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

特許第5490772号
(P5490772)

(45)発行日　平成26年5月14日(2014.5.14)　(24)登録日　平成26年3月7日(2014.3.7)

(51)Int.Cl.　F I
H04W 12/10 (2009.01)　H04W 12/10
H04W 8/24 (2009.01)　H04W 8/24
H04L 9/32 (2006.01)　H04L 9/00　673Z

請求項の数 20　外国語出願　(全 20 頁)

(21)出願番号　特願2011-251075 (P2011-251075)
(22)出願日　平成23年10月28日 (2011.10.28)
(65)公開番号　特開2012-120163 (P2012-120163A)
(43)公開日　平成24年6月21日 (2012.6.21)
審査請求日　平成23年12月26日 (2011.12.26)
(31)優先権主張番号　61/407,866
(32)優先日　平成22年10月28日 (2010.10.28)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　13/080,521
(32)優先日　平成23年4月5日 (2011.4.5)
(33)優先権主張国　米国 (US)

(73)特許権者　503260918
アップル　インコーポレイテッド
アメリカ合衆国　９５０１４　カリフォルニア州　クパチーノ　インフィニット　ループ　1
(74)代理人　100092093
弁理士　辻居　幸一
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100086771
弁理士　西島　孝喜
(74)代理人　100109335
弁理士　上杉　浩

最終頁に続く

(54)【発明の名称】アクセス制御クライアントの記憶及び演算に関する方法及び装置

(57)【特許請求の範囲】
【請求項１】
少なくとも１つのネットワークと通信する１以上の無線リンクと、
アクセス制御クライアントを記憶するよう構成されたセキュアな要素と、
前記セキュアな要素に対するインタフェースであって、暗号鍵とこれに関連する第１の承認証明とを有する前記インタフェースと、
プロセッサと、
前記プロセッサとデータ通信する記憶デバイスであって、コンピュータ実行可能な命令を含み、前記コンピュータ実行可能な命令の少なくともサブセットは１以上のセグメントにパーティション化され、前記プロセッサが実行するとき、前記コンピュータ実行可能な命令は、
a)前記少なくとも１つのネットワークに特有の前記アクセス制御クライアントのための１以上のコンポーネントに関する要求であって、前記セキュアな要素に関連し且つ証明する機関を識別するための前記第１の承認証明を含む当該要求を、前記インタフェースを介して送信し、
b)前記１以上の要求されたコンポーネント及び第２の承認証明を受信し、
c)前記第２の承認証明を検証し、前記第２の承認証明の発行者は少なくとも１つのネットワークのオペレータから離れており、
d)前記第２の承認証明の検証が成功したことに応じて、前記アクセス制御クライアントを前記セキュアな要素に記憶する、

ように構成されている前記記憶デバイスと、
を含む無線装置。
【請求項２】
前記アクセス制御クライアントは、電子加入者識別モジュール（ｅＳＩＭ）を含み、
前記セキュアな要素は、電子ユニバーサル集積回路カード（ｅＵＩＣＣ）を含み、前記１以上のｅＳＩＭのそれぞれは、国際移動電話加入者識別番号（ＩＭＳＩ）に関連し、
前記ｅＳＩＭの各々は、認証及びキー合意（ＡＫＡ）の少なくとも一部に基づき、セルラーネットワークとのセキュアな接続を確立するよう更に構成される、請求項１に記載の無線装置。
【請求項３】
前記少なくとも１つのネットワークは、グローバル・スタンダード・フォー・モバイル・コミュニケーションズ（ＧＳＭ）ネットワークを含む、請求項２に記載の無線装置。
【請求項４】
前記少なくとも１つのネットワークは、ユニバーサル・モバイル・テレコミュニケーション・システム（ＵＭＴＳ）ネットワークを含む、請求項２に記載の無線装置。
【請求項５】
前記少なくとも１つのネットワークは、符号分割多重アクセス方式２０００（ＣＤＭＡ２０００）ネットワークを含む、請求項２に記載の無線装置。
【請求項６】
前記暗号鍵は、前記第１の承認証明と一意的に関連する、請求項１に記載の無線装置。
【請求項７】
前記暗号鍵は、公開で配信され得る非対称のカウンターパート鍵を有する、請求項１に記載の無線装置。
【請求項８】
前記非対称のカウンターパート鍵は、前記無線装置に対してセキュアな送信を実現する、請求項７に記載の無線装置。
【請求項９】
前記１以上のコンポーネントは、セッション鍵で暗号化されたアクセス制御クライアントを含む、請求項１に記載の無線装置。
【請求項１０】
前記セッション鍵は、ランダムに生成される、請求項９に記載の無線装置。
【請求項１１】
無線ネットワークの使用のためにユーザアクセス制御クライアントを要求する方法であって、
無線装置が、前記無線ネットワークからユーザアクセス制御クライアントを要求する処理であって、その要求は第１の承認証明に関連する当該処理と、
前記無線装置が、前記ユーザアクセス制御クライアント及び第２の承認証明を受信する処理であって、前記第１及び第２の承認証明は、前記ユーザアクセス制御クライアントを提供する機関とは異なる信用機関によって発行される当該処理と、
前記第２の承認証明が有効であれば、前記ユーザアクセス制御クライアントを前記無線装置のセキュアな要素内に記憶する処理と、
前記無線ネットワークに対するアクセスは、(i)前記ユーザアクセス制御クライアントを介したアクセス、及び(ii)前記ユーザアクセス制御クライアントに関する要求に限定されることを特徴とする前記方法。
【請求項１２】
前記ユーザアクセス制御クライアントは、電子加入者識別モジュール（ｅＳＩＭ）を含む、請求項１１に記載の方法。
【請求項１３】
前記第１及び第２の承認証明は、第１及び第２の暗号鍵の組と一意的に関連する、請求項１１に記載の方法。

【請求項１４】
前記第１及び第２の暗号鍵の組は、非対称の鍵のペアを含む、請求項１３に記載の方法。
【請求項１５】
前記ユーザアクセス制御クライアントは、セッション鍵で更に暗号化される、システム１１に記載の方法。
【請求項１６】
前記ユーザアクセス制御クライアントを記憶する処理は、複数のメモリパーティションから選択された一つのメモリパーティション内に前記ユーザアクセス制御クライアントを記憶することを含む、請求項１１に記載の方法。
【請求項１７】
前記メモリパーティションは、前記ユーザアクセス制御クライアントに対して一意的である、請求項１６に記載の方法。
【請求項１８】
前記ユーザアクセス制御クライアントに対するその後の修正は、前記第２の承認証明によってのみ実行される、請求項１７に記載の方法。
【請求項１９】
無線ネットワークとともに使用する無線装置に、ユーザアクセス制御クライアントを提供するためのシステムであって、
第１の承認証明に関連するユーザアクセス制御クライアントを、要求メッセージを介して要求する無線装置と、
無線サーバが前記要求メッセージを受信することに応じて、前記要求されたユーザアクセス制御クライアントに第２の承認証明を提供する前記無線サーバとを備え、
前記第１及び第２の承認証明は、前記ユーザアクセス制御クライアントを提供する機関以外の信用機関によって発行されたものであり、
前記無線装置は、前記第２の承認証明が有効であれば、前記ユーザアクセス制御クライアントを記憶し、前記無線ネットワークに対するアクセスは、(i)前記ユーザアクセス制御クライアントを介したアクセス、及び(ii)前記ユーザアクセス制御クライアントに関する要求に限定されることを特徴とする前記システム。
【請求項２０】
無線ネットワークと無線ユーザ装置とを備えた無線システムであって、
前記無線ユーザ装置は、
1)少なくとも１つのネットワークと通信する１以上の無線リンクと、
2)アクセス制御クライアントを記憶するよう構成されたセキュアな要素と、
3)前記セキュアな要素に対するインタフェースであって、暗号鍵とこれに関連する第１の承認証明とを有する前記インタフェースと、
4)プロセッサと、
5)前記プロセッサとデータ通信する記憶デバイスであって、コンピュータ実行可能な命令を含み、前記コンピュータ実行可能な命令の少なくともサブセットは１以上のセグメントにパーティション化され、前記プロセッサが実行するとき、前記コンピュータ実行可能な命令は、
a)前記少なくとも１つのネットワークに特有の前記アクセス制御クライアントのための１以上のコンポーネントに関する要求であって、証明する機関を識別するための前記第１の承認証明を含む当該要求を、前記インタフェースを介して送信し、
b)前記１以上の要求されたコンポーネント及び第２の承認証明を受信し、
c)前記第２の承認証明を検証し、前記第２の承認証明の発行者は少なくとも１つのネットワークのオペレータから離れており、
d)前記第２の承認証明の検証が成功したことに応じて、前記アクセス制御クライアントを前記セキュアな要素に記憶するように構成された前記記憶デバイスと、
を含むことを特徴とする前記無線システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、無線通信及びデータネットワークの分野に係り、より詳細には、一態様として、アクセス制御エンティティ又はクライアントのセキュアな修正、記憶及び演算に関する方法及び装置に向けられている。
【０００２】
優先権及び関連出願：本出願は、２０１１年４月５日に出願された“METHODS AND APPARATUS FOR STORAGE AND EXECUTION OF ACCESS CONTROL CLIENTS”と題する米国特許出願第１３／０８０，５２１号の優先権を主張するもので、該特許出願は、２０１０年１０月２８日に出願された“METHODS AND APPARATUS FOR STORAGE AND EXECUTION OF ACCESS CONTROL CLIENTS”と題する米国仮特許出願第６１／４０７，８６６号の優先権を主張するものであり、各特許出願は、引用としてここにそのまま組み入れる。
【０００３】
また、本出願は、２０１１年４月５日に出願された“APPARATUS AND METHODS FOR CONTROLLING DISTRIBUTION OF ELECTRONIC ACCESS CLIENTS”と題する共同所有、同時係属中の米国特許出願第１３／０８０，５５８号、２０１０年１１月２２日に出願された“WIRELESS NETWORK AUTHENTICATION APPARATUS AND METHODS”と題する第１２／９５２，０８２号、２０１０年１１月２２日に出願された“APPARATUS AND METHODS FOR PROVISIONING SUBSCRIBER IDENTITY DATA IN A WIRELESS NETWORK”と題する第１２／９５２，０８９号、２０１０年１２月２８日に出願された“VIRTUAL SUBSCRIBER IDENTITY MODULE DISTRIBUTION SYSTEM”と題する第１２／９８０，２３２号、２００９年１月１３日に出願された“POSTPONED CARRIER CONFIGURATION”と題する第１２／３５３，２２７号、２０１１年４月５日に出願された“APPARATUS AND METHODS FOR STORING ELECTRONIC ACCESS CLIENTS”と題する米国仮特許出願第６１／４７２，１０９号、２０１１年４月５日に出願された“APPARATUS AND METHODS FOR DISTRIBUTING AND STORING ELECTRONIC ACCESS CLIENTS”と題する米国仮特許出願第６１／４７２，１１５号、２０１０年１０月２８日に出願された“METHODS AND APPARATUS FOR ACCESS CONTROL CLIENT ASSISTED ROAMING”と題する米国仮特許出願第６１／４０７，８５８号、２０１０年１０月２８日に出願された“MANAGEMENT SYSTEMS FOR MULTIPLE ACCESS CONTROL ENTITIES”と題する米国仮特許出願第６１／４０７，８６１号（今は、２０１１年４月４日に出願された同じ標題の米国特許出願第１３／０７９，６１４号）、２０１０年１０月２８日に出願された“METHODS AND APPARATUS FOR DELIVERING ELECTRONIC IDENTIFICATION COMPONENTS OVER A WIRELESS NETWORK”と題する第６１／４０７，８６２号、２０１０年１０月２９日に出願された“ACCESS DATA PROVISIONING SERVICE”と題する第６１／４０８，５０４号、（今は、２０１１年４月１日に出願された“ACCESS DATA PROVISIONING APPARATUS AND METHODS”と題する米国特許出願第１３／０７８，８１１号）、２０１０年１１月３日に出願された“METHODS AND APPARATUS FOR ACCESS DATA RECOVERY FROM A MALFUNCTIONING DEVICE”と題する第６１／４０９，８９１号、２０１０年１１月４日に出願された“SIMULACRUM OF PHYSICAL SECURITY DEVICE AND METHODS”と題する第６１／４１０，２９８号（今は、２０１１年４月５日に出願された同じ標題の米国特許出願第１３／０８０，５３３号）、及び、２０１０年１１月１２日に出願された“APPARATUS AND METHOD FOR RECORDATION OF DEVICE HISTRY ACROSS MULTIPLE SOFTWARE EMULATION”と題する第６１／４１３，３１７号にも関連しており、その各々は、引用としてここにそのまま組み入れる。
【背景技術】
【０００４】
殆どの無線通信システムに関する先行技術において、セキュアな通信のためにアクセス制御が要求される。例えば、一つの単純なアクセス制御スキームは、(i)通信するパーティの識別を認証すること、(ii)その認証された識別に見合ったアクセスレベルを獲得すること、を含む。典型的なセルラー（無線）システム（例えば、ユニバーサル・モバイル・

テレコミュニケーション・システム（ＵＭＴＳ））の環境内では、アクセス制御は、物理的ユニバーサル集積回路カード（ＵＩＣＣ）上で実行するユニバーサル加入識別モジュール（ＵＳＩＭ）と呼ばれるアクセス制御クライアンによって統括される。ＵＳＩＭアクセス制御クライアントはＵＭＴＳセルラーネットワークへの加入者を認証する。首尾良く認証された後に、加入者は、セルラーネットワークへアクセスすることが許される。この後に用いられるのだが、“アクセス制御クライアント”という用語は、一般的に、ハードウェア又はソフトウェアのいずれかに組み込まれる論理的エンティティを指し、これは、ネットワークに対して第１のデバイスのアクセスを制御するのに適している。アクセス制御クライアントの共通例は、上述したＵＳＩＭ、ＣＤＭＡ加入者識別モジュール（ＣＳＩＭ）、ＩＰマルチメディアサービス識別モジュール（ＩＳＩＭ）、加入識別モジュール（ＳＩＭ）、除去可能ユーザ識別モジュール（ＲＵＩＭ）などを含む。

【０００５】

典型的には、ＵＳＩＭ（もっと一般的には、“ＳＩＭ”）は、よく知られた認証及びキー合意（ＡＫＡ）手順を実行し、それはセキュアな初期化を保証するために適用可能なデータ及びプログラムを検証し暗号化する。詳しく言うと、ＵＳＩＭは、(i)リモートチャレンジを上手く回答してネットワークオペレータに自身の識別を立証すること、(ii)ネットワークの識別を検証するチャレンジを発行すること、の両方をしなければならない。

【０００６】

しかしながら、既存のＳＩＭ解決法は、多様な弱点と不都合さをもっている。まず、ＳＩＭソフトウェアは物理的ＵＩＣＣカードメディアに対してハードコード化される。加入者はＳＩＭオペレーションへの新たなＵＩＣＣを必要とする。これは、ＭＮＯと加入者双方に弊害をもたらし得る。例えば、認証の手順が（例えば、悪意に満ちた“ハッキング”行為）により“壊れてた”という場合、加入者には新たなＵＩＣＣが発行されなければならない。この処理は時間を浪費するとともに、コスト高となる。さらに、詳細は後述するが、物理的ＳＩＭのみが信頼された一つのエンティティ、つまり、通信できるよう構成されたモバイル・ネットワーク・オペレータ（ＭＮＯ）を認識する。その結果、デバイスとＭＮＯとの間の既存の信用のある関係を介することを除き、展開後プログラミングを組み込むための最新方法は存在しない。例えば、新たな又は更新されたＳＩＭソフトウェアの提供を望むサードパーティＳＩＭの開発者は、物理的ＳＩＭカードメディアの非柔軟性、及び加入者のＳＩＭとの間の信頼された関係を確立する能力の欠如の両方によって妨害される。この“ボトルネック”制御は、ＳＩＭベンダーに提供することができる多くの能力をかなり制限することになる。

【０００７】

したがって、展開後のＳＩＭ配信及び修正を可能にするために新たな解決法が必要とされる。理想的には、このような解決法は、携帯端末が“フィールド（展開後）”にありながら、この携帯端末によりＳＩＭオペレーションへの変化を受信し実行することができるようにしなければならない。さらに、改善された方法及び装置は、他の望ましい特徴、とりわけマルチＳＩＭプロファイル、フレキシブルオペレーション、更新などをサポートしるべきである。

【０００８】

しかしながら、一般的には、改善された方法及び装置は、セキュアな修正、記憶、及びアクセス制御クライアントの実行のために必要とされる。アクセス制御クライアントのオペレーションを修正する技術は、マルチ加入者アクセスプロファイル、セキュアなデバイス更新、加入者サービス準備のための代替方法などの特徴をサポートするのに必要とされる。さらにまた、アクセス制御の反応性の高い特性、及び密かな使用及びサービス窃盗の可能性の理由から、このような修正を行なうセキュアな方法は主な関心事である。

【発明の概要】

【課題を解決するための手段】

【０００９】

本発明は、セキュアな修正、記憶、及びアクセス制御クライアントの実行のための改善

された方法及び装置を提供することによって上述したニーズを満たすものである。

【００１０】

本発明の第１の態様において、無線装置が開示される。一実施例において、その装置は、アクセス制御クライアントを介して少なくとも１つのネットワークと通信する１以上の無線リンクと、アクセス制御クライアントを記憶するよう構成されたセキュアな要素と、前記セキュアな要素に対するインタフェースであって、暗号鍵とこれに関連する第１の証明とを有する前記インタフェースと、プロセッサと、前記プロセッサとデータ通信する記憶デバイスであって、コンピュータ実行可能な命令を含む。前記コンピュータ実行可能な命令の少なくともサブセットは、１以上のセグメントにパーティション化される。

【００１１】

一変形例では、前記コンピュータ実行可能な命令は、プロセッサが実行するとき、前記少なくとも１つのネットワークに特有の前記アクセス制御クライアントのための１以上のコンポーネントに関する承認証明と暗号鍵を含んだ要求を前記インタフェースを介して送信し、前記１以上の要求された、第２の承認証明に関連するコンポーネントを受信し、前記第２の証明を検証し、前記第２の証明の検証が成功したことに応じて、前記アクセス制御クライアントをロードする、ことを含む。

【００１２】

本発明の第１の態様において、相互認証のための方法が開示される。一実施例において、その方法は、第１の承認証明に関連する１以上のコンポーネントを要求し、前記１以上のコンポーネント及び第２の承認証明を受信し、前記第２の承認証明が有効であれば、前記１以上のコンポーネントをロードし、前記第１及び第２の承認証明は信用機関によって発行される、ことを含む。

【００１３】

本発明の第３の態様において、アクセス制御クライアントを実行するための方法が開示される。一実施例において、その方法は、セキュアなパーティションを選択する第１のブートストラップオペレーティングシステムを実行し、前記セキュアなパーティションは唯一つのアクセス制御クライアントに関連しており、一つの共通オペレーティングシステム及び一つのアクセス制御クライアントを含むセキュアなパーティションを検証し、一つのアクセス制御クライアントをロードする共通オペレーティングシステムを実行する。アクセス制御クライアントは外部セルラーネットワークなどのネットワークを認証するよう構成される。

【００１４】

本発明の第４の態様において、携帯装置が開示される。一実施例において、その携帯装置は、ブートストラップＯＳアーキテクチャを用いて、仮想又は電子的ＳＩＭデータ構造を、要求、受信及び利用する。

【００１５】

本発明の第５の態様において、コンポーネント読出し可能な装置が開示される。一実施例において、その装置は、その装置上で起動する少なくとも１つのコンポーネントプログラムをもつ記憶媒体を含む。前記少なくとも１つのコンポーネントプログラムは、ブートストラップＯＳアーキテクチャを用いて、仮想又は電子的ＳＩＭデータ構造のための要求を受信し、処理し、提供する。

【００１６】

本発明の第６の態様において、ユーザに仮想又は電子的ＳＩＭを配信するシステムが開示される。一実施例において、そのシステムは、インターネット又はＭＡＮやＷＬＡＮなどのネットワークを介してｅＳＩＭ配信をサポートするオペレーティングシステム・コンポーネントの配信のための装置を含む。

【００１７】

本発明の他の特徴及び優位な点は、添付の図面及び後述する例示の実施例の詳細な記載を参照することによって、当業者であれば直ちに理解されるであろう。

【図面の簡単な説明】

【００１８】
【図１】図１は、従来の（ＵＳＩＭ）を用いた、一典型的な認証及びキー合意（ＡＫＡ）の手順をグラフィカルに示した図である。
【図２】図２は、本発明に従うソフトウェア・エンティティ（例えば、ユーザ装置（ＵＥ）、サードパーティソフトウェアベンダー、ＳＩＭベンダーなど）に対するデバイス・キーの組を割り当てる方法の一実施例を示した論理フロー図である。
【図３】図３は、本発明の一実施例に従うＵＥ及びソフトウェアベンダー間の欄ライムコンポーネントのセキュアな配信に関する典型的なトランザクションをグラフィカルに示した図である。
【図４】図４は、本発明に従うｅＳＩＭのセキュアな実行に関する一実施例をグラフィカルに示した図である。
【図４Ａ】図４Ａは、本発明に従う、ブートストラップＯＳ、ｅＵＩＣＣ、及びｅＳＩＭアーキテクチャの一実施例をグラフィカルに示した図である。
【図５】図５は、アクセス制御クライアントによる使用に関して、セキュアな修正、及びコンポーネントの記憶のための一般化した方法の一実施例を示した論理フロー図である。
【図６】図６は、本発明に従うアクセス制御クライアントによる使用に関して、コンポーネントのセキュアな実行のための一般化した方法の一実施例を示した論理フロー図である。
【図７】本発明の方法を具現化するのに有用な典型的装置のブロック図である。（全図の著作権は２０１０アップル社にあり、全ての権利を保有する）
【発明を実施するための形態】
【００１９】
全体を通して同じ部分が同じ番号で示された添付図面を参照して説明する。
【００２０】
概略
本発明は、とりわけ、ユーザ装置及び使用されたサードパーティエンティティが相互に互いを検証するセキュアな方法及び装置を提供する。また、ユーザ装置が設置された後であっても、任意のサードパーティエンティティが信用されることができる方法及び装置を開示する。例えば、携帯デバイス（ＵＭＴＳ　ＵＥなど）は、サードパーティエンティティｅＳＩＭ（例えば、仮想的若しくは電気的なＳＩＭ、ここでは“ｅＳＩＭ”と呼ぶ。）ベンダーを識別し、そして信用されたダイアログがそのｅＳＩＭを購入し、獲得し、更新することを開始することができる。同様に、サードパーティエンティティｅＳＩＭベンダーは、ＵＥが信用されたデバイスであり、そして配信のためのそのｅＳＩＭをセキュアにエンコードすることを検証することができる。信用されたダイアログは、固有のデバイス鍵及び承認証明に基づく。後述するとおり、一実施例において、そのデバイス鍵は公開／秘密鍵による暗号化方法に基づいている。
【００２１】
本発明の様々な態様は、アクセス制御クライアントのセキュアな受信に（全部又は一部）向けられている。ネットワークオペレーションに関するアクセス制御部の反応しやすい特性のせいで、既存の解決法は物理的なカード形式のファクターを使用することを好んでいた。しかしながら、本発明は、仮想的若しくは電気的なアクセス制御クライアント（例えば、ｅＳＩＭ）のセキュアな配信を都合良く提供し、これにより、物理的カード及び関連する制限に関する要求を取り除くものである。
【００２２】
さらに、既存の解決法と異なり、本発明は、あらかじめ存在するアクセス制御クライアント無しに、アクセス制御クライアント部の配信を可能にする。これにより、ユーザの柔軟性及び使用経験を格段に拡大することになる。
【００２３】
本発明の他の態様において、デバイス（例えば、携帯ユーザデバイス）はマルチ記憶されたアクセス制御クライアント（例えば、ｅＳＩＭ）の一つを起動（アクティベート）し

、実行することができる。特に、ｅＳＩＭをローディングするとき、オペレーティングシステム（ＯＳ）は最新のランタイム環境に必要なソフトウェアのリストをロードするだけでよい。この、いわゆる“サンドボックス”の効果は、マルチｅＳＩＭが、他のｅＳＩＭに不適切にアクセスすることなしに同一のデバイス内に用いられ得ることを保証する。

【００２４】

典型的な実施形態の詳細な説明

本発明の典型的な実施形態を以下に詳細に説明する。これら実施例及び態様は、主として、ＧＳＭ（登録商標）、ＧＰＲＳ／ＥＤＧＥ、ＵＭＴＳセルラーネットワークの加入者識別モジュール（ＳＩＭ）に関して説明するが、当業者であれば、本発明がこれらに限定されないことが明らかであろう。実際、本発明の種々の態様は、セキュアな修正、アクセス制御エンティティ又はクライアントの記憶及び実行から利益が得られる任意の無線ネットワーク（セルラーであってもなくても）において有用である。

【００２５】

また、「加入者識別モジュール」という語は、ここでは、ｅＳＩＭと称するが、これは、必ずしも、（ｉ）加入者それ自体による使用（即ち、本発明は、加入者又は非加入者により実施される）、（ii）１人の個人のアイデンティティ（即ち、本発明は、家族のような個人のグループ、若しくは企業のような無形又は架空のエンティティのために実施される）、又は（iii）任意の有形の「モジュール」装置又はハードウェアを意味せず又は要求もしないことが理解されるであろう。

【００２６】

従来の加入者識別モジュール（ＳＩＭ）のオペレーション

典型的な従来のＵＭＴＳセルラーネットワークの状況において、ユーザ装置（ＵＥ）は、携帯装置及びユニバーサル加入者識別モジュール（ＵＳＩＭ）を備えている。このＵＳＩＭは、記憶され且つ物理的ユニバーサル集積回路カード（ＵＩＣＣ）から実行される論理的ソフトウェア・エンティティである。加入者情報、無線ネットワークサービスを得るためにネットワークオペレータとの認証に使用されるキー及びアルゴリズムのような種々の情報がこのＵＳＩＭに記憶される。

ＵＳＩＭソフトウェアは、Ｊａｖａカード（登録商標）プログラミング言語に基づいている。Ｊａｖａカードは、内蔵型“カード”タイプのデバイス（例えば、上述したＵＩＣＣ）のために修正されたＪａｖａ（登録商標）プログラミング言語のサブセットである。

【００２７】

一般的に、ＵＩＣＣは、加入者への配信の前にＵＳＩＭでプログラムされ、再プログラミング又は「パーソナル化」は、各ネットワークオペレータ特有のものである。例えば、配備の前に、ＵＳＩＭは、インターナショナルモバイル加入者識別ファイア（ＩＭＳＩ）、固有の集積回路カード識別子（ＩＣＣ－ＩＤ）、及び特定の認証キー（Ｋ）に関連付けられる。ネットワークオペレータは、その関連性を、ネットワーク認証センター（ＡｕＣ）内に収容されたレジストリーに記憶する。パーソナル化の後に、ＵＩＣＣは、加入者へ配布することができる。

【００２８】

図１には、上述した従来のＵＳＩＭを使用する１つの典型的な認証及びキー合意（ＡＫＡ）手順１００が詳細に示されている。通常の認証手順の間に、ＵＥ１０２は、ＵＳＩＭ１０４からインターナショナルモバイル加入者識別ファイア（ＩＭＳＩ）を取得する。ＵＥは、それを、ネットワークオペレータのサービングネットワーク（ＳＮ）１０６又は訪問先コアネットワークへ渡す。ＳＮは、認証要求をホームネットワーク（ＨＮ）のＡｕＣ１０８へ転送する。ＨＮは、受信したＩＭＳＩをＡｕＣのレジストリーと比較し、そして適当なＫを得る。ＨＮは、ランダム番号（ＲＡＮＤ）を発生し、そしてそれに、予想される応答（ＸＲＥＳ）を生成するためのアルゴリズムを使用してＫでサインする。ＨＮは、更に、暗号化及び完全性保護に使用するための暗号キー（ＣＫ）及び完全性キー（ＩＫ）、並びに認証トークン（ＡＵＴＮ）を、種々のアルゴリズムを使用して発生する。ＨＮは、ＲＡＮＤ、ＸＲＥＳ、ＣＫ及びＡＵＴＮより成る認証ベクトルをＳＮへ送信する。ＳＮ

は、認証ベクトルを一回の認証プロセスのみに使用するために記憶する。ＳＮは、ＲＡＮＤ及びＡＵＴＮをＵＥへ渡す。

【００２９】

ＵＥがＲＡＮＤ及びＡＵＴＮを受け取ると、ＵＳＩＭは、受け取ったＡＵＴＮが有効であるかどうか検証する。もしそうであれば、ＵＥは、受け取ったＲＡＮＤを使用し、記憶されたＫ、及びＸＲＥＳを発生した同じアルゴリズムを使用して、それ自身の応答（ＲＥＳ）を計算する。ＵＥは、ＲＥＳをＳＮへ返送する。ＳＮは、ＸＲＥＳを受け取ったＲＥＳと比較し、それらが一致する場合に、ＳＮは、オペレータのワイヤレスネットワークサービスの利用についてＵＥを認証する。

【００３０】

典型的な動作

本発明の様々な態様が典型的な一実施例に関して記載されている。本発明の典型的な実施形態の状況では、従来のように物理的なＵＩＣＣを使用するのではなく、ＵＩＣＣは、例えば、ＵＥのセキュアなエレメント（例えば、セキュアなマイクロプロセッサ又は記憶装置）内に収容されるソフトウェアアプリケーション、以下、電子ユニバーサル集積回路カード（ｅＵＩＣＣ）と称される、のような仮想又は電子的エンティティとしてエミュレートされる。ｅＵＩＣＣは、以下、電子的加入者識別モジュール（ｅＳＩＭ）と称される複数のＵＳＩＭエレメントを記憶し管理することができる。各ｅＳＩＭは、典型的なＵＳＩＭと同じ論理的エンティティを収容する。ｅＵＩＣＣは、ｅＳＩＭのＩＣＣ－ＩＤに基づいてｅＳＩＭを選択する。ｅＵＩＣＣが望ましいｅＳＩＭを選択すると、ＵＥは、認証手順を開始して、ｅＳＩＭの対応するネットワークオペレータからワイヤレスネットワークサービスを得ることができる。さらに、各ｅＳＩＭアプリケーションは、一般的に、上述したＵＳＩＭ、ＣＳＩＭ、ＩＳＩＭ、ＳＩＭ、ＲＵＩＭなどのアクセス制御クライアントを包含する。各ｅＳＩＭはユーザアカウントに関連し、その結果、“ｅＳＩＭ”はマルチアクセス制御クライアントを広範囲に包含することを理解されたい（例えば、ユーザはＵＳＩＭ、及び同じｅＳＩＭアカウントに関連するＳＩＭをもつかもしれない）。

【００３１】

前に示唆したとおり、従来のＵＳＩＭの上記した手順は、コアネットワーク（例えば、上述したホームネットワーク（ＨＮ）、サービングネットワーク（ＳＮ）、認証センター（ＡｕＣ）など）に対して認証するための予め共有化された鍵を使用する。したがって、ＵＳＩＭ手順は、ネットワークオペレータにとって必ず“閉じた”システムである。その理由は、予め共有化された鍵はクローズに保護されなければならないからである。これに対して、本発明はｅＵＩＣＣ及び互いに相互信用する任意のサードパーティ・エンティティ（機関）のためのセキュアな方法を提供し、そしてユーザ装置が設定された後であっても任意のサードパーティが信用されるようになることができるようにする。

【００３２】

よって、本発明は、幾つかの点において、かなり複雑なセキュリティ要求を有すると共に、一層の柔軟性を好都合に提示するものである。さらに、当業者であれば、本発明の様々な態様が“仮想”ソフトウェア構成（例えば、ｅＵＩＣＣ、ｅＳＩＭ）による使用から利益を生じながら、その利益はこれらの仮想の実施例に限定されるものではないことが認識されるであろう。事実、ここで述べた原理は、セキュアな修正や記憶、そしてとりわけ物理的カードメディア、専用セキュリティハードウェアなどの中に組み込まれたアクセス制御クライアントの実行に同じように適用可能である。

【００３３】

信用性のある通信の確立

図２は、ソフトウェア・エンティティ（例えば、ｅＵＩＣＣ、サードパーティソフトウェアベンダー、ＳＩＭベンダーなど）にデバイス・キーの組を割り当てるための典型的な一実施例である。ステップ２０２で、暗号化の公開／秘密鍵の組（例えば、ＲＳＡアルゴリズム）がソフトウェア・エンティティに割り当てられ、このソフトウェア・エンティティの物理的に保護されたセキュアな要素（例えば、ＵＥ内のｅＵＩＣＣ、サードパーティ

ソフトウェアベンダー内のセキュアなデータベース）内に記憶される。例えば、ｅＵＩＣＣは信用されたエンティティによってプログラム化されたり、或いは最初に製造／起動されるときに、公開／秘密鍵の組を内部に生成する。

【００３４】

公開／秘密鍵の組は、秘密のプライベート鍵及び公表可能な公開鍵に基づいている。公開／秘密鍵の組のスキームは、暗号化するために用いられる鍵と復号化するために用いられる鍵は異なり、その結果、暗号と復号は同一の鍵を共有しないので、“非対称”とみなされることである。一方、“対称”鍵のスキームは、暗号と復号の両方に同一の鍵（又は明らかに変換された鍵）を用いる。ＲＳＡアルゴリズムは、関連技術分野で普通に使用される公開／秘密鍵の組の暗号方法の一形式であるが、本発明はＲＳＡアルゴリズムに限定されるものではないことを理解されるであろう。

【００３５】

公開／秘密鍵の組のスキームは、メッセージを暗号化したり、及び／又は署名を生成するのに用いることができる。つまり、秘密鍵でメッセージを暗号化し、そして公開鍵で復号化する。これにより、メッセージは移送中に変更されないことが保証される。同様に、秘密鍵で生成された署名は公開鍵で検証され、署名を生成するエンティティは本物である。両方の使用において、秘密鍵は秘匿が維持され、公開鍵は自由に配布される。

【００３６】

ステップ２０４で、公開／秘密鍵の組のために承認証明が発行される。例えば、信用されたエンティティは、ｅＵＩＣＣ鍵の組に関する“承認証明”を発行することによって、ｅＵＩＣＣの認証性及び秘密鍵のセキュリティ性に対する証明を行う。この公開／秘密鍵の組は、今では、ｅＵＩＣＣのためのデバイス・キーの組である。

【００３７】

一実施例において、承認証明は、これに制限されるものではないが、(i)証明する認証機関に関する識別情報、(ii)デバイスに関する情報を識別すること、(iii)証明アルゴリズムを記述するメタデータ、及び／又は(iv)適切な公開鍵、をもつデータ集合を含む。これらのコンポーネントは、さらに承認者の秘密鍵によってサインされる。一実施例において、通常のオペレーションの間、このデジタル署名は、コンテンツがセキュアで改ざんされていないことを検証するために受信者によってチェックされる。

【００３８】

デバイス・キーの組は非対称であることから、公開鍵は秘密鍵との整合性を妥協することなく配信され得る。したがって、デバイス・キー及び証明は、それまで知られていなかったパーティ（例えば、ｅＵＩＣＣ、及びサードパーティ）との間での通信を保護し且つ検証するために用いられることができる。ｅＵＩＣＣとソフトウェアベンダー（図３に示す）との間のランタイムコンポーネントをセキュアに配信するための以下の典型的なトランザクションを考えることにする。

図３のステップ３０２で、ｅＵＩＣＣはサードパーティのｅＳＩＭベンダーからｅＳＩＭを要求する。以下の例はｅＳＩＭアプリケーションのセキュアな移動を記載するものであるが、ランタイム環境のアプリケーションにおける他の共通した例は、パッチや完全に特徴づけられたオペレーティングシステムなどを含む。

【００３９】

ステップ３０４で、サードパーティのｅＳＩＭベンダーは、承認証明からのｅＵＩＣＣに対応する公開デバイス・キーを受信する。例えば、承認証明はｅＵＩＣＣなどをクエリーするデータベースから得ることができる。ｅＵＩＣＣのもう一方の秘密鍵はこのプロセス中でサードパーティベンダーに決して都合よく露呈されることがないことを特に留意されたい。

【００４０】

サードパーティ３０５で、サードパーティのｅＳＩＭベンダーは、承認証明を検証する。一実施例において、承認証明は信用エンティティ（ＡＰＰＬＥ（Ｒ）のAssigneeなど）によって一義的に署名される。サードパーティのｅＳＩＭベンダーが承認証明を検証する

と、信用エンティティ（例えば、ＡＰＰＬＥ（Ｒ））及び機関がｅＵＩＣＣを信用して安全であることを、このサードパーティｅＳＩＭベンダーは保証することができる。

【００４１】

サードパーティ３０６で、ｅＳＩＭランタイム環境は暗号化され、ＵＥに対応する特別なｅＵＩＣＣのためのサードパーティソフトウェアベンダーによって署名される。別の実施例では、ｅＳＩＭランタイム環境は最初に署名され、次に暗号化される。典型的な一例の場合、ベンダーは自分のベンダー非対称の署名鍵及びＲＳＡ公開／秘密鍵、及び、ｅＳＩＭを書名するための証明チェーンを用い、そしてｅＳＩＭを暗号化するための一時的なすなわち当座の鍵を使用する。ｅＵＩＣＣのためのパッケージを準備しながら、当座の対象鍵はランダムに生成される。

【００４２】

サードパーティ３０８で、署名され且つ暗号化されたｅＳＩＭのランタイム環境は、サードパーティｅＳＩＭベンダーによって、（例えば、無線インタフェースなどを介して）配信のために複数のパッケージに分割される。例えば、署名され且つ暗号化されたｅＳＩＭは、通信リンクの質に適切なパケットに分割されサイズ調整される（パッケージされた配信は関連技術分野でよく知られた様々な好ましいエラー訂正スキームをサポートする）。

【００４３】

サードパーティ３１０で、一時的な対称鍵は、それを適当なｅＵＩＣＣ公開鍵などで暗号化することによってｅＵＩＣＣへ安全に渡される。ベンダー証明は平文として送信されたり、或いは暗号化される。一般的に、ベンダー証明は受信側の処理負担を軽減するためには暗号化されない（しかしながら、これはシステムの要求ではなく、暗号はすべてのケースか或いは選択的に適用されるケースの何れかで用いられる）。

【００４４】

サードパーティ３１２で、ｅＵＩＣＣはベンダー証明を検証する。ベンダーの公開署名鍵でベンダーの証明の検証が成功したことは、署名が改ざんされていないことの証拠をｅＵＩＣＣに提供する。

【００４５】

あるケースでは、ベンダー証明は外部の信用エンティティ（例えば、ＭＮＯ）によってさらに署名されることを含む。このベンダー証明が有効であれば、ＵＥは一時的な対称鍵をその（ｅＵＩＣＣの）秘密鍵で復号する。上述した交換が成功して終了したことは、ｅＵＩＣＣとサードパーティエンティティ間の経路が安全であること、そして更なるデータトランザクションのための一時的な共通対象鍵で暗号化されることを保証する。

【００４６】

したがって、サードパーティ３１４で、暗号化されたパッケージのかたまりはセキュアに受信され、再アセンブルされ、そしてＵＩＣＣによって復号化されることができる。この特別な例において、ｅＵＩＣＣはｅＳＩＭに関するパッケージをダウンロードする。

【００４７】

一実施例において、ベンダー証明、鍵、及び暗号パッケージは一緒に送信される。別の実施例では、他のパラダイムを用いる。例えば、ベンダー証明及び鍵を送信し、最初にセキュアな接続を確立してから、このセキュア接続上で暗号化されたパッケージの送信を開始する。

【００４８】

本発明の典型的な実施例は、ｅＳＩＭをｅＵＩＣＣからの分離エンティティとして取り扱う。したがって、ｅＵＩＣＣは既存ｅＳＩＭの利益なしに、そしてたとえユーザ装置が配備された後であっても、サードパーティエンティティへセキュアな接続を確立することができる。

【００４９】

典型的なｅＵＩＣＣは、ｅＳＩＭのセキュアな配信を可能にし、その結果、サードパーティｅＳＩＭベンダーによってｅＳＩＭを携帯端末へ、既存ＳＩＭ　ＡＫＡ手順上でそれ

までの信頼がなくても配信することを可能にする。

【００５０】

もっと明確に言えば、デバイスは個々の非対称なデバイス・キーの組をもち、それは単一のｅＳＩＭ（及びｅＳＩＭを発行するＭＮＯ）に関連する対称鍵から独立している。ｅＳＩＭとｅＵＩＣＣ間の差異は、デバイスオペレーティングシステムの複雑さに対する重要な反響を有する。

【００５１】

セキュアなパーティションの実行

これまで示唆してきたとおり、物理的ＵＩＣＣのための既存解決法は単一のＵＳＩＭエンティティを包含する。しかしながら、当業者であれば、本発明の様々な態様は、既存の複数のアクセス制御クライアントのプロファイルを記憶し実行することに容易にあてはまることを認識するであろう。したがって、本発明の他の実施例において、ｅＵＩＣＣはネットワーク及びｅＳＩＭの両方の有効性を決定しなければならない。上述したタスクの複雑さのせいで、従来のＳＩＭアーキテクチャは初期化にもはや十分とは言えない。むしろ、本発明の一実施例において、ブートストラップオペレーティングシステム（ＯＳ）は“共通の”又は“常駐する”オペレーティングシステムをロードする。この共通ＯＳは適当なｅＳＩＭをロードし、ロードされたｅＳＩＭは前に述べた認証及びキー合意（ＡＫＡ）手順を実行することができる。

【００５２】

詳細に言うと、本発明の、ブートストラップＯＳは、一実施例において、暗号の検証、復号化、共通ＯＳのロード、起動されたｅＳＩＭに関連するすべてのパッチに責任を負っている。ブートストラップＯＳは仮想ソフトウェアｅＵＩＣＣ上で実行され、したがってｅＳＩＭ及び関連する共通のＯＳは“サンドボックス”化される。それらはｅＵＩＣＣを通じて利用可能に行われる適当なパッチにアクセスすることだけができる。例えば、一実施例において、ｅＵＩＣＣだけがｅＳＩＭと同じ署名を共有するパッチを可能にする。

【００５３】

図４を参照すると、ｅＳＩＭのパーティションをセキュアに実行する一例としての方法が記載されている。

【００５４】

サードパーティ４０２で、ｅＵＩＣＣはチップレストで、ブートストラップＯＳを開始する。サードパーティ４０４で、ブートストラップＯＳはランタイム環境で開始する権利が付与されたパッチリストを解析する。例えば、ブートストラップＯＳはデフォルトのネットワーク、及びその関連するパッチを識別する。これらパッチの少なくとも１つは共通ＯＳであり、他のパッチはアクティブなｅＳＩＭ、及びｅＳＩＭに関連する追加パッチを含む。

【００５５】

ステップ４０６で、ブートストラップＯＳは、例えば、証明書を解析することによって、又は他の手段によって、パッチの整合性を検証する。例えば、一実施例において、信用エンティティ（例えば、レコードの譲受け人）は証明書を発行したり、そうでなければ署名チェーンの信用元として機能することになろう。パッチが正しく署名されたら、ブートストラップＯＳはそのパッチを実行することができる。適切なｅＳＩＭに対応する検証された唯一のパッチがロードされる（他のパッチは記憶されるが、“サンドボックス”内で実行されはしない）。

【００５６】

ステップ４０８で、ブートストラップＯＳは共通ＯＳを開始する。共通ＯＳはｅＳＩＭと残りのハードウェアとの間のインタフェースを提供する。共通ＯＳは、一般的には特別なｅＳＩＭに特有のＵＩＣＣをエミュレートする入力及び出力機能を提供する。一般的に、これはファイル入出力（ＩＯ）などの機能を含む。

【００５７】

その後、ステップ４１０で、共通ＯＳは適当なｅＳＩＭを実行することができる。図４

Ａは、ブートストラップＯＳ４５２、共通ＯＳ４５４、ｅＳＩＭ４５６との間のソフトウェア関係４５０を示す。なかでも注目すべきは、（図４及び４Ａに示した）典型的な実施例において、異なるｅＳＩＭプロファイルがそれら自身の共通ＯＳ内でオペレートするということである。異なるｅＳＩＭプロファイルのためのランタイム環境を個々のサンドボックスに分けることによって、上述した実施例はレガシーなＳＩＭアーキテクチャとの互換性を好都合にそのまま残すが、本発明の利益を活用する。一般的に、各ｅＳＩＭがそれぞれの環境内で実行することを保証することによって、既存のＳＩＭソフトウェアは直接的に仮想化され得る。さらに、サンドボックスは、他のｅＳＩＭの存在が逆の相互作用を生じさせないことを保証する。それはサードパーティｅＳＩＭベンダーの広範囲な分布をサポートするのに必要な要求（例えば、正規のプロトコル、及び能力をもつこと）である。

【００５８】

上述したように、上述した議論はＳＩＭベースのネットワークテクノロジー及び特徴に主に基づいている。それゆえに、本発明の１以上の態様を実行する一般方法及び装置の典型的な実施例の記載を、ここで提示する。

-方法-

図５を参照すると、セキュアな修正及びアクセス制御クライアントで使用される記憶コンポーネントに関する一般方法５００の実施例が示される。

【００５９】

サードパーティ５０２で、アクセス制御クライアントで使用される１以上のコンポーネントが要求されたり、提案されたりする。一実施例において、１以上のコンポーネントは、全体として或いは一部に、(i)共通オペレータシステム、(ii)少なくとも１つのｅＳＩＭ、及び／又は(iii)ｅＳＩＭに関連する１以上のパーソナリゼーション・パッチ、を含む。他の技術的な応用においては、このパッケージは、ＣＤＭＡ加入者識別モジュール（ＣＳＩＭ）、ＩＰマルチメディアサービス識別モジュール（ＩＳＩＭ）、加入者識別モジュール（ＳＩＭ）、除去可能ユーザ識別モジュール（ＲＵＩＭ）などに関連し得る。本発明の開示、ここで記載した方法及び装置の修正があたえられるとき、当業者であれば、様々な類似の構造の殆ど制限のない置換を認識するであろうし、本開示に基づき当業者の常識内に上手くそのような類似構造や置換が収まることになろう。

【００６０】

一実施例において、デバイスによって若しくはデバイスに関連する加入者によって、すなわち、肯定的な通信又は要求を発行するデバイス／ユーザによって、１以上のコンポーネントを要求したり、“プル”する。別の実施例では、１以上のコンポーネントはデバイスに対して割り当てられたり、“プッシュ”される。すなわち、肯定的な通信又は要求はなく、むしろ他の幾つかの基準又はスキーム（例えば、周期的にイベントの発生に基づくなど）に従う。１以上のコンポーネントの存在は広告され、そうでなければブロードキャストされたり、アクセス若しくはサーチされ得るレポジトリに記憶される。

【００６１】

別の実施例では、１以上のコンポーネントはクエリーされたり、そうでなければ１以上の文脈（コンテクチュアル）イベント（例えば、特定エリアを入力する、特定使用を超過するデバイス）によってトリガーされる。

【００６２】

この要求又は提示は信用パーティを起源にもつ署名や証明も含むことができる。他の代替の例において、この要求又は提示は暗号法のチャレンジを含む。さらに別の例では、要求又は提示は認証を決定する手段を含む（例えば、パスワード認証に基づくユーザインタフェースなど）。

【００６３】

また、要求又は提示はトランザクションキーを含む。一つの変形例として、このトランザクションキーは一時的なキーである。依然として、他の持続性トランザクションキーがインプリメントされ得る。例えば、そのキーは複数のトランザクションセッションや複数

のユーザについて同一のものであったりする。他の変形例では、トランザクションキーは対称鍵であるか、若しくは非対称鍵である。

【００６４】

ステップ５０４で、要求又は提示は信ぴょう性のために検証される。一実施例において、信用パーティから由来した署名又は証明は有効性についてチェックされる。或いはまた、署名又は証明の有効性は、自明の理であるか、そうでなければ信用パーティへの再分類なしに、認証者によって発見可能である。他のスキームは加入者入力、例えば、ユーザ名及びパスワード入力又は単純な肯定承認スキームに依存する。

【００６５】

検証が成功することは、１以上のチャレンジ応答の交換を要求するよう構成される。幾つかの変形例では、検証は一方向性（例えば、処理者の一方だけが検証される）、若しくは双方向性（例えば、処理者双方が成功しなければならない）である。他のスキームにおいては、検証は帯域外（例えば、別の通信経路経由）若しくは加入者支援を介して実行される。

【００６６】

検証の成功は、セキュアなトランザクションに必要な１以上のパラメータに関する合意を生じさせる。例えば、一実施例において、１以上のトランザクションキーが確立される。幾つかの変形例では、トランザクションキーは検証後に生成される。代替例においては、このトランザクションキーは検証前に提案され生成され、その後に条件付きで使用される。

【００６７】

その後、ステップ５０６で、デバイスはアクセス制御クライアントに関連する１以上のパッケージを受信する。このパッケージは、セキュアな転送を保証するためにトランザクションキーでさらに暗号化される。一つの変形例では、このパッケージは非対称に暗号化される。すなわち、公開鍵でパッケージを暗号化する。他の変形例では以前に合意した共有鍵を用いて対称的にパッケージを暗号化する。或いは、識別可能な署名でパッケージをサインする。当該関連分野で知られた検証可能なパッケージ配信に関する他の無数の解決法が本発明に一致して用いられる。

【００６８】

ステップ５０８で、デバイスはパッケージをアセンブルし、そして１以上のコンポーネントに復号する。一実施例において、その１以上のコンポーネントは適当な共通オペレーティングシステムに関連する。例えば、上述したように、パッチは少なくとも１つのｅＳＩＭ、及び／又は、上述したようなｅＳＩＭに関連するパーソナリゼーション（個人）パッチを含む。ステップ５０８の結論で、１以上のコンポーネントは成功し、ターゲットデバイスに安全に移動される。

【００６９】

図６を参照すると、アクセス制御クライアントで使用される記憶コンポーネントのセキュアな実行に関する一般方法６００の実施例が示される。ステップ６０２で、アクセス制御クライアント及び１以上のパッチが識別される。一実施例において、アクセス制御クライアント及び１以上の関連パッチは、オペレーティングシステムによって選択される。一つの具現化例では、このオペレーティングシステムは、単純なブートストラップオペレーティングシステムから更にブート化される。

【００７０】

一つのコンフィグレーションにおいて、ブートストラップオペレーティングシステムは複数のセキュアなパーティションを維持し、各パーティションは他のパーティションとは離れていて、そしてメモリパーティションから実行されるソフトウェアはアクセスすることができないか、又は他の関係のないパーティションによってアクセスされることができない。例えば、典型的なデバイスは単純なブートストラップＯＳを実行する。この単純なブートストラップＯＳは共通ＯＳ、その関連したｅＳＩＭ、パッチを、単一の“サンドボックス”パーティションにロードし実行する。

【００７１】
本発明の様々な実施例は、１以上のカテゴリーに従い、利用可能なコンポーネント及びパッチの全マニフェストを分ける。一応用例では、コンポーネント及びパッチは、共通の署名又は信用元に従い関連付けられる。例えば、あるシナリオの場合、単純なブートストラップＯＳは共通ＯＳを許可だけ行い、ｅＳＩＭは同一のｅＳＩＭベンダーによって実行のためサインされる。別の応用例では、コンポーネント及びパッチは、ユーザ選択或いは様々なレベルの信用に従い関連される。例えば、様々なコンポーネントは個々の協調的エンティティ（例えば、信用されたｅＳＩＭベンダー、信用ネットワーク・パーソナリゼーションなど）からまき散らされる。
【００７２】
方法６００のステップ６０４で、アクセス制御クライアント及び関連パッチはオペレーションのために検証される。一実施例において、アクセス制御クライアント及び関連パッチは完全（整合）性のためにチェックされる。すなわち、それらが改ざんされたり変更されたりしていないことである。このような完全性のチェックに関する共通の方法は、チェックサム、暗号ハッシュ、剰余などを含む。パッチ認証を検証する他の解決法は、証明の検証、ステータスの検証を含む。
【００７３】
ステップ６０６で、検証されたアクセス制御クライアントが実行される。ローディング及び実行が成功すると、アクセス制御クライアントは関連ネットワークのために初期アクセス制御手順を実行する。例えば、検証されたｅＳＩＭは認証及びキー合意（ＡＫＡ）手順を実行する。
【００７４】
典型的な移動装置
図７には、本発明の方法を具現化するのに有用な典型的なユーザ又はクライアント移動装置７００が示されている。
【００７５】
図７の典型的ＵＥ装置は、デジタル信号プロセッサ、マイクロプロセッサ、フィールドプログラマブルゲートアレイ、又は１つ以上の基板にマウントされた複数の処理コンポーネントのようなプロセッササブシステム７０２を伴うワイヤレス装置である。この処理サブシステムは、内部キャッシュメモリも含む。又、処理サブシステムは、例えば、ＳＲＡＭ、フラッシュ及びＳＤＲＡＭコンポーネントを含むメモリを備えたメモリサブシステム７０４に接続される。このメモリサブシステムは、この技術でよく知られたように、データアクセスを容易にするために１つ以上のＤＭＡタイプのハードウェアを具現化することができる。又、メモリサブシステムは、プロセッササブシステムにより実行できるコンピュータ実行可能なインストラクションを含む。
【００７６】
１つの典型的な実施形態において、装置は、１つ以上のワイヤレスネットワークに接続するようにされた１つ以上のワイヤレスインターフェイス（７０６）で構成される。これら複数のワイヤレスインターフェイスは、適当なアンテナ及びモデムサブシステムを具現化することにより、ＧＳＭ、ＣＤＭＡ、ＵＭＴＳ、ＬＴＥ／ＬＴＥ－Ａ、ＷｉＭＡＸ、ＷＬＡＮ、ブルーツース、等の異なる無線技術をサポートすることができる。
【００７７】
ユーザインターフェイスサブシステム７０８は、これに限定されないが、キーパッド、タッチスクリーン（例えば、マルチタッチインターフェイス）、ＬＣＤディスプレイ、バックライト、スピーカ及び／又はマイクロホンを含む多数の良く知られたＩ／Ｏを含む。しかしながら、あるアプリケーションでは、これらコンポーネントの１つ以上が除去されてもよいことが明らかである。例えば、ＰＣＭＣＩＡカードタイプクライアントの実施形態では、ユーザインターフェイスが欠けてもよい（それらが物理的及び／又は電気的に結合されるホスト装置のユーザインターフェイスに便乗させることができるので）。
【００７８】

ここに示す実施形態では、ｅＵＩＣＣアプリケーションを含んでいてそれを動作するセキュアなエレメント７１０を装置が備えている。このｅＵＩＣＣは、複数のアクセス制御クライアントを記憶しそしてネットワークオペレータとともに認証に用いられる複数のアクセス制御クライアントにアクセスすることができる。セキュアなエレメントは、プロセッササブシステムの要求時にメモリサブシステムによりアクセスすることができる。

【００７９】

典型的な実施例において、セキュアなエレメントは少なくともパーティション可能なメモリを含み、このパーティション可能なメモリは１以上のアクセス制御クライアント及び関連パッチを含むように適合される、各パーティションは他のパーティションから離れて維持され、メモリパーティションから実行されたソフトウェアはアクセスできなかったり、他の無関係なパーティションによってアクセスされない。

【００８０】

また、このセキュアな要素は、いわゆる“セキュアマイクロプロセッサ”又はセキュリティ分野でよく知られたタイプのＳＭを含む。

【００８１】

さらに、実施例の様々な現実化においては、実行時に、単純なブートストラップオペレーティングシステム（ＯＳ）を開始する命令を含む。ブートストラップオペレーティングシステム（ＯＳ）は、セキュアなエレメントからの少なくとも１つのパーティションを選択し、そこにロードされるべき適当なアクセス制御クライアントをロードするよう更に構成される。様々な具現化において、アクセス制御クライアントは信用署名に関連する１以上の証明を提供する。ブートストラップＯＳはアクセス制御クライアントの実行前に証明を検証する。

【００８２】

さらに、一実施例において、セキュアなエレメントは記憶されたアクセス制御クライアントのリスト又はマニフェストを保持する。マニフェストは記憶されたアクセス制御クライアントの現在ステータスに関する情報を含む。そのような情報は利用可能性、完全性、有効性、以前に経験したエラーなどを含む。マニフェストは、利用可能なアクセス制御クライアントのユーザ選択を可能にするため、ユーザインタフェースにリンクされたり、結合されたりする。

【００８３】

図７を参照すると、セキュアなエレメント７１０は、ネットワークオペレータによって認証に関する１以上のアクセス制御クライアントで使用されるコンポーネントを受信し且つ記憶することができる。一実施例において、セキュアなエレメントは関連するデバイス・キー及び承認証明を有する。このデバイス・キーはそれまで知られていないパーティ間（例えば、ＵＥ、及びサードパーティ）の通信を保護し且つ検証するのに用いられる。

【００８４】

一実施例において、デバイス・キーは非対称な公開／秘密鍵の組である。一方の公開鍵は秘密鍵の整合を妥協することなく、自由に配信されることができる。例えば、デバイスはＲＳＡ公開／秘密鍵が割り当てられ（又は内部で生成され）る。この公開鍵は配備後の通信で利用可能に作られる。

【００８５】

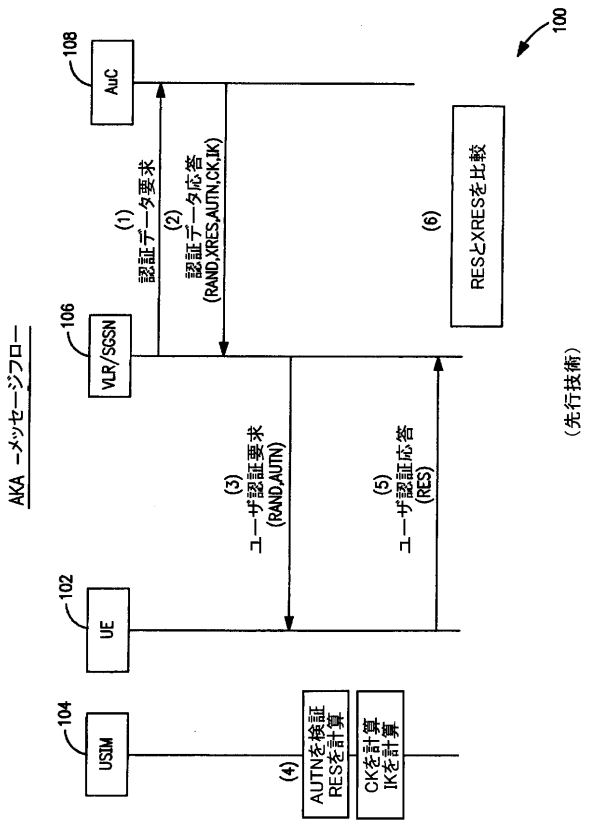
さらに、幾つかの変形例で、承認証明が信用エンティティに関連するデジタル署名で一義的にサインされる。一つの典型的なシナリオでは、承認証明はサードパーティエンティティによって検証され、そして装置との整合の証明を提供する。

【００８６】

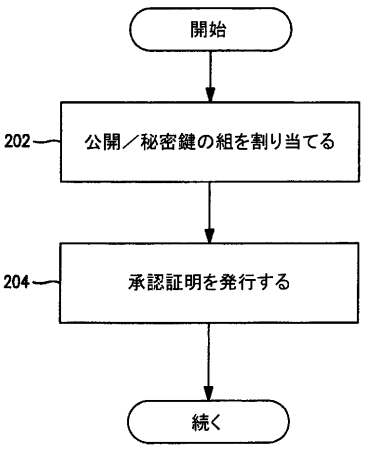
セキュアなエレメントをプログラミングするための方法及び装置はＲＳＡ鍵の組に関して例示したが、当業者であれば、他の認証スキームが同様に置き換えられることが容易に理解されるであろう。例えば、他の変形例では、デバイス・キーは共有鍵であり、この共有鍵の配布は高度に保証される。他の実施例は暗号交換というよりも証明に基づくこともある。

【００８７】
本発明の幾つかの態様を、方法ステップの特定のシーケンスに関して説明したが、これらの説明は、本発明の広い方法を例示するものに過ぎず、特定の用途により要求されるように変更できることが認識されよう。あるステップは、ある状況のもとでは、不要とされるか又は任意とされる。更に、ここに開示する実施形態にあるステップ又は機能を追加してもよいし、又は２つ以上のステップの実行順序を入れ替えてもよい。このような全ての変更は、ここに開示する本発明に包含されると考えられる。
【００８８】
以上、種々の実施形態に適用された本発明の新規な特徴が図示され、説明され及び指摘されたが、当業者であれば、本発明から逸脱せずに、装置又はプロセスの形態及び細部に種々の省略、置き換え及び変更がなされ得ることが理解されよう。以上の説明は、本発明を実施するよう現在意図される最良の態様である。この説明は、何ら限定を意図しておらず、本発明の一般的な原理の例示と考えるべきである。本発明の範囲は、特許請求の範囲によって限定される。

【図１】

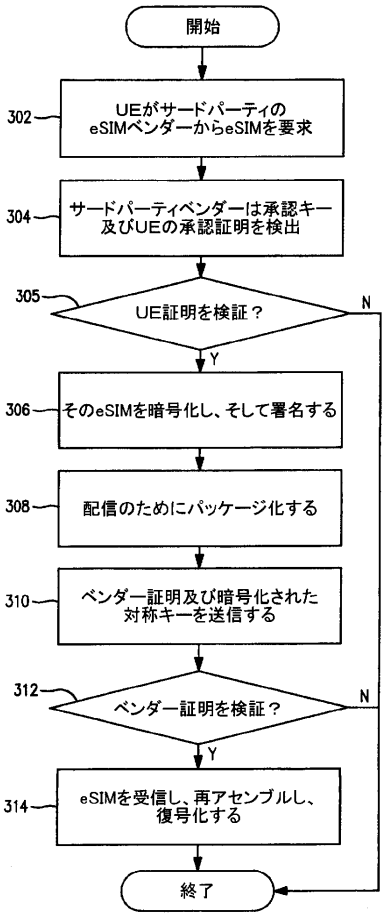


【図２】

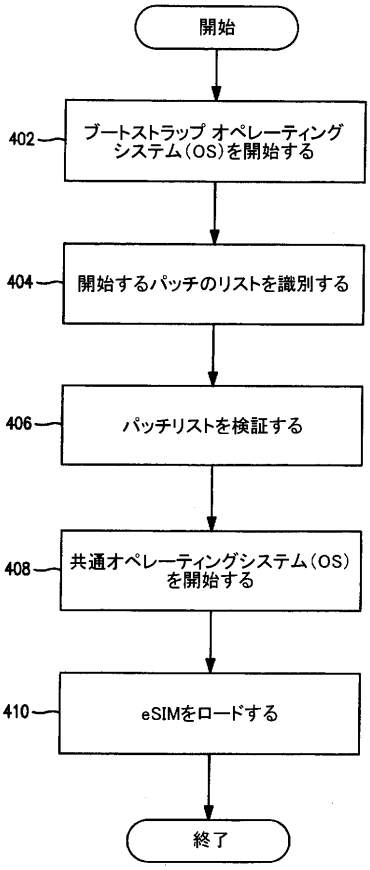


（先行技術）

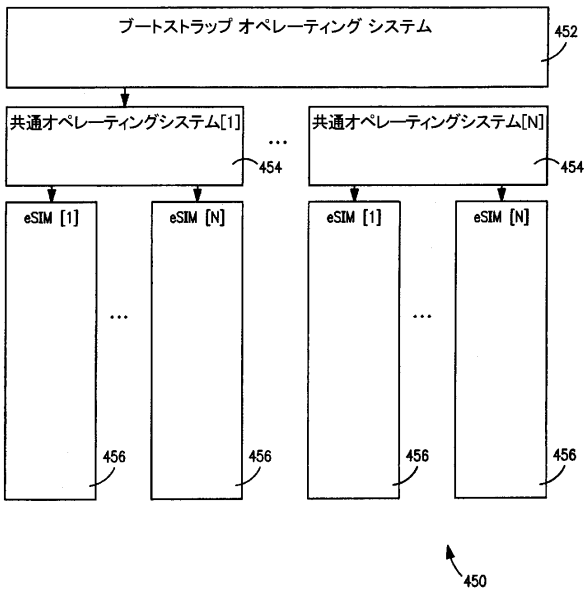
【図３】


開始
302
UEがサードパーティの
eSIMベンダーからeSIMを要求
304
サードパーティベンダーは承認キー
及びUEの承認証明を検出
305
UE証明を検証？
N
Y
306
そのeSIMを暗号化し、そして署名する
308
配信のためにパッケージ化する
310
ベンダー証明及び暗号化された
対称キーを送信する
312
ベンダー証明を検証？
N
Y
314
eSIMを受信し、再アセンブルし、
復号化する
終了

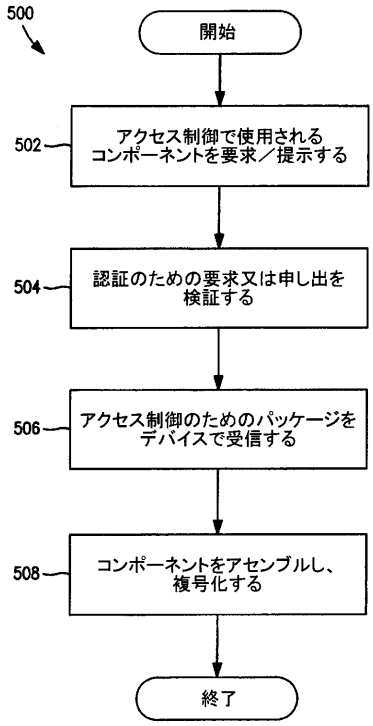
【図４】


開始
402
ブートストラップ オペレーティング
システム(OS)を開始する
404
開始するパッチのリストを識別する
406
パッチリストを検証する
408
共通オペレーティングシステム(OS)
を開始する
410
eSIMをロードする
終了

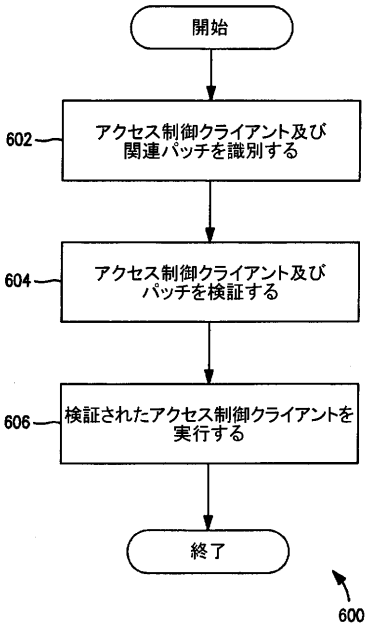
【図４Ａ】


ブートストラップ オペレーティング システム
452
共通オペレーティングシステム[1]
共通オペレーティングシステム[N]
454
454
eSIM [1]
eSIM [N]
eSIM [1]
eSIM [N]
456
456
456
456
450

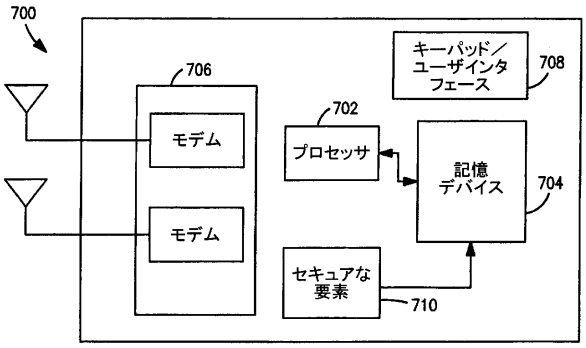
【図５】


500
開始
502
アクセス制御で使用される
コンポーネントを要求／提示する
504
認証のための要求又は申し出を
検証する
506
アクセス制御のためのパッケージを
デバイスで受信する
508
コンポーネントをアセンブルし、
複号化する
終了

【図６】


開始
602
アクセス制御クライアント及び関連パッチを識別する
604
アクセス制御クライアント及びパッチを検証する
606
検証されたアクセス制御クライアントを実行する
終了
600

【図７】


700
706
モデム
モデム
キーパッド／ユーザインタフェース
708
702
プロセッサ
記憶デバイス
704
セキュアな要素
710

フロントページの続き

(74)代理人 100122563
弁理士 越柴 絵里
(72)発明者 ステファン ブイ シェル
アメリカ合衆国 ９５０１４ カリフォルニア州 クパチーノ インフィニット ループ １ エムエス ３５－２エムピー
(72)発明者 ジェロルド フォン ハウク
アメリカ合衆国 ９５０１４ カリフォルニア州 クパチーノ インフィニット ループ １ エムエス １１１－エイチオーエム

審査官 松野 吉宏

(56)参考文献 国際公開第２０１０／１０２２３６（WO，Ａ２）
国際公開第２００９／１２６０８３（WO，Ａ１）
特開２００６－１５４９９７（ＪＰ，Ａ）
特開２００２－２７１２６１（ＪＰ，Ａ）
特開２０１０－１１７９９７（ＪＰ，Ａ）
Feasibility Study on Remote Management of USIM Application on M2M Equipment;(Release 8), 3GPP TR 33.812 V0.3.0(2008-05), フランス, 3GPP, ２００８年 ６月 ６日, paragraph 5.2.2.3.1,5.2.2.3.2, ＵＲＬ, http://www.3gpp.org/ftp/Specs/archive/33_series/33.812/33812-030.zip

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ ７／２４ － ７／２６
Ｈ０４Ｗ ４／００ － ９９／００
Ｈ０４Ｌ ９／３２