請求項1記載のポータブルデータキャリア(10)。

【請求項 3】

前記アプリケーション固有の機能(15)が、前記キャリアの記憶装置(12)内に記憶されているプログラムコードを実行することを含む、請求項1~2のいずれか1つに記載のポータブルデータキャリア(10)。

【請求項4】

前記外部装置から受信した問い合わせに応答し、前記アプリケーション固有の機能(15)を実行し、この機能の前記結果を前記外部装置(20)に送信するようになっている、請求項1~3のいずれか1つに記載のポータブルデータキャリア(10)。

【請求項5】

前記バイOMETリックテンプレート(13)が、個人固有の情報を含むデジタル画像に対応する、請求項1~4のいずれか1つに記載のポータブルデータキャリア(10)。

10

【請求項6】

前記バイOMETリックテンプレート(13)が、指紋の少なくとも一部を構成する、請求項1~5のいずれか1つに記載のポータブルデータキャリア(10)。

【請求項7】

前記バイOMETリックテンプレート(13)が、特徴基準データに対応する、請求項1~6のいずれか1つに記載のポータブルデータキャリア(10)。

【請求項8】

バイOMETリックサンプル(23)とバイOMETリックテンプレート(13)が一致すると判断するために、両者が対応する程度を定めるスレッシュホールド値を前記キャリアの記憶装置(12)内に記憶するようになっている、請求項1~7のいずれか1つに記載のポータブルデータキャリア(10)。

20

【請求項9】

データキャリアが、スマートカードである、請求項1~8のいずれか1つに記載のポータブルデータキャリア(10)。

【請求項10】

データキャリアが、電子パスポートである、請求項1~8のいずれか1つに記載のポータブルデータキャリア(10)。

【請求項11】

データキャリアが、携帯電話である、請求項1~8のいずれか1つに記載のポータブルデータキャリア(10)。

30

【請求項12】

データキャリアが、PDA(パーソナルデジタルアシスタント)である、請求項1~8のいずれか1つに記載のポータブルデータキャリア(10)。

【請求項13】

前記外部装置(20)が前記バイOMETリックテンプレート(13)にアクセスすることを防止するようになっている、請求項1~12のいずれか1つに記載のポータブルデータキャリア(10)。

【請求項14】

一致が存在すると見なされた後の所定時間に限り、前記外部装置(20)と通信するようになっている、請求項1~13のいずれか1つに記載のポータブルデータキャリア(10)。

40

【請求項15】

前記外部装置(20)から受信したサーチ信号に応答し、存在信号を送信し、前記外部装置の通信レンジ内に外部装置が存在することを確認するようになっている、請求項1~14のいずれか1つに記載のポータブルデータキャリア(10)。

【請求項16】

バイOMETリックテンプレート(13)およびアプリケーション固有の機能(15)を含むデータを記憶するためのキャリアの記憶装置(12)と、データを無接触で送受信するためのキャリアの通信手段(11)とを備えたポータブルデータキャリア(10)により、データを転送する方法において、

50

外部装置(20)からバイオメトリックサンプル(23)を受信するステップ(B3)と、

前記データキャリア内のキャリアの処理手段(16)により、前記バイオメトリックサンプルと前記バイオメトリックテンプレートとを比較するステップ(B4)と、

前記外部装置によりハンドシェイクプロセスを完了するだけでなく、アプリケーション固有の機能を実行し、前記バイオメトリックサンプルが前記バイオメトリックテンプレートに一致した場合に限り、前記機能の結果を前記外部装置に送信するステップ(B10)と、バイオメトリックテンプレートとバイオメトリックサンプルとが一致していると見なされる(B5)まで、前記ポータブルデータキャリア(10)からのデータのすべての送信を防止するステップと、を特徴とする、データを転送する方法。

10

【請求項17】

前記アプリケーション固有の機能(15)を実行するステップが、前記キャリアの記憶装置(12)から、この記憶装置に記憶されているアプリケーション固有の情報(14)を検索することを含み、前記機能の結果が前記アプリケーション固有の情報を含む、請求項16記載の方法。

【請求項18】

前記アプリケーション固有の機能(15)を実行するステップが、前記キャリアの記憶装置(12)内に記憶されているプログラムコードを実行することを含む、請求項16または17記載の方法。

【請求項19】

前記外部装置から受信(B9)した問い合わせに回答し、アプリケーション固有の機能(15)を実行し、その機能の前記結果を前記外部装置(20)に送信するステップ(B10)を含む、請求項16~18のうちのいずれか1つに記載の方法。

20

【請求項20】

前記バイオメトリックテンプレート(13)が、個人固有の情報を含むデジタル画像に対応する、請求項16~19のいずれか1つに記載の方法。

【請求項21】

前記バイオメトリックテンプレート(13)が、指紋の少なくとも一部を定める、請求項16~20のいずれか1つに記載の方法。

【請求項22】

前記バイオメトリックテンプレート(13)が、特徴基準データに対応する、請求項16~21のいずれか1つに記載の方法。

30

【請求項23】

バイオメトリックサンプルとバイオメトリックテンプレートが一致すると判断する(B6)のために、両者が対応する程度を定めるスレッシュホールド値を前記キャリアの記憶装置内に記憶するようになっている、請求項16~22のいずれか1つに記載の方法。

【請求項24】

データキャリア(10)が、スマートカードである、請求項16~23のいずれか1つに記載の方法。

【請求項25】

データキャリア(10)が、電子パスポートである、請求項16~23のいずれか1つに記載の方法。

40

【請求項26】

データキャリア(10)が、携帯電話である、請求項16~23のいずれか1つに記載の方法。

【請求項27】

データキャリア(10)が、PDA(パーソナルデジタルアシスタント)である、請求項16~23のいずれか1つに記載の方法。

【請求項28】

一致が存在すると見なされた(B5)後に、所定時間が経過したときに、前記外部装置

50

(20)との通信を防止するステップを更に含む、請求項16~27のうちのいずれか1つに記載の方法。

【請求項29】

前記外部装置(20)からのサーチ信号を受信するステップと、前記サーチ信号に応答し、前記外部装置の通信範囲内にあることを確認するために存在信号を送信するステップ(B2)を更に含む、請求項16~28のうちのいずれか1つに記載の方法。

【請求項30】

プログラム実行時に請求項16~29のうちのいずれか1つに記載の方法を実行するようになっている命令を有するコンピュータプログラムを備えた記憶媒体。

【請求項31】

データを無接触で送受信するための装置の通信手段(21)と、バイオメトリックサンプル(23)を記録するためのセンサ(25)とを備えた外部装置(20)において、

前記バイオメトリックサンプルをポータブルデータキャリア(10)に送信するようになっており、前記ポータブルデータキャリアとのハンドシェイクプロセスを完了すると共に、前記バイオメトリックサンプルが前記ポータブルデータキャリアに記憶されていたバイオメトリックテンプレート(13)と一致した場合に限り、前記ポータブルデータキャリアで実行されたアプリケーション固有の機能(15)の結果を、前記ポータブルデータキャリアから受信するようになっており、バイオメトリックテンプレートとバイオメトリックサンプルとが一致していると見なされるまで、所定のスケジュールに従ってバイオメトリックサンプル(23)を送信するようになっていることを特徴とする外部装置(20)。

【請求項32】

前記データキャリア内に記憶されていたアプリケーション固有の情報(14)を、前記結果として受信するようになっており、請求項31記載の外部装置(20)。

【請求項33】

前記ポータブルデータキャリア(10)に問い合わせを送信し、前記問い合わせに回答し、前記結果を受信するようになっており、請求項31または32記載の外部装置(20)。

【請求項34】

前記バイオメトリックサンプル(23)が、個人固有の情報を含むデジタル画像に対応する、請求項31~33のうちのいずれか1つに記載の外部装置(20)。

【請求項35】

前記バイオメトリックサンプル(23)が、指紋の少なくとも一部を構成する、請求項31~34のうちのいずれか1つに記載の外部装置(20)。

【請求項36】

前記バイオメトリックサンプル(23)が、特徴データに対応する、請求項31~35のうちのいずれか1つに記載の外部装置(20)。

【請求項37】

サーチ信号を送信し、該サーチ信号に回答して前記ポータブルデータキャリア(10)から存在信号を受信し、前記外部装置の通信レンジ内にポータブルデータキャリアが存在することを検出するようになっており、請求項31~36のうちのいずれか1つに記載の外部装置(20)。

【請求項38】

データを無接触で送受信するための装置の通信手段(21)とセンサ(25)とを備えた外部装置(20)によりデータを転送し、前記センサによりバイオメトリックサンプル(23)を記録するステップ(U3)を備えた方法において、

更に前記バイオメトリックサンプルをポータブルデータキャリア(10)に送信するステップ(U4)と、

前記ポータブルデータキャリアとのハンドシェイクプロセスを完了し、前記バイオメトリックサンプルが前記ポータブルデータキャリアに記憶されているバイオメトリックテン

10

20

30

40

50

プレート(13)と一致する場合に限り、前記ポータブルデータキャリア内で実行されるアプリケーション固有の機能(15)の結果を前記ポータブルデータキャリアから受信するステップ(U10)と、バイオメトリックテンプレートとバイオメトリックサンプルとが一致していると見なされるまで、所定のスケジュールに従ってバイオメトリックサンプル(23)を送信するようになっているステップを更に備えることを特徴とする、データを転送する方法。

【請求項39】

前記データキャリア(10)内に記憶されているアプリケーション固有の情報(14)を前記結果として受信するステップを更に含む、請求項38記載の方法。

【請求項40】

前記ポータブルデータキャリア(10)に問い合わせを送信するステップ(U5)と、前記問い合わせに応答し、前記結果を受信するステップ(U10)とを更に含む、請求項38または39記載の方法。

【請求項41】

サーチ信号(U1)を送信するステップと、このサーチ信号に応答し、前記ポータブルデータキャリア(10)から存在信号を受信(U2)し、前記外部装置(20)の通信レンジ内にデータキャリアが存在することを検出するステップとを更に備えた、請求項38~40のうちのいずれか1つに記載の方法。

【請求項42】

一致が存在すると見なされるまで、所定のスケジュールに従ってバイオメトリックサンプルを送信するステップを更に備えた、請求項38~41のうちのいずれか1つに記載の方法。

【請求項43】

プログラム実行時に請求項38~42のうちのいずれか1つに記載の方法を実行するようになっている命令を備えたコンピュータプログラムを含む記憶媒体。

【請求項44】

バイオメトリックテンプレート(13)およびアプリケーション固有の機能(15)を含むデータを記憶するためのキャリアの記憶装置(12)と、データを無接触で送受信するためのキャリアの通信手段(11)とを備えたポータブルデータキャリア(10)と、

データを無接触で送受信するための装置の通信手段(21)およびバイオメトリックサンプル(23)を記録するためのセンサ(25)を含む外部装置(20)とを備えた、データを転送するためのシステムにおいて、

前記外部装置が前記バイオメトリックサンプルを前記ポータブルデータキャリア(10)で送信するようになっており、

前記ポータブルデータキャリアが更に前記バイオメトリックテンプレートと前記外部装置(20)から受信したバイオメトリックサンプル(23)とを比較するためのキャリア処理手段(16)を更に備え、

前記ポータブルデータキャリアと前記外部装置とが相互ハンドシェイクプロセスを完了するようになっており、前記ポータブルデータキャリアがアプリケーション固有の機能を実行し、この結果を前記外部装置に送信するようになっており、前記バイオメトリックサンプルが前記バイオメトリックテンプレートに一致する場合に限り、前記外部装置が前記ポータブルデータキャリアから結果を受信するようになっており、バイオメトリックテンプレートとバイオメトリックサンプルとが一致していると見なされるまで、所定のスケジュールに従ってバイオメトリックサンプル(23)を送信するようになっていることを特徴とする、データを転送するためのシステム。

【請求項45】

バイオメトリックテンプレート(13)およびアプリケーション固有の機能(15)を含むデータを記憶するためのキャリアの記憶装置(12)と、データを無接触で送受信するためのキャリアの通信手段(11)とを備えたポータブルデータキャリア(10)と、

データを無接触で送受信するための装置の通信手段(21)およびセンサ(25)を含

10

20

30

40

50

む外部装置（20）との間でデータを転送する方法であって、

前記センサによりバイオメトリックサンプル（23）を記録するステップを備えた、データを転送する方法において、

前記外部装置から前記バイオメトリックサンプルを前記ポータブルデータキャリア（10）に送信するステップ（U4）と、

前記ポータブルデータキャリアにおいて、前記外部装置（20）から前記バイオメトリックサンプル（23）を受信するステップ（B3）と、

前記データキャリア内のキャリア処理手段（16）により、前記バイオメトリックサンプルと前記バイオメトリックテンプレートとを比較するステップ（B4）と、

前記ポータブルデータキャリアと前記外部装置との間のハンドシェイクプロセスを完了し、前記ポータブルデータキャリア内で前記アプリケーション固有の機能を実行し、この結果を前記外部装置に送信（B10）するだけでなく、前記バイオメトリックサンプルが前記バイオメトリックテンプレートに一致する場合に限り、前記外部装置において前記ポータブルデータキャリアから結果を受信するステップと、バイオメトリックテンプレートとバイオメトリックサンプルとが一致していると見なされるまで、所定のスケジュールに従ってバイオメトリックサンプル（23）を送信するステップを更に備えることを特徴とする、データを転送する方法。

10

【発明の詳細な説明】

【技術分野】

【0001】

20

（発明の分野）

本発明はバイオメトリックテンプレートおよびアプリケーション固有の機能を含むデータを記憶するためのキャリア記憶装置と、データを無接触で送受信するためのキャリア通信手段とを備えたポータブルデータキャリアに関し、本発明は更に上記ポータブルデータキャリアによりデータを転送するための方法およびデータを転送するための、命令を有する記憶媒体にも関する。

【0002】

本発明は更に、データを無接触で送受信するための装置通信手段と、バイオメトリック（生体計量）サンプルを記録するためのセンサとを備えた外部装置にも関し、本発明は更に上記外部装置によりデータを転送するための方法およびデータを転送するための、命令を有する記憶媒体にも関する。

30

【0003】

本発明は更に、上記ポータブルデータキャリアおよび外部装置を備えたデータを転送するためのシステムにも関する。更に本発明は、ポータブルデータキャリアによりデータを転送するための方法および上記外部装置によりデータを転送するための方法にも関する。

【背景技術】

【0004】

（背景技術）

情報へのアクセス、多くの部屋へのアクセスは、多くのケースでは特定の個人だけに限定しなければならない。例えばインターネットで電子マネー取引を行わなければならないとき、病院内で記録にアクセスすることを制限するとき、または仕事場での特定の個人だけに所定の情報または部屋へのアクセスを許可することが、このようなケースに該当する。これらに関連し、例えばインテリジェントカードまたはスマートカードのようなポータブルデータキャリアが頻繁に使用される。スマートカードは集積プロセッサまたは信号処理手段、記憶装置および通信インターフェースを備えたクレジットカードのサイズのカードとして説明することができる。

40

【0005】

上記ケースにおいて使用されるすべてのスマートカードには、機密情報が記憶されている。かかる機密情報は少なくとも1つのいわゆるテンプレートを含み、このテンプレートはカードユーザーに関するあらかじめ記憶された基準情報として記述できる。使用が試み

50

られるごとに、カードを使用するカードユーザーの権利はこのテンプレートによって証明される。スマートカードが使用されようとしている状況に応じて、カード記憶装置には他の機密情報も記憶できる。

【 0 0 0 6 】

上記テンプレートは、例えば1つのPINコード（PIN = パーソナル識別番号）に対応できる。カード所有者がカードを使用する自分の権利を証明したい場合、カード所有者はカードを端末に挿入し、PINコードを入力する。入力されたPINコードが記憶装置に記憶されているテンプレートに対応していれば、カード所有者のカード使用権利が証明される。別の例によれば、上記テンプレートはバイオメトリックにすることができる。すなわち生体に関連する個人固有の情報、例えばユーザーの指、手のひら、虹彩またはユーザーの声のパターンに対応する。カード所有者またはカードユーザーが従来技術に従って自らをバイオメトリック情報によって識別する方法は、一般に次のように進行する。

10

【 0 0 0 7 】

ユーザーは自分のスマートカードを端末に入れ、1本の指をセンサに載せると、センサは指のデジタル画像、すなわちデジタル表示を発生する。この指のデジタル画像は外部プロセッサ、例えばパソコンまで送られ、ここで予備処理される。予備処理において、例えば二進化された画像または二進化された画像の一部が発生されるように画像内の情報量が少なくされる。対応する予備処理された画像はテンプレートとしてカードに記憶される。外部プロセッサはカードからテンプレートを検索し、このテンプレートと指の予備処理された画像とを比較する。画像がテンプレートと一致すれば、カード所有者のカード使用権利が証明される。

20

【 0 0 0 8 】

上記ポータブルデータキャリアを使用する際に、データキャリアが端末と通信できるようにするために、ユーザーはポータブルデータキャリアを端末に物理的に接触させなければならない。従って、このことは正常な状況では、かかるポータブルデータキャリアのユーザーは常に自分のデータキャリアが端末と通信していることを認識していることを意味する。しかしながら、通信のために端末とデータキャリアとを物理的に接触させることは、特に接触がゆるかったり、接触表面などが腐食している等の理由から問題が生じる原因となることがときどきある。これら問題を解決するために、ポータブルデータキャリアと端末との間で無線通信を使用することが知られている。

30

【 0 0 0 9 】

米国特許第6,111,506号は、例えばパーソナル識別文書を、カード形状としたデータキャリアが端末と無線通信するシステムを開示している。識別文書が端末から信号を受信すると、識別文書は端末がこの識別文書と通信できる権限があるかどうかをチェックする。権限がある場合、端末は識別文書からデータを読み出すことが認められる。読み出されるデータは、例えば識別文書の所有者の指紋を示すバイオメトリックデータでよい。バイオメトリック識別チェックにおいて、識別文書を示す個人に対し、バイオメトリックデータを記録するために端末に接続されたデバイスと相互対話することが求められる。端末に接続されたコンピュータで、識別文書から読み出された前記バイオメトリックデータが前記記録されたバイオメトリックデータと比較される。両者が一致していれば、識別文書を示した個人がこの文書の正当な所有者である旨が証明される。このシステムに関係するケースにおいて、こうして識別文書が起動され、端末に識別文書と通信する権限があることが証明されるとすぐに、端末によって読み出されるように識別文書が起動される。このことは、識別文書のデータが、この識別文書を示した者が正当な所有者であるか、または例えば識別文書を盗んだ者であるかどうかに関係なく、識別文書のデータがオープンにされ、読み出し可能となることを意味する。上記システムの構造は、キャリアの知識がなくてもデータキャリアとの通信が可能となるという問題を生じさせる。不正に扱われている端末が秘密状態にあり、例えばデータキャリアが入っているバッグまたはポケットの近くにあり、データキャリアに記憶されていたデータを読み取ったり、または他の方法でデータキャリアと相互対話することが有り得る。この結果、多くの状況において大きな問

40

50

題が生じ得る。1つの例として、識別文書がパスポートであり、何らかの理由からパスポートの所有者がパスポートに記憶されている自分の国籍または他の情報を明らかにしたくない場合を挙げることができる。パスポートの所有者はパスポートの所有を秘密状態に単に維持したいだけの場合もあり得る。後者の理由は、会員であることを秘密にしたいときに、別の組織に対して会員番号の形態をした識別文書に関連しても当てはまる。最後に、上記システムに対応するシステムを銀行カードの形態をしたデータキャリアに関連して使用しなければならない場合、このことはポータブル端末を有する者が銀行カードに接続した口座から直接お金を比較的簡単に盗むことができることを意味する。

【0010】

米国特許第5,484,997号は、識別カードとしてのカードの形状をしたデータキャリアが端末と無線通信するシステムを開示している。識別カード上の光電池が照明されると、識別カード内に記憶されていたデータを自動的に送信するように、識別カードが起動される。識別カードを使おうとしていないときに、識別カードが例えば財布の中に保護されていない場合、識別カードは近所にある端末へ、望まなくてもデータが送信されることがあり得る。データキャリアを使ってデータキャリアを機能させようとするときに、更に十分な照明をしなければならない。したがって、照明源に関連してデータキャリアが所定の方法に配置されていない場合、またはユーザーが誤ってでフォトセルの上に自分の指を載せている場合に、データキャリアを使用できない恐れがある。最後に、の耐久性があり、実用的に設計された上記タイプのデータキャリアを製造することは困難である。

【発明の開示】

【発明が解決しようとする課題】

【0011】

(発明の概要)

本発明の目的は、従来技術に関連した問題を完全に、または部分的に解消することにある。

【0012】

この目的はポータブルデータキャリア、ポータブルデータキャリアによりデータを転送するための方法、および命令を有する記憶媒体、外部装置、外部装置によってデータを転送するための方法および命令を有する記憶媒体、並びに独立請求項に記載のデータを転送するためのシステムおよび方法によって達成される。本発明の実施例は、従属請求項に記載されている。

【0013】

本発明の基本的な原理は、キャリアの認識および同意なく、ポータブルデータキャリア内に記憶されている機密データが読み出されるのを防止することにある。本発明の更に別の基本的原理は、権利のある所有者の認識および同意なく、ポータブルデータキャリア内に記憶された機密データが読み出されるのを防止することにある。要するに、本発明の目的は、特にポータブルデータキャリアを所持する個人が、このポータブルデータキャリアの正当な所有者であること、およびこの所有者が読み出しに同意していることをチェックすることなく、ポータブルデータキャリア内に記憶されている機密データが読み出されるのを防止することにある。

【課題を解決するための手段】

【0014】

第1の態様によれば、本発明はより詳細には、バイオメトリックテンプレートおよびアプリケーション固有の機能を含むデータを記憶するためのキャリアの記憶装置と、データを無接触で送受信するためのキャリアの通信手段とを備えたポータブルデータキャリアに関する。このポータブルデータキャリアは、バイオメトリックテンプレートと外部装置から受信されたバイオメトリックサンプルとを比較するためのキャリアの処理手段を更に備え、外部装置によりハンドシェイクプロセスを完了すると共に、アプリケーション固有の機能を実行し、バイオメトリックサンプルがバイオメトリックテンプレートと一致した場合に限り、アプリケーション固有の機能の結果を前記外部装置に送信するようになってい

10

20

30

40

50

ることを特徴とする。

【0015】

データキャリアとは、パッシブおよびアクティブの双方の多数の異なるユニット、例えばスマートカード、電子パスポート、電子ビザおよび切符、RFタグ、携帯電話、PDA（パーソナルデジタルアシスタント）などを意味する。パッシブデータキャリアなる用語は、自己の電源を有しておらず、従って作動できるようにするために外部電源に依存するデータキャリアを意味する。アクティブデータキャリアなる用語は、反対のキャリア、すなわち自己の電源を有するデータキャリアを意味する。パッシブデータキャリアを選択するか、またはアクティブデータキャリアを選択するかは、このデータキャリアを使用しようとしているアプリケーションに従って決める。バイオメトリックテンプレートおよびバイオメトリックサンプルなる用語は、個人固有のデータ、すなわち各個人にユニークなデータを意味する。かかるデータの例として、個人の指、掌、虹彩または個人の顔、声のパターンまたはDNAである。テンプレートとは、データキャリアに記憶され、通常は最初に記憶した後には変更できない参考データを意味する。サンプルとは、個人がポータブルデータキャリアの使用を望むたびに個人によって提示しなければならないデータを意味する。

10

【0016】

ポータブルデータキャリアがデータを無接触で転送するためのキャリアの通信手段を含むということは、従来技術に関連する接触上の問題が解消されること、例えば接触表面が破壊または摩耗されている場合の問題が解消される。無接触転送であることは、ポータブルデータキャリアと外部装置との間で通信を行うためにポータブルデータキャリアを直接外部装置に接続するようにしなくてもよいことを意味する。理論的には、ユーザーさえも外部装置と通信する際に、例えばポケットまたはバッグから自分のデータキャリアを取り出す必要はない。このことは、ユーザーが自分の手に他の物、例えば航空機のチケットやスーツケースを持っている場合に実用的となり得る。更にこのようなユーザーが、例えば自分のバッグ内のデータキャリアを探す必要がなくなり、更にデータキャリアを失う恐れもなくなるという見地からも実用的である。

20

【0017】

ポータブルデータキャリアがバイオメトリックテンプレートと外部装置から受信したバイオメトリックサンプルとを比較するためのキャリアの処理手段を含むということは、バイオメトリックテンプレートは、このバイオメトリックの比較の際にデータキャリアから離れなくてよく、このことは安全性の見地から好ましいことを意味する。

30

【0018】

ポータブルデータキャリアがアプリケーション固有の機能を実行し、バイオメトリックサンプルがバイオメトリックテンプレートに一致するという条件に限り、この結果を外部装置に送るようになっているという特徴は、ポータブルデータキャリアを実際に所持する個人が、このキャリアの正当な所有者であることを証明するまで、秘密情報が環境から保護されることを意味する。

【0019】

ここで、一致とは、ポータブルデータキャリアを所持する個人がデータキャリアの正当な所有者と同じであると見なすのに十分な程度にバイオメトリックサンプルがバイオメトリックテンプレートに対応していることを意味する。

40

【0020】

アプリケーション固有の機能なる用語は、一組の命令を意味し、この命令に従い、データキャリアは所定の状況で作動するようになっている。これら命令の構成は、ポータブルデータキャリアを使用するようになっている用途に応じて決まる。

【0021】

データキャリアにおけるアプリケーション固有の機能は、キャリアの記憶装置から、その内部に記憶されているアプリケーション固有の情報を検索するための命令を含むことができ、この検索結果はアプリケーション固有の情報を含む外部装置へ送信される。アプリ

50

ケーション固有の情報の構成は、ポータブルデータキャリアを使用する用途に応じて決まる。例えば実際のデータキャリアに記憶される情報はデータファイルの形態、すなわちデータキャリアを使用して、例えば部屋へのドアを開けたり、実際のデータキャリアに記憶できるものと異なるタイプの情報、または異なるタイプのいわゆるデジタル証明にユーザーがアクセスできるようにする鍵の形態とすることができる。データキャリアを例えば電子パスポートとして使用するようになっているケースでは、アプリケーション固有の情報は従来のパスポートに記載できるような情報、例えば電子パスポートの所有者を識別する情報を含むことができる。

【0022】

データキャリアにおけるアプリケーション固有の機能は、キャリアの記憶装置に記憶されるプログラムコードを実行するための命令を含むことができる。このプログラムコードの実行によってデータキャリアは異なるタイプの機能、例えば暗号化、サイン、証明、評価などを行うことが可能となる。データキャリアが銀行カードの機能を有する携帯電話であるケースでは、プログラムコードを実行する結果、マネー取引のサインを行うことができ、このサインは外部装置に送られる結果に含まれる。

10

【0023】

ポータブルデータキャリアはアプリケーション固有の機能を実行し、外部装置から受信した問い合わせに回答し、この実施の結果を外部装置に送信するようである。かかる問い合わせは、外部装置がポータブルデータキャリアに情報を送信すること、および/または所定のパラメータに基づき、前記機能を実行することを求めることを意味する。

20

【0024】

バイオメトリックテンプレートは上記のような個人固有の情報を含むデジタル画像、すなわちデジタルの形態をした記録物に対応できる。デジタル表示を使用する利点は、これらデジタル表示を迅速かつ容易に記録することができ、種々の方法で処理することが容易であることである。

【0025】

バイオメトリックテンプレートは、指紋の少なくとも一部を定めることができ、この部分は指紋内のライン間の関心のある交差点に対応する特に関心のある情報コンテンツを有することが好ましい。バイオメトリック識別のために指紋を使用する利点は、特に通常の状態では同じ一人の個人からの指紋は永久的であることである。更に指紋は従来のセンサによって記録が容易である。

30

【0026】

バイオメトリックテンプレートは、例えばポータブルデータキャリアの所有者からの指紋の最も顕著な特徴を記述する特徴参照データに対応できる。この実施例では、バイオメトリックの一致が存在するか否かを判断するために、バイオメトリックテンプレートが全体の指紋に対応しているケースよりも、より少ない情報を比較するだけでよい。

【0027】

バイオメトリックテンプレートは上記代替情報の組み合わせにも対応できる。例えば指紋の少なくとも一部の画像と、指紋の特徴参照データとの組み合わせにも対応できる。

【0028】

40

ポータブルデータキャリアは一致すると判断するためにバイオメトリックサンプルがバイオメトリックテンプレートに対応する程度を定めるスレッシュールド値をキャリアの記憶装置に記憶するようである。この場合、データキャリアはバイオメトリックサンプルとバイオメトリックテンプレートとの一致の値を前記キャリアの処理手段により判断し、この値をスレッシュールド値とを比較するようになっている。一致の値がスレッシュールド値を越えた場合、上記定義に従う一致が存在すると見なされ、この逆に、スレッシュールド値を越えない場合は一致が存在しないと判断される。スレッシュールド値はポータブルデータキャリアを使用するようになっている用途に従って選択し、このように対して調節できる。例データキャリアが例えば電子パスポートである場合、データキャリアが例えば部屋への物理的なアクセスの同意信号または拒否信号を発生するのに使用できる単なる鍵カード

50

である場合よりも高いスレッシュホールド値を選択できる。

【0029】

ポータブルデータキャリアは従来のパスポートの代わりになる電子パスポートとすることができる。一実施例では、かかる電子パスポートはデータを記憶し、転送し、処理できるコンピュータチップが設けられた通常のパスポートから構成できる。かかる実施例は、通常のパスポートを廃棄しなくてもよく、上記のようなチップを追加することにより、通常のパスポートを新しい技術に合わせることができることを意味する。当然ながら、本発明に係わる電子パスポートは特許請求の範囲に記載の発明の範囲から逸脱することなく、他の種々の方法でデザインできる。

【0030】

本発明に係わる電子パスポートによって電子パスポートの審査がより容易となるだけでなく、より安全となる。パスポートの審査官がパスポートを提示した個人とパスポートに記載されている画像によって示された個人とを比較すること（このことは困難で時間がかかり、間違いを犯しやすい作業である）によって、マニュアルでパスポートを審査する代わりに、バイOMETリックサンプルを記録するだけでよく、この記録の結果、個人がなりすましている人物であるかどうかを回答できる。

【0031】

上記のように、バイOMETリックテンプレートはバイOMETリックサンプルとの比較を行うことができるようにするために、ポータブルデータキャリアから離れる必要はない。ポータブルデータキャリアはバイOMETリックテンプレートへの外部からのアクセスを完全に防止するようにできる。

【0032】

ポータブルデータキャリアは一致していると見なされた後の所定の時間の間に限り、外部装置と通信するようにできる。所定の時間が経過した後、データキャリアは外部装置との通信を中止するようになっている。この所定の時間は、アプリケーション固有の機能の実行の結果を転送できるのに十分長くすることが好ましい。かかる外部装置とデータキャリアとの間の通信リンクの自動中止は、データキャリアからの秘密情報の不正な読み取りに対する安全性を増すものである。

【0033】

本発明に係わるポータブルデータキャリアは外部装置から受信されたサーチ信号に応答して、存在信号を送信し、データキャリアが外部装置の通信レンジ内に存在することを確認するようにできる。かかる実施例の利点について、本発明に係わる外部装置と関連し、以下説明する。

【0034】

本発明に係わるポータブルデータキャリアは、むしろ、一致と見なされるまでデータキャリアからのデータのすべての送信を防止するようにできる。かかる実施例の利点は、個人が自分の意志に反し、本発明に係わるポータブルデータキャリアの所有を明らかにしないことである。個人はバイOMETリックサンプルを提供することによりデータキャリアの自らの所有を明らかにすることの同意を積極的に与えなければならない。サンプルが提供された外部装置の通信距離内に位置する、本発明に係わるすべてのポータブルデータキャリアにバイOMETリックサンプルが送信される。一致するバイOMETリックテンプレートを含む1つのポータブルデータキャリアだけで、その存在を明らかにすることができる。

【0035】

第2の態様によれば、本発明は、バイOMETリックテンプレートおよびアプリケーション固有の機能を含むデータを記憶するためのキャリアの記憶装置と、データを無接触で送信するためのキャリアの通信手段とを備えたポータブルデータキャリアにより、データを転送する方法に関する。この方法は、外部装置からバイOMETリックサンプルを受信するステップと、前記データキャリア内のキャリアの処理手段により、前記バイOMETリックサンプルと前記バイOMETリックテンプレートとを比較するステップと、前記外部装置によりハンドシェイクプロセスを完了するだけでなく、アプリケーション固有の機能を実

10

20

30

40

50

行し、前記バイOMETリックサンプルが前記バイOMETリックテンプレートに一致した場合に限り、前記機能の結果を前記外部装置に送信するステップとを特徴とする。

【0036】

第3の態様によれば、本発明は、プログラム実行時に上記方法を実行するようになっている命令を有するコンピュータプログラムを備えた記憶媒体に関する。

【0037】

ポータブルデータキャリアに関連してこれまで説明した特徴は、当然ながら本発明の第2の態様に係わる方法および第3の態様に係わる記憶媒体にも移すことができる。更に上記特徴は、当然ながら同じ実施例で組み合わせることもできる。

【0038】

第4の態様によれば、本発明は、データを無接触で送受信するための装置の通信手段と、バイOMETリックサンプルを記録するためのセンサとを備えた外部装置に関する。この外部装置は、前記バイOMETリックサンプルをポータブルデータキャリアに送信するようになり、前記ポータブルデータキャリアとのハンドシェイクプロセスを完了すると共に、前記バイOMETリックサンプルが前記ポータブルデータキャリアに記憶されていたバイOMETリックテンプレートと一致した場合に限り、前記ポータブルデータキャリアで実行されたアプリケーション固有の機能の結果を、前記ポータブルデータキャリアから受信するようになっていることを特徴とする。

【0039】

この外部装置は、データキャリアに記憶されているアプリケーション固有の情報を前記の結果として受信するようである。

【0040】

更にこの外部装置はポータブルデータキャリアに送信された問い合わせに回答して前記結果を受信するようである。

【0041】

キャリアの記憶装置内のバイOMETリックテンプレートが個人固有の情報を含むデジタル画像に対応する場合、このデジタル画像はバイOMETリックサンプルにも当てはまるはずである。

【0042】

キャリアの記憶装置内のバイOMETリックテンプレートが指紋の少なくとも一部を定める場合、このことはバイOMETリックサンプルにも同じように適用できるはずである。

【0043】

バイOMETリックテンプレートが特徴基準データに対応する場合、バイOMETリックテンプレートは特徴データに対応するはずである。

【0044】

バイOMETリックテンプレートが組み合わせに対応する場合、バイOMETリックテンプレートは上記別の例の対応する組み合わせに対応するはずである。

【0045】

外部装置はサーチ信号を送信し、このサーチ信号に回答し、ポータブルデータキャリアからの存在信号を受信し、外部装置の通信レンジ内にデータキャリアが存在することを検出できる。かかる実施例では、外部装置は存在信号を受信することにより記録のために外部装置を起動することができ、これによって理由なく、すなわちバイOMETリックサンプルを受信できるポータブルデータキャリアが外部装置の通信レンジ内で使用できない場合に、バイOMETリックサンプルを記録も送信もできないという利点が得られ、この結果、エネルギーを節約できる。別の実施例では、外部装置は常時アクティブである。

【0046】

外部装置は一致が存在すると見なされるまで、所定のスケジュールに従い、バイOMETリックサンプルを送信するようである。かかる実施例では、バイOMETリックサンプルが記録されるとすぐに、外部装置の通信レンジ内に位置する本発明にかかわるすべてのポータブルデータキャリアにバイOMETリックサンプルを送信できる。この場合、外部装置

10

20

30

40

50

は一致するバイOMETリックテンプレートを含むポータブルデータキャリア内でバイOMETリックの比較が行われるまで、ポータブルデータキャリアが存在することを完全に認識できない。バイOMETリックサンプルのための上記送信スケジュールは状況、すなわち外部装置を使用するようになっている用途に合わせて調節できる。送信スケジュールとは、例えばバイOMETリックサンプルを所定のインターバルで送信することを意味する。

【0047】

外部装置が上記実施例に従って構成されていることは、この外部装置が上記利点を得るために本発明の第1の態様に係わるポータブルデータキャリアの異なる実施例と共に満足できるように機能できることを意味する。

【0048】

第5の態様によれば、本発明は、データを無接触で送受信するための装置の通信手段とセンサとを備えた外部装置によりデータを転送し、前記センサによりバイOMETリックサンプルを記録するステップを備えた方法に関する。この方法は、更に前記バイOMETリックサンプルをポータブルデータキャリアに送信するステップと、前記ポータブルデータキャリアとのハンドシェイクプロセスを完了し、前記バイOMETリックサンプルが前記ポータブルデータキャリアに記憶されているバイOMETリックテンプレートと一致する場合に限り、前記ポータブルデータキャリア内で実行されるアプリケーション固有の機能の結果を前記ポータブルデータキャリアから受信するステップとを更に備えることを特徴とする。

【0049】

第6の態様によれば、本発明は、プログラム実行時に上記方法を実行するようになっている命令を備えたコンピュータプログラムを含む記憶媒体に関する。

【0050】

当然ながら、外部装置に関連してこれまで説明した特徴は、本発明の第5の態様に係わる方法および第6の態様に係わる記憶媒体にも移すことができる。言うまでもなく、上記特徴は同じ実施例で組み合わせることができる。

【0051】

第7の態様によれば、本発明は、本発明の第1の態様に係わるポータブルデータキャリアと、本発明の第4の態様に係わる外部装置とを含む、データを転送するためのシステムに関する。

【0052】

第8の態様によれば、本発明は、本発明の第2の態様に係わる方法と、本発明の第5の態様に係わる方法を含む、データを転送するための方法に関する。

【0053】

上記のように、本発明に係わる方法は、記憶装置内に記憶されており、前記処理手段または外部デバイスにて実行されるコンピュータプログラムとして実現できる。これとは異なり、これら方法は一部または全体を製品固有の回路、例えばASICとして、またはデジタル回路またはアナログ回路として、もしくはそれらの適当な組み合わせで実現できる。

【0054】

ポータブルデータキャリアおよび外部装置、並びにこれらによるデータを転送するための対応する方法に関連してこれまで説明した特徴は、本発明の第7の態様に係わるシステムおよび第8の態様に係わる方法にも移すことができる。

【0055】

本発明の第1の態様から第3の態様の説明に関連して、これまで説明した用語の定義は、本発明の第4から第8の態様にも適用できる。

【0056】

以下、本発明の実施例を示す添付した略図を参照し、本発明についてより詳細に説明する。

【実施例】

10

20

30

40

50

【 0 0 5 7 】

(好ましい実施例の説明)

図 1 は、本発明に係わる電子パスポートの形態をしたポータブルデータキャリア 1 0 を略図で示す。図 2 は、本発明に係わる外部装置 2 0 を略図で示す。ポータブルデータキャリア 1 0 および外部装置 2 0 はこれらキャリアと外部装置とが R F 通信するための公知の
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995

プロトコル、例えば I S O 1 4 4 4 3 に従って無接触で互いに通信するようになっているシステム内に含まれる。この通信のために、これらキャリアおよび外部装置はそれぞれキャリアの通信手段 1 1 と装置の通信手段 2 1 を含む。

【 0 0 5 8 】

標準的スマートカード、例えば J a v a (登録商標) または M U L T O S カードの機能を部分的に思い出すような機能を有するポータブルデータキャリア 1 0 は、バイオメトリック
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995

テンプレート 1 3、アプリケーション固有の情報 1 4 およびアプリケーション固有の機能 1 5 を含むデータを記憶するためのキャリアの記憶装置 1 2 を含む。バイオメトリックテンプレート 1 3 の記録と記憶は、従来の態様、例えば本願出願人の特許公開公報、例えば W O 0 1 / 1 1 5 7 7 号、W O 0 1 / 8 4 4 9 4 号、W O 0 1 / 0 6 4 4 5 号および W O 0 3 / 0 0 3 2 8 6 号に記載されている態様のうちの 1 つで行うことができ、上記刊行物は本明細書で参考例として援用する。本実施例では、バイオメトリックテンプレート 1 3 は電子パスポートの正当な所有者からの指紋のデータに対応する。名前が示すようにアプリケーション固有の情報 1 4 の構成はポータブルデータキャリアを使用しようとしている状況に応じて決まる。ポータブルデータキャリアが電子パスポートである本実施例では、アプリケーション固有の情報はポータブルデータキャリアの所有者を記述するデータ、すなわち従来のパスポートに含まれていたデータ、例えば所有者の年齢および国籍、更にパスポートを発行した権限のある機関に関する情報も含む。アプリケーション固有の機能 1 5 は一組の命令を含み、これら命令に従ってポータブルデータキャリアは所定の状況で作動するようになっている。名前が示すように、これら命令の構成はポータブルデータキャリアを使用しようとしている状況によって決まる。この実施例では、アプリケーション固有の機能はキャリアの記憶装置からアプリケーション固有の情報 1 4 を検索し、この情報を外部装置に送信するための命令を含む。このことは、図 3 および 4 を参照し、以下詳細に説明するように、バイオメトリクスが一致することが確認され、外部装置 2 0 との
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995

ハンドシェイクが実行され、情報転送に関する問い合わせが外部装置から受信されることを条件に実行すべきである。

【 0 0 5 9 】

最後に、ポータブルデータキャリア 1 0 はソフトウェアを使用したプロセッサの形態をしたキャリアの処理手段 1 6 を含み、ソフトウェアはポータブルデータキャリア内でデータを処理するように、キャリアの記憶装置 1 2 内に記憶されている。プロセッサは、例えば上記のバイオメトリクスの比較、ハンドシェイクおよびアプリケーション固有の機能を実行する。

【 0 0 6 0 】

本実施例では電子パスポートとの通信、例えばパスポートの電子審査を行うようになっている外部装置である外部装置 2 0 は、バイオメトリックサンプル 2 3 を含みデータを記憶するための装置の記憶装置 2 2 を含む。バイオメトリックサンプルの記録および記憶は、従来技術の態様、例えば本明細書で援用する本願出願人の上記特許公開公報に記載された態様のうちの 1 つで実行できる。本実施例におけるバイオメトリックテンプレート 1 3 は、電子パスポート 1 0 の正当な所有者からの指紋のデータに対応するので、バイオメトリックサンプル 2 3 は、電子パスポートを所有する個人からの指紋のデータに対応するが、この個人は必ずしも正当な所有者でなくてもよい。

【 0 0 6 1 】

外部装置 2 0 は更にバイオメトリックサンプル 2 3 が装置の記憶装置 2 2 に記憶される前に、このサンプルを記録するようになっているセンサ 2 5 を更に含む。本実施例では、センサ 2 5 は指紋を記録する容量センサであるが、本発明に関連して他の公知のタイプの

センサ、例えば熱センサまたは光センサも使用できる。最後に、外部装置 20 はソフトウェアを使用するプロセッサの形態をした装置の処理手段 26 を備え、ソフトウェアは外部装置内のデータを処理するよう、装置の記憶装置 22 内に記憶されている。プロセッサは図 3 および 4 を参照して後により詳細に説明する、ポータブルデータキャリア 10 とのハンドシェイクを実行する。ポータブルデータキャリアおよび外部装置にそれぞれ含まれる異なるユニット間の通信は、データバス（図示せず）を介して行われる。

【0062】

図 3 および 4 は、図 1 に示されたポータブルデータキャリア 10 と、図 2 に示された外部装置 20 とから成るシステム内でデータを転送するための方法を示す。図 3 はデータ転送に際し、ポータブルデータキャリア、すなわち電子パスポート内で実行される方法（ステップ B1 ~ B10）を示すが、一方、図 4 はデータ転送時に外部装置内で実行される方法（ステップ U1 ~ U10）を示す。

【0063】

本実施例では、上記システムにおいてデータを転送するための方法は、パスポートの非接触審査を実行するのに使用される。自分の電子パスポート 10 により審査を受ける個人は、外部装置 20 が設置されたパスポート制御装置に接近する。この方法の初期において、外部装置 20 は前記装置の通信手段 21 により、外部装置の通信レンジを定める距離内にポータブルデータキャリアが存在することを検出するためのサーチ信号を無線送信する（U1）。上記個人および、従ってその個人の電子パスポート 10 が外部装置の通信レンジ内に入ると、この外部装置は電子パスポート内に配置されたアンテナ（図示せず）により、従来の方法に従って電子パスポートを作動させ、よって外部装置が送信したサーチ信号を受信するようにパスポートを起動する。電子パスポートの起動後、電子パスポートはサーチ信号が受信されたかどうかをチェックする（B1）。外部装置からサーチ信号が受信されている場合、電子パスポート 10 は前記キャリア通信手段 11 により外部装置の通信レンジ内にパスポートが存在することを確認するための存在信号を送信する（B2）。サーチ信号が受信されなければ、このチェックを繰り返す（B1）。このチェックは電子パスポートが外部装置の通信レンジ内にある限り繰り返される。電子パスポートが通信レンジから離脱するとすぐに、電子パスポートの作動が終了し、電子パスポートは非作動状態となる。外部装置がサーチ信号を送信した（U1）後に、外部装置はサーチ信号の送信後の所定サーチ時間中に存在信号が受信されたかどうかをチェックする（U2）。存在信号が所定のサーチ時間中に受信されなかった場合、外部装置は新しいサーチ信号を送信する。しかしながら、所定のサーチ時間中に存在信号が受信された場合、このことは、可能な場合、電子パスポートであり得る少なくとも 1 つのポータブルデータキャリアが近くに存在することを意味する。

【0064】

次のステップは、ポータブルデータキャリアが存在することが確認されることを条件に、記録のために外部装置 20 が起動され、上記個人は上記従来技術の方法のうちの 1 つでバイオメトリックサンプルを記録するためにセンサ 25 の上に自分の指を載せることができる（U3）。外部装置がバイオメトリックサンプルを記録した後に、このサンプルは無線によって前記装置の通信手段 21 により電子パスポートへ送信される（U4）。これと同時に、電子パスポートは存在信号が送信された後に所定の受信時間中にバイオメトリックサンプルが受信されたかどうかをチェックする。当然ながら、このことは外部装置の通信レンジ内にまだ電子パスポートがあることを条件に行われる。所定の受信時間中にバイオメトリックサンプルが受信されなかった場合、外部装置との通信が中止される（B7）。そうでない場合、電子パスポート 10 は前記キャリア処理手段 16 により、受信されたバイオメトリックサンプルと記憶されたバイオメトリックテンプレートとを比較し（B4）、これらが一致しているかどうかを確認する。すなわちバイオメトリックサンプルとバイオメトリックテンプレートが同じ個人から得られたものであるかどうかをチェックする。比較の際に、バイオメトリックサンプルとバイオメトリックテンプレートとの間の相関値が計算され、この相関値がキャリアの記憶装置 12 に記憶されている所定のスレッシュヨ

10

20

30

40

50

ド値に対して重み付けされる。相関値がスレッシュホールドを越えた場合、一致していると見なされる。そうでない場合、一致していないと見なされる。

【 0 0 6 5 】

一致チェック (B 5) が肯定的な応答を示した場合、一致に関するメッセージが電子パスポートから外部装置へ送信される。そうでなく、一致チェックが否定的な応答を示した場合、外部装置との通信が中止される (B 7)。バイオメトリックサンプルを送信してから、所定の比較時間中に、外部装置は一致に関するメッセージが受信されたかどうかをチェックする (U 5)。かかる一致に関するメッセージが受信されると、電子パスポート 1 0 と外部装置 2 0 との間で従来のハンドシェイクプロセスが実施される (B 6、U 6)。しかしながら、所定の比較時間中に一致に関するメッセージが受信されなかった場合、電子パスポートと外部装置との間の通信は中止される (U 7)。

10

【 0 0 6 6 】

本実施例では、従来の方法、例えば「フィリップス・マイフェア (P h i l l i p s M i f a r e) 」レファレンス I S O / I E C 9 7 9 8 - 2 に記載されている「スリーパス相互認証」に従ってスリーウェイハンドシェイクが実行される。本実施例において、一致に関するメッセージの受信、すなわち装置側でチェック (U 5) にて肯定的な応答があったことは、バイオメトリックサンプルの送信後の所定の比較時間内に電子パスポートが上記ハンドシェイクプロセスを開始したことを意味する。電子パスポートがハンドシェイクを開始することにより外部装置には一致したことが通知される。別の実施例では、その代わりに外部装置がハンドシェイクプロセスを開始できるようにできる。この場合、一致に関するメッセージはハンドシェイクを開始させるだけでなく、一致したことを示す信号も送信する。

20

【 0 0 6 7 】

ハンドシェイクプロセスを実行すること (B 6) は、外部装置が正当なタイプのものであるかどうか、すなわち電子パスポートとフルに通信するようになっているタイプのものであるかどうかを電子パスポートがチェックすることを意味する。同じように、ハンドシェイクプロセスを実行すること (U 6) は、ポータブルデータキャリアが正当なタイプのものであるか、すなわち外部装置がフルに通信するようになっているタイプのものであるかどうかを外部装置がチェックすることを意味する。電子パスポートに対し、正当なタイプの外部装置はパスポートを審査するようになっている外部装置であり、またこの逆に正当なタイプの外部装置はパスポートを審査するようになっている外部装置である。

30

【 0 0 6 8 】

上記ハンドシェイクプロセス (B 6、U 6) の結果が成功することは、ハンドシェイクが OK であるかどうかをチェックする 2 つのチェック (B 8、U 8) によって肯定的な応答が得られることを意味する。上記ハンドシェイクプロセス (B 6、U 6) の結果に失敗することは、ハンドシェイクが OK であるかどうかの 2 つのチェック (B 8、U 8) のうちの少なくとも一方によって否定的な応答が得られることを意味する。電子パスポートはスリーウェイハンドシェイクを開始する本実施例では、電子パスポートにおけるハンドシェイクチェックからの応答 (B 8) は、外部装置におけるハンドシェイクチェック (U 8) が肯定的な応答を与えるには肯定的でなければならない。かかる肯定的な応答であることは、電子パスポートと外部装置とが互いにフルに通信することが許可されることを意味する。次に外部装置は、アプリケーション固有の情報の送信に関する問い合わせを電子パスポートに送信する (U 5)。同時に、電子パスポートはハンドシェイクプロセスを実行した後の所定の問い合わせ時間内に外部装置からかかる問い合わせが受信されたかどうかを電子パスポートがチェックする (B 5)。このような問い合わせがなかった場合、外部装置との通信が中止される (B 7)。しかしながら、所定の問い合わせ時間内に問い合わせが受信された場合、通信が中止される (B 7、U 7) 前に、電子パスポートから外部装置へ必要とされるアプリケーション固有の情報が転送される (B 1 0、U 1 0)。本実施例では、外部装置におけるハンドシェイクのチェック (U 8) からの否定的な応答が出されることは、電子パスポートにおいてハンドシェイクチェックから肯定的または否定的な

40

50

応答が出されること（B8）を意味し得る。いずれのケースにおいても、このことは電子パスポートと外部装置とが互いにフルに通信することが認められず、両者の間の通信が中止されることを意味する。

【0069】

電子パスポートから外部装置へのアプリケーション固有の情報の転送が完了すると、パスポートの審査官はディスプレイユニット、例えばコンピュータモニタ（図示せず）によりアプリケーション固有の情報を見ることを認められる。これに関連し、パスポートの審査官が入力手段（図示せず）により電子パスポートの記憶装置内に新しいデータ、例えばパスポートの所有者の訪問した国、所有者の到着日、および所有者の出国日を示すデータ、すなわち現在のパスポートにパスポート内のスタンプによって記録されているデータを記録することも可能である。

10

【0070】

上記実施例の説明を簡潔にするために、外部装置に関連し、1つのポータブルデータデバイスしか説明しなかった。しかしながら、この簡略にした実施例は、恐らくは本発明の実現例を示す。その理由は、現在、パスポートの電子審査用になっている外部装置の通信レンジは限られており、10～15cmとなっているからである。このように、レンジが比較的短距離であることに起因し、外部装置と複数のポータブルデータキャリアとが同時に通信することは全くあり得ない。このようなことは、複数のポータブルデータキャリアの所有者が外部装置の前で互いに押し合うことを意味するからである。上記のように、外部装置の通信レンジは通信手段の送信パワーを増すことによって拡張できる。しかしながら、このことは外部装置からの放射レベルが制限値よりも高い値に増加することを意味する。いずれのケースにおいても、複数のポータブルデータキャリアが外部装置の通信レンジ内に存在する場合において、外部装置が通信するポータブルデータキャリアに関して外部装置がチェックし続けることができるように、上記実施例では衝突防止のための機能が実施される。更に、上記実施例で転送される信号および情報は暗号化される。当然ながら、暗号化を用いない別の実施例を考え付くことも可能である。

20

【0071】

明瞭にするために、外部装置とポータブルデータキャリアとの間でデータを転送するためのシステム方法のステップは、ポータブルデータキャリアが外部装置の通信レンジ内にあるときにしか実行できないことを指摘しなければならない。上記実施例では、電子パスポートが外部装置の通信レンジから離脱した場合、電子パスポートが再び通信レンジ内に入ったときに、最初からもう1回システムの方法を実行しなければならない。従って、システムの方法のすべてのステップを実行するのに十分長い連続した時間の間、電子パスポートが通信レンジ内にある場合にしかシステムの方法のすべてのステップを実行できない。上記方法およびポータブルデータキャリア並びに外部装置の構造は、外部装置がデータキャリアのタイプさえも知ることができるようになる前に、ポータブルデータキャリアを実際に使用する個人がデータキャリアの正当な所有者であることを示すチェックを行わなければならないことを意味する。かかる所有者のチェックをするには、上記のようにユーザーの同意および相互対話を必要とするので、ポータブルデータキャリアからデータが不正に読み出されるのを防止できる。更に、個人および可能な場合にはデリケートな情報の読み出しは、所有者のチェックが肯定的であった場合でも条件付けなしでは許可されない。外部装置がポータブルデータキャリア内の情報にアクセスできるようになる前に、外部装置とポータブルデータキャリアとが互いにフルに通信するようになっていることを証明するのに、ハンドシェイクチェックも必要である。最後に、上記のことは、ポータブルデータキャリア内に記憶されているバイOMETリックテンプレートをキャリア記憶装置を残す必要がないことを意味する。その理由は、バイOMETリックサンプルとの比較はポータブルデータキャリア内で行われるからである。より詳細に説明すれば、本実施例におけるポータブルデータキャリアはバイOMETリックテンプレートへのアクセスを防止し、よってバイOMETリックテンプレートが外部装置によって読み出されることを防止するようになっているからである。

30

40

50

【 0 0 7 2 】

上記実施例におけるポータブルデータキャリアは電子パスポート状をしたパッシブなデータキャリアである。別の実施例では、その代わりにポータブルデータキャリアを携帯電話の形または銀行カード機能を備えた P D A の形をしたアクティブなデータキャリアである。このアクティブなデータキャリアの構造は図 1 のパッシブなデータキャリアの構造に対応するが、アクティブなデータキャリアは含まれる部品を作動させるためのエネルギー源も含む点が異なっている。アクティブなデータキャリアおよび図 2 に示された上記外部装置に類似する外部装置は、これらが従来の一部の通信技術、例えばBluetooth 技術に従って無接触で互いに通信するようになっているシステム内に含まれる。上記実施例と同じように、アクティブなデータキャリア内に記憶されたバイOMETリックテンプレートはアクティブなデータキャリアの正当な所有者からの指紋のデータに対応し、アクティブなデータキャリア内に記憶されたアプリケーション固有の機能は一組の命令を含み、これら命令に従ってアクティブなデータキャリアは外部装置から受信された問い合わせに応答して作動するようになっている。この実施例では、アプリケーション固有の機能は銀行カードアプリケーション、例えば外部装置から受信したデータを証明すること、およびマネー取引のサインに適した命令を含む。このような機能はバイOMETリックが一致することが証明され、外部装置とのハンドシェイクチェックが実行され、外部装置から問い合わせが受信されることを条件に実行すべきである。上記実施例と同じように、外部装置はセンサによりアクティブデータキャリアを所持する個人からの指紋のデータに対応するバイOMETリックサンプルを記録するようになっている。

10

20

【 0 0 7 3 】

ユーザーが自分のアクティブデータキャリアにより銀行ビジネスを行おうとしているとき、図 3 および 4 を参照してこれまで説明した方法に類似する方法が実行される。ユーザーが銀行ビジネスを実行すべき外部装置にアプローチすると、アクティブデータキャリアと外部装置との間でサーチ信号および存在信号が転送される。ユーザーが自分の指をセンサの上に置き、バイOMETリックサンプルを記録すると、このバイOMETリックサンプルはアクティブデータキャリアに無線で送信される。アクティブデータキャリアは受信されたバイOMETリックサンプルとバイOMETリックテンプレートとを比較し、両者の間が一致していることを確認する。アクティブデータキャリアと外部装置とが互いにフルに通信するようになっていることを証明するようにハンドシェイクが実行される。次に外部装置は、アクティブデータキャリアに問い合わせ信号を送信し、所定のデータを証明し、次に銀行ビジネスが関連するアプリケーションにサインする。このサインはアクティブデータキャリアと外部装置との間の通信を中止する前にデータキャリアから外部装置に転送される結果となる。こうして、銀行ビジネスが完了する。

30

【 0 0 7 4 】

パッシブデータキャリアを用いる実施例だけでなく、アクティブデータキャリアを用いる実施例に関連し、アプリケーション固有の機能の結果がデータキャリアから転送された後に、外部装置への通信リンクが自動的にどのように中止されるかについて説明した。パッシブデータキャリアおよびかかる自動中止をしない実施例に関連するケースでは、パッシブデータキャリアが外部装置の作動レンジから離脱すると、パッシブデータキャリアの作動は終了するので、いずれのケースにおいても通信リンクは中止される。しかしながら、このことはアクティブデータキャリアを用いる同様な実施例では生じない。その理由は、アクティブデータキャリアは自己の電源を有しているからである。不正な読み取りを防止する安全性を増すために、アクティブデータキャリアは結果の転送を開始した後に所定の転送時間が経過したかどうかをチェックするようにできる。このチェックが所定の転送時間が経過したことを表示すると、アクティブデータキャリアが外部装置との通信を中止するようになっている。

40

【 0 0 7 5 】

これまで本発明の特定の実施例について説明したが、当業者には上記説明を検討すれば、多くの代替例、変更例および変形例を想到できることは明らかであろう。以下、かかる

50

代替例について説明する。

【0076】

パッシブデータキャリアを用いる上記実施例では、外部装置の通信レンジはパッシブデータキャリアを作動させるためのレンジと同じであると仮定した。本発明の別の実施例では、パッシブデータキャリアを作動させるためのレンジは通信レンジと同じではない。更に別の実施例では、パッシブデータキャリアは外部装置によって作動されない。その代わりに外部装置の周辺にある別個のユニットによって作動される。かかる別個の作動ユニットは外部装置も位置する空間内の種々の戦略的位置に配置できる。かかる実施例ではキャリアがその空間内に入るとすぐに、パッシブデータキャリアが作動される。

【0077】

上記実施例と別の実施例によれば、サーチ信号を送信するステップ、サーチ信号の受信をチェックするステップ、存在信号を送信するステップ、および存在信号の受信をチェックするステップ（図3および4におけるシステム方法におけるU1、B1、B2、U2）が省略される。この実施例は、外部装置はバイオメトリックサンプルを記録し、ポータブルデータキャリアと一致していると見なされるまで、所定のスケジュール、例えば所定のインターバルに従ってこのサンプルを送信するようになっていることを意味する。更にこの実施例は、ポータブルデータキャリアは外部装置の通信レンジ内にデータキャリアが存在することを証明しなくても、バイオメトリックサンプルを受信し、キャリアの記憶装置内に記憶されているバイオメトリックテンプレートとの比較を行うようになっていることを意味する。従って、この場合、ポータブルデータキャリアはバイオメトリックサンプルと一致していると見なされるまで、ポータブルデータキャリアからのすべてのデータの送信を防止するようになっている。この実施例は、外部装置によって記録されたバイオメトリックサンプルが、外部装置の通信レンジ内にあるすべてのポータブルデータキャリアに送信されるが、バイオメトリックサンプルに一致するバイオメトリックテンプレートを記憶しているポータブルデータキャリアしか、そのサンプルが存在することを外部装置に明らかにしないことを意味する。従って、この実施例は所有者が望めば、本発明に従ってポータブルデータキャリアの単なる所有を秘密に維持することを可能にできる。

【0078】

上記実施例では、何らかの理由からデータキャリアがわずかの間、通信レンジから逸脱した場合に、ポータブルデータキャリアと外部装置との間の通信を中止し、通信を再スタートしなければならないような構造となっている。別の実施例によれば、通信を再開できる可能性が提供されており、このことは、データキャリアが所定の最大時間を越える時間の間、通信レンジを離脱しなければ、通信を中止した場所から通信を再開できることを意味する。

【0079】

上記実施例では、バイオメトリックの一致が確認された後にポータブルデータキャリアと外部装置の間のハンドシェイクプロセスを実行する。別の実施例によれば、この代わりにバイオメトリックが一致する前に、このハンドシェイクプロセスを実行できる。

【0080】

上記実施例では、ポータブルデータキャリアはバイオメトリックの一致が確認され、ハンドシェイクが実行され、問い合わせ信号が受信されたことを条件に、アプリケーション固有の機能を実行し、この機能の結果を外部装置に送信するようになっている。アプリケーション固有の機能を実行し、結果を転送するための別の条件を満たすような別の実施例を想到することもできる。一実施例では、例えばポータブルデータキャリア内の比較によりバイオメトリックの一致が確認された後に、補足的アイデンティティチェックを実行する。この補足的チェックはポータブルデータキャリア内でも、または外部装置でも行うことができ、例えば秘密コードの証明または別のバイオメトリックの一致を実行することができる。

【0081】

本発明は、添付した特許請求の範囲内にある上記実施例のすべての可能な代替例、変形

10

20

30

40

50

例および変更例を含むようになっていいる。

【図面の簡単な説明】

【0082】

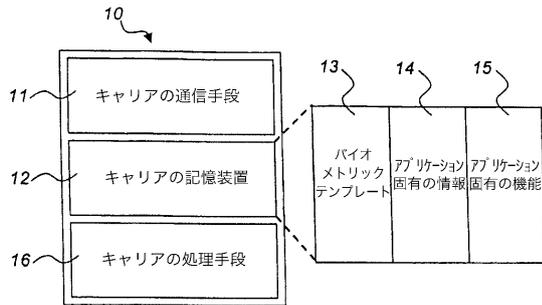
【図1】本発明の一実施例に係わるポータブルデータキャリアを示す図である。

【図2】本発明の一実施例に係わる外部装置を示す図である。

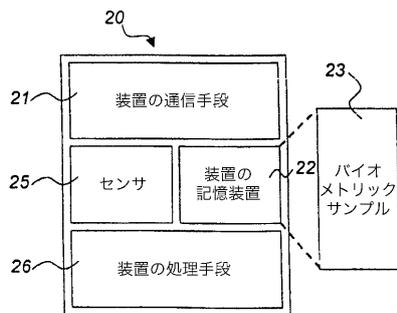
【図3】本発明の一実施例に係わるポータブルデータキャリアによるデータを転送するための方法を示すフローチャートである。

【図4】本発明の一実施例に係わる外部装置によりデータを転送するための方法を示すフローチャートである。

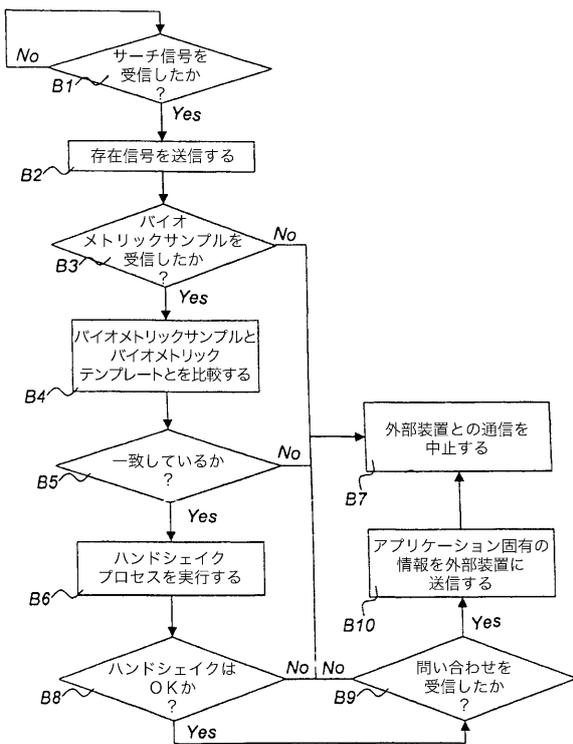
【図1】



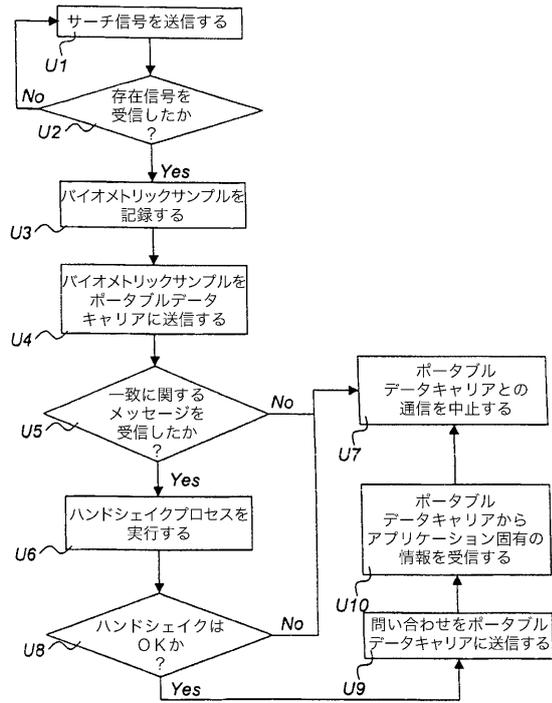
【図2】



【図3】



【図4】



フロントページの続き

(72)発明者 アンダーソン、ヨナス
スウェーデン国、ヘルヴィケン、 ヴェー：アー ファサンヴェーゲン 15

審査官 梅沢 俊

(56)参考文献 特開2000-132658(JP,A)
国際公開第01/084494(WO,A1)
特開2002-304448(JP,A)
国際公開第02/086808(WO,A1)
特開平08-221570(JP,A)
特開2003-296668(JP,A)
特開2001-283162(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06K 19/10

G06K 17/00