(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4999936号
(P4999936)

(45)発行日　平成24年8月15日(2012.8.15)　(24)登録日　平成24年5月25日(2012.5.25)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| H04M 1/02 | (2006.01) | H04M | 1/02 | C |
| H04W 12/06 | (2009.01) | H04Q | 7/00 | 183 |
| H04W 84/10 | (2009.01) | H04Q | 7/00 | 629 |
| H04W 88/02 | (2009.01) | H04Q | 7/00 | 644 |
| H04M 1/667 | (2006.01) | H04M | 1/667 | |

請求項の数 25　(全 14 頁)

(21)出願番号　特願2009-548710 (P2009-548710)
(86)(22)出願日　平成19年12月28日 (2007.12.28)
(65)公表番号　特表2010-525620 (P2010-525620A)
(43)公表日　平成22年7月22日 (2010.7.22)
(86)国際出願番号　PCT/FR2007/002183
(87)国際公開番号　WO2008/102081
(87)国際公開日　平成20年8月28日 (2008.8.28)
審査請求日　平成22年5月21日 (2010.5.21)
(31)優先権主張番号　0753202
(32)優先日　平成19年2月12日 (2007.2.12)
(33)優先権主張国　フランス(FR)

(73)特許権者　508372630
オベルトゥル　テクノロジ
フランス国, エフ－９２３００　ルバロワ　ペレ, ケ　ミシュレ　５０
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100092624
弁理士　鶴田　準一
(74)代理人　100122965
弁理士　水谷　好男
(74)代理人　100141162
弁理士　森　啓

最終頁に続く

(54)【発明の名称】移動電話の近距離無線通信モジュールにおける少なくとも１の機能の実行を制御するための方法と装置

(57)【特許請求の範囲】
【請求項１】
１の移動装置（300）の少なくとも１の'無線近距離通信モジュール（335）における機能'の実行を制御する方法であって、
前記モジュールは識別手段（310）を受信するように構成されており、
－前記無線近距離通信モジュールによる情報要求(RA2)を前記識別手段に送信するステップ(420)、前記情報要求は、少なくとも１の'前記識別手段の特性情報'の取得を目的とするものである；
－前記識別手段の前記情報要求に対する応答(RS2)を受信するステップ(440)、前記応答は少なくとも１の前記識別手段の特性情報を含むものである；
－前記無線近距離通信モジュールによる前記応答を認証するステップ(445)；及び
－仮に前記応答が認証された場合、少なくとも１の'前記識別手段の特性情報'に対し応答して、前記少なくとも１の機能を実行するステップ、
を有することを特徴とする方法。
【請求項２】
－前記無線近距離通信モジュールによる認証要求（RA1）を受信するステップ（415）；及び
－仮に前記応答が認証された場合、前記少なくとも１の機能を実行する前に少なくとも１の'前記識別手段の特性情報'に対し応答して、前記認証要求に対し、無線近距離通信モジュールにより許可（RS1）を送信するステップ（450）、

を更に有することを特徴とする請求項１に記載の方法。
【請求項３】
前記識別手段と前記無線近距離通信モジュールとの間の情報の伝送は、少なくとも部分的に前記移動装置のマイクロプロセッサ（305）を介して実施され、以下のステップを有することを特徴とする請求項１又は２に記載の方法。
－前記マイクロプロセッサに前記情報を伝送するステップ（415）、前記マイクロプロセッサは前記識別手段に対し前記情報要求を伝送するように構成されている；及び/又は、
－前記マイクロプロセッサから前記応答を受信するステップ（440）、前記マイクロプロセッサは前記識別手段から前記応答を受信する。
【請求項４】
前記応答と許可の少なくとも１が、コード化されセキュリティ化され、認証可能であることを特徴とする請求項１乃至３のいずれか１項に記載の方法。
【請求項５】
前記応答と許可の少なくとも１の前記コード化及び前記セキュリティ化は、前記応答と許可の少なくとも１をコード化し、セキュリティ化する前記識別手段又は前記無線近距離通信モジュールにおいて局部的に記憶されている認証情報に基づいて実施されることを特徴とする請求項４に記載の方法。
【請求項６】
記認証情報は、特にプライベート暗号化キーであることを特徴とする請求項５に記載の方法。
【請求項７】
前記応答と許可の少なくとも１の前記コード化及び前記セキュリティ化は、前記応答と許可の少なくとも１をコード化し、セキュリティ化する前記識別手段又は前記無線近距離通信モジュールにおいて、前記応答と許可の少なくとも１をコード化し、セキュリティ化する前記識別手段又は前記無線近距離通信モジュールにおいて局部的に記憶されている認証情報に基づいて局部的に実施されることを特徴とする請求項５又は６に記載の方法。
【請求項８】
前記無線近距離通信モジュールは少なくとも部分的にセキュリティ化されていることを特徴とする請求項１乃至７のいずれか１項に記載の方法。
【請求項９】
前記少なくとも１の機能は、前記無線近距離通信モジュールにおいて記憶されているデータをアップデートすることを特徴とする請求項１乃至８のいずれか１項に記載の方法。
【請求項１０】
前記少なくとも１の機能は、外部装置への又は外部装置からの前記無線近距離通信モジュールの無線通信モードを許可することを特徴とする請求項１乃至９のいずれか１項に記載の方法。
【請求項１１】
前記少なくとも１の機能は、外部装置により提供される(複数)サービスの少なくとも１にアクセスすることを特徴とする請求項１乃至１０のいずれか１項に記載の方法。
【請求項１２】
前記識別手段と前記無線近距離通信モジュールとの間の少なくとも複数の通信はセキュリティ化されていることを特徴とする請求項１乃至１１のいずれか１項に記載の方法。
【請求項１３】
前記情報要求は、前記少なくとも１の機能に関する表示を含むことを特徴とする請求項１乃至１２のいずれか１項に記載の方法。
【請求項１４】
請求項１ないし１３のいずれか１項に基づいて、前記方法の複数ステップの各ステップを実行するように構成された命令を有するコンピュータプログラム。
【請求項１５】
請求項１乃至１３のいずれか１項に基づいて、前記方法の複数ステップの各ステップを

実行するための前記コンピュータプログラムのコード命令を有する、コンピュータ又はマイクロプロセッサにより部分的に又は全体的に読み取り可能な、取出し可能又は不可能な情報記憶手段。
【請求項１６】
識別手段（310）を受け入れるように構成されている移動装置（300）の無線近距離通信手段（335）における少なくとも１の機能を実行するための制御装置であって、以下の手段を有することを特徴とする制御装置。
－少なくとも１の情報要求を前記識別手段に送信するための手段、前記情報要求は前記識別手段の特性情報を少なくとも１つ取得することを目的とする。
－前記識別手段から前記情報要求に対する応答を受信するための手段、前記応答は前記識別カードの特性情報の少なくとも一つを含む。
－前記応答を認証するための手段；及び
－前記識別カードの特性情報の少なくとも１つに応答して少なくとも一つの機能を実行するための手段。
【請求項１７】
前記移動装置は前記認証手段及び前記実行手段とは別のマイクロプロセッサを有することを特徴とする請求項１６に記載の装置。
【請求項１８】
－少なくとも１の認証要求を受信するための手段；及び
－少なくとも１の機能を実施する前に、前記識別カードの前記少なくとも１の特性情報に応答して、前記認証要求に対する許可を送信するための手段、
を更に有することを特徴とする請求項１６または請求項１７に記載の装置。
【請求項１９】
更に、前記許可をコード化するコーディング手段又はセキュリティ化するセキュリティ化手段を有し、前記許可が認証されることを特徴とする請求項１８に記載の装置。
【請求項２０】
更に、前記許可をコード化する前記コーディング手段又はセキュリティ化するセキュリティ化手段が使用する認証情報を記憶する記憶手段を有することを特徴とする請求項１９に記載の装置。
【請求項２１】
前記記憶手段は非揮発性であることを特徴とする請求項２０に記載の装置。
【請求項２２】
前記記憶手段は、前記応答を認証するためのデータを記憶することを特徴とする請求項２０又は請求項２１に記載の装置。
【請求項２３】
前記識別手段は、移動電話ネットワークへの加入者の識別カードであることを特徴とする請求項１６乃至２２のいずれか１項に記載の装置。
【請求項２４】
前記無線近距離通信手段は標準規格ＩＳＯ14443に準拠していることを特徴とする請求項１６乃至２３のいずれか１項に記載の装置。
【請求項２５】
前記無線近距離通信手段は前記移動装置に、取出しができないように一体化されていることを特徴とする請求項１６乃至２４のいずれか１項に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、機能の実行を制御することに関する。特に、移動装置の識別子に基づいて、移動電話の近距離無線通信モジュールにおける少なくとも１の機能の実行を認証したり禁止したりするためのメカニズムに関する。
【背景技術】

【０００２】
移動装置は特別な技術的特徴を有し、複数サービスを実施するという条件の下で、移動装置の所有者に制限を加えることなく、複数のサービスを提供することが提案されている。他方、所定のユーザ、所定の移動装置にだけアクセス可能なサービスが多数存在する。例えば、契約を結んだ者または特定の予約をした者である。
【０００３】
一例として、所定期間加入者が予約者とし契約して、電話オペレータが、加入者移動電話の購入を財政支援することがある。この契約が欺かれないように、移動電話は契約期間ロックされる。その結果、電話オペレータが認証する移動電話網しか使えない。この種のメカニズムは加入者カードの供給者により実施されることができる。加入者カードは、例えば、ＧＳＭまたは３Ｇ標準規格に基づくＳＩＭ(Subscriber Identity Module)カードに含まれている情報を使う。これは一般的にソフトウェアロッキング法とよばれるもので、不正行為者は比較的に簡単にこれを避けることができる。この方法によっては、電話の情報利用システムはほとんど保護されることはない。
【０００４】
同様にして、米国特許願ＵＳＰ2006-0112275には、ＳＩＭカード（例えば、ＧＭＳ電話で使われているタイプ）とコンピュータ（例えば、ＰＣで使われているタイプ）との間の通信制御法で使用されるハードウェアロック(hardware lock:dongle)について記載されている。ＳＩＭカードは電話網により認証される。これは移動電話のＳＩＭカードが電話網により認証されるのと同様である。このように、ＳＩＭカードはコンピュータのユーザを認証する。この認証により所定期間コンピュータを使うことができる。例えば、認証後、コンピュータにロードされる特定のアプリケーションを使うことができる。このアプリケーションは、認証後で、認証に応答して、第３者によりコンピュータにロードすることができる。費用は通信ネットワークによりユーザが負い、第３者に送ることができる。前記ハードウェアロックは、ＰＩＮ(Personal Identification Number)コードを使うことによりＳＩＭカードに記憶される認証データに対し追加的セキュリティ手段を提供する。前記ＰＩＮコードは入力される必要があり、コンピュータからの要求に応じるものである。コンピュータの要求はキーを使って暗号化され、コンピュータの特定のインターフェースを使って生成される。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】米国特許願ＵＳＰ2006-0112275
【発明の概要】
【発明が解決しようとする課題】
【０００６】
このように、ＳＩＭカード等の識別カードの特性に基づいて、各種サービスに対する装置（好ましくは携帯装置）によるアクセスをコントロールする必要性が存在する。
【課題を解決するための手段】
【０００７】
本発明は認証手段に対する代替手段を提供する。この手段は、識別カードの特性に基づいて所定サービスに対するアクセスを提供し、新規なアプリケーションにブロッキング・アンブロッキング原理を使用させることを可能にする。
【０００８】
従って、本発明は少なくとも１の‘無線近距離通信モジュールにおける機能’の実行を制御する方法を対象とする。前記モジュールは識別手段を受信するように構成されており、前記方法は、次のステップを有している。
－前記無線近距離通信モジュールによる情報要求を前記識別手段に送信するステップ。前記情報要求は、少なくとも１の‘前記識別手段の特性情報’の取得を目的とするものである；

－前記識別手段の前記情報要求に対する応答を受信するステップ。前記応答は少なくとも１の前記識別手段の特性情報を含むものである；
－前記無線近距離通信モジュールによる前記応答を認証するステップ；及び
－仮に前記応答が認証された場合、少なくとも１の‘前記識別手段の特性情報’に対し応答して、前記少なくとも１の機能を実行するステップ。

【０００９】

本発明による方法によれば、識別カードの特性に基づいて、前記無線近距離通信モジュールにおける機能の実行を許可する又は拒絶することができる。特に、機能の許可又は拒絶は、識別カードを発行するオペレータに関係付けることができる。

【００１０】

１の実施例によれば、本方法は次のステップを有している。
－前記無線近距離通信モジュールによる認証要求を受信するステップ；及び
－仮に前記応答が認証された場合、前記少なくとも１の機能を実行する前に少なくとも１の‘前記識別手段の特性情報’に対し応答して、前記認証要求に対し、無線近距離通信モジュールにより許可を送信するステップ。

【００１１】

この実施例において、本発明の方法は、識別カードの特性に基づいて無線近距離通信モジュールにおける（複数）機能が外部装置に接続されているとき、これら機能を許可又は拒否する。この実施例を使うと、特に所定のサービス(複数)へのアクセスを制御するために使うことができる。

【００１２】

別の実施例において、前記識別手段と前記無線近距離通信モジュールとの間の情報の伝送は、少なくとも部分的に前記移動装置のマイクロプロセッサを介して実施される。前記方法は、次のステップを有している。
－前記マイクロプロセッサに対し前記情報を伝送するステップ、前記マイクロプロセッサは前記識別手段に対し前記情報要求を伝送するように構成されている；
及び/又は、
－前記マイクロプロセッサから前記応答を受信するステップ、前記マイクロプロセッサは前記識別手段から前記応答を受信する。

【００１３】

この実施例を使うと、移動装置のアーキテクチャを使うことができる。前記アーキテクチャにおいて、本発明が実行され、より高いセキュリティレベルを提供する。

【００１４】

前記応答と許可の少なくとも１が、コード化されセキュリティ化され、認証可能であることが有利であり、前記応答と許可が不正なプログラムによりシミュレートされることを回避することができる。

【００１５】

また、特定の実施例によると、前記応答と許可の少なくとも１の前記コード化及び前記セキュリティ化は、前記識別手段又は前記無線近距離通信モジュールにおいて局部的に記憶されている認証情報に基づいて実施される。前記応答と許可の少なくとも１をコード化し、セキュリティ化して、本方法のセキュリティを改善する。前記認証情報は、特にプライベート暗号化キーであってもよい。

【００１６】

更に、特定の実施例によると、前記応答と許可の少なくとも１の前記コード化及び前記セキュリティ化は、前記応答と許可の少なくとも１をコード化し、セキュリティ化する前記識別手段又は前記無線近距離通信モジュールにおいて、局部的に記憶されている認証情報に基づいて、前記識別手段又は前記無線近距離通信モジュールにおいて局部的に実施される。これにより、本方法のセキュリティが向上される。

【００１７】

不正行為のリスクを低減するために、前記無線近距離通信モジュールは少なくとも部分的

にセキュリティ化されている。
【００１８】
特定の実施例において、前記無線近距離通信モジュールにより実行される機能は前記無線近距離通信モジュールにおいて記憶されているデータをアップデートすることである。本発明による方法によれば、記憶されたデータが不正に別のもの置き換えられることを回避することができる。
【００１９】
前記無線近距離通信モジュールにより実行される機能は、外部装置への又は外部装置からの前記無線近距離通信モジュールの無線通信モードを許可し、通信を制御する。
【００２０】
前記無線近距離通信モジュールにより実行される機能は、外部装置により提供される(複数)サービスの少なくとも１にアクセスすることを対象としている。本発明の方法を使うと、識別カードにより提供されるサービスへのアクセスを制御でき、特に所定タイプのオペレータ又は所定タイプの契約(contrat)へのアクセスを制限することができる。
【００２１】
一つの特定の実施例において、前記識別手段と前記無線近距離通信モジュールとの間の少なくとも複数の通信はセキュリティ化されている。
【００２２】
更に、一つの特定の実施例において、前記情報要求は、選択的許可又は複数の機能の禁止についての前記少なくとも１の機能に関する表示を含む。
【００２３】
また、本発明は前記方法の複数ステップの各ステップを実行するように構成された命令を有するプログラムを対象とする。
【００２４】
本発明は、コンピュータ又はマイクロプロセッサにより部分的に又は全体的に読み取り可能な、取出し可能又は不可能な情報記憶手段を対象とする。前記情報記憶手段は、前記方法の複数ステップの各ステップを実行するための前記コンピュータプログラムのコード命令を有している。
【００２５】
本発明は、識別手段を受け入れるように構成されている移動装置の無線近距離通信手段における少なくとも１の機能を実行するための制御装置を対象とする。この装置は、以下の手段を有することを特徴とする。
－少なくとも１の情報要求を前記識別手段に送信するための手段、前記情報要求は前記識別手段の特性情報を少なくとも１つ取得することを目的としている。
－前記識別手段から前記情報要求に対する応答を受信するための手段、前記応答は前記識別カードの特性情報の少なくとも一つを含む。
－前記応答を認証するための手段；及び
－前記識別カードの特性情報の少なくとも１つに応答する少なくとも一つの機能を実行するための手段。
【００２６】
本発明の装置は、識別カードの特性に基づいて、無線近距離通信モジュールにおける複数機能の実行を許可する又は拒否する。特に、機能の許可又は拒否は、前記識別カードを発行するオペレータに関係させることができる。
【００２７】
１の特定の実施例において、前記移動装置は前記認証手段から切り離されたマイクロプロセッサを有する。なお、前記マイクロプロセッサのセキュリティ事故は前記装置のセキュリティに影響を与えない。
【００２８】
前記装置は以下ものを有すると有利である。
－少なくとも１の認証要求を受信するための手段；及び

－少なくとも１の機能を実施する前に、前記識別カードの前記少なくとも１の特性情報に応答して、前記認証要求に対する許可を送信するための手段。

【００２９】

この実施例において、複数機能が外部装置に関係する場合、本発明の装置は、識別カードの特性に基づいて、無線近距離通信モジュールにおいて複数機能の実行を許可又は拒否する。特に、この実施例は複数サービスへのアクセスを制御するのに使用される。

【００３０】

前記装置は、更に、前記許可をコード化するコーディング手段又はセキュリティ化するセキュリティ化手段を有し、前記許可が不正プログラムによりシミュレートされないように認証されることが好ましい。

【００３１】

一つの特定の実施例において、前記装置は更に、前記許可をコード化する前記コーディング手段又はセキュリティ化するセキュリティ化手段が使用する認証情報を記憶する記憶手段を有し、前記装置のセキュリティを向上する。前記記憶手段は非揮発性であると有利である。前記記憶手段は、前記応答を認証するためのデータを記憶するように構成されると有利である。

【００３２】

又、一つの特定の実施例において、前記識別手段は、移動電話ネットワークへの加入者の識別カード（例えば、移動電話ユニットでよく使われるＳＩＭカード）を対象とする。

【００３３】

又、一つの特定の実施例において、前記無線近距離通信手段はＩＳＯ14443基準に準拠している。

【００３４】

又、一つの特定の実施例において、前記無線近距離通信手段は前記移動装置に取出しができないように一体化されている。

【００３５】

本発明の他の長所、目的、特徴は、図面を参照しつつ、非限定的な実施例を使った以下の詳細な説明から明らかである。

【図面の簡単な説明】

【００３６】

【図１】図１ａと図１ｂからなる。無線近距離通信のための集積回路カードの１つの例である。

【図２】図２ａと図２ｂからなる。移動電話アプリケーションのための集積回路カードを使った本発明の実施例である。図１及びＮＦＣモジュールに示されているものと同様である。

【図３】移動電話ユニットにおける本発明の実施例である。

【図４】本発明を実施するためのアルゴリズムの一つを概略的に示した図である。

【発明を実施するための形態】

【００３７】

更に具体的には、本発明は、広域無線通信ネットワーク（例えばＧＭＳ，ＵＭＴＳ）またはＷｉＦｉネットワークのようなＬＡＮを介して通信することができる移動装置（例えば、移動電話ユニットのような）の使用に関する。本発明は他の移動装置（例えばＰＤＡのような装置）を使って実施することができる。本発明によると、移動装置は、無線近距離通信手段（例えば、１ｍ、５０ｃｍまたは２０ｃｍ以内）及び、ＳＩＭカードのような無線通信ネットワーク識別モジュールを備えている。

【００３８】

本発明は、移動装置に組み込むことができる、新規な無線近距離通信技術を利用する。例えば、ＮＦＣ(Near Field Communnication)技術は、識別、データ交換、支払いアプリケーションに対し無線近距離通信手段を提供する。一般的に13.56ＭＨｚの周波数で動作し、424 KBits/s迄のデータ転送率を可能にして、ＮＦＣ技術は、簡単で信頼性の高い電子

装置間のデータ通信を提案する。

【００３９】

本発明によると、この無線近距離通信手段は１つのコントローラを備えている。このコントローラのアクセスは、(複数)移動電話ユニットにインストールされているプロセッサ及びオペレーティングシステムに比べて、より制限され、より安定である。それらはソフトウェアをインストールし、メモリにアクセスする可能性を提供する。これは本発明により実施され、無線近距離通信手段の部分的、全体的なブロッキング、アンブロッキング機能を確実にし、攻撃に対し抵抗力を高める。また、これら通信手段及び/又は提案される所定のサービスへのアクセスにおける所定機能の実行を許可又は禁止するために、これら手段が通信するのを、特定のオペレータのＳＩＭカードがある時しか許可しない。

【００４０】

これら無線近距離通信手段は、マイクロ回路カードの形態であることができ、本体に又は離れてアンテナを備えている。このカードは取り出し可能である。別の形態として、これら無線近距離通信手段は、アンテナを持つ印刷回路の上に搭載されるマイクロ回路のような、電話器本体に固定されたモジュールの形態を取ることができる。又は、プラスチックの中に埋め込まれた回路とアンテナのようなモジュールの形態をとってもよい。このモジュールは取り出すことはできない。

【００４１】

第１実施例によると、これら無線近距離通信手段は、例えば、マイクロ回路を持った、プラスチック材料のようにかなり硬い本体および、マイクロ回路に接続しているアンテナを有する柔軟性フィルムを備えている。フィルムによって担持されるそのアンテナは、少なくとも部分的に本体を越えて延びている。この装置を組み込むように構成される電子エンティティの例は、例えば、ＩＤ-000フォーマットのミニカードである。それらはマイクロチップカードであることができる。即ち、ＩＳＯ7816に準拠したマイクロ回路カードである。その厚みは約0.76ｍｍであり、セキュリティ化されたマイクロコントローラを有している。

【００４２】

又、フォーマットＭＭＣ(MultiMedia Card)，フォーマットＲＳ-ＭＭＣ (Reduced-Size MultiMedia Card)又はフォーマットＵＩＣＣ (Universal Integrated Circuit Card)のような別のフォーマットに準拠するカードであってもよい。

【００４３】

マイクロ回路カードを使って、ＩＳＯ14443標準規格に準拠して、約13.56ＭＨｚで通信することが好ましい。

【００４４】

図１は図１ａと図１ｂとからなる。図１には、無線近距離通信手段用のマイクロカードの１例が示されている。図１ａはマイクロカードの上面図、図１ｂはラインＡ－Ａにおける切断面の図である。

【００４５】

このカードは、かなり固いカード本体105と柔らかいフィルム110を有している。該フィルムの上には、アンテナ120が設けられている。マイクロ回路115はカード本体105に組み込まれている。回路115は、例えば、セキュリティ化された通信マイクロプロセッサ並びにプログラムとコード化キーを記憶するメモリを備えている。１つの実施例では、回路115は、“接続されている移動電話ユニットとデータ交換のための接触型通信手段（moyens de communication par contact）”および“外部電子装置とデータ交換のための非接触型通信手段（moyens de communication sans contact）”を有している。

【００４６】

フィルム110は、３つの部分を有することが好ましい。即ち、回路115とアンテナ120との間のコンタクトを確立するために本体に接続されている第１部分、カード本体105にアンテナ120を接続するために使われる２つの線路125を含む第２部分、ブリッジ130を含むアンテナ120を支持するために使われる第３部分である。

【００４７】
図１ｂに示されているように、カード本体105はコネクタ135に接続されている回路115を含んでいる。このコネクタ135はカード本体105の表面に露出している。これにより、該移動装置にカードが挿入されるときに、移動装置と電気的に接続することができる。回路115は、フィルム110の導電線路に接続している。アンテナ120は絶縁層140により保護されることが好ましい。前記保護層は、所定の位置に基づいてアンテナ120を圧力で維持するように構成される装置を形成する。フィルム110は、ナイロン、ＰＶＣ（即ち柔軟で抵抗性がある材料）のようなプラスチック部材であることが好ましい。
【００４８】
図２ａは、図１に示されたものと類似の無線近距離通信カードを使用する例が示されている。移動電話ユニット本体200には、３つの空洞があり、マイクロ回路カード（例えば、標準規格ＳＩＭカード）、無線近距離通信カード及びバッテリーを収容している。３空洞はカバー205により保護されている。マイクロ回路カード210を受け入れる空洞部分はコネクタを有することが好ましい。これにより、マイクロ回路が配置されるときに、電話とマイクロ回路カードとの間の電気的接続が成立する。マイクロ回路カードは標準規格的ロックシステム(図示しない)で維持してもよい。同様に、無線近距離通信カード105を収容する空洞にもコネクタがあり、カード105が配置されるときに、電話機とカードとの間に電気的接続が成立する。前記カード105は標準的ロックシステム(図示しない)で維持してもよい。従って、カード本体105が空洞に配置される時に、電話機と回路115とは電気的に接続される。フィルム110はバッテリー215に沿って配置されることが好ましい。その結果、図に示すように、アンテナ120をバッテリー215とカバー205との間に配置することができる。
【００４９】
バッテリー215とカバー205との間にアンテナ120を配置することにより、電話機本体200及びバッテリー215に関係する寄生効果を制限し、回路115は無接触で送受信機と、データを交換することができる。
【００５０】
更に、図２ｂに示す第２実施例では、無線近距離通信モジュール220を図２ａのカード100の代わりに使うことができる。モジュール220は、電話機本体200に接続する部品が組み込まれているカード100と同一の要素を具備することができる。前記モジュール220は機械的に又は溶接で接続されてもよい。その場合、モジュール220は、通常は、取り出し可能ではない。
【００５１】
以下の説明において、無線近距離通信モジュールは、区別することなく、モジュール220またはカード100（これらは同様なものである）の特性を持つカード又は部品を意味する。
【００５２】
図３は移動電話ユニット300において本発明の実施例を示す。図示されているように、移動電話ユニットは、移動電話で使われているアプリケーション、又は、ＰＩＭ(personal information manager)タイプ又はゲームのアプリケーションを実施するためのメインマイクロプロセッサ305を有している。
【００５３】
移動電話ユニット300は、又、ＳＩＭカード310のような識別カードを有している。識別カード310は、この例では、標準的なＳＩＭカードであって、マイクロプロセッサ315（好ましくはセキュリティ化マイクロプロセッサ）とメモリ320を有している。メモリ320は、例えば、機能、サービスのリスト並びに機能、サービスの利用制限を含むテーブル325を格納するように構成されている。又、メモリ320は、データにサインするための暗号化キーを格納している。その結果、サインされたデータを解析することにより、これらデータのソースを認証することができる。識別カード310はマイクロプロセッサ305に接続されており、マイクロプロセッサ305と315との間のデータ交換を可能にする。

【００５４】
移動電話ユニット300は、又、無線近距離通信モジュール335を含む。このモジュール335は、通信マイクロプロセッサ340を有している。この通信マイクロプロセッサ340はセキュリティ化されていると有利であり、それが標準規格ＩＳＯ14443に準拠することが好ましい。モジュール335は、メモリ345を有している。該メモリ345は、プログラム350、並びに例えば暗号化の２つのキー355と360を格納するように構成されている。第１キー355は、識別カード310のメモリ320に含まれるキー330を使って、データのサインを認証するのに使用される。第２キー360を使ってカード335がデータ（該データのソースは認証されることができるものである）にサインすることができる。モジュール335はアンテナ365を有している。これによりモジュール335は外部へデータを送信し、外部からのデータを受信することができる。説明のために、アンテナ365はモジュール335の外側に示している。モジュール335はマイクロプロセッサ305に接続されており、マイクロプロセッサ305と340との間のデータの交換を可能にしている。

【００５５】
データを送受信するために、モジュール335に接続されているアンテナ365は、アンテナ375を備える電子装置370に近距離に配置する必要がある。該アンテナ375は、移動電話ユニット300のモジュール335にデータを送信したり、モジュールからデータを受信するように構成されている。

【００５６】
有利な実施例によれば、無線近距離通信モジュール335と識別カード310との間の通信は、モジュールとカードによりセキュリティ化される（例えば、暗号化により）。前記通信では、当業者に公知の方法が使われ、交換されたコマンドの解析とシミュレーションを回避する。この方法は、例えば、暗号化され、サインされた、メッセージカウントメカニズムを含むメッセージを使うことができる。無線近距離通信モジュール335と識別カード310との間の通信は、無線通信であってもよい点に留意すべきである。

【００５７】
一例として、電子装置370は、例えば、電車または航空機のような輸送手段、ホテルの部屋、プールまたは劇場に対するアクセスを制御する装置である。電子装置370は、例えば、ゲームのようなアプリケーションの一時的な又は非一時的利用を許可するように、又はコンテンツ（マルチメディアのコンテンツのような）のダウンロードを許可するように構成されている。

【００５８】
図４は、図３に示される装置を使って本発明を実施するアルゴリズムの一例を概略的に表している。該アルゴリズムは識別カードの特性に基づいてサービスにアクセスするためのものである。この実施例では、特に、例えば、自動販売機から映画館の席、電車の切符を購入し、その支払いは電話口座で引き落すことができる。

【００５９】
図４に示されているアルゴリズムの左側の(複数)ステップは、サービス提供者のステップである。右側のステップは、移動電話ユニットに関係するものである。

【００６０】
移動電話ユニットの存在を検知すると、電子装置370は信号を送信し、無線近距離通信モジュール335（Moycomという）をアクティブ状態(動作可能状態)にする（ステップ405）。このアクティブ化は特に、モジュール335に電源を供給することにより行われる。前記アクティブ化信号は、例えば標準規格14443に準拠するものである。前記アクティブ化信号が送信されたときに、電子装置370と前記モジュール335との間の通信が開始されることが好ましい。

【００６１】
電子装置370は、１又は複数のサービス（Ｓと呼ぶ）に対するアクセスを提供する。このために、電子装置370は認証要求（requete d'authentification：ＲＡ１という）を送信する。これには、サービスＳへのアクセスの認証を得るために、要求識別子が含まれてお

り、更に、提供されるサービスの識別子が含まれていることが好ましい。

【００６２】

移動電話ユニット300の無線近距離通信モジュール335は認証要求ＲＡ１を受け取り、その性質（nature)を決定し、例えば、提供されるサービスが移動電話ユニット300により実施されるかを決める。実施される場合には、モジュール335は情報要求（ＲＡ２と呼ぶ）をマイクロプロセッサ305（MainProc）に送信する(ステップ415)。要求ＲＡ２の目的は、提供されるサービスを利用する識別カード310の許可を得ること、又は、これらサービスに対するアクセスが禁止されているかを決定することである。例えば、前記要求ＲＡ２は提供されるサービスの識別子を含んでおり、代わりに、許可又は禁止を得る。別の例として、要求ＲＡ２は識別カードの識別子の簡易要求を含み、前記モジュール335が、前記識別カードの識別子に基づいて、提供されるサービス（複数）へのアクセスが許可されるか否かを決定できるようにすることができる。前記マイクロプロセッサ305が認証要求ＲＡ２を受取ると、それをＳＩＭと呼ばれる識別カード310に送信する（ステップ420）。又、前記マイクロプロセッサ305は、電話機の表示部にメッセージを表示する、又は音響又は視覚信号を送信し、例えばユーザが認証コードを入力しなければならないことを知らせることができる。

【００６３】

認証要求ＲＡ２を受け取った後で、識別カード310は、提供されるサービスの識別子を前記テーブル325に予め記憶されている情報と比較して、認証要求されたサービスへのアクセスが許可されるかを確める(ステップ425)。提供されるサービスの識別子は、１のサービスに、関係するサービスの組に、又は、アクセスがケースバイケースで許可される又は拒否されるサービスの組に、関係することができることに注意すべきである。従って、一つの識別子であるのか又は識別子の１組であるのかが問題になる。例えば、前記テーブル325は、許可されたサービスの識別子のリスト及び拒否されたサービスの識別子のリストを含むことができる。サービスに対するアクセスが許可されない場合、要求は拒否される。この場合、識別カードは、（図示のように）メッセージを戻すことはできない。又は拒否のマークを付けてメッセージを戻す。

【００６４】

サービスに対するアクセスが許可される場合、識別カードは受理メッセージ（ＲＳ２と呼ぶ）を移動電話ユニット300のマイクロプロセッサ305に送り返す(ステップ430)。受理メッセージは330に記憶されているキーを使ってサインすることが好ましい。該メッセージが“不正プログラムがインストールされているマイクロプロセッサ305”によりシミュレートされないようにするためである。サインされた受理メッセージＲＳ１を受け取ると、前記マイクロプロセッサ305はそれをモジュール335に送る（ステップ435）。ユーザが認証コードを入力した場合、このコードは同様にモジュール335に送られる。別の例では、要求ＲＡ２を受け取ると、識別カード310は、サインして、１又は複数の特性（caracteristiques）を送り返すことができる。前記モジュール335が、提供される複数サービスにアクセスする又はアクセスしないという許可を決定できるようにするためである。この変形例は破線で示されている。

【００６５】

サインされた受理メッセージＲＳ２が受信されると（ステップ440）、前記モジュール335は、例えば355に記憶されたキーを使ってサイン済み受理メッセージＲＳ２の発信元を確認する（ステップ445）。330と355に記憶されたキー（複数）との関係は、次のようなものである。即ち、或るメッセージが330に記憶されたキーを使ってサインされる場合、355に記憶されたキーを使って、前記メッセージは確かに330に記憶されたキーによりサインされたものであることを証明することができる。このアルゴリズム、特にアルゴリズムＲＳＡ(Rivest Shamir Adleman) は当業者に公知である。このタイプのアルゴリズムを使うと、330に記憶されたキーはプライベートキーで、対応する355に記憶されたキーは公開キーである。

【００６６】

サイン済み受理メッセージＲＳ２のソースが確認できない場合、前記要求は拒否される。この場合再び、前記モジュール335はメッセージを送り返すことはできない（図示のように）。又は拒否のマークを付けてメッセージを戻す。

【００６７】

サイン済み受理メッセージＲＳ２のソースが確認されると、前記要求は受け付けられる。前記モジュール335は、360に記憶されたキーを使った認証メッセージＲＳ１を電子装置370に送信し（ステップ450）、真正であることが認証される。360に記憶されたキーはプライベートキーであることが好ましい。

【００６８】

別の変形例として、前記メッセージＲＳ２が認証され、識別カード310が持つ情報を含む場合、前記モジュール335はこれら情報を使って提供される(複数)サービスにアクセスできるかを決定する。再度、前記モジュールが前記提供されるサービスにアクセスできる場合、前記モジュール335は、360に記憶されたキーを使った認証メッセージＲＳ１を電子装置370に送信し、電子装置はモジュール335が真正であることを認証することができる。

【００６９】

認証メッセージＲＳ１を受信すると、前記電子装置370は、前記と同様なメカニズムを使って（例えば、360に記憶されているプライベートキーに対応する公開キーを使って）、前記認証メッセージの発信元を確認する。認証メッセージＲＳ１が確認されると、前記電子装置370はサービスＳへのアクセスを移動電話ユニット300に与える(ステップ460)。こうして、前記移動電話ユニット300は(複数)サービスＳを使うことができる。

【００７０】

識別カードに記憶されているプライベート暗号化キーは、複数の識別カードに共通であってよい。具体的には、各オペレータは１又は複数のプリベート暗号化キーを使用することができる。これにより、例えば、予約に従って、予約者に対し許可、拒絶することができる。

【００７１】

キーによる認証システムが本発明の実施例において使用される場合、本発明は本認証モードに限定されるものではない。

【００７２】

特定の実施例によれば、前記移動電話ユニット300のマイクロプロセッサ305は移動通信網を介して、プログラムを受信することができる。又、アップデートされたプログラムは、前記無線近距離通信モジュール335のメモリ350に記憶されねばならない。この実施例によると、前記モジュール335はプログラムをメモリに記憶する又はプログラムをアップデートすることは、識別カード310の許可がなければ、行わない。許可のメカニズムは、前記のものと同様である（特にステップ415乃至445を参照）。この実施例によれば、許可はメモリ機能に関係するが、提供されるサービスへのアクセスに関係しない。

【００７３】

また、特定の実施例によれば、前記無線近距離通信モジュール335は動作状態になった後、前記電子エンティティ370と通信を開始する前に前記識別カード310に許可を要求する。また、この許可メカニズムは前記のアルゴリズムと同様である（特にステップ415乃至445を参照）。

【００７４】

前記モジュール335は少なくとも部分的にセキュリティ化されていると有利である。このセキュリティ化は特に規格FIPS (Federal Information Processing Standards)又は共通の規格により定められている。

【００７５】

もちろん、特定の必要性を満たすために、本発明の当業者は前記説明において変更を加えることができる。

【図１】

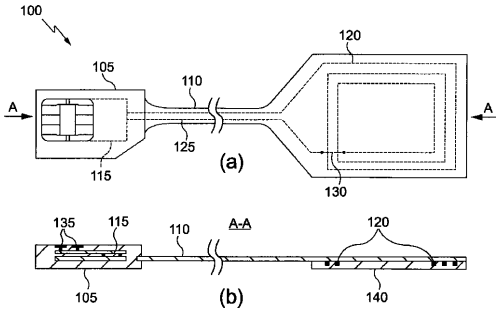


Fig. 1

【図２】

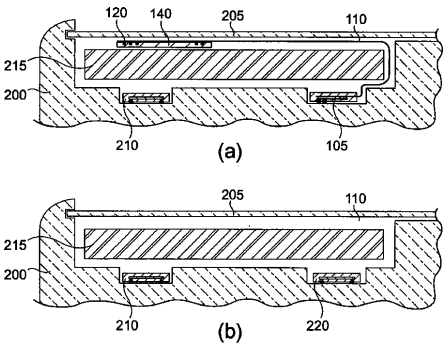


Fig. 2

【図３】

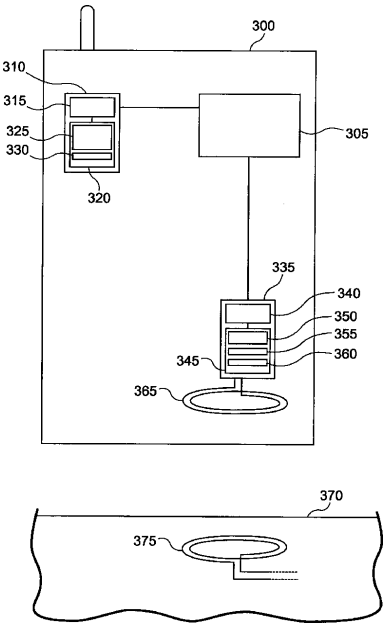


Fig. 3

【図４】

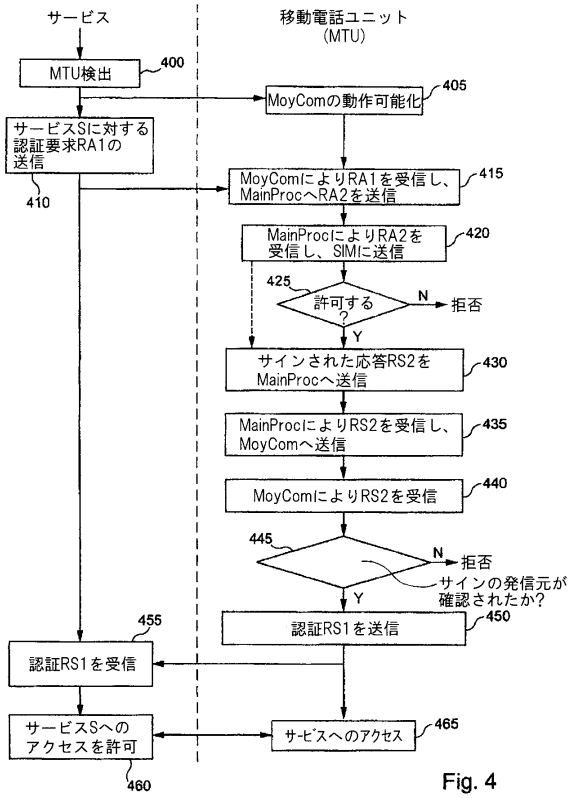


Fig. 4

フロントページの続き

(72)発明者　ベルタン，マルク
フランス国，エフ－７８７２０　ラ　セル　レ　ボルド，リュ　デュ　ムーラン　ドゥ　ベシュロー，３３

審査官　松元　伸次

(56)参考文献　特開２００３－１８９３５７（ＪＰ，Ａ）
国際公開第２００６／１１７００９（WO，Ａ１）
特開２００４－０９４５３９（ＪＰ，Ａ）
特開２００３－１０１６７９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/00、21/20、
G09C 1/00- 5/00、
H04B 7/24- 7/26、
H04K 1/00- 3/00、
H04L 9/00- 9/38、
H04M 1/00- 3/00、 3/16- 3/20、
3/38- 3/58、 7/00- 7/16、
11/00-11/10、99/00、
H04W 4/00-99/00