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

特許第4635244号
(P4635244)

(45)発行日　平成23年2月23日(2011.2.23)　(24)登録日　平成22年12月3日(2010.12.3)

(51)Int.Cl.　　F I
*G06K 17/00 (2006.01)*　　G06K 17/00 C
*G06K 19/07 (2006.01)*　　G06K 17/00 D
　　G06K 19/00 N

請求項の数 16　(全 17 頁)

(21)出願番号　特願2001-502080 (P2001-502080)
(86)(22)出願日　平成12年5月12日 (2000.5.12)
(65)公表番号　特表2003-501759 (P2003-501759A)
(43)公表日　平成15年1月14日 (2003.1.14)
(86)国際出願番号　PCT/FR2000/001285
(87)国際公開番号　WO2000/075883
(87)国際公開日　平成12年12月14日 (2000.12.14)
審査請求日　平成19年4月21日 (2007.4.21)
(31)優先権主張番号　99/07059
(32)優先日　平成11年6月3日 (1999.6.3)
(33)優先権主張国　フランス(FR)

(73)特許権者　509069331
ジェマルト　エスアー
ＧＥＭＡＬＴＯ　Ｓ．Ａ．
フランス共和国，９２１９０　ムードン，リュ　ドゥ　ラ　ヴェルリ，６
(74)代理人　100080447
弁理士　太田　恵一
(72)発明者　バスカン，ブリュノ
フランス共和国，エフ－１３００８　マルセイユ，ブルヴァール　ドゥ　ラ　グロット　ロラン，１３２

審査官　大塚　良平

最終頁に続く

(54)【発明の名称】端末の追加のチップカード内に保存されたプログラムの事前検査方法

(57)【特許請求の範囲】
【請求項１】
端末（ＴＥ）が接続された遠隔通信網（ＲＲ）に関連するデータを保存する第一のチップカード（Ｃ１）に加えて、端末（ＴＥ）内に挿入された第二のチップカード（Ｃ２）に保存されたプログラムの実行を事前に検査する方法であって、
第一のチップカードは端末内に含まれ、
端末、第一のチップカード、および第二のチップカードは、少なくとも一つのマイクロプロセッサと、少なくとも一つのメモリを備えており、
端末は第一のチップカード及び第二のチップカードとの入出力インターフェースを備えており、
該方法が以下の過程を含むことを特徴とする方法。
－第二のチップカードが第一のチップカードを認証し、および／または、
－第一のチップカードが第二のチップカードを認証し、
第二のチップカード及び第一のチップカードによる、第一のチップカードと第二のチップカード（Ｃ１，Ｃ２）のうち少なくとも一つの認証の成功が、それぞれ、プログラムの実行の条件となる。
【請求項２】
認証が、第一のチップカード（Ｃ１）による第二のチップカード（Ｃ２）の認証（Ａ１）を有しており、以下の過程を含むことを特徴とする、請求項１に記載の方法。
－第二のチップカードが第一のチップカードに伝送するプログラムの識別子（ＩＰＡ）と

鍵（Ｋａ）とを、第一のチップカードに保存されたアルゴリズム（ＡＡ１ａ）に適用して（Ａ１２１）、結果（Ｒ１）を生成し、
－結果（Ｒ１）と、第二のチップカードが第一のチップカードに伝送する証明書（ＣＥＲＴ）とを比較（Ａ１２３）して、結果が証明書と一致した場合にのみ、プログラムの実行を第一のチップカード、第二のチップカード、または端末が行う。
【請求項３】
認証が、第二のチップカードから第一のチップカードへと伝送されるプログラムの識別子（ＩＰＡ）に応じて、第一のチップカード（Ｃ１）に保存された鍵テーブル（ＴＫａ）から鍵（Ｋａ）を選定（Ａ１２０）することを含み、
前記プログラムの識別子と選定された鍵とが認証アルゴリズムに適用されて、
第一のチップカード内に保存された証明書と比較されるためのものである結果（Ｒ１）を生成することを特徴とする、請求項１に記載の方法。
【請求項４】
認証が、第一のチップカード（Ｃ１）による第二のチップカード（Ｃ２）の認証（Ａ１）を有しており、以下の過程を含むことを特徴とする、請求項１に記載の方法。
－第一のチップカード（Ｃ１）から第二のチップカード（Ｃ２）に乱数（ＮＡ１）を伝送し（Ａ１２４）、
－第二のチップカードに保存されたアルゴリズム（ＡＡ１ｂ）に、伝送された乱数と鍵（Ｋｂ）とを適用して（Ａ１２５，Ａ１２６）、第一のチップカード（Ｃ１）に伝送する署名（ＳＧ２）を生成し、
－第一のチップカード内に保存されたアルゴリズム（ＡＡ１ｂ）に、乱数と鍵（Ｋｂ）とを適用して（Ａ１２８）、結果（Ｒ２）を生成し、
－その結果を、第一のチップカードに伝送された署名と比較（Ａ１２９）して、結果が署名と一致した場合にのみ、プログラムの実行を第一のチップカード、第二のチップカード、または端末が行う。
【請求項５】
認証は、第二のチップカードが第一のチップカードに伝送したプログラムの識別子（ＩＰＡ）に応じて、第一のチップカード（Ｃ１）に保存された鍵テーブル（ＴＫｂ）から鍵（Ｋｂ）を選定すること（Ａ１２７）を含むことを特徴とする、請求項４に記載の方法。
【請求項６】
認証が、第二のチップカード（Ｃ２）による第一のチップカード（Ｃ１）の認証（Ａ２）を有する場合に、以下の過程を含むことを特徴とする、請求項１に記載の方法。
－第一のチップカード（Ｃ１）から第二のチップカードに番号（ＩＭＳＩ）の所定のフィールド（ＭＮＣ）を伝送し（Ａ２２０）、
－第二のチップカード内に保存された番号（ＭＮＣ２）と前記所定のフィールド（ＭＮＣ）を比較し（Ａ２２２）、前記所定のフィールドが該番号と一致した場合にのみ、プログラムを実行する。
【請求項７】
所定のフィールドが、少なくとも第一のチップカードの識別番号（ＩＭＳＩ）に保存された遠隔通信網（ＲＲ）の識別符号（ＭＮＣ）を含むことを特徴とする、請求項６に記載の方法。
【請求項８】
認証が、第二のチップカード（Ｃ２）による第一のチップカード（Ｃ１）の認証（Ａ２）を有する場合に、以下の過程を含むことを特徴とする、請求項１に記載の方法。
－第一のチップカード（Ｃ１）から第二のチップカード（Ｃ２）に乱数（ＮＡ２）を読み込み（Ａ２２３，Ａ２２４）、
－第一のチップカードに保存されたアルゴリズム（ＡＡ２）に、乱数と鍵（Ｃ）とを適用し（Ａ２２６）、第二のチップカード（Ｃ２）に伝送される署名（ＳＧ３）を生成し、
－第二のチップカードに保存されたアルゴリズム（ＡＡ２）に、乱数（ＮＡ２）と鍵（Ｃ）とを適用して（Ａ２２８）、結果（Ｒ３）を生成し、

－その結果を、第二のチップカードに伝送される署名と比較し（Ａ２２９）、結果が署名と一致した場合にのみ、プログラムを第一のチップカード、第二のチップカード、または端末が実行する。

【請求項９】

認証は、第二のチップカードが第一のチップカードに伝送したプログラムの識別子（ＩＰＡ）に応じて、第一のチップカード（Ｃ１）に保存された鍵テーブル（ＴＣ）から鍵（Ｃ）を選定（Ａ２２５）することを含むことを特徴とする、請求項８に記載の方法。

【請求項１０】

第一のチップカード（Ｃ１）による第二のチップカード（Ｃ２）の第一認証（Ａ１）と第二のチップカードによる第一のチップカードの第二認証（Ａ２）とを含み、該第二認証は、第二のチップカードが第一のチップカードによって認証されたら、第一認証に続いて行われ、該第二認証の後で、第一のチップカードが第二のチップカードによって認証されたら、プログラムが実行されるか、あるいは、

第二のチップカード（Ｃ２）による第一のチップカード（Ｃ１）の第一認証（Ａ２）と第一のチップカードによる第二のチップカードの第二認証（Ａ１）とを含み、該第二認証は、第一のチップカードが第二のチップカードによって認証されたら、第一認証に続いて行われ、該第二認証の後で、第二のチップカードが第一のチップカードによって認証されたら、プログラムが実行され、

該プログラムの実行は、第一のチップカード、第二のチップカード、または端末が行うことを特徴とする、請求項１から９のいずれか一つに記載の方法。

【請求項１１】

第二のチップカード（Ｃ２）から第一のチップカード（Ｃ１）に伝送される認証要求（ＤＡ１；ＤＡ２）の応答としてのみ、第二のチップカードによる第一のチップカードの認証、または、一方のチップカードの他方のチップカードによる相互認証（Ａ１，Ａ２；Ａ２）が実行されることを特徴とする、請求項１から１０のいずれか一つに記載の方法。

【請求項１２】

第一のチップカード及び第二のチップカードのうち少なくとも一つの認証（Ａ１，Ａ２）とプログラムの実行（Ｅ５）との間で、第二のチップカード（Ｃ２）から第一のチップカード（Ｃ１）にプログラム（ＰＡ）を遠隔ロードし（Ｅ５）、第一のチップカード（Ｃ１）によってプログラムを実行する（Ｅ５）ことを含み、

第一のチップカードが遠隔ロード及びプログラムの実行を制御することを特徴とする、請求項１から１１のいずれか一つに記載の方法。

【請求項１３】

プログラムは、第一のチップカード（Ｃ１）のコマンドの下で起動（Ｅ５）され、第二のチップカード（Ｃ２）によって実行され、コマンドと応答の交換を、第二のチップカード（Ｃ２）と端末（ＴＥ）との間で、直接、または第一のチップカード（Ｃ１）を介して行い、

該交換が第二のチップカード（Ｃ２）と端末（ＴＥ）との間で直接行なわれる場合には、第一のチップカード（Ｃ１）は、該交換の主導権を端末（ＴＥ）に委ねることを特徴とする、請求項１から１１のいずれか一つに記載の方法。

【請求項１４】

チップカードの認証（Ａ１，Ａ２）とプログラムの実行（Ｅ５）との間で、第二のチップカード（Ｃ２）から端末（ＴＥ）にプログラム（ＰＡ）を遠隔ロードし、端末によってプログラムを実行する（Ｅ５）ことを含み、

端末が遠隔ロード及びプログラムの実行を制御することを特徴とする、請求項１から１１のいずれか一つに記載の方法。

【請求項１５】

遠隔通信網は無線電話網（ＲＲ）であり、端末は移動無線電話端末（ＴＥ）であり、第一のチップカードは加入者の身元識別カード（Ｃ１）であることを特徴とする、請求項１から１４のいずれか一つに記載の方法。

【請求項１６】
端末（ＴＥ）が接続された遠隔通信網（ＲＲ）に関連するデータを保存する第一のチップカード（Ｃ１）に加えて、端末（ＴＥ）内に挿入された第二のチップカード（Ｃ２）に保存されたプログラムの実行を事前に検査するためのシステムであって、
第一のチップカードは端末内に含まれ、
端末、第一のチップカード、および第二のチップカードは、少なくとも一つのマイクロプロセッサと、少なくとも一つのメモリを備えており、
端末は第一のチップカード及び第二のチップカードとの入出力インターフェースを備えており、
－第一のチップカードを認証する為の手段を第二のチップカードが備え、および／または、第二のチップカードを認証する為の手段を第一のチップカードが備え、
第二のチップカード及び第一のチップカードによる、第一のチップカードと第二のチップカード（Ｃ１、Ｃ２）のうち少なくとも一つの認証の成功が、それぞれ、プログラムの実行の条件となることを特徴とするシステム。
【発明の詳細な説明】
【０００１】
本発明は、遠隔通信端末内に挿入可能な追加のチップカードによって供給されるアプリケーション・プログラムの安全化に関するものである。特に、端末は移動無線電話端末であり、該端末には、加入者の識別と遠隔通信網との通信の為の第一カードのみならず、追加のチップカードの読取り装置が含まれている。
【０００２】
ＧＳＭタイプのセルラー無線電話網では、ＳＩＭのチップカード内のアプリケーション・プログラムを実行することに基づくアプリケーション・サービスを、加入者に提供することが準備されている。これらのサービスを活用する技術は規格化されたものであり、一般にＳＩＭアプリケーション・ツールキットと呼ばれている。特に前もったアクティブ化と呼ばれる機能により、ＳＩＭカードは、一つのプログラムのラン中にも、外界、つまり端末、加入者、及びネットワークに要求を出すことが可能になる。
【０００３】
例えば、そのようなアプリケーション・プログラムには、銀行サーバーに問い合わせ、端末から銀行取引を遠隔操作する為のメニューが含まれている。付加価値サービスのアプリケーション開発をＳＩＭカード内で実行する為には、使用契約の進行中に、これらのアプリケーションを配付し保守する手段が必要となる。それは、ＳＩＭカードを、加入者に交付する前に、適切なプログラムで個人化したり、または無線手段によって遠隔ロードしたり、あるいは、販売時点で、ＳＩＭカードにこれらのプログラムを直接ロードすることで可能になる。
【０００４】
先行技術は追加のチップカードも備えており、該カードは、ＳＩＭカードとは別のものであって、端末に挿入可能であるか、あるいは外部の読取り装置によってＳＩＭカードの端末に接続することができるものである。第二カードは、ＳＩＭカード内で実行されるプログラムによって制御される。端末が演じる役割は透化的なものであり、ＳＩＭカードによって生成されたコマンドを第二カードに向けて伝送するだけのものである。コマンドのこの交換は、あらゆるタイプのチップカードを活用するサービスを開発することを目指すものである。例えば、第二カードは、銀行カードであり、移動端末上で遠隔支払のサービスを提供する。
【０００５】
第二カードは、アプリケーションの配布手段となるものであり、実際にＳＩＭカードの中に見いだせるような、付加価値のあるサービスを実現するプログラムを運ぶものである。
【０００６】
第二カードを端末に挿入する際の欠点は、アプリケーションを提供しているのが、もはや必ずしも、ネットワーク・オペレータではないので、その真正性についての一切の検査か

ら免れるということである。第二カードには、端末、第一カード、またはネットワークによって、その内容を証明するための手段が一切含まれていない。

【０００７】

本発明の目的は、一枚の追加カードに保存され、特に端末の第一カードあるいはその端末自体によって実行可能となるアプリケーションの、使用前及び使用中での安全性を強化することである。

【０００８】

その目的の為に、端末の接続先の遠隔通信網に関連するデータを保存する第一のチップカードに加えて、端末内に挿入される第二のチップカードに保存されたプログラムの実行を事前検査する手段は、プログラムの実行前、並びに実行中に、第一及び第二カードの一方を他方で認証することを含むことを特徴とする。

【０００９】

従って、認証により、第二カード内の一つまたは複数のアプリケーション・プログラムの不正使用、ハッキング、そして複製から防止される。

【００１０】

本発明においては、第二のチップカードは、様々なアプリケーション・プログラムを保存する複数の追加カードの中のいずれかの任意の一枚のカードであって、第二カードによる一つまたは複数のプログラムに基づいて、第二カードと、第一カードと、端末との間の通信ソフト手段に依存しないものである。

【００１１】

第二カードが複数あることにより、オペレータは、自分の加入者に対して、新しいサービスを提案することができ、該サービスは、提案されたサービスの検査を管理しながら、端末に挿入する第二カードの形で、従来の流通経路を通じて行われるものである。

【００１２】

第一の実施様態によると、第一カードにより第二カードを認証することが認証に含まれる場合は、以下の過程を含むことができる：

－第二カードによって伝送されるプログラムの識別子を第一カードに割り当て、第一カードに保存されたアルゴリズムに一つの鍵を割り当てることにより、一つの結果を生成し、そして、

－結果と、第二カードが第一カードに伝送した証明書とを比較して、両者が一致した場合にのみ、プログラムを実行する。

【００１３】

その場合、認証には、プログラムの識別子に応じて、第一カードに保存され鍵テーブルの中から鍵を選択することを含んでもよい。

【００１４】

第二の実施様態によると、第一カードにより第二カードを認証することが認証に含まれる場合は、以下の過程を含むことができる：

－第一カードから第二カードに乱数を伝送し、

－伝送された乱数と一つの鍵を、第二カードに保存されたアルゴリズムに適用し、第一カードに伝送される署名を生成し、

－乱数と一つの鍵を、第一カードに保存されたアルゴリズムに適用し、一つの結果を生成し、そして、

－結果と、第一カードに伝送された署名とを比較して、両者が一致した場合にのみ、プログラムを実行する。

【００１５】

その場合、認証には、第二カードから第一カードに伝送されたプログラムの識別子に応じて、第一カードに保存された鍵テーブルの中から鍵を選択することを含んでもよい。

【００１６】

第二カードにより第一カードを認証することが認証に含まれる場合は、第一の実施様態によると、以下の過程を含むことができる：

－一つの番号の所定のフィールドを第一カードから第二カードに向かって伝送し、
－所定のフィールドと第二カード内の一つの番号とを比較して、両者が一致した場合にのみ、プログラムを実行するか、または、その内容を読み込む。

【００１７】
その場合、所定のフィールドには、少なくとも第一カードの識別番号に含まれた遠隔通信網の識別符号を含むことができる。

【００１８】
第二カードにより第一カードを認証することが認証に含まれる場合は、第二の実施様態によると、以下の過程を含むことができる：
－第一カードから第二カードに一つの乱数を読み込み、
－乱数と一つの鍵を、第一カードに保存されている一つのアルゴリズムに適用し、第二カードに伝送される一つの署名を生成し、
－乱数と一つの鍵とを、第二カードに保存されている一つのアルゴリズムに適用し、一つの結果を生成し、そして、
－結果と、第二カードに伝送された署名とを比較することにより、両者が一致した場合にのみ、プログラムを実行するか、または、その内容を読み込む。

【００１９】
その場合、認証には、第二カードから第一カードに伝送されたプログラムの識別子に応じて、第一カードに保存された鍵テーブルの中から鍵を選択することを含んでもよい。

【００２０】
本方法が更に効果を発揮するのは、第一カードと第二カードとの間で相互に認証を行う場合である。

【００２１】
その方法は、第一カードによる第二カードの第一認証と、第二カードによる第一カードの第二認証とが含まれ、該第二認証は、第二カードが第一カードにより認証されるとき、第一認証の後に行われ、そして、第一カードが第二カードにより認証されるとき、該第二認証の後にプログラムが実行されるものである。

【００２２】
あるいは、その方法は、第二カードによる第一カードの第一認証と、第一カードによる第二カードの第二認証とが含まれ、該第二認証は、第一カードが第二カードにより認証されるとき、第一認証の後に行われ、そして、第二カードが第一カードにより認証されるとき、該第二認証の後にプログラムが実行されるものである。

【００２３】
第一カードの必ずしも全てが第二カードにより認証されるべきものではなく、また、第二カードの必ずしも全てが、逆に第一カードにより認証されるべきものではない。特に、認証の少なくとも一部は、第二カードから第一カードに伝送される認証要求への応答としてのみ行われることにしてもよい。

【００２４】
第一カードは、認証に関与する為のハードまたはソフトの手段を含まないことにしてもよい。その場合には、本方法には、第一カードからの要求への応答として遠隔通信網のサーバーで行われる認証の過程を含んでもよい。プログラムの実行は、少なくともその一部を、第一カードか端末か第二カードで行うのなら、これら三つの構成要素の適合性を前もって検証する必要がある。この点については、本方法には、端末に接続された読み取り手段に第二カードを挿入するのに応じて、第二カードでプログラムを実行する為の特性を第一カード端末から読み取り、第一カード及び／又は端末のハードとソフトの容量と比較してその特性を分析し、前記特性が第一カード及び／又は端末と適合性しない場合には第二カードを拒絶することを含んでもよい。

【００２５】
好ましい実施様態においては、遠隔通信網は無線電話網であり、端末は移動無線電話端末であり、第一のチップカードは加入者識別カードである。しかしながら、他の変形として

は、遠隔通信網は、単に交換機付きの電話網であったり、サービスの統合されたデジタル・ネットワークであったり、あるいは、特別なまたは専用のデータ伝送の電話網であってもよい。

【００２６】

本発明の他の特徴と利点は、添付図面を参照しつつ、本発明の望ましい幾つもの実施様態の以下の記述を読むことにより、更に明らかになっていく。

－図１は、セルラー無線電話網のブロック線図に詳細な移動端末を添えたものである。

－図２は、本発明によるプログラム実行の事前検査方法の主要な過程のアルゴリズムである。

－図３は、端末に接続された第一カードと第二カードとの相互認証アルゴリズムである。

－図４は、第一の実施様態に従う第一カードによる第二カードの第一認証アルゴリズムである。

－図５は、第二の実施様態に従う第一カードによる第二カードの第一認証アルゴリズムである。

－図６は、第一の実施様態に従う第二カードによる第一カードの第二認証アルゴリズムである。

－図７は、第二の実施様態に従う第二カードによる第一カードの第二認証アルゴリズムである。

【００２７】

図１に示されたようなＧＳＭタイプのデジタルセルラー電話網ＲＲのようなタイプの遠隔通信網の情況を、例として述べる。無線電話網の移動無線電話端末ＴＥの中には、端末から取り外し可能なマイクロプロセッサ付きモジュールを構成する第一のチップカードＣ１と、追加のアプリケーション・カードと呼ばれる第二のチップカードＣ２があり、該第二カードは、端末とは別のカード読取り装置を介して端末ＴＥに接続されるか、あるいは、端末の中に取り外し可能な状態で収納されている。

【００２８】

図１においては、ネットワークＲＲを概略的に示す為に、移動端末ＴＥがある時点で存在する位置登録区域についての移動サービス交換局ＭＳＣと、基地局ＢＴＳが示され、該基地局は基地局制御装置ＢＳＣによって交換局ＭＳＣに接続されるのは、無線手段によって端末ＴＥに接続されている。構成単位ＭＳＣ、ＢＳＣ、そしてＢＴＳは、主に固定網を構成しており、該固定網を通して伝送されるのは、特に、セマフォチャネルでの信号や、制御信号、データ信号、そして音声信号のメッセージである。端末ＴＥ内の第一カードとインタラクティブに作用することのできるネットワークＲＲの主な構成単位は、移動サービス交換局ＭＳＣであり、それは、ビジターロケーションレジスタＶＬＲに連結されており、かつ交換機付き電話網ＲＴＣの少なくとも一つの自動回線接続電話交換機CAAに接続されている。交換局ＭＳＣは、ビジター移動端末の為の通信を管理するものであるが、それには端末ＴＥも含まれ、交換局ＭＳＣに通じる位置登録区域内に、ある時点で存在するビジター移動端末である。基地局制御装置ＢＳＣが管理するのは、特に、ビジター移動端末へのチャネルの割り当てであり、基地局ＢＴＳは、端末ＭＳがある時点で存在する無線電気セルをカバーしている。

【００２９】

無線電話網ＲＲには、レジスタＶＬＲに接続され、データ・ベースに類似した名簿用のホームロケーションレジスタＨＬＲも含まれている。レジスタＨＬＲには、各無線電話端末ごとに、特にＳＩＭ（加入者識別モジュール）カードと呼ばれる、第一のチップカードＣ１のＩＭＳＩ（インターナショナル・モバイル・サブスクライバー・アイデンティティ）の国際識別があり、それは端末ＴＥの中にあり、それはつまり、ＳＩＭカードを所有する加入者の識別であり、加入者の使用契約のプロフィールであり、移動端末が一時的につながっているレジスタＶＬＲの番号である。

【００３０】

図１に細部の示された端末ＴＥには、無線電話網ＲＲとの無線インターフェース３０があ

り、それを構成している主なものは、送信路と受信路の送受信装置と、周波数変調回路と、アナログ・デジタル及びデジタル・アナログ変換器と、モデムと、チャネル符号化及び復号化回路である。端末ＴＥには更に、マイクロホン３１０とスピーカ３１１に接続された音声符号化・復号化回路３１、プログラムの不揮発性メモリＥＥＰＲＯＭ３３とデータ・メモリＲＡＭ３４につながったマイクロコントローラ３２、それにチップカードＣ１とＣ２、キーボード３６とグラフィック・ディスプレイ３７に通じる入出力インターフェース３５がある。マイクロコントローラー３２は、バスＢＵによって、インターフェース３０と、回路３１と、メモリ３３及び３４とに接続されており、もう一つのバスＢＳによって、入出力インターフェース３５に接続されている。マイクロコントローラ３２は、特にＩＳＯモデルのプロトコル層１、２及び３に関して、端末が受信し、周波数変調した上で送信するベースバンドでのデータ処理の全てを管理し、無線インターフェース３０を通してのネットワークＲＲと、入出力インターフェース３５を通しての第一のチップカードＣ１との間のデータの交換を監視する。

【００３１】

ＳＩＭチップカードＣ１は、端末内に少なくとも一つあるカード読取り装置と、移動端末の周辺機器取り付け口を含んだ、入出力インターフェース３５に接続される。チップカードＣ１に内蔵されているもので主なものは、マイクロプロセッサ１０、カードのオペレーティングシステムおよび通信と、アプリケーションと本発明に特有の認証とのアルゴリズムを含むＲＯＭタイプのメモリ１１、加入者に関連する全ての特性、特に、ＩＭＳＩ加入者の国際識別を保存するＥＥＰＲＯＭタイプの不揮発性メモリ１２、端末と第二カードＣ２の中にあるマイクロプロセッサ３２から受信し、それらを通して伝送するデータの処理を主な目的とするＲＡＭタイプのメモリ１３である。

【００３２】

図１で示されているように、認証サーバーＳＡは、オプションとして、無線電話網ＰＲの内部の構成単位として備えられ、ネットワークＲＲの標識ネットワークを通して、移動サービス交換局ＭＳＣとビジターロケーションレジスタＶＬＲの一つまたは複数の対に接続され、サーバーＳＶのアドレスは、カードＣ１のメモリ１２に予め記憶されている。

【００３３】

本発明によれば、幾つものソフトウェアが原則的にＲＯＭメモリ１１とＥＥＰＲＯＭメモリ１２に遠隔ロードされ、追加カードＣ２内のアプリケーションを管理する。特に、図２に示される本発明の事前検査方法のアルゴリズムは、メモリ１１と１２にインプリメンテーションされる。

【００３４】

ＳＩＭカードＣ１と同様に、第二カードＣ２の中にも、マイクロプロセッサ２０、カードＣ２のオペレーティングシステムと、アプリケーション・プログラムＰＡの少なくとも一部と、本発明に特有の認証アルゴリズムとを含むＲＯＭメモリ２１、本発明によれば、アプリケーション・プログラムの識別子ＩＰＡと、プログラムの実行に必要な特性ＣＰＡと、一つか二つの認証要求ＤＡ１とＤＡ２を保存するＥＥＰＲＯＭタイプの不揮発性メモリ１２、マイクロコントローラ３２とプロセッサ１０とから受信するデータを処理するＲＡＭメモリ１３がある。カードＣ２は、例えば銀行カードであったり、電子財布カードであったり、ゲーム・カード、または名刺であったりする。この最後の場合、名刺は、ＳＩＭカードの電話帳の中に、カードを差し出した人の名前と電話番号を挿入する為、および／または、その人を自動的に呼び出す為のものである。

【００３５】

カードＣ１とＣ２の中のＲＯＭメモリとＥＥＰＲＯＭメモリ１１、１２、２１及び２２の中には通信ソフトウェアがあって、一方では、端末ＴＥのマイクロコントローラ３２と対話し、他方では、端末ＴＥを通して、つまり、マイクロコントローラ３２と入出力インターフェース３６とを通して、プロセッサ１０と２０との間で対話を行う。

【００３６】

それらの間で対話を行うために、ＳＩＭカードＣ１と追加カードＣ２は、予めアクティブ

なタイプのものになっており、ＩＳＯ規格７８１６－３のプロトコル”Ｔ＝０”に従ってプレフォーマットされ、かつＧＳＭ１１．１４（ＳＩＭツールキット）推奨によりカプセル化されたコマンドを使って、移動端末ＭＳの中の作動を起動する。この推奨により、チップカードＣ１，Ｃ２のメモリ１１、２１の中に保存されているオペレーティングシステムのコマンド・セットを拡張して、チップカードＣ１，Ｃ２によって伝送されたデータをもう一つのカードＣ２，Ｃ１で使えるようになっている。後述するように、端末ＴＥは、カードＣ１とＣ２との間の幾つかのデータ交換に対して透化的であるか、または一枚のカードとは通信しないで他のもう一枚と通信することができる。

【００３７】

図２に示されているように、二枚目のカードＣ２に保存されたアプリケーション・プログラムＰＡの実行の事前検査方法は、主な四つの過程Ｅ１からＥ４によって行われる。まず、事前検査方法は、ステップＥ０から開始され、手動で行うなら、端末ＴＥのキーボード上の所定の有効化キーを押すか、または、カードＣ２を読取り装置に挿入した後に端末のスクリーンに表示される「追加カード挿入を有効にする」という指示を有効にして、あるいは、端末ＴＥにより自動的に行うなら、端末ＴＥとは別の、または、カードＣ１のものと同様に、入出力インターフェース３５と一体化した読取り装置によって伝送されるカードが存在するというメッセージに応えて開始される。その時、端末ＴＥは、第一カードＣ１、ＳＩＭカードを第二カードＣ２に問い合わせるよう促す。

【００３８】

図２に示された実施様態によると、以下の過程Ｅ１からＥ４を通して全てが行われるが、それはあたかも、端末ＴＥ、実際にはマイクロコントローラ３２と入出力インターフェース３５が、二枚のカードの間のデータ交換に対して透化的であるように行われる。

【００３９】

以下の過程Ｅ１で、カードＣ１は、端末ＴＥを通して、カードＣ２のＥＥＰＲＯＭメモリ２２中のサービスの情報ＩＳを読み取り、ＥＥＰＲＯＭメモリ１２に記憶する。サービスの情報の内容として含まれるのは、まず、アプリケーション・プログラムＰＡの識別子ＩＰＡと、そのプログラムの実行の為に必要とされる特性ＣＰＡと、多くの場合、認証要求ＤＡである。特性ＣＰＡは、特に、一種のソフトウェア環境であり、メモリの容量やプログラムＰＡの実行に必要な端末ＴＥのハードウェアパラメータであり、更に、第二カードＣＡの外でのプログラムＰＡの実行の禁止または許可である。従って、第二カードＣ２に読み込まれた情報ＩＳにより、第一カードＣ１は、第二カードに保存されているアプリケーション・プログラムに対応するアプリケーションの性質を認識する。

【００４０】

次の過程Ｅ２において、第一カードＣ１がＳＩＭカードＣ１も含めた端末ＴＥがアプリケーション・プログラムの特性ＣＰＡと適合しないと認めた場合には、カードＣ１は過程Ｅ２１で事前検査方法を続行することを拒絶し、「追加カード不適合」というメッセージを表示するように端末ＴＥに対して拒絶を知らせる。

【００４１】

逆の場合には、カードＣ１は中間の過程Ｅ２２において、事前検査方法を続行するか続行しないかの決定を行う。例えば、端末からの呼び出しなどの為に、カードＣ１が直ちに事前検査方法を続行しない場合には、カードＣ１は事前検査を延期して、後でプログラムＰＡを元に戻すか、カードＣ２においてそれを行うようにする。

【００４２】

過程Ｅ２２の後に、第一カードＣ１が事前検査方法を続行する場合には、第一カードは、カードＣ２に読み込まれたアプリケーション・プログラムの特性ＣＰＡに照らし、少なくともどちらか一枚のカードの認証が過程Ｅ３で第二カードＣ２により要求されていることを検証する。

【００４３】

認証要求がなければ、事前検査方法は、過程Ｅ３から過程Ｅ４に移るが、そこではアプリケーション・プログラムＰＡを実行すべき場所を決定することになる。プログラムの実行

場所は、三つの構成単位の中から選ばれるが、該三つの構成単位とは、ＳＩＭカードと呼ばれる第一カードＣ１、追加カードと呼ばれる第二カードＣ２、および端末ＴＥであって、ＳＩＭカードのアプリケーション・ツールキットの予めアクティブなコマンドを用いて、端末で行う。

【００４４】

第一の変形によると、アプリケーション・プログラムＰＡは、アプリケーション・ツールキットの多重カード読取り装置（マルチプル・カードリーダー）のソフトウェア手段を介して、第二カードＣ２から第一カードＣ１に遠隔ロードされ、プログラムＰＡを次の過程Ｅ５でカードＣ１内で実行するようにする。

【００４５】

第二の変形によると、プログラムＰＡの実行は、過程Ｅ５で、第二カードＣ２内で行われる。第一のオプションとしては、プログラムＰＡをＳＩＭカードＣ１の制御の下で起動させ、該カードＣ１は、次に、そのプログラム実行の為のコマンドと応答の交換の主導権を端末ＴＥに委ね、該端末が第二カードと直接通信するというものである。第二のオプションとしては、プログラムＰＡをＳＩＭカードＣ１の制御の下で起動させ、コマンドと応答の全ての交換は、カードＣ１を介して、第二カードＣ２と端末ＴＥの間で行われ、該カードＣ１は、端末に対して、あたかもカードＣ１が自分でプログラムＰＡを保存しかつ実行しているような錯覚を与える。

【００４６】

第三の変形によると、プログラムＰＡは第二カードＣ２から端末ＴＥに遠隔ロードされ、この為に、最初に端末内にインプリメンテーションされたソフトウェアの実行環境において、過程Ｅ５で実行される。

【００４７】

過程Ｅ４の後、カードＣ２に読み込まれたプログラムＰＡは過程Ｅ５で実行される。このプログラムは例えばディスプレイ３７上のテキスト・メニューの表示により、そしてＳＩＭカードＣ１により加入者のデータを取得することにより、さらにネットワークＲＲまたはＲＴＣに向けて要求を送ることにより、その要求への応答を解釈することにより、加入者にサービスを提供する。

【００４８】

他のもう一つの実施様態によると、過程Ｅ１からＥ４においてＳＩＭカードＣ１の中で実行されるオペレーションは、後で詳述する相互認証は別として、図２の左側に示されているが、該オペーレーションは、端末ＴＥにおいて実行され、それはすなわち、マイクロコントローラ３２の制御の下で実行される。従って、端末は、サービス情報ＩＳ（ＩＰＡ，ＣＰＡ，ＤＡ）を過程Ｅ１で読み込み、端末それ自体の決定により、過程Ｅ２，Ｅ３，及びＥ４でプログラムの実行の事前検査を継続する。

【００４９】

図２の過程Ｅ３に戻ると、認証要求ＤＡ１がカードＣ２に読み込まれたサービス情報ＩＳの中に含まれ、かつカードＣ１に記憶されている場合には、第一カードＣ１が、カードの相互認証を開始させる。相互認証は、図３に示された実施様態によると、第一カードＣ１による第二カードＣ２の第一認証Ａ１を含み、次に、第二カードの真正性への応答として、第二カードＣ２による第一カードＣ１の第二認証Ａ２を含む。しかしながら、本発明のもう一つの他の実施様態によると、その認証の順序は逆になる。まず、カードＣ２によるカードＣ１の認証Ａ２が行われ、次に、第一カードの真正性への応答として、カードＣ１によるカードＣ２の認証Ａ１が行われる。

【００５０】

第一認証Ａ１によって確実になることは、カードＣ２のような追加カードに保存されたアプリケーション・プログラムは、このプログラムが正当に証明された場合に限り実行できるということである。認証Ａ１は過程Ａ１１からＡ１５から成る。

【００５１】

過程Ｅ３に続く過程Ａ１１では、第一カードＣ１、つまりＳＩＭカードが、該カード内に

、ＲＯＭメモリ１１とＥＥＰＲＯＭメモリ１２で中書き込まれ管理される第一認証アルゴリズムＡＡ１を有することを検証する。それが肯定されれば、カードＣ１は過程Ａ１２でのカードＣ２の認証に進む。過程Ａ１１でカードＣ１によりカードＣ２の認証されない場合は、ＳＩＭカードＣ１は端末ＴＥを介して第一認証要求のメッセージを、認証サーバーＳＡに伝送するが、該サーバーは、固定網ＢＴＳ－ＢＳＣ－ＭＳＣを通して端末ＴＥが一時的に結合されたビジターロケーションレジスタＶＬＲに接続されている。サーバーＳＡは、カードＣ１に代わって直接カードＣ２の認証を行うが、それは、例として後述する第一の二つの認証のうちの一つに従うようなものである。カードＣ１かサーバーＳＡによる第一認証Ａ１の最後の過程Ａ１４では、カードＣ２が認証されれば、第二認証Ａ２によって相互認証が続行される。認証されなければ、相互認証は停止され、検査方法は過程Ａ１５で終了し、ＳＩＭカードは端末ＴＥに「追加カード認証されず」というメッセージを送り、それをディスプレイ３７上で一時的に表示する。

【００５２】

図４に示された第一の実施様態によると、カードＣ１（またはサーバーＳＡ）内のカードＣ２の第一認証Ａ１２ａは、過程Ｅ１でカードＣ２によりカードＣ１へサービス情報ＩＳに予め伝送された第二カードの証明書ＣＥＲＴを有効にすることから成り、基本的には過程Ａ１２０からＡ１２４への四つの過程を含む。

【００５３】

第一の過程Ａ１２０では、アプリケーション・プログラムＰＡの識別子ＩＰＡは、カードＣ１のＥＥＰＲＯＭメモリ１２で読み出だされる。識別子ＩＰＡは、メモリ１２に保存された秘密鍵テーブルＴＫａ内の読み取りアドレスの役割を果たし、そこから、プログラムＰＡまたはプログラムＰＡを含むプログラム・ファミリーに対応する秘密鍵Ｋａを読み取る。識別子ＩＰＡと鍵Ｋａを認証アルゴリズムＡＡ１ａに適用し、該アルゴリズムが過程Ａ１２１で結果Ｒ１を生成する。アルゴリズムＡＡ１ａは、例えば、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）タイプのものであり、それは後述にて引用される他の認証アルゴリズムと同様である。証明書ＣＥＲＴは過程Ａ１２２でカードＣ１に読み込まれ、過程Ａ１４に相当する過程Ａ１２３で結果Ｒ１と比較される。Ｒ１＝ＣＥＲＴであれば、証明書ＣＥＲＴは証明され、カードＣ２はカードＣ１によって認証されて、カードＣ１の認証は過程Ａ２で実行される。そうでなければ、認証と事前検査の方法は、過程Ａ１５で停止される。

【００５４】

カードＣ１内でのカードＣ２の他の第一認証Ａ１２ｂが図５に示されている。その認証は、過程Ａ１２４からＡ１２９を含み、第一カードＣ１によって伝送された乱数ＮＡに応じて、第二カードＣ２の中で行われる計算結果ＳＧを、カードＣ１によって有効化する。

【００５５】

過程Ａ１１に続いて、カードＣ１は、疑似乱数生成器によって供給される疑似乱数ＮＡ１を選定し、該疑似乱数は、プロセッサ１０が過程Ａ１２４で、端末ＴＥを介してカードＣ２に伝送される認証要求メッセージの中に導入するために保存しているものである。認証要求への応答として、第二カードＣ２は、伝送された乱数ＮＡ１を一時的にメモリ２３に記憶し、過程Ａ１２５で、ＥＥＰＲＯＭメモリ２２の中の秘密鍵Ｋｂを読み込む。過程Ａ１２６で、乱数ＮＡ１と鍵Ｋｂを認証アルゴリズムＡＡ１ｂに適用し、該アルゴリズムが署名ＳＧ２を生成する。

【００５６】

第一カードＣ１の中で、過程Ａ１２５とＡ１２６とほとんど同時に、類似の過程Ａ１２７とＡ１２８が行われる。過程Ａ１２７では、認証要求のメッセージを作成した後、乱数ＮＡ１はカードＣ１のＲＡＭメモリ１３に書き込まれ、識別子ＩＰＡはカードＣ１のＥＥＰＲＯＭメモリ１２で読み込まれて、ＥＥＰＲＯＭメモリ１２内の秘密鍵Kbテーブルで読み取りのアドレスを指定する。次に過程Ａ１２８で、メモリ１３に読み込まれた乱数ＮＡ１とテーブルＴＫｂに読み込まれた鍵Ｋｂを、カードＣ１のＲＯＭメモリ１１とＥＥＰＲＯＭメモリ１２にインプリメンテーションされたアルゴリズムＡＡ１ｂに同様に適用する

。カードＣ１の中のアルゴリズムＡＡ１ｂにより結果Ｒ２が生成される。
【００５７】
最後に過程Ａ１２９で、第二カードＣ２が署名ＳＧ２を端末ＴＥを介して第一カードＣ１に伝送し、それを結果Ｒ２と比較する。過程Ａ１４に相当する過程Ａ１２９では、もしＲ２＝ＳＧ２ならばカードＣ１において中でカードＣ２は過程A２０を実行するために認証され、あるいはＲ２がＳＧ２とは異なるならば、カードＣ２を拒絶して、過程Ｅ１５で認証と事前検査の方法が停止される。
【００５８】
過程Ａ１２０、Ａ１２４に先立って、第一認証のそれぞれにおいて、秘密鍵Ｋａ，Ｋｂは、カードを所持するユーザーが使用契約を結ぶ時にカードＣ１を最初に個人化する際に、ＳＩＭカードＣ１のＥＥＰＲＯＭメモリ１２にロードされるか、または、カードＣ１を使用中に、例えば、変更するか補完する為に、遠隔ロードされる。
【００５９】
第一認証を行う第三の実施様態では、過程Ｅ１で、第二カードから第一カードに向けて、アプリケーション・プログラムの識別子ＩＰＡ、第二カードの識別子、つまり典型的には英語でＣａｒｄ　Ｓｅｒｉａｌ　Ｎｕｍｂｅｒと言うシリアル番号ＣＳＮ、そして、ＩＰＡとＣＳＮに応じた番号ＲＮＤを伝送する。第一カードの中に既にＩＰＡ、ＣＳＮ、ＲＤＮの三要素についての許可があるなら、認証は成功する。その代わり、第一カードにまだこの三要素についての許可がないのなら、安全化されたチャネルを介して許可センタに接触し、この許可センタにＩＰＡ、ＣＳＮ、ＲＮＤの三要素、並びにそのＣＳＮまたはＩＭＳＩのような第一カードに関連した唯一の番号を伝送する。
【００６０】
許可センタはデータ・ベースの中で、ＩＰＡ、ＣＳＮ、ＲＮＤの三要素が許可されたカードに対応していることを検証する。もしそうでなければ、許可センタは第一カードに、第二カードは許可されていないことを示すメッセージを伝送する。もし三要素が許可された第二カードに対応しているならば、許可センタはデータ・ベースの中で、第二カードがまだもう一つの「第一の」カードと結びついていないことを検証する。もしその通りなら、許可センタは第一カードに、認証の失敗を意味するメッセージを送る。第二カードがまだ第一カードに結びついていない場合は、許可センタは、第二カードが第一カードに結びつくようにデータ・ベースを変更し、次に、許可センタは第一カードに認証の成功を意味するメッセージを送る。その時、第一カードは許可を記憶し、後に認証を行う段階で、許可センタに再度接触することを避けるようにする。
【００６１】
第一認証の第三の実施様態においては、オプションとして、第二カードを、もはや第一カード一枚だけにではなく、一群の複数の第一カードに結びつけ、少人数のユーザーが同一の第二カードを使えるようにすることもできることになる。
【００６２】
図３に戻ると、第二認証Ａ２は、過程Ａ１４で認証Ａ１２ａにより等式Ｒ１＝ＣＥＲＴが、あるいは認証Ａ１２ｂにより等式ＲＥＳ１＝ＳＧが満たされれば、開始される。認証Ａ２によって確実になるのは、第一カードＣ１、つまりＳＩＭカードが第二カードＣ２によって正当に適格であると認められ、カードＣ２においてアプリケーション・プログラムＰＡが起動され読みだされるということである。
【００６３】
第二認証Ａ２は、まずその必然性を過程Ａ２０において予め確認することから始まり、メモリ１２の中のサービス情報ＩＳの中で第二認証要求ＤＡ２の存在を検索する。要求ＤＡ２がなく認証Ａ２が実行されない場合は、事前検査方法は、直接アプリケーション・プログラム実行場所の特定Ｅ４に移行する。逆の場合には、第二認証の過程Ａ２１からＡ２５が、第一認証Ａ１の過程Ａ１１からＡ１５におけるのと同様に、それぞれ実行される。
【００６４】
過程Ａ２０に続く過程Ａ２１において、カードＣ１は、所謂第二認証に関与することがで

きることを検証する。不可能である場合には、カードＣ１は、端末ＴＥを介して、第二認証の要求メッセージを認証サーバーＳＡに送信し、該認証サーバーは、過程Ａ２３において、後に詳述する過程Ａ２２におけるのと同様に、カードＣ１に代わって、第二認証に関与する。カードＣ１の関与またはカードＣ２によるサーバーＳＡの関与を伴うカードＣ１の認証の過程Ａ２２またはＡ２３の後のＡ２４で、カードＣ１は、認証されて事前検査方法が実行場所特定過程Ｅ４に移行するか、あるいは認証されずに事前検査方法が過程Ａ２５で終了し、端末ＴＥのディスプレイ３７上に「ＳＩＭカード不許可」というメッセージを提示することになる。

【００６５】

図６に示された第一の実施様態によれば、第二認証Ａ２２ａは、過程Ａ２２０からＡ２２２を含み、ＳＩＭカードＣ１を所持する加入者の国際識別番号ＩＭＳＩ（Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｍｏｂｉｌｅ　Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｔｙ）の所定のフィールドを、第二カードＣ２に伝送すること、そして、伝送されたフィールドを予めカードＣ２の中に記憶された番号と比較する。

【００６６】

過程Ａ２２０では、カードＣ１のメモリ１２に保存された識別番号ＩＭＳＩ中の所定のフィールドが読み出される。所定のフィールドは、例えば加入者がつながっている無線電話網ＲＲの２ビットの識別符号ＭＮＣ（モバイル・ネットワーク・コード　Ｍｏｂｉｌｅ　Ｎｅｔｗｏｒｋ　Ｃｏｄｅ）であるか、あるいは、識別符号ＭＮＣとネットワークＲＲが属する国の識別符号ＭＣＣ（モバイル・カントリー・コード　Ｍｏｂｉｌｅ　Ｃｏｕｎｔｒｙ　Ｃｏｄｅ）の集合であって、一般的にネットワークＲＲのオペレータから発行されたカードＣ２が、ＳＩＭカードが確かにオペレータに属することを検証する。もう一つの他の変形によれば、所定のフィールドは、加入者の一つのグループに共通の加入者番号の接頭辞ＭＳＩＮ（Ｍｏｂｉｌｅ　Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）である。

【００６７】

第二カードＣ２内の、例えば識別符号ＭＮＣの所定のフィールドに応えて、同等の番号ＭＮＣ２は、過程Ａ２２１においてメモリ２２の中に読み込まれる。過程Ａ２４に相当する次の過程Ａ２２２では、番号ＭＮＣとＭＮＣ２を比較し、それらが等しい場合には、事前検査方法を過程Ｅ４に向かって進める。等しくなければ、カードＣ１の真正性は、カードＣ２によって認知されず、該カードＣ２は端末ＴＥを、直接もしくはＳＩＭカードＳ１を介して、過程Ａ２５のメッセージを表示するように促し、事前検査方法は停止される。

【００６８】

図７に示された第二の実施様態によれば、第二認証Ａ２２ｂは過程Ａ２２３からＡ２２９を含み、カードＣ１がカードＣ２に要求した乱数ＮＡ２に応じて、第一カードＣ１の中で行われた計算結果ＳＧ３をカードＣ２によって有効化することにある。

【００６９】

過程Ａ２１に続いて、カードＣ１は、過程Ａ２２３で、端末ＴＥを介して、乱数を要求するメッセージをカードＣ２に送る。カードＣ１は、プロセッサー２０の供給する乱数ＮＡ２をＥＥＰＲＯＭメモリ２２に読み込み、それを端末ＴＥを介してカードＣ１に伝送し、該カードＣ１は過程Ａ２２４でそれを一時的に記憶する。カードＣ１の中では、乱数を要求する過程の後に、ＥＥＰＲＯＭメモリ１２の中でアプリケーション・プログラムの識別子ＩＰＡを読む過程Ａ２２５が続く。識別子は秘密鍵テーブルＴＣの読み取りアドレス指定する役割を果たし、プログラムＰＡまたはプログラムＰＡ含むプログラム・ファミリーに対応する鍵Ｃを読み取る。受信された乱数ＮＡ２と読み取られた鍵Ｃを、カードＣ１の中で第二認証アルゴリズムＡＡ２に適用し、過程Ａ２２６で署名ＳＧ３を算出し、その署名は端末ＴＥを介してカードＣ２に伝送される。

【００７０】

乱数を選定する過程Ａ２２４の後、カードＣ２において、メモリ２２の鍵Ｃは、過程Ａ２２７で乱数ＮＡ２と共に読まれ、カードＣ２のメモリ２１と２２に同様にインプリメンテ

ーションされたアルゴリズムＡＡ２に適用される。過程Ａ２２８で、アルゴリズムＡＡ２は結果Ｒ３を生成する。カードＣ２が受け取った署名ＳＧ３を、過程Ａ２４に相当する過程Ａ２２９で、結果Ｒ３と比較する。ＳＧ３＝Ｒ３である場合は、カードＣ１はカードＣ２によって認証され、事前検査方法は過程Ｅ４に移行する。そうでない場合、つまりＳＧ３≠Ｒ３である場合は、カードＣ２はカードＣ１を過程Ａ２５で拒絶し、ＳＩＭカードは端末ＴＥに「ＳＩＭカード不許可」というメッセージを表示するように求め、事前検査方法は終了する。

【００７１】

一般的に、カードＣ２によるカードＣ１の認証が失敗の場合には、カードＣ２に保存されるプログラムの全部または一部が読み込み不可能で実行不可能なままになる。

【００７２】

本発明のもう一つの他の実施様態によれば、第二カードのプログラムの実行に先立って予め二枚のカードの相互認証が行われ、その後に、プログラム実行の全セッションを通じての認証が行われる。始めのうちは、各カードが乱数を生成して、それをもう一枚のカードに伝送する。二つの乱数に基づき、各カードがセッション鍵と呼ばれる鍵を計算する。各カードは、セッション鍵を用いる暗号化アルゴリズムを、二つの乱数のように、既知のメッセージに適用して、暗号化されたメッセージを得る。各カードはその暗号化されたメッセージをもう一枚のカードに伝送し、もう一枚のカードから受け取った暗号化メッセージの真正性を検証する。

【００７３】

プログラムの実行は、二枚のカードが相互に認証される場合に、続行可能となる。プログラムを実行する全セッションを通じて、一枚のカードからもう一枚のカードに向け伝送された全てのメッセージが次のように認証される。伝送すべきメッセージにアルゴリズムを適用し、前記メッセージの電子指紋を得る。セッション鍵を用いる署名アルゴリズムをその電子指紋に適用して、署名を得て、該署名が、それに対応するメッセージと共に伝送されることになる。一枚のカードがもう一枚のカードから署名付きのメッセージを受け取る場合には、カードがその電子指紋と受け取ったメッセージに対応する署名とを再計算し、この署名がメッセージと共に受け取った署名と同一であることを検証する。

【図面の簡単な説明】

【図１】　図１は、セルラー無線電話網のブロック線図に詳細な移動端末を添えたものである。

【図２】　図２は、本発明によるプログラム実行の事前検査方法の主要な過程のアルゴリズムである。

【図３】　図３は、端末に接続された第一カードと第二カードとの相互認証アルゴリズムである。

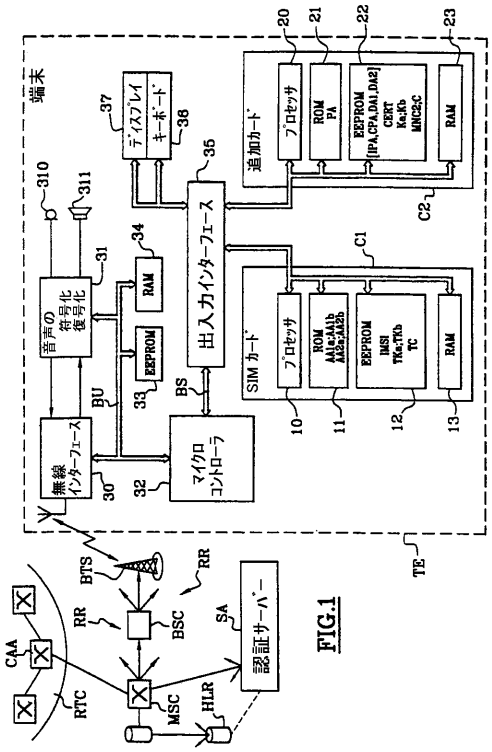
【図４】　図４は、第一の実施様態に従う第一カードによる第二カードの第一認証アルゴリズムである。

【図５】　図５は、第二の実施様態に従う第一カードによる第二カードの第一認証アルゴリズムである。

【図６】　図６は、第一の実施様態に従う第二カードによる第一カードの第二認証アルゴリズムである。

【図７】　図７は、第二の実施様態に従う第二カードによる第一カードの第二認証アルゴリズムである。

【図１】


端末
ディスプレイ
キーボード
追加カード
プロセッサ
ROM PA
EEPROM [IPA,CPA,DA1,DA2] CERT Ka,Ks MNC2C
RAM
出入力インターフェース
音声の符号化復号化
EEPROM
無線インターフェース
マイクロコントローラ
SIM カード
ROM AA1a,AA1b AA2a,AA2b
EEPROM IMSI TKa,TKb TC
BTS
BSC
RR
SA
認証サーバー
CAA
RTC
MSC
HLR
TE
FIG.1

【図２】

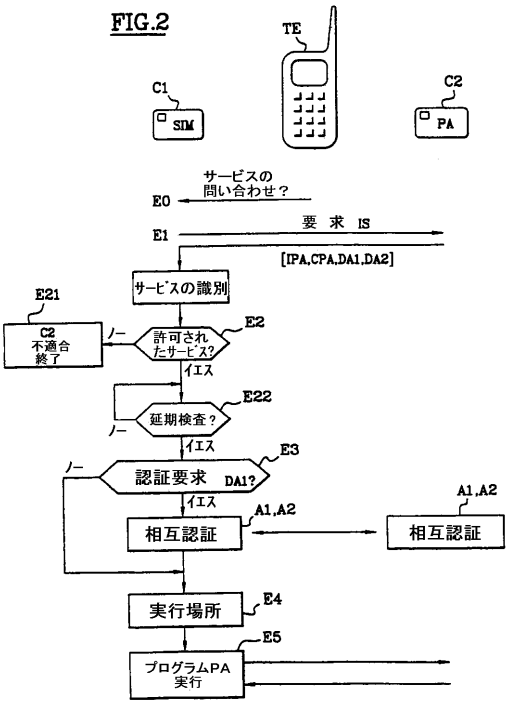


FIG.2
TE
C1
SIM
C2
PA
サービスの問い合わせ？
E0
要求 IS
E1
[IPA,CPA,DA1,DA2]
サービスの識別
E21
C2 不適合 終了
ノー
許可されたサービス?
E2
イエス
延期検査？
E22
認証要求 DA1?
E3
A1,A2
相互認証
相互認証
実行場所
E4
E5
プログラムPA 実行

【図３】

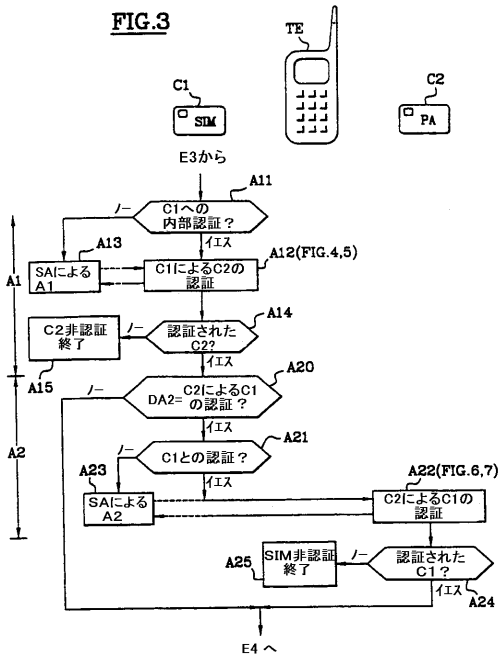


FIG.3
TE
C1
SIM
C2
PA
E3から
A11
C1への内部認証？
ノー
イエス
A13
SAによる A1
C1によるC2の認証
A12(FIG.4,5)
A1
C2非認証終了
ノー
認証された C2?
A14
A15
A20
DA2= C2によるC1の認証？
A2
C1との認証？
A21
A23
SAによる A2
A22(FIG.6,7)
C2によるC1の認証
SIM非認証終了
A25
認証された C1？
A24
E4へ

【図４】

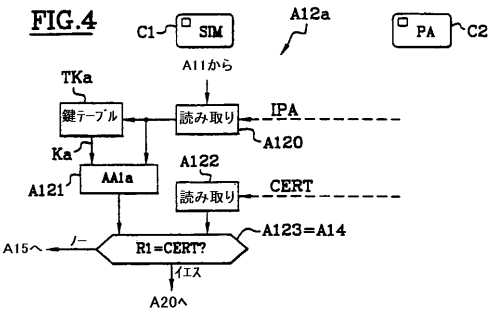


FIG.4
C1
SIM
A12a
PA
C2
A11から
TKa
鍵テーブル
読み取り
IPA
A120
Ka
A121
AA1a
A122
読み取り
CERT
A123=A14
A15へ
ノー
R1=CERT?
イエス
A20へ

【図５】

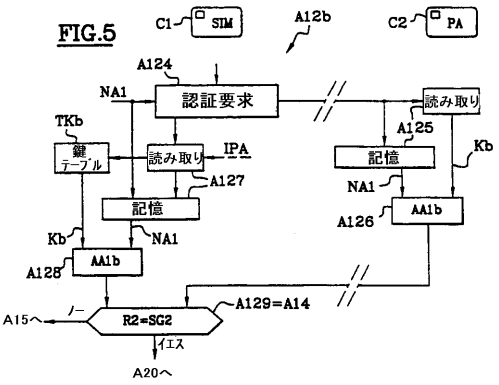
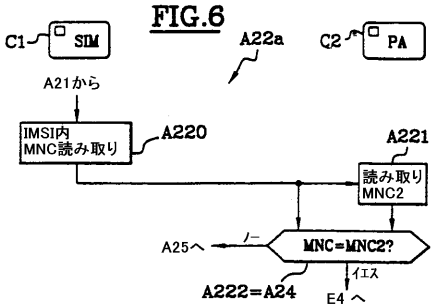


FIG.5
C1
SIM
A12b
C2
PA
A124
NA1
認証要求
読み取り
A125
TKb
鍵テーブル
読み取り
IPA
A127
記憶
Kb
NA1
A126
AA1b
記憶
Kb
NA1
A128
AA1b
A129=A14
A15へ
ノー
R2=SG2
イエス
A20へ

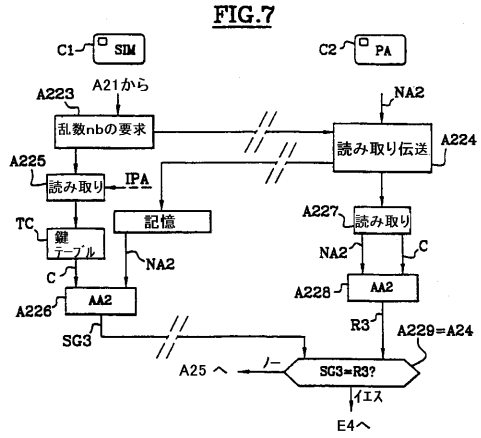
【図６】

FIG.6




【図７】

FIG.7



フロントページの続き

(56)参考文献 特開平０８－３３９４２９（ＪＰ，Ａ）
特表２００２－５３７６１８（ＪＰ，Ａ）
特表平０８－５０５０２７（ＪＰ，Ａ）
特開平１１－１３４１８９（ＪＰ，Ａ）
特表平１１－５０１４２４（ＪＰ，Ａ）
特開平０４－０８３４４７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06K 17/00
G06K 19/00-19/10