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

特許第5166524号
(P5166524)

(45)発行日　平成25年3月21日(2013.3.21)　(24)登録日　平成24年12月28日(2012.12.28)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675D
H04W 12/04 (2009.01)　H04W 12/04

請求項の数 6　(全 25 頁)

(21)出願番号　特願2010-512108 (P2010-512108)
(86)(22)出願日　平成19年6月11日 (2007.6.11)
(65)公表番号　特表2010-532596 (P2010-532596A)
(43)公表日　平成22年10月7日 (2010.10.7)
(86)国際出願番号　PCT/SE2007/050407
(87)国際公開番号　WO2008/153456
(87)国際公開日　平成20年12月18日 (2008.12.18)
審査請求日　平成22年5月11日 (2010.5.11)

(73)特許権者　598036300
テレフオンアクチーボラゲット　エル　エム　エリクソン（パブル）
スウェーデン国　ストックホルム　エス－１６４　８３
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治

最終頁に続く

(54)【発明の名称】証明書処理のための方法および装置

(57)【特許請求の範囲】
【請求項１】
ユーザ機器（１０５）が、セキュリティゲートウェイ（１２０／１２５）経由で訪問先ネットワークまたはホームネットワーク（１１０／１１５）にアクセスする場合における、アクセスネットワークへのアクセスにおける認証手順に従った処理を実行する方法であって、
前記ユーザ機器（１０５）と前記セキュリティゲートウェイ（１２０／１２５）とが、利用可能な証明書（群）についての情報を交換するステップ（３１０）と、
前記ユーザ機器（１０５）と前記セキュリティゲートウェイ（１２０／１２５）とが、前記利用可能な証明書（群）を比較することにより前記セキュリティゲートウェイ（１２０／１２５）の試行された認証の進行を妨げる不一致であって、前記ユーザ機器（１０５）と前記セキュリティゲートウェイ（１２０／１２５）との間の証明書の不一致を識別するステップ（３１５）と、
証明書サーバ（１４０）が前記認証手順の少なくとも一部を支援するステップ（３２０）であって、前記証明書サーバ（１４０）が、前記セキュリティゲートウェイ（１２０／１２５）あるいは前記ユーザ機器（１０５）に少なくとも１つの証明書を提供することによって、前記セキュリティゲートウェイ（１２０／１２５）と前記ユーザ機器（１０５）が、一致する証明書を少なくとも１つ有するように、前記認証手順の少なくとも一部を支援するステップと、
前記ユーザ機器（１０５）が、前記セキュリティゲートウェイ（１２０／１２５）に、

自身の利用可能なルート証明書（群）の指示を提供するステップ（４１０）と、
前記セキュリティゲートウェイ（１２０／１２５）が、前記ユーザ機器（１０５）から指示される利用可能な証明書（群）と、記憶されている証明書（群）とを比較するステップ（４１５）と、
前記セキュリティゲートウェイ（１２０／１２５）が、前記指示される証明書（群）に一致する記憶されている証明書を検出できない場合、前記セキュリティゲートウェイ（１２０／１２５）が、前記証明書サーバ（１４０）に一致する証明書をリクエストするステップ（４２０）と、
前記証明書サーバ（１４０）が、一致する証明書とそれに関係する鍵ペアを生成するステップ（４２２）と、
前記証明書サーバ（１４０）が、前記一致する証明書とそれに関係する鍵ペアを、前記セキュリティゲートウェイ（１２０／１２５）へ送信するステップ（４２５）と、
前記セキュリティゲートウェイ（１２０／１２５）が、前記一致する証明書を、前記ユーザ機器（１０５）へ送信するステップ（４２７）と、
前記ユーザ機器（１０５）が、受信した前記一致する証明書を有効にするステップ（４２８）と
を備えることを特徴とする方法。
【請求項２】
前記証明書サーバは、前記ユーザ機器（１０５）の前記ホームネットワーク内のＡＡＡサーバである
ことを特徴とする請求項１に記載の方法。
【請求項３】
前記認証手順の少なくとも一部を支援するステップは、前記ユーザ機器（１０５）に代って、前記セキュリティゲートウェイの認証の一部を実行することによって、前記認証手順を支援することを含むステップであって、
前記セキュリティゲートウェイ（１２０／１２５）が、少なくとも１つの証明書を、前記ユーザ機器（１０５）へ送信するステップ（５１０）と、
前記ユーザ機器（１０５）が、前記セキュリティゲートウェイ（１２０／１２５）から受信される前記証明書と、記憶されているルート証明書群とを比較するステップ（５１５）と、
前記ユーザ機器（１０５）が、前記ユーザ機器（１０５）に記憶されているルート証明書群を使用して、前記セキュリティゲートウェイ（１２０／１２５）から受信した前記証明書を有効にできない場合、前記ユーザ機器（１０５）が、前記受信した証明書を、前記セキュリティゲートウェイ（１２０／１２５）を介して前記証明書サーバ（１４０）へ送信するステップ（５２０）と、
前記証明書サーバ（１４０）が、前記セキュリティゲートウェイ（１２０／１２５）からの前記証明書を有効にするステップ（５２２）と、
前記証明書サーバ（１４０）が、前記有効にすることである有効化の結果の指示を、前記ユーザ機器（１０５）へ送信するステップ（５２５）と
を更に備えることを特徴とする請求項１に記載の方法。
【請求項４】
前記ステップ（５２０）において前記ユーザ機器（１０５）が、前記セキュリティゲートウェイ（１２０／１２５）を介して前記証明書サーバ（１４０）へ送信される前記証明書は、ＥＡＰ認証手順中に前記証明書サーバ（１４０）へ送信され、
前記証明書は、メッセージ属性に含まれる
ことを特徴とする請求項３に記載の方法。
【請求項５】
前記有効化の結果の指示は、ＥＡＰ認証手順中に前記ユーザ機器へ送信され、
前記指示は、メッセージ属性に含まれる
ことを特徴とする請求項３に記載の方法。

【請求項６】
通信ネットワークにおけるユーザ機器（１０５）と証明書サーバ（１４０）と通信するように構成されているセキュリティゲートウェイ（１２０／１２５）であって、
通信モジュール（８３５）と、
証明書記憶モジュール（８４５）に接続している証明書処理モジュール（８４０）とを備え、
前記証明書処理モジュール（８４０）は、前記ユーザ機器（１０５）との認証手順において、少なくとも１つ提供されている証明書と、予め記憶されている少なくとも１つの証明書とを比較し、一致する証明書が識別されない場合、前記証明書処理モジュール（８４０）は、前記証明書サーバに、一致する証明書を提供することをリクエストし、前記一致する証明書を受信し、前記ユーザ機器との前記認証手順において前記一致する証明書を使用するように構成されている
ことを特徴とするセキュリティゲートウェイ。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、アクセスネットワークにおける認証（authentication）および認（authorization）のための方法および装置に関するものである。特に、本発明は、そのようなネットワークにおける証明書（certificate）の処理に関するものである。
【背景技術】
【０００２】
ネットワークにアクセスしているユーザのアイデンティティを認証する必要性、および同等の意味でユーザもしくはクライアントに対するネットワークエンティティを認証する必要性は、既存および将来の通信システムの多くにおいて明らかにある。特に、認証問題は、ユーザが複数の異なるネットワークにアクセスし、異なるオペレータおよびサービスプロバイダによって提供される広範なサービスを利用するローミング状況で生じる。ユーザ／クライアントとネットワークエンティティとの間の安全な通信のための広く行き渡っている技術は、クライアントとアクセスネットワークのセキュリティゲートウェイ（ＳＥＧＷ：Security Gateway）との間に、いわゆるセキュアトンネル（secure tunnel）を確立することである。
【０００３】
確立されたセキュアトンネル技術の一例は、ＩＰｓｅｃ（インターネットプロトコルセキュリティ：Internet Protocol security）として知られており、これは、様々な通信システムにおいていくつかのアクセス方法のために利用されている［７］［８］。このセキュアな接続は、ＩＫＥｖ２（インターネットキー交換バージョン２：Internet Key Exchange version 2）［６］と呼ばれるキー交換手順を使用して確立され、これは、クライアントに対するユーザ認証方法として、例えば、加入者アイデンティティモジュール（ＥＡＰ－ＳＩＭ）［１０］に基づく拡張認証プロトコル（ＥＡＰ：Extensible Authentication Protocol）、または認証とキーアグリーメント（鍵共有）（ＥＡＰ－ＡＫＡ（Extensible Authentication Protocol Authentication and Key Agreement））［１１］を利用する。このアクセスメカニズムの使用の一例は、ＷＬＡＮまたはＢｌｕｅｔｏｏｔｈによって提供される端末へのレイヤ２接続を使用して、ＩＰネットワーク経由でＧＳＭネットワークにアクセスする方法である。これについては、第３世代パートナーシッププロジェクト（３ＧＰＰ）によってリリース６から仕様が定められており、汎用アクセスネットワーク（ＧＡＮ：Generic Access Network）［１２］［１３］（ときにはまたは以前は、未認可移動体アクセス、ＵＭＡ（Unlicensed Mobile Access）と呼ばれる）として一般に知られている。別の例は、３ＧＰＰによって仕様が定められているインターワーキングＷＬＡＮ［１４］［１５］［１６］アクセス方法である。第３の例は、予想される３ＧＧのＳＡＥ（System Architecture Evolution）アーキテクチャの中での、非３ＧＰＰアクセスネットワーク経由のホームエージェント（ＨＡ）へのモバイルＩＰｖ６（ＭＩＰｖ６）アク

セスである。ＩＫＥｖ２では、一方の通話者に対してＥＡＰ［９］に基づく認証が使用される場合、他方の通話者に対しては証明書に基づく認証が使用されなければならないと指示している。関係するアクセスタイプに関しては、これは、ＩＫＥｖ２では、端末、すなわち、ユーザ機器（ＵＥ）／移動局（ＭＳ）に対して、ＳＥＧＷが証明書を用いて認証されることを意味する（例えば、Ｉ－ＷＡＮに関する［１６］参照）。ＩＫＥｖ２ネゴシエーション中、ＳＥＧＷは、自装置の証明書をＵＥに提供する。これは、実際には証明書チェーンで、１つの証明書だけではなくてもよいが、簡単にするために本明細書では、以下では、このＳＥＧＷの動作を証明書の提供と呼ぶことに留意されたい。用語「証明書チェーン」については、詳細な説明の中で定義する。ＳＥＧＷの証明書に関する証明書チェーンの最上位にあり、それゆえ、証明書の有効性に最高の保証を与える認証局（ＣＡ）と同じ認証局からの「ルート」証明書を、ＵＥは有すると想定している。このルート証明書を用いて、ＵＥは、ＳＥＧＷから受信される証明書を認証することができ、それゆえ、ＳＥＧＷを認証することができる。

【０００４】

オペレータ間のローミングの場合に、ＵＥは、ホーム公衆陸上移動通信ネットワーク（ＨＰＬＭＮ：Home Public Land Mobile Network）から、訪問先ＰＬＭＮ（ＶＰＬＭＮ）のＳＥＧＷに連絡し使用するように指示されてもよい。このローミング状況は、ＧＡＮの中に、およびＩ－ＷＬＡＮアクセスに関するいくつかの状況に、およびたぶんＳＡＥの中で存在する。ＵＥは、ＳＥＧＷにロードされている証明書につながる証明書チェーンの最上位を提供する認証局（ＣＡ）のルート証明書を有する必要がある。第１のＰＬＭＮのオペレータが別のＰＬＭＮのオペレータとローミングアグリーメント（協定）に署名する場合、第１のオペレータのすべてのＵＥは、その別のＰＬＭＮで使用されるＣＡのルート証明書で更新される必要があるであろう。また、オペレータは、何らかの理由で使用しているＣＡを変更する必要があるかもしれないし、また、複数のＣＡを有する必要があるかもしれない。特に、現在のところ「ＯＴＡ」（Over The Air）プロビジョニングを使用して端末に新規の証明書をロードさせることができないので、これは手作業のタスクであるから、すべてのＵＥのルート証明書を更新することは非常に大きなタスクである。

【０００５】

現在想定している状況からさらなる問題が生じる。例えば、ＧＡＮの場合は、各移動機器（ＭＥ：Mobile Equipment）、すなわち、加入者アイデンティティモジュール（ＳＩＭ：Subscriber Identity Module）カード／ユニバーサル集積回路カード（ＵＩＣＣ：Universal Integrated Circuit Card）を除くＵＥは、製造時に１つ以上の限られたセットのルート証明書がロードされる。従って、このまたはこれらの証明書（群）は、ＭＥ製造業者が適切であると考える証明書であろう。ＭＥは潜在的に任意のネットワークの任意のユーザによって使用されるので、ＭＥのルート証明書（群）と連絡されたＳＥＧＷによってリクエストされるルート証明書との間のマッチング（一致）問題が、非ローミングの場合にも存在することがある、すなわち、ＭＥがユーザのＨＰＬＭＮのＳＥＧＷにアクセスする場合にも存在することがある。

【０００６】

このように、既存のソリューションに付随する問題は、ＳＥＧＷの証明書（群）とＵＥのルート証明書（群）との間で起こり得る不一致または非互換性として説明され得り、これは、ＵＥがＳＥＧＷの証明書の有効性を検証することができない結果となり、これは、ＵＥがＳＥＧＷを認証できないことを意味する。

【発明の概要】

【発明が解決しようとする課題】

【０００７】

明らかに、アクセスしているユーザ機器に対してセキュリティゲートウェイの認証に使用可能な証明書を提供するための方法および装置の改善が必要である。

【課題を解決するための手段】

【０００８】

本発明の目的は、先行技術の課題を解消する方法および装置を提供することである。本発明の目的は、請求項１に定義される方法、請求項２４に定義される証明書サーバ、請求項２８に定義されるユーザ機器、および請求項３０に定義されるゲートウェイによって達成される。

【０００９】

本発明に従う方法は、ユーザ機器が通信ネットワークのセキュリティゲートウェイ経由で訪問先ネットワークまたはホームネットワークにアクセスする場合に適用できる認証手順を提供する。初期フェーズでは、ユーザ機器とセキュリティゲートウェイが、自装置で証明書を提供する、または利用可能な証明書を特定する指示を提供することによって、利用可能な証明書（群）についての情報を交換する。

【００１０】

ユーザ機器とセキュリティゲートウェイに一致する証明書がない場合、既存のプロトコルおよび装置に従って、セキュリティゲートウェイの試行された認証を行うことができない。本発明に従えば、証明書の不一致が確認される場合、証明書サーバを参加させる。証明書サーバは、セキュリティゲートウェイとは別のエンティティであり、認証手順の少なくとも一部を支援する。いったん認証が確認されると、ユーザ機器とセキュリティゲートウェイとの間にセキュアトンネルを確立でき、そして、ペイロードトラヒックを送信することができる。

【００１１】

本発明の一実施形態に従えば、証明書サーバは、セキュリティゲートウェイまたはユーザ機器に少なくとも１つの証明書を提供することによって、セキュリティゲートウェイとユーザ機器が少なくとも１つの一致する証明書を有するようにすることにより、認証の一部を支援する。この実施形態は、

－ユーザ機器が、その利用可能なルート証明書の指示をセキュリティゲートウェイに提供するステップと、

－セキュリティゲートウェイが、ユーザ機器からの利用可能な証明書の指示を記憶されている証明書と比較するステップと、

－セキュリティゲートウェイが、指示されている証明書に一致する記憶されている証明書を検出できない場合、証明書サーバから一致する証明書をリクエストするステップと、

－証明書サーバが、一致する証明書およびそれに関連する鍵ペアを生成するステップと、

－証明書サーバが、その証明書およびそれに関連する鍵ペアをセキュリティゲートウェイに送信するステップと、

－セキュリティゲートウェイが、一致する証明書をユーザ機器に送信するステップと、

－ユーザ機器が、受信した証明書を有効にするステップと

を備える。

【００１２】

別の実施形態に従えば、証明書サーバが、ユーザ機器に代わって、セキュリティゲートウェイの認証の一部を実行することによって、認証を支援する。この実施形態は、

－セキュリティゲートウェイが、少なくとも１つの証明書をユーザ機器に送信するステップと、

－ユーザ機器が、セキュリティゲートウェイから受信される証明書を、記憶されているルート証明書と比較するステップと、

－ユーザ機器が、自身に記憶されているルート証明書を使用して、セキュリティゲートウェイから受信される証明書の有効にできない場合に、その受信した証明書を証明書サーバに送信するステップと、

－証明書サーバが、セキュリティゲートウェイからの証明書を有効にするステップと、

－証明書サーバが、有効性にすることである有効化の結果の表示を、ユーザ機器に送信するステップと

を備えてもよい。

【００１３】
代替形態として、証明書サーバにセキュリティゲートウェイの証明書を有効にするようにリクエストする代わりに、ユーザ機器は、証明書サーバに必要なルート証明書を送信するようにリクエストし、ユーザ機器自体がセキュリティゲートウェイの証明書を有効にしてもよい。そのルート証明書に対するリクエストにおいて、ユーザ機器は、セキュリティゲートウェイの証明書、または必要とされるルート証明書の表示のどちらかを含める。証明書サーバは、必要とされるルート証明書にアクセスできるなら、ルート証明書をユーザ機器に返信する。ユーザ機器は、セキュリティゲートウェイの証明書を有効にするために、取得されているルート証明書を使用し、また、追加およびオプションで、後での使用のためにルート証明書を記憶してもよい。
【００１４】
本発明の一実施形態は、証明書サーバとセキュリティゲートウェイとの間および証明書サーバとユーザ機器との間の信頼／セキュリティ関係を活用する。
【００１５】
本発明のおかげで、セキュリティゲートウェイの証明書と、アクセスしているユーザ機器のルート証明書（群）との間の不適合／不一致の問題が解決される。
【００１６】
本発明の実施形態は、ネットワークに完全に限定されていて、ＵＥに全く影響を及ぼさないようにできる解決手段を提供し、これは一定の環境では好ましいことがある。他の実施形態では、ホームＡＡＡサーバ（証明書サーバ）とセキュリティゲートウェイとの間の、およびホームＡＡＡサーバとユーザ機器との間の、信頼／セキュリティ関係を活用することによって、潜在的な管理上の問題を回避する。
【００１７】
本発明に従う方法は、求められているネットワークのゲートウェイ（ＳＥＧＷと示される）への動的に確立されているＩＰｓｅｃトンネルをアクセスメカニズムとして使用する、任意のタイプのアクセスにも十分に適用できるほど汎用的である。典型的な例には、ＧＡＮ（以前は、ＵＭＡと呼ばれている）およびＩ－ＷＬＡＮを含んでいる。この解決手段を適用できる追加の例は、予想される３ＧＰＰのＳＡＥアーキテクチャにおけるＭＩＰｖ６のホームエージェントへのアクセスである。
【００１８】
本発明の実施形態は、ユーザ機器へのオンライン証明書状態プロトコル（ＯＣＳＰ：Online Certificate Status Protocol）の実装およびユーザ機器での使用の必要性も排除する。本発明の実施形態に従えば、ＯＳＣＰは、代わりに、証明書サーバに実装されてもよい。
【００１９】
本発明の実施形態は、従属請求項に規定されている。本発明の他の目的、利点および新規の特徴は、本発明の以下の詳細な説明を、添付の図面および請求項とともに考慮することによって、明らかになるであろう。
【００２０】
本発明について、これより図を参照して詳細に説明する。
【図面の簡単な説明】
【００２１】
【図１】本発明に従う方法および装置を利用し得るアクセス状況を示す概念図である。
【図２ａ】完全なＥＡＰ－ＳＩＭ認証手順を利用するＩＰｓｅｃトンネルの確立を示すシグナリング図である。
【図２ｂ】ＥＡＰ－ＳＩＭ高速再認証手順を利用するＩＰｓｅｃトンネルの確立を示すシグナリング図である。
【図２ｃ】完全なＥＡＰ－ＡＫＡ認証手順を利用するＩＰｓｅｃトンネルの確立を示すシグナリング図である。
【図２ｄ】ＥＡＰ－ＡＫＡ高速再認証手順を利用するＩＰｓｅｃトンネルの確立を示すシ

グナリング図である。
【図３】本発明の一実施形態に従う認証方法を示す概念図である。
【図４ａ】本発明の一実施形態に従う認証方法を示す概念図である。
【図４ｂ】図４ａの認証方法に対応するシグナリング図である。
【図５ａ】本発明の一実施形態に従う認証方法を示す概念図である。
【図５ｂ】図５ａの認証方法に対応する完全なＥＡＰ－ＳＩＭ認証手順のシグナリング図である。
【図５ｃ】図５ａの認証方法に対応するＥＡＰ－ＳＩＭ高速再認証手順のシグナリング図である。
【図５ｄ】図５ａの認証方法に対応する完全なＥＡＰ－ＡＫＡ認証手順のシグナリング図である。
【図５ｅ】図５ａの認証方法に対応するＥＡＰ－ＡＫＡ高速再認証手順のシグナリング図である。
【図６ａ】本発明の一実施形態に従う認証方法を示す概念図である。
【図６ｂ】図６ａの認証方法に対応するシグナリング図である。
【図７】本発明の一実施形態を示すシグナリング図である。
【図８ａ】本発明に従う証明書サーバを示す概念図である。
【図８ｂ】本発明に従うユーザ機器を示す概念図である。
【図８ｃ】本発明に従うセキュリティゲートウェイを示す概念図である。
【発明を実施するための形態】
【００２２】
本発明について、以下に本発明の好ましい実施形態を示す添付の図面を参照して、より詳細に説明する。しかしながら、本発明は、異なる多くの形態で例示されてもよいので、本明細書に記載されている実施形態に限定されると解釈されるべきでない。むしろ、これらの実施形態は、本開示が完全かつ完成されているものであり、かつ、当業者に本発明の範囲を十分に伝えるために提供されている。
【００２３】
これからの説明では、以下の定義を使用する。
【００２４】
「ＡＡＡ」（Authentication, Authorization and Accounting）：認証・認可・課金は、ユーザのアイデンティティを認証し、ユーザにネットワークのサービスおよびリソースを使用することを認可し、料金請求（charging）および統計に使用する目的でユーザの通信セッションに関する課金データを収集するために、ネットワークによって実行される手順および動作を示している。この手順には、アクセスネットワークとホームネットワークとの間の通信、具体的には、ＡＡＡクライアントとＡＡＡサーバとの間の（場合によっては、訪問先ネットワークのＡＡＡプロキシ経由の）通信が介在する。この通信では、例えば、ＲＡＤＩＵＳ［１］［２］またはＤｉａｍｅｔｅｒ［３］［４］［５］等のＡＡＡプロトコルを使用する。
【００２５】
証明書（Certificate）：証明書の目的は、ある公開鍵（public key：パブリックキー）（公開鍵－秘密鍵ペアの中から）がある当事者に発行されていることを証明することである。証明書には、典型的には、関係する公開鍵、所有者のアイデンティティ、有効期限、証明書発行者のアイデンティティ、および場合によっては他の関連属性を含んでいる。証明書が有効であることを証明するために、公開鍵－秘密鍵ペアの発行者、つまり、証明書の発行者は、証明書にその（すなわち、発行者の）秘密鍵でデジタル署名する。
【００２６】
通信セッション中にＢがＡから証明書を受信する場合、Ｂが発行者を信頼する、すなわち、発行者が信頼できる第三者機関であるという条件で、Ｂは、証明書発行者の公開鍵を使用して、証明書ひいては関係する公開鍵の有効性を検証することができる。
【００２７】

証明書チェーン（Certificate chain）：Ａが公開鍵－秘密鍵ペアおよび関係する証明書をＢに発行し、証明書にその秘密鍵で署名すると想定する。公開鍵－秘密鍵ペアを有することで、Ｂは次いで別の公開鍵－秘密鍵ペアおよび証明書をＣに発行でき、今度はＣが公開鍵－秘密鍵ペアおよび証明書をＤに発行することもできる。証明書の各発行者は、証明書に各自の秘密鍵で署名し、その有効性を証明する。このようにして、証明書は、信頼と有効性保証の階層的シーケンスで一緒に結びつけられ、そこでは、チェーン内の各証明書の有効性は、その発行者の公開鍵を使用して検証することができ、この公開鍵は、その証明書チェーン内の次の階層レベルの証明書の中に含まれている。この場合、この発行者の公開鍵の有効性は、順に次の階層レベルの証明書の中の公開鍵を使用して検証することができる。従って、ある証明書を有効にする（validate）ために、当事者は、階層チェーンを追跡してもよく、途中で各証明書の有効性を検証して、信頼できる発行者が検出されるまで続けて、検出されたら検証シーケンスを終了することができる。このような証明書の階層的チェーンは、証明書チェーンと呼ばれる。

【００２８】

ルート証明書（Root certificate）：証明書チェーンの最上位は、ルート証明書と呼ばれる。ルート証明書の有効性を証明することができる階層的にそれより高いレベルがないので、ルート証明書は、署名されていないかまたはその所有者の秘密鍵で署名されている（すなわち、自己署名されている）。

【００２９】

ルート証明書が実用的であるためには、ルート証明書を使用する当事者が、所有者の公開鍵を公知と見なさなければならず、その所有者を信頼しなければならない。（実際には、例えば、ソフトウェアアプリケーションの中に事前に記憶されている等の「安全な」方法でのルート証明書の提供が、公開鍵を周知させる１つの方法であり、この場合、必要とされる信頼が「安全な」提供（プロビジョン）の前提条件となる。

【００３０】

認証局（ＣＡ：Certificate Authority）：証明書チェーンを最終的に有効にする成功に導くためには、証明書チェーンは信頼できる第三者機関を含まなければならない。信頼できる第三者機関は、多対多の関係の環境の中で公開鍵－秘密鍵ペアおよび証明書を使用するための前提とも見なされてもよい。証明書を発行する信頼できる第三者機関は認証局（ＣＡ）と呼ばれる。ＣＡのルート証明書は、典型的には、証明書チェーンの最上位にある。それゆえ、ＣＡのルート証明書は、典型的には、署名されていない、または自己署名されているが、異なるＣＡが互いのルート証明書に相互署名（cross-sign）する可能性もある（これは、証明書チェーンに階層レベルを加えると見なすべきでない）。相互署名の目的は、異なる当事者が異なるＣＡのサブセットを信頼する場合に備えて、ある当事者があるルート証明書を信頼できる確率を高めることである。

【００３１】

推移信頼（Transitive trust）：ＡがＢを信頼し、ＢがＣを信頼する場合、推移信頼は、ＡがＣを自動的に信頼することを意味する。

【００３２】

以下の表記法が、図２～図７のシグナリング図で使用される。

【００３３】

プロトコルＸ（…）｛プロトコルＹ｝

これは、プロトコルＸメッセージにカプセル化されているプロトコルＹメッセージを示している。例えば、ＩＫＥｖ２｛ＥＡＰ｝は、ＩＫＥｖ２［６］メッセージにカプセル化されているＥＡＰパケットを示している。「（…）」の表記は、プロトコルＸメッセージの取り得る属性／パラメータ／ペイロードを示している。

【００３４】

プロトコルＸ（属性Ｚ…）

これは、属性Ｚを含むプロトコルＸのメッセージを示している。例えば、ＩＫＥｖ２（ＣＥＲＴＲＥＱ…）は、少なくとも（点々で示される）ＣＥＲＴＲＥＱペイロー

ドを含むＩＫＥｖ２メッセージを示している。
【００３５】
プロトコルＸ（［属性Ｒ］…）
これは、オプションの属性Ｒを含むことができるプロトコルＸのメッセージを示している。例えば、ＩＫＥｖ２（［ＣＥＲＴＲＥＱ］…）は、オプションで（少なくとも）ＣＥＲＴＲＥＱペイロードを含むＩＫＥｖ２メッセージを示している。
【００３６】
プロトコルＸ（属性Ｚ＝ｚ）
これは、属性Ｚが「ｚ」を示すプロトコルＸのメッセージを示している。これは、例えば、ＩＫＥｖ２（ＣＥＲＴＲＥＱ＝ＶｅｒｉＳｉｇｎ）は、ＣＡ ＶｅｒｉＳｉｇｎを示すＣＥＲＴＲＥＱペイロードを有するＩＫＥｖ２メッセージを示している。
【００３７】
本発明に従う方法および装置を適用できるアクセス状況が、図１に概念的に示されている。ユーザ機器（ＵＥ）１０５は、そのホームネットワーク１１０または訪問先ネットワーク１１５にアクセスしている。このアクセスは、ホームネットワークのセキュリティゲートウェイ（ＳＥＧＷ）であるＳＥＧＷｈ１２０経由、または訪問先ネットワークのセキュリティゲートウェイであるＳＥＧＷｖ１２５経由であり、それぞれ非ローミング状況Ａおよびローミング状況Ｂに対応する。ホームネットワーク１１０のＡＡＡサーバＡＡＡｈ１３０は認証のために利用され、訪問先ネットワーク１１５にアクセスする場合は、ＡＡＡｈ１３０に加えて、訪問先ネットワークの訪問先ＡＡＡプロキシＡＡＡｖ１３５も関与する。この認証は、以下でさらに説明するプロセスの中で、例えば、ＩＫＥｖ２シグナリング、ＡＡＡシグナリングおよびＥＡＰシグナリングを使用して実行される。アクセス手順は、正しく認証されると、ＵＥと、ＳＥＧＷであるＳＥＧＷｈ１２０またはＳＥＧＷｖ１２５との間のセキュアトンネル１６５であるＩＰｓｅｃトンネルをもたらし、そのトンネルはトラヒックを搬送することになる。
【００３８】
いくつかの様々なアクセス手順が使用され、図２ａ～ｄのシグナリング図に概念的に示されている。
【００３９】
図２ａは、完全なＥＡＰ－ＳＩＭ認証手順が使用される場合に、アクセスメカニズムで使用されるＩＰｓｅｃトンネルの確立を示すシグナリング図である。「ＡＡＡ」は、ＡＡＡプロトコル、典型的には、ＲＡＤＩＵＳまたはＤｉａｍｅｔｅｒを示している。
【００４０】
ＩＰｓｅｃトンネル確立のためのＩＫＥｖ２手順は、２つのフェーズから構成される。第１のフェーズは、以降のＩＫＥｖ２シグナリングを保護するために使用されるＩＫＥセキュリティアソシエーション（ＳＡ群）を確立する。第２のフェーズは、実際のＩＰｓｅｃトンネルのためのＳＡ群を確立する。ＥＡＰに基づく認証が使用される場合、第１のフェーズはＥＡＰに基づく認証手順を搬送するメッセージで拡張される。
【００４１】
図２ａのメッセージａおよびｂは、フェーズ１の交換を開始する。この第１のメッセージ（ＩＫＥ＿ＳＡ＿ＩＮＩＴ）のペアは、ＩＫＥ ＳＡ用の暗号鍵を確立するために、暗号アルゴリズムをネゴシエートし、ナンス（nonce）を交換し、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ（デフィーヘルマン）交換を行う。第２のメッセージｃおよびｄのペアは、前のメッセージに加えて２つのピア（peer：同位）を認証するために通常使用され、また、このメッセージ交換で第１のフェーズは通常完了する。しかしながら、ＥＡＰに基づく認証が使用される場合、この手順は異なる。メッセージｃからＡＵＴＨペイロードを除くことによって、ＵＥは、ＥＡＰに基づく認証を使用したいことを示す。ＵＥは、どのＣＡをサポートしているかを示すために、このメッセージにオプションでＣＥＲＴＲＥＱペイロードも含めることができる。メッセージｄでは、ＳＥＧＷがその証明書（これは証明書チェーン全体であってもよい）をＵＥに転送する。メッセージｅ～ｊは、ＥＡＰに基づく認証手

順を搬送するためのフェーズ１の拡張であり、この場合は、完全なＥＡＰ－ＳＩＭ認証手順のためのＥＡＰメッセージから構成される。ＳＥＧＷは、ＵＥ自体を認証しないが、ＥＡＰメッセージをＡＡＡメッセージにカプセル化することによって、ＳＥＧＷ－ＡＡＡｈパスでＥＡＰメッセージをＵＥのホームＡＡＡサーバであるＡＡＡｈへ中継しおよびＡＡＡｈから中継する。ＡＡＡｈは、ＵＥの実際の認証を実行し、かつメッセージｊでＳＥＧＷに結果（この例では、成功）を通知する。ＥＡＰ－ＳＩＭ認証手順後、ＵＥとＳＥＧＷは、前のメッセージ群の全部を認証するために、フェーズ１のもう２つのＩＫＥｖ２メッセージであるメッセージｋおよびｌを交換する。

【００４２】

フェーズ２は、ＣＲＥＡＴＥ＿ＣＨＩＬＤ＿ＳＡ交換とも呼ばれる。このフェーズは、１つのメッセージのペアであるメッセージｍおよびｎから構成され、それらのメッセージで、ＵＥとＳＥＧＷは、ＩＫＥ　ＳＡ群によって保護され、ＩＰｓｅｃトンネル用のＳＡを確立するために必要な情報を交換する。

【００４３】

図１では、ＵＥ１０５と、ＳＥＧＷｈ１２０またはＳＥＧＷｖ１２５との間のＩＫＥｖ２シグナリング１５０が、縞の太矢印で示されていて、ＳＥＧＷｈ１２０とＡＡＡｈ１３０との間、またはＳＥＧＷｖ１２５とＡＡＡｖ１３５との間のＡＡＡシグナリング１５１は、それぞれ格子縞の太矢印で示されていて、また、ＵＥ１０５とＡＡＡｈ１３０との間のエンドツーエンドＥＡＰシグナリング１６０は実線で示されている。ローミングの場合は、ＡＡＡシグナリング１５１、つまり、カプセル化されているＥＡＰシグナリング１６０は、訪問先ネットワーク１１５のＡＡＡｖ１３５経由で進む。細い実線は、ＩＰｓｅｃトンネル１６５が確立されている後のトラヒックフロー１６７のパスを示している。

【００４４】

図２ａの完全なＥＡＰ－ＳＩＭ認証手順は、メッセージｄのアイデンティティリクエストから始まる。ＵＥが、メッセージｅでユーザアイデンティティを与える。メッセージｆおよびｇは、ＥＡＰ－リクエスト／ＳＩＭ／開始メッセージおよびＥＡＰ－応答／ＳＩＭ／開始メッセージである。これらの２つのメッセージは、使用すべきＥＡＰ－ＳＩＭのバージョンをネゴシエートして、とりわけ以降のメッセージ群の保護のために鍵材料（keying material）を導出する場合に使用される、ＵＥからのナンスを含むデータを使用して、交換する。従って、以降のＥＡＰ－ＳＩＭメッセージは、メッセージ認証コードであるＡＴ＿ＭＡＣ属性によって保護されてもよい。メッセージｈでは、ＡＡＡｈがＵＥにチャレンジを送信する。ＵＥは、ＳＩＭに基づくＧＳＭ認証アルゴリズムを使用してチャレンジに対する応答を計算し、この応答をメッセージｉで返信する。ＡＡＡｈは、応答を検証し、検証が成功であることが与えられると、メッセージｊで認証の成功を確認する。

【００４５】

図２ｂは、ＥＡＰ－ＳＩＭ高速再認証手順が使用される場合に、アクセスメカニズムで使用されるＩＰｓｅｃトンネルの確立を示すシグナリング図である。このシグナリング図は、図２ａのシグナリング図とは、ＥＡＰ－ＳＩＭ認証手順を搬送するメッセージだけが異なる。ユーザアイデンティティの代わりに、ＵＥは、前の完全な認証手順中にＡＡＡｈと合意されている高速再認証アイデンティティを送信する。ＥＡＰ－リクエスト／ＳＩＭ／開始メッセージおよびＥＡＰ－応答／ＳＩＭ／開始メッセージは、高速再認証手順では必要とされない。代わりに、ＥＡＰ－リクエスト／ＳＩＭ／再認証メッセージおよびＥＡＰ－リクエスト／ＳＩＭ／再認証メッセージでは、チャレンジ－応答交換だけがあり、ＡＡＡｈからのＥＡＰ－成功メッセージでの認証成功の確認が続くことになる。

【００４６】

図２ｃは、完全なＥＡＰ－ＡＫＡ認証手順が使用される場合に、アクセスメカニズムで使用されるＩＰｓｅｃトンネルの確立を示すシグナリング図である。このシグナリング図では、図２ａの完全なＥＡＰ－ＳＩＭ認証手順が、完全なＥＡＰ－ＡＫＡ認証手順で置換されている。完全なＥＡＰ－ＳＩＭ認証手順と同様に、完全なＥＡＰ－ＡＫＡ認証手順はアイデンティティリクエストで始まり、これが、ＡＡＡｈへユーザアイデンティティを送

信するようにＵＥをトリガする。次いで、ＡＡＡｈは、ＥＡＰ－リクエスト／ＡＫＡ－チャレンジメッセージで、ＵＥにチャレンジおよびネットワーク認証トークン（ＵＥにおけるネットワークの認証のための）を送信することによって、実際のＡＫＡ認証手順を開始する。ＵＥは、ネットワーク認証トークンを検証し、ＡＫＡアルゴリズムを使用してチャレンジに対する応答を計算し、この応答をＥＡＰ－応答／ＡＫＡ－チャレンジメッセージでＡＡＡｈに返信する。ＡＡＡｈは、応答を検証し、検証が成功ならば、認証が成功であることが与えられると、その認証の成功を確認する。

【００４７】

図２ｄは、ＥＡＰ－ＡＫＡ高速再認証手順が使用される場合に、アクセスメカニズムで使用されるＩＰｓｅｃトンネルの確立を示すシグナリング図である。このシグナリング図は、図２ｃのシグナリング図とは、ＥＡＰ－ＡＫＡ認証手順を搬送するメッセージだけが異なる。ユーザアイデンティティの代わりに、ＵＥは、前の完全な認証手順中にＡＡＡｈと合意されている高速再認証アイデンティティを送信する。これに、ＥＡＰ－リクエスト／ＡＫＡ－再認証メッセージおよびＥＡＰ－応答／ＡＫＡ－再認証メッセージでのチャレンジ－応答交換が続き、これに、今度は、ＡＡＡｈからの認証成功の確認が続く。

【００４８】

上記の認証の方法はすべて、ＵＥと、ＵＥがアクセスするＳＥＧＷとの間でのルート証明書の一致に依存する。背景技術で説明されるように、これは常に当てはまるわけではない。一致するルート証明書を提供する問題は、ローミング状況で最もはっきりと表れるが、前述の通り、ホームネットワークのアクセス手順でも生じることがある。

【００４９】

図３に示される本発明の方法および装置に従えば、証明書サーバ（ＣＳ）が認証手順のフェーズ１で導入され利用される。証明書サーバ１４０は、訪問先ネットワークに属してもよいし、またＵＥのホームネットワークに属してもよい。認証手順は、ＵＥ１０５が、ＳＥＧＷ１２０／１２５経由でホームネットワークまたは訪問先ネットワークへアクセスする時に開始され、以下の主なステップを備える。

【００５０】

３１０：ＵＥ１０５とＳＥＧＷ１２０／１２５が、利用可能な証明書（群）についての情報を交換する。

【００５１】

３１５：ＵＥ１０５とＳＥＧＷ１２５との間の証明書の不一致の識別は、試行された認証手順の進行を妨げる。

【００５２】

３２０：証明書サーバ１４０が参加する。証明書サーバ１４０の選択は、ＵＥ１０５によって提供されるユーザアイデンティティに基づいてもよい。

【００５３】

３２５：証明書サーバ１４０は、ルート証明書を、ＳＥＧＷ１２０／１２５に提供する（実線で示されている）、もしくはＵＥ１０５に提供する（破線で示されている）ことによって、またはＵＥ１０５に代わってＳＥＧＷ自体の認証もしくはＳＥＧＷの認証の一部を実行して、その結果をＳＥＧＷ１２０／１２５またはＵＥ１０５に通知することによって、認証手順の少なくとも一部に関与する。

【００５４】

３３０：ＵＥ１０５とＳＥＧＷ１２０／１２５との間にセキュアトンネルが確立されると、ペイロードトラヒックを転送することができる。

【００５５】

用語「証明書サーバ」は、認証目的で使用し得る、中心となる場所の総称であることが意図されている。証明書サーバは、例えば、ＡＡＡサーバでもよいし、また専用サーバでもよい。

【００５６】

上述のＩＫＥｖ２シグナリングは、ＵＥ１０５とＳＥＧＷ１２０、１２５との間で使用

されることが好ましいので、ＡＡＡシグナリングは、ＳＥＧＷと証明書サーバ１４０との間で使用されることが好ましい。

【００５７】

本発明の一実施形態に従えば、ＳＥＧＷ１２０／１２５は、証明書サーバからＵＥのルート証明書（群）（の１つ）に一致する証明書が提供される。この実施形態は、図４ａに概念的に示され、対応するシグナリングは、図４ｂのシグナリング図に示されている。ＵＥ１０５が、ＳＥＧＷ１２０／１２５経由でホームネットワークまたは訪問先ネットワーク１１０／１１５（図１）にアクセスして、かつ認証手順が開始される。好ましくは、このアクセスは、上述のＩＫＥｖ２手順の変更形態である。この実施形態では、証明書サーバは、ＳＥＧＷのネットワークに配置される。このネットワークがＵＥのホームネットワークでもある場合（非ローミングの場合）、証明書サーバは、図４ａに示されているＡＡＡｈ１３０に統合されてもよい。ＳＥＧＷのネットワークが訪問先ネットワークの場合（ローミングの場合）、証明書サーバはＡＡＡｖ１３５に統合されてもよい。図４ｂのシグナリング図では、代替実施を示す個別のエンティティとして示されている。この実施形態は、

４１０：ＵＥ１０５が、その利用可能なルート証明書（群）の指示をＳＥＧＷ１２０／１２５に提供する。この指示は、ＵＥ１０５によってサポートされるＣＡを指示する形式である。ＣＡの指示は、ＩＫＶＥｖ２交換の第３のメッセージであるメッセージｃのＣＥＲＴＲＥＱパラメータの中に含まれてもよい。

【００５８】

４１５：ＳＥＧＷ１２０／１２５が、ＵＥ１０５からのＣＡを、記憶されている証明書と比較する。

【００５９】

４２０：ＳＥＧＷ１２０／１２５は、ＣＡに一致する証明書を検出することができない場合、メッセージｃ’で証明書サーバＡＡＡｈ１３０に（実線矢印で）またはＡＡＡｖ１３５に（破線矢印で）、一致する証明書をリクエストする。証明書サーバは、好ましくは、サービスを提供する可能性があるＵＥが頼るかもしれないＣＡの大多数に対応する多数の証明書をオペレータによって事前に提供され、それらの証明書およびそれに関係する鍵ペアを記憶している。

【００６０】

４２２：証明書サーバＡＡＡｈ１３０またはＡＡＡｖ１３５は、関係する鍵ペアを使用してそれに一致する証明書を生成し、その証明書に、関係するＣＡからの自身の秘密鍵で署名する。選択的には、証明書および鍵ペアは、リアルタイム性能を向上するために前もって生成されてもよい。

【００６１】

４２５：証明書サーバＡＡＡｈ１３０またはＡＡＡｖ１３５は、実線矢印および破線矢印でそれぞれ示されているように、メッセージｃ”で証明書およびそれに関係する鍵ペアをＳＥＧＷ１２０／１２５に送信する。

【００６２】

４２７：ＳＥＧＷ１２０／１２５は、メッセージｄで、一致する証明書をＵＥ１０５に送信する。

【００６３】

４２８：ＵＥ１０５は、受信した証明書を有効にする。

【００６４】

４３０：ＵＥ１０５とＳＥＧＷ１２０／１２５との間にセキュアトンネルが確立され、ペイロードトラヒックを転送することができる。

【００６５】

ローミングの場合、ＡＡＡ／ＥＡＰシグナリングは、ＡＡＡｈ１３０で終了し、一方、証明書のリクエスト／返信のためのシグナリングは、証明書サーバ、例えば、ＡＡＡｖ１３５で終了することに注目すべきである。ＳＥＧＷ１２０／１２５とＡＡＡｈまたはＡＡ

ＡｖとＡＡＡｈとの間の証明書のリクエスト／返信の通信は、複数の周知のプロトコルに準拠してもよい。

【００６６】

以下の実施形態で例示される代替アプローチは、ＵＥ１０５にＳＥＧＷの証明書の有効性を検証するための手段を提供することである。このアプローチは、ＡＡＡｈ１３０がＳＥＧＷの証明書を（ＵＥ１０５に代わって）有効にする（有効化する）、またはＵＥ１０５に有効にするために必要とされるルート証明書を提供するように、ＵＥと証明書サーバ１４０、例えば、そして、好ましくは、ＡＡＡｈ１３０との間の信頼／セキュリティ関係を活用する。有効化の結果は、（ＥＡＰによる）簡単な成功の表示として、またはＡＡＡｈのデジタル署名をＳＥＧＷの証明書と関係付けることによって、ＵＥ１０５に通知されることができる。ＡＡＡｈ１３０は、ルート証明書を使用する通常の方法で、または訪問先ネットワークのＡＡＡプロキシであるＡＡＡｖ１３５を介する推移信頼をできる限り使用して、ＡＡＡｈ１３０とＳＥＧＷ１２０／１２５との間の既存の信頼／セキュリティ関係を活用することによって、ＳＥＧＷの証明書を有効にしてもよい。

【００６７】

図５ａに概念的に示されていて、対応するシグナリングが図５ｂ～ｅのシグナリング図に示されている本発明の一実施形態では、ホームＡＡＡサーバであるＡＡＡｈ１３０が、ＳＥＧＷの証明書を有効にする際に、ＵＥ１０５を支援する。ＵＥ１０５が、ＳＥＧＷ１２０／１２５経由でホームネットワークまたは訪問先ネットワークにアクセスして、認証手順が開始される。好ましくは、この認証手順は、上記のＥＡＰ手順の変更形態である。シグナリング図５ｂはＥＡＰ－ＳＩＭ完全認証手順を示し、図５ｃはＥＡＰ－ＳＩＭ高速再認証手順を示し、図５ｄはＥＡＰ－ＡＫＡ完全認証手順を示し、図５ｅはＥＡＰ－ＡＫＡ高速再認証手順を示している。この実施形態は、以下のステップを備える。

【００６８】

５１０：ＳＥＧＷ１２０／１２５が、メッセージｄで少なくとも１つの証明書をＵＥ１０５に送信する。

【００６９】

５１５：ＵＥ１０５が、ＳＥＧＷ１２０／１２５から受信した証明書を、記憶されているルート証明書と比較する。

【００７０】

５２０：ＵＥ１０５は、ＵＥ内に記憶されているルート証明書（群）を使用してＳＥＧＷの証明書を有効にできない場合、ＳＥＧＷの証明書をＡＡＡｈ１３０（証明書サーバ）に、好ましくは、ＥＡＰ（すなわち、ＥＡＰ－ＳＩＭまたはＥＡＰ－ＡＫＡ）認証手順中に送信する。ＳＥＧＷの証明書は、ＥＡＰ－ＳＩＭおよびＥＡＰ－ＡＫＡへの属性拡張のために使用されるＴＬＶ（タイプ－レングス－値、Type-Length-Value）フォーマットの後に続く、新規のＥＡＰ－ＳＩＭ属性またはＥＡＰ－ＡＫＡ属性である「ＳＥＧＷ証明書」に含まれることが好ましい。ＵＥは、メッセージｇ’で、ＥＡＰ－ＳＩＭおよびＥＡＰ－ＡＫＡのＡＴ＿ＭＡＣ属性によって完全性を保護できる第１のＥＡＰメッセージの中にＳＥＧＷの証明書を有する属性を含める。

【００７１】

５２２：ＡＡＡｈ１３０が、ＳＥＧＷの証明書を有効にする。ＡＡＡｈ１３０は、少なくとも２つの異なる方法を使用することができる。それらは、ａ）ＡＡＡｈが関係するＣＡのルート証明書にアクセスしていることが与えられると、ルート証明書を使用し、通常の方法で証明書を有効にする、ｂ）ＡＡＡｈ１３０とＳＥＧＷ１２０／１２５との間の既存の信頼／セキュリティ関係に頼る。ＡＡＡｈとＳＥＧＷが同一のネットワークに属する場合、ＡＡＡｈはＳＥＧＷが有効な証明書を供給することを当然に信頼し、その証明書の完全性はＳＥＧＷとＡＡＡｈとの間のＡＡＡシグナリングの必須の保護によって、およびＥＡＰシグナリングのＡＴ＿ＭＡＣ属性によって保証され、かつそれに従って、ＳＥＧＷの証明書は有効であることをＵＥ１０５に保証することができる。ＡＡＡｈ１３０とＳＥＧＷ１２０／１２５が異なるネットワークに属する場合、すなわち、異なるオペレータま

たは管理ドメインに属する場合、ＡＡＡｈ１３０とＳＥＧＷ１２０／１２５、または、選択的には、訪問先ネットワークの介在するＡＡＡプロキシとは、ローミングアグリーメント（協定）およびセキュア（安全な）ＡＡＡ通信を保証するセキュリティアソシエーションに基づく、信頼関係を有する。それゆえ、ＡＡＡｈは、ＳＥＧＷの証明書はローミングの状況でもやはり有効であることを、ＵＥに保証することができる。

【００７２】

５２５：ＡＡＡｈ１３０は、メッセージｈ’で「ＯＫ」表示（または有効化が失敗である場合は「ｎｏｔ　ＯＫ」表示）をＵＥ１０５に送信する。この表示も、好ましくは、新規のＥＡＰ－ＳＩＭ属性またはＥＡＰ－ＡＫＡ属性に含まれ、また、ＡＴ＿ＭＡＣ属性で保護されなければならない。ＡＡＡｈがＳＥＧＷの証明書を受信したメッセージが、認証手順の中の最後の（固有の）ＥＡＰ－ＳＩＭメッセージまたはＥＡＰ－ＡＫＡメッセージであった場合、（方法包括的な）ＥＡＰ－成功メッセージが認証手順の残っている唯一のＥＡＰメッセージである。ＥＡＰ－成功メッセージは、「ＯＫ」（または「ｎｏｔ　ＯＫ」）表示のための新規の属性のような、方法固有の属性を搬送することができないので、ＡＡＡｈは、その表示をＵＥに転送するために、追加のＥＡＰ－リクエスト／ＳＩＭ／通知メッセージ（ＥＡＰ－ＳＩＭの場合）またはＥＡＰ－リクエスト／ＡＫＡ－通知メッセージ（ＥＡＰ－ＡＫＡの場合）を使用する。この場合、ＵＥは、ＥＡＰ－応答／ＳＩＭ／通知メッセージまたはＥＡＰ－応答／ＡＫＡ－通知メッセージで応答し、次いでＡＡＡｈが、ＥＡＰ－成功メッセージを送信して、ＥＡＰ認証手順を終了する。表示を転送するために、ＥＡＰ－リクエスト／ＳＩＭ／通知メッセージまたはＥＡＰ－リクエスト／ＡＫＡ－通知メッセージが使用される場合、新規の通知コード（すなわち、既存のメッセージフィールドの新規の値）も新規の属性の代わりに使用されてもよい。

【００７３】

５３０：ＵＥ１０５とＳＥＧＷ１２０／１２５との間にセキュアトンネルが確立され、ペイロードトラヒックを転送することができる。

【００７４】

証明書の有効化が信頼／セキュリティ関係に基づいている場合、ＡＡＡｈ１３０は、どのようなルート証明書を有する必要がない。ＵＥ１０５のＳＩＭカード（またはＵＩＣＣ）とＡＡＡｈ１３０（または、より正確には、ＡＡＡｈに認証パラメータを供給する認証センタ（Authentication Center）であるＡｕＣ）との間にセキュリティ関係が常に存在するが、そのセキュリティ関係が唯一の必須の前提条件である。

【００７５】

ＧＡＮの場合、ＵＥ１０５は、証明書をＡＡＡｈに送信する前に、ＳＥＧＷの証明書のＳｕｂｊｅｃｔＡｌｔＮａｍｅデータがＧＡＮ標準仕様書［１３］に記載されている要件に準拠しているかをチェックし、その要件に満足している場合のみ、その証明書を送信することを選択してもよい。この要件は、ＳＥＧＷによって提供される証明書の中のＳｕｂｊｅｃｔＡｌｔＮａｍｅデータがＳＥＧＷから受信されるＩＤｒペイロードに一致するだけでなく、ＵＥが、プロビジョニング（例えば、コンフィグレーション（構成））、ディスカバリ（発見）（ＧＡ－ＲＣ　ＤＩＳＣＯＶＥＲＹ　ＡＣＣＥＰＴ（ＧＡ－ＲＣディスカバリ受諾）メッセージの中）または登録リダイレクト（ＧＡ－ＲＣ　ＲＥＧＩＳＴＥＲ　ＲＥＤＩＲＥＣＴ（ＧＡ－ＲＣ登録リダイレクト）メッセージの中）で、以前取得しているＳＥＧＷアイデンティティに一致する項目も含むということである。このＳＥＧＷアイデンティティは、ＩＰｖ４アドレス、ＩＰｖ６アドレスまたはＦＱＤＮであってもよい。

【００７６】

代替実施形態として、ＳＥＧＷの証明書を有効にするようにＡＡＡｈ１３０にリクエストする代わりに、ＵＥ１０５は、必要とされるルート証明書を送信するようにＡＡＡｈ１３０にリクエストし、そうすることで、ＵＥ１０５自体がＳＥＧＷの証明書を有効にしてもよい。そのルート証明書に対するリクエストの中に、ＵＥ１０５は、ＳＥＧＷの証明書または必要とされるルート証明書の表示を含める。ＡＡＡｈ１３０が必要とされるルート

証明書にアクセスできるならば、ＡＡＡｈ１３０は、ルート証明書をＵＥ１０５に返信する。このＵＥ１０５は、ＳＥＧＷの証明書を有効にするために、取得しているルート証明書を使用し、また、後での使用のために追加でまたはオプションでルート証明書を記憶してもよい。

【００７７】

図６ａに概念的に示され、対応するシグナリングが図６ｂのシグナリング図に示されている本発明のさらなる実施形態では、ＳＥＧＷ１２０／１２５とＡＡＡｈ１３０との間の対話が変更されている。証明書の有効性をＵＥ１０５に保証するために、ＳＥＧＷの証明書に署名するＡＡＡｈの能力が利用されている。ＵＥ１０５がＳＥＧＷ１２０／１２５経由でホームネットワーク１１０または訪問先ネットワーク１１５（図１）にアクセスし、そして、認証手順が開始される。好ましくは、このアクセスは、上述のＩＫＥｖ２およびＡＡＡ手順の変更形態である。この実施形態は、以下のステップを備える。

【００７８】

６１０：ＵＥ１０５が、その利用可能な証明書（群）の表示をＳＥＧＷ１２０／１２５に提供する。その表示は、ＵＥ１０５によってサポートされるＣＡを表示する形式である。

【００７９】

６１５：ＳＥＧＷ１２０／１２５が、ＵＥ１０５からのＣＡ群を、記憶されている証明書と比較する。

【００８０】

６２０：ＳＥＧＷ１２０／１２５は、ＵＥ１０５によって提供されているＣＡ群に一致する証明書を検出することができなかった場合、その証明書（群）（の１つ）をＡＡＡｈ１３０に送信し、ＡＡＡｈ１３０にそれに署名するようにリクエストする。

【００８１】

６２２：ＡＡＡｈ１３０は、ルート証明書を使用する通常の証明書の有効化後、またはＡＡＡｈ１３０とＳＥＧＷ１２０／１２５（またはＡＡＡプロキシ１３５）との間の既存の信頼／セキュリティ関係およびセキュア通信を利用して、ＳＥＧＷ１２０／１２５によって提供される証明書に署名する。

【００８２】

６２５：ＡＡＡｈ１３０は、署名されている証明書をＳＥＧＷ１２０／１２５に返信する。

【００８３】

６２７：ＳＥＧＷ１２０／１２５は、続いて、その証明書をＵＥ１０５に送信し、かつＡＡＡｈの署名を含める。

【００８４】

６２８：ＵＥ１０５は、ＡＡＡｈの署名を有効にし、そして、ＳＥＧＷの証明書の有効化としてそのことを受け付ける。

【００８５】

６３０：ＵＥ１０５とＳＥＧＷ１２０／１２５との間にセキュアトンネルが確立されることで、ペイロードトラヒックを転送することができる。

【００８６】

ステップ６２２で、ＡＡＡｈ１３０がその秘密鍵を用いてＳＥＧＷの証明書に署名することは可能であろうが、ＵＥ１０５とＡＡＡｈ１３０が以前から共有している鍵、例えば、ごく最近生成されたマスタセッション鍵ＭＳＫまたは拡張マスタセッション鍵ＥＭＳＫ（これらの鍵は、ＥＡＰ－ＳＩＭ認証手順およびＥＡＰ－ＡＫＡ認証手順で使用される）、またはこれらの鍵から導出される鍵で、証明書に署名することが好ましい。ＡＡＡｈ１３０は、ＵＥ１０５が最新のＭＳＫ／ＥＭＳＫを記憶しているかどうかが不確かである場合、その秘密鍵で生成される署名と、最新のＭＳＫ／ＥＭＳＫもしくはそれらから導出される鍵で生成される署名の２つの署名を送信してもよい。

【００８７】

ＳＥＧＷ－ＡＡＡｈの通信は、図６ｂに示されるように、新規のメッセージタイプおよび／または新規の属性を使用するＡＡＡプロトコル（すなわち、ＲＡＤＩＵＳまたはＤｉａｍｅｔｅｒ）を利用することが好ましい。ＳＥＧＷ（および、もしあればＡＡＡプロキシ）は、ＳＥＧＷがＣＥＲＴＲＥＱペイロードのメッセージｃの「ＩＫＥｖ２（ＣＥＲＴＲＱ…）」と同一のＩＫＥｖ２メッセージの中でＵＥから受信されているユーザＩＤに含まれる情報を使用して、ＡＡＡルーティングによってメッセージｃ’の「ＡＡＡ（ＳＥＧＷ証明書，…）」でＡＡＡｈに到達する。この情報は、最終的には、ホームオペレータのドメインを指すアドレス体系、例えば、「ｔｈｅ－ｗｏｒｌｄｓ－ｂｅｓｔ－ｏｐｅｒａｔｏｒ．ｃｏｍ」等の形態を取らなければならない。ＵＥから受信される情報は、ＮＡＩの形式、例えば、＜ｕｓｅｒ－ｎａｍｅ＞@ｔｈｅ－ｗｏｒｌｄｓ－ｂｅｓｔ－ｏｐｅｒａｔｏｒ．ｃｏｍ、あるいはユーザの国際移動体加入者識別番号（ＩＭＳＩ：International Mobile Subscriber Identity）を含む他の形式、またはＩＭＳＩに通常含まれている移動国コード（ＭＣＣ：Mobile Country Code）および移動ネットワークコード（ＭＮＣ：Mobile Network Code）を少なくとも含む他の形式でもよい。ＭＣＣおよびＭＮＣを使用して、ＵＥまたはＳＥＧＷは、ＭＣＣおよびＭＮＣを含むデフォルトのアドレス体系、例えば、ＷＬＡＮと３ＧＰＰネットワークとの間のインターワーキング（Ｉ－ＷＬＡＮ）とともに使用されるアドレス体系フォーマット、すなわち、「ｗｌａｎ．ｍｎｃ＜ＭＮＣ＞．ｍｃｃ＜ＭＣＣ＞．３ｇｐｐｎｅｔｗｏｒｋ．ｏｒｇ」と類似（または同一）のデフォルトのアドレス体系を作成することができる。ＡＡＡｈ１３０は、同様の手段によって、メッセージｃ”の「ＡＡＡ（署名付きＳＥＧＷ証明書，…）」で、署名付きの証明書を返信する。ＳＥＧＷ１２０／１２５は、変更済みのＩＫＥｖ２メッセージであるメッセージｄ’のＩＫＥｖ２（ＣＥＲＴ＝署名付き証明書，…）｛ＥＡＰ－リクエスト／アイデンティティ｝で署名付き証明書（および署名）を転送する。

【００８８】

図７のシグナリング図に示されている代替実施形態では、ＳＥＧＷ１２０／１２５は、ステップ６２０と同様に、（必要な場合）署名してもらうために自身の証明書をＡＡＡｈ１３０に送信する。ＡＡＡｈ１３０は、ステップ６２２と同様に証明書に署名する。専用の新規のメッセージで、ＳＥＧＷ１２０／１２５に署名付きのメッセージを返信する代わりに、ＡＡＡｈ１３０は、ＥＡＰ－ＳＩＭメッセージまたはＥＡＰ－ＡＫＡメッセージの１つ、例えば、変更済のメッセージｈ’の「ＡＡＡ｛ＥＡＰ－リクエスト／ＳＩＭ／チャレンジ（署名付き証明書，…）｝」および「ＩＫＥｖ２｛ＥＡＰ－リクエスト／ＳＩＭ／チャレンジ（署名付き証明書，…）｝」のそれぞれで、その証明書をＵＥに送信する。同様の変更は、上述のＥＡＰ－ＳＩＭ／ＥＡＰ－ＡＫＡ手順の他のところで実行することができる。

【００８９】

本発明は、これまで一般用語で説明されているが、３ＧＰＰのＧＡＮシステムに暗黙的に焦点を当てている。それゆえ、本発明は、例えば、３ＧＰＰのＩ－ＷＬＡＮシステム等の複数の他の通信システムにも適用できることに注意すべきである。

【００９０】

Ｉ－ＷＬＡＮのＵＥが、ＰＬＭＮのＰＤＧまたはＴＴＧへのＩＰｓｅｃトンネルを確立する。通常は、このＰＤＧ／ＴＴＧは、ホームＰＬＭＮに配置されているが、オプションで訪問先ＰＬＭＮに配置されてもよい。ホームＰＬＭＮに配置される場合は、本発明が解決する問題は、ＵＥにおけるＰＤＧ／ＴＴＧの証明書とルート証明書との間の不一致が、Ｉ－ＷＬＡＮシステムにおいてもＧＡＮの場合と同一である場合に限り存在する。訪問先ＰＬＭＮに配置される場合、訪問先ＰＬＭＮ（すなわち、ホームＰＬＭＮのオペレータのローミング相手のＰＬＭＮ）のＰＤＧ／ＴＴＧへＩＰｓｅｃトンネルが確立される場合、問題はどの場合にも当てはまる。

【００９１】

解決策は、Ｉ－ＷＬＡＮシステムにおいては、上述のように、ＰＤＧまたはＴＴＧであるＳＥＧＷを伴う場合と同じである。

【００９２】
３ＧＰＰのＳＡＥアーキテクチャは注目すべき分野であり、この状況では、本発明は効果的に実施される。予想されるＳＡＥアーキテクチャでは、非３ＧＰＰアクセスネットワーク（または、おそらくはＩ－ＷＬＡＮ）経由でネットワークにアクセスしているＵＥが、ＭＩＰｖ６シグナリングの保護用に、およびおそらくＵＥ－ＨＡトンネルの保護用にＩＰｓｅｃ　ＳＡ群を確立するために、ＭＩＰｖ６のＨＡ向けの統合認証メカニズムとしてＥＡＰ－ＡＫＡを有するＩＫＥｖ２を使用する。典型的には、ＨＡは、ホームＰＬＭＮに配置されており、この場合、本発明が解決する問題は、ＵＥにおけるＨＡ証明書とルート証明書との間の不一致が、ＧＡＮの場合と同一である場合に限り存在する。しかしながら、ＵＥは潜在的には訪問先ＰＬＭＮのＨＡまたはＩＡＳＡ（Ｉｎｔｅｒ　Ａｃｃｅｓｓ　Ｓｙｓｔｅｍ　Ａｎｃｈｏｒ）にも割り当てられてもよく、この場合、問題はやはり当てはまる。

【００９３】
図８ａ～ｃに、本発明の実施形態に従う、証明書サーバ１４０、ユーザ機器１０５およびセキュリティゲートウェイ１２０／１２５が概念的に示されている。証明書サーバ１４０、ユーザ機器１０５およびセキュリティゲートウェイ１２０／１２５には、上述の方法のそれぞれの部分を実行するための手段がそれぞれ提供されている。本発明に従うモジュールおよびブロックは、ノードの機能部分と見なされるものであり、必ずしもそれ自体で物理的対象物と見なされるものではない。モジュールおよびブロックは、本発明に従う方法を達成するように構成されているソフトウェアコード手段として少なくとも一部は実施されることが好ましい。用語「備える（ｃｏｍｐｒｉｓｉｎｇ）」は、主に論理構造を指し、用語「接続されている（ｃｏｎｎｅｃｔｅｄ）」は、本明細書では機能部分間のリンクと解釈すべきであり、必ずしも物理的な接続であると解釈されるべきではない。しかしながら、選択された実装次第で、あるモジュールは、受信デバイスまたは送信デバイスの中の物理的な特徴を示す対象物として実現されてもよい。

【００９４】
認証サーバ１４０は、通信ネットワーク内の他のエンティティとの通信用に構成されている通信モジュール８０５を備える。通信モジュール８０５は、典型的には、また、好ましくは、複数の異なるプロトコルを扱うように構成されている。証明書サーバ１４０は、通信モジュール８０５によってＳＥＧＷと通信するように構成されている。本発明に従えば、証明書サーバ１４０は、ＳＥＧＷにアクセスしているＵＥに向けてのＳＥＧＷが認証されるる認証手順の少なくとも一部を実行または支援するように構成されている認証モジュール８１０を備え、この認証手順には、ＳＥＧＷおよびＳＥＧＷにアクセスしているＵＥを含んでいる。この認証サーバは、ＡＡＡサーバまたはＡＡＡプロキシに統合されてもよい。

【００９５】
一実施形態に従えば、認証モジュール８１０は、証明書記憶モジュール８１５を備える、またはそれに接続しており、証明書サーバ１４０は、ＳＥＧＷまたはＵＥに、証明書記憶モジュール８１５から取得されるルート証明書を提供するように構成されている。

【００９６】
別の実施形態に従えば、認証モジュール８１０は、ＳＥＧＷの認証の少なくとも一部を実行し、その結果の表示を生成するように構成されている。その結果の表示は、通信モジュール８０５によってＳＥＧＷまたはＵＥに転送される。

【００９７】
ユーザ機器（ＵＥ）１０５は、通信ネットワーク内の他のエンティティと通信するように構成されている無線通信モジュール８２０を備える。この無線通信モジュール８２０は、複数の無線通信技術を扱うように構成されているのが一般的であり好ましい。ＵＥ１０５は、通信モジュール８２０によって、複数の一般通信ノード（不図示）経由でＳＥＧＷと通信するように構成されている。本発明の一実施形態に従えば、ＵＥ１０５は、証明書記憶モジュール８３０に接続している証明書処理モジュール８２５を備える。証明書処理

モジュール８２５は、ＳＥＧＷの認証の試行中に、一致する証明書が証明書記憶モジュール８３０に記憶されていないかどうかを確認し、一致する証明書が記憶されていない場合、証明書サーバＣＳに認証への参加をリクエストするように構成されている。証明書処理モジュール８２５は、ＣＳから証明書を受信し、この証明書をＳＥＧＷの認証で使用するようにさらに構成されている。選択的には、証明書処理モジュール８２５は、ＵＥ１０５と通信中の別のノードによってＳＥＧＷが有効にしているという表示を受信するように構成されている。

【００９８】

セキュリティゲートウェイ（ＳＥＧＷ）１２０／１２５は、通信ネットワーク内の他のエンティティと通信するように構成されている通信モジュール８３５を備える。通信モジュール８３５は、複数の異なるプロトコルを扱うように構成されていることが一般的であり好ましい。ＳＥＧＷ１２０／１２５は、通信モジュール８３５を介して証明書サーバと通信するように構成されている。本発明の実施形態に従えば、ＳＥＧＷ１２０／１２５は、証明書記憶モジュール８４５に接続している証明書処理モジュール８４０を備える。証明書処理モジュール８４０は、ＵＥとの認証手順において、提供されている証明書（群）の表示（群）を、前もって記憶されている証明書と比較し、一致する証明書がないと確認される場合、認証手順にさらなる通信ノードの証明書サーバを参加させるように構成されている。一実施形態では、証明書処理モジュール８４０は、参加した証明書サーバに、一致する証明書の提供をリクエストするようにさらに構成され、また、その一致する証明書を受信し、ＵＥとの認証手順でそれを使用するようにさらに構成されている。代替実施形態では、証明書処理モジュール８４０は、参加した証明書サーバに証明書を送信し、かつ証明書サーバに証明書への署名をリクエストするようにさらに構成され、かつ署名付き証明書を受信し、そして、それをＵＥとの認証手順で使用するようにさらに構成されている。

【００９９】

本発明に従う方法は、方法のステップを実行するソフトウェアコード手段を備えるプログラム製品またはプログラムモジュール製品によって、その少なくとも一部が実施されてもよい。このプログラム製品は、ネットワーク内の複数のエンティティで実行されることが好ましい。このプログラムは、例えば、ＵＳＢメモリ、ＣＤ等のコンピュータで使用可能な記憶媒体、または無線送信、またはインターネットからのダウンロード等で、配信またはロードされる。

【０１００】

本発明は、最も実用的で好ましいと現在考えられている実施形態に関連して説明しているが、本発明は、開示の実施形態に限定されるものではなく、添付の特許請求の範囲内の種々の変更形態および均等の装置を包含することを意図していることが理解されるべきである。

【０１０１】

＜引用文献一覧＞

［1］ Ｃ．Ｒｉｇｎｅｙ他著、「ＲＡＤＩＵＳ（Ｒｅｍｏｔｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｄｉａｌ Ｉｎ Ｕｓｅｒ Ｓｅｒｖｉｃｅ）（Ｒｅｍｏｔｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｄｉａｌ Ｉｎ Ｕｓｅｒ Ｓｅｒｖｉｃｅ（ＲＡＤＩＵＳ））」、ＲＦＣ ２８６５、２０００年６月

［2］ Ｃ．Ｒｉｇｎｅｙ他著、「ＲＡＤＩＵＳ拡張（ＲＡＤＩＵＳ Ｅｘｔｅｎｓｉｏｎｓ）」、ＲＦＣ ２８６９、２０００年６月

［3］ Ｐａｔ Ｃａｌｈｏｕｎ他著、「Ｄｉａｍｅｔｅｒに基づくプロトコル（Ｄｉａｍｅｔｅｒ Ｂａｓｅ Ｐｒｏｔｏｃｏｌ）」、ＲＦＣ ３５８８、２００３年９月

［4］ Ｐ．Ｅｒｏｎｅｎ他著、「Ｄｉａｍｅｔｅｒ拡張認証プロトコル（ＥＡＰ）アプリケーション（Ｄｉａｍｅｔｅｒ Ｅｘｔｅｎｓｉｂｌｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ （ＥＡＰ） Ａｐｐｌｉｃａｔｉｏｎ）」、インターネットドラフト ｄｒａｆｔ－ｉｅｔｆ－ａａａ－ ｅａｐ－１０．ｔｘｔ、２００４年１１月

［5］ Ｐａｔ Ｃａｌｈｏｕｎ他著、「Ｄｉａｍｅｔｅｒネットワーク・アクセス・サーバ・アプリケーション（Ｄｉａｍｅｔｅｒ Ｎｅｔｗｏｒｋ Ａｃｃｅｓｓ Ｓｅｒｖｅｒ Ａｐｐｌｉｃａｔｉｏｎ）」、インターネットドラフト ｄｒａｆｔ－ｉｅｔｆ－ａａａ－ｄｉａｍｅｔｅｒ－ｎａｓｒｅｑ－１７．ｔｘｔ、２００４年7月
［6］ Ｃ．Ｋａｕｆｍａｎ著、「インターネット鍵交換（ＩＫＥｖ２）プロトコル（Ｉｎｔｅｒｎｅｔ Ｋｅｙ Ｅｘｃｈａｎｇｅ （ＩＫＥｖ２） Ｐｒｏｔｏｃｏｌ）」、ＲＦＣ ４３０６、２００５年１２月
［7］ Ｓ．Ｋｅｎｔ、Ｒ．Ａｔｋｉｎｓｏｎ共著、「インターネットプロトコル用のセキュリティアーキテクチャ（Ｓｅｃｕｒｉｔｙ Ａｒｃｈｉｔｅｃｔｕｒｅ ｆｏｒ ｔｈｅ Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）」、ＲＦＣ ２４０１、１９９８年１１月
［8］ Ｓ．Ｋｅｎｔ、Ｋ．Ｓｅｏ共著、「インターネットプロトコル用のセキュリティアーキテクチャ（Ｓｅｃｕｒｉｔｙ Ａｒｃｈｉｔｅｃｔｕｒｅ ｆｏｒ ｔｈｅ Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）」、ＲＦＣ ４３０１、２００５年１２月
［9］ Ｂ．Ａｂｏｂａ他著、「拡張認証プロトコル（ＥＡＰ）（Ｅｘｔｅｎｓｉｂｌｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ （ＥＡＰ））」、ＲＦＣ ３７４８、２００４年6月
［１０］ Ｈ．Ｈａｖｅｒｉｎｅｎ、Ｊ．Ｓａｌｏｗｅｙ共著、「ＧＳＭ（Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ）ＳＩＭ（Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）のための拡張認証プロトコル方法（ＥＡＰ－ＳＩＭ）（Ｅｘｔｅｎｓｉｂｌｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ Ｍｅｔｈｏｄ ｆｏｒ Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ （ＧＳＭ） Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅｓ （ＥＡＰ－ＳＩＭ））」、ＲＦＣ ４１８６、２００６年1月
［１１］ Ｊ．Ａｒｋｋｏ、Ｈ．Ｈａｖｅｒｉｎｅｎ共著、「第３世代認証および鍵協定用の拡張認証プロトコル方法（ＥＡＰ－ＡＫＡ）（Ｅｘｔｅｎｓｉｂｌｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ Ｍｅｔｈｏｄ ｆｏｒ ３ｒｄ Ｇｅｎｅｒａｔｉｏｎ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ａｇｒｅｅｍｅｎｔ （ＥＡＰ－ＡＫＡ））」、ＲＦＣ ４１８７、２００６年1月
［１２］ ３ＧＰＰ ＴＳ ４３．３１８ ｖ６．９．０、「第３世代パートナーシッププロジェクト：ＧＳＭ／ＥＤＧＥ無線アクセスネットワーク技術仕様グループ：Ａ／Ｇｂインタフェースへの包括的アクセス：ステージ２（リリース６）（３ｒｄ Ｇｅｎｅｒａｔｉｏｎ Ｐａｒｔｎｅｒｓｈｉｐ Ｐｒｏｊｅｃｔ； Ｔｅｃｈｎｉｃａｌ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｇｒｏｕｐ ＧＳＭ／ＥＤＧＥ Ｒａｄｉｏ Ａｃｃｅｓｓ Ｎｅｔｗｏｒｋ； Ｇｅｎｅｒｉｃ ａｃｃｅｓｓ ｔｏ ｔｈｅ Ａ／Ｇｂ ｉｎｔｅｒｆａｃｅ； Ｓｔａｇｅ ２ （Ｒｅｌｅａｓｅ ６））」
［１３］ ３ＧＰＰ ＴＳ ４４．３１８ ｖ６．８．０、「第３世代パートナーシッププロジェクト：ＧＳＭ／ＥＤＧＥ無線アクセスネットワーク技術仕様グループ：Ａ／Ｇｂインタフェースへの包括的アクセス（ＧＡ）：モバイルＧＡインタフェースレイヤ３仕様（リリース６）（３ｒｄ Ｇｅｎｅｒａｔｉｏｎ Ｐａｒｔｎｅｒｓｈｉｐ Ｐｒｏｊｅｃｔ； Ｔｅｃｈｎｉｃａｌ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｇｒｏｕｐ ＧＳＭ／ＥＤＧＥ Ｒａｄｉｏ Ａｃｃｅｓｓ Ｎｅｔｗｏｒｋ； Ｇｅｎｅｒｉｃ Ａｃｃｅｓｓ （ＧＡ） ｔｏ ｔｈｅ Ａ／Ｇｂ ｉｎｔｅｒｆａｃｅ； Ｍｏｂｉｌｅ ＧＡ ｉｎｔｅｒｆａｃｅ ｌａｙｅｒ ３ ｓｐｅｃｉｆｉｃａｔｉｏｎ （Ｒｅｌｅａｓｅ ６））」
［１４］ ３ＧＰＰ ＴＳ ２３．２３４ ｖ６．１０．０、「第３世代パートナーシッププロジェクト：サービス・システムアスペクト技術仕様グループ：３ＧＰＰシステムと無線ローカルエリアネットワーク（ＷＬＡＮ）のインターワーキング：システム解説（リリース６）（３ｒｄ Ｇｅｎｅｒａｔｉｏｎ Ｐａｒｔｎｅｒｓｈｉｐ Ｐｒｏｊｅｃｔ； Ｔｅｃｈｎｉｃａｌ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｇｒｏｕｐ Ｓｅｒｖｉｃｅ

s and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 6))」
［15］ 3GPP TS 24.234 v7.5.0、「第3世代パートナーシッププロジェクト：コアネットワークおよび端末技術仕様グループ：3GPPシステムと無線ローカルエリアネットワーク（WLAN）のインターワーキング：ユーザ機器（UE）からネットワークプロトコル：ステージ3（リリース7）（3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP system to Wireless Local Area Network (WLAN) interworking; User Equipment (UE) to network protocols; Stage 3 (Release 7))」
［16］ 3GPP TS 33.234 v7.4.0、「第3世代パートナーシッププロジェクト：サービス・システムアスペクト技術仕様グループ：3Gセキュリティ：無線ローカルエリアネットワーク（WLAN）インターワーキングセキュリティ（リリース7）（3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Wireless Local Area Network (WLAN) interworking security (Release 7))」

【図１】

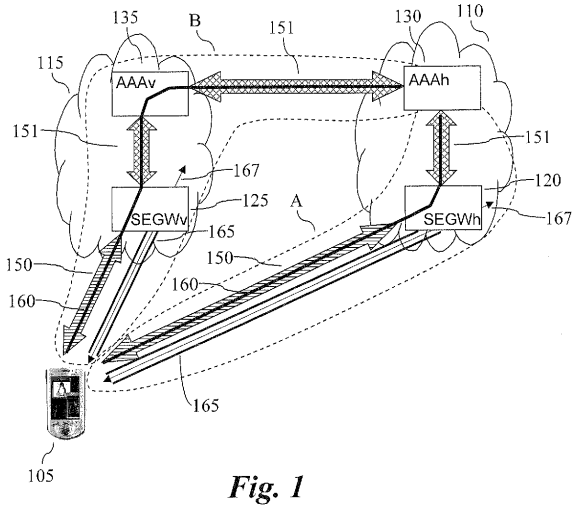

Fig. 1

【図２ａ】

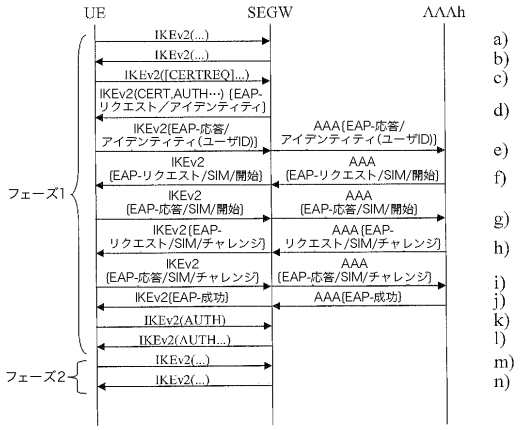

Fig. 2a

【図２ｂ】

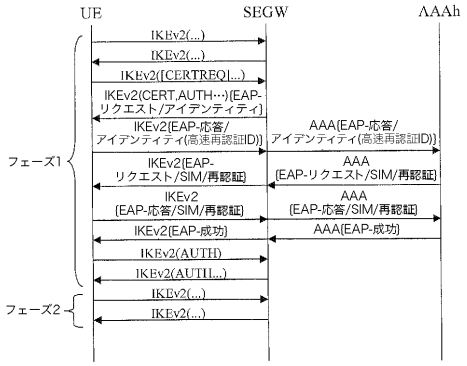

Fig. 2b

【図２ｃ】

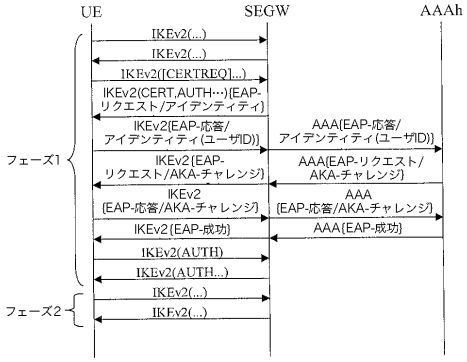

Fig. 2c

【図２ｄ】

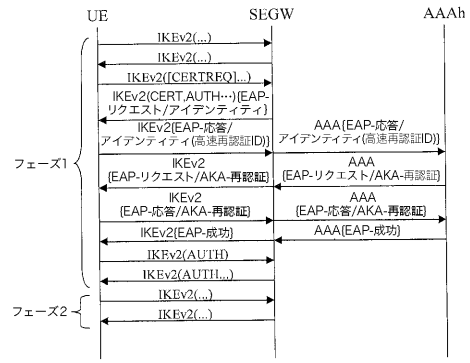

Fig. 2d

【図３】

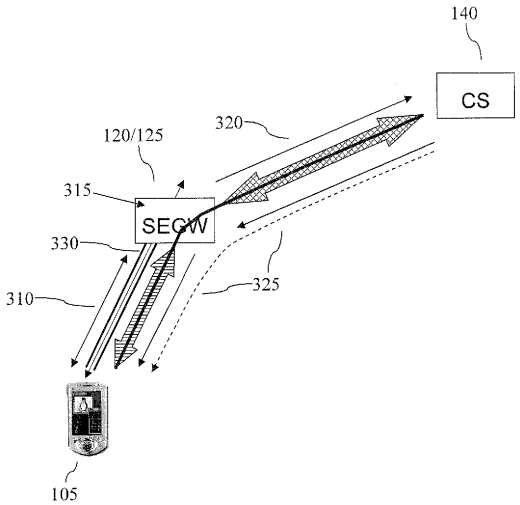

Fig. 3

【図４ａ】

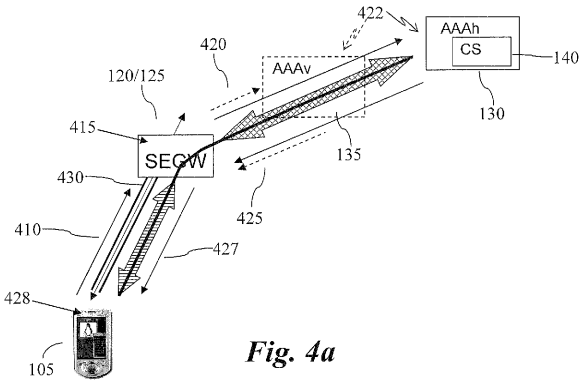

Fig. 4a

【図４ｂ】

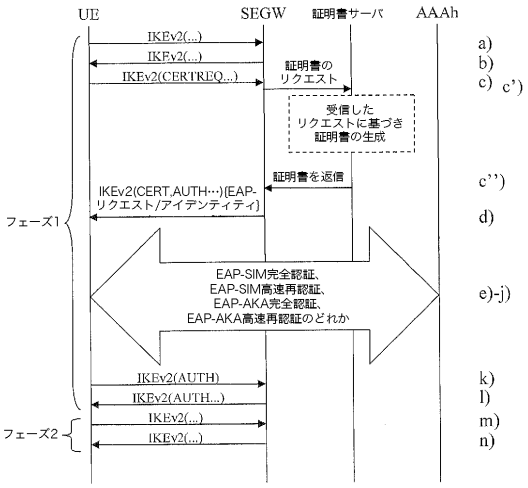

Fig. 4b

【図５ａ】

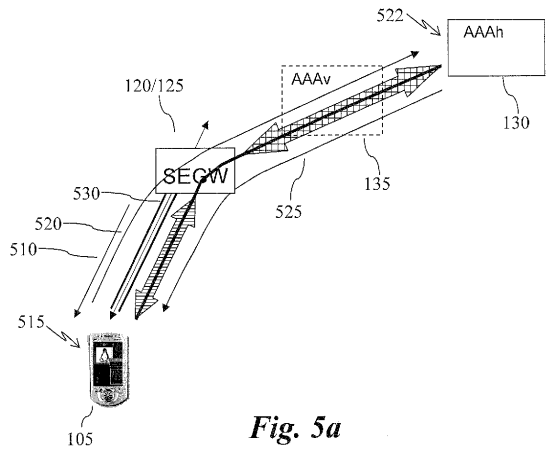

Fig. 5a

【図５ｂ】

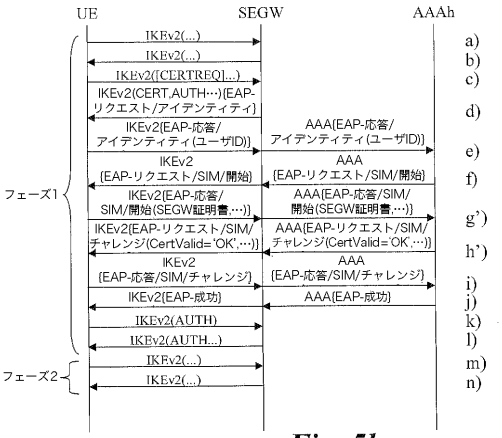

Fig. 5b

【図５ｃ】

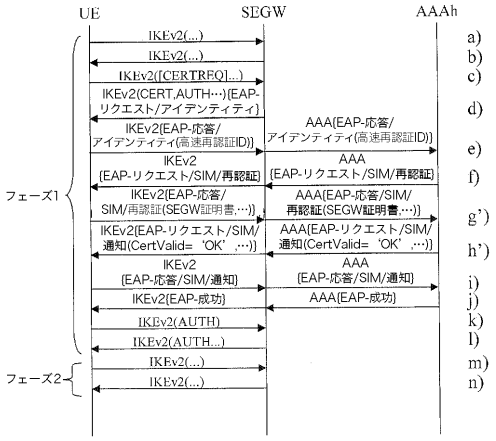

Fig. 5c

【図５ｄ】

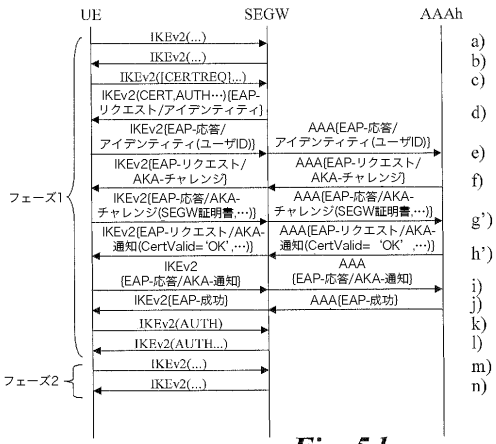

Fig. 5d

【図５ｅ】

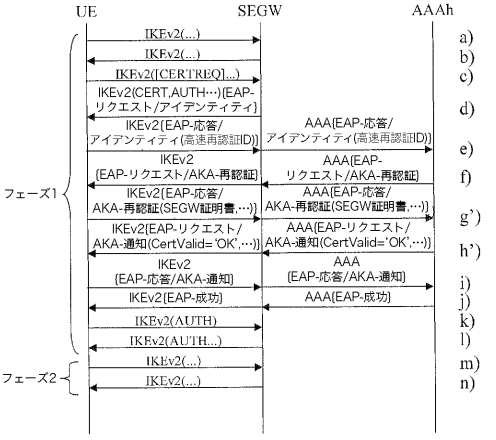

Fig. 5e

【図６ａ】

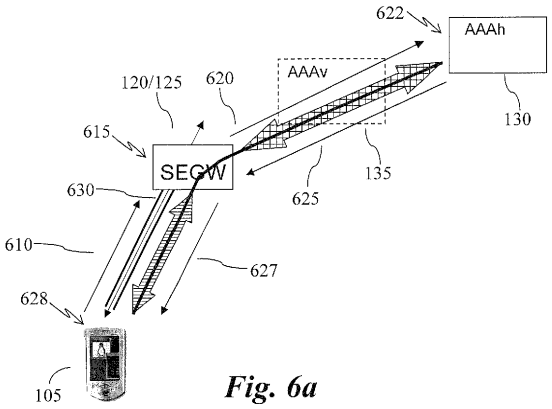

Fig. 6a

【図６ｂ】

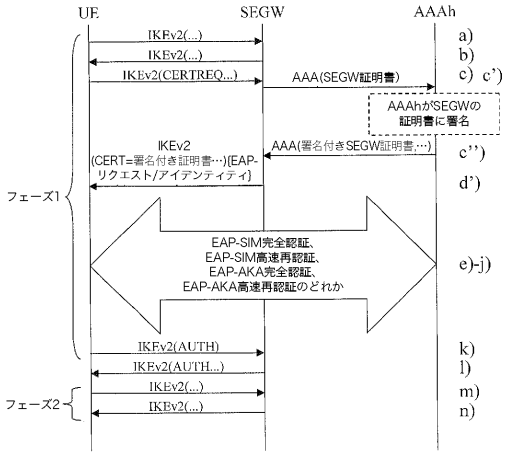

Fig. 6b

【図７】

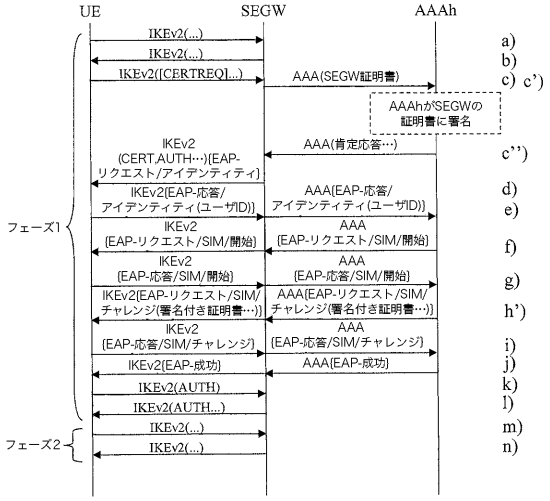

Fig. 7

【図８ａ】

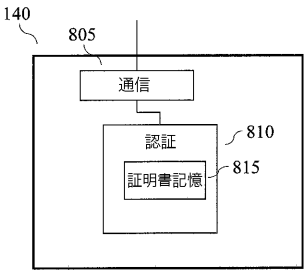

Fig. 8a

【図８ｂ】

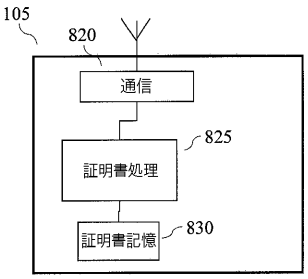

Fig. 8b

【図８ｃ】

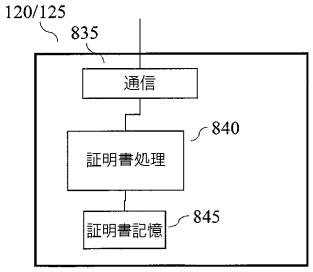

Fig. 8c

フロントページの続き

(72)発明者　ルネ，　ヨハン
スウェーデン国　リディンゲ　エス－１８１３０，　テレングヴェーゲン　１２
(72)発明者　ニランダー，　トマス
スウェーデン国　ヴェルムデ　エス－１３９３４，　ヘグトルプスヴェーゲン　２８
(72)発明者　ヴィクベリ，　ヤリ
スウェーデン国　イェルナ　エス－１５１３８，　スヴァルセテーシュヴェーゲン　１２

審査官　石田　信行

(56)参考文献　特開２００４－２３１６６（ＪＰ，Ａ）
特表２００６－５２７９６７（ＪＰ，Ａ）
特開２００８－２２８０８９（ＪＰ，Ａ）
米国特許出願公開第２００２／０１５２３８２（ＵＳ，Ａ１）
米国特許出願公開第２００３／００２８８０５（ＵＳ，Ａ１）
米国特許出願公開第２００６／０２５３７０３（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　9/32
H04W　12/04