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

特許第4475596号
(P4475596)

(45)発行日　平成22年6月9日(2010.6.9)　(24)登録日　平成22年3月19日(2010.3.19)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| G06F 21/20 | (2006.01) | G06F | 15/00 | 330A |
| H04W 12/06 | (2009.01) | H04Q | 7/00 | 183 |
| G09C 1/00 | (2006.01) | G09C | 1/00 | 640E |

請求項の数 33　(全 29 頁)

| | |
|---|---|
| (21)出願番号 | 特願2006-530754 (P2006-530754) |
| (86)(22)出願日 | 平成16年10月12日 (2004.10.12) |
| (65)公表番号 | 特表2007-508614 (P2007-508614A) |
| (43)公表日 | 平成19年4月5日 (2007.4.5) |
| (86)国際出願番号 | PCT/IB2004/003313 |
| (87)国際公開番号 | WO2005/036852 |
| (87)国際公開日 | 平成17年4月21日 (2005.4.21) |
| 審査請求日 | 平成18年4月25日 (2006.4.25) |
| (31)優先権主張番号 | 60/510,787 |
| (32)優先日 | 平成15年10月13日 (2003.10.13) |
| (33)優先権主張国 | 米国(US) |
| (31)優先権主張番号 | 10/960,641 |
| (32)優先日 | 平成16年10月8日 (2004.10.8) |
| (33)優先権主張国 | 米国(US) |

(73)特許権者　398012616
ノキア　コーポレイション
フィンランド　エフイーエンー０２１５０
エスプー　ケイララーデンティエ　４
(74)代理人　100127188
弁理士　川守田　光紀
(72)発明者　マリネン　ティー.　ヤリ
アメリカ合衆国カリフォルニア州９４０８６，サニーヴェイル，エス．フェアオークスアヴェニュー６５５，エイチ１０４番
(72)発明者　ナイヴェトン　ジェー.　ティモスィー
アメリカ合衆国カリフォルニア州９４１０３，サンフランシスコ，テハマストリート４６８，４番

最終頁に続く

(54)【発明の名称】異種ＩＰネットワークにおける認証のための装置および方法

(57)【特許請求の範囲】

【請求項１】

ネットワークサービスを認証および認可するためのシステムであって、該システムはモバイル機器を有し、

該モバイル機器は、少なくともひとつのネットワークアクセスタイプを示す情報メッセージを受けてネットワークアクセスタイプを判定し、

少なくともユーザＩＤを含む開始メッセージを作成し、

前記情報メッセージにおいて識別されるアクセスネットワークと互換性がある認証メッセージ内に前記開始メッセージをカプセル化するよう構成され、

さらに該システムは、前記モバイル機器から届いた前記カプセル化された前記開始メッセージを読み出し、前記カプセル化された前記開始メッセージを、前記カプセル化された前記開始メッセージから識別されうる認証サーバに転送するアクセスコントローラをさらに備えるシステム。

【請求項２】

前記情報メッセージを発行するためのルータをさらに備え、前記情報メッセージがルータ通知を含む、請求項１に記載のシステム。

【請求項３】

前記ルータは、

前記少なくともひとつのネットワークアクセスタイプを示す前記情報メッセージを作成する作成手段と、

前記情報メッセージを前記モバイル機器に送信する送信手段と、
を備える、請求項２に記載のシステム。
【請求項４】
前記ルータが、前記モバイル機器がネットワークに入る際に前記情報メッセージを発行するように構成される、請求項２又は３に記載のシステム。
【請求項５】
前記ルータは前記アクセスコントローラの一部である、請求項２から４のいずれかに記載のシステム。
【請求項６】
前記情報メッセージが拡張認証プロトコル（ＥＡＰ）サポートを示す、請求項１から５のいずれかに記載のシステム。
【請求項７】
前記開始メッセージが、クライアント識別子オプションメッセージおよび拡張認証プロトコルサポート識別子オプションメッセージを含み、前記クライアント識別子オプションメッセージおよび拡張認証プロトコルサポート識別子オプションメッセージは、クライアントタイプ、ユーザＩＤ、コアアドレス情報のうち少なくともひとつに関する情報を含む、請求項１から６のいずれかに記載のシステム。
【請求項８】
前記モバイル機器および前記アクセスネットワークの間のプロトコルが、ＵＤＰ、ＩＣＭＰｖ６、ＩＥＥＥ８０２．１ｘ、ＩＥＥＥ８０２．１１ｉ、およびブルートゥースプロファイルのうち少なくともひとつを備える、請求項１から７のいずれかに記載のシステム。
【請求項９】
適用される認証機構が拡張認証プロトコル（ＥＡＰ）を備える、請求項１から８のいずれかに記載のシステム。
【請求項１０】
適用される認証機構が、携帯電話認証および音声暗号化（ＣＡＶＥ）アルゴリズムを適用するリムーバブルユーザ識別モジュール（Ｒ－ＵＩＭ）を使用する認証機構である、請求項１から８のいずれかに記載のシステム。
【請求項１１】
前記アクセスコントローラが、前記モバイル機器のホームエージェントに備えられる、請求項１から１０のいずれかに記載のシステム。
【請求項１２】
ネットワークサービスを認証または認可するための方法であって、
前記モバイル機器が、
・　少なくともひとつのネットワークアクセスタイプを示す情報メッセージを受信することに応じてネットワークアクセスタイプを判定し、
・　少なくともユーザＩＤを含む開始メッセージを作成し、
・　前記情報メッセージにおいて識別されるアクセスネットワークと互換性がある認証メッセージ内に前記開始メッセージをカプセル化することと、　アクセスコントローラが、
・　前記モバイル機器から届いた前記カプセル化された前記開始メッセージを読み出し、前記カプセル化された前記開始メッセージを、前記カプセル化された前記開始メッセージから識別される認証サーバに転送することと、
を含む方法。
【請求項１３】
前記ネットワークが前記情報メッセージを発行するルータをさらに含み、前記情報メッセージがルータ通知を含む、請求項１２に記載の方法。
【請求項１４】
前記ルータにより発行される前記情報メッセージは、前記モバイル機器が前記ネットワークに入る際に発行される、請求項１３に記載の方法。

【請求項１５】
前記情報メッセージが拡張認証プロトコル（ＥＡＰ）サポートを示す、請求項１２から１４のいずれかに記載の方法。
【請求項１６】
前記開始メッセージが、クライアント識別子オプションメッセージおよび拡張認証プロトコルサポート識別子オプションメッセージを含み、これらがクライアントタイプ、ユーザＩＤ、コアアドレス情報のうち少なくともひとつに関する情報を含む、請求項１２から１５のいずれかに記載の方法。
【請求項１７】
前記モバイル機器および前記アクセスネットワークの間のプロトコルが、ＵＤＰ、ＩＣＭＰｖ６、ＩＥＥＥ８０２．１ｘ、ＩＥＥＥ８０２．１１ｉ、およびブルートゥースプロファイルのうち少なくともひとつを備える、請求項１２から１６のいずれかに記載の方法。
【請求項１８】
適用される認証機構が拡張認証プロトコル（ＥＡＰ）を備える、請求項１２から１７のいずれかに記載の方法。
【請求項１９】
適用される認証機構が、携帯電話認証および音声暗号化（ＣＡＶＥ）アルゴリズムを適用するリムーバブルユーザ識別モジュール（Ｒ－ＵＩＭ）を使用する認証機構を備える、請求項１２から１７のいずれかに記載の方法。
【請求項２０】
前記アクセスコントローラが、前記モバイル機器のホームエージェント（ＨＡ）に備えられる、請求項１２から１９のいずれかに記載の方法。
【請求項２１】
アクセスコントロール機器であって、
内部で開始メッセージがカプセル化されている認証メッセージであって、前記カプセル化された前記開始メッセージで特定されるアクセスネットワークと互換性のある認証メッセージを受信する受信手段と、
前記カプセル化された前記開始メッセージを読み出す処理手段と、
前記カプセル化された前記開始メッセージを、前記カプセル化された前記開始メッセージから識別されうる認証サーバに転送する転送手段と、
を備えるアクセスコントロール機器。
【請求項２２】
前記開始メッセージが、クライアント識別子オプションメッセージおよび拡張認証プロトコルサポート識別子オプションメッセージを含み、前記クライアント識別子オプションメッセージおよび拡張認証プロトコルサポート識別子オプションメッセージは、クライアントタイプ、ユーザＩＤ、コアアドレス情報のうち少なくともひとつに関する情報を含む、請求項２１に記載のアクセスコントロール機器。
【請求項２３】
前記開始メッセージを送信したモバイル機器のホームエージェントに備えられる、請求項２１又は２２に記載のアクセスコントロール機器。
【請求項２４】
情報メッセージを、少なくともひとつのネットワークアクセスタイプを示す加入者機器へ送信する送信手段をさらに備える、請求項２１から２３のいずれかに記載のアクセスコントロール機器。
【請求項２５】
前記情報メッセージがルータ通知を含む、請求項２４に記載のアクセスコントロール機器。
【請求項２６】
前記情報メッセージが拡張認証プロトコル（ＥＡＰ）サポートを示す、請求項２４又は

２５に記載のアクセスコントロール機器。
【請求項２７】
前記情報メッセージが、前記モバイル機器がネットワークに入る際に発行される、請求項２４から２６のいずれかに記載のアクセスコントロール機器。
【請求項２８】
少なくともひとつのネットワークアクセスタイプを示す情報メッセージを受けてネットワークアクセスタイプを判定する判定手段と、
少なくともユーザＩＤを含む開始メッセージを作成する作成手段と、
前記情報メッセージにおいて識別されるアクセスネットワークと互換性がある認証メッセージ内に前記開始メッセージをカプセル化するカプセル化手段と、
前記開始メッセージをアクセスコントロール機器に送信する送信手段と、
を備える加入者機器。
【請求項２９】
前記加入者機器がモバイル機器である、請求項２８に記載の加入者機器。
【請求項３０】
前記情報メッセージが拡張認証プロトコル（ＥＡＰ）サポートを示す、請求項２８又は２９に記載の加入者機器。
【請求項３１】
前記情報メッセージが、前記加入者機器がネットワークに入る際に発行される、請求項２８から３０のいずれかに記載の加入者機器。
【請求項３２】
前記開始メッセージが、クライアント識別子オプションメッセージおよび拡張認証プロトコルサポート識別子オプションメッセージを含み、前記クライアント識別子オプションメッセージおよび拡張認証プロトコルサポート識別子オプションメッセージは、クライアントタイプ、ユーザＩＤ、コアアドレス情報のうち少なくともひとつに関する情報を含む、請求項２８から３１のいずれかに記載の加入者機器。
【請求項３３】
適用される認証機構が、携帯電話認証および音声暗号化（ＣＡＶＥ）アルゴリズムを適用するリムーバブルユーザ識別モジュール（Ｒ－ＵＩＭ）を使用する認証機構である、請求項２８から３２のいずれかに記載の加入者機器。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークサービスを認証および認可するためのシステムおよび方法に関する。
【背景技術】
【０００２】
今後の3G（第三世代）システムアーキテクチャにおいて、例えばCDMA2000（符号分割多元接続バージョン2000）、携帯電話以外のIPベースのネットワーク、802．11ワイヤレスLAN（ローカルエリアネットワーク）、ブルートゥース（登録商標）、イーサネット（登録商標）等、多数の異なるネットワークアクセス方法によりネットワークサービスが供給される可能性がある。しかし、3GPP2においてモバイル機器が現在アクセスできるのは、CDMA2000アクセス方法を使用するネットワークサービスのみである。従って、より確実かつ効果的にネットワークサービスを供給するためには、異なるアクセスネットワークがサービスを認可できるよう、モバイル機器に異なるタイプのアクセスネットワークを通じて認証する能力を持たせる必要がある。
【０００３】
いかなる種類のネットワークアクセス技術においても、ユーザ（端末）を認証するためのひとつの普遍的な認証プロセスはない。また、このことがマルチアクセスシナリオにおけるアクセスおよびセッションの可動性を難しくしている。一般的なIPネットワーク、携

帯電話または携帯電話以外において同じ権限を使用するサービスプロビジョニングを可能にするため、ネットワークおよび移動局の間でメッセージ交換が必要とされている。しかし、CDMA2000携帯電話ネットワークを使用していない場合、端末はオペレータのネットワークでそれ自体を認証しサービスを受けるために、いくつかの別の方法を使用しなければならないという問題がある。

【０００４】

SIM（加入者識別モジュール）カードがGSM（グローバルシステムフォーモバイルコミュニケーションズ）ネットワークにおけるユーザIDを保持するのと同様に、CDMAネットワークにおいて、携帯電話を使用するためのユーザIDを保持するR-UIMチップを使用する際にも、同様の問題が生じる。R-UIMについては、3GGP2文書C．S0023-0に記載されている。

【０００５】

例えば、端末がWLAN（ワイヤレスLAN）またはブルートゥース（登録商標）無線をインターネットなどへの接続に使用している場合、およびR-UIMモジュールから同じ登録IDを使用している場合、これを実現するには携帯電話以外の個別プロトコルが必要であり、本出願はこの問題に取り組むものである。

【発明の開示】

【０００６】

従って、本発明の第一の目的は、モバイル機器に異なる種類のアクセスネットワークを介して認証を行う可能性を提供することにある。

【０００７】

この目的は、次のようなシステムによって解決される。このシステムは、ネットワークサービスを認証および認可するためのシステムであって、該システムはモバイル機器を有し、

該モバイル機器は、少なくともひとつのネットワークアクセスタイプを示す情報メッセージを受けてネットワークアクセスタイプを判定し、

少なくともユーザIDを含む開始メッセージを作成し、

前記情報メッセージにおいて識別されるアクセスネットワークと互換性がある認証メッセージ内に前記開始メッセージをカプセル化するよう構成され、

さらに該システムは、カプセル化された前記メッセージを前記モバイル機器から読み出し、前記カプセル化されたメッセージを前記カプセル化されたメッセージにおいて識別される認証サーバに転送するアクセスコントローラをさらに備えるシステムである。

【０００８】

あるいは、上記目的は、ネットワークサービスを認証および認可するための方法であって、前記ネットワークはモバイル機器および認証制御機能を備え、

少なくともひとつのネットワークアクセスタイプを示す情報メッセージを受けて前記モバイル機器によりネットワークアクセスタイプを判定するステップと、

少なくともユーザIDを含む開始メッセージを作成するステップと、

前記情報メッセージにおいて識別されるアクセスネットワークと互換性がある認証メッセージ内に前記開始メッセージをカプセル化するステップと、

アクセスコントローラにより、カプセル化されたメッセージを前記モバイル機器から読み出し、前記カプセル化されたメッセージを前記カプセル化されたメッセージにおいて識別された認証サーバに転送するステップと、を含む方法により解決される。

【０００９】

このように、本発明によると、モバイル機器はネットワークアクセスタイプに関する情報を受信する（この情報メッセージはモバイル機器に送信される明示的メッセージであってよく、ネットワークにおいて一般的に利用可能な情報であってもよい）。モバイル機器はユーザIDを含む開始メッセージを作成し、認証メッセージ内のそれをアクセスコントローラへ送信する。アクセスコントローラは開始メッセージを評価し、それを的確な認証サーバへ転送する。

【００１０】

従って、モバイル機器は、認証メッセージを的確な認証サーバへ転送するひとつのコントローラだけをアドレス指定する必要がある。すなわち、モバイル機器は、どのようにして認証サーバに達するかを見極める必要がない。

【００１１】

さらに、異なるサービスのための複数の認証サーバが提供されてもよい。上述した従来技術によると、モバイル機器は複数の認証メッセージを、そのサービスが使用されるすべての異なる認証サーバに送信しなければならないことになる。それとは対照的に、本発明によれば、モバイル機器は、複数の認証サーバに対応する認証メッセージがカプセル化されるひとつの開始メッセージを送信するだけでよい。

【００１２】

従って、認証手順は簡略化される。加えて、複数のサービスが使用される場合であっても、単一の開始メッセージしか必要とされないため、ネットワークのトラフィック負荷は軽減される。

【００１３】

さらに、情報メッセージであって、ルータ通知を含む情報メッセージを発行するためのルータが提供されてもよい。

【００１４】

情報メッセージは拡張認証プロトコル（EAP）サポートを示してもよい。

【００１５】

情報メッセージはモバイル機器がネットワークに入る際に発行されてもよい。

【００１６】

開始メッセージは、クライアント識別子オプションメッセージおよび拡張認証プロトコルサポート識別子オプションメッセージを含んでよく、前記メッセージは、クライアントタイプ、ユーザID、コアIPネットワーク内のクライアントをアドレス指定する方法に関わる情報（以下、「コアアドレス情報」という）のうち少なくともひとつに関する情報を含む。

【００１７】

モバイル機器およびアクセスネットワークの間のプロトコルは、UDP、ICMP、ICMPv6等のネットワーク層プロトコルまたはIEEE802．1x、IEEE802．11i、およびブルートゥースプロファイル等のリンク層プロトコルのうち少なくともひとつを備えてよい。

【００１８】

適用される認証機構は、拡張認証プロトコル（EAP）を備えてよい。

【００１９】

適用される認証機構は、携帯電話認証および音声暗号化（CAVE）アルゴリズムを適用するリムーバブルユーザ識別モジュール（R－UIM）を使用する認証機構、または、AKAアルゴリズムを適用するUSIMを使用する認証機構であってよい。

【００２０】

本発明はまた、ネットワークサービスを認証および認可するためのシステムであって、モバイル機器手段であって、少なくともひとつのネットワークアクセスタイプを示す情報メッセージを受けてネットワークアクセスタイプを判定し、少なくともユーザIDを含む開始メッセージを作成し、前記情報メッセージにおいて識別されるアクセスネットワークと互換性がある認証メッセージ内に前記開始メッセージをカプセル化するための前記モバイル機器手段と、カプセル化されたメッセージを前記モバイル機器手段から読み出し、前記カプセル化されたメッセージを前記カプセル化されたメッセージにおいて識別された認証サーバに転送するためのアクセスコントローラとを備えるシステムも提案する。

【００２１】

さらに、本発明は、ネットワークサービスを認証および認可するためのシステムであって、前記ネットワークはモバイル機器および認証制御機能を備え、前記モバイル機器は、少なくともひとつのネットワークアクセスタイプを示す情報メッセージを受けて前記モバイル機器によりネットワークアクセスタイプを判定するための判定手段と、

少なくともユーザIDを含む開始メッセージを作成するための作成手段と、
前記情報メッセージにおいて識別されるアクセスネットワークと互換性がある認証メッセージ内に前記開始メッセージをカプセル化するためのカプセル化手段と、
カプセル化されたメッセージを前記モバイル機器から読み出すための読み出し手段および前記カプセル化されたメッセージを前記カプセル化されたメッセージにおいて識別された認証サーバに転送するための転送手段を備えるアクセスコントローラ手段とを備える、システムを提案する。

【００２２】

これに関して、アクセスコントローラにより読み出されるメッセージは、別のタイプのメッセージ内においてカプセル化され、よってそのアクセスコントローラが認証サーバに送信することが知られている。

【００２３】

本発明は、アクセスコントロール機器であって、内部に開始メッセージがカプセル化されている認証メッセージを受信するための受信手段と、カプセル化されたメッセージを読み出すための処理手段と、前記カプセル化されたメッセージを前記カプセル化されたメッセージにおいて識別された認証サーバに転送するための転送手段とを備えるアクセスコントロール機器も提案する。

【００２４】

また、この場合、アクセスコントローラにより読み出されるメッセージは、認証サーバに送信するため別のタイプのメッセージ内にカプセル化されてよい。

【００２５】

さらに、本発明は、加入者機器であって、
少なくともひとつのネットワークアクセスタイプを示す情報メッセージを受けてネットワークアクセスタイプを判定するための判定手段と、
少なくともユーザIDを含む開始メッセージを作成するための作成手段と、
前記情報メッセージにおいて識別されるアクセスネットワークと互換性がある認証メッセージ内に前記開始メッセージをカプセル化するためのカプセル化手段と、
前記開始メッセージをアクセスコントロール機器に送信するための送信手段とを備える、加入者機器を提案する。

【００２６】

また本発明は、ルータ機器であって、少なくともひとつのネットワークアクセスタイプを示す情報メッセージを作成するための作成手段と、前記情報メッセージを加入者機器に送信するための送信手段とを備えるルータ機器を提案する。

【好適な実施形態の詳細な説明】

【００２７】

上述のように、本発明に従ってネットワークサービスを認証および認可するためのシステムが提供され、このシステムは、ネットワークアクセスタイプおよび拡張認証プロトコルサポートを示すルータ通知を発行するためのルータと、前記ルータ通知を受けてネットワークアクセスタイプを判定し、クライアントタイプ、ユーザIDおよびコアアドレス情報を備えたクライアント識別子オプションメッセージおよびEAP（拡張認証プロトコル）識別子オプションメッセージを含む開始メッセージを作成し、カプセル化するモバイル機器を有する。このモバイル機器は、当該開始メッセージを、ルータ通知から識別されるアクセスネットワークと互換性のあるIPv4またはIPv6プロトコル、例えばUDP、ICMPv6（インターネットコントロールメッセージプロトコルバージョン6（IPv6用））にカプセル化する。もしくは、IEEE802．1x、IEEE802．11i、適合するブルートゥースプロファイル等のリンク層プロトコルに前記開始メッセージをカプセル化する。システムは、さらに、モバイル機器から届いたカプセル化されたメッセージをから読み出し、前記カプセル化されたメッセージを前記カプセル化されたメッセージにおいて識別された認証サーバに転送するためのアクセスコントローラを備える。

【００２８】

数種の認証機構が使用されてもよい。以下の好適な実施形態の説明において、USIM（汎用加入者識別モジュール）を使用するEAP-AKA（認証とキー合致）認証機構（第一の実施形態）およびCAVE（携帯電話認証および音声暗号化）アルゴリズムを適用するR-UIM（リムーバブルユーザ識別モジュール）を使用する認証機構（第二の実施形態）が例として挙げられる。

【００２９】

第一の実施形態は、CDMA2000携帯電話および携帯電話以外のパケットデータネットワークの併用に関し、特にユーザ認証およびEAP-AKA仕様を複数タイプのアクセスネットワークにわたって通信する際に汎用加入者識別モジュール（USIM）を使用するサービスの認可に関する。この性能は、他の携帯電話環境における同様の方法と同じ方式で、ノンデータ認証のためのキーインフラストラクチャを活用するキー管理を自動化するのに有効である。ユーザ認証およびサービス認可を行うことにより、携帯電話オペレータはユーザに様々なアクセスネットワークタイプを提供すると同時に、統一サービスプロビジョニング、ユーザ基準のネットワークアクセス管理およびローミング認可を維持し、現存する認可／アカウンティング／請求インフラストラクチャからこれらすべてを活用することができる。要約すると、利点は複数のアクセス方法に使用するスマートカードベースのCDMA2000認証の統合であるといえる。

【００３０】

この実施形態は、WLAN／CDMA2000ユーザのためのネットワークアクセス、モビリティシ・グナリング、およびその他のサービス認可を説明する。特に、第一の実施形態によると、モビリティ・マネジメント・シグナリング保護と同様に、WLANからのネットワーク認可がAAAv6（Ipv6用認証、認可およびアカウンティング）、EAP-AKA（拡張認証プロトコル認証とキー合致）、および、提示されている方法のためのCDMA2000仕様の多元接続アーキテクチャと同様に、RADIUSプロトコルを使用する多元接続スキームが提供される。

【００３１】

上述したように、第一の実施形態によると、解決すべき問題は、CDMA2000携帯電話ネットワークを使用していない場合、端末はオペレータのネットワークでそれ自体を認証しサービスを受けるために、いくつかの別の方法を使用しなければならないということである。本実施形態によると、この問題は、以下に詳しく説明するように、ユーザがユーザIDを保持するUSIMを有する限り、任意のアクセス技術およびコア技術を実行するために、EAP-AKA仕様を使用してユーザを認証する方法を定義することにより克服される。

【００３２】

第一の実施形態によると、EAP-AKA認証機構（例えば、J.Arkko・H.Haverinen著、EAP AKA Authentication（作業中）、インターネットドラフト（draft-arkko-pppext-eap-aka-10.txt）、インターネットエンジニアリングタスクフォース（2003年6月）で定義されているようなもの）は、任意のネットワークアクセス技術を使用するネットワークに対しユーザを認証するために適用される。従って、端末、USIM（汎用加入者識別モジュール）、アクセスコントローラ、認証ゲートウェイ、およびCDMA2000ネットワークの認証センター（AuC／HLR（ホームロケーションレジスタ、AuCはHLR内に位置する））のエンティティを伴う（がこれらに限定されない）多方面増加インターアクションによる相互認証、ネットワーク認可、およびサービスプロビジョニングが実現する。以下、これがどのようにして実現し得るのか、詳しく説明する。

【００３３】

図1は、CDMA2000マルチアクセスネットワーク参照モデルを示し、これにはアクセスコントローラ（AC）および認証サーバ（AS）も提供される。

【００３４】

図1の左上部分に、訪問アクセスプロバイダネットワーク（特に、サービングネットワーク）が示されている。ソース無線ネットワーク（RN）はRAN-PDSNインターフェイス（R-Pインターフェイス）を経由しサービングPDSNに接続されている。A10およびA11は、CDMA2000において定義される制御メッセージのためのインターフェイスである。PDSN（パケッ

トデータサービングネットワーク）はフォーリンエージェントとしての役割を果たし、インターネット、イントラネットおよびワイヤレスアプリケーションプロトコル（WAP）へのアクセスを移動局等に提供する。ソースRNは、インターフェイスA1を経由し移動通信交換局（MSC）にも接続されている。

【００３５】

MSCはSS7ネットワークを経由し移動局のホームアクセスプロバイダネットワークに接続されている。ホームアクセスプロバイダネットワークは、ホームロケーションレジスタ（HLR）および認証センター（AuC）を備え、以下に説明する実施形態によるとこれは必要なものである。

【００３６】

図1の左中部分に、ターゲットの訪問アクセスプロバイダネットワーク（visited access provider network，在圏アクセスプロバイダネットワーク）が示されており、これに移動局が接続されてもよい。ターゲット訪問アクセスプロバイダネットワークは、ターゲットRNおよびターゲットPDSNを備え、これらはR-Pインターフェイスによってサービング訪問アクセスプロバイダネットワーク内と同様に接続されている。双方のPDSNは、IPネットワーク（インターネットプロトコルバージョン4（Ipv4）および／またはインターネットプロトコルバージョン6（Ipv6））にも接続されている。この接続のために、CDMA2000においてインターフェイスPiが定義されている。サービングPDSNは、AAAL（ローカルAAA（認証、認可およびアカウンティング））サーバにも接続されており、このサーバはIPネットワークにもアクセスできる。

【００３７】

図1の右側に、上述したホームアクセスプロバイダネットワーク、IPネットワークに接続されAAAH（ホームAAA）を備えるホームIPネットワーク、およびAAAサーバを備えるブローカーネットワークが示されている。さらに、ホームエージェント（HA）が図解されており、これはホームIPネットワーク、プライベートネットワーク、またはホームアクセスプロバイダネットワーク内に配置されてもよい。

【００３８】

移動局に対する追加のアクセスの可能性が図1の左下部分に示されており、ここで追加のターゲット訪問アクセスプロバイダネットワークが図解されている。これは以下に説明する実施形態のシナリオである。ここで移動局は、ターゲットWLAN（ワイヤレスローカルエリアネットワーク）に接続されている。WLANは、IPインターフェイスを経由して、後に詳細を説明するアクセスコントローラ（AC）に接続されている。ACは、アクセスサーバ（AS）に接続されており、これがIPネットワークおよびホームアクセスプロバイダネットワーク、特にホームアクセスプロバイダネットワークのAuCへの接続を提供する。

【００３９】

以下に説明する実施形態に記載の新しい機能性（すなわち、新しい機能性を備えた機器）は、斜線で塗りつぶしたボックスで示されている。換言すれば、これらの新しい機能性はACおよびASにあるということである。さらに、任意でホームIPネットワークのAAAH内にASが提供されてもよい。

【００４０】

端末は、携帯電話ネットワークおよびOWLAN（オペレータワイヤレスLAN）アクセスネットワークの一部であるIPネットワークを含む、あらゆる種類のIPネットワークにアクセス可能である必要がある機器である。端末は、USIMを有することにより、AKAアルゴリズムを実行できることも必要である。また、IPv6プロトコルを実行する必要もある。MIPv6が使用される場合、このプロセスは、ホームエージェントと端末の間のセキュリティアソシエーションを動的に作成するために利用されることもできる。EAP-AKA仕様は、AKA認証がEAPメッセージを使用してどのように実行されるかを示す。この実施形態に従って、この仕様がアクセス技術にかかわらず、どのように認証に使用されることができるかを説明する。

【００４１】

この機能性を実行できるネットワークに入る際、端末は、その機能性をサポートしていることを示すルータ通知（Router Advertisement； RA）を受信する。このルータ通知は、例えば、上のタイプのAAA（認証、認可およびアカウンティング）をサポートしていることを示す、ローカルアクセスコントローラ（AC）からの、ルータ通知オプション又はエージェント通知オプションを含む。これは、本実施形態に従って認証、キー生成、およびサービスプロビジョニングを指示する。

【００４２】

EAPメッセージは、端末とユーザのIPネットワークへのアクセス制御に関与するネットワーク要素であるアクセスコントローラとの間で交換される際に、AAAv6メッセージまたはWLANリンク層（IEEE802．1x、IEEE802．11i、適合するブルートゥースプロファイルメッセージ、PPP EAPカプセル化、または任意の適合するlast－hop PANAプロトコルメッセージ等において、将来標準化されるとして）のいずれかにおいてカプセル化される。AAAv6が使用される場合、初期のEAP／AKA IDメッセージは、AAAv6メッセージ内のEAP IDオプションに加わる。

【００４３】

アクセスコントローラと認証サーバの間で、EAPメッセージがDiameterまたはRadiusのようなコアネットワークプロトコルに運ばれる。ACは、それをIMSI（国際移動電話加入者識別番号）およびアドレス体系から割り当てることにより認証サーバのIPアドレスを決定する。認証サーバは、MSCを経由しHLR／認証センター（AuC）に達する論理インターフェイスを有する。これは、MAPプロトコル（SS7ネットワーク）とIPで使用される認証プロトコルの間のゲートウェイとしての役割を果たす。

【００４４】

以下、本実施形態に従ってOWLANネットワークにおいてユーザを認証するためのシナリオを、メッセージフローを用いて説明する。

【００４５】

1．端末がアクセス要求メッセージ（AAAv6リクエストメッセージまたはネットワークアクセスを要求するその他任意のメッセージであってもよい）をアクセスコントローラに送信する。このメッセージにはEAP応答／AKA IDメッセージが組み込まれている。また、このメッセージ内にはユーザNAIを回送するための機構も必要である。

【００４６】

2．アクセスコントローラが当該EAPメッセージをフェッチし、それを、コアネットワークにおいて認証サーバ（AS）に送信される要求メッセージ（Diameter AA要求メッセージまたはRadiusアクセス要求メッセージであってもよい）に入れる。例えば、DiameterにおいてEAPメッセージはEAPペイロードAVPにあるであろう。アクセスコントローラは、ユーザNAIのアドレス体系部分に基づいて、要求がどのASに行くべきかを割り出す。

【００４７】

3．メッセージを受信すると、ASは、第一に、ユーザのための認証情報を有するAuCを識別する。これは、ユーザNAIのユーザ部分に基づいていてもよい。例えば、使用されるユーザNAIがIMSI@アドレスの体系の形をとる場合、IMSIは、ユーザHLR／AuCを識別するために使用されることができる。ASは、AuCからUMTS認証クインテットを要求する。このクインテットは、5つの値、すなわち、a）ネットワークチャレンジRAND、b）予測されるユーザ応答XRES、c）暗号解読キーCK、d）完全性キーIK、および、e）ネットワーク認証トークンAUTNから成る。ASは、これらの値を得ると、AT_RAND属性（乱数）、AT_AUTN（認可ベクトル）、およびAT_MAC（メッセージ認証コード）を作成する。後の使用のために、ASは、値AT_RESを計算し格納する。ASは、AT_RAND値・AT_AUTN値・およびAT_MAC値を含むEAP要求／AKA／チャレンジメッセージを作成する。最後にASは、EAP要求／AKA／チャレンジメッセージやユーザを（ユーザ名属性において）識別するNAIをその中に含むメッセージをACへ送信する。メッセージはDiameter AA回答メッセージまたはRadiusアクセスチャレンジメッセージであってもよい。Diameterメッセージである場合、EAPメッセージはEAPペイロードAVPに運ばれる。

【００４８】
4．ACが、EAP要求／AKA／チャレンジを含むメッセージを端末に送信する。これは、AAAv6メッセージまたは端末とアクセスコントローラとの間で使用する、その他任意のネットワークアクセスプロトコルであってよい。
【００４９】
5．端末はこのメッセージを受信すると、まず、EAP要求／AKA／チャレンジメッセージを抽出する。次いでAKAを使用してAT_RES値を計算し、EAP要求／AKA／チャレンジ内でAKAに対するインプットとして受信したAT_RAND値およびAT_MAC値を得る。また端末は、AT_AUTN値を計算し、それをEAP要求／AKA／チャレンジにおいて受信したAT_AUTNと比較する。これらの値が一致した場合、EAP要求／AKA／チャレンジメッセージは認証に成功し、そうでない場合、このメッセージの認証は失敗する。値が一致していた場合、端末は、EAP要求／AKA／チャレンジメッセージを含むメッセージ（AAAv6）を作成し、ACへ送信する。EAP要求／AKA／チャレンジメッセージは、計算されたAT_RES値を含む。
【００５０】
6．ACは、再度要求メッセージを送信する（Diameter AA要求／Radiusアクセス要求）。このときメッセージは、EAP要求／AKA／チャレンジを含む。
【００５１】
7．ASはこのメッセージを受信すると、先に計算しておいたAT_RES値を受信したEAPメッセージ内のAT_RES値と比較する。値が一致する場合、AKA認証は成功し、そうでない場合、認証は失敗する。結果に応じて、アクセス認可またはアクセス拒否メッセージのいずれかを送信する（Radiusの場合）。Diameterであれば、結果コードAVP内の結果とともにAA回答メッセージを送信する。
【００５２】
8．このメッセージを受けて、ACは、認証が成功したか否かを知る。ACは適切な応答メッセージを端末に送信する。端末がこのメッセージを受信すると、OWLANアクセスネットワーク認証は完了する。認証が成功した場合、ACは、認証された端末から送信されたパケットを通過させることを許可するフィルタリングルールを適用しなければならない。
【００５３】
次に、図2Aおよび2Bに示すシグナルフロー図を参照し、上述の手順をもう少し詳しく説明する。シグナルフロー図は、端末（端末機すなわちUE）、認証センター（AC）および認証サーバ（AS）の間で交換される信号を図解したものである。
【００５４】
ステップ2-Aにおいて、端末は、ACからルータ通知（非請求または応答型）を受信する。ルータ通知（RA）は、ローカルチャレンジを含むAAAチャレンジオプションを含む。メッセージを送信する前に、端末は割り当てられたIPアドレスを取得していなければならない（例えばDHCP（動的ホスト構成プロトコル）サーバからのIPv4の場合。IPv6アドレスの場合、自動構成アドレスであってもよい）。
【００５５】
ステップ2-Bにおいて、端末は、ルータ通知におけるAAAフラグの存在により、AAAアクセス認証を実行する必要があることを推論する。端末は、AAA要求メッセージを（RQ1に指示されて）ACへ送信することにより、認証シーケンスを開始する。AAA要求は、EAP IDメッセージを運ぶオプションと同様に、AAAクライアント識別子オプション（シグナルフロー図ではcIDとして示される）を含む。AAAクライアント識別子オプションおよびEAP IDメッセージは双方ともユーザのNAI（IMSI@アドレス体系）を含む。
【００５６】
ステップ2-Cにおいて、ACは、AAAクライアント識別子オプションに含まれるNAIからASのアドレスを（必要な場合はDNSを使用して）導出し、AAA要求メッセージ（AR）をASに送信する。ARは、ステップBのAAAクライアント識別子オプション内で受信したEAP IDメッセージ（EAPペイロード属性において）およびNAI（ユーザ名属性において）を含む。
【００５７】

ステップ2-Dにおいて、ASは、ステップ2-CにおけるARメッセージを受けて、以下を実行する。
・ NAIのIMSI部分に基づき、ASは、ユーザのための認証情報を有するAuCを識別する。
・ UMTS認証クインテットを要求し、AuCから得る。このクインテットは、5つの値、すなわち、a）ネットワークチャレンジRAND、b）予測されるユーザ応答XRES、c）暗号解読キーCK、d）完全性キーIK、およびe）ネットワーク認証トークンAUTNから成る。
・ AT_RAND属性（乱数）、AT_AUTN（認可ベクトル）、およびAT_MAC（メッセージ認証コード）を計算する。
・ 後の使用のために、値AT_RESを計算し格納する（XRESから導出）。
・ AT_RAND値、AT_AUTN値、およびAT_MAC値を含む、EAP要求／AKA／チャレンジメッセージを作成する。
・ EAP要求／AKA／チャレンジ（3GPP2におけるベンダー固有属性）およびユーザを（ユーザ名属性において）識別するNAIを含む、アクセスチャレンジ（AA）メッセージをACへ送信する。

【００５８】

ステップ2-Eにおいて、ACは、AAAv6組み込みデータオプション内にEAP要求（シグナルフロー図ではERp）／AKA／チャレンジを含むAAA応答メッセージ（RP2）と、NAIを含むAAAクライアント識別子オプションと、AAAv6チャレンジオプションとを端末へ送信する。AAAv6チャレンジオプションは、ACにより設定されたローカルチャレンジ値を含む。

【００５９】

ステップ2-Fにおいて、端末は、ステップ2-EにおけるAAA応答を受けて、以下を実行する。
・ AKAを使用してAT_RES値を計算し、EAP要求／AKA／チャレンジ内でAKAに対するインプットとして受信したAT_RAND値およびAT_MAC値を得る。
・ AKAにおいて指定されたように値AT_AUTNを計算する。
・ 計算したAT_AUTN値を、EAP要求／AKA／チャレンジにおいて受信した値と比較する。値が一致した場合、EAP要求／AKA／チャレンジメッセージは認証に成功し、そうでない場合、このメッセージの認証は失敗する。
・ AAA要求メッセージ（RQ3）を、ACへ送信する。AAA要求メッセージ（RQ3）は、AAAv6チャレンジオプション内にローカルチャレンジを含み、また、AAAクライアント識別子オプション（IMSI@アドレス体系の形のNAI）と、AAAv6組み込みデータオプション内にEAP応答（ER）／AKA／チャレンジメッセージとを含む。EAP応答／AKA／チャレンジは、計算されたAT_RES値を含む。

【００６０】

ステップ2-Gにおいて、ACは、AAA要求（AR）メッセージをAS（NAIにより識別される）へ送信する。ARメッセージは、AAA要求のAAAクライアント識別子オプションにおいて受信したEAP要求／AKA／チャレンジ（3GPP2におけるベンダー固有属性）およびNAIを（ユーザ名属性において）含む。

【００６１】

ステップ2-Hにおいて、ASはステップ2-GにおけるARメッセージを受けて、以下を実行する。
・ ステップDにおいて計算されたAT_RES値を、EAP応答／AKA／チャレンジに含まれるAT_RES値と比較する。値が一致する場合、AKA認証は成功であり、そうでない場合、認証は失敗する。
・ 認証が成功の場合、ユーザを（ユーザ名属性において）識別するNAIを含むAAメッセージをACへ送信する。認証が失敗した場合、アクセス拒否メッセージをACへ送信する。

【００６２】

ステップ2-Iにおいて、ACは、ステップ2-HにおけるAAメッセージを受けて、AKA認証が成功したことを知る。ACはAAA応答メッセージ（図2AにおいてRP3により示される）をSUCCESS（値0）を示すように設定されたコードフィールドとともに端末へ送信する。端末がこ

のメッセージを受信すると、OWLANアクセスネットワーク認証は完了する。

【００６３】

認証が成功した場合、ACは、認証された端末から送信されたパケットを通過させることを認可するフィルタリングルールを適用しなければならない。

【００６４】

以下、第一の実施形態に記載のモビリティバインディングのために、どのようにして汎用の認証確立が行われるかを説明する。

【００６５】

1．シーケンスが、要求メッセージ（AAAv6、WLANリンク層またはその他任意のネットワークアクセスプロトコル）をホームエージェント（HA）へ送信する端末から開始する。要求は、組み込みEAP応答／AKA／IDメッセージと同様にユーザ（IMSI@アドレス体系）のNAIを含む。

【００６６】

2．HAが、EAPメッセージを取りに行き、それをコアネットワークにおいて認証サーバ（AS）に送信された要求メッセージ（Diameter AAA要求メッセージまたはRadiusアクセス要求メッセージであってもよい）に入れる。例えば、Diameterにおいて、EAPメッセージはEAPペイロードAVPにあるであろう。NAIのアドレス体系部分はASが存在するドメインを示すため、HAは、ユーザNAIのアドレス体系部分に基づいて、要求がどのASに行くべきかを割り出す。

【００６７】

3．メッセージを受信すると、ASは、第一にユーザのための認証情報を有するAuCを識別する。これは、ユーザNAIのユーザ部分に基づいていてもよい。例えば、使用されるユーザNAIがIMSI@アドレス体系の形をとる場合、IMSIは、ユーザHLR／AuCを識別するために使用されることができる。IMSIは、AuCからUMTS認証クインテットを要求する。このクインテットは、5つの値、すなわち、a）ネットワークチャレンジRAND、b）予測されるユーザ応答XRES、c）暗号解読キーCK、d）完全性キーIK、および、e）ネットワーク認証トークンAUTNから成る。これらの値を得ると、ASは、AT_RAND属性（乱数）、AT_AUTN（認可ベクトル）、およびAT_MAC（メッセージ認証コード）を作成する。後の使用のために、値AT_RESおよびセッションキーKを計算し格納する。AT_RAND値、AT_AUTN値およびAT_MAC値を含むEAP要求／AKA／チャレンジメッセージを作成する。最後にASは、EAP要求／AKA／チャレンジメッセージをその中に含むメッセージおよびユーザを（ユーザ名属性において）識別するNAIを、HAへ送信する。メッセージはDiameter AA回答メッセージまたはRadiusアクセスチャレンジメッセージであってもよい。Diameterメッセージである場合、EAPメッセージはEAPペイロードAVPに運ばれる。

【００６８】

4．HAが、EAP要求／AKA／チャレンジを含むメッセージを端末に送信する。これは、AAAv6メッセージまたは端末とアクセスコントローラとの間で使用する、その他任意のネットワークアクセスプロトコルであってよい。

【００６９】

5．端末は、このメッセージを受信すると、まずEAP要求／AKA／チャレンジメッセージを抽出する。次いでAKAを使用してAT_RES値を計算し、EAP要求／AKA／チャレンジ内でAKAに対するインプットとして受信した、AT_RAND値およびAT_MAC値を得る。次いで値Kを計算する。またAT_AUTN値を計算し、それをEAP要求／AKA／チャレンジにおいて受信したAT_AUTNと比較する。これらの値が一致した場合、EAP要求／AKA／チャレンジメッセージは認証に成功し、そうでない場合、このメッセージの認証は失敗する。値が一致していた場合、端末は、EAP応答／AKA／チャレンジメッセージを含むメッセージ（AAAv6）を作成し、HAへ送信する。EAP応答／AKA／チャレンジメッセージは計算されたAT_RES値を含む。端末は、今後のセキュリティアソシエーション（SA）に使用するため、値KをHAとともに格納する。

【００７０】

6．HAは再度要求メッセージを送信する（Diameter AA要求／Radiusアクセス要求）。このときメッセージはEAP応答／AKA／チャレンジを含む。

【００７１】

7．ASは、このメッセージを受信すると、先に計算しておいたAT_RES値を受信したEAPメッセージ内のAT_RES値と比較する。値が一致する場合、AKA認証は成功し、そうでない場合、認証は失敗する。結果に応じて、アクセス認可またはアクセス拒否メッセージのいずれかを送信する（Radiusの場合）。Diameterであれば、結果コードAVP内の結果とともにAA回答メッセージを送信する。また、BU認証キーを搬送するのに必要なため、鍵配送AVPをHAおよびBU認証キーの関連存続期間を有する認可存続期間AVPへ送信する。

【００７２】

8．このメッセージを受けて、HAは認証が成功したか否かを知る。HAは、対応付け更新（Binding update）を認証する目的で、端末を使用しセキュリティアソシエーションを作成する。認証キーKをこのSAに関連付け、メッセージ内において受信された際にその存続期間を初期化する。HAは、適切な応答メッセージを端末に送信する。端末がこのメッセージを受信すると、BU認証キー確立は完了する。

【００７３】

以下、図3Aおよび3Bに示すシグナルフロー図を参照し、上述の手順をもう少し詳しく説明する。

【００７４】

ステップ3-Aにおいて、端末は、そのHAがAKA認証を実行できるという知識を自動的に受信する。以下のメッセージを送信する前に、端末は割り当てられたIPv4アドレスを、例えばDHCPを使用して取得していなければならない。

【００７５】

ステップ3-Bにおいて、端末はそのホームネットワークによるその静的知識により、結合認証を実行する必要があることを推論する。端末は、AAA要求メッセージを（図3AのRQ1に指示されて）HAへ送信することにより認証シーケンスを開始する。AAA要求は、EAP応答およびEAP IDメッセージ（ERs／EAP ID）を運ぶオプションと同様にAAAクライアント識別子オプション（cID）を含む。AAAクライアント識別子オプションおよびEAP IDメッセージは双方ともユーザのNAI（IMSI@アドレス体系）を含む。

【００７６】

ステップ3-Cにおいて、HAは、AAAクライアント識別子オプションに含まれるNAIからASのアドレスを（必要な場合はダイナミックネームサーバ（DNS）を使用して）導出し、AAA要求メッセージ（AR）をASに送信する。ARは、ステップBのAAAクライアント識別子オプション内で受信したEAP IDメッセージ（EAPペイロード属性において）およびNAI（ユーザ名属性において）を含む。

【００７７】

ステップ3-Dにおいて、ASは、ステップ3-BにおけるARメッセージを受けて、以下を実行する。

・　EAP応答／IDの理由フィールドから、この手順で確立されたセッションキーがクライアントアテンダント認証に使用されることを認識する（そのため、後にキーをアテンダントとしての役割を果たすもの以外のHAに送信する必要がない）。
・　NAIのIMSI部分に基づき、ユーザのための認証情報を有するAuCを識別する。
・　UMTS認証クインテットを要求し、AuCから得る。
・　AT_RAND属性（乱数）、AT_AUTN（認可ベクトル）、およびAT_MAC（メッセージ認証コード）を計算する。
・　後の使用のために、値AT_RESおよびKを計算し格納する。
・　AT_RAND値、AT_AUTN値、およびAT_MAC値を含む、EAP要求／AKA／チャレンジメッセージを作成する。
・　EAP要求／AKA／チャレンジ（3GPP2におけるベンダー固有属性）およびユーザを（ユーザ名属性において）識別するNAIを含むアクセスチャレンジ（AC）メッセージを、HAへ

送信する。

【００７８】

ステップ3-Eにおいて、HAは、AAAv6組み込みデータオプション、NAIを含むAAAクライアント識別子オプション、およびAAAv6チャレンジオプション内にEAP要求／AKA／チャレンジを含むAAA応答メッセージ（図ではRP2で示される）を端末へ送信する。AAAクライアント識別子オプションはユーザを識別するNAIを、AAAv6チャレンジオプションはHAにより設定されたローカルチャレンジ値を含む。

【００７９】

ステップ3-Fにおいて、端末は、ステップ3-EにおけるAAA応答を受けて、以下を実行する。

・　AKAを使用してAT_RES値およびK値を計算し、EAP要求／AKA／チャレンジ内で、AKAに対するインプットとして受信したAT_RAND値を得る。

・　計算したAT_AUTN値を、EAP要求／AKA／チャレンジにおいて受信した値と比較する。値が一致した場合、EAP要求／AKA／チャレンジメッセージは認証に成功し、そうでない場合、このメッセージの認証は失敗する。

・　セキュリティアソシエーションに使用するため、キーKをHAとともに格納する。

・　更新の必要がある際に推論できるよう、セキュリティアソシエーションの存続期間をHAとともに格納する。

・　AAAv6チャレンジオプションにローカルチャレンジを含み、AAAv6組み込みデータオプションにAAAクライアント識別子オプション（IMSI@アドレス体系の形のNAI）およびEAP応答（ER）／AKA／チャレンジメッセージを含む、AAA要求メッセージ（RQ3）をHAへ送信する。EAP応答／AKA／チャレンジは、計算されたSRES値を含む。

【００８０】

ステップ3-Gにおいて、HAは、ARメッセージを（NAIにより識別された）ASへ送信する。ARメッセージは、AAA要求のAAAクライアント識別子オプションにおいて受信したEAP応答／AKA／チャレンジ（3GPP2におけるベンダー固有属性）およびNAIを（ユーザ名属性において）を含む。

【００８１】

ステップ3-Hにおいて、ASはステップ3-FにおけるARメッセージを受けて、以下を実行する。

・　ステップ3-Cにおいて計算されたAT_RES値を、EAP応答／AKA／チャレンジに含まれるAT_RES値と比較する。値が一致する場合、AKA認証は成功であり、そうでない場合、認証は失敗する。

・　AAメッセージをHAへ送信する。AAメッセージは、ベンダー固有属性におけるBU認証キーと、ユーザ名属性においてユーザを識別するNAIと、および別のベンダー固有属性におけるBU認証キー存続期間とを含む。キー存続期間フィールドは、ASによって例えば値259200（3日間）に設定される。

【００８２】

ステップ3-Iにおいて、HAは、端末とともに対応付け更新を認証するためにセキュリティアソシエーションを作成または更新し、キーKを認証キーとしてそれに関連付け、キー存続期間属性において受信した値に従ってSAの存続期間を初期化する。次いでHAは、AAA汎用キー応答オプションおよびSUCCESS（値0）を示すよう設定されたコードフィールドを含むAAA応答メッセージ（RP3）を、端末に送信する。AAA汎用キー応答オプションはキーKを含まないが、存続期間フィールドはキー存続期間属性において受信した値に設定され、キーSPIフィールドの値はHAと端末の間のセキュリティアソシエーションを示すように設定される。端末がこのメッセージを受信すると、汎用BU認証キー確立は完了する。

【００８３】

ステップ3-Jにおいて、端末は、Mobile IPv4アプリケーションに対し、BSAのものを使用して、キー材料から作成されたように、Mobile-Home認証拡張をMobile IPv4登録要求（RREQ）の中へ形成するだろう。HAは、RREQのメッセージ認証を実行する際、対応するBSA

をMN-HA認証拡張に対し自動的に適用するであろう。

【００８４】

Mobile IPv6アプリケーションに対しては、IPSecセキュリティアソシエーションを入力されたR-UIMが送信パケットに自動的に適用されるよう、端末がIPSec保護の対応付け更新をHAに送信するだろう。HAがパケットを受信すると、そのIPSecモジュールは、SAが着信するモビリティヘッダーパケットにもう適用できることを自動的に知る。このパケットはMobile IPv6 HOTIまたは対応付け更新メッセージであってよい。

【００８５】

ステップ3-Kにおいて、HAは、Mobile IPv6アプリケーションに対し、受信したキー材料から作成されるように、Mobile-Home認証拡張を、BSAのものを使用して、構築されたMobile IPv4登録応答（RREP）へ適用するだろう。次いで端末は、RREPのメッセージ認証を実行する際、対応するBSAをMN-HA認証拡張に対し自動的に適用するであろう。

【００８６】

Mobile IPv6アプリケーションに対しては、HAのIPSecモジュールはSAが入力されたR－UIMを使用して送信されたBAckメッセージを自動的に保護するであろう。次いで、IPSecで保護されたHAのモビリティヘッダーパケットを受信すると、端末は、自動的にIPSecセキュリティアソシエーションが入力されたR-UIMを、ステップNで使用されたものと逆方向に適用する。

【００８７】

これは、モビリティシ・グナリング保護アプリケーションプロトコルのフローをうまく完了させる。Mobile IP／IPv6ホーム登録以外のアプリケーションでは、この種の手順を任意のIPsecSAを入力するために使用することができる。

【００８８】

以下、本発明の第二の実施形態を説明する。

【００８９】

第一の実施形態と同様に、第二の実施形態は、CDMA2000携帯電話および携帯電話以外のパケットデータネットワークを併用する領域を対象とし、特にユーザ認証および複数タイプのアクセスネットワークにわたって通信する際に、リムーバブルユーザ識別モジュール（R－UIM）を使用するサービスの認可に関する。現在、携帯電話以外のIPネットワーク上でR－UIM認証を行うためのプロトコルは存在しないが、この機能は、他の携帯電話環境における同様の方法と同じ方式で、ノンデータ認証のための現存するキーインフラストラクチャを活用するキー管理を自動化するのに有効である。ユーザ認証およびサービス認可を行うことにより、携帯電話オペレータは、現存する認可／アカウンティング／請求インフラストラクチャからこれらすべてを活用しながら、ユーザに様々なアクセスネットワークタイプを提供すると同時に、統一されたサービスやユーザ基準のネットワークアクセス管理、およびローミング認可を供給しつづけることができる。利点を要約すると、複数のアクセス方法のためのスマートカードをベースとしたCDMA2000認証の統合であるといえる。

【００９０】

第二の実施形態によると、異なるリンク層のIPにおよぶ様々なプロトコルがR-UIMに基づくマルチアクセス認証および鍵配送機構に結合されている。このシステムは、異なる段階において様々なカプセル化メッセージを使用することにより、端末装置およびオペレータネットワークの双方が、IPに基づく携帯電話以外または携帯電話のパケットデータサービスのためにCDMA2000 CAVE（携帯電話認証および音声暗号化）アルゴリズムを実行することができるよう、ネットワーク要素にデータ交換をさせる。交換されたデータおよびCAVEアルゴリズムの結果を使用することにより、端末およびアクセスネットワークは、相互に認証し合い、ネットワークアクセス認可またはローミングシグナリング認証のメッセージ保護等、期間限定アプリケーションのためのセキュアキーを導出することができる。CAVEアルゴリズムについては、例えば1997年の「Cellular Radio Telecommunications Intersystem Operations」、ANSI－TIA／EIA－41においてさらに説明されていることが知られている。

【００９１】
端末は、CDMA2000、802．11ワイヤレスLAN、ブルートゥース（登録商標）、またはイーサネット（登録商標）を含む異種ネットワークタイプにおいて、IPに基づいて認証されたセッションを実行することができる。アクセスネットワークは、ポイントツーポイントまたはポイントツーマルチポイントであってよい。
【００９２】
端末は、この方法をMobile Ipv6によって実行してもよいし、モビリティサポートなしにIPv6アクセスだけによって実行してもよい。
【００９３】
携帯電話以外の場合、本第二の実施形態によると、モバイル装置およびオペレータネットワークが任意のIP利用可能なネットワーク上で互いに通信を行い、安全に証明書を交換し、サービスプロビジョニングを確立するために、使用されるネットワークの基本的特性にかかわらず、同一の方法が提供される。この方法は、説明のとおり、この方法を使用することで、オペレータが各技術を改革する必要はないが、リンク層固有の機構が使用されていないときにこのより一般的な方法を活用できるよう、登録IDを共有することだけにより、現存するCDMA2000方式に関係している。わずかなネットワーク要素を加えることにより、本発明において述べられるように、オペレータは現存するネットワーク要素をほとんど、あるいはまったく変化させずに、それらの現存するCDMA2000サービスインフラストラクチャを活用することができる。
【００９４】
以下、第二の実施形態に記載の手順をもう少し詳しく説明する。
【００９５】
この実施形態は、携帯電話またはその他のモバイル機器（これまで「ME」または「モバイル装置」と称してきた）を対象とし、これらは通常ワイヤレスリンク上でIPに基づく通信機能を有すると共に、R-UIMモジュールを有する。この実施形態は、固定機器の起動時に使用されることもできるが、モバイル機器に使用されるのが最も有効である。この実施形態により、第一の実施形態と同様、ME・R-UIM（その内蔵プロセッサ、不揮発性メモリ、およびプライベートデータの長所およびアルゴリズムにより、個別エンティティとみなされる）・アクセスコントローラ・認証ゲートウェイ・およびCDMA2000ネットワークの認証センター（AuC／HLR（ホームロケーションレジスタ）のエンティティを伴う（がこれらに限定されない）、複数の構成要素が連動することによる相互認証やネットワーク認可、およびサービスプロビジョニングが実現できる。
【００９６】
MEが、GRASP（汎用R-UIM認証およびサービスプロビジョニング、本第二の実施形態に記載されているプロトコル例）機能を使用できるネットワークに入る際、MEは、例えばこのタイプのAAAサポートを示すローカルACからのルータまたはエージェント通知オプション等、GRASPサポート指示を含むルータ通知を受信する。これは、本発明に記載されているように、認証、キー生成、およびサービスプロビジョニングを開始する。次に、MEが、クライアント識別子オプションおよびEAP IDオプションを含むEAP R-UIM／開始メッセージでACに応答する。いずれのオプションも、ME起動時に、R-UIM内のユーザのIMSIから構成されるユーザID（IMSI@アドレス体系）と、R-UIMまたはMEの不揮発性メモリ内の予備ファイルに含まれるアドレス体系とを含む。このID EAPメッセージは、IP／IPv6においてアクセスリンクAAAメッセージとしてカプセル化される。アクセスリンクAAAメッセージは、将来標準化されるものとして、IPv4またはIPv6それぞれの付録A中の最もよい実施事例に記載されているように、例えばUDPまたはICMv6メッセージ、IEEE802．1x、IEEE802．11i、または適合するブルートゥースプロファイルメッセージ等のリンク層カプセル化、PPP EAPカプセル化、または任意の適合するlast－hop PANAプロトコルメッセージ内等にあってよい。
【００９７】
ACは、それをIMSIおよびアドレス体系から割り当てることにより、認証サーバのIPアド

レスを決定し、例えばRADIUSまたはDIAMETER等その他任意のコアAAAプロトコルを使用して、カプセル化輸送のためにAAAメッセージをIPコアに転送する。このメッセージはその後ASに受信され、ASは次いでAuC／HLRに連絡する。

【００９８】

ASは、SS7または音声回路認証を模倣したA1メッセージングを使用することにより、直接またはサービングMSCを経由してAuC／HLRと通信を行うAAAサーバであってよい。換言すると、ASは、AuC／HLRと通信を行うための機能性を有するということになる。この構造上の選択により、現存するCDMAネットワークは修正されないままでよく、ASを加える必要があるだけである。これは非侵害的オーバーレイアプローチである。

【００９９】

あるいは、より密接な統合を伴うアプローチは、CDMA2000ネットワークに変化をもたらすであろう。ASは、CDMA2000パケットコアネットワーク内の標準に修正されたホームAAAサーバ（AAAH）へ認証を転送する、PDSN内のAAA（RADIUS）クライアント／ブローカーであってよい。後者は、AAAHがAuC／HLRと通信を行うための機能性を有することを要求するが、これはCDMA2000パケットコアに対する修正である。後者の構造上の選択は、それらの認証がPDSNにおけるPPPセッションの終わりに終了し、AAAHサーバとのRADIUSメッセージ交換をもたらすため、現在EAP-CHAPまたはEAP-PAPで行われているように、PDSNを経由してR-UIM認証を本来のCDMA2000パケットデータセッションに使用する可能性を与えるであろう。換言すれば、後者の代替は、携帯電話以外のR-UIM認証をPDSN経由でまたは直接ホームAAAサーバへ仲介し、または、拡張PDSN RADIUSクライアント機能を使用して携帯電話PPP-R-UIM認証を同じ終点へ転送するであろう。この拡張は、EAP-R-UIM性能およびRADIUSメッセージへのマッピングであり、潜在的に上述の方法のための携帯電話以外のRADIUSメッセージ再利用であろう。

【０１００】

ASは、登録を受信すると、AuCからの無作為化されたキーイングマテリアル検索をRANDまたはRANDU（実行される認証の大域的または固有の性質による）の形で開始し、この無作為情報を、クライアントIDオプションをAAA回答（RADIUS上で輸送される）内に含むEAP R-UIM／チャレンジメッセージの形でチャレンジとしてMEに返す。

【０１０１】

MEは、ASから無作為チャレンジ（RAND）を受信したら、そのものを認証しセッションのための暗号化キーを生成するためのCAVEアルゴリズムを実行できる状態となる。MEは、RunCaveアルゴリズムを開始させるコマンドをR-UIMに送信し、必要ならばこのR-UIMに対し、ESN（電話の電子シリアル番号、決定済みおよびME起動時）・RAND／RANDU・ランドタイプ（固有または大域的、何が供給されるかにより異なる）・およびPIN番号を提供する。次いでMEは、Get Responseを実行して、R-UIMにアウトプットAUTHRまたはAUTHU（大域的または固有のチャレンジ応答）をMEへ回送させる。

【０１０２】

MEはチャレンジ応答を受信した後、上述したものと同様のパケットでそれをACへ送信するが、このチャレンジ応答は、ローカルチャレンジ、クライアントIDおよびチャレンジ応答マテリアルを含む組み込みデータオプションを伴うEAP／R-UIM／開始メッセージである。その後ACは、前のステップでしたように、ASのアドレスを調べ、メッセージをRADIUS経由で転送する。ASはメッセージを受け取り、IDサブオプションにおいて受信したIMSIおよびアドレス体系に基づいてマッピング検索を行うことで、どちらのAuC／HLRに連絡するか判断し、IMSI@アドレス体系に基づいて、その格納されたセッション状態の検索も行う。ASは、AuC／HLRからCAVE証明書を検索し、CAVEアルゴリズムを実行し、MEから受信した応答をAuC／HLRから受信した応答と比較することで、クライアントの信頼性検証を進める。

【０１０３】

MEおよびAuC／HLRから受信した応答が等しい場合、ASは、セッションキーおよびサクセスコードを別のEAPメッセージ内のACに送り返す。このEAPメッセージを受けて、ACは、MEへのアクセスを承諾し、セッションキーをセッションの間使用するため保存する。これは

、例えばACにおけるコアAAAクライアント機能性によって起こる。ACは、MEにネットワークへのアクセスを承諾するため、IPsecセキュリティアソシエーションをMEによってAC内に入力し、またはファイアウォールルールを作成する。

【０１０４】

次いでACは、前述したようにlast-hop AAAプロトコル（例えばICMv6）に組み込み、キーサブオプションを除去して、メッセージをMEに送り返す。従って、キーがlast-hop上に送られることはなく、安全でない可能性があり、MEはR-UIMにおいてそのMEが導出したキーを使用し、ACはRADIUSを経由してASからキーを送り返す。

【０１０５】

次に、図4Aおよび4Bに示すシグナルフロー図を参照し、上述の手順をもう少し詳しく説明する。図2Aおよび2Bに関連して記載した省略等を再度説明しないため、このシグナルフローは、図2Aおよび2Bに示したものと類似していることに注意されたい。

【０１０６】

ステップ4-Aにおいて、端末は、ACからルータ通知（非請求または応答型）を受信する。ルータ通知（RA）は、AAAサポートを示すフラグを含む。メッセージを送信する前に、端末は割り当てられたIPv4アドレスを、例えばDHCPを使用して取得していなければならない。

【０１０７】

ステップ4-Bにおいて、端末は、ルータ通知におけるAAAフラグの存在から、AAAアクセス認証を実行する必要があることを推論する。端末は、AAA要求メッセージ（RQ1）をACへ送信することにより認証シーケンスを開始する。AAA要求は、EAP応答およびEAP IDメッセージを運ぶオプションと同様にAAAクライアント識別子オプションを含む。AAAクライアント識別子オプションおよびEAP IDメッセージは双方ともユーザのNAI（IMSI@アドレス体系）を含む。

【０１０８】

ステップ4-Cにおいて、ACは、AAAクライアント識別子オプションに含まれるNAIからASのアドレスを（必要な場合はDNSを使用して）導出し、AAA要求メッセージ（AR）をASに送信する。ARは、ステップBのAAAクライアント識別子オプション内で受信したEAP IDメッセージ（EAPペイロード属性において）およびNAI（ユーザ名属性において）を含む。

【０１０９】

ステップ4-Dにおいて、ASは、ステップ4-CにおけるARメッセージを受けて、以下を実行する。

・　R-UIM認証手順の開始を示すEAP要求／R-UIM／要求開始メッセージを作成する。

・　EAP要求／R-UIM／開始（EAPペイロード属性において）およびユーザを（ユーザ名属性において）識別するNAIを含むAAA回答（AA）メッセージをACへ送信する。

【０１１０】

ステップ4-Eにおいて、ACは、組み込みデータオプションにEAP要求／R-UIM／開始を含むと共にAAAクライアント識別子オプション含む、AAA応答メッセージ（RP1）を端末へ送信する。AAAクライアント識別子オプションは、ユーザを識別するNAIを含む。

【０１１１】

ステップ4-Fにおいて、端末は、NAI（IMSI@アドレス体系）を含むAAAクライアント識別子オプションおよびEAP応答／R-UIM／開始メッセージを運搬するAAA組み込みデータオプションを含むAAA要求メッセージ（RQ1）を送信する。EAP応答／R-UIM／開始メッセージの理由フィールドは、セッションキーがいかなる場合でも使用されないことを示す0（ゼロ）に設定される（CAVE認証のみ実行される）。

【０１１２】

ステップ4-Gにおいて、ACは、AAAクライアント識別子オプションに含まれるNAIからASのアドレスを（必要な場合はDNSを使用して）導出し、AAA要求メッセージ（AR）をASに送信する。ARは、ステップ4-FのAAAクライアント識別子オプション内で受信したような、EAP応答／R-UIM／開始メッセージおよびNAIを（ベンダー固有Radius属性フィールドにおい

て）含む。
【０１１３】
ステップ4-Hにおいて、ASは、ステップGにおけるARメッセージを受けて、以下を実行する。
・ NAIのIMSI部分に基づき、ASはユーザのための認証情報を有するAuCを識別する。
・ Cave認証トリプレットを要求し、AuCから得る。
・ 例えば、このEAP-R-UIMのために、H. Haverinenの「EAP SIM Authentication（作業中）」インターネットドラフト（draft－haverinen－pppext－eap－sim－10. txt）、インターネットエンジニアリングタスクフォース（2003年2月）に明記されている、値MAC_RANDおよびMAC_AUTHRを、AT RANDおよびAT MACとして計算する。
・ 後の使用のために、値MAC_AUTHRを格納する。
・ MAC_RAND値および2つのRAND値（認証トリプレットから得たもの）を含むEAP要求／R-UIM／チャレンジメッセージを作成する。
・ EAP要求／R-UIM／チャレンジと、（ベンダー固有Radius属性フィールドにおいて）ユーザを識別するNAIとを含む、AAA回答（AA）メッセージをACへ送信する。
【０１１４】
ステップ4-Iにおいて、ACは、AAA組み込みデータオプションにEAP要求／R-UIM／チャレンジを含むAAA応答メッセージ（RP2）、NAIを含むAAAクライアント識別子オプションを送信する。
【０１１５】
ステップ4-Jにおいて、端末はステップ4-IにおけるAAA応答を受けて、以下を実行する。
・ R-UIMを使用してAUTHR／AUTHUIの2つの値を計算し、EAP要求／R-UIM／チャレンジ内でR-UIMモジュールに対するインプットとして受信した2つのRNAD値を得る。
・ 例えば、上記で参照した文書H. Haverinenの「EAP SIM Authentication（作業中）」インターネットドラフト（draft－haverinen－pppext－eap－sim－10. txt）、インターネットエンジニアリングタスクフォース（2003年2月）に明記されている、値MAC_RANDおよびMAC_AUTHRを、AT_RANDおよびAT_MACとして計算する。
・ MAC_RAND値を、EAP要求／R-UIM／チャレンジ内で受信した値と比較する。値が一致する場合、EAP要求／R-UIM／チャレンジメッセージの認証は成功であり、そうでない場合、そのメッセージの認証は失敗する。
・ AAAクライアント識別子オプション（IMSI@アドレス体系の形をとるNAI）を含むと共にEAP要求／R-UIM／チャレンジをAAA組み込みデータオプションに含むAAA要求メッセージ（RP3）をACへ送信する。EAP要求／R-UIM／チャレンジメッセージは、計算されたMAC_AUTHR値を含む。
【０１１６】
ステップ4-Kにおいて、ACは、ARメッセージを（NAIにより識別された）ASに送信する。ARメッセージは、AAA要求のAAAクライアント識別子オプションにおいて受信したものとして、EAP要求／R-UIM／チャレンジおよびNAIを、（ベンダー固有Radius属性フィールドにおいて）含む。
【０１１７】
ステップ4-Lにおいて、ASは、ステップKにおけるARメッセージを受けて、以下を実行する。
・ ステップ4-Dにおいて計算されたMAC_AUTHR値を、EAP応答／R-UIM／チャレンジに含まれるMAC_AUTHR値と比較する。値が一致する場合、CAVE認証は成功であり、そうでない場合、認証は失敗する。
・ ユーザを（Radius属性フィールドにおいて）識別するNAIおよび認証の成功（AAにおける応答メッセージ属性）または失敗（アクセス拒否メッセージにおける応答メッセージ属性）を示す結果コードを含むAAメッセージをACへ送信する。
【０１１８】

ステップ4-Mにおいて、ACは、ステップ4-LにおけるAAメッセージを受けて、CAVE認証が成功したか否かを知る。認証が成功した場合、ACは、AAA応答メッセージを、SUCCESS（値0）を示すように設定されたコードフィールドとともに端末へ送信する。端末がこのメッセージを受信すると、OWLANアクセスネットワーク認証は完了する。

【０１１９】

認証が成功した場合、ACは、認証された端末から送信されたパケットを通過させることを認可するフィルタリングルールを適用しなければならない。代替として、以下のMobile IP／IPv6アプリケーションのために説明するのと同種のキーイング機構を使用することにより、ネットワークアクセスIPsecエントリーまたは端末とこのアプリケーション（または別のアプリケーションコード）を有するACの間に作成されたエントリーペアがあってもよい。

【０１２０】

第二の実施形態による第二の事例において、MSやHA、ASの間のシグナリングフローを、アクセスリンクシグナリング（NAAP、PPP-LCP等）、コアリンクシグナリング（RadiusまたはDIAMETER）、およびエンドツーエンドシグナリングとして、EAP-R-UIMを使用して説明する。結合したシグナリングを図5Aおよび5Bに示す。

【０１２１】

ステップ5-Aにおいて、端末はそのHAがR-UIM認証を実行できるという知識を自動的に受信する。以下のメッセージを送信する前に、端末は割り当てられたIPv4アドレスを、例えばDHCPを使用して取得していなければならない。

【０１２２】

ステップ5-Bにおいて、端末はそのホームネットワークによるその静的知識により、結合認証を実行する必要があることを推論する。端末は、AAA要求メッセージ（RQ1）をHAへ送信することにより、認証シーケンスを開始する。AAA要求は、EAP IDメッセージを運ぶオプションと同様に、AAAクライアント識別子オプションをも含む。AAAクライアント識別子オプションおよびEAP IDメッセージは、双方ともユーザのNAI（IMSI@アドレス体系）を含む。

【０１２３】

ステップ5-Cにおいて、HAは、AAAクライアント識別子オプションに含まれるNAIからASのアドレスを（必要な場合はDNSを使用して）導出し、AAA要求（AR）メッセージをASに送信する。ARは、ステップ5-BのAAAクライアント識別子オプション内で受信したEAP IDメッセージ（EAPペイロード属性において）およびNAI（ユーザ名属性において）を含む。

【０１２４】

ステップ5-Dにおいて、ASは、ステップCにおけるARメッセージを受けて、以下を実行する。

・　R-UIM認証手順の開始を示すEAP要求／R-UIM／要求開始メッセージを作成する。これを実行するため、ASはAuC（認証センター）とも連絡する。

・　EAP要求-UIM／開始（EAPペイロード属性において）と、ユーザを（ユーザ名属性において）識別するNAIとを含むAAA回答（AA）メッセージを、HAへ送信する。

【０１２５】

ステップ5-Eにおいて、HAは、組み込みデータオプションにEAP要求／R-UIM／開始を含むと共にAAAクライアント識別子オプション含む、AAA応答メッセージ（RP1）を端末へ送信する。AAAクライアント識別子オプションはユーザを識別するNAIを含む。

【０１２６】

ステップ5-Fにおいて、端末は、NAI（IMSI@アドレス体系）を含むAAAクライアント識別子オプションおよびEAP応答／R-UIM／開始メッセージを運ぶAAA組み込みデータオプションを含むAAA要求メッセージ（RQ2）を送信する。EAP応答／R-UIM／開始の理由フィールドは、セッションキーがホーム登録保護に使用されることを示す2（バイナリ10）に設定される（CAVE認証はステップIの後に実行され、ステップMの後、保護モビリティヘッダーのためHAによりIpsecセキュリティアソシエーションが作成される）。

【０１２７】
ステップ5-Gにおいて、HAは、AAAクライアント識別子オプションに含まれるNAIからASのアドレスを（必要な場合はDNSを使用して）導出し、AAA要求（AR）メッセージをASに送信する。ARは、ステップFのAAAクライアント識別子オプション内で受信したような、EAP応答／R-UIM／開始メッセージおよびNAIを（ベンダー固有Radius属性フィールドにおいて）含む。
【０１２８】
ステップ5-Hにおいて、ASは、ステップGにおけるARメッセージを受けて、以下を実行する。
・ NAIのIMSI部分に基づき、ASはユーザのための認証情報を有するAuCを識別する。
・ 必要な数だけのCave認証トリプレットを要求し、AuCから得る。これは、CAVEアルゴリズムのキー長さおよび使用されるIPsecサイファプロファイルID（IKE（インターネットキーエクスチェンジ）バージョン2において定義されているもののひとつ）により決定される。このプロファイルIDはEAPパケットで通信される。
・ 例えば、このEAP-R-UIMのために、上記で参照した文書H. Haverinenの「EAP SIM Authentication（作業中）」インターネットドラフト（draft－haverinen－pppext－eap－sim－10. txt）、インターネットエンジニアリングタスクフォース（2003年2月）に明記されている、値MAC_RANDおよびMAC_AUTHRを、AT_RANDおよびAT_MACとして計算する。
・ 後の使用のために、値MAC_AUTHRを格納する。
・ MAC_RAND値および2つのRAND値（認証トリプレットから得たもの）を含むEAP要求／R-UIM／チャレンジメッセージを作成する。
・ EAP要求／R-UIM／チャレンジおよびユーザを（ベンダー固有Radius属性フィールドにおいて）識別するNAIを含む、AAA回答（AA）メッセージをHAへ送信する。
【０１２９】
ステップ5-Iにおいて、HAは、AAA組み込みデータオプションにEAP要求／R-UIM／チャレンジを含むAAA応答メッセージ（RP2）、NAIを含むAAAクライアント識別子オプションを送信する。
【０１３０】
ステップ5-Jにおいて、端末は、ステップ5-IにおけるAAA応答を受けて、以下を実行する。
・ R-UIMを使用してAUTHR／AUTHUの2つの値を計算し、EAP要求／R-UIM／チャレンジ内でR-UIMモジュールにおけるRun_CAVEアルゴリズムに対するインプットとして受信した2つのRNAD値を得る。
・ 例えば、上記で参照した文書H. Haverinenの「EAP SIMAuthentication（作業中）」インターネットドラフト（draft－haverinen－pppext－eap－sim－10. txt）、インターネットエンジニアリングタスクフォース（2003年2月）に明記されている、値MAC_RANDおよびMAC_AUTHRを、AT_RANDおよびAT_MACとして計算する。
・ MAC_RAND値を、EAP要求／R-UIM／チャレンジ内で受信した値と比較する。値が一致する場合、EAP要求／R-UIM／チャレンジメッセージの認証は成功であり、そうでない場合、そのメッセージの認証は失敗する。
・ AAAクライアント識別子オプション（IMSI@アドレス体系の形をとるNAI）およびEAP要求／R-UIM／チャレンジをAAA組み込みデータオプションに含むAAA要求メッセージ（RQ3）をHAへ送信する。EAP要求／R-UIM／チャレンジメッセージは、計算されたMAC_AUTHR値を含む。
【０１３１】
ステップ5-Kにおいて、HAは、ARメッセージを（NAIにより識別された）ASに送信する。ARメッセージは、AAA要求のAAAクライアント識別子オプションにおいて受信したものとしてEAP要求／R-UIM／チャレンジおよびNAIを（ベンダー固有Radius属性フィールドにおいて）含む。
【０１３２】

ステップ5-Lにおいて、ASは、ステップKにおけるARメッセージを受けて、以下を実行する。

・ ステップ5-Dにおいて計算されたMAC_AUTHR値を、EAP要求／R-UIM／チャレンジに含まれるMAC_AUTHR値と比較する。値が一致する場合、CAVE認証は成功であり、そうでない場合、認証は失敗する。

・ ユーザを（Radius属性フィールドにおいて）識別するNAI，認証の成功（AAにおける応答メッセージ属性）または失敗（アクセス拒否メッセージにおける応答メッセージ属性）を示す結果コード，およびキー応答（サイファプロファイルID，キー，存続期間）を含む、AAメッセージをHAへ送信する。

【０１３３】

ステップ5-Mにおいて、HAは、ステップ5-LにおけるAAメッセージを受けて、CAVE認証が成功したか否かを知る。認証が成功した場合、HAはAAA応答メッセージ（RP3）をSUCCESS（値0）を示すように設定されたコードフィールドとともに端末へ送信する。端末がこのメッセージを受信すると、OWLANホーム登録認証およびキーイングは終了である。R-UIM認証が成功した場合、HAは、

【０１３４】

・ Mobile IPv4アプリケーションに関しては、Run_CAVEアルゴリズムを RUIMのために実行した際に得られたキー材料から適切なMobile IPv4状態へのMN-HA認証拡張に使用されるバインディングセキュリティアソシエーション（BSA）を必ず入力する。

・ Mobile IPv6アプリケーションに関しては、Run_CAVEアルゴリズムをR-UIMにおいて実行した際に得られたキー材料からSADBのための2つのIPSecセキュリティアソシエーションを必ず入力する。これらのSA（セキュリティアソシエーション）は、着信および発信登録（MIPv4）またはモビリティヘッダー（MIPv6）パケットのために、端末および使用されるIPsecサイファプロファイルIDにより識別されるようなその他のパラメータによって構成されている。この可能性のある作用は、IPsecモジュールのPfkeyインターフェイスを使用し、従ってR-UIMキーイングデーモンとIPsecモジュールとの間にいかなる特別なインターフェイスも必要としない。

【０１３５】

ステップ5Nにおいて、端末は、Mobile IPv4アプリケーションに関し、キー材料から作成されるように、BSAのものを使用して、Mobile-Home認証拡張をMobile IPv4登録要求（RREQ）の中へ形成するであろう。HAは、RREQのメッセージ認証を実行する際、対応するBSAをMN-HA認証拡張に対して自動的に適用するであろう。

【０１３６】

さらにステップ5-Nにおいて、Mobile IPv6アプリケーションに関しては、IPSecセキュリティアソシエーションが入力されたR-UIMが、送信されたパケットに自動的に適用されるよう、端末がIPSecで保護された対応付け更新をHAへ送信するであろう。HAがパケットを受信すると、そのIPSecモジュールはSAがもう着信するモビリティヘッダーパケットに適用できることを自動的に知る。このパケットはMobile IPv6 HOTI（ホーム試験開始）または対応付け更新（BU）メッセージであってよい。

【０１３７】

ステップ5-Oにおいて、HAは、Mobile IPv6アプリケーションに対し、受信したキー材料から作成されるように、Mobile-Home認証拡張を、BSAのものを使用して、構築されたMobile IPv4登録応答（RREP）へ適用するだろう。次いで端末は、RREPのメッセージ認証を実行する際、対応するBSAをMN-HA認証拡張に対し自動的に適用するであろう。

【０１３８】

さらに、Mobile IPv6アプリケーションに関しては、ステップ5-Oにおいて、HAのIPSecモジュールは、SAが入力されたR－UIMを使用して送信されたBack（結合確認）メッセージを自動的に保護するであろう。次いで、IPSecで保護されたモビリティヘッダーパケットをHAから受信すると、端末は自動的にIPSecセキュリティアソシエーションが入力されたR-UIMを、ステップNで使用されたものと逆方向に適用する。

【０１３９】
これは、モビリティシ・グナリング保護アプリケーションプロトコルのフローをうまく完了させる。Mobile IP／IPv6ホーム登録以外のアプリケーションでは、この種の手順を任意のIPsecSAを入力するために使用することができる。
【０１４０】
本発明は、上記の実施形態において説明したように、交換にかかわる様々なネットワークエンティティを実行することによって、ソフトウェアまたは組み込みハードウェアシステム、またはチップ要素において実施されることができる。端末における実装の重要な機能性は、標準R-UIM機能のためのAPIへのアクセス、およびカプセル化されたアドレスを含む任意IPパケットを構成するための能力である。アクセスコントローラにおいて、重要な機能はパケットカプセル化および、UDPまたはICMPv6等のアクセスAAAメッセージおよびRADIUSまたはDIAMETERメッセージ等のコアAAAメッセージへのカプセル開放、例えばNASREQアプリケーションから（例えば、P. Calhoun、W. Bulley、A. Rubens、J. Haag、G. Zorn. Diameter NASREQ Application（進行中）、インターネットドラフト（draft－ietf－aaa－diameter－nasreq－08. txt）、インターネットエンジニアリングタスクフォース（2001年11月）に記載されているように）適合することによるものである。また、本発明は、この方法のためのアクセス認証サービスポイントがどこに位置するかに応じて、アクセスルータ、ネットワークサーバ、またはPDSNの汎用パケットフィルタリング機能を再利用する可能性がある。
【０１４１】
第二の実施形態の実装における最良の形態の概要を図1に示す。最良の形態では、ネットワークやR-UIMハードウェア（第二の実施形態の場合）とのインターフェイスを備えるモバイル機器において、端末機能性を実装することであろう。この機能性は、IPアクセスルータ、アクセスサーバ、またはモバイル機器が無線ネットワークを通じて接続されている基地局によって、GRASPプロトコルメッセージを送受信するであろう。モバイル機器は、入力情報（チャレンジまたはRAND）を認証アルゴリズムに提供するネットワーク要素からメッセージを受信すると、CAVEアルゴリズムを実行するために、R-UIMにアクセスするであろう。これは、局所的に、応答およびネットワークと共有の秘密を生成する。
【０１４２】
ネットワークにおいて、本発明は、カプセル化されたメッセージをモバイル装置から受け取り、オペレータのネットワークに送り返すためにそれらをサーバベースのRADIUSプロトコルにおいて再カプセル化するような、アクセスルータ／WLAN基地局に追加されるソフトウェアによって実施されることができる。追加のソフトウェアを伴う任意のMobile IPホームエージェントがオペレータのネットワークに加えられると共に、RADIUSとCDMA2000 SS7メッセージの間のメッセージを翻訳するために、追加的にゲートウェイ（ASまたはAAAH）が使用される。このように、CAVEプロトコルのセキュリティは、MEおよびAuC／HLRの領域に制限され、CDMA2000ネットワークにおいて現存するインフラストラクチャは認証および認可のため、また場合により請求およびアカウンティングのためにさえ、再利用される。従って、IPまたはCDMA2000ネットワークへの変更は、まったく必要ないか、最小限ですむ。
【０１４３】
機能的な実装は、実装の仕様に応じて、例えばOS（オペレーションシステム）カーネル、ユーザレベルのソフトウェア等、オペレーションシステムの様々な場所で生じる可能性がある。
【０１４４】
以下、図6Aから6Cを参照し関連するネットワーク要素を簡単に説明する。上記の実施形態の説明に必要な手段のみを説明することが知られている。
【０１４５】
図6Aは、上記の実施形態に記載のアクセスコントローラ（AC）を示す。アクセスコントローラ1は、上述の開始メッセージが中でカプセル化された認証メッセージを受信する受

信手段1aを備える。さらにアクセスコントローラは処理手段1bを備える。処理手段1bは、カプセル化された開始メッセージ（例えば、上述のようにクライアントタイプ、ユーザID、およびコアアドレス情報を含むクライアント識別子オプションメッセージおよびEAP（拡張認証プロトコル）IDオプションメッセージ）を読み出す。カプセル化されたメッセージは、その後、転送手段1cにより、そのカプセル化されたメッセージ内において識別された認証サーバへ転送される。

【０１４６】

図6Bはモバイル端末2を示す。モバイル端末は、加入者機器の一例にすぎないことに注意されたい。モバイル端末2は、少なくともひとつのネットワークアクセスタイプを示す情報メッセージ（すなわち上述のルータ通知RA）を受けて、ネットワークアクセスタイプを判定する、判定手段2aを備える。さらにモバイル端末3は、上述のような開始メッセージを作成する作成手段2bを備える。移動局2のカプセル化手段2cは、情報メッセージにおいて識別されるアクセスネットワークと互換性がある認証メッセージ内において、開始メッセージをカプセル化し、移動局2の送信手段2dは、開始メッセージをアクセスコントローラへ送信する。

【０１４７】

図6cは上記の実施形態において使用されるようなルータ3を示す。ルータ3は、上述した情報メッセージ、すなわちルータ通知を作成する作成手段3aを備える。ルータ3の送信手段3bは、情報メッセージを加入者機器へ送信する。ルータ3およびアクセスコントローラ1はひとつのユニット内に配置されてもよいことが知られている（上述の実施形態に記載のとおり）。

【０１４８】

本発明は、上述の実施形態に限定されるものではなく、特許請求の範囲内において変化してもよい。

【０１４９】

例えば、上記の実施形態は、USIMを使用するEAP-AKA認証機構およびCAVEアルゴリズムに基づくR-UIMを使用する認証が両方使用されるように、自由に結合されることができる。

【０１５０】

モバイル機器およびアクセスネットワークの間のプロトコルはUDP、ICMP、ICMPv6等のネットワーク層プロトコルまたはIEEE802．1x、IEEE802．11i、およびブルートゥースプロファイル等のリンク層プロトコルのうち少なくともひとつを備えてよい。

【０１５１】

さらに、上述した実施形態には以下のバリエーションが存在する。

【０１５２】

1．EAP-SIM方法の再利用

（例えば上述のように第二の実施形態に関連して）認証機構がR-UIMを使用する方法は、EAP-SIMと呼ばれるSIMのための方法と同じプロトコルカプセル化に組み込まれる。この使用法では、CAVEアルゴリズムによる、R-UIMに基づく認証の運搬のためのEAP-SIMプロトコルを再利用している。

【０１５３】

EAP-SIMの代替使用の指示は、EAP-SIMプロトコルにおいて予備フィールドを使用して示されてよく、あるいは追加の属性であってよく、それをAT-R-UIMと呼ぶ。

【０１５４】

2．スマートカードアルゴリズムのためのネットワーク側の終端位置

スマートカード（CAVEまたはAKA秘密アルゴリズム）で動作するものに対応するアルゴリズムのネットワーク側の終端ポイントは、原理上、HLR／AuCにあるか、ホームAAAサーバAAAH（図1）内で同一場所に位置する可能性がある。前者の場合には、G_hと呼ばれるインターフェイスが存在し、それによってホームAAAサーバはトリプレット／クインテットを表すダイアログをG_h上の携帯電話ネットワークプロトコルを使用して関連するスマート

カードアルゴリズムに伝播する。

【０１５５】

さらに、モバイル端末または機器は、加入者端末の一例にすぎないことが知られている。「モバイル」という用語は、モバイル端末が無線リンクを経由してネットワークに接続されていることだけを意味するのではなく、例えば固定ケーブルを経由して異なるネットワークアクセス手段に接続される可能性がある端末をも意味する。例えばこれは、ホテルの部屋や電車等の中で固定ネットワークに接続される可能性のあるコンピュータのような、固定ネットワーク端末に接続可能なコンピュータを含んでよい。

【図面の簡単な説明】

【０１５６】

【図１】本発明の実施形態に従うCDMA2000マルチアクセスネットワーク参照モデルを示す。

【図２Ａ】本発明の第一の実施形態に従ったシグナルフローを示す。

【図２Ｂ】本発明の第一の実施形態に従ったシグナルフローを示す。

【図３Ａ】本発明の第一の実施形態の第二例に従ったシグナルフローを示す。

【図３Ｂ】本発明の第一の実施形態の第二例に従ったシグナルフローを示す。

【図４Ａ】本発明の第二の実施形態の第一例に従ったシグナルフローを示す。

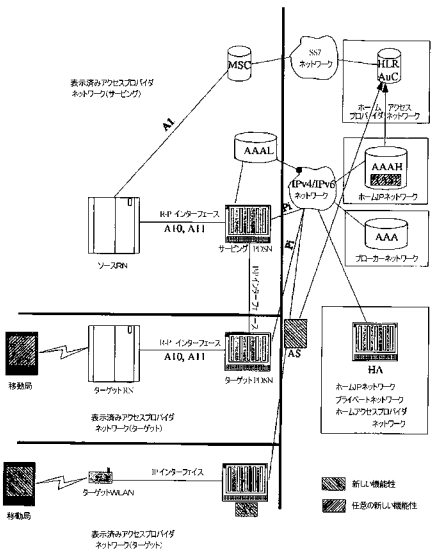
【図４Ｂ】本発明の第二の実施形態の第一例に従ったシグナルフローを示す。

【図５Ａ】本発明の第二の実施形態の第二例に従ったシグナルフローを示す。

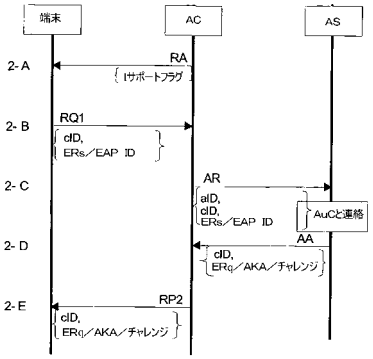
【図５Ｂ】本発明の第二の実施形態の第二例に従ったシグナルフローを示す。

【図６】図6A～Cは、それぞれ本発明の実施形態に従って使用可能なアクセスコントローラ、移動局、ルータを示す。

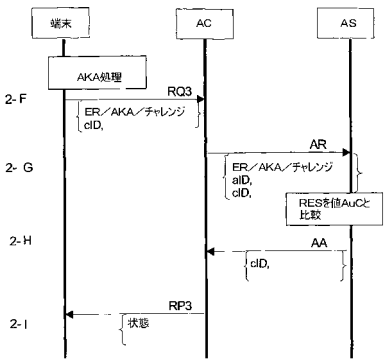
【図１】



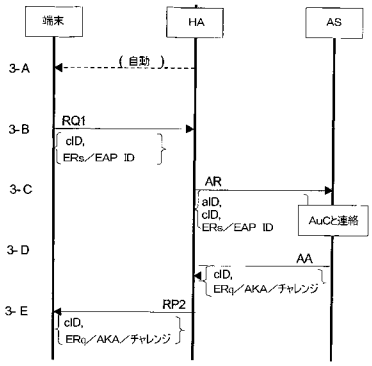

【図２Ａ】



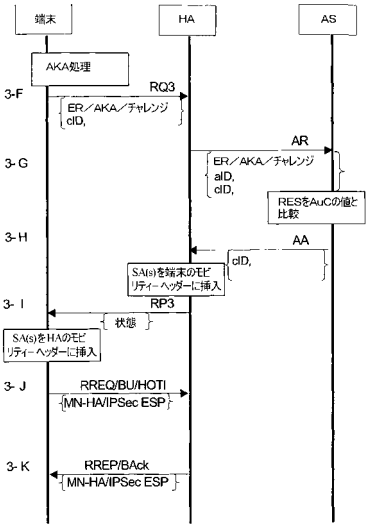

【図２Ｂ】



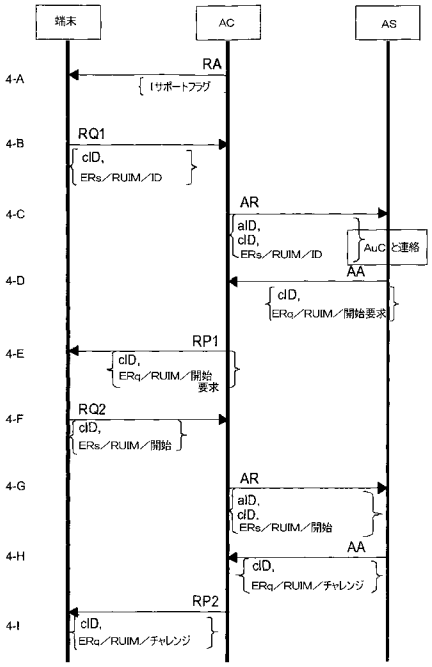
【図３Ａ】



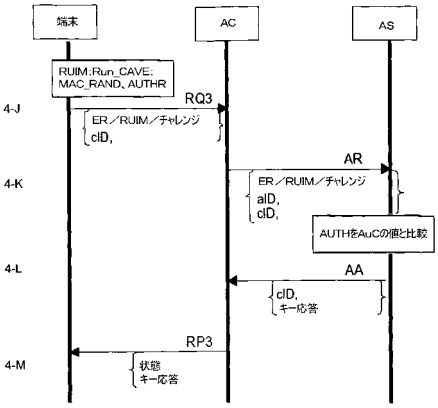

【図３Ｂ】



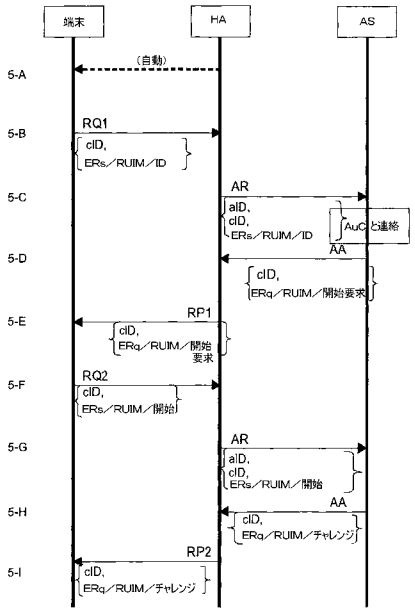

【図４Ａ】



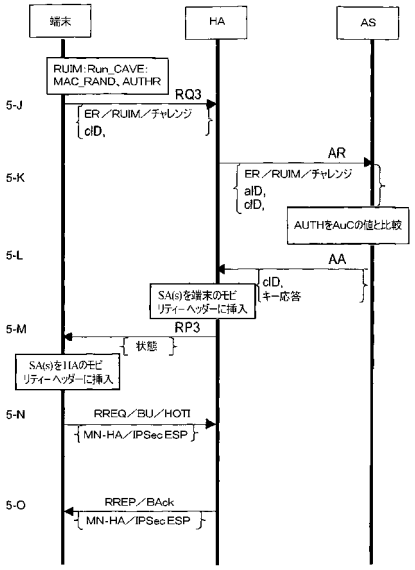

【図４Ｂ】



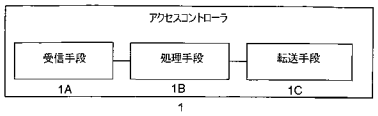
【図５Ａ】



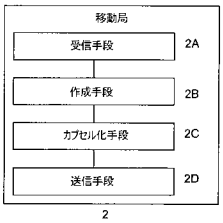

【図５Ｂ】



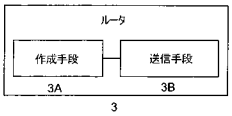

【図６】




6A




6B




6C

フロントページの続き

(72)発明者　サハスラバデェ　メガーナ
アメリカ合衆国カリフォルニア州９５１３４，サンノゼ，リバーオークスサークル３７３，１４０２番

審査官　岸野　徹

(56)参考文献　米国特許出願公開第２００３／０１１９４８１（ＵＳ，Ａ１）
特開平１０－２１０５３５（ＪＰ，Ａ）
特開２００２－０７３４２４（ＪＰ，Ａ）
国際公開第０２／０４５４５２（WO，Ａ１）
国際公開第０３／０３０４４５（WO，Ａ１）
国際公開第０１／０７６１３４（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/20
G09C　 1/00
H04W　12/06