(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2004-506258
(P2004-506258A)
(43)公表日　平成16年2月26日(2004.2.26)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 12/14	G06F	12/14	320D	5B017
	G06F	12/14	320A	

審査請求 未請求　予備審査請求 有　（全 66 頁）

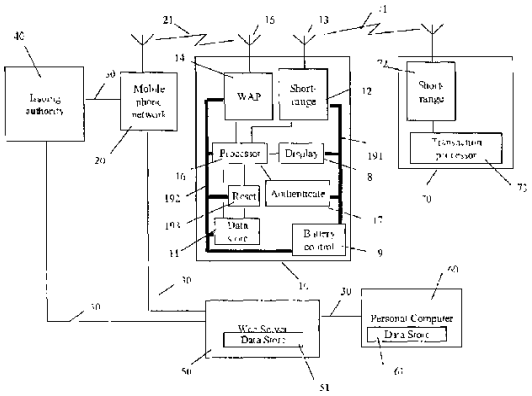
(21)出願番号	特願2002-517605(P2002-517605)
(86)(22)出願日	平成13年7月25日(2001.7.25)
(85)翻訳文提出日	平成15年2月7日(2003.2.7)
(86)国際出願番号	PCT/GB2001/003342
(87)国際公開番号	WO2002/012985
(87)国際公開日	平成14年2月14日(2002.2.14)
(31)優先権主張番号	0019628.7
(32)優先日	平成12年8月9日(2000.8.9)
(33)優先権主張国	イギリス(GB)
(31)優先権主張番号	0022848.6
(32)優先日	平成12年9月18日(2000.9.18)
(33)優先権主張国	イギリス(GB)

(71)出願人　503052944
データワイプ　マネッジメント　サーヴィスィズ　リミテッド
イギリス国，バークシャー　エスエル４　３ビービー，ウィンザー，セント・レナーズ・ロード　２４－２８，ディーダブリュジー　５６７
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100120307
弁理士　中村　雅文

最終頁に続く

(54)【発明の名称】個人データを格納し且つ保護する個人データ装置及び保護システム及び方法

(57)【要約】
個人データを格納する、個人データ装置、システム及び方法は、格納された個人データへのアクセスを、許可されたユーザへ制限する認証手段と、個人データ装置とサーバの間で、少なくとも幾つかの個人データを転送する通信手段を有する。データベースサーバ上に、個人データのコピーが格納されそして、個人データ装置のデータとデータベースサーバのデータは、通信ネットワーク上の通信により、相互に更新され且つ同期される。許可されていないユーザにより個人データ装置を使用する試みがなされるときに、個人データ装置上に格納された個人データを消去する設備が供給される。個人データは、続いて、データベースサーバから、個人データ装置又は置換個人データ装置に再ロードされる。



【特許請求の範囲】
【請求項１】
個人データ及び／又はソフトウェアを格納するストレージ手段と、格納された個人データ及び／又はソフトウェアへのアクセスを、許可されたユーザへ制限する認証手段と、サーバ上に、少なくとも幾つかの格納された個人データ及び／又はソフトウェアの複製コピーを維持するために、サーバへ、少なくとも幾つかの格納された個人データ及び／又はソフトウェアをアップロードするために、個人データ装置とサーバの間で、少なくとも幾つかの個人データ及び／又はソフトウェアを転送する通信手段と、許可されていない使用から個人データ及び／又はソフトウェアを保護するために、ストレージ手段内に格納された少なくとも幾つかのデータ及び／又はソフトウェアを消去する消去手段とを有する、個人データ装置。
【請求項２】
消去手段は、個人データ装置を使用するために、許可されていないユーザにより試みがなされたときに、少なくとも幾つかのデータ及び／又はソフトウェアを消去するように適合される、請求項１に記載の個人データ装置。
【請求項３】
消去手段は、予め定められた複数の試みの後に、認証手段の認証基準が満たされないときに、少なくとも幾つかのデータ及び／又はソフトウェアを消去するように適合される、請求項２に記載の個人データ装置。
【請求項４】
消去手段は、サーバから信号を受信したときに、少なくとも幾つかの個人データ及び／又はソフトウェアを消去するように適合される、請求項１乃至３のうちいずれか一項に記載の個人データ装置。
【請求項５】
個人データ装置には、サーバからの信号の受信のために受信手段に電力を供給するのに十分であり且つ個人データ及び／又はソフトウェアを消去する消去手段に電力を供給するのに十分である不断のスタンバイ電力供給手段が設けられている、請求項４に記載の個人データ装置。
【請求項６】
消去手段は、個人データ装置の未使用の第１の所定の時間の期間の後に及び／又は、個人データ装置とサーバが同期してから第２の所定の時間の期間の後に、少なくとも幾つかの個人データ及び／又はソフトウェアを消去するように適合される、請求項１乃至４のうちいずれか一項に記載の個人データ装置。
【請求項７】
消去手段は、許可されていないユーザが消去が発生したことを知らされずに、少なくとも幾つかの個人データ及び／又はソフトウェアを消去するように適合される、請求項１乃至６のうちいずれか一項に記載の個人データ装置。
【請求項８】
消去手段は、個人データ装置に格納された変数をデフォルト値にリセットするように適合される、請求項１乃至７のうちいずれか一項に記載の個人データ装置。
【請求項９】
個人データ装置は、個人データ及び／又はソフトウェアをサーバからダウンロードする手段を含む、請求項１乃至８のうちいずれか一項に記載の個人データ装置。
【請求項１０】
暗号化されたフォーマットで、個人データ装置上に、個人データ及び／又はソフトウェアを格納するために、暗号化手段及び復号手段が、設けられる、請求項１乃至９のうちいずれか一項に記載の個人データ装置。
【請求項１１】
格納されたデータ及び／又はソフトウェアへの予め定められた数の追加又は修正がなされた後に、サーバへ、新たな又は修正された格納された個人データ及び／又はソフトウェア

をアップロードするために、サーバと通信を確立する手段を有する、請求項１乃至１０のうちいずれか一項に記載の個人データ装置。
【請求項１２】
通信手段は、個人データ装置と、取引端末で取引を実行するための取引端末の間で、少なくとも幾つかの格納された個人データを転送する手段を有する、請求項１乃至１１のうちいずれか一項に記載の個人データ装置。
【請求項１３】
通信手段は、取引端末と通信する短距離無線第１通信手段と、サーバと通信するネットワークへの接続のための第２の通信手段とを有する、請求項１０に記載の個人データ装置。
【請求項１４】
短距離無線通信手段は、１００メートルまでの範囲をわたって動作するように適合される、請求項１１に記載の個人データ装置。
【請求項１５】
認証手段は、パターン認識手段を有する、請求項１乃至１４のうちいずれか一項に記載の個人データ装置。
【請求項１６】
パターン認識手段は、認可されたユーザの指紋パターン、虹彩パターン及び音声パターンのうちの少なくとも１つを認識するように適合される、請求項１４に記載の個人データ装置。
【請求項１７】
ストレージ手段は、対応する発行する権威者によってのみ更新可能なデータを格納し且つ、認可されたユーザにより更新可能なユーザデータを格納するように適合される、請求項１乃至１６のうちいずれか一項に記載の個人データ装置。
【請求項１８】
ストレージ手段は、クレジットカード、デビットカード、パスポート、社会保障データ、運転免許証及びメンバーシップパスのうちの１つ又はそれ以上に対応するデータを含むデータを格納するように適合される、請求項１乃至１７のうちいずれか一項に記載の個人データ装置。
【請求項１９】
ストレージ手段は、電子キャッシュ及び／又はトラベラーズチェックを格納するように適合される、請求項１乃至１８のうちいずれか一項に記載の個人データ装置。
【請求項２０】
ストレージ手段は、チケット、ボーディングパス、処方箋、及びホテルの部屋のアクセスキーのうちの１つ又はそれ以上を含む、発行する権威者により更新可能なデータを格納するように適合される、請求項１乃至１９のうちいずれか一項に記載の個人データ装置。
【請求項２１】
ストレージ手段は、アクセスキー、アラーム制御、自動ドア及び門制御の内の１つ又はそれ以上を含む、ユーザの自宅及び／又は自動車に関連するデータを格納するように適合される、請求項１乃至２０のうちいずれか一項に記載の個人データ装置。
【請求項２２】
ストレージ手段は、マルチメディアファイル、アドレス帳エントリー、名刺、予約日誌、銀行の細目、保険の細目、ドナーカード及び医療履歴の内の１つ又はそれ以上を含むユーザの更新可能なデータを格納するように適合される、請求項１乃至２１のうちいずれか一項に記載の個人データ装置。
【請求項２３】
個人データ及び／又はソフトウェアを格納するストレージ手段と、許可されていないアクセスから、少なくとも幾つかの個人データ及び／又はソフトウェアを保護するために、少なくとも幾つかの個人データ及び／又はソフトウェアを消去する消去手段とを有する個人データ装置を有し、且つ
少なくとも幾つかの個人データ及び／又はソフトウェアのコピーを格納する個人データ装

置に接続出来るデータベースサーバを有し、個人データ装置内のデータとデータベースサーバ内のデータが、相互に更新され且つ同期されうる、個人データ保護システム。

【請求項２４】

データベースサーバは、少なくとも幾つかの個人データ及び／又はソフトウェアを消去するように消去手段に信号を送るために、個人データ装置と通信する信号送信手段が設けられる、請求項２３に記載の個人データ保護システム。

【請求項２５】

データベースサーバは、個人データ装置状態記録手段を有し、その個人データ装置が紛失した又は盗難された報告されたと状態記録手段が更新されたときに、信号送信手段がその個人データ装置に、その個人データ装置内に格納された少なくとも幾つかの個人データ及び／又はソフトウェアを消去するように信号を送る、請求項２４に記載の個人データ保護システム。

【請求項２６】

通信ネットワークを介して、データベースサーバを個人データ装置に接続する通信手段を有する、請求項２３乃至２５のうちいずれか一項に記載の個人データ保護システム。

【請求項２７】

個人データ装置とデータベースサーバの少なくとも１つは、暗号化されたフォーマットで、個人データ及び／又はソフトウェアが格納されるように、暗号化手段及び復号手段を有する、請求項２３乃至２６のうちいずれか一項に記載の個人データ保護システム。

【請求項２８】

更に、個人データ装置内に格納された個人データを更新するための、発行する権威者通信手段を有する、発行する権威者サーバを有する、請求項２３乃至２７のうちいずれか一項に記載の個人データ保護システム。

【請求項２９】

発行する権威者サーバは、サーバ内に格納された個人データを更新するためにサーバに接続可能である、請求項２５に記載の個人データ保護システム。

【請求項３０】

データベースサーバは、個人データ装置からアップロードされた第１バージョンの個人データと、データベースサーバ内に蓄積された第２バージョンの個人データとを比較するデータ比較手段と、個人データ装置とデータベースサーバの両方に格納されているデータを置換するために同期されたバージョンをそれから構成する、第１と第２のバージョンから現在のバージョンのデータを抽出する手段とを有する、請求項２２乃至２８のうちいずれか一項に記載の個人データ保護システム。

【請求項３１】

紛失した又は盗難されたと報告された個人データ装置を、データベースサーバ内に格納されている個人データ及び／又はソフトウェアが再ロードされる、置換個人データ装置と置きかえるために、置換手段が設けられる、請求項２２乃至２９のうちいずれか一項に記載の個人データ保護システム。

【請求項３２】

データベースサーバは、ユーザの個人データをパーソナルコンピュータへダウンロードする手段が設けられる、請求項２２乃至３０のうちいずれか一項に記載の個人データ保護システム。

【請求項３３】

ユーザの個人データをパーソナルコンピュータへダウンロードする手段は、パーソナルコンピュータに、暗号化されたフォーマットで格納するために、個人データをダウンロードする手段を有する、請求項３１に記載の個人データ保護システム。

【請求項３４】

個人データを格納し且つ保護する方法であって、

ａ）個人データ及び／又はソフトウェアを格納するストレージ手段と、個人データ及び／又はソフトウェアへのアクセスを制限する認証手段と、それへの許可されていないアクセ

スを防ぐために、少なくとも幾つかの格納されたデータ及び／又はソフトウェアを消去する消去手段とを有する、個人データ装置を設けるステップと；
ｂ）そのストレージ手段に個人データ及び／又はソフトウェアを格納するステップと；
ｃ）その個人データ装置に格納された少なくとも幾つかの個人データのコピーを格納するためのその個人データ装置に接続可能なデータベースサーバを設けるステップと；
ｄ）その個人データ装置に格納された少なくとも幾つかのデータ及び／又はソフトウェアとそのデータベースサーバに格納された少なくとも幾つかのデータのコピーを、相互に更新し且つ同期させるステップと；
ｅ）その個人データ装置に格納されたデータへの認可されていないアクセスを得る試みがなされたときに、その個人データ装置に格納された少なくとも幾つかのデータを消去するステップとを有する方法。
【請求項３５】
ステップｅ）は、認証手段が、少なくとも幾つかの格納された個人データ及び／又はソフトウェアへアクセスする認可されていない試みを検出したときに、実行される、請求項３３に記載の方法。
【請求項３６】
ステップｅ）は、認証手段が、その認証手段の認証要求を満たすための、予め定められた数より多い不成功の試みを検出したときに、実行される、請求項３４に記載の方法。
【請求項３７】
その個人データ装置は、第１の短距離無線通信手段と、通信ネットワークを介して通信する第２の通信手段が設けられる、請求項３３乃至３５のうちいずれか一項に記載の方法。
【請求項３８】
そのストレージ手段に個人データ及び／又はソフトウェアを格納するステップｂ）は、通信ネットワークに接続された発行する権威者サーバと通信ネットワークを介して通信する第２の通信手段を使用すること及び／又は、短距離通信手段を有する発行する権威者端末と通信する第１の通信手段を使用することを含む、請求項３６に記載の方法。
【請求項３９】
短距離無線通信手段を有し且つ、その取引端末で取引を開始するために、その個人データ装置とその取引端末の間で、格納された個人データを通信するために、その個人データ装置第１通信手段を使用する、サービス提供者取引端末を設けるステップを有する、請求項３６或は３７に記載の方法。
【請求項４０】
そのプログラムが１つ又はそれ以上のコンピュータで実行されたときに、請求項３３乃至３８のうちいずれか一項に記載の方法のステップを実行するコード手段を有するコンピュータプログラム。
【請求項４１】
コンピュータ読み出し可能な媒体上で具体化された、請求項３９に記載のコンピュータプログラム。
【請求項４２】
そのプログラムプロダクトが１つ又はそれ以上のコンピュータで実行されたときに、請求項３３乃至３８のうちいずれか一項に記載の方法を実行するために、コンピュータ読み出し可能な媒体に格納されたプログラムコード手段を有するコンピュータプログラムプロダクト。
【発明の詳細な説明】
【０００１】
本発明は、個人データストレージ及び保護に関連する。
【０００２】
例えば、ディジタル携帯情報端末、ラップトップコンピュータ、個人コンピュータ又は、同様な装置のような、個人データ装置は、例えば、個人オルガナイザーとして働くために、関連するメモリモジュールに、個人データを格納することが知られている。しかしなが

ら、格納されたデータを使用するために、データはディスプレイに表示されそして、手動で読み出され又は他の装置へ再度鍵をかけられねばならない。

【０００３】

例えば、コンピュータの周辺装置と通信するために、そのような装置には、短距離の無線通信を使用する提案がある。例えば、いわゆるブルーツース技術が、例えば、データとメディアファイルの伝送のために、ポイントオブセールス端末との通信のために、電子財布へ金銭を入れるために、ホテルと空港への自動的なチェックインのために、店とレストランの支払いのために、電灯と暖房の遠隔スイッチオンとオフ及びドアの遠隔ロックのために、提案されている。ブルーツースは、１００メートルまでの典型的な範囲をわたって動作する、２．４ＧＨｚ周波数帯を使用する、グローバルな標準である。

【０００４】

しかしながら、個人データ装置と関連するそのようなアプリケーションは、悪用を受けやすい。本発明の目的は、そのような格納された個人データのさらなる安全性を提供することである。

【０００５】

本発明の第１の特徴に従って、個人データ及び／又はソフトウェアを格納するストレージ手段と、格納された個人データ及び／又はソフトウェアへのアクセスを、許可されたユーザへ制限する認証手段と、サーバ上に、少なくとも幾つかの格納された個人データ及び／又はソフトウェアの複製コピーを維持するために、サーバへ、少なくとも幾つかの格納された個人データ及び／又はソフトウェアをアップロードするために、個人データ装置とサーバの間で、少なくとも幾つかの個人データ及び／又はソフトウェアを転送する通信手段と、許可されていない使用から個人データ及び／又はソフトウェアを保護するために、ストレージ手段内に格納された少なくとも幾つかのデータ及び／又はソフトウェアを消去する消去手段とを有する、個人データ装置が提供される。

【０００６】

好ましくは、消去手段は、個人データ装置を使用するために、許可されていないユーザにより試みがなされたときに、少なくとも幾つかのデータ及び／又はソフトウェアを消去するように適合される。

【０００７】

便利に、消去手段は、予め定められた複数の試みの後に、認証手段の認証基準が満たされないときに、少なくとも幾つかのデータ及び／又はソフトウェアを消去するように適合される。

【０００８】

代わりに、消去手段は、サーバから信号を受信したときに、少なくとも幾つかの個人データ及び／又はソフトウェアを消去するように適合される。

【０００９】

好ましくは、個人データ装置には、サーバからの信号の受信のために受信手段に電力を供給するのに十分であり且つ個人データ及び／又はソフトウェアを消去する消去手段に電力を供給するのに十分である不断のスタンバイ電力供給手段が設けられている。

【００１０】

代わりに、消去手段は、個人データ装置の未使用の第１の所定の時間の期間の後に及び／又は、個人データ装置とサーバが同期してから第２の所定の時間の期間の後に、少なくとも幾つかの個人データ及び／又はソフトウェアを消去するように適合される。

【００１１】

便利に、消去手段は、許可されていないユーザが消去が発生したことを知らされずに、少なくとも幾つかの個人データ及び／又はソフトウェアを消去するように適合される。

【００１２】

優位に、消去手段は、個人データ装置に格納された変数をデフォルト値にリセットするように適合される。

【００１３】

好ましくは、個人データ装置は、個人データ及び／又はソフトウェアをサーバからダウンロードする手段を含む。

【００１４】

優位に、暗号化されたフォーマットで、個人データ装置上に、個人データ及び／又はソフトウェアを格納するために、暗号化手段及び復号手段が、設けられる。

【００１５】

好ましくは、個人データ装置は、格納されたデータ及び／又はソフトウェアへの予め定められた数の追加又は修正がなされた後に、サーバへ、新たな又は修正された格納された個人データ及び／又はソフトウェアをアップロードするために、サーバと通信を確立する手段を有する。

【００１６】

優位に、通信手段は、個人データ装置と、取引端末で取引を実行するための取引端末の間で、少なくとも幾つかの格納された個人データを転送する手段を有する。

【００１７】

好ましくは、通信手段は、取引端末と通信する短距離無線第１通信手段と、サーバと通信するネットワークへの接続のための第２の通信手段とを有する。

【００１８】

便利に、短距離無線通信手段は、１００メートルまでの範囲をわたって動作するように適合される。

【００１９】

優位に、認証手段は、パターン認識手段を有する。

【００２０】

便利に、パターン認識手段は、認可されたユーザの指紋パターン、虹彩パターン及び音声パターンのうちの少なくとも１つを認識するように適合される。

【００２１】

便利に、ストレージ手段は、対応する発行する権威者によってのみ更新可能なデータを格納し且つ、認可されたユーザにより更新可能なユーザデータを格納するように適合される。

【００２２】

好ましくは、ストレージ手段は、クレジットカード、デビットカード、パスポート、社会保障データ、運転免許証及びメンバーシップパスのうちの１つ又はそれ以上に対応するデータを含むデータを格納するように適合される。

【００２３】

優位に、ストレージ手段は、電子キャッシュ及び／又はトラベラーズチェックを格納するように適合される。

【００２４】

便利に、ストレージ手段は、チケット、ボーディングパス、処方箋、及びホテルの部屋のアクセスキーのうちの１つ又はそれ以上を含む、発行する権威者により更新可能なデータを格納するように適合される。

【００２５】

便利に、ストレージ手段は、アクセスキー、アラーム制御、自動ドア及び門制御の内の１つ又はそれ以上を含む、ユーザの自宅及び／又は自動車に関連するデータを格納するように適合される。

【００２６】

優位に、ストレージ手段は、マルチメディアファイル、アドレス帳エントリー、名刺、予約日誌、銀行の細目、保険の細目、ドナーカード及び医療履歴の内の１つ又はそれ以上を含むユーザの更新可能なデータを格納するように適合される。

【００２７】

本発明の第２の特徴に従って、個人データ及び／又はソフトウェアを格納するストレージ手段と、許可されていないアクセスから、少なくとも幾つかの個人データ及び／又はソフ

トウェアを保護するために、少なくとも幾つかの個人データ及び／又はソフトウェアを消去する消去手段とを有する個人データ装置を有し、且つ少なくとも幾つかの個人データ及び／又はソフトウェアのコピーを格納する個人データ装置に接続出来るデータベースサーバを有し、個人データ装置内のデータとデータベースサーバ内のデータが、相互に更新され且つ同期されうる、個人データ保護システムが提供される。

【００２８】

好ましくは、データベースサーバは、少なくとも幾つかの個人データ及び／又はソフトウェアを消去するように消去手段に信号を送るために、個人データ装置と通信する信号送信手段が設けられる。

【００２９】

便利に、データベースサーバは、個人データ装置状態記録手段を有し、その個人データ装置が紛失した又は盗難された報告されたと状態記録手段が更新されたときに、信号送信手段がその個人データ装置に、その個人データ装置内に格納された少なくとも幾つかの個人データ及び／又はソフトウェアを消去するように信号を送る。

【００３０】

優位に、データ保護システムは、通信ネットワークを介して、データベースサーバを個人データ装置に接続する通信手段を有する。

【００３１】

便利に、個人データ装置とデータベースサーバの少なくとも１つは、暗号化されたフォーマットで、個人データ及び／又はソフトウェアが格納されるように、暗号化手段及び復号手段を有する。

【００３２】

優位に、データ保護システムは、更に、個人データ装置内に格納された個人データを更新するための、発行する権威者通信手段を有する、発行する権威者サーバを有する。

【００３３】

好ましくは、発行する権威者サーバは、サーバ内に格納された個人データを更新するためにサーバに接続可能である。

【００３４】

優位に、データベースサーバは、個人データ装置からアップロードされた第１バージョンの個人データと、データベースサーバ内に蓄積された第２バージョンの個人データとを比較するデータ比較手段と、個人データ装置とデータベースサーバの両方に格納されているデータを置換するために同期されたバージョンをそれから構成する、第１と第２のバージョンから現在のバージョンのデータを抽出する手段とを有する。

【００３５】

便利に、紛失した又は盗難されたと報告された個人データ装置を、データベースサーバ内に格納されている個人データ及び／又はソフトウェアが再ロードされる、置換個人データ装置と置きかえるために、置換手段が設けられる。

【００３６】

好ましくは、データベースサーバは、ユーザの個人データをパーソナルコンピュータへダウンロードする手段が設けられる。

【００３７】

優位に、ユーザの個人データをパーソナルコンピュータへダウンロードする手段は、パーソナルコンピュータに、暗号化されたフォーマットで格納するために、個人データをダウンロードする手段を有する。

【００３８】

本発明の第３の特徴に従って、個人データを格納し且つ保護する方法であって、ａ）個人データ及び／又はソフトウェアを格納するストレージ手段と、個人データ及び／又はソフトウェアへのアクセスを制限する認証手段と、それへの許可されていないアクセスを防ぐために、少なくとも幾つかの格納されたデータ及び／又はソフトウェアを消去する消去手段とを有する、個人データ装置を設けるステップと；ｂ）そのストレージ手段に個人デー

タ及び／又はソフトウェアを格納するステップと；ｃ）その個人データ装置に格納された少なくとも幾つかの個人データのコピーを格納するためのその個人データ装置に接続可能なデータベースサーバを設けるステップと；ｄ）その個人データ装置に格納された少なくとも幾つかのデータ及び／又はソフトウェアとそのデータベースサーバに格納された少なくとも幾つかのデータのコピーを、相互に更新し且つ同期させるステップと；ｅ）その個人データ装置に格納されたデータへの認可されていないアクセスを得る試みがなされたときに、その個人データ装置に格納された少なくとも幾つかのデータを消去するステップとを有する方法が提供される。

【００３９】

便利に、ステップｅ）は、認証手段が、少なくとも幾つかの格納された個人データ及び／又はソフトウェアへアクセスする認可されていない試みを検出したときに、実行される。

【００４０】

代わりに、ステップｅ）は、認証手段が、その認証手段の認証要求を満たすための、予め定められた数より多い不成功の試みを検出したときに、実行される。

【００４１】

好ましくは、その個人データ装置は、第１の短距離無線通信手段と、通信ネットワークを介して通信する第２の通信手段が設けられる、且つ、そのストレージ手段に個人データ及び／又はソフトウェアを格納するステップｂ）は、通信ネットワークに接続された発行する権威者サーバと通信ネットワークを介して通信する第２の通信手段を使用すること及び／又は、短距離通信手段を有する発行する権威者端末と通信する第１の通信手段を使用することを含む。

【００４２】

便利に、この方法は、短距離無線通信手段を有し且つ、その取引端末で取引を開始するために、その個人データ装置とその取引端末の間で、格納された個人データを通信するために、その個人データ装置第１通信手段を使用する、サービス提供者取引端末を設けるステップを有する。

【００４３】

本発明の第４の特徴に従って、そのプログラムが１つ又はそれ以上のコンピュータで実行されたときに、上述の方法のステップを実行するコード手段を有するコンピュータプログラムが提供される。

【００４４】

便利に、コンピュータプログラムは、コンピュータ読み出し可能な媒体上で具体化される。

【００４５】

本発明の第５の特徴に従って、そのプログラムプロダクトが１つ又はそれ以上のコンピュータで実行されたときに、上述の方法を実行するために、コンピュータ読み出し可能な媒体に格納されたプログラムコード手段を有するコンピュータプログラムプロダクトが提供される。

【００４６】

本発明の特定の実施例を、添付の図面を参照して、例により説明する。

【００４７】

図において、同様な参照番号は、同様な部分又はステップを示す。

【００４８】

図１に示されたように、本発明の１つの観点である本システムは、プロセッサ１６によりアクセス可能なデータメモリ１１を有する個人データ装置１０を有する。プロセッサには、第１の無線アンテナ１３が接続された短距離無線通信送信器／受信機１２、及び第２の無線アンテナ１５が接続された、移動電話送信器／受信機１４も接続されている。移動電話送信器／受信機１４は、インターネットネットワーク３０へアクセスするために、無線リンク２１を介して移動電話ネットワーク２０を使用するように適合されている。アンテナ１３と１５は、他に角アンテナに結合されることは理解されよう。また、プロセッサに

は、認証装置１７及びディスプレイ１８が接続されている。個人データ装置のこれらの構成要素は、以下に説明する理由のために、第１と第２の別々の電源バス１９１と１９２を通して、電池制御１９により制御される電池により電力が与えられている。電源バス１９２は、リセット設備１９３にも電力を与えている。

【００４９】

インターネット３０により、個人データ装置１０は、発行する権威者ウェブサイトサーバー４０又は、ウェブサイトデータベースサーバ５０に接続されてもよい。データベースサーバ５０は、データメモリ５１が設けられている。

【００５０】

データベースウェブサイトサーバは、インターネット３０により、データメモリ６１を有するパーソナルコンピュータ６０にも接続される。

【００５１】

短距離無線通信送信器／受信機１２を使用して、個人データ装置１０は、無線リンク７１を介して、取引端末内の、取引プロセッサ７３と通信する、互換性のある短距離通信送信器／受信機７２が装備された、取引端末７０と無線通信する。

【００５２】

短距離通信送信器／受信機１２、７２は便利に、既知のいわゆるブルーツースプロトコルを使用してもよい。

【００５３】

図２に示されたように、個人データ装置データメモリ１１は、次のようなデータのグループを含む：マルチメディアデータ、個人及び／又は法人データ、固定データ２１０、一時的なデータ２２０、ホテルデータ２３０、自動車データ２４０、自宅データ２５０及び情報データとソフトウェア２６０。これらの形式のデータは説明のためのみに与えられそして、１つ又はそれ以上のこのようなグループ又は異なるグループが使用され得る。更に、データの組織化の方法は本発明の一部を構成せず、かつ、データを組織化するどのような既知の便利な方法も使用され得る。更に、データを格納するのに使用される物理的なストレージ手段は、本発明に無関係である。

【００５４】

データが暗号化されたフォーマットで格納されるように、暗号化／復号設備が設けられるのが好ましい。

【００５５】

固定データ２１０は、図３に更に詳細に示され、これは、保持されている、デビットカードの細目３０１のような固定データ３０１－３１２の形式の例を示す。このデータは、発行する権威者３２１－３２６から得られ、そして、データは、説明される方法で、サービス提供者３３１－３３５からサービスを得るために使用される。

【００５６】

個人データ装置１０に格納された一時的なデータ２２０は、図４に、それぞれの発行する権威者４２１－４２３及びサービス提供者４３１－４３３の表示と共に、チケット４０１、ボーディングパス４０２及び処方箋４０３に関連するデータの例と共に、更に詳細に示されている。

【００５７】

図５には、個人データ装置１０内に格納されたホテルデータ２３０の例が、即ち、ホテルの記帳デスク５２１から個人データ装置１０に入力されそして、続いて、部屋の照明と暖房５３１を設定しそして、説明される方法で部屋のロック５３２を作動させる、照明と暖房の遠隔制御５０１及び部屋の鍵データ５０２のような、部屋の設定データが、示されている。

【００５８】

図６は、例えば、ユーザの自動者製造者又は販売者６２１から得られそして、個人データ装置１０のデータメモリ１１に格納され、そして、続いて、ロック６３１、自動車のアラーム６３２又は、他のアクセサリー６３３を作動させるように使用される、自動車データ

２４０の例６０１－６０５を示す。更に加えて、データ６０４、６０５は、個人データ装置から作動されうるように、ドア６３４及び門６３５のそれぞれの製造者６２２、６２３からダウンロードされてもよい。

【００５９】

同様に、図７は、例えば、ハウスエージェント又は対応する製造者７２１、７２２からダウンロードされそして、後に対応する装置７３１－７３３を作動させるのに使用される、ドア鍵コード７０１、アラームコード７０２及び暖房、照明、オーディオ及びビデオコード７０３のような、格納されうる対応する自宅データ２５０を示す。

【００６０】

データのグループ化の更なる例は、図８に示された、いわゆる情報データとソフトウェア２６０である。これは、アドレス帳８０１、名刺８０２、予約日誌８０３、銀行の細目８０４、保険の細目８０５、ドナーカード８０６及びユーザの医療履歴８０７のような、半永久的な更新可能なデータを含む。これは、そのソフトウェアが説明される方法でデータと同様に保護されるように、個人データ装置で使用される現在のバージョンのソフトウェア８０８のコピーを含んでもよい。

【００６１】

最も一般的な形式の、個人データストレージ及び保護システムの動作の方法を、図９のフローチャートに示す。図１を参照すると、個人データ装置１０は、知られた移動電話又は、ディジタル個人オルガナイザーを有しうるが、しかし、更に、指紋、虹彩パターン、音声認識、個人識別番号又は、他の認証保護のような、認証装置１７が設けられている。装置の最初の使用時に、ユーザの指紋又は虹彩パターンが、例えば、それ自体で知られた方法で装置に登録される。ステップ９１０で、ログインで、個人データ装置１０の後の使用時に、指紋、虹彩又は、ターン又は、声紋は、格納されたデータへのアクセスを許す前に装置を使用することをユーザが登録されているかを決定するために、例えば、登録されたパターンと比較される。未使用のユーザの可変期間後に、装置を不能化するために、タイミング機能が設けられてもよい。

【００６２】

図１に示されたように、個人データ装置内に格納されるデータのコピーが格納されるデータベースデータメモリ５１を有するデータベースサーバ５０が、個人データ装置１０に関連している。データベースサーバは、個人データが暗号化されたフォーマットで格納されるように、暗号化／復号設備を有することが好ましい。データベースサーバ５０は、インターネット３０と接続されたサーバであるのが便利である。この場合には、個人データ装置は、インターネット３０にアクセスするために、個人データ装置内の移動電話互換送信器／受信機１４から、無線電話リンク２１を介してサーバと通信することが、可能である。個人データ装置１０に最初にログインすると、従って、個人データ装置にログインし且つインターネットデータベースサーバ５０で登録することが必要である。この登録は、通常の識別データを送るように、データベースサーバへ、以下に説明する目的で、個人データ装置内に登録されている、登録された指紋又は虹彩パターン又は、他の認証データを送信することを含む。データベースサーバに格納されたデータは、認可されていないアクセスから、国内又は国際標準化団体により設定された少なくとも標準への、パスワード保護又は暗号化を含むことが好ましい、既知の方法で保護される。データベースサーバに登録する登録料を支払う準備がなされる。登録に際して、データベースサーバは、個人データ装置へ、本発明を動作させるのに必要な追加のソフトウェアをダウンロードしてもよい。

【００６３】

データベースサーバ５０に登録する、保護される個人データを、個人データ装置へ入れることが必要である。これは、図９で、便利に、インターネット接続を使用して、ステップ９２０で、発行する権威者にアクセスすることにより、そして、ステップ９３０での適切な認証の後に、ステップ９４０で、データをダウンロードして、実行される。例えば、図３を参照すると、デビットカードに通常格納されたデータは、インターネット３０への移動電話リンク２１を使用して個人データ装置に接続し、そして、銀行サーバ３２１へアク

セスすることにより、銀行のデビットカードデータ３０１として格納される個人データ装置へ、ステップ９４０で、ダウンロードされることが出来る。

【００６４】

代わりに、銀行サーバ又は、サーバに接続された端末が、個人データ装置の短距離通信送信器／受信機１２により使用されるブルーツースのような、同じプロトコルを使用する、短距離無線通信設備が装備されている場合には、データは、個人データ装置が銀行サーバ送信機／受信機の範囲内にあるときに、短距離無線リンク７１を使用して、その装置上にダウンロードされることができる。

【００６５】

同様な方法で、電子キャッシュ３０２又は、トラベラーズチェックは、インターネット３０を使用して又は既知の現金自動預け払い機に似たブルーツースを装備した端末使用して、個人データ装置にダウンロードされることが可能であり、そして、ユーザの銀行口座は借方に記入される。

【００６６】

さらに加えて、クレジットカードデータ３０４及びメモリカードデータ３０５は、好ましくは、ユーザの現在のクレジット限度を含む、クレジット会社のサーバ３２２からダウンロードされることができる。代わりに、要求により、装置はユーザ口座の状態をチェックする設備を含んでもよい。

【００６７】

商品券データ３０６は、例えば、電子メールによるドナーから受信された又は命令で、データメモリ１１に入力される。

【００６８】

そのようなデータが個人データ装置にロードされると、ユーザは、例えば、店やレストランのような小売店で支払いを行うために個人データ装置を使用しうる。ユーザが支払いを行えるためには、小売店は、例えば、ブルーツースプロトコルのような個人データ装置と同じ通信プロトコルを使用する短距離無線通信機能を有するポイントオフセールス端末３３１が装備される。個人データ装置にログインすると、ユーザは、指紋、虹彩パターン又は、他の認証装置１７により、認可されたユーザとして確認される。これは、装置が、認可されていないユーザにより支払いを行うのに、不正に使用されることを防ぐ。ポイントオフセールス端末と個人データ装置の間の通信リンク７１は、そして、図９、ステップ９５０で確立される。取引のコストは、ポイントオフセールス端末から個人データ装置へ通信され、ユーザは、例えば、クレジットカード、デビットカード、又は、電子キャッシュのような、支払方法を選択し、そして、支払いを認可する。ユーザデータレコードは、対応する総計で借方に記入され、例えば、クレジットカードの支払いが選択された場合には、ユーザのクレジットカード細目３０４は、図９、ステップ９６０で、ポイントオブセールス端末３３１へアップロードされ、そして、ステップ９７０で、既知の方法で、クレジット会社又は銀行から払い戻しを得ることにより、小売店の口座が続いて、貸方に記入される。要求される場合には、取引は、さらに電子署名により認証されてもよい。代わりに、電子キャッシュは、例えば、個人データ装置から取引端末へ転送される。

【００６９】

個人データ装置のクレジットカードデータがユーザの現在のクレジット限度も含んでいる場合には、クレジットチェックが個人データ装置と直接的に実行されることが出来るので、小売店は、支払いを受ける前にクレジットカード会社から認可を受ける要求はない。さらに加えて、個人データ装置内のユーザの利用できるクレジット限度は、ユーザの新たな利用できるクレジット限度を示す取引の値により、すぐに借方に記入されることができる。利用できるクレジットの現在の値は、ユーザが次に、クレジットカード会社へ、説明される方法で、支払いを行うときに、明らかに、再び増加される。ユーザがクレジットカードの支払いを、個人データ装置を使用する以外で、行うときには、利用できるクレジット限度は、データベースサーバ上の個人データを更新することにより、クレジットカード会社により更新もされ、それにより、個人データ装置上の対応するデータは続いて更新され

うる。

【００７０】

個人データ装置は、図３に示されたような多くの他の形式のデータも保持する。例えば、個人識別データ３０７又は、パスポートを発行する権威者３２３からダウンロードされたパスポートデータは、金銭データがダウンロードされるのと同様な方法である。そのようなデータは、典型的には、認可されたユーザのパスポート形式の写真を含む。個人データ装置は、そして、例えば、空港チェックインデスク又は、空港の入り口で、ブルーツースを装備する端末と通信するために使用され、格納された写真を含むパスポートデータが、操作者に表示され又は、例えば、データ内のキーへの操作者の要求なしに、自動確認又は入国管理チェックで使用される。

【００７１】

図３に示されているように、格納されたデータは、社会保障局３２４からダウンロードされそして、利益オフィス３３３で利益を請求するのに使用される、社会保障データ３０９も含みうる。そのような支払いは、個人データ装置に支払われる、電子キャッシュ３０２の形式でもよい。同様に、運転免許データ３１０は、運転免許局３２５からダウンロードされ、そして、自動的に、例えば、ブルーツースに準拠する装置３３４を装備する警察官により、再び、遅延又は遠隔の警察操作者によるキーボードでデータを入力するのに関連する誤りの可能性なしに、読まれる。他の応用では、メンバーシップの細目が、例えば、ユーザの装置が、ブルーツースに準拠する装置３３５により読まれたときに、メンバーシップのユーザの特権を認めるために、クラブ又は会のインターネットウェブサイトから自動的にダウンロードされうる。国際電話カードデータ３１２は、固定データ２１０ともに保持されうる。

【００７２】

図４を参照すると、個人データ装置は、あまり恒久的ではない又は一時的なデータ２２０を格納することも出来る。例えば、装置は、例えば、交通又は娯楽のための、チケットの細目４０１を格納しうる。従って、汽車の季節チケット又は航空機チケットは、装置の移動電話送設備１４を使用してインターネット３０を介して又は、短距離無線リンク７１を使用して予約オフィスから、オンラインで購入できる。そして、この装置は、例えば、ブルーツースに準拠するチケット境界４３１を通して、入場をするのに使用されうる。同様に、ボーディングパスデータ４０２は、空港のチェックインデスクで、ブルーツースに準拠する無線リンク７１を介してダウンロードされそして読まれることが可能であり、そして、要求される場合には、ブルーツースに準拠の装備されたボーディングゲート４３２で消去されることが出来る。更に加えて、処方箋データ４０３は、医者又は検眼士の医院でダウンロードされそして読まれることができ、そして、要求される場合には、他のブルーツース準拠の端末４３３を使用して、薬局又は検眼士への支払いでそれぞれ、消去されることが可能である。代わりに、患者から離れた場所から、医師により、健康状態が診断される場合には、又は処方箋を繰返すために、処方箋が、インターネット３０を使用して患者の装置にダウンロードされてもよい。

【００７３】

図５に示されたように、本発明は、ホテル環境での応用も有する。チェックインデスク５２０でホテルに記帳するときに、割当てられたルームキー５０２についてのコードは、個人データ装置１０にダウンロードされ、そして、他のブルーツースに準拠の無線リンク７１を使用して、ドアロックに格納されたコードを伝送することにより、部屋のドア５３２の鍵を開ける又は施錠するのに使用される。同様に、部屋の設定コード５０１は、例えば、部屋の照明と暖房を制御するために、装置が遠隔的に使用されることを許すために、ダウンロードされてもよい。本発明の実施例に従って、装置が制御範囲内にきてそして個人データ装置のディスプレイ上に照明スイッチを示すアイコンの表示を発生するときに、装置は、遠隔照明制御と、通信リンク７１を確立してもよい。ホテルのチェックインデスクでデータがロードされる代わりに、部屋が前もって予約されている場合に、時間制限されたデータが、ユーザの個人データ装置へ、例えば、インターネット３０を使用して、遠隔

的にダウンロードされ、それにより、チェックインを急がせ、又は、到着時のチェックインの必要を避ける。データが時間制限されていない場合には、それにより、データ２３０は、予約された滞在の最後に、個人データ装置から自動的に消去されず、データはチェックアウトの手続の一部として消去されうる。

【００７４】

図６に示されたように、本発明は、自動車の使用に関連するデータ２４０に関連する応用も有する。ホテル応用と同様な方法で、個人データ装置は、鍵コード６０１、アラームコード６０２及び、暖房、及びオーディオ、座席調整及びナビゲーション制御のような、アクセサリーの動作のためのコード６０３を格納するのに使用される。これらのコードは、例えば、自動車又はアクセサリ製造者サーバ６２１から遠隔的にダウンロードされ、自動車販売者からローカルに又は遠隔的にダウンロードされうる。代わりに、自動車に新たなアクセサリーが追加された場合には、それらは、バーコード又は、個人データ装置へコード６０３を入力するための機械読み出し可能な装置が設けられる。同様な方法で、コード６０４、６０５が、それぞれの製造者６２２、６２３から、遠隔的に制御されたガレージドア６３４又は門６３５を動作させるために、ダウンロードされる。

【００７５】

本発明のシステムは、自動車と同様な方法で、例えば、対応する製造者又はハウスエージェント７２１、７２２からダウンロードされることにより、鍵コード７０１、アラームコード７０２及び、他の遠隔的制御コード７０３が格納され、そして、ブルーツースに準拠のロック７３１、アラーム７３２及び他の装置７３３を動作させるのに使用される、図７に示されたように、自宅で使用されるデータ２５０についての応用も有する。個人データ装置が、ユーザの自宅内のブルーツース端末の範囲内にもたらされたときに、装置は、照明を点灯し、そして、予め定められた温度に暖房する設定を開始しうる。

【００７６】

図８を参照すると、個人データ装置は、例えば、キーボードから入力され又は、説明された方法でパーソナルコンピュータ６０からダウンロードされる、他の可変データ２６０を、知られた方法で、格納するのにも使用されうる。従って、装置は、アドレス帳８０１、名刺８０２と予約日誌８０３を組み込み、これは、インターネット３０を介して電子メールされ、又は、ブルーツースリンク７１により、他の個人データ装置へ転送される。装置は、例えば、保険細目８０５、ドナーカードデータ８０６及びユーザの医療履歴８０７を格納するのにも使用される。医療履歴は、そして、診療、医療干渉、又は緊急で、ブルーツース準拠の装置により読み出され且つ更新されることは理解されよう。

【００７７】

設備は、医療履歴データへの緊急アクセスが提供され、これは、認可されたユーザが意識不明の又は、その他の無能化されたときに、使用するための認証設備を迂回する。

【００７８】

上述のように、図１を再び参照し、個人データ装置は、例えば、インターネット３０を使用して、個人データ装置１０のデータメモリ１１に格納されるデータのコピーを格納するデータベースデータメモリ５１を有するデータベースサーバ５０と接続される。データベースサーバは、個人データ装置に格納されたデータとソフトウェアの複製版を格納するのに使用され得る。従って、個人データ装置とデータベースサーバ上に格納されたデーを同期させるために、個人データ装置は、時々、データベースサーバにログインされることが必要である。例えば、個人データ装置は、個人データ装置に格納された個人データが修正又は追加がされたときに毎回、インターネット３０上でデータベースサーバ５０と交信する。代わりに、３回の変更後に又はユーザにより選択された他の頻度で、更新がなされる。既に格納された個人データのバージョンと個人データ装置内の現在のデータが比較されそして、変更された又は装置又はサーバのいずれか上で新しいデータが適切として、いずれかの方向にコピーのみがされ、装置とサーバの両方で新たな現在のバージョンを生成する、設備がデータベースサーバ上に設けられる。

【００７９】

データベースサーバは、例えば、クレジットカード会社へ支払いがユーザによりなされたときに又は、クレジットカードの支払いが個人データ装置以外によりなされたときに、それにより、個人データ装置は、装置１０がデータベースサーバ５０に次にログインしたときに、新たなデータで更新される、例えば、新たな利用できるクレジット限度のような、発行する権威者からの更新を格納するのにも使用されるので、この２方向チェックは必要である。

【００８０】

認可されたユーザは、認可を受ける、個人データ装置又はデータベースサーバ上に格納された自分の個人データを見る。このデータは、対応する発行する権威者のインターネットアドレスに関連され、それにより、ユーザは、例えば、発行する権威者サーバ上のユーザの細目又は口座にアクセスするために、発行する権威者へアクセスしうる。

【００８１】

このデータベースサーバは、個人データ装置が紛失した又は交換されたときに、重要な機能も実行する。図１１を参照すると、ステップ１１０で、個人データ装置１０が紛失したとデータベースサーバ５０へ報告されると、データベースサーバは紛失した装置に交信を求める。例えば、装置は、インターネット又は電話を介してデータベースサーバへアクセスすることにより紛失したと報告されうる。データベースサーバは、好ましくは、装置が次に電源が入れられたときに、移動電話ネットワーク２０を介して、例えば、”サイレントコール”により、ユーザに検出されないような方法で、装置と交信する。代わりに、個人データ装置は、名目上電源がオフさえているときでさえ、”サイレントコール”を受信し且つしれにより動作する十分な機能性が設けられている。そのような機能性は、個人データ装置の主電池又は、補助スタンバイ電池により電力が与えられる。代わりに、図１に示されているように、個人データ装置の構成要素は、別々の電源バス１９１と１９２により電力が供給されている。通常動作では、電力は、両方の電力バスを通してすべての構成要素に供給されるが、しかしスタンバイモードでは、電力は、電力バス１９２を介して、データメモリ１１、プロセッサ１６及び移動電話送信器／受信機１４にのみ供給される。スタンバイ電力バス１９２は、説明される目的のために、リセット１９３にも電力を供給する。装置が電源が切られたときに、データベースサーバ上で複製されることによりデータが保護されることを示すために、アイコンが、個人データ装置のディスプレイに表示されてもよい。個人データ装置が、もはや認可されたユーザの所有でないことが知らされると、データベースサーバは、個人データ装置内に格納されたデータとデータベース内の装置のために格納されたデータを比較し、適切な場合には、個人データ装置内に格納されたデータを使用してデータベース内に格納されたバージョンを更新する。データベースサーバは、そして、ステップ１１１で、例えば、個人データ装置内に格納されている全ての変数をデフォルト値にリセットするようにリセット設備１９３を使用することにより、認可されていないユーザによりデータが使用されないように、個人データ装置内に保持されているデータを消去するように、個人データ装置へ信号を送る。更に、データベースサーバは、認可されたユーザによる場合を除いて、データベースサーバで個人データ装置の後の登録を許可しない。従って、認可されていないユーザが、個人データ装置に組み込まれてる指紋又は他の認証設備を迂回しようとする場合でさえも、装置は、認可されていないユーザに、制限された機能性のみを提供する。更に加えて、個人データ装置のデータメモリ１１が十分に揮発性であるように設計され、盗人が格納されたデータを消去する”サイレンとコール”を防止するために電源を除去しようとするなら、格納されたデータは、自動的に消去され、そして、例えば、電源が回復されたときに、全ての変数をデフォルト値にリセットされる。データベースサーバは、装置が紛失したということを全ての発行する権威者に知らせるために、全ての発行する権威者へ交信もし、それにより、発行する権威者は、望むなら、置換個人データ装置で、認可されたユーザにより後に使用するための、新たな口座番号、コード又は、他の細目を発行してもよい。この目的のために、発行する権威者は、適する認証後に、ユーザの置換個人データ装置へ後にダウンロードされるデータベースサーバ上のユーザデータへ、新たなデータをダウンロードしうる。

【００８２】
認可されたユーザは、紛失した個人データ装置を交換でき、又は、後のモデルにアップグレードでき、そして、ステップ１１２で、初期化後に、新たな装置は、ステップ１１３で、データベースサーバ５０にログインでき、そして、ステップ１１４で、データベースサーバからの全ての又は幾つかのユーザの複製データを、新たな個人データ装置上にダウンロードできる。データをダウンロードするために、認可されたユーザの名前とパスワードを入力することが必要である。ユーザが自分のアクセス情報を忘れた場合には、ユーザは、例えば、データベースサーバウェブサイト上のアイコンを選択することによりサーバオペレータと交信し、そして、自身の個人データへのアクセスを得るために、音声又はテキストのいずれかにより、確認する質問に回答する。データベースサーバは、ユーザがログオフする前に、ユーザに、登録された名前とパスワードを思い出させる機会を提供する。代わりに、認可されたユーザを確認するために、パターン認識が採用されている場合には、パターンもデータベースサーバに格納されている場合には、これは、ユーザの個人データ装置又パーソナルコンピュータのいずれかを通して、サーバ上のユーザの個人データへのアクセスを提供する。このように、ユーザは、装置を交換し、そして、ユーザがいるときはいつでも、装置に、インターネットを使用してデータを再ロードする。

【００８３】
更なる改良として、個人データ装置の損失の報告に従い、ユーザに直接交換装置を送るか又は、ユーザに交換の装置を発行することをローカルな供給者に認可するかのいずれかを行う、設備が、データベースサーバ上に設けられる。そのようなサービスは保険によりまかなわれる。

【００８４】
図１０に示されているように、本発明の実施例では、例えば、第２の試み後に、個人データ装置へ成功的にログオンすることを失敗すると、個人データ装置内に格納されているデータの自動的な消去により、装置は、さらに保護される。このように、ユーザは、ステップ１００で、装置にログインする第１の試みを行い、そして、成功の場合には、ステップ１０１で、装置の主メニューが提示される。成功しない場合には、ステップ１０２で、第２の試みがなされ、成功する場合には、ステップ１０１で、主メニューが提示される。しかしながら、第２の試みでログインが成功しない場合には、ステップ１０４で、装置は、個人データ装置内の全てのデータを消去する。データを消去する前に、装置はデータベースサーバ５０と交信し、そして、ステップ１０３で、現在のバックアップを生成する必要のあるデータベースサーバへ、少なくとも何らかのデータをアップロードするのが、好ましい。認可されたユーザは、適切な認証を受け、続いて、バックアップから、個人データ装置へデータを再ロードする。

【００８５】
本発明の実施例では、図１に示されているように、ユーザのパーソナルコンピュータ６０から、データベースサーバ５０へ、アクセスが、供給される。ユーザは、パーソナルコンピュータのデータメモリ６１内に、個人データ装置内に格納されたデータのコピーを維持する。代わりに、パーソナルコンピュータは、データベースサーバにより実行されるのとは別の、全ての機能について使用されるデータベースサーバとパーソナルコンピュータを使用することなしに、個人通信データのバックアップのみを保持するために使用されることが可能である。本発明の実施例では、パーソナルコンピュータは短距離無線通信設備を装備し、個人データ装置とパーソナルコンピュータの間の通信は、更に加えて又は代わりに、短距離無線リンクによってでもよい。

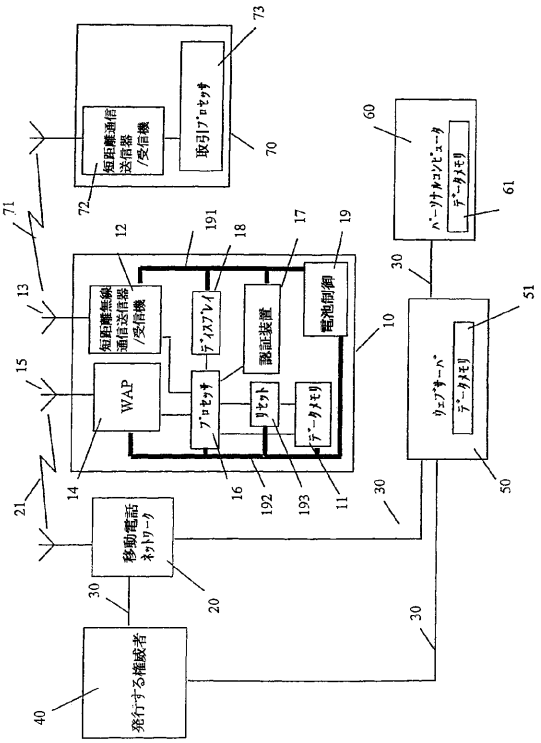
【図面の簡単な説明】

【図１】
本システムの概略のブロック図を示す図である。

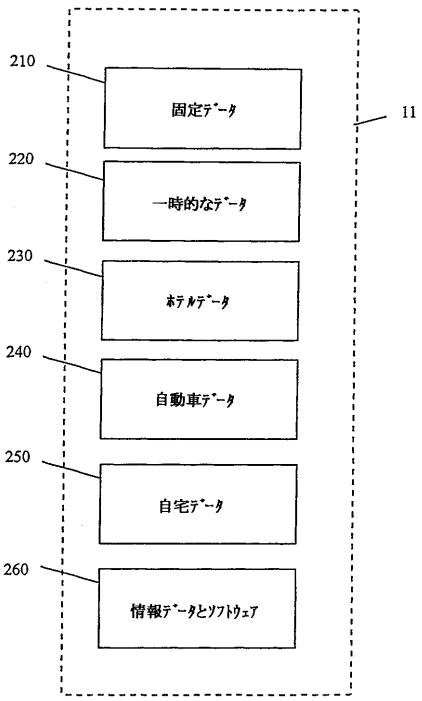
【図２】
図１のシステムとともに使用される個人データ装置内に格納された個人データのグループを示す図である。

【図３】
図２の固定データと、固定データをダウンロード及びアップロードする例を示す図である。
【図４】
図２の一時的なデータと、一時的なデータをダウンロード及びアップロードする例を示す図である。
【図５】
図２のホテルデータと、ホテルデータをダウンロード及びアップロードする例を示す図である。
【図６】
図２の自動車データと、自動車データをダウンロード及びアップロードする例を示す図である。
【図７】
図２の自宅データと、自宅データをダウンロード及びアップロードする例を示す図である。
【図８】
図２の情報データを示す図である。
【図９】
図１に示されたシステムと共に使用される個人データ装置へデータをダウンロードし且つ個人データ装置からデータを通信する方法を示すフローチャートを示す図である。
【図１０】
図９の方法のログインステップのフローチャートを示す図である。
【図１１】
図１のシステムの個人データ装置が紛失したと分かったときに続く手順のフローチャートを示す図である。

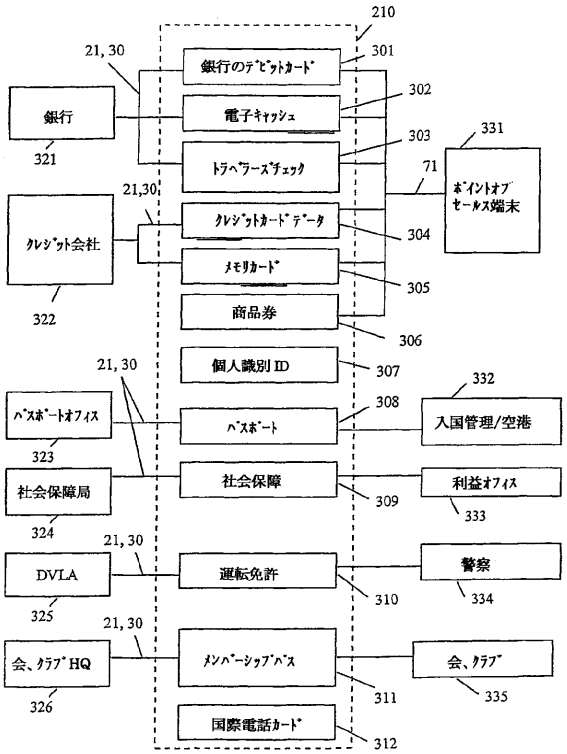
【図１】



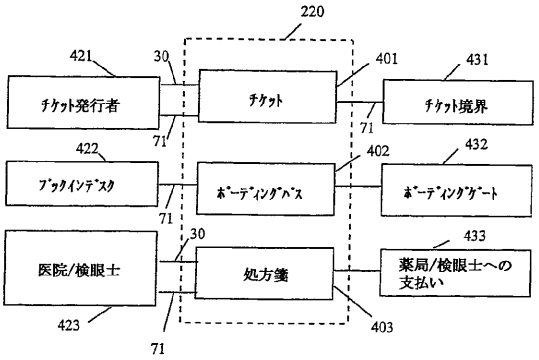
【図２】



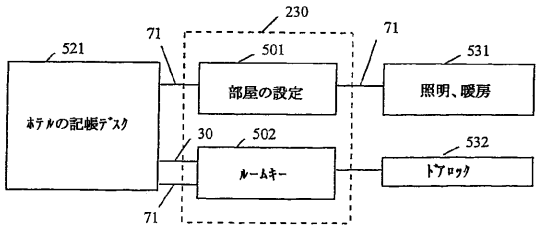
【図３】


210
21, 30
銀行のデビットカード
301
銀行
302
電子キャッシュ
303
トラベラーズチェック
331
71
ポイントオブセールス端末
21,30
クレジットカードデータ
304
クレジット会社
メモリカード
305
322
商品券
306
個人識別 ID
307
21, 30
332
パスポートオフィス
308
パスポート
入国管理/空港
323
社会保障局
社会保障
利益オフィス
309
324
333
21, 30
DVLA
運転免許
警察
310
325
334
21, 30
会、クラブ HQ
メンバーシップバス
会、クラブ
311
326
335
国際電話カード
312

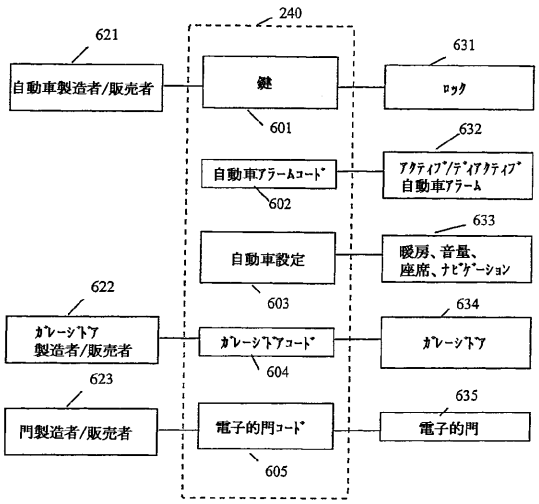
【図４】


220
421
30
401
431
チケット発行者
チケット
チケット境界
71
71
422
402
432
ブックインデスク
ボーディングパス
ボーディングゲート
71
30
433
医院/検眼士
処方箋
薬局/検眼士への支払い
423
403
71

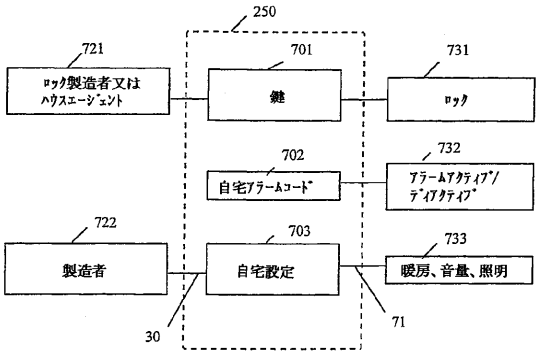
【図５】


230
71
71
521
501
531
ホテルの記帳デスク
部屋の設定
照明、暖房
30
502
532
ルームキー
ドアロック
71

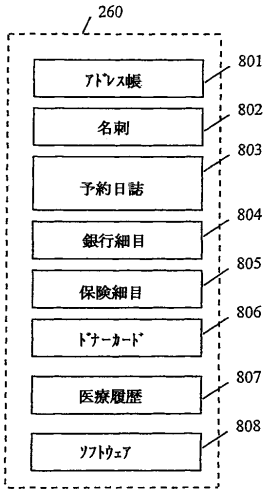
【図６】


240
621
631
自動車製造者/販売者
鍵
ロック
601
632
自動車アラームコード
アクティブ/ディアクティブ 自動車アラーム
602
633
自動車設定
暖房、音量、座席、ナビゲーション
603
622
ガレージドア製造者/販売者
ガレージドアコード
ガレージドア
604
634
623
門製造者/販売者
電子的門コード
電子的門
635
605

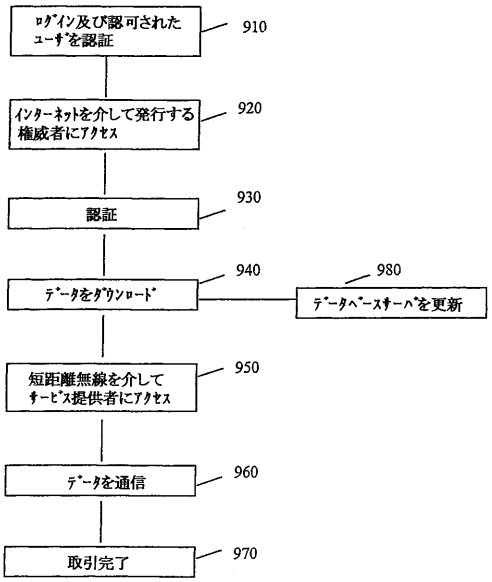
【図７】


250
721
701
731
ロック製造者又はハウスエージェント
鍵
ロック
702
732
自宅アラームコード
アラームアクティブ/ディアクティブ
722
703
733
製造者
自宅設定
暖房、音量、照明
30
71

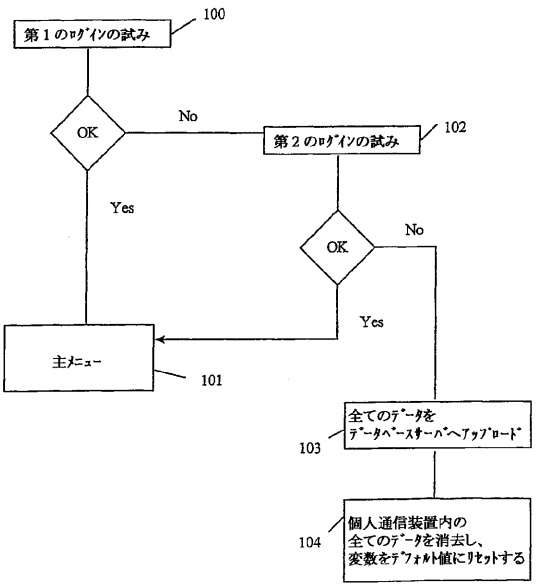
【図８】


260
アドレス帳
801
名刺
802
予約日誌
803
銀行細目
804
保険細目
805
ドナーカード
806
医療履歴
807
ソフトウェア
808

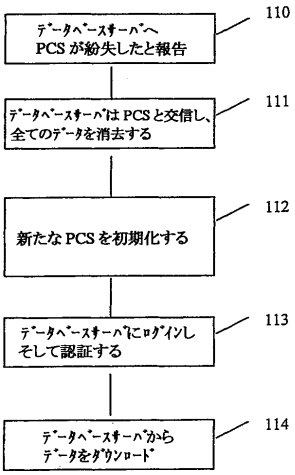
【図９】


ログイン及び認可された
ユーザを認証
910
インターネットを介して発行する
権威者にアクセス
920
認証
930
データをダウンロード
940
980
データベースサーバを更新
短距離無線を介して
サービス提供者にアクセス
950
データを通信
960
取引完了
970

【図１０】


第１のログインの試み
100
OK
No
第２のログインの試み
102
Yes
OK
No
Yes
主メニュー
101
全てのデータを
データベースサーバへアップロード
103
個人通信装置内の
全てのデータを消去し、
変数をデフォルト値にリセットする
104

【図１１】


データベースサーバへ
PCS が紛失したと報告
110
データベースサーバは PCS と交信し、
全てのデータを消去する
111
新たな PCS を初期化する
112
データベースサーバにログインし
そして認証する
113
データベースサーバから
データをダウンロード
114

【国際公開パンフレット】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 February 2002 (14.02.2002)

PCT

(10) International Publication Number
WO 02/12985 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/GB01/03342

(22) International Filing Date: 25 July 2001 (25.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0019628.7 9 August 2000 (09.08.2000) GB
0022848.6 18 September 2000 (18.09.2000) GB

(71) Applicant *(for all designated States except US)*: **DATAWIPE MANAGEMENT SERVICES LIMITED.** [GB/GB]; Unit A, Cromwell Road, Camberley, Surrey GU15 4HY (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **HAYWARD, Philip, John** [GB/GB]; La Pequenita, Portnall Drive, Wentworth, Surrey GU25 4NW (GB).

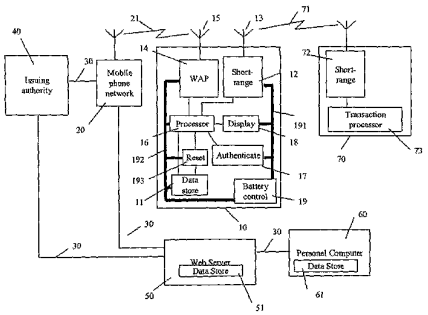
(74) Agents: **WANT, Clifford, J.** et al.; Wildman Harrold Allen & Dixon, 11th Floor, Tower 3, Clements Inn, London WC2A 2AZ (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: PERSONAL DATA DEVICE AND PROTECTION SYSTEM AND METHOD FOR STORING AND PROTECTING PERSONAL DATA



(57) Abstract: A personal data device, system and method for storing personal data including authentication means for restricting access to the stored personal data to an authorised user and communication means for transferring at least some of the personal data between the personal data device and a server. A copy of the personal data is stored on a database server and the data on the personal data device and the data on the database server is mutually updated and synchronised by communications over a communications network. A facility is supplied to delete the personal data stored on the personal data device when attempts are made by an unauthorised user to use the personal data device. The personal data may subsequently be reloaded into the personal data device, or into a replacement personal data device, from the database server.

WO 02/12985 A2

WO 02/12985 A2

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PERSONAL DATA DEVICE AND PROTECTION SYSTEM AND METHOD FOR STORING AND PROTECTING PERSONAL DATA

The present invention relates to personal data storage and protection.

Personal data devices, for example digital personal assistants, lap top computers, personal computers or similar devices are known for storing personal data in associated memory modules, for example, to act as personal organisers. However, in order to use the stored data the data has to be displayed on a display and to be manually read out or re-keyed into another device.

There are proposals to use short-range radio communications in such devices for communicating with, for example, computer peripherals. For example, so-called Bluetooth technology has been proposed, for example, for transmission of data and media files, for use for communicating with point of sale terminals, for loading money into electronic wallets, for automatic checking in at hotels and airports, for payment in stores and restaurants, for remote switching on and off of lights and heating and remote locking of doors. Bluetooth is a global standard using a 2.4 GHz frequency band, working over a typical range of up to 100 metres.

However, such applications in relation to a personal data device are susceptible to misuse. It is an object of the present invention to provide greater security of such stored personal data.

According to a first aspect of the invention there is provided a personal data device including storage means for storing personal data and/or software, authentication means for restricting access to the stored personal data and/or software to an authorised user, communication means for transferring at least some of the personal data and/or software between the personal data device and a server for uploading the at least some of the stored personal data and/or software to the server to maintain a duplicate copy of the at least some of the stored personal data and/or software on the server, and deletion means to delete the at least some of the data and/or software stored in the storage means to protect the personal data and/or software from unauthorised use.

Preferably, the deletion means is adapted to delete the at least some of the data and/or software when an attempt is made by an unauthorised user to use the personal data device.

Conveniently, the deletion means is adapted to delete the at least some of the data and/or software when authentication criteria of the authentication means are not met after a predetermined plurality of attempts.

Alternatively, the deletion means is adapted to delete the at least some of the personal data and/or software on receipt of a signal from the server.

Preferably, the personal data device is provided with uninterruptable standby power supply means sufficient to power receiving means for the reception of the signal from the server and to power the deletion means to delete the personal data and/or software.

Alternatively, the deletion means is adapted to delete the at least some of the personal data and/or software after a first predetermined period of time of non-use of the personal data device and/or after a second predetermined period of time since synchronising the personal data device with the server.

Conveniently, the deletion means is adapted to delete the at least some of the personal data and/or software without an unauthorised user being made aware that deletion is taking place.

Advantageously, the deletion means is adapted to reset variables stored in the personal data device to default values.

Preferably, the personal data device includes means to download personal data and/or software from the server.

Advantageously, encryption means and decryption means are provided for storing the personal data and/or software on the personal data device in an encrypted format.

Preferably, the personal data device includes means for establishing communications with the server to upload new or amended stored personal data and/or software to the server after a predetermined number of additions or amendments to the stored data and/or software have been made.

Advantageously, the communications means includes means for transferring at least some of the stored personal data between the personal data device and a transaction terminal for performing a transaction at the transaction terminal.

Preferably, the communication means includes short-range wireless first communication means for communicating with the transaction terminal; and second communication means for connection to a network for communicating with the server.

Conveniently, the short-range wireless communications means is adapted to operate over a range up to 100 metres.

Advantageously, the authentication means includes pattern recognition means.

Conveniently, the pattern recognition means is adapted to recognise at least one of the authorised user's fingerprint pattern, iris pattern and voice pattern.

Conveniently, the storage means is adapted to store data updatable only by a corresponding issuing authority and to store user data updatable by the authorised user.

Preferably, the storage means is adapted to store data including data corresponding to any one or more of a credit card, a debit card, a passport, social security data, a driving licence and a membership pass.

Advantageously, the storage means is adapted to store electronic cash and/or travellers' cheques.

Conveniently, the storage means is adapted to store data updatable by an issuing authority, including any one or more of tickets, boarding passes, prescriptions and hotel room access keys.

Conveniently, the storage means is adapted to store data relating to a user's home and/or car, including any one or more of access keys, alarm control, automatic door and gate control.

Advantageously, the storage means is adapted to store user-updatable data including any one or more of multimedia files, address book entries, business cards, appointment diary, bank details, insurance details, donor card and medical history.

According to a second aspect of the invention, there is provided a personal data protection system comprising: a personal data device including storage means for storing personal data and/or software and deletion means for deleting at least some of the personal data and/or software to protect the at least some of the personal data and/or software from unauthorised access; and a database server connectable to the personal data device for storing a copy of the at least some of the personal data and/or software such that the data in the personal data device and the data in the database server may be mutually updated and synchronised.

Preferably, the database server is provided with signalling means to communicate with the personal data device to signal the deletion means to delete the at least some of the personal data and/or software.

Conveniently, the database server includes personal data device status recording means such that the signalling means signals the personal data device to delete the at least some of the personal data and/or software stored in the personal data device on the status recording means being updated that the personal data device has been reported lost or stolen.

Advantageously, the data protection system includes communications means for connecting the database server to the personal data device over a communications network.

Conveniently, at least one of the personal data device and the database server includes encryption means and decryption means such that the personal data and/or software may be stored in an encrypted format.

Advantageously, the data protection system further comprises an issuing authority server having issuing authority communication means for updating the personal data stored in the personal data device.

Preferably, the issuing authority server is connectable to the server for updating the personal data stored in the server.

Advantageously, the database server includes data comparison means for comparing a first version of the personal data uploaded from the personal data device and a second version of the personal data stored in the database server and means to extract a current version of the data from the first and second versions from which to form a synchronised version to replace data stored on both the personal data device and the database server.

Conveniently, replacement means are provided to replace a personal data device that has been reported lost or stolen with a replacement personal data device into which the personal data and/or software stored in the database server may be reloaded.

Preferably, the database server is provided with means to download a user's personal data to a personal computer.

Advantageously, the means to download a user's personal data to a personal computer includes means to download the personal data for storing in an encrypted format on the personal computer.

According to a third aspect of the invention, there is provided a method for storing and protecting personal data comprising the steps of: a) providing a personal data device including storage means for storing personal data and/or software, authentication means for restricting access to the personal data and/or software and deletion means for deleting at least some of the stored data and/or software to prevent unauthorised access thereto; b) storing personal data and/or software in the storage means; c) providing a database server connectable to the personal data device for storing a copy of at least some of the personal data stored in the personal data device; d) mutually updating and synchronising the at least some of the data and/or software stored in the personal data device and the copy of the at least some of the data stored in the database server; and e) deleting the at least some of the data and/or software stored in the personal data device when an attempt is made to gain unauthorised access to data stored in the personal data device.

Conveniently, step e) is performed when the authentication means detects an unauthorised attempt to access the at least some of the stored personal data and/or software.

Alternatively, step e) is performed when the authentication means detects more than a predetermined number of unsuccessful attempts to meet authentication requirements of the authentication means.

Preferably, the personal data device is provided with first short-range wireless communication means, and second communication means for communicating over a communications network and step b) of storing personal data and/or software in the storage means includes using the second communication means to communicate over the communications network with an issuing authority server connected to the communications

network and/or by using the first communication means to communicate with an issuing authority terminal having short-range communications means.

Conveniently, the method includes the step of providing a service provider transaction terminal having short-range wireless communication means and using the personal data device first communication means to communicate stored personal data between the personal data device and the transaction terminal to initiate a transaction on the transaction terminal.

According to a fourth aspect of the invention, there is provided a computer program comprising code means for performing the steps of the method described above, when the program is run on one or more computers.

Conveniently, the computer program is embodied on a computer-readable medium.

According to a fifth aspect of the invention, there is provided a computer program product comprising program code means stored in a computer-readable medium for performing the method described above, when that program product is run on one or more computers.

Specific embodiments of the invention will now be described by way of example with reference to the accompanying drawings, in which:

Fig. 1 shows a schematic block diagram of the system;

Fig. 2 shows groups of personal data stored in the personal data device used with the system of Fig. 1;

Fig. 3 shows fixed data of Fig. 2, and examples of downloading and uploading the fixed data;

Fig. 4 shows temporary data of Fig. 2, and examples of downloading and uploading the temporary data;

Fig. 5 shows hotel data of Fig. 2, and examples of downloading and uploading the hotel data;

Fig. 6 shows car data of Fig. 2, and examples of downloading and uploading the car data;

Fig.7 shows home data of Fig. 2, and examples of downloading and uploading the home data;

Fig.8 shows information data of Fig. 2;

Fig. 9 is a flowchart showing the method of downloading data to and communicating data from the personal data device used with the system shown in Fig. 1;

Fig. 10 is a flowchart of the logging in step of the method of Fig. 9;

Fig. 11 is a flowchart of the procedure followed when a personal data device of the system of Fig.1 is found to be missing.

In the figures, like reference numerals denote like parts or steps.

As shown in Fig. 1, the system of one aspect of the invention includes a personal data device 10 including a data store 11 accessible by a processor 16. Also connected to the processor is a short-range radio communications transmitter/receiver 12, connected to a first radio antenna 13, and a mobile telephone transmitter/receiver 14 connected to a second radio antenna 15. The mobile telephone transmitter/receiver 14 is adapted to use a mobile telephone network 20 over a radio link 21 to access an Internet network 30. It will be understood that the antennas 13 and 15 may be combined into a single antenna. Also connected to the processor is an authentication device 17 and a display 18. These components of the personal data device are powered by battery controlled by a battery control 19 through first and second separate power buses 191 and 192, for a reason to be discussed below. The power bus 192 also powers a reset facility 193.

By means of the Internet 30, the personal data device 10 may be connected to an issuing authority web-site server 40 or a web-site database server 50. The database server 50 is provided with a data store 51.

The database web-site server is also connectable by the Internet 30 to a personal computer 60 having a data store 61.

Using the short-range radio transmitter/receiver 12 the personal data device 10 may also be in radio communication over a radio link 71 with a transaction terminal 70 equipped with a compatible short-range transmitter/receiver 72 in communication with a transaction processor 73 within the transaction terminal.

The short-range transmitter/receivers 12, 72 may conveniently use the known so-called Bluetooth protocol.

As shown in Fig. 2, the personal data device data store 11 may include groups of data as follows: multimedia data, personal and/or corporate data, fixed data 210, temporary data 220, hotel data 230, car data 240, home data 250 and information data and software 260. These types of data are given for illustration only and one or more such grouping or different groupings may be used. Moreover, the method of organisation of the data does not form part of the invention and any convenient known method of organising the data may be used. Furthermore, the physical storage means used for storing the data is irrelevant to the invention.

Preferably encryption/decryption facilities are provided such that the data may be stored in an encrypted format.

The fixed data 210 is shown in greater detail in Fig. 3, which shows examples of the types of fixed data 301-312, such as debit card details 301, that may be held. This data is obtained from issuing authorities 321-326 and the data is used to obtain services from service providers 331-335 in a manner to be described.

The temporary data 220 stored in the personal data device 10 is shown in greater detail in Fig. 4, with examples of data relating to a ticket 401, a boarding pass 402 and a prescription 403 with indications of the respective issuing authorities 421-423 and the service providers 431-433.

An example of hotel data 230 stored in the personal data device 10 is shown in Fig. 5, namely room settings data, such as lighting and heating remote control codes 501 and room key data 502 which are entered into the personal data device 10 from the hotel booking desk 521 and subsequently used to set the room lighting and heating 531 and operate the room lock 532 in a manner to be described.

Fig. 6 shows examples 601-605 of car data 240 which may obtained, for example, from the user's car manufacturer or dealer 621 and stored in the data store 11 of the personal data device 10 and subsequently used to operate locks 631, a car alarm 632 or other accessories 633. In addition data 604, 605 may be downloaded from the respective manufacturers 622, 623 of doors 634 and gates 635 so that they may be operated from the personal data device.

Similarly, Fig. 7 shows corresponding home data 250 which may be stored, such as door key codes 701, alarm codes 702 and heat, light, audio and video codes 703 that may downloaded, for example, from a house agent or corresponding manufacturer 721, 722 and subsequently used to operate the corresponding devices 731-733.

A further example of a data grouping is so-called information data and software 260 shown in Fig. 8. This may include such semi-permanent updatable data as an address book 801, a business card 802, an appointments diary 803, bank details 804, insurance details 805, a donor card 806 and the user's medical history 807. This may include a copy of the current version of software 808 used on the personal data device so that this software may also be protected as well as the data in a manner to be described.

The method of operation of the personal data storage and protection system in its most general form is shown in the flowchart of Fig. 9. Referring also to Fig. 1, the personal data device 10 may have the functions of a known mobile telephone or a digital personal organiser, but is further provided with an authentication device 17 such as a fingerprint, iris pattern, voice recognition, personal identity number or other authentication protection. On first use of the device the user's fingerprint or iris pattern, for example, are registered by the device in a manner known, *per se*. On subsequent use of the personal data device 10 on logging in, step 910, the fingerprint, iris pattern or voice print, for example, is compared with the registered pattern to determine whether the user is registered to use the device before allowing access to the stored data. A timing function may be provided to disable the device after a user-variable period of non-use.

As shown in Fig. 1, associated with the personal data device 10 is a database server 50 having a database data store 51 in which can be stored a copy of the data to be stored in the personal data device. Preferably the database server includes encryption/decryption facilities so that the personal data may be stored in an encrypted format. The database server 50 may

conveniently be a server connected to the Internet 30. In this case it is possible for the personal data device to communicate with the server over a mobile telephone link 21 from the mobile telephone compatible transmitter/receiver 14 in the personal data device to access the Internet 30. On first logging into the personal data device 10, it is therefore necessary to log into and register the personal data device with the Internet database server 50. This registration, as well as submitting usual identification data includes transmitting to the database server the registered fingerprint or iris pattern or other authentication data registered in the personal data device for a purpose described below. The data stored on the database server is protected in known ways from unauthorised access, preferably including password protection and encryption to at least a standard set by national or international standards bodies. Arrangements may be made to pay a registration fee on registering with the database server. On registration, the database server may download to the personal data device such additional software as is necessary to operate the invention.

Having registered with the database server 50, it is necessary to populate the personal data device with personal data to be protected. This may be conveniently performed using the Internet connection by accessing, step 920, an issuing authority and downloading data, step 940, after suitable authentication, step 930, see Fig. 9. For example, referring to Fig. 3, data normally stored on a debit card can be downloaded, step 940, to the personal data device to be stored as bank debit card data 301 by connecting the personal data device using the mobile telephone link 21 to the Internet 30 and then accessing a bank's server 321.

Alternatively, if the bank server, or a terminal connected to the server, is equipped with short-range wireless communications facilities using the same protocol, such as Bluetooth, which is used by the short-range transmitter/receiver 12 of the personal data device, then the data can be downloaded onto the device using the short-range wireless link 71 when the personal data device is within range of the bank server's transmitter/receiver.

In a similar manner electronic cash 302 or traveller's cheques can be downloaded into the personal data device either using the Internet 30 or by using a Bluetooth equipped terminal similar to a known Automatic Teller Machine, and the user's bank account debited.

In addition, credit card data 304 and store card data 305 can be downloaded from a credit company server 322, preferably including the user's current credit limits. Alternatively, the device may include facilities for checking the status of the user's account on demand.

Gift voucher data 306 may be entered into the data store 11, for example, when received from, or on the instructions of, a donor by email.

With such data loaded in the personal data device the user may use the personal data device to make payments, for example at retail outlets such as shops and restaurants. In order for the user to be able to make payments the retail outlet is equipped with a point of sale terminal 331 having short-range wireless communications functionality using the same communications protocol as the personal data device, for example, the Bluetooth protocol. In logging into the personal data device the user is identified as an authorised user by the fingerprint, iris pattern or other authentication facility 17. This prevents the device being fraudulently used to make payments by an unauthorised user. A communications link 71 is then established, step 950, Fig. 9, between the point of sale terminal and the personal data device. The cost of the transaction is communicated to the personal data device from the point of sale terminal, the user selects a method of payment, for example by credit card, debit card or electronic cash, and authorises the payment. The user's data record is debited with the corresponding amount and, for example, if credit card payment has been selected, the user's credit card details 304 are uploaded, step 960, Fig. 9, to the point of sale terminal 331 and the retailer's account subsequently credited by obtaining a refund from the credit company or bank in a known manner, step 970. Where required, the transaction may be further authenticated by an electronic signature. Alternatively, electronic cash, for example, may be transferred from the personal data device to the transaction terminal.

If the personal data device credit card data also includes the user's current credit limit, there is no requirement for the retailer to receive authorisation from the credit card company before accepting payment since a credit check can be carried out directly with the personal data device. In addition, the user's available credit limit in his personal data device can be immediately debited by the value of the transaction to indicate the user's new available credit limit. The current value of credit available will obviously be raised again when the user next makes a payment to the credit card company, in a manner to be described. When the user makes credit card payments, other than by using the personal data device, the available credit limit may also be updated by the credit card company by updating the personal data on the database server so that the corresponding data on the personal data device may subsequently be updated.

The personal data device may also hold many other types of data as illustrated in Fig. 3. For example, personal identification data 307, or passport data downloaded from a passport issuing authority 323, in an analogous manner to that in which the monetary data is downloaded. Such data would typically include a passport-type photo of the authorised user. The personal data device may then be used at, for example, an airport check-in desk or a port of entry to communicate with a Bluetooth-equipped terminal so that the passport data, including the stored photograph, may be displayed to an operator or used in, for example, automatic validation or immigration checks without any requirement for the operator to key in the data.

As illustrated in Fig. 3, the stored data may also include social security data 309 downloaded from Social Security authorities 324 and used for example for claiming benefit at benefit offices 333. Such payments could be in the form of electronic cash 302 paid into the personal data device. Similarly, driving licence data 310 may be downloaded from a driving licence authority 325 and read automatically by, for example, police officers equipped with Bluetooth compliant equipment 334, again without the delay or possibility of error associated with the data being keyboarded by a remote police operator. In another application, membership details may be downloaded from, for example, a club or society Internet website automatically to grant the user privileges of membership when the user's device is read by Bluetooth compliant equipment 335. International calling card data 312 may also be held with the fixed data 210.

Referring to Fig. 4, the personal data device can also be used to store less permanent or temporary data 220. For example, the device may store ticket details 401, for example for transport or entertainment. Thus, a train season ticket or airline ticket may be bought online over the Internet 30 using the device's mobile telephone facilities 14 or from a booking office using the short-range wireless link 71. The device then may be used to gain entrance through a ticket barrier 431 that is, for example, Bluetooth-compliant. Similarly, boarding pass data 402 can be downloaded over the Bluetooth-compliant wireless link 71 at an airport check-in desk and then read, and if required, deleted, at a Bluetooth-compliant equipped boarding gate 432. In addition, prescription data 403 can be downloaded at a doctor's or optician's surgery using Bluetooth-compliant terminal and read and if required deleted using another Bluetooth-compliant terminal 433 at a pharmacy or dispensing optician respectively. Alternatively, if a medical condition is diagnosed by a doctor from a location remote from a patient, or for

repeat prescriptions, the prescription may be downloaded to the patient's device using the Internet 30.

As shown in Fig. 5, the invention also has application in an hotel environment. On booking into the hotel at a check-in desk 520 a code for an assigned room key 502 may be downloaded into the personal data device 10 and then the data used to unlock and lock the room door 532 by transmitting the stored code to the door lock using another Bluetooth compliant wireless link 71. Similarly, room setting codes 501 may be downloaded to allow the device to be used remotely to control the room lighting and heating, for example. In an embodiment of the invention, the device may establish a communication link 71 with the remote light control, for example, when the device comes within range of the control and cause the display of an icon depicting the light switch on a display of the personal data device. As an alternative to the data being loaded at the hotel check-in desk, where a room is booked in advance, time-limited data may be downloaded remotely, using, for example, the Internet 30, into the user's personal data device, thereby hastening checking in, or avoiding the need to check in on arrival. Where the data is not time-limited, so that the data 230 is not automatically deleted from the personal data device at the end of the booked stay, the data may be deleted as part of the checking-out procedure.

As shown in Fig. 6, the invention also has application in relation to data 240 related to use of a car. In a manner analogous to the hotel application the personal data device may be used to store key codes 601, alarm codes 602 and codes 603 for the operation of such accessories as heating, audio, seat adjustment and navigation controls. These codes may, for example, be remotely downloaded from the car or accessory manufacturer's server 621 or downloaded locally or remotely from a car dealer. Alternatively, where new accessories are added to a car, they may be supplied with a barcode or other machine-readable device for entering the code 603 into the personal data device. In an analogous manner, codes 604,605 may be downloaded from respective manufacturers 622, 623 for operating a remotely controlled garage door 634 or a gate 635.

The system of the invention also has application for data 250 used in a home, as illustrated in Fig. 7, in a manner analogous to that of the car in that key codes 701, alarm codes 702 and other remote control codes 703 can be stored by, for example, downloading from the corresponding manufacturer or house agent 721, 722 and used to operate Bluetooth-compliant locks 731, alarms 732 and other devices 733. When the personal data device is

brought within range of a Bluetooth terminal in the user's home, the device may initiate the turning on of lights, and setting heating to a predetermined temperature.

Referring to Fig. 8, the personal data device may also be used to store other variable data 260, in a known manner, which may, for example, be entered from a keyboard, or downloaded from a personal computer 60 in a manner to be described. Thus the device may incorporate an address book 801, an appointments diary 803 as well as a business card 802, which may be emailed over the Internet 30 or transmitted by a Bluetooth link 71 to another personal data device. The device may also be used to store, for example, insurance details 805, donor card data 806 and the user's medical history 807. It will be appreciated that the medical history may then be read and updated in any medical consultation, intervention or emergency by Bluetooth-compliant equipment.

Facilities may be provided for emergency access to the medical history data, which bypasses the authentication facilities for use when the authorised user is unconscious or otherwise incapacitated.

As indicated above, and referring again to Fig. 1, the personal data device is also connectable, for example using the Internet 30, to a database server 50 having a database data store 51 for storing a copy of the data stored in the data store 11 of the personal data device 10. The database server may thus be used to store a duplicate version of the data and software stored in the personal data device. It is therefore necessary for the personal data device to be logged into the database server from time to time to synchronise the data stored on the personal data device and on the database server. For example, the personal data device may contact the database server 50 over the internet 30 every time an amendment or addition is made to the personal data stored on the personal data device. Alternatively, updates may be made after, say, every three changes or at some other frequency chosen by the user. Facilities may be provided on the database server to compare the version of the personal data already stored with the current data in the personal data device and only to copy in either direction, as appropriate, any data which has changed or is new on either the device or the server, to create new current versions on both the device and the server.

This two-way checking is necessary because the database server may also be used to store updates from the issuing authorities, for example a new available credit limit, for example, when a payment is made by the user to the credit card company or when credit card

payments are made other than by the personal data device, so that the personal data device may be updated with the new data when the device 10 is next logged into the database server 50.

An authorised user may view his or her personal data stored on the personal data device or on the database server, subject to authorisation. The data may have associated internet addresses of the corresponding issuing authorities, so that a user may, for example, access the issuing authority server to access the user's details or account on the issuing authority server.

The database server also performs an important function when a personal data device is missing or replaced. Referring to Fig.11, if a personal data device 10 is reported missing, step 110, to the database server 50, the database server seeks to contact the missing device. The device may, for example, be reported missing by contacting the database server via the Internet or telephone. The database server preferably contacts the device in a manner undetectable to a user, for example by a "silent call" over the mobile telephone network 20, when the device is next switched on. Alternatively, the personal data device may be provided with sufficient functionality even when nominally powered off to receive the "silent call" and act upon it. Such functionality may be powered by a main battery of the personal data device or by an auxiliary standby battery. Alternatively, as shown in Fig. 1, the components of the personal data device may be powered by separate power buses 191 and 192. Under normal operation power will be supplied to all the components through both the power buses but in a standby mode, power is supplied only via power bus 192 to the data store 11, processor 16 and mobile telephone transmitter receiver 14. The standby power bus 192 also powers a reset 193 for a purpose to be described. An icon may be displayed on the personal data device display when the device is powered off to indicate that the data is protected by being duplicated on the database server. On being notified that the personal data device is no longer in the possession of the authorised user, the database server compares the data stored in the personal data device with that stored for that device in the database and, if appropriate, updates the version stored in the database using the data stored in the personal data device. The database server then signals the personal data device to delete, step 111, the data held in the personal data device so that the data cannot be used by an unauthorised user, for example, by using the reset facility 193 to reset all variables stored in the personal data device to default values. Moreover, the database server does not authorise subsequent registration of the

personal data device with the database server, except by the authorised user. Therefore, even if an unauthorised user manages to bypass the fingerprint or other authentication facility incorporated in the personal data device, the device provides only limited functionality to the unauthorised user. In addition, the data store 11 of the personal data device may be designed to be sufficiently volatile that should a thief remove the power supply to prevent a "silent call" deleting the stored data, the stored data will be automatically deleted and, for example, all variables reset to default values when the power supply is restored. The database server may also contact all issuing authorities to inform them that the device is missing, so that the issuing authorities may, if desired, issue new account numbers, codes or other details for subsequent use by the authorised user on a replacement personal data device. For this purpose, the issuing authority may, after suitable authentication, download the new data into the user's data on the database server to be subsequently downloaded to the user's replacement personal data device.

The authorised user can replace the missing personal data device, or upgrade to a later model, and after initialising, step 112, the new device, can log into the database server 50, step 113, and download, step 114, all, or some of, the user's duplicate data from the database server onto the new personal data device. In order to download the data it is necessary to enter the authorised user's name and password. If the user has forgotten his or her access information the user may, for example, contact a server operator by selecting an icon on the database server website and answer identifying questions either by voice or text communication, in order to obtain access to his or her personal data. The database server will provide an opportunity to remind the user of the registered name and password before the user logs off. Alternatively, where pattern recognition is employed to identify authorised users, this will provide access to the user's personal data on the server either through the user's personal data device or a personal computer, provided the pattern is also stored on the database server. In this manner the user can replace a device and reload the device with data using the Internet, wherever the user may be in the world.

As a further refinement, a facility may be provided on the database server, following a report of a loss of a personal data device, either to despatch a replacement directly to the user or to authorise a local supplier to issue a replacement device to the user. Such a service may be covered by insurance.

As shown in Fig. 10, in an embodiment of the invention, the device may be further protected by automatic deletion of the data stored in the personal data device on failure successfully to log into the personal data device after, for example, a second attempt. Thus, the user makes a first attempt to log into the device, step 100, and if successful is presented, step 101, with a device main menu. If unsuccessful, a second attempt, step 102, may be made and if successful the main menu is presented, step 101. However, if logging in is unsuccessful at the second attempt the device deletes, step 104, all the data in the personal data device. Preferably, before deleting the data, the device contacts the database server 50 and uploads, step 103, at least any data to the database server that is necessary to create a current backup. An authorised user may, subject to proper authentication, subsequently reload the data from the back-up into the personal data device.

In an embodiment of the invention, access is provided to the database server 50 from a user's personal computer 60, as shown in Fig. 1. The user may then maintain a copy of the data stored in the personal data device in a data store 61 of the personal computer. Alternatively, a personal computer could be used to keep the only backup of the personal communications data, without the use of a database server and the personal computer used for all the functions otherwise carried out by the database server. In an embodiment of the invention, where the personal computer is equipped with short-range wireless communications facilities, communication between the personal data device and the personal computer may, in addition or alternatively, be by a short-range wireless link.

CLAIMS

1. A personal data device including storage means for storing personal data and/or software, authentication means for restricting access to the stored personal data and/or software to an authorised user, communication means for transferring at least some of the personal data and/or software between the personal data device and a server for uploading the at least some of the stored personal data and/or software to the server to maintain a duplicate copy of the at least some of the stored personal data and/or software on the server, and deletion means to delete the at least some of the data and/or software stored in the storage means to protect the personal data and/or software from unauthorised use.

2. A personal data device as claimed in claim 1, wherein the deletion means is adapted to delete the at least some of the data and/or software when an attempt is made by an unauthorised user to use the personal data device.

3. A personal data device as claimed in claim 2, wherein the deletion means is adapted to delete the at least some of the data and/or software when authentication criteria of the authentication means are not met after a predetermined plurality of attempts.

4. A personal data device as claimed in any of claims 1 to 3, wherein the deletion means is adapted to delete the at least some of the personal data and/or software on receipt of a signal from the server.

5. A personal data device as claimed in claim 4, wherein the personal data device is provided with uninterruptable standby power supply means sufficient to power receiving means for the reception of the signal from the server and to power the deletion means to delete the personal data and/or software.

6. A personal data device as claimed in any of claims 1 to 4, wherein the deletion means is adapted to delete the at least some of the personal data and/or software after a first predetermined period of time of non-use of the personal data device and/or after a second predetermined period of time since synchronising the personal data device with the server.

7. A personal data device as claimed in any of the preceding claims, wherein the deletion means is adapted to delete the at least some of the personal data and/or software without an unauthorised user being made aware that deletion is taking place.

8. A personal data device as claimed in any of the preceding claims, wherein the deletion means is adapted to reset variables stored in the personal data device to default values.

9. A personal data device as claimed in any of the preceding claims, wherein the personal data device includes means to download personal data and/or software from the server.

10. A personal data device as claimed in any of the preceding claims, wherein encryption means and decryption means are provided for storing the personal data and/or software on the personal data device in an encrypted format.

11. A personal data device as claimed in any of the preceding claims, including means for establishing communications with the server to upload new or amended stored personal data and/or software to the server after a predetermined number of additions or amendments to the stored data and/or software have been made.

12. A personal data device as claimed in any of the preceding claims, wherein the communications means includes means for transferring at least some of the stored personal data between the personal data device and a transaction terminal for performing a transaction at the transaction terminal.

13. A personal data device as claimed in claim 10, wherein the communication means includes short-range wireless first communication means for communicating with the transaction terminal; and second communication means for connection to a network for communicating with the server.

14. A personal data device as claimed in claim 11, wherein the short-range wireless communications means is adapted to operate over a range up to 100 metres.

15. A personal data device as claimed in any of the preceding claims, wherein the authentication means includes pattern recognition means.

16. A personal data device as claimed in claim 14, wherein the pattern recognition means is adapted to recognise at least one of the authorised user's fingerprint pattern, iris pattern and voice pattern.

17. A personal data device as claimed in any of the preceding claims, wherein the storage means is adapted to store data updatable only by a corresponding issuing authority and to store user data updatable by the authorised user.

18. A personal data device as claimed in any of the preceding claims, wherein the storage means is adapted to store data including data corresponding to any one or more of a credit card, a debit card, a passport, social security data, a driving licence and a membership pass.

19. A personal data device as claimed in any of the preceding claims, wherein the storage means is adapted to store electronic cash and/or travellers' cheques.

20. A personal data device as claimed in any of the preceding claims, wherein the storage means is adapted to store data updatable by an issuing authority, including any one or more of tickets, boarding passes, prescriptions and hotel room access keys.

21. A personal data device as claimed in any of the preceding claims, wherein the storage means is adapted to store data relating to a user's home and/or car, including any one or more of access keys, alarm control, automatic door and gate control.

22. A personal data device as claimed in any of the preceding claims, wherein the storage means is adapted to store user-updatable data including any one or more of multimedia files, address book entries, business cards, appointment diary, bank details, insurance details, donor card and medical history.

23. A personal data protection system comprising:

a personal data device including storage means for storing personal data and/or software and deletion means for deleting at least some of the personal data and/or software to protect the at least some of the personal data and/or software from unauthorised access; and

a database server connectable to the personal data device for storing a copy of the at least some of the personal data and/or software such that the data in the personal data device and the data in the database server may be mutually updated and synchronised.

24. A personal data protection system as claimed in claim 23, wherein the database server is provided with signalling means to communicate with the personal data device to signal the deletion means to delete the at least some of the personal data and/or software.

25. A personal data protection system as claimed in claim 24, wherein the database server includes personal data device status recording means such that the signalling means signals the personal data device to delete the at least some of the personal data and/or software stored in the personal data device on the status recording means being updated that the personal data device has been reported lost or stolen.

26. A personal data protection system as claimed in any of claims 23 to 25, including communications means for connecting the database server to the personal data device over a communications network.

27. A personal data protection system as claimed in any of claims 23 to 26 wherein at least one of the personal data device and the database server includes encryption means and decryption means such that the personal data and/or software may be stored in an encrypted format.

28. A personal data protection system as claimed in any of claims 23 to 27, further comprising an issuing authority server having issuing authority communication means for updating the personal data stored in the personal data device.

29. A personal data protection system as claimed in claim 25, wherein the issuing authority server is connectable to the server for updating the personal data stored in the server.

30. A personal data protection system as claimed in any of claims 22 to 28, wherein the database server includes data comparison means for comparing a first version of the personal data uploaded from the personal data device and a second version of the personal data stored in the database server and means to extract a current version of the data from the first and second versions from which to form a synchronised version to replace data stored on both the personal data device and the database server.

31. A personal data protection system as claimed in any of claims 22 to 29, wherein replacement means are provided to replace a personal data device that has been reported lost or stolen with a replacement personal data device into which the personal data and/or software stored in the database server may be reloaded.

32. A personal data protection system as claimed in any of claims 22 to 30, wherein the database server is provided with means to download a user's personal data to a personal computer.

33. A personal data protection system as claimed in claim 31, wherein the means to download a user's personal data to a personal computer includes means to download the personal data for storing in an encrypted format on the personal computer.

34. A method for storing and protecting personal data comprising the steps of:

a) providing a personal data device including storage means for storing personal data and/or software, authentication means for restricting access to the personal data and/or software and deletion means for deleting at least some of the stored data and/or software to prevent unauthorised access thereto;

b) storing personal data and/or software in the storage means;

c) providing a database server connectable to the personal data device for storing a copy of at least some of the personal data stored in the personal data device;

d) mutually updating and synchronising the at least some of the data and/or software stored in the personal data device and the copy of the at least some of the data stored in the database server; and

e) deleting the at least some of the data and/or software stored in the personal data device when an attempt is made to gain unauthorised access to data stored in the personal data device.

35. A method as claimed in claim 33, wherein step e) is performed when the authentication means detects an unauthorised attempt to access the at least some of the stored personal data and/or software.

36. A method as claimed in claim 34, wherein step e) is performed when the authentication means detects more than a predetermined number of unsuccessful attempts to meet authentication requirements of the authentication means.

37. A method as claimed in any of claims 33 to 35, wherein the personal data device is provided with first short-range wireless communication means, and second communication means for communicating over a communications network.

38. A method as claimed in claim 36, wherein step b) of storing personal data and/or software in the storage means includes using the second communication means to communicate over the communications network with an issuing authority server connected to the communications network and/or by using the first communication means to communicate with an issuing authority terminal having short-range communications means.

39. A method as claimed in claims 36 or 37, including the step of providing a service provider transaction terminal having short-range wireless communication means and using the personal data device first communication

means to communicate stored personal data between the personal data device and the transaction terminal to initiate a transaction on the transaction terminal.

40. A computer program comprising code means for performing the steps of the method claimed in any of claims 33 to 38 when the program is run on one or more computers.

41. A computer program as claimed in claim 39 embodied on a computer-readable medium.

42. A computer program product comprising program code means stored in a computer-readable medium for performing the method described in any of claims 33 to 38 when that program product is run on one or more computers.

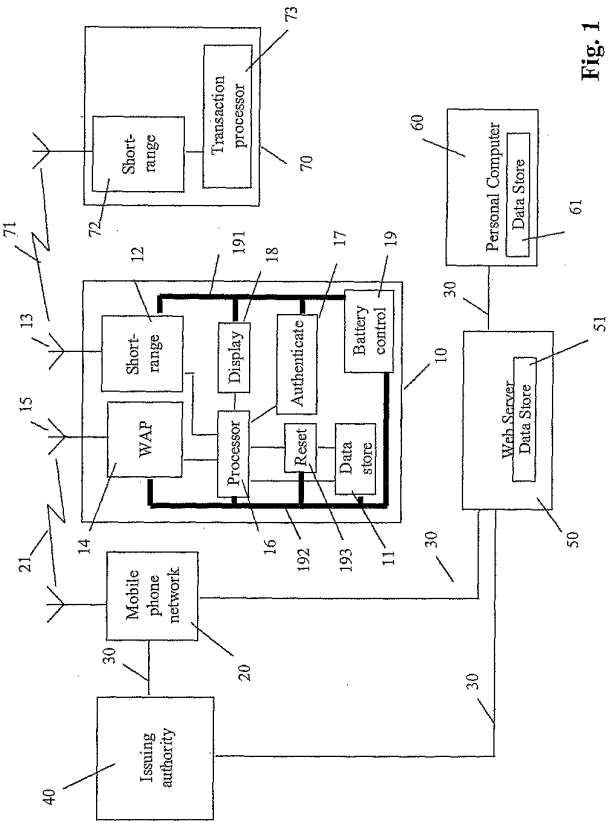

Short-range
Transaction processor
73
70
72
71
60
Personal Computer
Data Store
61
12
191
18
17
19
13
Short-range
Display
Authenticate
Battery control
30
51
10
15
WAP
Processor
Reset
Data store
Web Server
Data Store
14
16
192
193
11
50
21
30
Mobile phone network
20
30
30
40
Issuing authority

Fig. 1

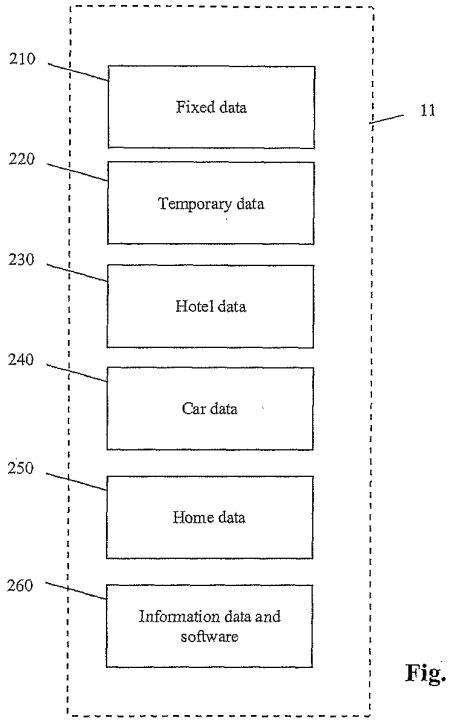

210
Fixed data
11
220
Temporary data
230
Hotel data
240
Car data
250
Home data
260
Information data and software

Fig. 2

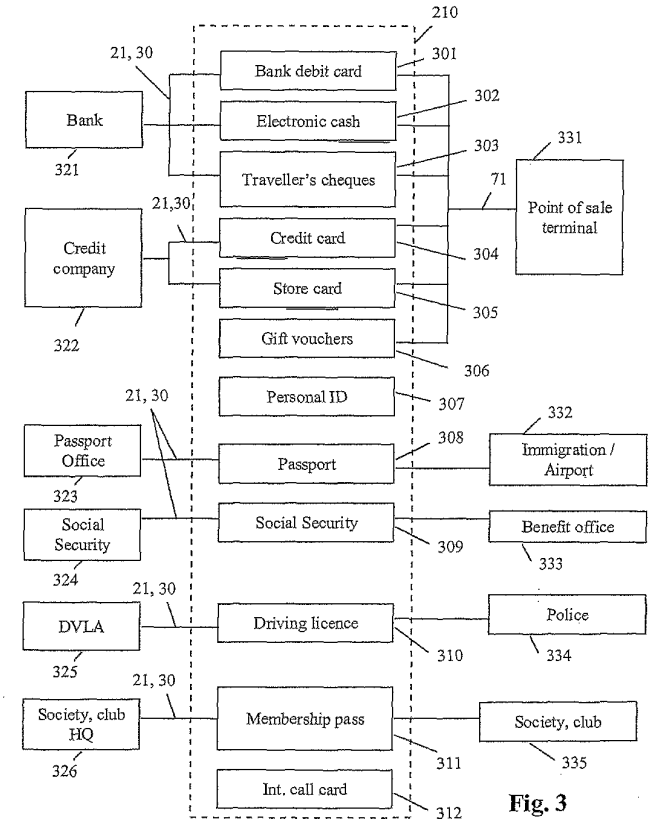

210
21, 30
Bank debit card
301
Bank
Electronic cash
302
321
303
331
Traveller's cheques
71
Point of sale terminal
21,30
Credit card
Credit company
304
Store card
305
322
Gift vouchers
306
Personal ID
307
21, 30
332
Passport Office
308
Passport
Immigration / Airport
323
Social Security
Social Security
Benefit office
309
333
324
21, 30
DVLA
Driving licence
Police
325
310
334
21, 30
Society, club HQ
Membership pass
Society, club
326
311
335
Int. call card
312

Fig. 3

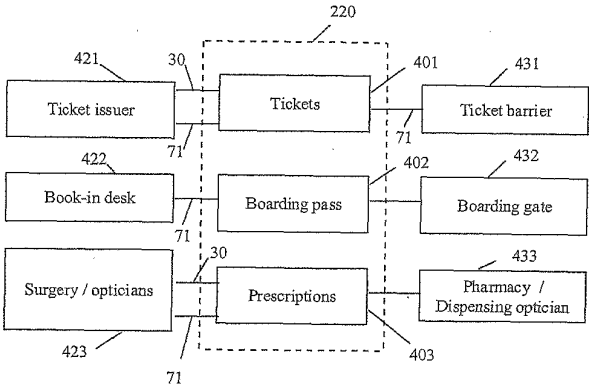

220
421
30
401
431
Ticket issuer
Tickets
Ticket barrier
71
71
422
402
432
Book-in desk
Boarding pass
Boarding gate
71
30
433
Surgery / opticians
Prescriptions
Pharmacy /
Dispensing optician
423
71
403

Fig. 4

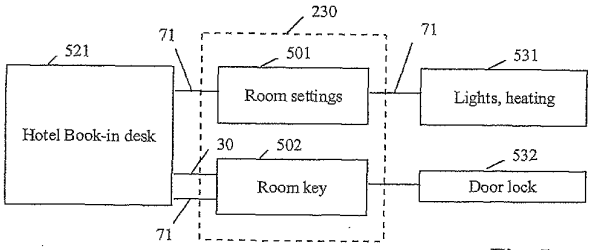

230
71
71
521
501
531
Hotel Book-in desk
Room settings
Lights, heating
30
502
532
Room key
Door lock
71

Fig. 5

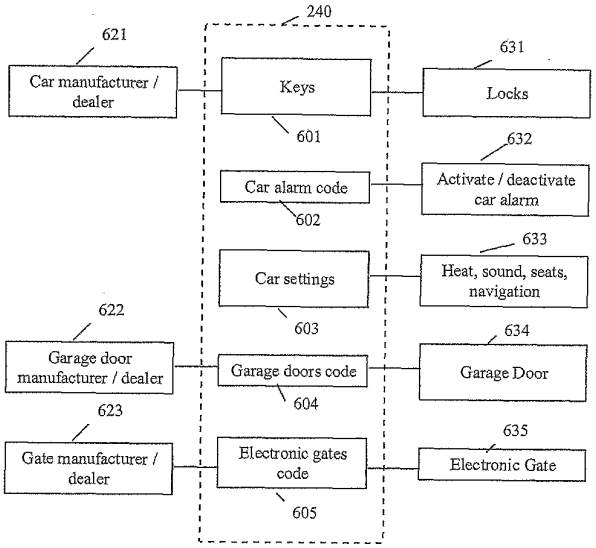

240
621
Car manufacturer / dealer
Keys
601
631
Locks
632
Car alarm code
602
Activate / deactivate car alarm
633
Car settings
603
Heat, sound, seats, navigation
622
Garage door manufacturer / dealer
Garage doors code
604
634
Garage Door
623
Gate manufacturer / dealer
Electronic gates code
605
635
Electronic Gate

Fig. 6

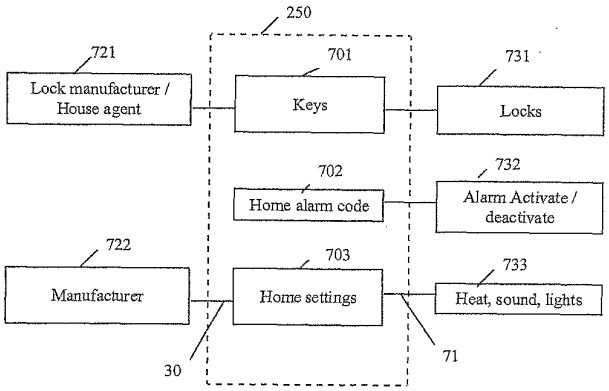

250
721
Lock manufacturer / House agent
701
Keys
731
Locks
702
Home alarm code
732
Alarm Activate / deactivate
722
Manufacturer
703
Home settings
733
Heat, sound, lights
30
71

Fig. 7

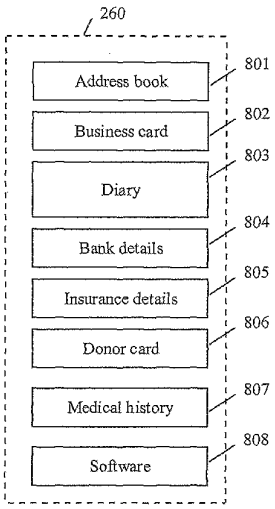

260
Address book
801
Business card
802
Diary
803
Bank details
804
Insurance details
805
Donor card
806
Medical history
807
Software
808

Fig. 8

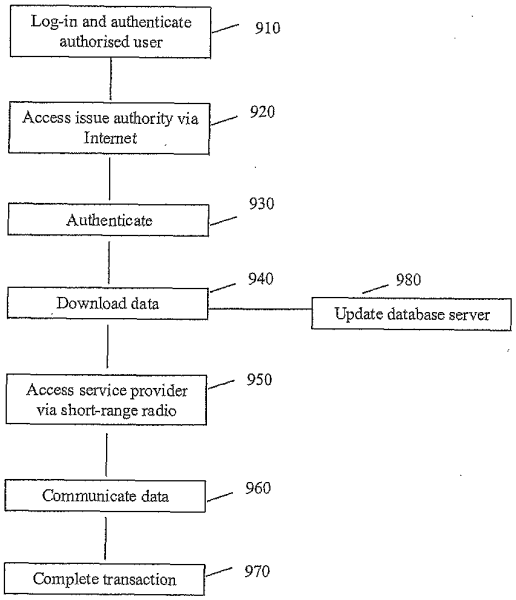
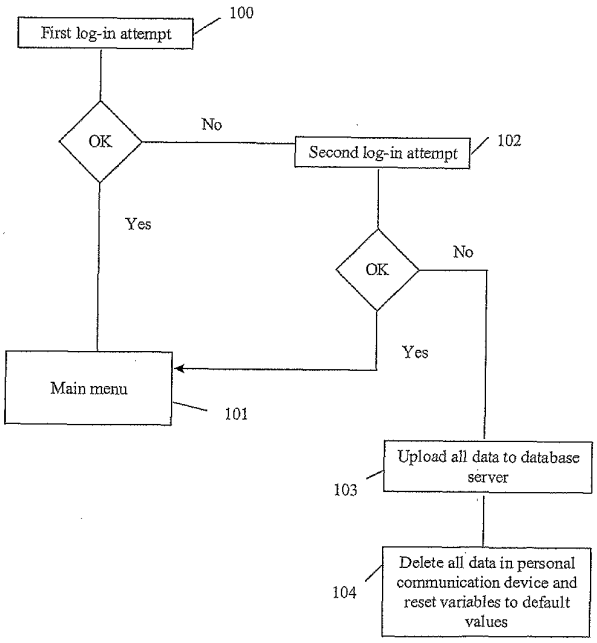

Log-in and authenticate authorised user
910
Access issue authority via Internet
920
Authenticate
930
Download data
940
980
Update database server
Access service provider via short-range radio
950
Communicate data
960
Complete transaction
970

Fig. 9

Fig. 10


First log-in attempt
100
OK
No
Second log-in attempt
102
Yes
OK
No
Yes
Main menu
101
Upload all data to database server
103
Delete all data in personal communication device and reset variables to default values
104

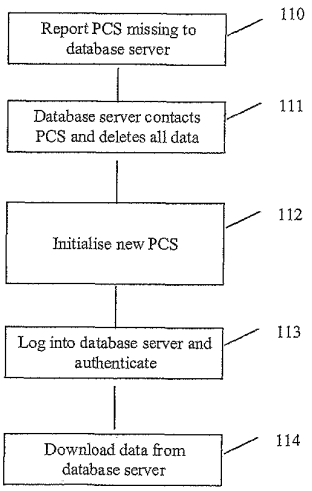

Report PCS missing to database server
110
Database server contacts PCS and deletes all data
111
Initialise new PCS
112
Log into database server and authenticate
113
Download data from database server
114

Fig. 11

【国際公開パンフレット（コレクトバージョン）】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 February 2002 (14.02.2002)

PCT

(10) International Publication Number
WO 02/012985 A3

(51) International Patent Classification⁷: G06F 1/00

(21) International Application Number: PCT/GB01/03342

(22) International Filing Date: 25 July 2001 (25.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0019628.7 9 August 2000 (09.08.2000) GB
0022848.6 18 September 2000 (18.09.2000) GB

(71) Applicant *(for all designated States except US)*: **DATAWIPE MANAGEMENT SERVICES LIMITED.** [GB/GB]; DWG 567, 24-28 St Leonards Road, Windsor, Berkshire SL4 3BB (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **HAYWARD, Philip, John** [GB/GB]; Cyprus Cottage, 35 Guildford Road, Bagshot, Surrey GU19 5JW (GB).

(74) Agents: **WANT, Clifford, J.** et al.; Wildman Harrold Allen & Dixon, 11th Floor, Tower 3, Clements Inn, London WC2A 2AZ (GB).

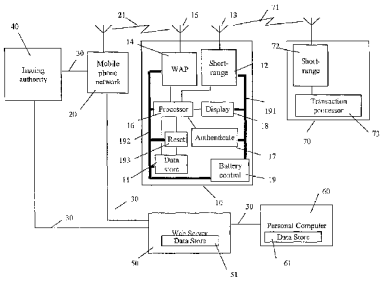
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
with international search report

[Continued on next page]

(54) **Title:** PERSONAL DATA DEVICE AND PROTECTION SYSTEM AND METHOD FOR STORING AND PROTECTING PERSONAL DATA



(57) **Abstract:** A personal data device, system and method for storing personal data including authentication means for restricting access to the stored personal data to an authorised user and communication means for transferring at least some of the personal data between the personal data device and a server. A copy of the personal data is stored on a database server and the data on the personal data device and the data on the database server is mutually updated and synchronised by communications over a communications network. A facility is supplied to delete the personal data stored on the personal data device when attempts are made by an unauthorised user to use the personal data device. The personal data may subsequently be reloaded into the personal data device, or into a replacement personal data device, from the database server.

WO 02/012985 A3

WO 02/012985 A3

before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(88) Date of publication of the international search report:
13 March 2003

【手続補正書】
【提出日】平成15年1月31日(2003.1.31)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
個人データ及び／又はソフトウェアを格納するストレージ手段と、格納された個人データ及び／又はソフトウェアへの試みられたアクセスが、許可されたユーザによってなされたかどうかを決定する認証手段と、個人データ及び／又はソフトウェアが更新されて、個人データ装置とサーバ上に、少なくとも幾つかの個人データ及び／又はソフトウェアの同期されたコピーを維持するために、その個人データ装置とそのサーバの間で、少なくとも幾つかの個人データ及び／又はソフトウェアを転送する通信手段と、その認証手段が、格納された個人データ及び／又はソフトウェアへの試みられたアクセスが、許可されたユーザ以外によってなされた決定したときに、その個人データ装置から、少なくとも幾つかの個人データ及び／又はソフトウェアを消去する消去手段とを有する、個人データ装置。
【請求項２】
消去手段は、個人データ装置を使用するために、許可されていないユーザにより試みがなされたときに、少なくとも幾つかのデータ及び／又はソフトウェアを消去するように適合される、請求項１に記載の個人データ装置。
【請求項３】
消去手段は、予め定められた複数の試みの後に、認証手段の認証基準が満たされないときに、少なくとも幾つかのデータ及び／又はソフトウェアを消去するように適合される、請求項２に記載の個人データ装置。
【請求項４】
消去手段は、サーバから信号を受信したときに、少なくとも幾つかの個人データ及び／又はソフトウェアを消去するように適合される、請求項１乃至３のうちいずれか一項に記載の個人データ装置。
【請求項５】
個人データ装置には、サーバからの信号の受信のために受信手段に電力を供給するのに十分であり且つ個人データ及び／又はソフトウェアを消去する消去手段に電力を供給するのに十分である不断のスタンバイ電力供給手段が設けられている、請求項４に記載の個人データ装置。
【請求項６】
消去手段は、個人データ装置の未使用の第１の所定の時間の期間の後に及び／又は、個人データ装置とサーバが同期してから第２の所定の時間の期間の後に、少なくとも幾つかの個人データ及び／又はソフトウェアを消去するように適合される、請求項１乃至５のうちいずれか一項に記載の個人データ装置。
【請求項７】
消去手段は、許可されていないユーザが消去が発生したことを知らされずに、少なくとも幾つかの個人データ及び／又はソフトウェアを消去するように適合される、請求項１乃至６のうちいずれか一項に記載の個人データ装置。
【請求項８】
消去手段は、個人データ装置に格納された変数をデフォルト値にリセットするように適合される、請求項１乃至７のうちいずれか一項に記載の個人データ装置。
【請求項９】
個人データ装置は、個人データ及び／又はソフトウェアをサーバからダウンロードする手段を含む、請求項１乃至８のうちいずれか一項に記載の個人データ装置。

【請求項１０】
暗号化されたフォーマットで、個人データ装置上に、個人データ及び／又はソフトウェアを格納するために、暗号化手段及び復号手段が、設けられる、請求項１乃至９のうちいずれか一項に記載の個人データ装置。
【請求項１１】
格納されたデータ及び／又はソフトウェアへの予め定められた数の追加又は修正がなされた後に、サーバへ、新たな又は修正された格納された個人データ及び／又はソフトウェアをアップロードするために、サーバと通信を確立する手段を有する、請求項１乃至１０のうちいずれか一項に記載の個人データ装置。
【請求項１２】
通信手段は、個人データ装置と、取引端末で取引を実行するためのその取引端末の間で、少なくとも幾つかの格納された個人データを転送する手段を有する、請求項１乃至１１のうちいずれか一項に記載の個人データ装置。
【請求項１３】
通信手段は、取引端末と通信する短距離無線第１通信手段と、サーバと通信するネットワークへの接続のための第２の通信手段とを有する、請求項１２に記載の個人データ装置。
【請求項１４】
短距離無線通信手段は、１００メートルまでの範囲をわたって動作するように適合される、請求項１３に記載の個人データ装置。
【請求項１５】
認証手段は、パターン認識手段を有する、請求項１乃至１４のうちいずれか一項に記載の個人データ装置。
【請求項１６】
パターン認識手段は、認可されたユーザの指紋パターン、虹彩パターン及び音声パターンのうちの少なくとも１つを認識するように適合される、請求項１５に記載の個人データ装置。
【請求項１７】
ストレージ手段は、対応する発行する権威者によってのみ更新可能なデータを格納し且つ、認可されたユーザにより更新可能なユーザデータを格納するように適合される、請求項１乃至１６のうちいずれか一項に記載の個人データ装置。
【請求項１８】
ストレージ手段は、クレジットカード、デビットカード、パスポート、社会保障データ、運転免許証及びメンバーシップパスのうちの１つ又はそれ以上に対応するデータを含むデータを格納するように適合される、請求項１乃至１７のうちいずれか一項に記載の個人データ装置。
【請求項１９】
ストレージ手段は、電子キャッシュ及び／又はトラベラーズチェックを格納するように適合される、請求項１乃至１８のうちいずれか一項に記載の個人データ装置。
【請求項２０】
ストレージ手段は、チケット、ボーディングパス、処方箋、及びホテルの部屋のアクセスキーのうちの１つ又はそれ以上を含む、発行する権威者により更新可能なデータを格納するように適合される、請求項１乃至１９のうちいずれか一項に記載の個人データ装置。
【請求項２１】
ストレージ手段は、アクセスキー、アラーム制御、自動ドア及び門制御の内の１つ又はそれ以上を含む、ユーザの自宅及び／又は自動車に関連するデータを格納するように適合される、請求項１乃至２０のうちいずれか一項に記載の個人データ装置。
【請求項２２】
ストレージ手段は、マルチメディアファイル、アドレス帳エントリー、名刺、予約日誌、銀行の細目、保険の細目、ドナーカード及び医療履歴の内の１つ又はそれ以上を含むユーザの更新可能なデータを格納するように適合される、請求項１乃至２１のうちいずれか一

項に記載の個人データ装置。
【請求項２３】
個人データ及び／又はソフトウェアを格納するストレージ手段と、許可されていないユーザにより、格納された個人データ及び／又はソフトウェアへの試みられたアクセスがなされたかどうかを決定する認証手段と、その認証手段が、格納された個人データ及び／又はソフトウェアへの試みられたアクセスが、許可されたユーザ以外によってなされたと決定したときに、個人データ装置から、少なくとも幾つかの個人データ及び／又はソフトウェアを消去する消去手段とを有する個人データ装置と、
その個人データ装置へ接続可能なデータベースサーバと、
個人データ及び／又はソフトウェアが続いて更新されて、その個人データ装置とそのサーバ上で、少なくとも幾つかの個人データ及び／又はソフトウェアの同期されたコピーを維持するために、その個人データ装置とそのデータベースサーバの間で、少なくとも幾つかの個人データ及び／又はソフトウェアを転送する通信手段とを有する、個人データ保護システム。
【請求項２４】
データベースサーバは、少なくとも幾つかの個人データ及び／又はソフトウェアを消去するように消去手段に信号を送るために、個人データ装置と通信する信号送信手段が設けられる、請求項２３に記載の個人データ保護システム。
【請求項２５】
データベースサーバは、個人データ装置状態記録手段を有し、その個人データ装置が紛失した又は盗難された報告されたと状態記録手段が更新されたときに、信号送信手段がその個人データ装置に、その個人データ装置内に格納された少なくとも幾つかの個人データ及び／又はソフトウェアを消去するように信号を送る、請求項２４に記載の個人データ保護システム。
【請求項２６】
通信ネットワークを介して、データベースサーバを個人データ装置に接続する通信手段を有する、請求項２３乃至２５のうちいずれか一項に記載の個人データ保護システム。
【請求項２７】
個人データ装置とデータベースサーバの少なくとも１つは、暗号化されたフォーマットで、個人データ及び／又はソフトウェアが格納されるように、暗号化手段及び復号手段を有する、請求項２３乃至２６のうちいずれか一項に記載の個人データ保護システム。
【請求項２８】
更に、個人データ装置内に格納された個人データを更新するための、発行する権威者通信手段を有する、発行する権威者サーバを有する、請求項２３乃至２７のうちいずれか一項に記載の個人データ保護システム。
【請求項２９】
発行する権威者サーバは、サーバ内に格納された個人データを更新するためにサーバに接続可能である、請求項２８に記載の個人データ保護システム。
【請求項３０】
データベースサーバは、個人データ装置からアップロードされた第１バージョンの個人データと、データベースサーバ内に蓄積された第２バージョンの個人データとを比較するデータ比較手段と、個人データ装置とデータベースサーバの両方に格納されているデータを置換するために同期されたバージョンをそれから構成する、第１と第２のバージョンから現在のバージョンのデータを抽出する手段とを有する、請求項２３乃至２９のうちいずれか一項に記載の個人データ保護システム。
【請求項３１】
紛失した又は盗難されたと報告された個人データ装置を、データベースサーバ内に格納されている個人データ及び／又はソフトウェアが再ロードされる、置換個人データ装置と置きかえるために、置換手段が設けられる、請求項２３乃至３０のうちいずれか一項に記載の個人データ保護システム。

【請求項３２】
データベースサーバは、ユーザの個人データをパーソナルコンピュータへダウンロードする手段が設けられる、請求項２３乃至３１のうちいずれか一項に記載の個人データ保護システム。
【請求項３３】
ユーザの個人データをパーソナルコンピュータへダウンロードする手段は、パーソナルコンピュータに、暗号化されたフォーマットで格納するために、個人データをダウンロードする手段を有する、請求項３２に記載の個人データ保護システム。
【請求項３４】
個人データを格納し且つ保護する方法であって、
ａ）個人データ及び／又はソフトウェアを格納するストレージ手段と、格納された個人データ及び／又はソフトウェアへの試みられたアクセスが、許可されたユーザによってなされたかどうかを決定する認証手段と、個人データ装置から、少なくとも幾つかの個人データ及び／又はソフトウェアを消去する消去手段とを有する、個人データ装置を設けるステップと；
ｂ）そのストレージ手段に個人データ及び／又はソフトウェアを格納するステップと；
ｃ）その個人データ装置へ通信システムにより接続可能なデータベースサーバを設けるステップと；
ｄ）個人データ及び／又はソフトウェアが続いて更新されて、その個人データ装置とそのデータベースサーバ上で少なくとも一部の個人データ及び／又はソフトウェアの同期されたコピーを維持するために、その個人データ装置とそのデータベースサーバの間で、その通信システムを介して通信するステップと；
ｅ）個人データ及び／又はソフトウェアへの試みられたアクセスが、許可されたユーザ以外によってなされたかどうかを決定するためにその認証手段を使用し且つそのようであれば、個人データ装置から、少なくとも幾つかの個人データ及び／又はソフトウェアを消去するその消去手段を使用するステップとを有する方法。
【請求項３５】
ステップｅ）では、認証手段が、その認証手段の認証要求を満たすための、予め定められた数以上の未成功の試みを検出したときに、少なくとも幾つかの個人データ及び／又はソフトウェアが消去される、請求項３４に記載の方法。
【請求項３６】
その個人データ装置は、第１の短距離無線通信手段と、通信ネットワークを介して通信する第２の通信手段が設けられる、請求項３４或は３５に記載の方法。
【請求項３７】
そのストレージ手段に個人データ及び／又はソフトウェアを格納するステップｂ）は、通信ネットワークに接続された発行する権威者サーバとその通信ネットワークを介して通信する第２の通信手段を使用すること及び／又は、短距離通信手段を有する発行する権威者端末と通信する第１の通信手段を使用することを含む、請求項３６に記載の方法。
【請求項３８】
短距離無線通信手段を有し且つ、その取引端末で取引を開始するために、その個人データ装置とその取引端末の間で、格納された個人データを通信するために、その個人データ装置第１通信手段を使用する、サービス提供者取引端末を設けるステップを有する、請求項３６或は３７に記載の方法。
【請求項３９】
そのプログラムが１つ又はそれ以上のコンピュータで実行されたときに、請求項３４乃至３８のうちいずれか一項に記載の方法のステップを実行するコード手段を有するコンピュータプログラム。
【請求項４０】
コンピュータ読み出し可能な媒体上で具体化された、請求項３９に記載のコンピュータプログラム。

【請求項４１】
そのプログラムプロダクトが１つ又はそれ以上のコンピュータで実行されたときに、請求項３４乃至３８のうちいずれか一項に記載の方法を実行するために、コンピュータ読み出し可能な媒体に格納されたプログラムコード手段を有するコンピュータプログラムプロダクト。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 01/03342

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

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 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 748 084 A (ISIKOFF JEREMY M) 5 May 1998 (1998-05-05) column 1, line 48 -column 2, line 25 column 3, line 5 - line 29	1,2,23, 26,34, 35,40,42
A	column 7, line 46 - line 67 column 8, line 22 -column 9, line 14 column 10, line 44 - line 67 figure 1 ---	4,5,24, 25
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* 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 document 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
16 December 2002	27/12/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Arbutina, L

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 01/03342

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 45243 A (TELIA AB) 3 August 2000 (2000-08-03) abstract page 6, line 30 -page 7, line 17 page 9, line 9 -page 11, line 34 page 12, line 15 - line 23	1,2,4,9, 22-26, 34,35, 40,42
A	US 5 239 166 A (GRAVES MARCEL A) 24 August 1993 (1993-08-24) abstract column 1, line 10 - line 20 column 2, line 29 -column 5, line 2 figures 1-3	1,2, 12-23,34
A	EP 0 965 902 A (NAT SEMICONDUCTOR CORP) 22 December 1999 (1999-12-22) paragraph '0010! - paragraph '0013! paragraph '0125!	1-3,10, 15,16, 18-22

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

formation on patent family members

International Application No
PCT/GB 01/03342

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5748084	A	05-05-1998	NONE		
WO 0045243	A	03-08-2000	SE	515488 C2	13-08-2001
			WO	0045243 A1	03-08-2000
			SE	9900306 A	30-07-2000
US 5239166	A	24-08-1993	CA	1326304 A1	18-01-1994
			AT	125054 T	15-07-1995
			AU	633534 B2	04-02-1993
			AU	4781590 A	26-07-1990
			DE	69020746 D1	17-08-1995
			EP	0379333 A1	25-07-1990
			JP	2271466 A	06-11-1990
			NZ	232106 A	26-05-1993
			NZ	244768 A	26-05-1993
EP 0965902	A	22-12-1999	US	5533123 A	02-07-1996
			EP	0965902 A2	22-12-1999
			DE	69519662 D1	25-01-2001
			DE	69519662 T2	23-05-2001
			EP	0715733 A1	12-06-1996
			WO	9600953 A2	11-01-1996

Form PCT/ISA/210 (patent family annex) (July 1998)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,US,UZ,VN,YU,ZA,ZW

(72)発明者 ヘイワード，フィリップ，ジョン
イギリス国，サリー ジーユー１９ ５ジェイダブリュ，バグショット，ギルドフォード・ロード ３５，サイプラス・コテージ

Ｆターム(参考) 5B017 AA07 BA08 CA16