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

特許第5865992号
(P5865992)

(45)発行日　平成28年2月17日(2016.2.17)　(24)登録日　平成28年1月8日(2016.1.8)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| H04L 9/32 | (2006.01) | H04L | 9/00 | 675A |
| H04W 12/06 | (2009.01) | H04W | 12/06 | |
| G06F 21/44 | (2013.01) | G06F | 21/44 | |

請求項の数 17　(全 54 頁)

| | |
|---|---|
| (21)出願番号 | 特願2014-501278 (P2014-501278) |
| (86)(22)出願日 | 平成24年3月23日 (2012.3.23) |
| (65)公表番号 | 特表2014-515207 (P2014-515207A) |
| (43)公表日 | 平成26年6月26日 (2014.6.26) |
| (86)国際出願番号 | PCT/US2012/030352 |
| (87)国際公開番号 | WO2012/129503 |
| (87)国際公開日 | 平成24年9月27日 (2012.9.27) |
| 審査請求日 | 平成25年11月21日 (2013.11.21) |
| (31)優先権主張番号 | 61/525,575 |
| (32)優先日 | 平成23年8月19日 (2011.8.19) |
| (33)優先権主張国 | 米国 (US) |
| (31)優先権主張番号 | 61/466,852 |
| (32)優先日 | 平成23年3月23日 (2011.3.23) |
| (33)優先権主張国 | 米国 (US) |

(73)特許権者　510030995
インターデイジタル　パテント　ホールディングス　インコーポレイテッド
アメリカ合衆国　１９８０９　デラウェア州　ウィルミントン　ベルビュー　パークウェイ　２００　スイート　３００
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　インヒョク　チャ
大韓民国　ソウル　カンナム－ク　サムスン－ドン　１４－１ヨン－アン　ハイツビレッジ　１０２－ドン　２０２－ホ

最終頁に続く

(54)【発明の名称】ネットワーク通信をセキュアにするためのシステムおよび方法

(57)【特許請求の範囲】

【請求項１】

ＵＥ（ユーザ装置）、クラウドホストされたバーチャルマシンに関連付けられたサービスプロバイダ、およびローカルＩＤプロバイダを備えるＩＤプロバイダ、を備えるシステムにおいて、前記サービスプロバイダと前記ＵＥとの間におけるセキュアな通信を確立するための方法であって、

前記ＵＥにおいて、前記ＵＥと前記サービスプロバイダとの間におけるセキュアチャネルを確立するステップと、

前記ＩＤプロバイダを用いて前記ＵＥの認証を実行するための認証パラメータを前記ＩＤプロバイダへ送信するステップと、

前記ＵＥにおいて、前記ＵＥの成功した認証を示す認証アサーションを決定するステップと、

前記ＵＥにおいて、前記セキュアチャネルが確立された前記サービスプロバイダが、前記ＵＥがサービスへのアクセスのための認証を実行することを望んだ、意図されたサービスプロバイダであることを検証するステップであって、前記サービスプロバイダは、前記セキュアチャネルの前記確立中に生成された少なくとも１つのパラメータを使用して検証される、ステップと、

を含み、

前記ＵＥと前記サービスプロバイダとの間における前記セキュアチャネルを確立するステップは、前記ローカルＩＤプロバイダと前記クラウドホストされたバーチャルマシンに

関連付けられた前記サービスプロバイダとの間において前記セキュアチャネルを確立して、前記クラウドホストされたバーチャルマシンによって提供されたサービスへのアクセスを可能とすることを含む、方法。

【請求項２】

前記ＵＥの前記認証を前記セキュアチャネルの前記確立にバインドするステップをさらに含む、請求項１に記載の方法。

【請求項３】

前記ＵＥの前記認証は、ＳＩＰ－Ｄｉｇｅｓｔ（Ｓｅｓｓｉｏｎ Ｉｎｉｔｉａｔｉｏｎ Ｐｒｏｔｏｃｏｌ Ｄｉｇｅｓｔ）認証を含み、前記ＵＥの前記認証を前記セキュアチャネルの前記確立にバインドする前記ステップは、前記ＳＩＰ－Ｄｉｇｅｓｔ認証を前記セキュアチャネルの前記確立にバインドするステップを含む、請求項２に記載の方法。

【請求項４】

前記ＵＥの前記認証を前記セキュアチャネルの前記確立にバインドする前記ステップは、前記認証アサーション内に含まれている情報を使用して実行され、前記情報は、前記ＵＥと前記サービスプロバイダとの間における前記セキュアチャネルの前記確立に関連付けられている、請求項２に記載の方法。

【請求項５】

前記ＵＥの前記認証を前記セキュアチャネルの前記確立にバインドする前記ステップは、前記セキュアチャネルが確立された前記サービスプロバイダが前記意図されたサービスプロバイダであることを前記ＵＥが検証できるようにする、請求項２に記載の方法。

【請求項６】

前記ＵＥにおいて前記サービスプロバイダの認証を決定するステップをさらに含む、請求項１に記載の方法。

【請求項７】

前記サービスプロバイダの前記認証を、前記ＵＥと前記サービスプロバイダとの間における前記セキュアチャネルの前記確立にバインドするステップをさらに含む、請求項６に記載の方法。

【請求項８】

前記サービスプロバイダの前記認証を前記セキュアチャネルの前記確立にバインドする前記ステップは、前記セキュアチャネルが確立された前記サービスプロバイダが前記意図されたサービスプロバイダであることを前記ＵＥが検証できることによって前記サービスプロバイダの認証が決定されることを可能にする、請求項７に記載の方法。

【請求項９】

前記サービスプロバイダの前記認証を決定する前記ステップは、外部のＩＤプロバイダからサービスプロバイダ認証アサーションを受信するステップを含む、請求項６に記載の方法。

【請求項１０】

前記認証アサーションを決定する前記ステップは、前記ローカルＩＤプロバイダを使用して前記認証アサーションを生成するステップを含む、請求項１に記載の方法。

【請求項１１】

前記ローカルＩＤプロバイダは、前記ＵＥの前記認証から生成されて事前に確立された共有キーに関連付けられており、前記事前に確立された共有キーは、前記ＵＥと前記サービスプロバイダとの間における前記セキュアチャネルを確立するために使用される、請求項１に記載の方法。

【請求項１２】

前記認証中に生成された前記少なくとも１つのパラメータは、前記認証アサーションを含み、前記セキュアチャネルの確立中に生成された前記少なくとも１つのパラメータは、暗号化されたシード値、前記ＵＥと前記サービスプロバイダとの間におけるセキュアなＴＬＳ（ｔｒａｎｓｐｏｒｔ－ｌａｙｅｒ ｓｅｃｕｒｉｔｙ）トンネルから抽出されたキーマテリアルから導出されたバインディング応答、または前記セキュアチャネルの確立の

ために使用されたノンスを含む、請求項１に記載の方法。
【請求項１３】
前記サービスプロバイダは、前記ＵＥと前記サービスプロバイダとの間における前記セキュアチャネルを介して前記サービスプロバイダから受信された情報の妥当性を確認することによって、前記意図されたサービスプロバイダとして検証される、請求項１に記載の方法。
【請求項１４】
クラウドホストされたバーチャルマシンに関連付けられたサービスプロバイダとのセキュアな通信を確立するように構成されたＵＥ（ユーザ装置）であって、
コンピュータ実行可能命令が格納されたメモリと、
前記ＵＥと前記サービスプロバイダとの間におけるセキュアチャネルを確立するステップと、
認証パラメータを、前記ＵＥ上に存在するローカルＩＤプロバイダを備えるＩＤプロバイダへ送信するステップであって、前記認証パラメータは、前記ＩＤプロバイダを用いて前記ＵＥの認証を実行するためのものである、ステップと、
前記ＵＥの成功した認証を示す認証アサーションを決定するステップと、
前記セキュアチャネルが確立された前記サービスプロバイダが、前記ＵＥがサービスのための認証を実行することを望んだ、意図されたサービスプロバイダであることを検証するステップであって、前記サービスプロバイダは、前記セキュアチャネルの前記確立中に生成された少なくとも１つのパラメータを使用して検証される、ステップと、
を実行するための前記コンピュータ実行可能命令を実行するように構成されたプロセッサと、
を備え、
前記プロセッサは、前記ローカルＩＤプロバイダと前記クラウドホストされたバーチャルマシンに関連付けられた前記サービスプロバイダとの間において前記セキュアチャネルを確立することによって、前記ＵＥと前記サービスプロバイダとの間における前記セキュアチャネルを確立し、前記クラウドホストされたバーチャルマシンによって提供されたサービスへのアクセスを可能とするようにさらに構成された、ＵＥ。
【請求項１５】
前記プロセッサは、前記ＵＥの前記認証を前記セキュアチャネルの前記確立とバインドするようにさらに構成された、請求項１４に記載のＵＥ。
【請求項１６】
前記プロセッサは、
前記サービスプロバイダの認証を決定し、
前記サービスプロバイダの前記認証を、前記ＵＥと前記サービスプロバイダとの間における前記セキュアチャネルの前記確立にバインドする
ようにさらに構成された、請求項１４に記載のＵＥ。
【請求項１７】
前記ローカルＩＤプロバイダは、前記ＵＥの前記認証から生成されて事前に確立された共有キーに関連付けられており、前記事前に確立された共有キーは、前記ＵＥと前記サービスプロバイダとの間における前記セキュアチャネルを確立するために使用される、請求項１４に記載のＵＥ。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線通信技術に関する。
【０００２】
関連出願の相互参照
本出願は、２０１１年３月２３日に出願された米国特許仮出願第６１／４６６，６６２号明細書、２０１１年８月１９日に出願された米国特許仮出願第６１／５２５，５７５号

明細書、および２０１１年３月２３日に出願された米国特許仮出願第６１／４６６，８５２号明細書の利益を主張するものであり、これらの仮出願の内容は、それらの全体が参照によって本明細書に組み込まれている。

【背景技術】

【０００３】

通信ネットワークにおいては、ネットワークエンティティーどうしの間におけるさまざまな形態の通信が、サードパーティーの攻撃の影響を受ける可能性がある。たとえば、一実施形態によれば、ユーザデバイスが、通信ネットワークを介してサービスプロバイダからのサービス（たとえば、ウェブサイト）にアクセスしようと試みる場合がある。ユーザデバイスからのこのアクセスの試み、および／またはその他の通信は、サードパーティーまたはＭｉｔＭ（ｍａｎ－ｉｎ－ｔｈｅ－ｍｉｄｄｌｅ）によってインターセプトされる可能性がある。そのサードパーティーは、たとえば認証情報（たとえば、ユーザ名および／またはパスワード）など、ユーザデバイスに関連付けられている情報へのアクセスを得るために、意図されたサービスプロバイダのふりをすることができる。そのサードパーティーは、ユーザデバイスから認証情報を得ることに成功した場合には、その認証情報を意図されていない目的または悪意のある目的のために使用することができる。たとえば、そのサードパーティーは、意図されたサービスプロバイダからのサービスおよび／またはその他の情報にアクセスするために、ユーザデバイスのふりをすることができる。

【０００４】

一実施形態においては、ネットワーク通信は、攻撃に対して脆弱である場合がある。なぜなら、それらの通信は、十分に保護されていない場合があるためであり、および／または、それらの通信は、それらの通信が送信されんとしている先のネットワークエンティティーが、それらの通信を受信するための真正なまたは意図されたネットワークエンティティーであるという適正な保証を伴わずに送信される場合があるためである。たとえば、ネットワーク通信は、一面だけの認証プロトコルを使用して、たとえばパブリックキーの送信を介して実施される場合があり、それによってネットワーク通信は、サードパーティーまたはＭｉｔＭの攻撃に対して脆弱なままとなる場合がある。

【発明の概要】

【０００５】

この「発明の概要」は、以降の「発明を実施するための形態」においてさらに説明されるさまざまなコンセプトを、簡略化された形式で紹介するために提供されている。

【０００６】

サービスプロバイダとＵＥ（ユーザ装置：ｕｓｅｒ　ｅｑｕｉｐｍｅｎｔ）との間におけるセキュアな通信を確立するためのシステム、方法、および装置の実施形態が、本明細書に記載されている。たとえば、ネットワーク通信が、ＵＥ、サービスプロバイダ、および／またはＩＤプロバイダ（ｉｄｅｎｔｉｔｙ　ｐｒｏｖｉｄｅｒ）を含むシステムにおいて実施されることが可能である。セキュアチャネルが、ＵＥとサービスプロバイダとの間において確立されることが可能である。ＩＤプロバイダを用いてＵＥの認証を実行するための認証パラメータが、ＩＤプロバイダへ送信されることが可能である。ＵＥの成功した認証を示すＵＥ認証アサーションが、ＵＥにおいて決定されることが可能である。たとえば、ＵＥ認証アサーションは、外部のネットワークエンティティーから受信されること、またはＵＥにおいてローカルに決定されることが可能である。ＵＥは、セキュアチャネルが確立されたサービスプロバイダが、意図されたサービスプロバイダであることを検証することができる。意図されたサービスプロバイダは、サービスが受信されるように意図された、および／またはそのようなサービスへのアクセスのための認証が実行されることになるサービスプロバイダを含みうる。サービスプロバイダは、ＩＤプロバイダを用いたＵＥの認証中に、および／またはセキュアチャネルの確立中に生成された少なくとも１つのパラメータを使用して、意図されたサービスプロバイダとして検証されることが可能である。

【０００７】

別の例示的な実施形態によれば、ＵＥは、サービスプロバイダとのセキュアな通信を確立するように構成されることが可能である。ＵＥは、その上にコンピュータ実行可能命令が格納されているメモリと、それらのコンピュータ実行可能命令を実行するように構成されているプロセッサとを含むことができる。ＵＥは、ＵＥとサービスプロバイダとの間におけるセキュアチャネルを確立するように構成されることが可能である。ＵＥは、ＩＤプロバイダを用いてＵＥの認証を実行するための認証パラメータをＩＤプロバイダへ送信することができる。ＵＥの成功した認証を示す認証アサーションが、ＵＥにおいて決定されることが可能である。たとえば、ＵＥ認証アサーションは、外部のネットワークエンティティーから受信されること、またはＵＥにおいてローカルに決定されることが可能である。ＵＥは、サービスのための認証を実行するために、セキュアチャネルが確立されたサービスプロバイダが、意図されたサービスプロバイダであることを検証するように構成されることも可能である。意図されたサービスプロバイダは、サービスが受信されるように意図された、および／またはそのようなサービスへのアクセスのための認証が実行されることになるサービスプロバイダを含みうる。ＵＥは、ＩＤプロバイダを用いたＵＥの認証中に、および／またはセキュアチャネルの確立中に生成された少なくとも１つのパラメータを使用して、サービスプロバイダが、意図されたサービスプロバイダであることを検証することができる。

【０００８】

別の例示的な実施形態によれば、セキュアチャネルが、ＩＤプロバイダとサービスプロバイダとの間において確立されることが可能である。たとえば、キー情報が、ＩＤプロバイダとサービスプロバイダとの間におけるセキュアチャネルを介してサービスプロバイダにおいて受信されることが可能である。セキュアチャネルは、たとえば受信されたキー情報を使用することなどによって、サービスプロバイダとＵＥとの間において確立されることも可能である。サービスプロバイダにおいて、ＵＥの認証を示す認証アサーションが受信されることが可能である。認証アサーションは、ＩＤプロバイダとサービスプロバイダとの間におけるセキュアチャネル、および／またはサービスプロバイダとＵＥとの間におけるセキュアチャネルを介して受信された情報を使用して、サービスプロバイダにおいて検証されることが可能である。

【０００９】

この「発明の概要」は、以降の「発明を実施するための形態」においてさらに説明されるコンセプトから抜粋したものを、簡略化された形式で紹介するために提供される。この「発明の概要」は、特許請求される主題の鍵となる特徴または必要不可欠な特徴を特定することを意図されておらず、特許請求される主題の範囲を限定するために使用されることも意図されていない。さらに、特許請求される主題は、本開示の任意の部分に記載されているあらゆるまたはすべての不利な点を解決するいかなる制限にも限定されるものではない。

【図面の簡単な説明】

【００１０】

以降の説明から、より詳細な理解が得られ、以降の説明は、例として添付の図面とともに与えられている。

【図１】ＩＤプロバイダとＵＥ（ユーザ装置：ｕｓｅｒ　ｅｑｕｉｐｍｅｎｔ）との間におけるセキュアチャネルを確立するためのプロビジョニングフェーズに関する例示的なメッセージフロー図である。

【図２】ローカルＩＤプロバイダを使用する認証フェーズに関する例示的なメッセージフロー図である。

【図３】サービスプロバイダ認証のためのメッセージのやり取りに関する例示的なメッセージフロー図である。

【図４】サービスプロバイダ認証のためのメッセージのやり取りに関する別の例示的なメッセージフロー図である。

【図５】ＵＥとサービスプロバイダとの間における事前に確立されたセキュアチャネルを

使用するローカルＩＤプロバイダ認証のためのセキュアチャネルの確立を示す例示的なメッセージフロー図である。
【図６】ＧＢＡ（Ｇｅｎｅｒｉｃ Ｂｏｏｔｓｔｒａｐ Ａｒｃｈｉｔｅｃｔｕｒｅ）／ＧＢＡ＿Ｈプロトコルの一例に関する例示的なメッセージフロー図である。
【図７】ＳＩＰ－Ｄｉｇｅｓｔ（Ｓｅｓｓｉｏｎ Ｉｎｉｔｉａｔｉｏｎ Ｐｒｏｔｏｃｏｌ Ｄｉｇｅｓｔ）認証を用いた、ＴＬＳ（Ｔｒａｎｓｐｏｒｔ－Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ）とＧＢＡとをバインドするための例示的なメッセージフロー図である。
【図８】ローカル認証エンティティー／ＩＤプロバイダおよびクラウド／リモートコンピューティングサービスを実装している例示的な通信システムを示す図である。
【図９】ＳＩＰ－Ｄｉｇｅｓｔ認証を使用し、サービスプロバイダ認証を含む例示的なメッセージフロー図である。
【図１０】ＩＤプロバイダに対するサービスプロバイダ認証を用いた例示的なプロトコルの例示的なメッセージフロー図である。
【図１１】ローカルＩＤプロバイダを用いたプロビジョニングフェーズの例示的なメッセージフロー図である。
【図１２】ローカルアサーションプロバイダを用いた例示的な認証フェーズの例示的なメッセージフロー図である。
【図１３Ａ】１つまたは複数の開示されている実施形態が実施されることが可能である例示的な通信システムのシステム図である。
【図１３Ｂ】図１３Ａにおいて示されている通信システム内で使用されることが可能である例示的なＷＴＲＵ（ｗｉｒｅｌｅｓｓ ｔｒａｎｓｍｉｔ／ｒｅｃｅｉｖｅ ｕｎｉｔ）のシステム図である。
【図１３Ｃ】図１３Ａにおいて示されている通信システム内で使用されることが可能である例示的なＲＡＮ（ｒａｄｉｏ ａｃｃｅｓｓ ｎｅｔｗｏｒｋ）および例示的なコアネットワークのシステム図である。
【図１３Ｄ】一実施形態による例示的なＲＡＮおよびコアネットワークの別のシステム図である。
【図１３Ｅ】一実施形態による例示的なＲＡＮおよびコアネットワークの別のシステム図である。
【発明を実施するための形態】
【００１１】
本明細書において開示されているシステム、方法、および装置の実施形態は、たとえばユーザ／ＵＥ（ユーザ装置：ｕｓｅｒ ｅｑｕｉｐｍｅｎｔ）、サービスプロバイダ、および／またはＩＤプロバイダなどのネットワークエンティティーどうしの間におけるセキュアな通信を提供する。本明細書に記載されているように、セキュアな通信は、ネットワークエンティティーどうしの間における共有キー／シークレットを使用して、および／またはパブリック／プライベートキーを使用してネットワークエンティティーどうしの間において確立されたセキュアチャネルを介して実行されることが可能である。これらのセキュアチャネルは、たとえばＭｉｔＭ（ｍａｎ－ｉｎ－ｔｈｅ－ｍｉｄｄｌｅ）攻撃など、サードパーティーからの攻撃を防止するために使用されることが可能である。
【００１２】
本明細書に記載されている一実施形態においては、セキュアな通信は、通信を送信および／または受信するための意図された認証されたエンティティーを識別するための共有キーまたは共有シークレットを使用して実行されることが可能である。たとえば、共有キーまたは共有シークレットは、ネットワークエンティティーどうしの間において送信されるメッセージに、それらのネットワークエンティティーの真正性を示す様式で暗号化および／または署名を行うために使用されることが可能である。
【００１３】
例示的な一実施形態においては、本明細書に記載されているセキュアな通信は、ＯｐｅｎＩＤ認証プロトコルに基づくことおよび／またはバインドされることが可能である。Ｏ

ｐｅｎＩＤ認証においては、サービスプロバイダは、ＲＰ（ｒｅｌｙｉｎｇ　ｐａｒｔｙ）であることが可能であり、および／またはＩＤプロバイダは、ＯＰ（ＯｐｅｎＩＤ　ｉｄｅｎｔｉｔｙ　ｐｒｏｖｉｄｅｒ）であることが可能である。ＯｐｅｎＩＤ認証は、ＯｐｅｎＩＤ、および／またはローカルＯｐｅｎＩＤと呼ばれる変形形態の使用を含むことができ、ローカルＯｐｅｎＩＤでは、ＯｐｅｎＩＤにおけるＯＰの何らかの機能が、ローカルエンティティー（たとえば、ＵＥ、ゲートウェイ、スマートカード、ＵＩＣＣ（Ｕｎｉｖｅｒｓａｌ　Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ　Ｃａｒｄ）など）によって実行される。

【００１４】

ここでは、ＯｐｅｎＩＤ認証フローにおけるＲＰの認証が説明される。これが役立つことができるのは、たとえば、ユーザ／ＵＥとＲＰが、信頼関係（ウェブサイト証明書を、および／または、たとえばＡＡＡデータベースからＲＰによってアクセス可能なＵＥに関するクレデンシャルのセットを使用して確立されることが可能であるような信頼関係）を有することができないケースである。別の実施形態は、本明細書に記載されているようなローカルＯＰ／ＲＰプライベート共有シークレット（ｌｏｃａｌ　ＯＰ－ＲＰ　ｐｒｉｖａｔｅ　ｓｈａｒｅｄ　ｓｅｃｒｅｔ）の確立を含むことができる。

【００１５】

ローカルモバイルＳＳＯ（ｓｉｎｇｌｅ　ｓｉｇｎ－ｏｎ）は、ＳＳＯおよび／または関連したＩＤマネージメント機能の一部または全体を総称するための用語であり、それらは、従来であれば、たとえばウェブベースのＳＳＯサーバによって実行されるかもしれないが、現在は、ローカルベースのエンティティーまたはモジュール（たとえば、ＵＥ、スマートカード、またはＵＩＣＣにおいて存在するセキュアな環境）によって実行されており、そうしたエンティティーまたはモジュールは、通信デバイス自体の一部もしくは全体である場合があり、または、そのようなエンティティー／モジュールは、通信デバイスおよび／もしくはそのユーザのすぐそばに物理的におよび／もしくは論理的に配置されている（たとえば、ゲートウェイを介して接続されているなど、ローカルに配置されている）場合がある。たとえば、エンティティー／モジュールは、デバイス内に組み込まれること、デバイスに接続されること、および／または、ローカルインターフェース、配線、もしくは短距離ワイヤレス手段によってデバイスに接続されることが可能である。

【００１６】

ローカルＯｐｅｎＩＤは、ローカルモバイルＳＳＯのタイプを示すための用語として使用されることが可能であり、それによって、そのＳＳＯまたはＩＤマネージメントは、そのＯｐｅｎＩＤプロトコルに基づく。たとえば、ローカルＯｐｅｎＩＤは、ローカルに配置されているエンティティー／モジュールによって実行されることが可能であるＯＰまたはＩｄＰ（ＯｐｅｎＩＤ　Ｉｄｅｎｔｉｔｙ　Ｐｒｏｖｉｄｅｒ）の機能を示すために使用されることが可能である。

【００１７】

ローカルＩｄＰは、ローカル認証および／またはアサーション機能を実行するローカルエンティティーまたはモジュールを示すために使用される用語である。たとえば、ローカルＩｄＰは、ローカルＯｐｅｎＩＤのためのＯｐｅｎＩＤサーバの認証および／またはアサーション機能を実行することができる。ＯｐｅｎＩＤ機能を実施するローカルＩｄＰを示すために、$OP_{loc}$という略称が使用されることが可能であるが、ローカルＩｄＰは、同様の機能を実行することができ、ＯｐｅｎＩＤプロトコルを実施することを求められないことが可能である。ローカルＩｄＰの１つの機能は、ユーザおよび／またはデバイスのＩＤに関する（１つまたは複数の）アサーションを通じてユーザおよび／またはデバイスの認証を容易にすることであると言える。例示的な一実施形態においては、そのような認証アサーションは、ローカルＩｄＰから、デバイス上で動作しているＢＡ（ｂｒｏｗｓｅｒ　ａｇｅｎｔ）へ送信されることが可能であり、ＢＡは、その認証アサーションを外部のＲＰへ転送することができる。ローカルＩｄＰによって提供される（１つまたは複数の）機能が、主として、そのような認証アサーションを提供することに限定されている場

合には、そのローカルＩｄＰは、ＬＡＥ（Ｌｏｃａｌ　Ａｓｓｅｒｔｉｏｎ　Ｅｎｔｉｔｙ）と呼ばれうる。

【００１８】

ローカルＩｄＰは、認証アサーションメッセージを処理し、作成し、管理し、および／または、１つもしくは複数の外部の受信者へ送信することができる。認証アサーションメッセージは、ユーザおよび／またはデバイスに関連している１つまたは複数のＩＤの検証の状態をアサートすることができる。たとえば、ＯｐｅｎＩＤプロトコルにおいては、ＲＰなどのサードパーティーエンティティーは、認証アサーションメッセージの受信者のうちの１人であることが可能である。ローカルＩｄＰは、たとえば共有キーまたはパブリック／プライベートキーの取り合わせなどの暗号技術を使用して、認証アサーションメッセージに署名することもできる。

【００１９】

ローカルＯｐｅｎＩＤの実施態様は、ルートセッションキーなどの１つまたは複数の暗号化キーを使用することができる。ルートセッションキーは、ＲＰと、ＵＥ上に存在しているＯＰ$_{loc}$との間において使用することを意図される場合がある。そのようなキーは、ＲＰと、その他のキーが導出されることが可能である元となるＯＰとの間におけるルートセッションキーとして機能することができる。ローカルＯｐｅｎＩＤの方法は、認証アサーションキーを使用することもでき、認証アサーションキーは、ユーザの認証のために（１つまたは複数の）認証アサーションメッセージのうちの１つまたは複数に署名するために使用されることが可能である。そのような認証アサーションキーは、ルートセッションキーから導出されることが可能である。

【００２０】

ローカルＯｐｅｎＩＤの実施態様は、ＯＰＳＦ（ＯｐｅｎＩＤ　Ｓｅｒｖｅｒ　Ｆｕｎｃｔｉｏｎ）と呼ばれるサービスを使用することができ、ＯＰＳＦの役割は、ローカルＩｄＰおよび／またはＲＰによって使用されることが可能であるシークレットを生成すること、共有すること、および／または配布することであると言える。例示的な一実施形態においては、ＯＰＳＦおよびローカルＩｄＰは、外部のＲＰによって単一のエンティティーとして見られることが可能である。ＯＰＳＦは、ローカルＯｐｅｎＩＤによって発行された署名を検証することを可能にすることができ、および／または、ＲＰによって、たとえば公的なインターネットを介して、直接到達可能にすることができる。ＯＰＳＦのアドレスがローカルＩｄＰにマップするようにデバイス上のローカルＤＮＳリゾルビングモジュール（ｌｏｃａｌ　ＤＮＳ　ｒｅｓｏｌｖｉｎｇ　ｍｏｄｕｌｅ）を修正することによって、デバイス上のブラウザは、ローカルＩｄＰへリダイレクトされることが可能である。

【００２１】

ＯｐｅｎＩＤの実施態様は、ＲＰのためにローカルＩｄＰのディスカバリーを容易にするサービスを使用することができる。そのようなサービスは、たとえばＯＰ－ａｇｇによって示されることが可能である。

【００２２】

本明細書において開示されているのは、ＯｐｅｎＩＤ（たとえば、ＯｐｅｎＩＤおよび／またはローカルＯｐｅｎＩＤを含む）を使用して実施されることが可能であるセキュリティーシステム、方法、および装置である。本明細書に記載されている実施形態のうちのいくつかは、たとえばＵＥにおいて実施されることが可能である。ユーザ機器は、ＯｐｅｎＩＤ要求をＯＰへ通信することができる。ＯＰは、本明細書にさらに記載されているように、ＵＥおよび／またはＲＰを認証するために使用されることが可能である。

【００２３】

ローカルＯＰに対するＲＰのトランスペアレントな委任された認証に関する実施形態が説明される。本明細書に記載されている実施形態によれば、ＯｐｅｎＩＤを使用して、および／または、たとえばＯＰ$_{loc}$など、署名された認証アサーションのローカルプロバイダを利用して、どのようにＲＰ認証を実行するかを示すプロトコルが開示される。本明細書に記載されているように、リプレイ保護（ｒｅｐｌａｙ　ｐｒｏｔｅｃｔｉｏｎ）の

ためにチャレンジ値および／またはノンス（ｎｏｎｃｅ）が付加されることが可能である（たとえば、図１におけるプロトコルのステップ１１２および１２０）。

【００２４】

ＲＰを認証するための記載されている実施態様の一態様は、ＯＰＳＦノードによる委任された認証の態様を含むことができる。その態様は、$OP_{loc}$がチャレンジ$RP_{Chv}$を提示する一般的なチャレンジ／応答戦略（ｇｅｎｅｒａｌ ｃｈａｌｌｅｎｇｅ－ｒｅｓｐｏｎｓｅ ｓｔｒａｔｅｇｙ）に従うことができる。このチャレンジは、真正なＲＰがそのチャレンジを復号することができるように適切な方法でＯＰＳＦによって暗号化されることが可能である。たとえば、ＲＰとＯＰＳＦは、シークレット$K_{r,o}$を共有することができ、そのシークレット$K_{r,o}$は、チャレンジを暗号化および復号するために使用されることが可能である。

【００２５】

図１は、例示的なプロビジョニングフェーズ（ＰＰ）のメッセージフロー図を示している。図１において示されているように、このプロビジョニングフェーズは、ＵＥ／$OP_{loc}$１０２、ＲＰ１０４、ＯＰＳＦ１０６、および／またはＨＳＳ（Ｈｏｍｅ Ｓｕｂｓｃｒｉｐｔｉｏｎ Ｓｅｒｖｉｃｅ）１０８を含むことができる。ＵＥ／$OP_{loc}$１０２は、１１０においてログイン識別子（たとえば、ｈｔｔｐアドレスまたはＥメールなどのＯＩＤ（ＯｐｅｎＩＤ ｉｄｅｎｔｉｆｉｅｒ））をＲＰ１０４へサブミットすることができる。１１０におけるメッセージは、ＲＰチャレンジ値$RP_{Chv}$を含むことができる。ＲＰチャレンジ値$RP_{Chv}$は、ＲＰ１０４が自分の真正性を証明するために適切に応答することができる値である。たとえば、これは、１回だけ使用することができるランダムな値とすることができる。１１２において、ＲＰ１０４は、アソシエーション要求（たとえば、ｈｔｔｐ ＰＯＳＴ ＯｐｅｎＩＤアソシエーション要求）をＯＰＳＦ１０６へ送信することができる。このアソシエーション要求は、ＲＰ１０４に対応するＲＰクレデンシャル$RP_{Cred}$、および／または$RP_{Chv}$を含むことができる。$RP_{Cred}$は、ＲＰ１０４の識別子であることが可能であり、この識別子は、ＯＰＳＦ１０６が、ＯＰＳＦ１０６とＲＰ１０４との間において共有される正しい事前共有キー$K_{r,o}$を選択することを可能にすることができる。$RP_{Cred}$は、ＯＰＳＦ１０６がその他の手段（たとえば、インターネットＵＲＬ）によってＲＰ１０４を識別する場合には、メッセージングから省略されることが可能である。１１４において、ＯＰＳＦ１０６は、ＯＰＳＦ１０６とＵＥ／$OP_{loc}$１０２との間における共有シークレット$K_0$がプロビジョンされているかどうかを判定することができる。共有シークレット$K_0$がプロビジョンされている場合には、ＯＰＳＦ１０６は、（たとえば、図２において示されているように）認証フェーズ（ＡＰ）へ進みうる。共有シークレット$K_0$がプロビジョンされていない場合には、プロビジョニングフェーズが続行しうる。

【００２６】

１１６において、ＯＰＳＦ１０６は、たとえば$RP_{Cred}$、またはＲＰ１０４の別の信頼されている識別子に基づいて、共有シークレット$K_{r,o}$を選択することができる。ＯＰＳＦ１０６は、１１８においてＲＰ１０４とのアソシエーションを実行することができる。ＯＰＳＦ１０６は、１１８においてアソシエーションハンドルＡおよび／または署名キーＳを生成することができる。署名キーＳは、アソシエーションハンドルＡの関数に基づいて生成されることが可能である。ＯＰＳＦ１０６は、アソシエーションハンドルＡおよび署名キーＳをＲＰ１０４へ送信することができる。署名キーＳは、共有キー$K_{r,o}$を用いて暗号化されることが可能であり、これは、たとえば$EK_{r,o}$（Ｓ）と呼ばれうる。ＲＰ１０４は、１２０においてリダイレクトメッセージをＵＥ／$OP_{loc}$１０２へ送信することができる。リダイレクトメッセージは、たとえば、ｓｅｓｓｉｏｎＩＤ、ｒｅｔｕｒｎＵＲＬ、ノンス、ログイン識別子（たとえば、ＯＩＤ）、および／またはアソシエーションハンドルＡなどのパラメータを含むことができる。ＵＥ／$OP_{loc}$１０２は、１２２において要求（たとえば、ｈｔｔｐ ＧＥＴ要求）をＯＰＳＦ１０６へ送信することができる。要求（たとえば、ｈｔｔｐ ＧＥＴ要求）は、たとえば、ｓｅｓｓｉ

ｏｎＩＤ、ｒｅｔｕｒｎＵＲＬ、ノンス、ログイン識別子（たとえば、ＯＩＤ）、および／またはアソシエーションハンドルＡなどのパラメータを含むことができる。

【００２７】

１２４において、ＯＰＳＦ１０６は、認証ベクトルおよび／またはその他の情報をＨＳＳ１０８から得ることができる。ＯＰＳＦ１０６は、１２６において認証チャレンジをＵＥ／$OP_{loc}$１０２へ送信することができる。１２８において、ＵＥ／$OP_{loc}$１０２は、認証応答を計算して、その認証応答をＯＰＳＦ１０６へ送信することができる。１３０において、ＯＰＳＦ１０６は、その認証応答の妥当性を確認して、ＯＰＳＦ１０６とＵＥ／$OP_{loc}$１０２との間において共有される共有シークレット$K_0$を生成することができる。認証応答の妥当性を確認した後に共有シークレット$K_0$をこのように生成することによって、ＵＥ／$OP_{loc}$１０２とＯＰＳＦ１０６との間におけるセキュリティーアソシエーションの確立をこの認証にバインドすることができる。たとえば、図１において示されているように、このバインディングは、認証応答の妥当性確認を共有シークレット$K_0$の生成に手順の上でバインドすることであると言える。ＵＥ／$OP_{loc}$１０２は、１３２において共有シークレット$K_0$を生成することができる。１３４においては、ＯＰＳＦ１０６は、ＵＥ／$OP_{loc}$１０２を認証した後に認証アサーションメッセージ$UE_{Assert}$を生成することができる。この認証アサーションは、$K_0$によって暗号化されている$RP_{Cred}$および$RP_{Chv}$を含むことができ、これは、たとえば$K_0$（$RP_{Cred}$，$RP_{Chv}$）と呼ばれうる。$K_0$（$RP_{Cred}$，$RP_{Chv}$）を含むこの認証アサーションは、ＯＰＳＦ１０６が$RP_{104}$を認証したことをＵＥ／$OP_{loc}$１０２に示すことができ、それによってＵＥ／$OP_{loc}$１０２は、自分が本物の$RP_{104}$と対話していることを保証されることが可能である。例示的な一実施形態においては、$RP_{Cred}$は、ＵＥ／$OP_{loc}$１０２によって識別可能である、$RP_{104}$を表す名前（または、その他のテキスト値）であることが可能である。ＯＰＳＦ１０６は、署名キーＳを用いて認証アサーションメッセージ$UE_{Assert}$を暗号化することもでき、これは、たとえば$E_S$（$UE_{Assert}$）と呼ばれうる。ＯＰＳＦ１０６は、１３６においてリダイレクトメッセージをＵＥ／$OP_{loc}$１０２へ送信することができる。このリダイレクトメッセージは、署名されたアサーションメッセージとともにＵＥ／$OP_{loc}$１０２を$RP_{104}$へリダイレクトすることができる。ＵＥ／$OP_{loc}$１０２は、署名されたアサーションメッセージとともに１３８において要求（たとえば、ｈｔｔｐ ＧＥＴ要求）を$RP_{104}$へ送信することができる。１４０において、$RP_{104}$は、共有キー$K_{r,o}$を使用して署名キーＳを復号することができ、および／または、$E_S$（$UE_{Assert}$）を復号することによって、署名キーＳを使用して認証アサーションメッセージ（たとえば、ＯｐｅｎＩＤアサーションメッセージ）を検証することができる。$RP_{104}$は、認証アサーション$UE_{Assert}$を含む通知を１４２においてＵＥ／$OP_{loc}$１０２へ送信することができる。１４４において、ＵＥ／$OP_{loc}$１０２は、$RP_{Chv}$および／または$RP_{Cred}$を復号することによって、認証アサーション$UE_{Assert}$の妥当性を確認することができる。

【００２８】

図１において示されているように、ＯＰＳＦ１０６とＵＥ／$OP_{loc}$１０２との間における共有シークレット$K_0$を確立することができるプロトコルが実施されることが可能である。例示的な一実施形態においては、プロビジョニングフェーズの前に、またはその最中に、ＯＰＳＦ１０６とＵＥ／$OP_{loc}$１０２は、まだシークレットを共有することができない。この共有シークレットは、たとえばネットワークエンティティーＨＳＳ１０８を使用して、ネットワークベースの認証を含めることによってプロトコルが実行されたときに確立されることが可能である。$K_0$を用いて暗号化された$UE_{Assert}$内に$RP_{Chv}$および$RP_{Cred}$を含めることによって、ＵＥ／$OP_{loc}$１０２は、受信されたメッセージが、$RP_{Cred}$によって識別される$RP_{104}$から生じたものであることを保証されることが可能である。$RP_{Cred}$において申告されているＩＤを$RP_{104}$のＩＤと比較することによって、ＵＥ／$OP_{loc}$１０２は、認証情報を受信したＲＰ

がほかにないことと、ＲＰ１０４が、ＵＥ／ＯＰ$_{loc}$１０２が認証を実行したいと望んだ意図されたＲＰであることとを検証することができる。ＵＥ$_{Assert}$内の情報片ＲＰ$_{Cred}$は、ＲＰ１０４のＩＤをＵＥ１０２に示すためにＯＰＳＦ１０６によって生成されるいくらか明示的なステートメントＲＰ$_{Assert}$によって置換されることが可能である。ＵＥ$_{Assert}$は、署名キーＳを用いて署名された署名済みのＯｐｅｎＩＤアサーションメッセージであることが可能である。

【００２９】

図１はまた、ＲＰ１０４がＵＥ／ＯＰ$_{loc}$１０２に対して認証されること（たとえば、黙示的に認証されること）が可能であるということを示している。ＲＰ１０４は、そのＲＰ１０４が、ＲＰ$_{Cred}$によって識別された真正なＲＰである場合には、ＵＥ／ＯＰ$_{loc}$１０２のＯｐｅｎＩＤ認証を実行することができる（それ以降、署名キーＳを復号することが可能である）。ＲＰ１０４に対してＯＰＳＦ１０６によってプロトコルにおいて認証される一意のＵＥ／ＯＰ$_{loc}$１０２は、ＲＰ１０４を認証することができる。例示的な一実施形態においては、プロトコルフローは、ローカルＯｐｅｎＩＤ認証から修正されないことが可能である。また、ネットワーク認証は、影響を受けないままでいることが可能である。さらなる保護を確実にするために、プロトコルにおける１人または複数の当事者において、さらなる暗号オペレーションが実施されることが可能である。

【００３０】

ＧＢＡ（Ｇｅｎｅｒｉｃ Ｂｏｏｔｓｔｒａｐｐｉｎｇ Ａｒｃｈｉｔｅｃｔｕｒｅ）（たとえば、３ＧＰＰ ＧＢＡ）とローカルＯｐｅｎＩＤの相互作用のための可能な実施態様に関しては、ＵＥ／ＯＰ$_{loc}$１０２とＯＰＳＦ１０６との間における事前共有シークレットＫ$_0$が存在する場合には、プロトコルが実施されることが可能である。

【００３１】

図２は、認証フェーズ（ＡＰ：Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｈａｓｅ）の例示的なメッセージフロー図を示している。たとえば、認証フェーズは、ＵＥ／ＯＰ$_{loc}$２０２、ＲＰ２０４、ＯＰＳＦ２０６、および／またはＨＳＳ２０８を実装することができる。図２において示されているプロトコルフローは、ＵＥ／ＯＰ$_{loc}$１０２とＯＰＳＦ１０６との間における共有シークレットを使用して（たとえば、その共有シークレットが事前共有キーとして既に存在しているわけではない場合などに）、セキュアチャネルを確立するために、単独で、または図１に記載されているプロトコルプロビジョニングフェーズ（ＰＰ）とともに適用されることが可能である。

【００３２】

図２において示されているように、ＵＥ／ＯＰ$_{loc}$２０２は、２１０においてログイン識別子（たとえば、ｈｔｔｐアドレスまたはＥメールなどのＯＩＤ（ＯｐｅｎＩＤ ｉｄｅｎｔｉｆｉｅｒ））をＲＰ２０４へサブミットすることができる。２１２において、ＲＰ２０４は、アソシエーション要求（たとえば、ｈｔｔｐ ＰＯＳＴ ＯｐｅｎＩＤアソシエーション要求）をＯＰＳＦ２０６へ送信することができる。このアソシエーション要求は、ＲＰ２０４を識別するＲＰクレデンシャルＲＰ$_{Cred}$を含むことができる。２１４において、ＯＰＳＦ２０６は、共有キーＫ$_0$が決定またはプロビジョンされているかどうかを判定することができ、共有キーＫ$_0$が決定またはプロビジョンされていない場合には、プロトコルは、プロビジョニングフェーズにおいてＫ$_0$のプロビジョニングを進めることができる。Ｋ$_0$が既にプロビジョンされている場合には、プロトコルは、認証フェーズへ進むことができる。たとえば、２１６においてＯＰＳＦ２０６は、ＲＰ２０４に対応するＲＰ$_{Cred}$に基づいて、共有キーＫ$_{r,o}$を選択することができる。２１８において、ＯＰＳＦ２０６は、ＲＰ２０４とのアソシエーションを実行することができる。ＯＰＳＦ２０６は、アソシエーションハンドルＡおよび／または共有キーＫ$_1$を生成することができる。共有キーＫ$_1$は、たとえばアソシエーションハンドルＡ、ＲＰ$_{Cred}$、および／または共有キーＫ$_0$の関数から生成される、ＯＰＳＦ２０６、ＵＥ／ＯＰ$_{loc}$２０２、および／またはＲＰ２０４の間における共有キーであることが可能である。たとえば、ＵＥ／ＯＰ$_{loc}$２０２および／またはＯＰＳＦ２０６は、共有キーＫ$_1$を生成する

ように構成されることが可能である。ＲＰ２０４は、共有キー$K_1$を受信して、その共有キー$K_1$を、ＵＥ／$OP_{loc}$２０２とのセキュアな通信のために使用することができる。ＯＰＳＦ２０６は、アソシエーションハンドルＡと、暗号化された$K_1$とをＲＰ２０４へ送信することができ、$K_1$は、共有キー$K_{r,o}$によって暗号化されており、これは、たとえば$EK_{r,o}$（$K_1$）と呼ばれうる。ＲＰ２０４は、ｓｅｓｓｉｏｎＩＤ、ｒｅｔｕｒｎＵＲＬ、ノンス、ログイン識別子（たとえば、ＯＩＤ）、アソシエーションハンドルＡ、および／または$RP_{Cred}$などのパラメータを含むメッセージを２２０においてＵＥ／$OP_{loc}$２０２へ送信することができる。２２０におけるメッセージは、たとえばＵＥ／$OP_{loc}$２０２をＲＰ２０４へリダイレクトするリダイレクトメッセージであることが可能である。２２２において、ＵＥ／$OP_{loc}$２０２は、$K_1$を生成することができる。たとえば、$K_1$は、アソシエーションハンドルＡ、$RP_{Cred}$、および／または$K_0$の関数から生成されることが可能である。ＵＥ／$OP_{loc}$２０２は、２２２においてローカル認証を実行することができ、$RP_{Chv}$を含む認証アサーションメッセージ$UE_{Assert}$を生成することができ、および／または、２２２においてキー$K_1$を用いて$UE_{Assert}$を暗号化することができ、これは、たとえば$EK_1$（$UE_{Assert}$）と呼ばれうる。$UE_{Assert}$は、たとえばＯｐｅｎＩＤアサーションメッセージであることが可能である。ＵＥ／$OP_{loc}$２０２は、暗号化されたアサーションメッセージ$UE_{Assert}$をＲＰ２０４へ送信することができる。２２４において、ＵＥ／$OP_{loc}$２０２は、署名されたアサーションとともに要求（たとえば、ｈｔｔｐ ＧＥＴ要求）をＲＰ２０４へ送信することができる。ＲＰ２０４は、２２６において$K_{r,o}$を使用して、$K_1$を復号することができる。ＲＰ２０４は、復号された$K_1$を使用して、２２６において認証アサーションメッセージ$UE_{Assert}$を復号することができる。ＲＰ２０４は、共有キー$K_1$を使用して、ＯｐｅｎＩＤアサーションを検証することができる。２２８において、ＲＰ２０４は、認証アサーションメッセージ$UE_{Assert}$を含む通知をＵＥ／$OP_{loc}$２０２へ送信することができる。ＵＥ／$OP_{loc}$２０２は、２３０において認証アサーションメッセージ$UE_{Assert}$の妥当性を確認することができる。

【００３３】

２２８において受信された$UE_{Assert}$内の情報が、２２４において送信された$UE_{Assert}$内の情報と合致することを確認することによって、ＵＥ／$OP_{loc}$２０２は、２２８における受信されたメッセージが、$RP_{Cred}$によって識別されるＲＰ２０４（自分が２１０においてログイン情報をサブミットした先のＲＰ２０４）から生じたものであることを保証されることが可能である。たとえば、$RP_{Cred}$において申告されているＩＤをＲＰ１０４のＩＤと比較することによって、ＵＥ／$OP_{loc}$２０２は、認証情報を受信したＲＰがほかにないことと、ＲＰ１０４が、ＵＥ／$OP_{loc}$２０２が認証を実行したいと望んだ意図されたＲＰであることとを検証することができる。

【００３４】

認証の新しさは、$UE_{Assert}$内に新しいチャレンジ$RP_{Chv}$を含めることによって確かなものにされることが可能である。ＵＥ／$OP_{loc}$２０２は、受信された$UE_{Assert}$がこのチャレンジ値を含んでいることを検証することによって、その受信された$UE_{Assert}$の妥当性を確認することができ、ＲＰ２０４は、ＵＥ／$OP_{loc}$２０２とＲＰ２０４とによって共有されることが可能である本物の$K_1$を用いて$UE_{Assert}$を復号することができる場合に、そのチャレンジ値を知ることができる。本物の$K_1$を使用すれば、ＯＰＳＦ２０６と、$RP_{Cred}$によって識別されるＲＰとによって共有されている$K_{r,o}$をＲＰ２０４が所有していることを証明することができる。

【００３５】

例示的な一実施形態によれば、ＲＰ認証は、ローカルＯｐｅｎＩＤを伴わずに（たとえば、非ローカルＯｐｅｎＩＤを用いて）ＯＰを使用して実行されることが可能である。ＲＰ認証をＯｐｅｎＩＤプロトコル内に含めることは、ＯｐｅｎＩＤプロトコル自体に対する変更、ならびに／または、ＯＰおよび／もしくはＲＰの実施態様に対する変更を含むこ

とができる。ＲＰ認証は、たとえば偽のまたは不正なＲＰによって生じ得る攻撃に対する対抗手段を提供することなど、セキュリティー上の利点を付加することができる。ＯｐｅｎＩＤ（またはローカルＯｐｅｎＩＤ）に関するＵＥ上の実施態様は、そのようなあらゆるＲＰ認証によって影響を受けないことが可能である。たとえば、ＵＥは、ローカルＯＰ機能を組み込むことができず、一実施形態においては、チャレンジ$RP_{Chv}$をＲＰへ送信することができない場合がある。ＲＰ認証は、ＯＰとＲＰとの間におけるチャレンジ応答ステップを含むことができ、その場合には、ＯＰは、チャレンジを新しさの証明とともにＲＰへ（たとえば、暗号化されたノンスを介して）送信することができる。ＲＰは、事前に確立された共有シークレット$K_{r,o}$を使用して、このノンスを復号し、返信をＯＰへ返すことができる。代替として、または追加として、このノンスが暗号化されずに、その返信の中でＲＰによって署名されることも可能である。認証チャレンジに対する応答は、ＯＰ認証チャレンジに対する直接の応答として行うことができ、またはリダイレクトメッセージ内に統合されることも可能であり、たとえば、そのリダイレクトメッセージがＵＥをＯＰへ送ることができる。いずれのケースにおいても、ＯＰは、ＵＥ認証に従事する前にＲＰを認証する上で信頼できる証拠を有することができる。これは、失敗したＲＰ認証のケースにおいてプロトコルの停止を可能にすることができ、および／または、そのような失敗したＲＰ認証のケースにおいてＵＥとＯＰとの間における通信の労力を省くことができる。次いでＯＰは、失敗したＲＰ認証に関する情報をＵＥへ直接伝達することができる。

【００３６】

図３は、ＲＰ３０４を認証するためのメッセージのやり取りのうちの例示的な一部分のメッセージフロー図を示している。このメッセージフロー図は、ＵＥ３０２、ＲＰ３０４、およびＯＰ３０６の間における通信を含む。認証の失敗のケースにおいては、ＯＰ３０６は、ＵＥ３０２とのＨＴＴＰＳ（Ｈｙｐｅｒｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ　Ｓｅｃｕｒｅ）通信を強制すること、および／または失敗をＵＥ３０２に通知することが可能である。認証の成功のケースにおいては、ＯｐｅｎＩＤ認証は、先に進むことができる。

【００３７】

図３において示されているように、ＵＥ３０２は、３０８においてログイン識別子（たとえば、ＯＩＤ）をＲＰ３０４へサブミットすることができる。ＲＰ３０４は、アソシエーション要求（たとえば、ｈｔｔｐ　ＰＯＳＴ　ＯｐｅｎＩＤアソシエーション要求）を３１０においてＯＰ３０６へ送信することができる。３１０におけるアソシエーション要求は、$RP_{Cred}$を含むことができる。３１２において、ＯＰ３０６は、たとえば$RP_{Cred}$、またはＲＰ３０４の別の信頼されている識別子に基づいて、ＯＰ３０６とＲＰ３０４との間における共有シークレット$K_{r,o}$を選択することができる。ＯＰ３０６は、３１４においてＲＰ３０４とのアソシエーションを実行することができる。３１４において、ＯＰ３０６は、アソシエーションハンドルＡ、署名キーＳ、および／または$RP_{Chv}$を生成することができる。$RP_{Chv}$は、$K_{r,o}$を使用して暗号化されることが可能であり、これは、たとえば$EK_{r,o}(RP_{Chv})$と呼ばれうる。ＯＰ３０６は、アソシエーションハンドルＡ、署名キーＳ、および／または$EK_{r,o}(RP_{Chv})$をＲＰ３０４へ送信することができる。

【００３８】

ＲＰ３０４は、３１６において共有キー$K_{r,o}$を使用して$RP_{Chv}$を復号することができる。３１８において、ＲＰ３０４は、ＵＥ３０２を介してＯＰ３０６へメッセージを送信することができ、そのメッセージは、ｓｅｓｓｉｏｎＩＤ、ｒｅｔｕｒｎＵＲＬ、ノンス、ログイン識別子（たとえば、ＯＩＤ）、アソシエーションハンドルＡ、および／または$RP_{Chv}$などのパラメータを含むことができる。たとえば、３１８におけるメッセージは、リダイレクトメッセージを含むことができ、そのリダイレクトメッセージは、ＵＥ３０２をＯＰ３０６へリダイレクトすることができる。ＵＥ３０２は、３２０においてメッセージ（たとえば、ｈｔｔｐ　ＧＥＴ要求）をＯＰ３０６へ送信することができる

。３２０におけるメッセージは、ｓｅｓｓｉｏｎＩＤ、ｒｅｔｕｒｎＵＲＬ、ノンス、ログイン識別子（たとえば、ＯＩＤ）、アソシエーションハンドルＡ、および／またはＲＰ$_{Ｃｈｖ}$などのパラメータを含むことができる。３２２において、ＯＰ３０６は、ＲＰ$_{Ｃｈｖ}$を用いてＲＰ３０４のＩＤの妥当性を確認することができる。３２４においてＲＰ３０４のＩＤが妥当ではないと判定された場合には、ＯＰ３０６は、ＲＰ３０４が妥当ではない旨を示す通知を（たとえば、ＲＰ３０４が妥当ではない旨を示すＨＴＴＰＳ通知を介して）３２６においてＵＥ３０２へ送信することができる。ＲＰ３０４のＩＤが妥当である場合には、認証（たとえば、ＯｐｅｎＩＤ認証）は、３２８において続行することができ、および／またはＯＰ３０６は、ＲＰ３０４のＩＤが妥当である旨を示す通知（図示せず）を送信することができる。

【００３９】

別の実施形態において、ＲＰ３０４がＯＰ３０６とのセキュリティーアソシエーションを確立する場合には、対応するステップは、セキュリティーアソシエーションを確立するためのプロトコル内にＯＰ３０６からのチャレンジを組み込むように修正されることが可能である。アソシエーションの確立中に、ＯＰ３０６およびＲＰ３０４は、ＭＡＣ（ｍｅｓｓａｇｅ ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｃｏｄｅ）キーをセットアップすることができ、このＭＡＣキーは、認証アサーションメッセージＵＥ$_{Ａｓｓｅｒｔ}$に署名するために使用されることが可能である。このキーは、一時的なシークレットキーを使用して暗号化されて送信されることが可能であり、その一時的なシークレットキーは、ＯＰ３０６とＲＰ３０４との間において（たとえば、ＤＨ（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）手順を使用して）ネゴシエートされることが可能である。ＯＰ３０６は、その一時的なシークレットキーに加えて、ノンスをＲＰ３０４への応答内に含めることができる。このノンスは、たとえば、その一時的なシークレットキー（たとえば、ＤＨキー）を用いて暗号化されることが可能である。

【００４０】

ＲＰ３０４は、ネゴシエートされたキー（たとえば、ＤＨキー）に基づいてノンスおよび／またはＭＡＣキーを復号することができる。ＲＰ３０４は、ＯＰ３０６から受信されたノンスに暗号化または署名を行うために、自分自身の事前に確立されたＫ$_{ｒ，ｏ}$キーを使用することができる。ＲＰ３０４は、このキーをパラメータとして、たとえばＵＥ３０２へ送信されることが可能であるリダイレクトメッセージに付加することができる。ＵＥ３０２は、ＯＰ３０６へのリダイレクトに従うことができるため、ＯＰ３０６は、署名されたまたは暗号化されたノンスを受信することができ、共有キーＫ$_{ｒ，ｏ}$を使用してＲＰ３０４を認証することができる。失敗した認証のケースにおいては、ＯＰ３０６は、認証されていないＲＰからＵＥ３０２を保護するためのアラートメッセージをＵＥ３０２へ送信することができる。成功したＲＰ認証のケースにおいては、ＯＰ３０６は、プロトコルを進めることができる。

【００４１】

例示的な一実施形態においては、ＯＰ３０６は、ＯＰ３０６とＲＰ３０４との間においてアソシエーションが確立されていない場合（たとえば、ＯｐｅｎＩＤにおけるステートレスモード）においてＲＰ３０４へ情報を送信することを可能にすることができる。ステートレスモードにおいては、情報は、たとえばディスカバリー中などに、ＯＰ３０６とＲＰ３０４との間においてやり取りされることが可能である。しかし、ディスカバリーがＯＰ３０６を含むということが保証されない場合がある（たとえば、委任されたディスカバリーのケースにおいて。そのケースでは、ユーザ識別子は、たとえば、http://myblog.blog.comにある可能性があり、および／またはhttp://myblog.myopenid.comにおけるＯＰのＯｐｅｎＩＤ ＯＰエンドポイントＵＲＬ（ＯｐｅｎＩＤ ＯＰ ｅｎｄｐｏｉｎｔ ＵＲＬ）を指す可能性がある）。したがって、ｍｙｏｐｅｎｉｄ．ｃｏｍにおけるＯＰ３０６は、直接ディスカバリーに含まれない場合があり、このステージにおいてＲＰ３０４を認証することができない場合がある。

【００４２】

ＯＰ３０６は、ディスカバリーステップ中に情報をＲＰ３０４へ提供することができる場合（たとえば、ユーザ識別子ページが、ＯＰ３０６自体においてホストされることが可能である場合）には、ディスカバリー情報ページの一部としてノンスを動的に生成すること、および／またはそのノンスを、ＨＴＴＰ要求を行っているＲＰ３０４の識別子（たとえば、ＵＲＬまたはＥメールアドレス）に関連付けることが可能である。ＯＰ３０６は、ＲＰ３０４が、このノンスに署名または暗号化を行うこと、および／またはその情報をリダイレクトメッセージ内に含めることを予期することができる。

【００４３】

ＯＰ３０６は、ＨＴＴＰＳの使用を強制することができる。たとえば、ＵＥ３０２は、ＯＰ３０６によってＨＴＴＰＳの使用へとリダイレクトされることが可能であり、それによって、ＵＥ３０２とＯＰ３０６との間におけるその後のいかなる通信も、ＨＴＴＰＳを使用して保護されることが可能である。この特徴は、たとえば、OpenID Authentication 2.0などのＯｐｅｎＩＤ標準の実施形態によって明示的に可能にすることができる。そのような保護は、たとえばＯＰ３０６からＵＥ３０２へのＯｐｅｎＩＤ認証チャレンジメッセージ上でのＭｉｔＭ（ｍａｎ－ｉｎ－ｔｈｅ－ｍｉｄｄｌｅ）攻撃の防止を可能にすることができる。そのような保護は、アラートメッセージが、失敗したＲＰ認証のケースにおいてＵＥ３０２へ保護された様式で送信されることを可能にすることができる。

【００４４】

ここでは、分割された端末の実施態様に関する例示的な実施形態が説明される。分割された端末の実施態様とは、２つのエンティティーがネットワークのユーザ側に存在することが可能であるシナリオを指すことができる。たとえば、ＡＡ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ａｇｅｎｔ）およびＢＡ（Ｂｒｏｗｓｉｎｇ Ａｇｅｎｔ）は、たとえばＵＥ３０２などのＵＥに関連付けられること、および／またはそうしたＵＥ上に存在することが可能である。ＡＡは、認証のためのステップを実行することができ、その一方でＢＡは、サービスの視聴者または消費エンティティーであることが可能である。分割された端末の実施態様の一例においては、ユーザは、たとえばＲＰ３０４などのＲＰから何らかのサービス（たとえば、ウェブサイト）を検索するためにブラウザを開くことができる。ＲＰ３０４は、ＯＰ３０６およびユーザのＡＡを用いていくつかのステップ（たとえば、アソシエーションおよび／またはディスカバリー）を実行することができる。たとえば、ＵＥ３０２は、ＯＰ３０６によってコンタクトされることが可能である。ＯＰ３０６およびＵＥ３０２は、たとえばＧＢＡネットワーククレデンシャルに基づいて、認証を実行することができ、それらのＧＢＡネットワーククレデンシャルは、ＢＡに知られていない可能性がある。ＢＡは、たとえばＯＰ３０６とＡＡとの間における認証が成功した場合などに、ＲＰ３０４におけるサービスへのアクセスを得ることができる。実施されることが可能である複数の変形形態が存在することができる。それぞれの変形形態は、ＡＡとＢＡとの間における物理チャネルを含むことができ、その物理チャネルは、たとえばローカルインターフェース（たとえば、ＢＬＵＥＴＯＯＴＨ（登録商標）など）または論理チャネルであることが可能である。そのロジックチャネルは、ＡＡ上に示されている情報をユーザがＢＡに入力することによって作成されることが可能であり、それによって２つのセッションは、たとえば論理的に結合されることが可能である。

【００４５】

ＭＮＯ（Ｍｏｂｉｌｅ Ｎｅｔｗｏｒｋ Ｏｐｅｒａｔｏｒ）自身のサービス、および／またはサードパーティーサービスプロバイダのサービスが、ＵＥ３０２へ、またはＭＮＯに知られていないデバイスへ提供されることが可能である。ユーザが別々の／複数のデバイスを単独のオーセンティケータ（たとえば、ＵＥ３０２）と接続できるようにしたいとＭＮＯが望む場合には、分割された端末の実施態様が使用されることが可能である。

【００４６】

分割された端末の実施態様に関する例示的なオプションは、２つのセッションの間における暗号バインディングが作成されるオプションを含むことができる。複数の実施態様は、ＡＡがクレデンシャル情報をユーザに表示し、そのクレデンシャル情報をユーザがＢＡ

に入力して、（たとえば、本明細書に記載されている論理チャネルを使用して）ＲＰ３０４に対する認証を行うことができるシナリオを含むこともできる。

【００４７】

代替として、または追加として、クレデンシャルは、ＢＡとＡＡとの間におけるセキュアにされたローカルリンクを介して（たとえば、本明細書に記載されている物理チャネルを使用して）送信されることが可能である。この実施態様においては、ＡＡは、認証トークン／パスワードジェネレータとして使用されることが可能である。例示的な一実施形態においては、ＢＡは、共有キー$K_1$および認証アサーションメッセージ$UE_{Assert}$（これらは、$K_{r,o}$によって暗号化されることが可能であり、たとえば$EK_{r,o}$（$K_1$，$UE_{Assert}$）と呼ばれうる）をＡＡから受信して、ＲＰ３０４へ送信することができる。この情報は、ユーザを認証するためにＲＰ３０４によって使用されることが可能である。例示的な一実施形態においては、分割された端末の実施態様は、ローカルアサーションプロバイダを用いてセットアップされることが可能であり、ローカルアサーションプロバイダは、ＵＥ３０２／ＡＡの内部で認証アサーションメッセージ$UE_{Assert}$を生成する。

【００４８】

ローカルＯｐｅｎＩＤに基づく認証に応じて、さらなるセキュリティー機能が実施されることが可能である。認証は、プライベートシークレット（たとえば、図４の４１０および４１４において示されている暗号化キーＥ）を提供するためにローカルＯｐｅｎＩＤに基づくことが可能である。このシークレットは、たとえば、$OP_{loc}$、および／または、その$OP_{loc}$が存在している信頼されている環境（たとえば、スマートカード、もしくはその他の信頼されているコンピューティング環境）と、ＲＰとの間においてプライベートなセキュアチャネルを確立するために使用されることが可能である。あるいは、そのセキュアチャネルは、ＵＥの何らかの相対的にセキュアでない部分においてエンドポイントを有することができ、これは、ＵＥプラットフォームと呼ばれうる。

【００４９】

ここで説明されるのは、そのようなセキュアチャネルをローカルＯｐｅｎＩＤ認証にバインドするオプションである。例示的な一実施形態においては、ＵＥプラットフォームとの間でセキュアチャネルが確立されることが可能であり、このセキュアチャネル内でＲＰおよびローカルＯｐｅｎＩＤの認証が実行されることが可能である。この例示的な実施形態は、いくつかの実施態様にとっては十分であるかもしれないが、その他の実施態様のセキュリティー需要を満たさない場合がある。たとえば、セキュアチャネルを確立するＵＥプラットフォームは、$OP_{loc}$が存在している信頼されている環境（たとえば、スマートカード、またはその他の信頼されているコンピューティング環境）よりもセキュアでない場合がある。同じ信頼されている環境から来てＲＰへと導かれるプライベートデータは、ＵＥ内の相対的にセキュアでないインナーノードを有するチャネル上を進む場合がある。したがって、ある代替実施形態が実施されることが可能であり、この代替実施形態は、$OP_{loc}$、および／または、その$OP_{loc}$が存在している信頼されているコンピューティング環境が、ＵＥプラットフォームのプロパティーに左右されずにＲＰとの間でシークレットをやり取りすること、および、メッセージのそのようなプライバシープロパティーをＲＰに対するローカルＯｐｅｎＩＤ認証にバインドすることを可能にすることができる。

【００５０】

図４は、たとえば$UE／OP_{loc}$４０２などのローカル認証エンティティーと、ＲＰ４０４との間においてセキュアチャネルを作成および／または実施する例示的な一実施形態のメッセージフロー図を示している。図４において示されている流れ図は、$UE／OP_{loc}$４０２、ＲＰ４０４、および／またはＯＰＳＦ４０６の間における通信を含む。４０８において示されているように、$UE／OP_{loc}$４０２が、署名された認証アサーションを４１０において生成する時点まで、ローカルＯｐｅｎＩＤ認証が実行されることが可能である。４１０において、$UE／OP_{loc}$４０２は、署名キーＳを生成することが

でき、この署名キーＳは、ＫＤＦ（ｋｅｙ　ｄｅｒｉｖａｔｉｏｎ　ｆｕｎｃｔｉｏｎ）を使用してアソシエーションハンドルＡおよび共有キー$K_0$の関数から導出されることが可能である。共有キー$K_0$は、セキュアな通信のためにＵＥ／$OP_{loc}$４０２とＯＰＳＦ４０６との間において共有されることが可能である。署名キーＳは、たとえばＯｐｅｎＩＤ署名キーであることが可能である。ＵＥ／$OP_{loc}$４０２は、ローカル認証を実行することができ、認証アサーションメッセージ$UE_{Assert}$が、４１０において生成されることが可能であり、この認証アサーションメッセージ$UE_{Assert}$は、暗号化されたシード値（Ｓｅｅｄ）を含むことができる。Ｓｅｅｄは、複数の当事者の間において共有シークレットを隠すために使用されることが可能である。たとえば、共有シークレットが当事者どうしの間において送信されることはあり得ないため、共有シークレットは隠されることが可能である。代わりに、共有シークレットを、そのシークレットが共有されている当事者のうちのそれぞれにおいて（たとえば、ローカルに）導出するために、Ｓｅｅｄが転送されて使用されることが可能である。

【００５１】

認証アサーションメッセージ$UE_{Assert}$は、たとえばＯｐｅｎＩＤアサーションであることが可能である。ＵＥ／$OP_{loc}$４０２は、署名キーＳを用いてＳｅｅｄを暗号化することができ（$E_S$（Ｓｅｅｄ）と呼ばれる）、それは、ＯＰＳＦ４０６、ＵＥ／$OP_{loc}$４０２、および／またはＲＰ４０４にとってプライベートであることが可能である。ある代替実施形態においては、ＵＥ／$OP_{loc}$４０２は、所定の方法でＳから導出されたキーを使用してＳｅｅｄを暗号化することができる。ＵＥ／$OP_{loc}$４０２は、所定の方法でＳｅｅｄから暗号化キーＥを生成することができ、その暗号化キーＥは、たとえばＲＰ４０４に知られていることが可能である。ＵＥ／$OP_{loc}$４０２は、署名キーＳを用いて認証アサーションメッセージ$UE_{Assert}$に署名することができる。ローカル認証から暗号化キーＥをこのように生成することによって、ＵＥ／$OP_{loc}$４０２とＲＰ４０４との間におけるセキュアチャネルの確立をこのローカル認証にバインドすることができる。

【００５２】

４１２において、ＵＥ／$OP_{loc}$４０２は、署名されたアサーション$UE_{Assert}$とともにメッセージ（たとえば、ｈｔｔｐ　ＧＥＴ要求）をＲＰ４０４へ送信することができる。ＲＰ４０４は、４１４において、認証アサーションメッセージ$UE_{Assert}$を検証し、署名キーＳを使用してＳｅｅｄ情報を復号することができる。ＲＰ４０４は、Ｓｅｅｄ情報に基づいて暗号化キーＥを生成することができる。たとえば、ＲＰ４０４は、所定の方法でＳｅｅｄ情報から暗号化キーＥを生成することができ、その暗号化キーＥは、ＵＥ／$OP_{loc}$４０２に知られていることが可能である。暗号化キーＥは、ＵＥ／$OP_{loc}$４０２およびＲＰ４０４にとってプライベートであることが可能である。

【００５３】

ＲＰ４０４は、前もって検証された認証アサーション$UE_{Assert}$を、暗号化キーＥを用いて暗号化し、ＵＥ／$OP_{loc}$４０２へ返信することができる。たとえば、４１６において、ＲＰ４０４は、認証アサーションメッセージ$UE_{Assert}$を含む通知をＵＥ／$OP_{loc}$４０２へ送信することができ、その認証アサーションメッセージ$UE_{Assert}$は、たとえば暗号化キーＥを用いて暗号化されることが可能である（$E_E$（$UE_{Assert}$））。これは、シークレットが確立された旨の確認をＵＥ／$OP_{loc}$４０２に提供することができる。ＵＥ／$OP_{loc}$４０２は、４１８において、暗号化キーＥを使用して認証アサーションメッセージ$UE_{Assert}$を復号することによって、認証アサーションメッセージ$UE_{Assert}$の妥当性を確認することができる。４１６において受信された$UE_{Assert}$内の情報が、４１２において送信された情報$UE_{Assert}$と合致することを確認することによって、ＵＥ／$OP_{loc}$４０２は、４１６における受信されたメッセージが、意図されたＲＰ４０４から生じたものであることを保証されることが可能である。たとえば、４１６においてＲＰ４０４から受信された通知内のＳｅｅｄを、４１０において$UE_{Assert}$内に含められたＳｅｅｄと比較することに

よって、ＵＥ／ＯＰ$_{loc}$４０２は、認証情報を受信したＲＰがほかにないことと、ＲＰ４０４が、ＵＥ／ＯＰ$_{loc}$４０２が認証を実行したいと望んだ意図されたＲＰであることとを検証することができる。ＵＥ／ＯＰ$_{loc}$４０２は、４１８におけるこの検証を、ＲＰ４０４がＳｅｅｄを復号してＥを導出する際に使用することができるキーＳをＲＰ４０４が得た旨の表示として、信頼することができる。４２０においては、ＵＥ／ＯＰ$_{loc}$４０２とＲＰ４０４との間においてセキュアチャネルを確立するために、暗号化キーＥが（たとえば、別のプロトコルにおいて）使用されることが可能である。このセキュアチャネルを確立するために使用されることが可能である１つの例示的なプロトコルとしては、ＴＬＳ－ＰＳＫプロトコルを含むことができ、このＴＬＳ－ＰＳＫプロトコルは、入力として事前共有キーを受け入れてその事前共有キーに基づいてセキュアチャネルを実現する一般的なＴＬＳプロトコルの変形形態であると言える。ＴＬＳ－ＰＳＫの例示的な一実施形態は、ＩＥＴＦ（Ｉｎｔｅｒｎｅｔ Ｅｎｇｉｎｅｅｒｉｎｇ Ｔａｓｋ Ｆｏｒｃｅ）によって、Request for Comments (RFC) document 4279およびRequest for Comments (RFC) document 4785において示されている。

【００５４】

図４において示されているように、暗号化キーＥの導出は、ＳｅｅｄおよびＫＤＦ（公開されている場合がある）の知識を使用して実行されることが可能である。Ｓｅｅｄは、ＲＰ４０４に知られていることが可能であり、署名キーＳを用いて暗号化されるため、他者から保護されることが可能である。Ｓは、たとえば証明書ベースのＴＬＳ（ｔｒａｎｓｐｏｒｔ ｌａｙｅｒ ｓｅｃｕｒｉｔｙ）などのセキュアチャネルを介して、ＯＰＳＦ４０６によって、ＲＰ４０４に対して明らかにされることが可能である。ＵＥ４０２は、ＲＰ４０４が署名キーＳを所有している旨の確認を得ることができる。なぜなら、ＲＰ４０４は、Ｅ$_{E}$（ＵＥ$_{Assert}$）をＵＥ４０２に返信することができ、これは、ＲＰ４０４がＳｅｅｄを復号することができる場合に実施可能になることができるためである。したがって、ＵＥ４０２は、ＲＰ４０４からキーの確認を得ることができる。図４において示されているプロトコルフローは、セキュアな通信を可能にするために、本明細書に記載されているＲＰ認証プロトコルなどのＲＰ認証プロトコルと組み合わされることが可能である。

【００５５】

エンティティーどうしの間におけるプライベートな共有キーを導出するためにＳｅｅｄ情報が使用されることが可能であるということが示されているが、プライベートな共有キーは、その他の方法で導出されることも可能である。たとえば、複数の実施形態は、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎキーの確立を実施することができる。

【００５６】

本明細書に記載されているように、たとえばＳｅｅｄなどの何らかの初期値が、共有シークレットを確立したいと望むエンティティーどうしの間において転送されることが可能である。Ｓｅｅｄをｍａｎ－ｉｎ－ｔｈｅ－ｍｉｄｄｌｅ攻撃から保護するために、Ｓｅｅｄの暗号化が使用されることが可能である。ローカルＯｐｅｎＩＤ認証へのバインディングのために、署名キーＳ、またはＳから導出されたキーを用いた特定の暗号化が使用されることが可能である。ローカルＯｐｅｎＩＤ認証へバインドするために、暗号化された通知メッセージが使用されることが可能である。これは、ＵＥ／ＯＰ$_{loc}$４０２に対してシークレットの確立について確認する機能を付加することができる。

【００５７】

シークレットの確立は、ＲＰ４０４が、暗号化されたＳｅｅｄをリダイレクトメッセージ内に含めてＵＥ／ＯＰ$_{loc}$４０２へ送信することによって、ローカルＯｐｅｎＩＤプロトコルフロー内のより早い段階で開始することができる。

【００５８】

別の実施形態においては、ＲＰ４０４は、所望のセキュアチャネルのエンドポイントへのパス上の中間ノードであることが可能である。このケースにおいては、ＲＰ４０４は、このエンドポイントからＳｅｅｄを受信することができ、このエンドポイントは、ＵＥ／

$OP_{loc}$４０２がセキュアチャネルを確立したいと望む場合がある相手のサーバであることが可能であり、これに対して、ＲＰ４０４は、認証ゲートウェイとして、および任意選択で許可ゲートウェイとして機能することができる。ＵＥ／$OP_{loc}$４０２またはＵＥプラットフォームと、ＲＰ４０４との間においてセキュアチャネルを確立するために、暗号化キーＥが別のプロトコルにおいて使用されることが可能である。暗号化キーＥをそのような様式で使用するための候補プロトコルとしては、ＴＬＳ－ＰＳＫプロトコルを含むことができ、このＴＬＳ－ＰＳＫプロトコルは、入力として事前共有キーを受け入れてその事前共有キーに基づいてセキュアチャネルを実現するＴＬＳプロトコルの変形形態であると言える。いくつかの実施形態においては、シークレットの確立は、ＲＰ認証と組み合わされることが可能である。

【００５９】

図５は、ポスト認証キー確認（ｐｏｓｔ－ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｋｅｙ ｃｏｎｆｉｒｍａｔｉｏｎ）を伴うＵＥ／ＲＰ間の事前に確立されたセキュアチャネル（ＵＥ－ＲＰ ｐｒｅ－ｅｓｔａｂｌｉｓｈｅｄ ｓｅｃｕｒｅ ｃｈａｎｎｅｌ）を使用するローカルＯｐｅｎＩＤ認証のためのセキュアチャネルの確立を示す流れ図である。たとえば、セキュアチャネルの確立は、ＵＥ／$OP_{loc}$５０２またはＵＥプラットフォームと、ＲＰ５０４とが、セキュアチャネルを確立すること、およびローカルＯｐｅｎＩＤ認証を進めることを可能にすることができる。図５において示されている流れ図は、認証中にＲＰ５０４に対してセキュアチャネルキーを確認するために使用されることが可能であり、たとえば認証にバインドされることが可能である。これは、たとえばＴＬＳ（ｔｒａｎｓｐｏｒｔ－ｌａｙｅｒ ｓｅｃｕｒｉｔｙ）トンネルなどのセキュアチャネルからキーマテリアルＸＳを抽出すること、および／またはそこからバインディング応答$B_{res}$を導出することによって行われることが可能である。

【００６０】

図５において示されているように、ＵＥ／$OP_{loc}$５０２およびＲＰ５０４は、５０８においてセキュアチャネルを確立することができる。たとえば、このセキュアチャネルは、ＴＬＳを使用して確立されることが可能である。５１０において、ＵＥ／$OP_{loc}$５０２は、ログイン識別子（たとえば、ＯＩＤ）をＲＰ５０４へサブミットすることができる。ＲＰ５０４は、アソシエーション要求（たとえば、ｈｔｔｐ ＰＯＳＴ ＯｐｅｎＩＤアソシエーション要求）を５１２においてＯＰＳＦ５０６へ送信することができる。ＯＰＳＦ５０６は、５１４においてＲＰ５０４とのアソシエーションを実行することができる。たとえば、ＯＰＳＦ５０６は、アソシエーションハンドルＡおよび／または共有キー$K_1$を生成することができる。共有キー$K_1$は、ＯＰＳＦ５０６、ＲＰ５０４、および／またはＵＥ／$OP_{loc}$５０２の間における共有キーであることが可能である。共有キー$K_1$は、アソシエーションハンドルＡおよび／または共有キー$K_0$から導出されることが可能である。ＯＰＳＦ５０６は、アソシエーションハンドルＡおよび／または共有キー$K_1$をＲＰ５０４へ送信することができる。

【００６１】

５１６において、ＲＰ５０４は、リダイレクトメッセージをＵＥ／$OP_{loc}$５０２へ送信することができ、このリダイレクトメッセージは、ＵＥ／$OP_{loc}$５０２をＯＰへリダイレクトし、ＵＥ／$OP_{loc}$５０２上にローカルに駐在する。このリダイレクトメッセージは、ｓｅｓｓｉｏｎＩＤ、ｒｅｔｕｒｎＵＲＬ、ノンス、ログイン識別子（たとえば、ＯＩＤ）、および／またはアソシエーションハンドルＡなどのパラメータを含むことができる。５１８において、ＵＥ／$OP_{loc}$５０２は、ローカル認証を実行することができ、共有キー$K_1$を生成することができる。共有キー$K_1$は、アソシエーションハンドルＡおよび／または共有キー$K_0$から生成されることが可能である。ローカル認証から共有シークレット$K_1$をこのように生成することによって、ＵＥ／$OP_{loc}$５０２とＲＰ５０６との間におけるセキュアチャネル５０８の確立をこのローカル認証にバインドすることができる。ＵＥ／$OP_{loc}$５０２は、セキュアチャネルからキーマテリアルＸＳを抽出することができ、ＸＳからバインディング応答$B_{res}$を生成することができる（

$B_{res}$＝ｇ（ＸＳ））。例示的な一実施形態によれば、バインディング応答$B_{res}$の導出は、たとえばアソシエーションハンドルＡなどのさらなるノンスを伴うＭＡＣアルゴリズムを使用することによって行われることが可能である。ＵＥ／$OP_{loc}$５０２は、バインディング応答$B_{res}$を認証アサーションメッセージ$UE_{Assert}$に含めることができる。$B_{res}$は、たとえばＯｐｅｎＩＤによる許可に応じて、認証アサーションメッセージ$UE_{Assert}$の拡張フィールド内に含まれることが可能である。認証アサーションメッセージ$UE_{Assert}$は、共有キー$K_1$を使用してＵＥ／$OP_{loc}$５０２によって署名されることが可能であり、たとえば$SigK_1$（$UE_{Assert}$）と呼ばれうる。５２０において、ＵＥ／$OP_{loc}$５０２は、署名されたアサーションメッセージ$SigK_1$（$UE_{Assert}$）をＲＰ５０４へ送信することができる。たとえば、署名されたアサーションメッセージは、ｈｔｔｐ　ＧＥＴ要求内に含めて送信されることが可能である。例示的な一実施形態においては、ＸＳがＲＰ５０４へのメッセージ内で直接使用されてはならない。なぜなら、これによって、セキュアチャネルに関する情報が攻撃者に漏洩する可能性があるためである。

【００６２】

ＲＰ５０４は、署名されたアサーション$SigK_1$（$UE_{Assert}$）を５２２において共有キー$K_1$を使用して検証することができる。たとえばＵＥ／$OP_{loc}$５０２からの認証アサーションの検証が成功した後に、ＲＰ５０４は、ＲＰ５０４自身のセキュアチャネルキーマテリアルＸＳ＊から比較値$B_{res}$＊を導出すること、およびその比較値$B_{res}$＊が、受信された$B_{res}$と一致することに気づくことが可能である。たとえば、ＲＰ５０４は、セキュアチャネルからキーマテリアルＸＳ＊を抽出することができ、そのキーマテリアルＸＳ＊からバインディング応答$B_{res}$＊を生成することができ（$B_{res}$＊＝ｇ（ＸＳ＊））、バインディング応答$B_{res}$＊が、署名されたアサーション内に示されているバインディング応答$B_{res}$に等しいことを検証することができる。ＲＰ５０４は、認証された当事者がセキュアチャネルエンドポイントであることを知ることができる。なぜなら、その当事者は、認証プロトコルが実行されたチャネルに関する正しいセキュアチャネルキーを所有しているためであり、その認証プロトコルは、セキュアチャネルキーのキー確認として使用されることが可能である。バインディング応答$B_{res}$＊がバインディング応答$B_{res}$に等しいことをＲＰ５０４が検証した場合には、認証は成功したと判定されることが可能であり、ＵＥ／$OP_{loc}$５０２とＲＰ５０４との間におけるチャネルはセキュアであると言える。５２４において、ＲＰ５０４は、認証が成功したこと、およびそのチャネルがセキュアであることを示す通知をＵＥ／$OP_{loc}$５０２へ送信することができる。

【００６３】

図５において示されているように、セキュアチャネルは、ＴＬＳを使用して確立されることが可能である。ＵＥ／$OP_{loc}$５０２およびＲＰ５０４は、（たとえば、ＯｐｅｎＩＤ認証によって）認証された当事者が、前もって確立されたセキュアチャネルのエンドポイントでもあると言えることをＲＰ５０４に保証することができるキー確認をプロトコル内に含めることができる。図５において示されている例示的な実施形態は、キー確認、およびセキュアチャネルの確立、ならびに認証のための信頼アンカーとしての$OP_{loc}$の使用を含むことができる。$OP_{loc}$の使用を伴わずに（たとえば、外部のＯＰを使用して）同じまたは同様のセキュリティーを達成しようと試みる実施形態は、ＲＰ５０４とネットワークＯＰとの間におけるさらなる通信ステップを招く場合がある。図５において示されている例示的な実施形態は、ＭｉｔＭ（ｍａｎ－ｉｎ－ｔｈｅ－ｍｉｄｄｌｅ）攻撃（ＭｉｔＭが自分自身を、はじめにセキュアな（ＴＬＳ）チャネルのセットアップ時に、たとえばＴＬＳリレーとして確立する攻撃など）を軽減することができる。本明細書に記載されている実施形態は、ＭｉｔＭをＲＰ５０４によって明示的に検知できるようにすることができる。

【００６４】

認証アサーションの拡張フィールドを使用することが所望されていない場合には、キー

確認のためにＸＳが使用されることが可能である。たとえば、ＵＥ／ＯＰ$_{loc}$５０２は、署名キー

【００６５】

【数１】

$$K_1' = g(K_1, XS)$$

【００６６】

（図示せず）を導出することができ、認証アサーションに署名するためにその署名キーを使用する。ＲＰ５０４は、署名されたアサーションを検証するために同じことを行うことができる。成功すれば、ＲＰ５０４は、セキュアチャネルのための認証およびキー確認を同時に達成することができる。これは、セマンティクスの低下と引き換えに実現することができる。なぜなら、ＭｉｔＭの存在がもはや認証の失敗から認識できなくなる可能性があるためである。

【００６７】

図５において示されている実施形態は、たとえば本明細書に記載されているＲＰ認証の実施形態などのＲＰ認証と組み合わされることが可能である。たとえば、チャネルセキュリティーの保証は、図５のプロトコルにおいて示されているように一面だけのものになる場合がある。それを両面からのものにするために、プロトコルは、たとえば図２および図３において示されているＲＰ認証プロトコルなどのＲＰ認証プロトコルと組み合わされることが可能である。このために、ＵＥ／ＯＰ$_{loc}$５０２は、暗号化されたチャレンジ値ＥＫ$_1$（ＲＰ$_{Chv}$）を認証アサーションメッセージ内に含めることができる。Ｋ$_1$がＭｉｔＭに決して洩らされないならば、ＵＥ／ＯＰ$_{loc}$５０２は、ＲＰチャレンジ値ＲＰ$_{Chv}$を含む通知を受信すると、妥当なＲＰ５０４がＢ$_{res}$の評価を成功裏に実行したこと、ひいてはＭｉｔＭが存在する可能性はないことを想定することができる。したがって、ＲＰ５０４は、正しいＫ$_1$を所有している場合には、ＲＰ$_{Chv}$を復号することができる。

【００６８】

別の実施形態においては、ＲＰ５０４は、バインディング応答Ｂ$_{res}$の知識を有することができる。たとえば、Ｂ$_{res}$は、５２４においてＵＥ／ＯＰ$_{loc}$５０２に返信される通知内のＲＰチャレンジ値ＲＰ$_{Chv}$を暗号化するために使用されることが可能である。ＵＥ／ＯＰ$_{loc}$５０２は、認証アサーションメッセージＵＥ$_{Assert}$内のＲＰ$_{Chv}$を暗号化するために、たとえばＫ$_0$またはＫ$_1$よりも、

【００６９】

【数２】

$$K_1'$$

【００７０】

を使用することができる。次いでＲＰ５０４は、正しいＸＳ値から導出された

【００７１】

【数３】

$$K_1'$$

【００７２】

を所有している場合には、ＲＰ$_{Chv}$を抽出することができる。

【００７３】

本明細書に記載されている認証およびキー合意プロトコルは、攻撃、たとえばＭｉｔＭ攻撃のような攻撃からの保護のためのさまざまな実施態様を含むことができる。そのような保護を提供するための１つの方法は、認証フローの前に、たとえばＴＬＳトンネルなどのセキュアチャネル（外部チャネルと呼ばれる場合がある）を確立することである。認証は、このセキュアチャネル内で実行されることが可能である。たとえば、ＧＢＡ＿Ｈと呼ばれるプロトコルは、ＴＬＳトンネルによって確立された外部認証プロトコルに関する攻撃に対抗する上で十分にセキュアであることが可能である。ＧＢＡ＿Ｈは、たとえばＴＬＳを介したＨＴＴＰダイジェストに基づく認証手順を含むことができる。ＧＢＡ＿Ｈの例示的な一実施形態は、3rd Generation Partnership Project (3GPP) Technical Specification (TS) number 33.220において示されている。

【００７４】

図６は、ＨＴＴＰ－ＳＩＰダイジェストを使用するＧＢＡ＿Ｈプロトコルの一例を示すメッセージフロー図を示している。図６において示されているように、ＵＥ６０２、ＢＳＦ６０４、および／またはＨＳＳ６０６を使用して通信が実行されることが可能である。６０８において、ＵＥ６０２は、ＢＳＦ６０４とのＴＬＳトンネルを確立することができる。ＵＥ６０２は、６１０において、たとえばＴＬＳトンネルを使用して、要求をＢＳＦ６０４へ送信することができる。６１０における要求は、６１２において示されているように、プライベートＩＤを含む許可ヘッダを含むことができる。ＢＳＦ６０４およびＨＳＳ６０６は、認証情報をやり取りするために、６１４におけるＺｈリファレンスポイントを使用することができる。たとえば、６１６において示されているように、ＢＳＦ６０４は、ＨＳＳ６０６からＡＶ（ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｖｅｃｔｏｒ）および／またはユーザプロファイル情報を検索するために、Ｚｈリファレンスポイントを使用することができる。

【００７５】

６１８において、ＢＳＦ６０４は、認証チャレンジを（たとえば、認証チャレンジをＨＴＴＰ４０１無許可応答内に含めて）ＵＥ６０２へ送信することができる。６２０において示されているように、６１８におけるメッセージは、プライベートＩＤ情報、レルム（ｒｅａｌｍ）、ノンス、ｑｏｐ（ｑｕａｌｉｔｙ　ｏｆ　ｐｒｏｔｅｃｔｉｏｎ）値、認証アルゴリズム、ドメイン、および／またはオパーク（ｏｐａｑｕｅ）を含むことができる。例示的な一実施形態においては、この情報は、メッセージの認証ヘッダ内に含まれることが可能である。プライベートＩＤ情報は、ネットワークがユーザを識別するために使用するＩＤを含むことができる。このプライベートＩＤは、ネットワークが、チャレンジのためにユーザプロファイルおよび／または認証ベクトルを検索することを可能にすることができる。例示的な一実施形態においては、レルム、ノンス、ｑｏｐ値、認証アルゴリズム、ドメイン、および／またはオパークは、ＩＥＴＦによって、RFC document 2617において示されていると言える。６２２において、ＵＥ６０２は、認証応答を計算することができる。ＵＥは、６２４において認証要求をＢＳＦ６０４へ送信することができる。６２６において示されているように、認証要求は、プライベートＩＤ情報、レルム、ノンス、ｃノンス（ｃｎｏｎｃｅ）、ｑｏｐ値、ノンスカウント、認証アルゴリズム、ダイジェストＵＲＩ、およびオパークを含むことができる。例示的な一実施形態においては、ｃノンス、ノンスカウント、および／またはダイジェストＵＲＩは、ＩＥＴＦによって、RFC document 2617において示されていると言える。６２８において、ＢＳＦ６０４は、応答を計算すること、およびＵＥ６０２から受信された値を、ＢＳＦ６０４における計算された値と比較することが可能である。６３０において、ＢＳＦ６０４は、認証が成功したことをＵＥ６０２に対して確認するメッセージ（たとえば、２００　ＯＫメッセージ）をＵＥ６０２へ送信することができる。６３０におけるメッセージは、６３２において示されているように、Ｂ＿ＴＩＤ（ｂｉｎｄｉｎｇ　ｔｒｕｓｔｅｄ　ｉｄｅｎｔｉｆｉｅｒ）および／またはキーＫｓの有効期間を含むことができる。例示的な一実施形態においては、Ｂ＿ＴＩＤおよびＫｓの有効期間は、3GPP TS number 33.220において示されていると言える。６３４において、ＵＥ６０２およびＢＳＦ６０４は、Ｋｓ＿ＮＡＦを計算するこ

とができる。

【００７６】

別の例示的な実施形態は、ＴＬＳ外部認証と、本明細書に記載されているＧＢＡメカニズムによって確立される認証との間におけるバインディングを含むことができる。提案されるバインディングソリューションは、たとえば、ＵＥ６０２がバインディング応答$B_{res}$を６２４におけるメッセージに付加することによって編成されることが可能である。$B_{res}$は、ＢＳＦ６０４およびＵＥ６０２には知られているがＭｉｔＭには知られていない方法でセキュアチャネルに依存することができる。$B_{res}$は、内部認証（たとえば、ＡＫＡ）応答と同様の（または、まったく同じ）方法でセキュアチャネルメッセージから導出されることが可能であるが、その応答には左右されないことが可能である。たとえば、$B_{res}$は、一般的な公に知られている方法で応答から導出されることは不可能であり、さもなければ、ＭｉｔＭが同様の方法で$B_{res}$を導出することができるおそれがある。ＭｉｔＭが存在する場合には、ＢＳＦ６０４は、セキュアチャネルＵＥ６０２－ＭｉｔＭのパラメータとは異なるセキュアチャネルＢＳＦ６０４－ＭｉｔＭからのパラメータを使用して、$B_{res}$の検証を実行することができる。このための前提条件は、ＢＳＦ６０４およびＵＥ６０２が両方とも自分自身の選択したパラメータ（たとえば、ノンス）をチャネルの確立において導入することを可能にすることができるプロトコル（たとえばＴＬＳなど）によって満たされることが可能であるセキュアチャネルの一意性を含むことができる。$B_{res}$の検証および／または再計算は、ＭｉｔＭによって実行された場合には、失敗に終わることが可能である。なぜなら、ＭｉｔＭは、許容可能な$B_{res}$の値をどのようにして導出するかを知ることができないためであり、その一方で、ＭｉｔＭによるＧＢＡ応答の再計算は、成功することができる。このようにして、ＭｉｔＭは検知されることが可能である。

【００７７】

例示的な一実施形態においては、ＵＥ６０２は、ＴＬＳ暗号化キーを取って、そのＴＬＳ暗号化キーを、キーがＡＫＡ認証チャレンジに依存するキー付きハッシュ関数Ｈを使用してハッシュすることができる。これは、ＢＳＦ６０４によって６１８におけるメッセージ内で提示されることが可能である。たとえば、ＡＶが適切にフォーマットされて、ＡＫＡチャレンジ値の代わりにＧＢＡ応答計算アルゴリズム内に直接投入されることが可能である。これによって、リプレイを軽減することができ、セキュアなＴＬＳチャネル６０８をＧＢＡ認証の実行にバインドすることができる。

【００７８】

例示的な一実施形態によれば、チャレンジ応答認証６１８－６３０へのセキュアチャネル６０８のバインディングが確立されることが可能である。たとえば、ＵＥ６０２は、認証チャレンジ６２０（たとえば、ｉｎｎｅｒ＿ａｕｔｈ＿ｃｈａｌｌｅｎｇｅ）を受信した後に、６０８におけるＴＬＳチャネルから抽出されたＴＬＳ＿ｋｅｙとともにダイジェストアルゴリズムＨ（たとえば、ＨＭＡＣアルゴリズム）を適用して、修正されたｃｈａｌｌｅｎｇｅ$^{*}$を得ることができる。これは、たとえば、Ｈ（ＴＬＳ＿ｋｅｙ，ｉｎｎｅｒ＿ａｕｔｈ＿ｃｈａｌｌｅｎｇｅ）→ｃｈａｌｌｅｎｇｅ$^{*}$と表されることが可能である。ＴＬＳに関するキー抽出方法の例示的な一実施形態は、ＩＥＴＦによって、RFC document 5705において示されている。ＵＥ６０８は、６２２において、ＢＳＦ６０４によって提示されたチャレンジへの応答を計算することができ、また同時に、同じまたは同様のアルゴリズムを使用して、バインディング応答$B_{res}$を計算することができる。これは、たとえば、ＡＫＡ－ＲＥＳＰＯＮＳＥ（ｉｎｎｅｒ＿ａｕｔｈ＿ｃｈａｌｌｅｎｇｅ）→ｒｅｓｐｏｎｓｅ；ＡＫＡ－ＲＥＳＰＯＮＳＥ（ｃｈａｌｌｅｎｇｅ$^{*}$，ＩＫ）→$B_{res}$と表されることが可能である。ＵＥは、６２４において応答および$B_{res}$を両方ともＢＳＦ６０４に返信することができる。

【００７９】

ＢＳＦ６０４は、ＵＥ６０２応答をチェックすることを介してバインディングの保証を得ることができる。応答が確認された場合には、ＢＳＦ６０４は、通信の他方のエンドに

おけるエンティティーが認証されていることがわかる。ＢＳＦ６０４が検証のために自分自身のエンドのＴＬＳキーを使用している状態で、$B_{res}$も確認された場合には、認証されているエンティティーは、ＢＳＦ６０４とのＴＬＳトンネルを有するエンティティーであるとも言え、$B_{res}$が確認されない場合には、ＭｉｔＭの疑いがあると言える。

【００８０】

図７は、ＳＩＰ－Ｄｉｇｅｓｔ認証を用いた、ＴＬＳとＧＢＡとをバインドする例示的なコールフローの図である。図７において示されているように、ＵＥ７０２は、ＢＳＦ７０４とのＴＬＳセッションを開始することによって、ブートストラッピング手順を開始することができる。ＵＥ７０２は、ＢＳＦ７０４によって提示される証明書によってＢＳＦ７０４を認証することができる。ＢＳＦ７０４は、この時点でＵＥ７０２からの認証を必要としない場合がある。７０８におけるＴＬＳトンネルの確立に続いて、ＵＥ７０２は、プライベート識別子（たとえば、ＩＭＰＩ（ＩＰ ｍｕｌｔｉｍｅｄｉａ ｓｕｂｓｙｓｔｅｍ ｐｒｉｖａｔｅ ｉｄｅｎｔｉｆｉｅｒ））を含む要求メッセージ（たとえば、ＨＴＴＰ ＧＥＴ要求）を７１０においてＢＳＦ７０４へ送信することができる。ＢＳＦ７０４は、７１２において認証情報（たとえば、（１つまたは複数の）ＡＶ）をＨＳＳ７０６に要求することができる。７１４において、ＨＳＳ７０６は、（たとえば、（１つまたは複数の）ＡＶを含む）要求されたデータをＢＳＦ７０４に提供することができる。ＢＳＦ７０４は、７１６において認証チャレンジを（たとえば、ＨＴＴＰ４０１無許可応答内に含めて）ＵＥ７０２へ送信することができる。その認証チャレンジは、認証ヘッダおよび／またはランダムに生成されたノンスを含むことができる。認証ヘッダは、ノンスに加えて、プライベートＩＤ、レルム、ｑｏｐ値、アルゴリズム情報、および／またはドメインなどのさらなるパラメータを含むことができる。

【００８１】

７１８において示されているように、ＢＳＦ７０４からのチャレンジに応答する場合には、ＵＥ７０２は、ランダムなｃノンスを生成することができ、ＳＩＰ Ｄｉｇｅｓｔクレデンシャルを使用することによって認証応答を計算することができる。ＵＥ７０２は、たとえばＴＬＳトンネルセッションキーと、セッションキーとの両方を使用して、ＭＡＣ（ｍｅｓｓａｇｅｓ ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｃｏｄｅ）値$B_{res}$を生成することもできる。ＴＬＳトンネルセッションキーおよび／またはセッションキーは、たとえばＩＫ（ｉｎｔｅｇｒｉｔｙ ｋｅｙ）またはＣＫ（ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ ｋｅｙ）を含むことができる。例示的な一実施形態においては、ＣＫの代わりにＩＫが使用されることが可能である。なぜなら、ＩＫは、インテグリティ保護の目的で使用されるように指定されることが可能であるためである。これらのキーは、ＵＥ７０２が受信したＡＶから取られた認証チャレンジＲＡＮＤから生成されることが可能である。これによって、ＴＬＳトンネル認証をＧＢＡプロトコルとバインドすることができる。認証チャレンジ応答および$B_{res}$は両方とも、許可ヘッダ内に置かれて、７２０における要求メッセージ（たとえば、ＨＴＴＰ ＧＥＴ要求メッセージ）内に含めてＢＳＦ７０４に返信されることが可能である。$B_{res}$は、認証応答と同じアルゴリズムによって計算されることが可能であるが、記載されているように別の入力パラメータを用いて計算されることも可能である。

【００８２】

ＢＳＦ７０４は、$B_{res}$を自分自身の予想値$B_{res}^{*}$に照らしてチェックすることができる。ＢＳＦ７０４がこれを行うことができるのは、$B_{res}$の計算において使用されたキーと、予想される認証応答の計算において使用されたキーとの両方をＢＳＦ７０４が知っているためである。受信された$B_{res}$が$B_{res}^{*}$と一致し、受信された認証応答がその予想値と一致した場合には、ＢＳＦ７０４は、ＵＥ７０２が真正であると判定することができ、また、２つの比較の一致から検証されたバインディング効果のおかげで、ＴＬＳトンネルの編成において自分が認証したＵＥ７０２が、プロトコルのＧＢＡの側面において自分が認証したＵＥ７０２と同じであることを確かめることができる。ＢＳＦ７０４は、７２２においてＧＢＡ／ＧＡＡマスターセッションキーＫｓのキー有効期間およ

びＢ－ＴＩＤなどのブートストラッピングキーマテリアルを生成することができる。７２４において、ＢＳＦ７０４は、Ｂ－ＴＩＤとキーＫｓとを含むメッセージ（たとえば、２００　ＯＫメッセージ）をＵＥ７０２へ送信することができる。ＵＥ７０２および／またはＢＳＦ７０４は、Ｋｓを使用してブートストラッピングキーマテリアルＫｓ＿ＮＡＦを導出することができる。たとえば、７２６において、ＵＥ７０２は、ＫｓからＫｓ＿ＮＡＦを生成することができる。Ｋｓ＿ＮＡＦは、Ｕａリファレンスポイントをセキュアにするために使用されることが可能である。

【００８３】

（ＵＥ７０２とＮＡＦ（ｎｅｔｗｏｒｋ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｆｕｎｃｔｉｏｎ）（図示せず）との間における）Ｕａリファレンスポイントを介したセキュリティーのためのアプリケーション固有のキーが、少なくとも部分的に、ＧＢＡを介して、ブートストラップされたキーから導出されることが可能である。たとえば、Ｋｓ＿ＮＡＦは、Ｋｓ＝ＣＫ‖ＩＫから導出されることが可能であり、この場合、ＣＫおよびＩＫは、７１４においてＨＳＳ７０６からＢＳＦ７０４へ配信されたＡＶの一部である。Ｋｓ＿ＮＡＦが、ＴＬＳトンネルの編成中に確立されたＫｓおよびマスターキーの両方から導出されている場合には、バインディングは、依然として有効であることが可能である。したがってＫｓ＿ＮＡＦは、ＵＥ７０２とネットワークとの間において共有されることが可能である。Ｋｓ＿ＮＡＦは、いかなるＭｉｔＭにとっても利用不可能とすることができる。

【００８４】

本明細書に記載されている実施形態は、クラウドコンピューティングシナリオにおいて実施されることが可能である。例示的な一実施形態によれば、ローカルＯｐｅｎＩＤの特色どうしおよび／または技術的特徴どうしを組み合わせて、１つまたは複数のプライベートデバイスからのマルチテナント対応のクラウドアクセスを可能にすることができる。たとえば、ローカルＯＰ認証、ＲＰ認証、シークレットの確立、および／または登録の手順が組み合わされることが可能である。組織のコンピューティングリソースに関するアウトソーシングの少なくとも２つの側面が、本明細書に記載されているように組み合わされることが可能である。１つの例示的な側面においては、リモート労働者、外部労働者、モバイル労働者、および現場労働者という現代の労働力階級が、労働者のプライベートデバイスを業務目的で活用するよう組織に促していると言える。別の例示的な側面においては、情報およびコンピューティングリソースが、コンピュータクラウド（たとえば、複数のインフラストラクチャーおよび／または複数のサーバをホストするマルチテナント）にますますアウトソースされていると言える。この二元的なアウトソーシングシナリオにおけるアウトソーシングを行う組織のセキュリティー要件は、アウトソーシングの実施のために選択されるセキュリティーアーキテクチャー上に制約を課す場合がある。これらは、保護の目的、および／または、たとえば組織の資産を保護するために使用されることが可能であるセキュリティーコントロールという点から説明されることが可能である。

【００８５】

ユーザデバイスは、セキュアではないとみなされる場合がある。たとえコーポレートデータの完全な保護がデバイス上で可能ではない場合があるとしても、組織のデータは、少なくともクラウドストレージ内では、ユーザデバイスを通じたデータの喪失および／または漏洩を防止するためになど、可能な範囲内でセキュアにされることが可能である。これを行うための１つの方法は、たとえばクラウド内のバーチャルワークステーションに接続することができるリモートデスクトップアプリケーションを介したクラウドへのアクセスを可能にすることであると言える。１つの利点として、これによって、リモート労働者および／またはバーチャルワークステーションが別のＯＳ（ｏｐｅｒａｔｉｎｇ　ｓｙｓｔｅｍ）を使用することを可能にすることができる。たとえば、ユーザデバイスは、ＡＮＤＲＯＩＤ（登録商標）またはＡＰＰＬＥ（登録商標）　ＯＳを実行するタブレットであることが可能であり、たとえば何らかのＲＤＰ（ｒｅｍｏｔｅ　ｄｅｓｋｔｏｐ　ｐｒｏｔｏｃｏｌ）クライアントアプリケーションを介してなど、ＭＩＣＲＯＳＯＦＴ　ＷＩＮＤＯＷＳ（登録商標）バーチャルマシンに接続することができる。ユーザ認証は、ユーザの

エンドにおけるハードウェア保護手段によってセキュアにされることが可能であり、これは、たとえばスマートカードまたはその他の信頼されている環境にバインドされることが可能である。本明細書に記載されているように、ローカルＯｐｅｎＩＤを用いてユーザ機器の（１人または複数の）ユーザに対して使用可能にされるスマートカードまたはその他の信頼されている環境が支給されることが可能である。ユーザアカウントが、本明細書に記載されているスマートカードまたはその他のセキュアな環境の実施形態において使用するために登録されることが可能である。

【００８６】

クラウドホストは、いくつかのセキュリティーコントロールおよび／または契約上の保証を提供することができる。クラウドサービスを使用する組織は、そのようなマルチテナント環境におけるデータの喪失および／または漏洩に対抗するさらなる独自のセキュリティーコントロールを確立することができる。一例として、組織のＩＴ部門は、クラウドワークステーションの（バーチャル）ハードドライブのためのディスク暗号化ソリューションをインストールすることができる。

【００８７】

クラウドコンピュータ上のディスク暗号化によって提供される保護は、制限される場合がある。クラウドホストのハイパーバイザは、バーチャルワークステーションがオペレーション中である間に完全なデータアクセスを有することができる。クラウドホストのハイパーバイザは、ユーザがワークステーションにログオンするときに、ハードドライブを復号するために使用される送信されてくるクレデンシャルをリッスンすることができる。ディスク暗号化は、たとえばＴｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇベースのバーチャル化サポートテクノロジーを使用することによってなど、何らかの様式でホスティングハードウェアにバインドされる場合がある。

【００８８】

リモートユーザデバイスは、たとえばディスク暗号化クレデンシャル（たとえば、パスワード）などのシークレットデータをクラウド内のバーチャルマシンにサブミットすることができる。そのようなデータは、ひそかにその宛先に到着するように保護されることが可能であり、ユーザに知られないことが可能である。このクレデンシャルは、指定されたバーチャルマシンへ転送されるような様式でローカルＯｐｅｎＩＤを用いて使用可能にされるスマートカードまたはその他の信頼されている環境上にひそかに格納されることが可能である。

【００８９】

図８は、ローカル認証エンティティーおよびクラウド／リモートコンピューティングサービスを実装している例示的な通信システムの図を示している。図８に示されているように、８１６においては、あるコーポレートユーザが、たとえばスマートカード８１８、またはその他の信頼されている環境を会社８１４から得ることができる。このスマートカードは、ローカルＯｐｅｎＩＤ対応のスマートカードであることが可能である。スマートカード８１８は、たとえばＯＰ$_{loc}$を含むことができる。スマートカード８１８は、クラウドホストされているＶＭ（ｖｉｒｔｕａｌ　ｍａｃｈｉｎｅ）８１０内など、その他の場所にホストされている会社８１４のリソースへのプライベートアクセスのためのクレデンシャルボールトを含むことができる。８１２において、会社８１４は、クラウドホストされているＶＭ８１０に接続することができ、スマートカード８１８を介したユーザデバイス８０２によるアクセスのために会社８１４の情報、サービス、ドキュメントなどを格納／アップロードすることができる。

【００９０】

ユーザは、８２０においてスマートカード８１８（たとえば、ＯＰ$_{loc}$機能を実行するためにローカルＯｐｅｎＩＤテクノロジーを用いて使用可能にされるスマートカード）をユーザデバイス８０２内に挿入することができる。ユーザデバイス８０２は、たとえばタブレット、スマートフォン、モバイル電話、ラップトップコンピュータ、またはその他のモバイルデバイスであることが可能である。ユーザデバイス８０２は、モバイルデバイ

スである必要はなく、スマートカード８１８またはその他の信頼されている環境を使用して、クラウドホストされているＶＭ８１０上のサービスにアクセスするように構成されているその他の任意のコンピューティングデバイスであることが可能である。いくつかのアプリケーションが、ユーザデバイス８０２上にインストールされることが可能であり、それは、たとえばクラウドホストされているＶＭ８１０上のリモートデスクトップにアクセスするためのＲＤＰ（ｒｅｍｏｔｅ　ｄｅｓｋｔｏｐ　ｐｒｏｔｏｃｏｌ）クライアントを含むことができる。リモートデスクトップへのログインは、ウェブベースのゲートウェイ８０６を通じて仲介されることが可能であり、ウェブベースのゲートウェイ８０６は、スマートカード認証（たとえば、ＯｐｅｎＩＤ認証）手順のためのＲＰとして機能することができる。このＲＰ８０６は、クラウドホストされているＶＭ８１０内に存在することができ、または独立したエンティティーであることも可能である。ＲＰ８０６は、アウトソーシングを行う会社へのセキュリティーサービスとして提供されることが可能であり、または会社８１４自体によって運営されることも可能である。ゲートウェイＲＰ８０６は、８０８において、クラウドホストされているＶＭ８１０へのセキュアでプライベートな接続を有することができる。

【００９１】

ローカルＯｐｅｎＩＤベースのログオンは、ここで説明される少なくとも３つのセキュリティー機能のうちの１つまたは複数を組み合わせることができる。たとえば、ローカルＯｐｅｎＩＤベースのログオンは、（１）$OP_{loc}$を介したユーザの認証、（２）スマートカード８１８上の$OP_{loc}$に対するＲＰ８０６（たとえば、セキュリティーゲートウェイ）の認証、ならびに／または（３）スマートカード８１８とＲＰ８０６との間における、および任意選択で、クラウドホストされているＶＭ８１０へさらに委任されるプライベートでシークレットなエンドツーエンドの確立を含むことができる。スマートカード８１８上の$OP_{loc}$を介したユーザの認証は、スマートカード８１８の所有および認証シークレットの知識と、バイオメトリックユーザ認証とを介した（少なくとも）２つのファクタからなる認証を含むことができる。認証および／またはシークレットの通信は、８０４において、ユーザデバイス８０２とＲＰ８０６との間におけるセキュアな通信を介して実行されることが可能である。スマートカード８１８上の$OP_{loc}$に対するＲＰ８０６の認証は、スプーフィングされたサイトではなく必ず指定のコーポレートリソースにユーザが接続するようにユーザへ拡張することができる。たとえば、ＲＰ８０６の認証のためのクレデンシャルは、スマートカード８１８内にセキュアに含まれることが可能である。ＲＰ８０６は、ユーザデバイス８０２とのシークレットを、クラウドホストされているＶＭ８１０へ委任すること、または、たとえば２つのセキュアチャネルの中間ポイントとして機能することが可能である。

【００９２】

スマートカード８１８上の$OP_{loc}$と、ＲＰ８０６との間においてシークレットが確立された場合には、スマートカード８１８上のクレデンシャルボールトのロックが解除されることが可能である。クラウドホストされているＶＭ８１０上のデータアクセスのためのクレデンシャルは、（たとえば、カード上の）確立されたシークレットを用いて暗号化されること、および／またはクラウドホストされているＶＭ８１０へサブミットされることが可能である。そこで、そのクレデンシャルは、復号されて検証されることが可能であり、検証が成功した場合には、ユーザデータを復号するためにシークレットが使用されることが可能である。ユーザは、リモートデスクトップアプリケーションを介して、クラウドホストされているＶＭ８１０上で作業を行うことができる。ユーザは、たとえば、クラウドホストされているＶＭ８１０からコーポレートイントラネットへのセキュアな接続を介してコーポレートリソースへのアクセスを有することができる。

【００９３】

図９は、例示的なプロトコルフローを示しており、このプロトコルフローは、ＳＩＰ　Ｄｉｇｅｓｔ認証を使用し、ＯｐｅｎＩＤにおけるＲＰ９０４認証を含む。この認証は、ＲＰ９０４とＯＰ９０８との間における事前共有キー$K_{r,o}$を使用したＯＰ９０８に対

するＵＥ９０２の認証を含むことができる。そしてＯｐｅｎＩＤ認証におけるＲＰ認証は、ＳＩＰ　Ｄｉｇｅｓｔ認証からブートストラップされることが可能である。図９において示されているプロトコルフローは、ＵＥ９０２、ＲＰ９０４（たとえば、アプリケーションサーバ）、ＯＰ９０８（たとえば、ＳＳＯ（Ｓｉｎｇｌｅ－Ｓｉｇｎ－ｏｎ）サーバ）、およびＨＳＳ９１０の間における通信を含む。ＲＰ９０４およびＯＰ９０８は、エンティティーどうしの間におけるセキュアな通信のために使用される共有シークレット$K_{r,o}$を９０６において事前に確立しておくことができる。

【００９４】

図９に示されているプロトコルにおいては、ＯｐｅｎＩＤは、ＵＥ９０２認証のためにステートレスモードで使用されることが可能である。ＯＰ９０８においてＲＰ９０４認証を達成するために、ステップ９１２から９１８の組合せが使用されることが可能である。９１２において、ＵＥ９０２は、ＩＭＳ（ＩＰ（ｉｎｔｅｒｎｅｔ　ｐｒｏｔｏｃｏｌ）　ｍｕｌｔｉｍｅｄｉａ　ｓｕｂｓｙｓｔｅｍ）に登録することができる。ＵＥ９０２は、９１４において認証要求（たとえば、ＯｐｅｎＩＤ認証要求）をＲＰ９０４へ送信することができる。認証要求は、認証識別子（たとえば、ＯＩＤ）を含むことができる。ＲＰ９０４は、９１６においてリダイレクト要求をＵＥ９０２へ送信することができる。９１６におけるリダイレクト要求は、ＵＥ９０２をＯＰ９０８へリダイレクトすることができる。このリダイレクト要求は、認証識別子（たとえば、ＯＩＤ）、および／または、ＲＰ９０４に対応するＲＰクレデンシャル$RP_{Cred}$を含むことができる。$RP_{Cred}$は、ＯＰ９０８との間で共有されている事前共有キー$K_{r,o}$を用いて署名されることが可能である。９１８において、ＵＥ９０２は、リダイレクト要求メッセージをＯＰ９０８へ送信することができる。このリダイレクト要求メッセージは、９１６においてＲＰ９０４から受信された認証識別子（たとえば、ＯＩＤ）および／または$RP_{Cred}$を含むことができる。

【００９５】

９２０において、ＯＰ９０８は、$RP_{Cred}$を使用してＲＰ９０４の認証を実行すること、および／またはＲＰ認証アサーションを生成することが可能である。ＯＰ９０８は、ＵＥ９０２とＯＰ９０８との間におけるセキュアな通信を確かなものにするために、共有キー$K_0$（これは、ＵＥ９０２とＯＰ９０８との間における共有キーであることが可能である）のチェックを実行することもできる。９２２において、ＯＰ９０８は、ＲＰ９０４が認証されたかどうかを判定することができる。９２２においてＲＰ９０４が適切に認証されていない場合には、ＯＰ９０８は、ＲＰ９０４が偽のＲＰであることと、手順を終了すべきであることとを示すアラートを９２４においてＵＥ９０２へ送信することができる。９２２においてＲＰ９０４が適切に認証されている場合には、ＯＰ９０８は、プロトコルを続けることができる。例示的な一実施形態においては、９２０におけるＲＰ９０４認証アサーションの生成は、９２６においてＲＰ９０４が真正であると判定されている場合に生じることができる。（図９には示されていない）例示的な一実施形態においては、９２２におけるＲＰ９０４認証判定が、ＲＰ認証に関する判定をＯＰ９０８が行うポイントとみなされる場合には、$RP_{Assert}$の使用は、ＲＰ９０４認証判定に続くステップにおいてプロトコルから省略されることが可能である。

【００９６】

例示的な一変形形態においては、$RP_{Cred}$は、ＲＰ９０４のプレーンテキスト識別子であること（すなわち、いかなるキーによっても署名されていないこと）が可能であり、これは、ＯＰ９０８がさらなる使用のために正しい共有キー$K_{r,o}$を選択することを可能にすることができる。このケースにおいては、$RP_{Cred}$が、ＯＰ９０８によって知られているいかなるＲＰにも対応しない場合には、ＯＰ９０８は、手順を終了することを決定して、ＵＥ９０２に通知することができる。

【００９７】

図９において示されている例示的なメッセージフローを続けると、ＳＩＰ－Ｄｉｇｅｓｔ認証が実行されることが可能である。たとえば、ＯＰ９０８は、９２８においてＳＤ－

ＡＶ（ＳＩＰ ｄｉｇｅｓｔ ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｖｅｃｔｏｒ）および／またはユーザプロファイル情報をＨＳＳ９１０から得ることができる。ＯＰ９０８は、ユーザクレデンシャル（たとえば、ユーザ名／パスワード）に基づいて、そのような情報を得ることができる。ＯＰ９０８は、ユーザクレデンシャル、レルム、ｑｏｐ値、認証アルゴリズム、および／またはハッシュＨ（Ａ１）をＨＳＳ９１０から得ることもできる。例示的な一実施形態においては、レルム、ｑｏｐ値、認証アルゴリズム、および／またはハッシュＨ（Ａ１）は、ＩＥＴＦによって、RFC document 2069およびRFC document 2617において示されていると言える。

【００９８】

９３０において、ＯＰ９０８は、ノンスを生成すること、ならびにそのノンスおよびＨ（Ａ１）を格納することが可能である。ＯＰ９０８は、９３２において認証チャレンジ（たとえば、認証チャレンジを伴うＨＴＴＰ４０１無許可メッセージ）をＵＥ９０２へ送信することができる。その認証チャレンジは、ユーザクレデンシャル、ノンス、レルム、ｑｏｐ値、および／または認証アルゴリズムを含むことができる。９３４において、ＵＥ９０２は、ｃノンス、Ｈ（Ａ１）、および／または、セキュアな通信のためにＯＰ９０８との間で共有されるシークレットキー$K_0$を生成することができる。ＵＥ９０２は、チャレンジ応答を計算して、そのチャレンジ応答（たとえば、認証応答を伴うＨＴＴＰ ＧＥＴメッセージ）を９３６においてＯＰ９０８へ送信することもできる。チャレンジ応答は、ｃノンス、応答、ノンス、ユーザクレデンシャル、レルム、ｑｏｐ値、認証アルゴリズム、ダイジェストＵＲＬ、および／またはノンスカウントを含むことができる。例示的な一実施形態においては、ｃノンス、ノンス、レルム、ｑｏｐ値、認証アルゴリズム、ダイジェストＵＲＬ、および／またはノンスカウントは、ＩＥＴＦによって、RFC document 2617において示されていると言える。共有キー$K_0$は、共有キー$K_0$をＳＩＰ Ｄｉｇｅｓｔ認証にバインドすることができる認証応答から導出されることが可能である。９３８において、ＯＰ９０８は、ノンスに照らしてチェックを行うこと、Ｘｒｅｓｐｏｎｓｅを計算すること、および／またはそのＸｒｅｓｐｏｎｓｅを、ＵＥ９０２から受信された応答と比較することが可能である。

【００９９】

ＳＩＰ Ｄｉｇｅｓｔ認証が成功した場合（たとえば、Ｘｒｅｓｐｏｎｓｅまたはその中の特定のパラメータが、応答またはその中の特定のパラメータと一致した場合）には、ＯＰ９０８は、９３８においてＵＥ認証アサーション$UE_{Assert}$および／または共有キー$K_0$を生成することができる。９４０において、ＯＰ９０８は、ノンス１および／または$K_1$を生成することができ、$K_1$は、ＵＥ９０２とＲＰ９０４との間においてセキュアチャネルを確立するために使用される、ＵＥ９０２、ＯＰ９０８、および／またはＲＰ９０４の間における共有キーであることが可能である。$K_1$は、新しさのために生成においてノンス１を使用してＯＰ９０８によって生成されることが可能である。ノンス１および／またはＲＰ認証アサーションメッセージ$RP_{Assert}$を暗号化するために、$K_0$が使用されることが可能であり、これは、たとえば$EK_0$（ｎｏｎｃｅ １，$RP_{Assert}$）と呼ばれうる。$K_0$を用いた暗号化は、正当な認証されたＵＥ９０２が$RP_{Assert}$を得ることを可能にすることができ、これは、そのＵＥ９０２が、意図された真正なＲＰ９０４と通信していることをそのＵＥ９０２に対して確認することであると言える。ＯＰ９０８は、共有キー$K_{r,o}$を使用して、キー$K_1$および／またはＵＥ認証アサーションメッセージ$UE_{Assert}$を暗号化することができ、これは、たとえば$EK_{r,o}$（$K_1$，$UE_{Assert}$）と呼ばれうる。９４２において、ＯＰ９０８は、リダイレクトメッセージをＵＥ９０２へ送信することができ、このリダイレクトメッセージは、ＵＥ９０２をＲＰ９０４へリダイレクトすることができる。このリダイレクトメッセージは、$EK_0$（ｎｏｎｃｅ １，$RP_{Assert}$）および／または$EK_{r,o}$（$K_1$，$UE_{Assert}$）を含むことができる。例示的な一実施形態においては、ＲＰ認証アサーションメッセージ$RP_{Assert}$は、９４４において示されているように、プロトコルフロー内の特定のポイントにおいて使用されなくなる場合がある。なぜなら、ＯＰ９０

８が、ＲＰ９０４の信頼性に関する判定ポイントになることができるためである。ＲＰ９０４がＵＥ９０２との通信を実行している場合に（たとえば、実施態様固有のステップ９５２および／または９５４を実行している場合などに）、ＵＥ９０２が、意図されたＲＰ９０４とセキュアに通信している状態を確実にするために、$K_1$が使用されることが可能である。

【０１００】

９４６において、ＵＥ９０２は、$K_0$を使用してノンス１および／またはＲＰ認証アサーションメッセージ$RP_{Assert}$を復号することができる。$K_0$を使用してＲＰ認証アサーション$RP_{Assert}$を復号できることによって、ＵＥ９０２は、自分が、意図された真正なＲＰ９０４と通信していることを確認することができる。ＵＥ９０２は、ＲＰ認証アサーションメッセージ$RP_{Assert}$およびノンス１を得ることができる。ＵＥ９０２は、受信されたＲＰ認証アサーション$RP_{Assert}$に基づいてＲＰ９０４を認証することができる。ＵＥ９０２は、ノンス１を使用して$K_1$を生成することができる。共有キー$K_1$を用いた暗号化は、正当な認証されたＵＥ９０２が$UE_{Author}$を得ることを可能にすることができ、$UE_{Author}$は、サービスに伴って使用するためのアクセストークンとして機能することができる。ＵＥ９０２は、９４８においてＲＰ９０４へリダイレクトされることが可能である。９４８において、ＵＥ９０２は、キー$K_1$およびＵＥ認証アサーションメッセージ$UE_{Assert}$をＲＰ９０４へ送信することができる。キー$K_1$および$UE_{Assert}$は、共有キー$K_{r,o}$を用いて暗号化されることが可能であり、これは、たとえば$EK_{r,o}$（$K_1$，$UE_{Assert}$）と呼ばれうる。この暗号化は、ＯＰ９０８によって前もって実行されていることが可能である。９５０において、ＲＰ９０４は、$K_{r,o}$を使用して$EK_{r,o}$（$K_1$，$UE_{Assert}$）を復号して、$UE_{Assert}$および$K_1$を得ることができる。ＵＥ９０２に関する情報は、９５０において許可されることが可能である。たとえば、ＲＰ９０４は、$K_1$を使用して、$UE_{Assert}$の署名を検証することができる。$UE_{Assert}$の検証に成功した後に、ＲＰ９０４は、許可情報$UE_{Author}$を生成することができ、この許可情報$UE_{Author}$は、キー$K_1$を用いて暗号化されることが可能であり、たとえば$EK_1$（$UE_{Author}$）と呼ばれうる。$UE_{Author}$は、ＵＥ９０２がＲＰ９０４における１つまたは複数のサービスにアクセスすることを許可されている旨を示す許可情報または許可パラメータを含むことができる。ＲＰ９０４は、ＵＥ９０２がＲＰ９０４におけるサービスに関して許可を受けているかどうかについて、９５２においてＵＥ９０２に通知することができる。たとえば、ＲＰ９０４は、ＵＥ許可パラメータまたは情報$UE_{Author}$を送信することができる。$UE_{Author}$は、シークレットキー$K_1$を用いて暗号化されて（$EK_1$（$UE_{Author}$））、ＵＥ９０２とＲＰ９０４との間において共有されることが可能である。９５４において、ＵＥ９０２は、$EK_1$（$UE_{Author}$）を復号することができ、要求されているサービスに、$UE_{Author}$を使用してＲＰ９０４からアクセスすることができる。ステップ９５２および／または９５４は、実施態様固有のステップであることが可能であり、任意選択であることが可能であり、ＵＥ９０２および／またはＲＰ９０４のサービス実施態様に依存することができる。たとえば、これらは、認証後に一般的なサービスアクセスをＵＥ９０２に提供するという所望の用途に固有であることが可能である。これらのステップが使用されない場合には、$K_1$は必要とされないと言える。

【０１０１】

例示的な一実施形態においては、図９において示されているプロトコルフローは、シークレット$K_{r,o}$を使用して、ＯＰ９０８に対するＲＰ９０４認証を達成することができる。たとえば、シークレット$K_{r,o}$は、ＯＰ９０８に対して（たとえば、ステップ９１２から９１８において）$RP_{Cred}$を伴うメッセージに署名するために使用されない場合には、認証のために使用されることが可能である。たとえば、ＯＰ９０８とＲＰ９０４がシークレット$K_{r,o}$を既に共有している場合には、このシークレットは、ＯＰ９０８との間でのＲＰ９０４認証のために使用されることが可能である。認証プロトコル（たと

えば、ＯｐｅｎＩＤプロトコル）のディスカバリーステップおよび（任意選択の）アソシエーション作成ステップは、図９に示されているプロトコルにおいては示されていない。ＵＥ９０２上での実施態様は、そのようなあらゆるＲＰ９０４認証によって影響されないことが可能である。たとえば、一実施形態においては、ＵＥ９０２は、$OP_{loc}$機能を含まない場合があり、したがって、チャレンジ$RP_{Chv}$をＲＰへ送信することができない場合がある。

【０１０２】

図１０は、ＯＰ１００８に対するＲＰ１００４認証を用いた例示的なプロトコルのメッセージフロー図を示している。図１０においては、ＵＥ１００２、ＲＰ１００４（たとえば、アプリケーションサーバ）、ＯＰ１００８（たとえば、ＳＳＯサーバ）、および／またはＨＳＳ１０１０の間において通信が実行されることが可能である。ＲＰ１００４とＯＰ１００８は、セキュアチャネルを介してセキュアな通信を可能にするために、１００６において示されている、事前に確立された共有シークレットを有することができる。

【０１０３】

図１０において示されているように、ＵＥ１００２は、１０１２において認証要求（たとえば、ＯｐｅｎＩＤ認証要求）をＲＰ１００４に発行することができ、この認証要求は、ログイン識別子（たとえば、ＵＲＬまたはＥメールアドレスなどのＯｐｅｎＩＤ識別子）を含む。ＲＰ１００４は、１０１４においてＯＰ１００８をディスカバーすることができる。１０１６において、ＲＰ１００４は、アソシエーション要求（たとえば、ＯｐｅｎＩＤアソシエーション要求）をＯＰ１００８へ送信することができる。ＲＰ１００４およびＯＰ１００８は、Ｄｉｆｆｉｅ－ＨｅｌｌｍａｎキーＤ－Ｈを確立することができる。ＯＰ１００８は、アソシエーションシークレットおよび／またはアソシエーションハンドルを生成することができ、アソシエーションシークレットおよび／またはアソシエーションハンドルは、まとめてアソシエーションと呼ばれる場合がある。１０１８において、ＯＰ１００８は、ＲＰ１００４にアソシエーション応答を送信することができ、アソシエーション応答は、アソシエーションシークレットおよびノンス０を含むことができる。アソシエーションシークレットおよび／またはノンス０は、確立されたＤ－Ｈキーを用いて暗号化されることが可能である。ＲＰ１００４は、受信した暗号化されたノンス０および暗号化されたアソシエーションシークレットを１０２０において復号することができる。次いでＲＰ１００４は、共有キー$K_{r,o}$を用いてノンス０に署名することができ、共有キー$K_{r,o}$は、ＲＰ１００４とＯＰ１００８との間において共有されている事前に確立されたキーであることが可能である。ノンス０に署名するために、ＨＭＡＣまたは別の適切な対称署名アルゴリズムが使用されることが可能である。ＲＰ１００４およびＯＰ１００８は、知られているメカニズムを使用して、たとえば、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎキー交換プロトコルまたは事前共有シークレットを使用して、共有シークレット$K_{r,o}$を有することができる。この共有シークレットを用いて、ＯＰ１００８およびＲＰ１００４は、メッセージに署名すること、および共有シークレット$K_{r,o}$を用いて署名された互いのメッセージを検証することが可能である。

【０１０４】

１０２２において、ＲＰ１００４は、ＵＥ１００２によって送信された認証要求を、リダイレクトメッセージを使用してリダイレクトすることができる。このリダイレクトメッセージは、ログイン識別子（たとえば、ＯｐｅｎＩＤ識別子）、ＲＰ１００４識別子（$RP_{Cred}$）、および／または署名されたノンス０を含むことができる。たとえば、ＵＥ１００２は、ＯＰ１００８へリダイレクトされることが可能である。認証要求は、１０２４においてＯＰ１００８へリダイレクトされることが可能である。このリダイレクションは、ログイン識別子（たとえば、ＯｐｅｎＩＤ識別子）および／または$RP_{Cred}$を含むことができる。ＯＰ１００６は、セキュアな通信のために、１０２６において、ＵＥ１００２との通信用としてＨＴＴＰＳの使用を強制することができる。ＨＴＴＰＳの使用の強制は、ＯＰ１００２のウェブサーバの構成（たとえば、アドレスのリライト）によって実行されることが可能である。１０２８において、ＯＰ１００８は、ＲＰ１００４を認証

するためにノンス０の署名を検証することができる。たとえば、ＯＰ１００８は、共有キー$K_{r,o}$を使用して、署名を検証することができる。ステップ１０２８のＲＰ１００４認証は、１０３０において判定されることが可能であり、ＲＰ１００４認証が失敗した場合には、ＯＰ１００８は、ＲＰ１００４認証の失敗を示すためのアラートメッセージ（これは、たとえばＨＴＴＰＳによって保護されることが可能である）を１０３２においてＵＥ１００２へ送信することができる。ステップ１０２８におけるＲＰ１００４認証が成功した場合には、プロトコルフローは、たとえばステップ１０３４などにおいて続行することができる。

【０１０５】

１０３４において、ＯＰ１００８は、ＯＰ１００８とＵＥ１００２との間においてセキュアチャネルが確立されたかどうかを判定することができる。たとえば、ＯＰ１００８は、有効なキー$K_0$が存在するかどうかを判定することができる。有効なキー$K_0$が実際に存在する場合には、プロトコルフローは、ＵＥ認証アサーション$UE_{Assert}$の生成を伴うステップ１０４８へ進むことができる。有効なキー$K_0$が存在しない場合には、プロトコルフローは、ＵＥ１００２の認証の実行へ進むことができる。例示的な一実施形態においては、（たとえば、図４において示されているような）セキュアチャネルの確立と、ＵＥ１００２の認証とは、同じプロトコルフロー内でともにバインドされることが可能である。１０３６において示されているように、ＯＰ１００８は、認証要求をＨＳＳ（Ｈｏｍｅ Ｓｕｂｓｃｒｉｐｔｉｏｎ Ｓｅｒｖｅｒ）１０１０へ送信することができ、ＨＳＳ１０１０からのユーザクレデンシャルに基づいてＳＤ－ＡＶ（ＳＩＰ Ｄｉｇｅｓｔ ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｖｅｃｔｏｒ）および／またはユーザプロファイルを得ることができる。ＳＤ－ＡＶは、ｑｏｐ値と、認証アルゴリズムと、レルムと、ユーザクレデンシャル、レルム、およびパスワードのハッシュ（Ｈ（Ａ１）と呼ばれる）とを含むことができる。複数のＨＳＳ環境においては、ＯＰ１００８は、ＳＬＦ（Ｓｅｒｖｉｃｅ Ｌａｙｅｒ Ｆｕｎｃｔｉｏｎ）にクエリーを行うことによって、ＵＥ１００２のサブスクリプションの詳細が格納されているＨＳＳ１０１０のアドレスを得ることができる。１０３８において、ＯＰ１００８は、ランダムなノンスを生成することができ、ハッシュＨ（Ａ１）およびノンスをユーザクレデンシャルと対比させて格納することができる。ＯＰ１００８は、１０４０において認証チャレンジメッセージ（たとえば、ＳＩＰ－Ｄｉｇｅｓｔ認証チャレンジとしての４０１認証チャレンジ）を（たとえば、保護されたＨＴＴＰＳメッセージ内に含めて）ＵＥ１００２へ送信することができ、この認証チャレンジメッセージは、ノンス、レルム、ｑｏｐ値、認証アルゴリズム、および／またはユーザクレデンシャルを含むことができる。

【０１０６】

１０４０においてチャレンジを受信すると、ＵＥ１００２は、１０４２においてランダムなｃノンスおよびＨ（Ａ１）を生成することができる。ＵＥ１００２は、Ｈ（Ａ１）、ｃノンス、および／または、たとえば認証チャレンジ内に含まれているマテリアルなどのその他の情報に基づいて、共有シークレット$K_0$を生成することができる。共有シークレット$K_0$は、ＵＥ１００２とＯＰ１００８との間における共有シークレットであることが可能であり、この共有シークレットは、ＵＥ１００２とＯＰ１００８との間における通信がセキュアチャネルを使用して送信されることを可能にすることができる。ＵＥ１００２は、ｃノンス、ならびに／または、認証チャレンジ内に含めて提供されたその他のパラメータ（たとえば、ノンス、ユーザクレデンシャル、および／もしくはｑｏｐ値など）を使用して、認証応答を計算することができる。１０４４において、ＵＥ１００２は、（たとえば、保護されたＨＴＴＰＳメッセージであることが可能である）チャレンジ応答をＯＰ１００８へ送信することができる。このチャレンジ応答は、たとえば、ｃノンス、ノンス、応答、レルム、ユーザクレデンシャル、ｑｏｐ値、認証アルゴリズム、ノンスカウント、および／またはダイジェストＵＲＬを含むことができる。１０４４においてその応答を受信すると、ＯＰ１００８は、前もって格納されているノンスを使用して、その応答内に含まれているノンスに対するチェックを行うことができる。そのチェックが成功した場合

には、ＯＰ１００８は、前もって格納されているハッシュＨ（Ａ１）およびノンスを、応答内に含まれているその他のパラメータ（たとえば、ｃノンス、ノンスカウント、ｑｏｐ値など）とともに使用して、予想される応答（Ｘｒｅｓｐｏｎｓｅ）を計算することができ、この予想される応答を使用して、ＵＥ１００２から受信された応答に対するチェックを行うことができる。そのチェックが成功した場合には、ＵＥ１００２の認証は成功したとみなされることが可能である。そのチェックが成功しなかった場合には、その認証は失敗したとみなされることが可能である。ＵＥ１００２の認証が成功した場合には、ＯＰ１００８は、共有シークレット$K_0$を生成することができ、この共有シークレット$K_0$は、ハッシュＨ（Ａ１）、ｃノンス、および／または、たとえば認証チャレンジ内に含まれているマテリアルなどのその他の情報に基づいて生成されることが可能である。代替として、または追加として、ＯＰ１００８は、１０４４において応答を受信すると、認証アサーション$UE_{Assert}$を作成することができる。$UE_{Assert}$は、アソシエーションシークレットを使用して署名されることが可能であり、そのアソシエーションシークレットは、たとえば１０１８におけるメッセージ内で使用されたアソシエーションシークレットであることが可能である。

【０１０７】

１０５０において、ＯＰ１００８は、ランダムなノンス１を生成することができ、ならびに／または$K_0$およびノンス１に基づいて共有シークレット$K_1$を生成することができる。共有シークレット$K_1$は、ＵＥ１００２とＲＰ１００４との間においてセキュアチャネルを確立するための、ＵＥ１００２、ＯＰ１００８、および／またはＲＰ１００４の間における共有シークレットであることが可能である。ＯＰ１００８は、$K_0$を使用してノンス１を暗号化することができ（これは、たとえば$EK_0$（ｎｏｎｃｅ　１）と呼ばれうる）、$K_{r,o}$を使用して$K_1$および署名されたアサーションメッセージ$UE_{Assert}$を暗号化することができる（これは、たとえば$EK_{r,o}$（$K_1$，ｓｉｇｎｅｄ（$UE_{Assert}$））と呼ばれうる）。ＯＰ１００８は、１０５２においてメッセージ（たとえば、リダイレクトメッセージ）をＵＥ１００２へ送信することができ、このメッセージは、ＲＰ１００４へのリダイレクションとともに$EK_0$（ｎｏｎｃｅ　１）および／または$EK_{r,o}$（$K_1$，ｓｉｇｎｅｄ（$UE_{Assert}$））を含むことができる。１０５４において、ＵＥ１００２は、共有キー$K_0$を使用して$EK_0$（ｎｏｎｃｅ　１）を復号することができ、ノンス１を得ることができる。ＵＥ１００２は、$K_0$およびノンス１に基づいて共有シークレット$K_1$を生成することができる。ＯＰ１００８によって送信されたメッセージは、１０５６においてＲＰ１００４へリダイレクトされることが可能である。１０５６におけるメッセージは、$EK_{r,o}$（$K_1$，ｓｉｇｎｅｄ　$UE_{Assert}$）を含むことができる。ＲＰ１００４は、１０５８において$EK_{r,o}$（$K_1$，ｓｉｇｎｅｄ　$UE_{Assert}$）を復号して、$UE_{Assert}$および$K_1$を得ることができる。ＲＰ１００４は、ＯＰ１００８との間で共有されているアソシエーションシークレットを使用して、アサーションメッセージ$UE_{Assert}$の署名を検証することができる。アサーションメッセージ$UE_{Assert}$を検証した後に、ＲＰ１００４は、ＵＥ１００２のための許可情報を生成することができる。たとえば、ＲＰ１００４は、許可情報$UE_{Author}$を生成して、$K_1$を使用して$UE_{Author}$を暗号化することができ、これは、たとえば$EK_1$（$UE_{Author}$）と呼ばれうる。ＲＰ１００４は、１０６０において、このメッセージ内に含まれているアプリケーション固有の許可情報について、$K_1$を用いて暗号化してＵＥ１００２に通知することができる。ＵＥ１００２は、１０６２において、共有キー$K_1$を使用して$EK_1$（$UE_{Author}$）を復号することができ、次いで、要求されているサービスにアクセスすることができる。

【０１０８】

図１０においては、許可情報またはパラメータ$UE_{Author}$は、アプリケーションに固有であること、および／またはＯＰ１００８に固有であることが可能である。$UE_{Author}$がＯＰ１００８に固有である場合には、$UE_{Author}$は、$K_0$によって署名されることが可能である。許可情報またはパラメータ$UE_{Author}$がアプリケーシ

ョンに固有である場合には、ＵＥ$_{Ａｕｔｈｏｒ}$は、Ｋ$_{ｒ，ｏ}$または署名キーＳのいずれかによって署名されることが可能である。転送は、署名キーＳを用いて機能することができる。

【０１０９】

例示的な一実施形態においては、図１０に示されているプロトコルフローは、本明細書に記載されているような分割された端末のシナリオを使用する際に実施されることが可能である。

【０１１０】

別の例示的な実施形態においては、ＲＰ１００４認証は、ＯＰ１００８とＲＰ１００４との間におけるチャレンジ応答ステップ内に含まれることが可能であり、その場合には、ＯＰ１００８は、チャレンジを新しさの証明とともにＲＰ１００４へ（たとえば、ノンスを介して）送信することができる。ＲＰ１００４は、事前に確立された共有シークレットＫ$_{ｒ，ｏ}$を使用して、このノンスに署名し、返信をＯＰ１００８へ返すことができる。認証チャレンジに対する応答は、ＯＰ１００８認証チャレンジに対する直接の応答として行うことができ、またはリダイレクトメッセージ内に統合されることも可能であり、そのリダイレクトメッセージがＵＥ１００２をＯＰ１００８へ送る。いずれのケースにおいても、ＯＰ１００８は、（たとえば、ＵＥ認証に従事する前に）ＲＰ１００４を認証する上で信頼できる証拠を有することができる。これは、失敗したＲＰ１００４認証のケースにおいてＯＰ１００８がプロトコルを停止することを可能にすることができ、そのような失敗したＲＰ１００４認証のケースにおいてＵＥ１００２とＯＰ１００８との間における通信の労力を省くことができる。ＯＰ１００８は、たとえば１０３２において示されているように、失敗したＲＰ１００４認証に関する情報をＵＥ１００２へ直接伝達することができる。

【０１１１】

本明細書に記載されているように、ＲＰ１００４認証のためにアソシエーションが使用されることが可能である。たとえば、ＲＰ１００４がＯＰ１００８とのアソシエーションを確立する場合には、対応するステップは、ＯＰ１００８からのチャレンジを組み込むように修正されることが可能である。アソシエーションの確立中に、ＯＰ１００８およびＲＰ１００４は、ＭＡＣキーをセットアップすることができ、このＭＡＣキーは、認証アサーションメッセージに署名するために使用されることが可能である。このキーは、一時的なシークレットキーを使用して暗号化されて送信されることが可能であり、その一時的なシークレットキーは、ＯＰ１００８とＲＰ１００４との間において、たとえばＤＨ（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）キーを使用して、ネゴシエートされることが可能である。ＯＰ１００８は、その一時的なシークレットキーに加えて、（たとえばＤＨキーを用いて暗号化されることも可能である）ノンスをＲＰ１００４への応答内に含めることができる。

【０１１２】

ＲＰ１００４は、ネゴシエートされたＤＨキーに基づいてノンスおよびＭＡＣキーを復号することができる。ＲＰ１００４は、ＯＰ１００８から受信されたノンスに署名または暗号化を行うために、自分自身の事前に確立された共有キーＫ$_{ｒ，ｏ}$を使用することができ、そのキーをさらなるパラメータとして、ＵＥ１００２へ送信されるリダイレクトメッセージに付加することができる。ＵＥ１００２は、ＯＰ１００８へのリダイレクトに従うため、ＯＰ１００８は、署名されたまたは暗号化されたノンスを受信することができ、共有キーＫ$_{ｒ，ｏ}$を使用してＲＰ１００４を認証することができる。失敗した認証のケースにおいては、ＯＰ１００８は、認証されていないＲＰからＵＥ１００２を保護するためのアラートメッセージをＵＥ１００２へ送信することができる。成功したＲＰ１００４認証のケースにおいては、ＯＰ１００２は、プロトコルを進めることができる。

【０１１３】

ＲＰ１００４認証のためにディスカバリーモードを使用するための例示的な実施形態が説明される。たとえば、ＯＰ１００８は、ＯＰ１００８とＲＰ１００４との間においてアソシエーションが確立されていないケース（すなわち、ＯｐｅｎＩＤにおけるステートレ

スモード）においてＲＰ１００４へ情報を送信することを可能にすることができる。ステートレスモードにおいては、ＯＰ１００８とＲＰ１００４との間における情報のやり取りは、ディスカバリー中に行われることが可能である。しかし、ディスカバリーは、たとえば委任されたディスカバリーのケースにおいてなど、ＯＰ１００８を含む場合もあり、または含まない場合もある。委任されたディスカバリーにおいては、ユーザ識別子は、たとえば、http://myblog.blog.comにある可能性があり、そして（たとえば、http://myblog.myopenid.comにおける）ＯＰ１００８のＯＰエンドポイントＵＲＬを指す可能性がある。したがって、（たとえば、ｍｙｏｐｅｎｉｄ．ｃｏｍにおける）ＯＰ１００８は、直接ディスカバリーに含まれない場合があり、このステージにおいてＲＰ１００４を認証することができない場合がある。ＯＰ１００８は、たとえば図１０に示されているように、１０２８、１０３０において認証を判定する代わりに、１０１６、１０１８においてアソシエーション中にＲＰ１００４を認証することができる場合がある。

【０１１４】

ＯＰ１００８は、ディスカバリーステップ中にさらなる情報をＲＰ１００４へ提供することを可能にすることができる場合（すなわち、ユーザ識別子ページが、ＯＰ１００８自体においてホストされる場合）には、ディスカバリー情報ページの一部としてノンスを動的に生成すること、およびそのノンスを、ＨＴＴＰ要求を行っているＲＰ１００４の識別子（たとえば、ＵＲＬまたはＥメールアドレス）に関連付けることが可能である。次いでＯＰ１００８は、ＲＰ１００４が、このノンスに署名または暗号化を行うこと、およびその情報をリダイレクトメッセージ内に含めることを予期することができる。

【０１１５】

本明細書において示されているように、ＯＰ１００８は、ＯＰ１００８とＵＥ１００２との間における通信を保護することができる。たとえば、１０２６において示されているように、ＯＰ１００８は、ＨＴＴＰＳの使用を強制することができる（すなわち、ＵＥ１００２は、ＯＰ１００８によってＨＴＴＰＳの使用へとリダイレクトされることが可能であり、それによって、ＵＥ１００２とＯＰ１００８との間におけるその後のいかなる通信も保護されることが可能である）。たとえば、ＴＬＳが使用されることが可能である。ＴＬＳは、ＯＰ１００８の証明書を自動的にインポートすること、または事前にインストールされたＯＰ証明書を使用することをＵＥ１００２に強制することによって機能することができる。強制される両方のことは、たとえば、ＢＡによって（たとえば、ルートＣＡにより署名された）ルート証明書に照らしてチェックされることが可能である。そのような保護は、たとえば１０４０におけるＯＰ１００８からＵＥ１００２への認証チャレンジメッセージ上でのＭｉｔＭ攻撃を防止することを可能にすることができる。また、失敗したＲＰ１００４認証のケースにおいては、そのような保護は、ＯＰ１００８がアラートメッセージをＵＥ１００２へ保護された様式で送信することを可能にすることができる。

【０１１６】

ここで説明される実施形態は、ローカルアサーションプロバイダを用いて実施されることが可能である。ここで説明されるのは、ＲＰ認証とＯｐｅｎＩＤを調和させてローカルアサーションプロバイダを活用する例示的なプロトコルである。説明される実施形態は、ＲＰと（ネットワーク側の）ＯＰとの間においてコンタクト（たとえば、最初のコンタクト）があった場合に、ＲＰとＯＰとの間における事前に確立された共有シークレット$K_{r,o}$に基づいて、ＲＰの認証を可能にすることができる。ＯｐｅｎＩＤのアソシエーションモードにおいては、これは、アソシエーションフェーズである。

【０１１７】

図１１は、ローカルアサーションプロバイダを用いたプロビジョニングフェーズのメッセージフロー図の例示的な一実施形態を示している。図１１において示されているように、ローカルアサーションプロバイダを伴うプロビジョニングフェーズ内で実行される通信においては、ＵＥ１１０２、ＲＰ１１０４、ＯＰ１１０６、および／またはＨＳＳ１１０８が実装されることが可能である。プロビジョニングフェーズ内のさまざまなステージにおいては、リプレイ保護のためにノンスが実施されることが可能である。

【０１１８】
図１１において示されているように、ＵＥ１１０２は、１１１０においてログイン識別子（たとえば、ＯＩＤ）をＲＰ１１０４へサブミットすることができる。ＲＰ１１０４は、アソシエーション要求（たとえば、ｈｔｔｐ　ＰＯＳＴ　ＯｐｅｎＩＤアソシエーション要求）を１１１２においてＯＰ１１０６へ送信することができる。このアソシエーション要求は、ＲＰ１１０４クレデンシャル$RP_{Cred}$を含むことができ、ＲＰ１１０４クレデンシャル$RP_{Cred}$は、ＲＰ１１０４とＯＰ１１０６との間において共有されている共有キー$K_{r,o}$を用いて暗号化されることが可能である。この暗号化された$RP_{Cred}$は、たとえば$EK_{r,o}$（$RP_{Cred}$）と呼ばれうる。ＲＰクレデンシャル$RP_{Cred}$は、事前共有シークレットまたは識別子を含むことができる一般的なタイプのクレデンシャルであることが可能である。１１１４において、ＯＰ１１０６は、共有キー$K_0$が存在するかどうかを判定することができる。共有キー$K_0$が実際に存在する場合には、ＯＰ１１０６は、認証フェーズ（ＡＰ）へ進むことができる。共有キー$K_0$が存在しない場合には、ＯＰ１１０６は、プロビジョニングフェーズを進めることができる。たとえば、ＯＰ１１０６は、ステップ１１１６へ進むことができる。
【０１１９】
１１１６において、ＯＰ１１０６は、ＲＰ１１０４とのアソシエーションを実行することができる。たとえば、ＯＰ１１０６は、アソシエーションハンドルＡおよび／または署名キーＳを生成することができる。署名キーＳは、アソシエーションハンドルＡの関数から生成されることが可能である。ＯＰ１１０６は、キー$K_{r,o}$を用いて署名キーＳを暗号化することができ、これは、たとえば$EK_{r,o}$（Ｓ）と呼ばれうる。ＯＰ１１０６は、アソシエーションハンドルＡおよび／または暗号化された署名キーＳをＲＰ１１０４へ送信することができる。１１１８において、ＲＰ１１０４は、ＵＥ１１０２をＯＰ１１０６へリダイレクトするメッセージ（たとえば、リダイレクトメッセージ）をＵＥ１１０２へ送信することができる。１１１８におけるメッセージは、ｓｅｓｓｉｏｎＩＤ、ｒｅｔｕｒｎＵＲＬ、ノンス、ログイン識別子（たとえば、ＯＩＤ）、および／またはアソシエーションハンドルＡなどのパラメータを含むことができる。１１２０において、ＵＥ１１０２は、ＲＰ１１０４から受信されたパラメータのうちの１つまたは複数を含むメッセージ（たとえば、ｈｔｔｐ　ＧＥＴ要求）をＯＰ１１０６へ送信することができる。たとえば、１１２０におけるメッセージは、ｓｅｓｓｉｏｎＩＤ、ｒｅｔｕｒｎＵＲＬ、ノンス、ログイン識別子（たとえば、ＯＩＤ）、および／またはアソシエーションハンドルを含むことができる。
【０１２０】
ＯＰ１１０６は、１１２２において、ＳＤ－ＡＶ（ＳＩＰ　ｄｉｇｅｓｔ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｖｅｃｔｏｒ）および／またはその他の情報をＨＳＳ１１０８から得ることができる。ＯＰ１１０６は、１１２４において、認証チャレンジをＵＥ１１０２へ送信することができる。ＵＥ１１０２は、１１２６において、共有キー$K_0$を生成することができる。ＵＥ１１０２はまた、１１２６において、認証応答を計算すること、および／またはその認証応答をＯＰ１１０６へ送信することが可能である。たとえば、認証応答は、事前にプロビジョンされたユーザクレデンシャル（たとえば、ユーザ名およびパスワード）を使用してＵＥ１１０２によって計算されることが可能である。１１２８において、ＯＰ１１０６は、たとえば受信された応答を、認証ベクトルＳＤ－ＡＶから計算された予想される応答と比較することなどによって、認証応答の妥当性を確認することができる。ＯＰ１１０６においてユーザ／ＵＥ１１０２が認証されると、ＯＰ１１０６は、共有シークレット$K_0$を生成することができ、この共有シークレット$K_0$は、ＵＥ１１０２とＯＰ１１０６との間において共有されることが可能である。$K_0$を用いた暗号化は、必ず正当な認証されたＵＥ１１０２が$UE_{Author}$を得るようにすることができ、$UE_{Author}$は、サービスに伴ってその後に使用するためのサービスアクセストークンであることが可能である。例示的な一実施形態においては、$K_0$は、乱数であることが可能であり、暗号関数を使用して生成されることが可能である。

【０１２１】
１１３０において、ＯＰ１１０６は、ユーザ／ＵＥ１１０２の認証が成功した旨を示す認証アサーションメッセージ$UE_{Assert}$に署名することができる。たとえば、ＯＰ１１０６は、署名キーＳを使用して$UE_{Assert}$に署名することができる。署名された$UE_{Assert}$は、$Sig_S(UE_{Assert})$と呼ばれうる。ＯＰ１１０６は、アソシエーションハンドルＡ、署名されたアサーション$UE_{Assert}$、および／または許可メッセージ$UE_{Author}$をＵＥ１１０２へ送信することができる。署名されたアサーション$UE_{Assert}$は、署名キーＳを用いて暗号化されることが可能であり、これは、たとえば$E_S(Sig_S(UE_{Assert}))$と呼ばれうる。許可メッセージ$UE_{Author}$は、共有キー$K_0$を用いて暗号化されることが可能であり、これは、たとえば$EK_0(UE_{Author})$と呼ばれうる。例示的な一実施形態においては、認証アサーションメッセージ$UE_{Assert}$に暗号化および署名の両方を行う代わりに、署名キーＳを使用して認証アサーションメッセージに署名するだけで十分である場合がある。アソシエーションハンドルＡ、$UE_{Assert}$、および／または$UE_{Author}$は、１１３２においてリダイレクトメッセージ内に含めて送信されることが可能であり、そのリダイレクトメッセージは、ＵＥ１１０２をＲＰ１１０４へリダイレクトすることができる。１１３４において、ＵＥ１１０２は、メッセージ（たとえば、ｈｔｔｐ　ＧＥＴ要求）をＲＰ１１０４へ送信することができ、そのメッセージは、アソシエーションハンドル、$E_S(Sig_S(UE_{Assert}))$、および／または$EK_0(UE_{Author})$を含むことができる。１１３６において、ＲＰ１１０４は、署名キーＳを復号すること、署名されたアサーション$Sig_S(UE_{Assert})$を復号すること、Ｓを使用してアサーション（たとえば、ＯｐｅｎＩＤアサーション）を検証すること、および／または暗号化された許可メッセージ$EK_0(UE_{Author})$を復号することが可能である。ＲＰ１１０４は、$EK_0(UE_{Author})$を含む通知を１１３８においてＵＥ１１０２へ送信することができる。$EK_0(UE_{Author})$は、ＲＰ１１０４が、正当なＲＰとして認証されており、不正なＲＰまたはその他のＭｉｔＭではないことをＵＥ１１０２に示すことができる。なぜなら、その通知は、$EK_0(UE_{Author})$を含むことができるためであり、不正なＲＰまたはその他のＭｉｔＭならば、その$EK_0(UE_{Author})$を復号することができないからである。

【０１２２】
図１１において示されているＲＰ認証は、本明細書に記載されているその他の実施形態において同様に実施されることが可能である。たとえば、図１１において示されている認証実施態様は、図２に示されている認証フェーズにおいて同様に実施されることが可能である。

【０１２３】
図１２は、本明細書に記載されている実施形態によるローカルアサーションプロバイダを用いた例示的な認証フェーズのメッセージフロー図を示している。図１２において示されているように、認証フェーズは、ＵＥ１２０２、ＲＰ１２０４、ＯＰ１２０６、および／またはＨＳＳ１２０８の間における通信を含むことができる。例示的な一実施形態においては、ＵＥ１２０２は、ローカル認証を実行して認証アサーション（たとえば、ＯｐｅｎＩＤ認証アサーション）に署名するためのローカルＯＰ機能$OP_{loc}$を含むことができ、その一方でＯＰ１２０６は、外部のＯＰであることが可能であり、そうした外部のＯＰは、たとえばネットワークに配置されることが可能である。ＵＥ１２０２は、１２１０においてログイン識別子（たとえばＯＩＤ）をＲＰ１２０４へ送信することができる。１２１２において、ＲＰ１２０４は、アソシエーション要求メッセージ（たとえば、ｈｔｔｐ　ＰＯＳＴ　ＯｐｅｎＩＤアソシエーション要求）をＯＰ１２０６へ送信することができる。このアソシエーション要求メッセージは、ＲＰ１２０４に対応するＲＰクレデンシャル$RP_{Cred}$を含むことができる。$RP_{Cred}$は、共有キー$K_{r,o}$を用いて暗号化されることが可能であり、共有キー$K_{r,o}$は、ＲＰ１２０４とＯＰ１２０６との間において共有されることが可能である。

【０１２４】
１２１４において、ＯＰ１２０６は、ＵＥ１２０２とＯＰ１２０６との間におけるセキュアな通信のためにこれらのエンティティーの間において共有される共有キー$K_0$がプロビジョンされているかどうかを判定することができる。共有キー$K_0$がプロビジョンされていない場合には、プロトコルは、共有キー$K_0$をプロビジョンするためのプロビジョニングフェーズへ進むことができる。共有キー$K_0$がプロビジョンされている場合には、プロトコルは、認証フェーズを進めることができる。例示的な一実施形態においては、ＯＰ１２０６は、共有キー$K_0$がプロビジョンされているかどうかを判定しない場合があり、プロトコルフローは、そのような判定を伴わずに続行することができる。
【０１２５】
１２１６において、ＯＰ１２０６は、ＲＰ１２０４とのアソシエーションを実行することができる。たとえば、ＯＰ１２０６は、アソシエーションハンドルＡおよび／または署名キー$K_1$を生成することができる。共有キー$K_1$は、たとえば共有キー$K_0$およびアソシエーションハンドルＡの関数から導出されることが可能である。共有キー$K_1$は、共有キー$K_{r,o}$を用いて暗号化されることが可能であり、これは、たとえば$EK_{r,o}$（$K_1$）と呼ばれうる。アソシエーションハンドルＡおよび暗号化されたキー$K_1$は、ＲＰ１２０４へ送信されることが可能である。ＲＰ１２０４は、ｓｅｓｓｉｏｎＩＤ、ｒｅｔｕｒｎＵＲＬ、ノンス、ログイン識別子（たとえば、ＯＩＤ）、および／またはアソシエーションハンドルＡなどのパラメータを含むメッセージを１２１８においてＵＥ１２０２へ送信することができる。１２１８におけるメッセージは、そのＵＥ１２０２を認証のためにＵＥ１２０２上の$OP_{loc}$（図示せず）へリダイレクトするリダイレクトメッセージであることが可能である。１２２０において、ＵＥ１２０２は、ローカル認証を実行することができる。ＵＥ１２０２は、１２２０において、共有キー$K_0$およびアソシエーションハンドルＡの関数を使用して、共有キー$K_1$を生成することができる。$K_0$を用いた暗号化は、必ず正当な認証されたＵＥ１２０２が$UE_{Author}$を得るようにすることができ、$UE_{Author}$は、サービスに伴ってその後に使用するためのサービスアクセストークンであることが可能である。ＵＥ１２０２は、共有キー$K_1$を用いて認証アサーションメッセージ$UE_{Assert}$に署名することができ、これは、$SigK_1$（$UE_{Assert}$）と呼ばれうる。ＵＥ１２０２は、（たとえば、ＵＥ１２０２上のローカルＯＰを使用して、）許可情報またはパラメータ$UE_{Author}$を生成することができる。ＵＥ１２０２は、共有キー$K_0$を用いて$UE_{Author}$を暗号化することができ、これは、たとえば$EK_0$（$UE_{Author}$）と呼ばれうる。ＵＥ１２０２は、共有キー$K_1$を用いて$SigK_1$（$UE_{Assert}$）および／または$EK_0$（$UE_{Author}$）を暗号化することができ（これは、$EK_1$（$SigK_1$（$UE_{Assert}$），$EK_0$（$UE_{Author}$））と呼ばれうる）、また、アソシエーションハンドルＡおよび$EK_1$（$SigK_1$（$UE_{Assert}$），$EK_0$（$UE_{Author}$））をＲＰ１２０４へ送信することができる。１２２２において示されているように、ＵＥ１２０２は、メッセージ（たとえば、ｈｔｔｐ　ＧＥＴ要求）を、署名されたアサーション$UE_{Assert}$とともにＲＰ１２０４へ送信することができる。
【０１２６】
ＲＰ１２０４は、１２２４において、共有キー$K_{r,o}$を使用して$K_1$を復号することができる。ＲＰ１２０４は、$SigK_1$（$UE_{Assert}$）を復号することができ、$K_1$を使用して認証アサーションメッセージ$UE_{Assert}$を検証することができる。１２２４において、ＲＰ１２０４は、$K_1$を使用して$EK_0$（$UE_{Author}$）を復号することができる。ＲＰ１２０４は、$UE_{Author}$を復号することができない場合がある。なぜなら、$UE_{Author}$は、ＵＥ１２０２とＯＰ１２０６との間において共有されている共有キー$K_0$によって暗号化されている場合があるためである。１２２６において、ＲＰ１２０４は、通知をＵＥ１２０２へ送信することができ、その通知は、ＲＰ１２０４が、ＵＥ１２０２が$K_1$を使用してセキュアチャネルを確立している相手の正当なＲＰであり、不正なＲＰまたはその他のＭｉｔＭではないことを示す。なぜなら、その通知

は、情報$EK_0$（$UE_{Author}$）を含むことができるためであり、不正なＲＰまたはその他のＭｉｔＭならば、その$EK_0$（$UE_{Author}$）を復号することができないからである。

【０１２７】

図１３Ａ～図１３Ｅは、本明細書に記載されている実施形態を実行する際に実施されることが可能である例示的なネットワークシステムおよびネットワークデバイスを示している。図１３Ａは、１つまたは複数の開示されている実施形態が実施されることが可能である例示的な通信システム１３００の図である。通信システム１３００は、コンテンツ、たとえば音声、データ、ビデオ、メッセージング、放送などを複数のワイヤレスユーザに提供するマルチプルアクセスシステムとすることができる。通信システム１３００は、複数のワイヤレスユーザが、ワイヤレス帯域幅を含むシステムリソースの共有を通じてそのようなコンテンツにアクセスすることを可能にすることができる。たとえば、通信システム１３００は、１つまたは複数のチャネルアクセス方法、たとえばＣＤＭＡ（ｃｏｄｅ ｄｉｖｉｓｉｏｎ ｍｕｌｔｉｐｌｅ ａｃｃｅｓｓ）、ＴＤＭＡ（ｔｉｍｅ ｄｉｖｉｓｉｏｎ ｍｕｌｔｉｐｌｅ ａｃｃｅｓｓ）、ＦＤＭＡ（ｆｒｅｑｕｅｎｃｙ ｄｉｖｉｓｉｏｎ ｍｕｌｔｉｐｌｅ ａｃｃｅｓｓ）、ＯＦＤＭＡ（ｏｒｔｈｏｇｏｎａｌ ＦＤＭＡ）、ＳＣ－ＦＤＭＡ（ｓｉｎｇｌｅ－ｃａｒｒｉｅｒ ＦＤＭＡ）などを採用することができる。

【０１２８】

図１３Ａにおいて示されているように、通信システム１３００は、ＷＴＲＵ（ｗｉｒｅｌｅｓｓ ｔｒａｎｓｍｉｔ／ｒｅｃｅｉｖｅ ｕｎｉｔ）１３０２ａ、１３０２ｂ、１３０２ｃ、１３０２ｄ、ＲＡＮ（ｒａｄｉｏ ａｃｃｅｓｓ ｎｅｔｗｏｒｋ）１３０４、コアネットワーク１３０６、ＰＳＴＮ（ｐｕｂｌｉｃ ｓｗｉｔｃｈｅｄ ｔｅｌｅｐｈｏｎｅ ｎｅｔｗｏｒｋ）１３０８、インターネット１３１０、およびその他のネットワーク１３１２を含むことができるが、開示されている実施形態では、任意の数のＷＴＲＵ、基地局、ネットワーク、および／またはネットワーク要素が考えられるということがわかるであろう。ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃ、１３０２ｄのそれぞれは、ワイヤレス環境において動作および／または通信を行うように構成されている任意のタイプのデバイスとすることができる。例として、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃ、１３０２ｄは、ワイヤレス信号を送信および／または受信するように構成されることが可能であり、ＵＥ（ユーザ装置：ｕｓｅｒ ｅｑｕｉｐｍｅｎｔ）、移動局、固定式または移動式のサブスクライバーユニット、ページャー、セルラー電話、ＰＤＡ（ｐｅｒｓｏｎａｌ ｄｉｇｉｔａｌ ａｓｓｉｓｔａｎｔ）、スマートフォン、ラップトップ、ネットブック、パーソナルコンピュータ、ワイヤレスセンサ、家庭用電化製品などを含むことができる。

【０１２９】

通信システム１３００は、基地局１３１４ａおよび基地局１３１４ｂを含むこともできる。基地局１３１４ａ、１３１４ｂのそれぞれは、コアネットワーク１３０６、インターネット１３１０、および／またはネットワーク１３１２などの１つまたは複数の通信ネットワークへのアクセスを容易にするために、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃ、１３０２ｄのうちの少なくとも１つとワイヤレスにインターフェースを取るように構成されている任意のタイプのデバイスとすることができる。例として、基地局１３１４ａ、１３１４ｂは、ＢＴＳ（ｂａｓｅ ｔｒａｎｓｃｅｉｖｅｒ ｓｔａｔｉｏｎ）、Ｎｏｄｅ－Ｂ、ｅＮｏｄｅ Ｂ、Ｈｏｍｅ Ｎｏｄｅ Ｂ、Ｈｏｍｅ ｅＮｏｄｅ Ｂ、サイトコントローラ、ＡＰ（ａｃｃｅｓｓ ｐｏｉｎｔ）、ワイヤレスルータなどとすることができる。基地局１３１４ａ、１３１４ｂは、それぞれ単一の要素として示されているが、基地局１３１４ａ、１３１４ｂは、任意の数の相互接続された基地局および／またはネットワーク要素を含むことができるということがわかるであろう。

【０１３０】

基地局１３１４ａは、ＲＡＮ１３０４の一部とすることができ、ＲＡＮ１３０４は、そ

の他の基地局および／またはネットワーク要素（図示せず）、たとえばＢＳＣ（ｂａｓｅ ｓｔａｔｉｏｎ ｃｏｎｔｒｏｌｌｅｒ）、ＲＮＣ（ｒａｄｉｏ ｎｅｔｗｏｒｋ ｃｏｎｔｒｏｌｌｅｒ）、中継ノードなどを含むこともできる。基地局１３１４ａおよび／または基地局１３１４ｂは、特定の地理的領域内でワイヤレス信号を送信および／または受信するように構成されることが可能であり、この地理的領域は、セル（図示せず）と呼ばれることもある。セルは、複数のセルセクタへとさらに分割されることが可能である。たとえば、基地局１３１４ａに関連付けられているセルは、３つのセクタへと分割されることが可能である。したがって一実施形態においては、基地局１３１４ａは、３つのトランシーバ、すなわち、セルのそれぞれのセクタごとに１つのトランシーバを含むことができる。別の実施形態においては、基地局１３１４ａは、ＭＩＭＯ（ｍｕｌｔｉｐｌｅ－ｉｎｐｕｔ ｍｕｌｔｉｐｌｅ ｏｕｔｐｕｔ）テクノロジーを採用することができ、したがって、セルのそれぞれのセクタごとに複数のトランシーバを利用することができる。

【０１３１】

基地局１３１４ａ、１３１４ｂは、エアインターフェース１３１６を介してＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃ、１３０２ｄのうちの１つまたは複数と通信することができ、エアインターフェース１３１６は、任意の適切なワイヤレス通信リンク（たとえば、ＲＦ（ｒａｄｉｏ ｆｒｅｑｕｅｎｃｙ）、マイクロ波、ＩＲ（ｉｎｆｒａｒｅｄ）、ＵＶ（ｕｌｔｒａｖｉｏｌｅｔ）、可視光など）とすることができる。エアインターフェース１３１６は、任意の適切なＲＡＴ（ｒａｄｉｏ ａｃｃｅｓｓ ｔｅｃｈｎｏｌｏｇｙ）を使用して確立されることが可能である。

【０１３２】

より具体的には、上述したように、通信システム１３００は、マルチプルアクセスシステムとすることができ、１つまたは複数のチャネルアクセススキーム、たとえばＣＤＭＡ、ＴＤＭＡ、ＦＤＭＡ、ＯＦＤＭＡ、ＳＣ－ＦＤＭＡなどを採用することができる。たとえば、ＲＡＮ１３０４内の基地局１３１４ａおよびＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃは、ＵＴＲＡ（ＵＭＴＳ（Ｕｎｉｖｅｒｓａｌ Ｍｏｂｉｌｅ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｓｙｓｔｅｍ） Ｔｅｒｒｅｓｔｒｉａｌ Ｒａｄｉｏ Ａｃｃｅｓｓ）などの無線テクノロジーを実施することができ、この無線テクノロジーは、ＷＣＤＭＡ（登録商標）（ｗｉｄｅｂａｎｄ ＣＤＭＡ）を使用してエアインターフェース１３１６を確立することができる。ＷＣＤＭＡは、ＨＳＰＡ（Ｈｉｇｈ－Ｓｐｅｅｄ Ｐａｃｋｅｔ Ａｃｃｅｓｓ）および／またはＨＳＰＡ＋（Ｅｖｏｌｖｅｄ ＨＳＰＡ）などの通信プロトコルを含むことができる。ＨＳＰＡは、ＨＳＤＰＡ（Ｈｉｇｈ－Ｓｐｅｅｄ Ｄｏｗｎｌｉｎｋ Ｐａｃｋｅｔ Ａｃｃｅｓｓ）および／またはＨＳＵＰＡ（Ｈｉｇｈ－Ｓｐｅｅｄ Ｕｐｌｉｎｋ Ｐａｃｋｅｔ Ａｃｃｅｓｓ）を含むことができる。

【０１３３】

別の実施形態においては、基地局１３１４ａおよびＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃは、Ｅ－ＵＴＲＡ（Ｅｖｏｌｖｅｄ ＵＭＴＳ Ｔｅｒｒｅｓｔｒｉａｌ Ｒａｄｉｏ Ａｃｃｅｓｓ）などの無線テクノロジーを実施することができ、この無線テクノロジーは、ＬＴＥ（Ｌｏｎｇ Ｔｅｒｍ Ｅｖｏｌｕｔｉｏｎ）および／またはＬＴＥ－Ａ（ＬＴＥ－Ａｄｖａｎｃｅｄ）を使用してエアインターフェース１３１６を確立することができる。

【０１３４】

その他の実施形態においては、基地局１３１４ａおよびＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃは、無線テクノロジー、たとえばＩＥＥＥ ８０２．１６（すなわちＷｉＭＡＸ（Ｗｏｒｌｄｗｉｄｅ Ｉｎｔｅｒｏｐｅｒａｂｉｌｉｔｙ ｆｏｒ Ｍｉｃｒｏｗａｖｅ Ａｃｃｅｓｓ））、ＣＤＭＡ２０００、ＣＤＭＡ２０００ １Ｘ、ＣＤＭＡ２０００ ＥＶ－ＤＯ、ＩＳ－２０００（Ｉｎｔｅｒｉｍ Ｓｔａｎｄａｒｄ ２０００）、ＩＳ－９５（Ｉｎｔｅｒｉｍ Ｓｔａｎｄａｒｄ ９５）、ＩＳ－８５６（Ｉｎｔｅｒｉｍ Ｓｔａｎｄａｒｄ ８５６）、ＧＳＭ（登録商標）（Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ ｃｏｍｍｕｎｉｃａｔｉｏｎｓ）、ＥＤＧＥ（Ｅｎｈａｎｃｅ

ｄ Ｄａｔａ ｒａｔｅｓ ｆｏｒ ＧＳＭ Ｅｖｏｌｕｔｉｏｎ）、ＧＥＲＡＮ（ＧＳＭ ＥＤＧＥ）などを実施することができる。

【０１３５】

図１３Ａにおける基地局１３１４ｂは、たとえばワイヤレスルータ、Ｈｏｍｅ ＮｏｄｅＢ、Ｈｏｍｅ ｅＮｏｄｅ Ｂ、またはアクセスポイントとすることができ、局所的なエリア、たとえば事業所、家庭、乗り物、キャンパスなどにおけるワイヤレス接続を容易にするために、任意の適切なＲＡＴを利用することができる。一実施形態においては、基地局１３１４ｂおよびＷＴＲＵ１３０２ｃ、１３０２ｄは、ＷＬＡＮ（ｗｉｒｅｌｅｓｓ ｌｏｃａｌ ａｒｅａ ｎｅｔｗｏｒｋ）を確立するために、ＩＥＥＥ ８０２．１１などの無線テクノロジーを実施することができる。別の実施形態においては、基地局１３１４ｂおよびＷＴＲＵ１３０２ｃ、１３０２ｄは、ＷＰＡＮ（ｗｉｒｅｌｅｓｓ ｐｅｒｓｏｎａｌ ａｒｅａ ｎｅｔｗｏｒｋ）を確立するために、ＩＥＥＥ ８０２．１５などの無線テクノロジーを実施することができる。さらに別の実施形態においては、基地局１３１４ｂおよびＷＴＲＵ１３０２ｃ、１３０２ｄは、ピコセルまたはフェムトセルを確立するために、セルラーベースのＲＡＴ（たとえば、ＷＣＤＭＡ、ＣＤＭＡ２０００、ＧＳＭ、ＬＴＥ、ＬＴＥ－Ａなど）を利用することができる。図１３Ａにおいて示されているように、基地局１３１４ｂは、インターネット１３１０への直接接続を有することができる。したがって、基地局１３１４ｂは、コアネットワーク１３０６を介してインターネット１３１０にアクセスすることを求められないことが可能である。

【０１３６】

ＲＡＮ１３０４は、コアネットワーク１３０６と通信状態にあることが可能であり、コアネットワーク１３０６は、音声、データ、アプリケーション、および／またはＶｏＩＰ（ｖｏｉｃｅ ｏｖｅｒ ｉｎｔｅｒｎｅｔ ｐｒｏｔｏｃｏｌ）サービスをＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃ、１３０２ｄのうちの１つまたは複数に提供するように構成されている任意のタイプのネットワークとすることができる。たとえば、コアネットワーク１３０６は、コール制御、課金サービス、モバイルロケーションベースサービス、プリペイドコーリング、インターネット接続、ビデオ配信などを提供すること、および／またはユーザ認証などのハイレベルセキュリティー機能を実行することが可能である。図１３Ａにおいては示されていないが、ＲＡＮ１３０４および／またはコアネットワーク１３０６は、ＲＡＮ１３０４と同じＲＡＴまたは異なるＲＡＴを採用しているその他のＲＡＮと直接または間接の通信状態にあることが可能であるということがわかるであろう。たとえば、コアネットワーク１３０６は、Ｅ－ＵＴＲＡ無線テクノロジーを利用している可能性があるＲＡＮ１３０４に接続されていることに加えて、ＧＳＭ無線テクノロジーを採用している別のＲＡＮ（図示せず）と通信状態にあることも可能である。

【０１３７】

コアネットワーク１３０６は、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃ、１３０２ｄがＰＳＴＮ１３０８、インターネット１３１０、および／またはその他のネットワーク１３１２にアクセスするためのゲートウェイとして機能することもできる。ＰＳＴＮ１３０８は、ＰＯＴＳ（ｐｌａｉｎ ｏｌｄ ｔｅｌｅｐｈｏｎｅ ｓｅｒｖｉｃｅ）を提供する回路交換電話ネットワークを含むことができる。インターネット１３１０は、ＴＣＰ／ＩＰインターネットプロトコルスイートにおけるＴＣＰ（ｔｒａｎｓｍｉｓｓｉｏｎ ｃｏｎｔｒｏｌ ｐｒｏｔｏｃｏｌ）、ＵＤＰ（ｕｓｅｒ ｄａｔａｇｒａｍ ｐｒｏｔｏｃｏｌ）、およびＩＰ（ｉｎｔｅｒｎｅｔ ｐｒｏｔｏｃｏｌ）など、共通の通信プロトコルを使用する相互接続されたコンピュータネットワークおよびデバイスからなるグローバルシステムを含むことができる。ネットワーク１３１２は、その他のサービスプロバイダによって所有および／または運営されている有線またはワイヤレスの通信ネットワークを含むことができる。たとえば、ネットワーク１３１２は、ＲＡＮ１３０４と同じＲＡＴまたは異なるＲＡＴを採用している可能性がある１つまたは複数のＲＡＮに接続されている別のコアネットワークを含むことができる。

【０１３８】

通信システム１３００内のＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃ、１３０２ｄのうちのいくつかまたはすべては、マルチモード機能を含むことができ、すなわち、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃ、１３０２ｄは、別々のワイヤレスリンクを介して別々のワイヤレスネットワークと通信するために複数のトランシーバを含むことができる。たとえば、図１３Ａにおいて示されているＷＴＲＵ１３０２ｃは、セルラーベースの無線テクノロジーを採用している可能性がある基地局１３１４ａ、およびＩＥＥＥ　８０２無線テクノロジーを採用している可能性がある基地局１３１４ｂと通信するように構成されることが可能である。

【０１３９】

図１３Ｂは、例示的なＷＴＲＵ１３０２のシステム図である。図１３Ｂにおいて示されているように、ＷＴＲＵ１３０２は、プロセッサ１３１８、トランシーバ１３２０、送信／受信要素１３２２、スピーカー／マイクロフォン１３２４、キーパッド１３２６、ディスプレイ／タッチパッド１３２８、非リムーバブルメモリ１３３０、リムーバブルメモリ１３３２、電源１３３４、ＧＰＳ（ｇｌｏｂａｌ　ｐｏｓｉｔｉｏｎｉｎｇ　ｓｙｓｔｅｍ）チップセット１３３６、およびその他の周辺機器１３３８を含むことができる。ＷＴＲＵ１３０２は、一実施形態との整合性を保持しながら、上述の要素どうしの任意の下位組合せを含むことができるということがわかるであろう。

【０１４０】

プロセッサ１３１８は、汎用プロセッサ、専用プロセッサ、従来型プロセッサ、ＤＳＰ（ｄｉｇｉｔａｌ　ｓｉｇｎａｌ　ｐｒｏｃｅｓｓｏｒ）、複数のマイクロプロセッサ、ＤＳＰコアと関連付けられている１つもしくは複数のマイクロプロセッサ、コントローラ、マイクロコントローラ、ＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｐｅｃｉｆｉｃ　Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）、ＦＰＧＡ（Ｆｉｅｌｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）回路、その他の任意のタイプのＩＣ（ｉｎｔｅｇｒａｔｅｄ　ｃｉｒｃｕｉｔ）、状態マシンなどとすることができる。プロセッサ１３１８は、信号コーディング、データ処理、電力制御、入力／出力処理、および／またはＷＴＲＵ１３０２をワイヤレス環境内で機能できるようにするその他の任意の機能を実行することができる。プロセッサ１３１８は、トランシーバ１３２０に結合されることが可能であり、トランシーバ１３２０は、送信／受信要素１３２２に結合されることが可能である。図１３Ｂは、プロセッサ１３１８とトランシーバ１３２０を別々のコンポーネントとして示しているが、プロセッサ１３１８とトランシーバ１３２０は、１つの電子パッケージまたはチップ内に統合されることが可能であるということがわかるであろう。

【０１４１】

送信／受信要素１３２２は、エアインターフェース１３１６を介して、基地局（たとえば、基地局１３１４ａ）に信号を送信するように、または基地局（たとえば、基地局１３１４ａ）から信号を受信するように構成されることが可能である。たとえば、一実施形態においては、送信／受信要素１３２２は、ＲＦ信号を送信および／または受信するように構成されているアンテナとすることができる。別の実施形態においては、送信／受信要素１３２２は、たとえば、ＩＲ信号、ＵＶ信号、または可視光信号を送信および／または受信するように構成されているエミッタ／検知器とすることができる。さらに別の実施形態においては、送信／受信要素１３２２は、ＲＦ信号と光信号との両方を送信および受信するように構成されることが可能である。送信／受信要素１３２２は、ワイヤレス信号の任意の組合せを送信および／または受信するように構成されることが可能であるということがわかるであろう。

【０１４２】

加えて、送信／受信要素１３２２は、図１３Ｂにおいては単一の要素として示されているが、ＷＴＲＵ１３０２は、任意の数の送信／受信要素１３２２を含むことができる。より具体的には、ＷＴＲＵ１３０２は、ＭＩＭＯテクノロジーを採用することができる。したがって、一実施形態においては、ＷＴＲＵ１３０２は、エアインターフェース１３１６を介してワイヤレス信号を送信および受信するために、複数の送信／受信要素１３２２（

たとえば、複数のアンテナ）を含むことができる。

【０１４３】

トランシーバ１３２０は、送信／受信要素１３２２によって送信される信号を変調するように、また、送信／受信要素１３２２によって受信される信号を復調するように構成されることが可能である。上述したように、ＷＴＲＵ１３０２は、マルチモード機能を有することができる。したがってトランシーバ１３２０は、ＷＴＲＵ１３０２が、たとえばＵＴＲＡおよびＩＥＥＥ　８０２．１１など、複数のＲＡＴを介して通信できるようにするために複数のトランシーバを含むことができる。

【０１４４】

ＷＴＲＵ１３０２のプロセッサ１３１８は、スピーカー／マイクロフォン１３２４、キーパッド１３２６、および／またはディスプレイ／タッチパッド１３２８（たとえば、ＬＣＤ（ｌｉｑｕｉｄ　ｃｒｙｓｔａｌ　ｄｉｓｐｌａｙ）ディスプレイユニットまたはＯＬＥＤ（ｏｒｇａｎｉｃ　ｌｉｇｈｔ－ｅｍｉｔｔｉｎｇ　ｄｉｏｄｅ）ディスプレイユニット）に結合されることが可能であり、そこからユーザ入力データを受け取ることができる。プロセッサ１３１８は、ユーザデータをスピーカー／マイクロフォン１３２４、キーパッド１３２６、および／またはディスプレイ／タッチパッド１３２８へ出力することもできる。加えて、プロセッサ１３１８は、非リムーバブルメモリ１３３０および／またはリムーバブルメモリ１３３２など、任意のタイプの適切なメモリからの情報にアクセスすること、およびそれらのメモリにデータを格納することが可能である。非リムーバブルメモリ１３３０は、ＲＡＭ（ｒａｎｄｏｍ－ａｃｃｅｓｓ　ｍｅｍｏｒｙ）、ＲＯＭ（ｒｅａｄ－ｏｎｌｙ　ｍｅｍｏｒｙ）、ハードディスク、またはその他の任意のタイプのメモリストレージデバイスを含むことができる。リムーバブルメモリ１３３２は、ＧＳＭ　ＳＩＭ（Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｔｙ　Ｍｏｄｕｌｅ）カード、ＵＩＣＣ（すなわち、ＳＩＭカードのＵＭＴＳバージョン）、メモリスティック、ＳＤ（ｓｅｃｕｒｅ　ｄｉｇｉｔａｌ）メモリカードなどを含むことができる。その他の実施形態においては、プロセッサ１３１８は、サーバまたはホームコンピュータ（図示せず）上など、ＷＴＲＵ１３０２上に物理的に配置されていないメモリからの情報にアクセスすること、およびそのメモリにデータを格納することが可能である。

【０１４５】

プロセッサ１３１８は、電源１３３４から電力を受け取ることができ、また、ＷＴＲＵ１３０２内のその他のコンポーネントへの電力を分配および／または制御するように構成されることが可能である。電源１３３４は、ＷＴＲＵ１３０２に電力供給するための任意の適切なデバイスとすることができる。たとえば、電源１３３４は、１つまたは複数の乾電池（たとえばＮｉＣｄ（ｎｉｃｋｅｌ－ｃａｄｍｉｕｍ）、ＮｉＺｎ（ｎｉｃｋｅｌ－ｚｉｎｃ）、ＮｉＭＨ（ｎｉｃｋｅｌ　ｍｅｔａｌ　ｈｙｄｒｉｄｅ）、Ｌｉ－ｉｏｎ（ｌｉｔｈｉｕｍ－ｉｏｎ）など）、太陽電池、燃料電池などを含むことができる。

【０１４６】

プロセッサ１３１８は、ＧＰＳチップセット１３３６に結合されることも可能であり、ＧＰＳチップセット１３３６は、ＷＴＲＵ１３０２の現在位置に関する位置情報（たとえば、経度および緯度）を提供するように構成されることが可能である。ＧＰＳチップセット１３３６からの情報に加えて、またはその情報の代わりに、ＷＴＲＵ１３０２は、基地局（たとえば、基地局１３１４ａ、１３１４ｂ）からエアインターフェース１３１６を介して位置情報を受信すること、および／または複数の近隣の基地局から受信されている信号のタイミングに基づいて自分の位置を特定することが可能である。ＷＴＲＵ１３０２は、一実施形態との整合性を保持しながら、任意の適切な位置特定方法を通じて位置情報を得ることができるということがわかるであろう。

【０１４７】

プロセッサ１３１８は、その他の周辺機器１３３８にさらに結合されることが可能であり、その他の周辺機器１３３８は、さらなる特徴、機能、および／または有線接続もしくはワイヤレス接続を提供する１つまたは複数のソフトウェアモジュールおよび／またはハ

ードウェアモジュールを含むことができる。たとえば、周辺機器１３３８は、加速度計、ｅ－コンパス、衛星トランシーバ、デジタルカメラ（写真またはビデオ用）、ＵＳＢ（ｕｎｉｖｅｒｓａｌ　ｓｅｒｉａｌ　ｂｕｓ）ポート、振動デバイス、テレビジョントランシーバ、ハンドフリーヘッドセット、ＢＬＵＥＴＯＯＴＨ（登録商標）モジュール、ＦＭ（ｆｒｅｑｕｅｎｃｙ　ｍｏｄｕｌａｔｅｄ）ラジオユニット、デジタルミュージックプレーヤ、メディアプレーヤ、ビデオゲームプレーヤモジュール、インターネットブラウザなどを含むことができる。

【０１４８】

図１３Ｃは、一実施形態によるＲＡＮ１３０４およびコアネットワーク１３０６のシステム図である。上述したように、ＲＡＮ１３０４は、エアインターフェース１３１６を介してＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃと通信するためにＵＴＲＡ無線テクノロジーを採用することができる。ＲＡＮ１３０４は、コアネットワーク１３０６と通信状態にあることも可能である。図１３Ｃにおいて示されているように、ＲＡＮ１３０４は、Ｎｏｄｅ－Ｂ１３４０ａ、１３４０ｂ、１３４０ｃを含むことができ、これらのＮｏｄｅ－Ｂはそれぞれ、エアインターフェース１３１６を介してＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃと通信するために１つまたは複数のトランシーバを含むことができる。Ｎｏｄｅ－Ｂ１３４０ａ、１３４０ｂ、１３４０ｃはそれぞれ、ＲＡＮ１３０４内の特定のセル（図示せず）に関連付けられることが可能である。ＲＡＮ１３０４は、ＲＮＣ１３４２ａ、１３４２ｂを含むこともできる。ＲＡＮ１３０４は、一実施形態との整合性を保持しながら、任意の数のＮｏｄｅ－ＢおよびＲＮＣを含むことができるということがわかるであろう。

【０１４９】

図１３Ｃにおいて示されているように、Ｎｏｄｅ－Ｂ１３４０ａ、１３４０ｂは、ＲＮＣ１３４２ａと通信状態にあることが可能である。加えて、Ｎｏｄｅ－Ｂ１３４０ｃは、ＲＮＣ１３４２ｂと通信状態にあることが可能である。Ｎｏｄｅ－Ｂ１３４０ａ、１３４０ｂ、１３４０ｃは、Ｉｕｂインターフェースを介してそれぞれのＲＮＣ１３４２ａ、１３４２ｂと通信することができる。ＲＮＣ１３４２ａ、１３４２ｂは、Ｉｕｒインターフェースを介して互いに通信状態にあることが可能である。ＲＮＣ１３４２ａ、１３４２ｂのそれぞれは、自分が接続されているそれぞれのＮｏｄｅ－Ｂ１３４０ａ、１３４０ｂ、１３４０ｃを制御するように構成されることが可能である。加えて、ＲＮＣ１３４２ａ、１３４２ｂのそれぞれは、その他の機能、たとえば、アウターループ電力制御、負荷制御、アドミッション制御、パケットスケジューリング、ハンドオーバ制御、マクロダイバーシティー、セキュリティー機能、データ暗号化などを実行またはサポートするように構成されることが可能である。

【０１５０】

図１３Ｃにおいて示されているコアネットワーク１３０６は、ＭＧＷ（ｍｅｄｉａ　ｇａｔｅｗａｙ）１３４４、ＭＳＣ（ｍｏｂｉｌｅ　ｓｗｉｔｃｈｉｎｇ　ｃｅｎｔｅｒ）１３４６、ＳＧＳＮ（ｓｅｒｖｉｎｇ　ＧＰＲＳ　ｓｕｐｐｏｒｔ　ｎｏｄｅ）１３４８、および／またはＧＧＳＮ（ｇａｔｅｗａｙ　ＧＰＲＳ　ｓｕｐｐｏｒｔ　ｎｏｄｅ）１３５０を含むことができる。上述の要素のうちのそれぞれは、コアネットワーク１３０６の一部として示されているが、これらの要素のいずれかが、コアネットワークオペレータ以外のエンティティーによって所有および／または運営されることも可能であるということがわかるであろう。

【０１５１】

ＲＡＮ１３０４内のＲＮＣ１３４２ａは、ＩｕＣＳインターフェースを介してコアネットワーク１３０６内のＭＳＣ１３４６に接続されることが可能である。ＭＳＣ１３４６は、ＭＧＷ１３４４に接続されることが可能である。ＭＳＣ１３４６およびＭＧＷ１３４４は、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃと、従来の地上通信線の通信デバイスとの間における通信を容易にするために、ＰＳＴＮ１３０８などの回路交換ネットワークへのアクセスをＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃに提供することができる。

【０１５２】
ＲＡＮ１３０４内のＲＮＣ１３４２ａは、ＩｕＰＳインターフェースを介してコアネットワーク１３０６内のＳＧＳＮ１３４８に接続されることも可能である。ＳＧＳＮ１３４８は、ＧＧＳＮ１３５０に接続されることが可能である。ＳＧＳＮ１３４８およびＧＧＳＮ１３５０は、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃと、ＩＰ対応デバイスとの間における通信を容易にするために、インターネット１３１０などのパケット交換ネットワークへのアクセスをＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃに提供することができる。
【０１５３】
上述したように、コアネットワーク１３０６は、ネットワーク１３１２に接続されることも可能であり、ネットワーク１３１２は、その他のサービスプロバイダによって所有および／または運営されているその他の有線またはワイヤレスのネットワークを含むことができる。
【０１５４】
図１３Ｄは、一実施形態によるＲＡＮ１３０４およびコアネットワーク１３０６のシステム図である。上述したように、ＲＡＮ１３０４は、エアインターフェース１３１６を介してＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃと通信するためにＥ－ＵＴＲＡ無線テクノロジーを採用することができる。ＲＡＮ１３０４は、コアネットワーク１３０６と通信状態にあることも可能である。
【０１５５】
ＲＡＮ１３０４は、ｅＮｏｄｅ－Ｂ１３４０ａ、１３４０ｂ、１３４０ｃを含むことができるが、ＲＡＮ１３０４は、一実施形態との整合性を保持しながら、任意の数のｅＮｏｄｅ－Ｂを含むことができるということがわかるであろう。ｅＮｏｄｅ－Ｂ１３４０ａ、１３４０ｂ、１３４０ｃはそれぞれ、エアインターフェース１３１６を介してＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃと通信するために１つまたは複数のトランシーバを含むことができる。一実施形態においては、ｅＮｏｄｅ－Ｂ１３４０ａ、１３４０ｂ、１３４０ｃは、ＭＩＭＯテクノロジーを実施することができる。したがって、ｅＮｏｄｅ－Ｂ１３４０ａは、たとえば、ＷＴＲＵ１３０２ａにワイヤレス信号を送信するために、およびＷＴＲＵ１３０２ａからワイヤレス信号を受信するために、複数のアンテナを使用することができる。
【０１５６】
ｅＮｏｄｅ－Ｂ１３４０ａ、１３４０ｂ、１３４０ｃのそれぞれは、特定のセル（図示せず）に関連付けられることが可能であり、無線リソースマネージメントの決定、ハンドオーバの決定、アップリンクおよび／またはダウンリンクにおけるユーザのスケジューリングなどを取り扱うように構成されることが可能である。図１３Ｄにおいて示されているように、ｅＮｏｄｅ－Ｂ１３４０ａ、１３４０ｂ、１３４０ｃは、Ｘ２インターフェースを介して互いに通信することができる。
【０１５７】
図１３Ｄにおいて示されているコアネットワーク１３０６は、ＭＭＥ（ｍｏｂｉｌｉｔｙ ｍａｎａｇｅｍｅｎｔ ｇａｔｅｗａｙ）１３６０、サービングゲートウェイ１３６２、および／またはＰＤＮ（ｐａｃｋｅｔ ｄａｔａ ｎｅｔｗｏｒｋ）ゲートウェイ１３６４を含むことができる。上述の要素のうちのそれぞれは、コアネットワーク１３０６の一部として示されているが、これらの要素のいずれかが、コアネットワークオペレータ以外のエンティティーによって所有および／または運営されることも可能であるということがわかるであろう。
【０１５８】
ＭＭＥ１３６０は、Ｓ１インターフェースを介してＲＡＮ１３０４内のｅＮｏｄｅ－Ｂ１３４０ａ、１３４０ｂ、１３４０ｃのそれぞれに接続されることが可能であり、コントロールノードとして機能することができる。たとえば、ＭＭＥ１３６０は、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃのユーザを認証すること、ベアラのアクティブ化／非ア

クティブ化、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃの最初の接続中に特定のサービングゲートウェイを選択することなどを担当することができる。ＭＭＥ１３６０は、ＲＡＮ１３０４と、ＧＳＭまたはＷＣＤＭＡなどのその他の無線テクノロジーを採用しているその他のＲＡＮ（図示せず）との間における切り替えを行うためのコントロールプレーン機能を提供することもできる。

【０１５９】

サービングゲートウェイ１３６２は、Ｓ１インターフェースを介してＲＡＮ１３０４内のｅＮｏｄｅ　Ｂ１３４０ａ、１３４０ｂ、１３４０ｃのそれぞれに接続されることが可能である。サービングゲートウェイ１３６２は一般に、ユーザデータパケットをＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃへ／ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃから回送および転送することができる。サービングゲートウェイ１３６２は、その他の機能、たとえば、ｅＮｏｄｅ　Ｂ間でのハンドオーバ中にユーザプレーンを固定すること、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃにとってダウンリンクデータが利用可能である場合にページングをトリガーすること、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃのコンテキストを管理および記憶することなどを実行することもできる。

【０１６０】

サービングゲートウェイ１３６２は、ＰＤＮゲートウェイ１３６４に接続されることも可能であり、ＰＤＮゲートウェイ１３６４は、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃと、ＩＰ対応デバイスとの間における通信を容易にするために、インターネット１３１０などのパケット交換ネットワークへのアクセスをＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃに提供することができる。

【０１６１】

コアネットワーク１３０６は、その他のネットワークとの通信を容易にすることができる。たとえば、コアネットワーク１３０６は、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃと、従来の地上通信線の通信デバイスとの間における通信を容易にするために、ＰＳＴＮ１３０８などの回路交換ネットワークへのアクセスをＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃに提供することができる。たとえば、コアネットワーク１３０６は、コアネットワーク１３０６とＰＳＴＮ１３０８との間におけるインターフェースとして機能するＩＰゲートウェイ（たとえば、ＩＭＳ（ＩＰ　ｍｕｌｔｉｍｅｄｉａ　ｓｕｂｓｙｓｔｅｍ）サーバ）を含むことができ、またはそうしたＩＰゲートウェイと通信することができる。加えて、コアネットワーク１３０６は、ネットワーク１３１２へのアクセスをＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃに提供することができ、ネットワーク１３１２は、その他のサービスプロバイダによって所有および／または運営されているその他の有線またはワイヤレスのネットワークを含むことができる。

【０１６２】

図１３Ｅは、一実施形態によるＲＡＮ１３０４およびコアネットワーク１３０６のシステム図である。ＲＡＮ１３０４は、エアインターフェース１３１６を介してＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃと通信するためにＩＥＥＥ８０２．１６無線テクノロジーを採用しているＡＳＮ（ａｃｃｅｓｓ　ｓｅｒｖｉｃｅ　ｎｅｔｗｏｒｋ）とすることができる。以降でさらに論じるように、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃ、ＲＡＮ１３０４、およびコアネットワーク１３０６という別々の機能エンティティーの間における通信リンクは、リファレンスポイントとして定義されることが可能である。

【０１６３】

図１３Ｅにおいて示されているように、ＲＡＮ１３０４は、基地局１３４０ａ、１３４０ｂ、１３４０ｃ、およびＡＳＮゲートウェイ１３７０を含むことができるが、ＲＡＮ１３０４は、一実施形態との整合性を保持しながら、任意の数の基地局およびＡＳＮゲートウェイを含むことができるということがわかるであろう。基地局１３４０ａ、１３４０ｂ、１３４０ｃは、ＲＡＮ１３０４内の特定のセル（図示せず）にそれぞれ関連付けられることが可能であり、エアインターフェース１３１６を介してＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃと通信するために１つまたは複数のトランシーバをそれぞれ含むことが

できる。一実施形態においては、基地局１３４０ａ、１３４０ｂ、１３４０ｃは、ＭＩＭＯテクノロジーを実施することができる。したがって、基地局１３４０ａは、たとえば、ＷＴＲＵ１３０２ａにワイヤレス信号を送信するために、およびＷＴＲＵ１３０２ａからワイヤレス信号を受信するために、複数のアンテナを使用することができる。基地局１３４０ａ、１３４０ｂ、１３４０ｃは、モビリティーマネージメント機能、たとえば、ハンドオフのトリガリング、トンネルの確立、無線リソースマネージメント、トラフィックの分類、ＱｏＳ（ｑｕａｌｉｔｙ　ｏｆ　ｓｅｒｖｉｃｅ）ポリシーの実施などを提供することもできる。ＡＳＮゲートウェイ１３７０は、トラフィックアグリゲーションポイントとして機能することができ、ページング、サブスクライバープロファイルのキャッシング、コアネットワーク１３０６へのルーティングなどを担当することができる。

【０１６４】

ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃと、ＲＡＮ１３０４との間におけるエアインターフェース１３１６は、ＩＥＥＥ８０２．１６仕様を実施するＲ１リファレンスポイントとして定義されることが可能である。加えて、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃのそれぞれは、コアネットワーク１３０６との論理インターフェース（図示せず）を確立することができる。ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃと、コアネットワーク１３０６との間における論理インターフェースは、Ｒ２リファレンスポイントとして定義されることが可能であり、このＲ２リファレンスポイントは、認証、許可、ＩＰホスト構成マネージメント、および／またはモビリティーマネージメントのために使用されることが可能である。

【０１６５】

基地局１３４０ａ、１３４０ｂ、１３４０ｃのそれぞれの間における通信リンクは、ＷＴＲＵのハンドオーバ、および基地局どうしの間におけるデータの転送を容易にするためのプロトコルを含むＲ８リファレンスポイントとして定義されることが可能である。基地局１３４０ａ、１３４０ｂ、１３４０ｃと、ＡＳＮゲートウェイ１３７０との間における通信リンクは、Ｒ６リファレンスポイントとして定義されることが可能である。このＲ６リファレンスポイントは、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃのそれぞれに関連付けられているモビリティーイベントに基づいてモビリティーマネージメントを容易にするためのプロトコルを含むことができる。

【０１６６】

図１３Ｅにおいて示されているように、ＲＡＮ１３０４は、コアネットワーク１３０６に接続されることが可能である。ＲＡＮ１３０４と、コアネットワーク１３０６との間における通信リンクは、たとえば、データ転送およびモビリティーマネージメント機能を容易にするためのプロトコルを含むＲ３リファレンスポイントとして定義されることが可能である。コアネットワーク１３０６は、ＭＩＰ－ＨＡ（ｍｏｂｉｌｅ　ＩＰ　ｈｏｍｅ　ａｇｅｎｔ）１３７２、ＡＡＡ（ａｕｔｈｅｎｔｉｃａｔｉｏｎ，　ａｕｔｈｏｒｉｚａｔｉｏｎ，　ａｃｃｏｕｎｔｉｎｇ）サーバ１３７４、およびゲートウェイ１３７６を含むことができる。上述の要素のうちのそれぞれは、コアネットワーク１３０６の一部として示されているが、これらの要素のいずれかが、コアネットワークオペレータ以外のエンティティーによって所有および／または運営されることも可能であるということがわかるであろう。

【０１６７】

ＭＩＰ－ＨＡ１３７２は、ＩＰアドレスマネージメントを担当することができ、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃが、別々のＡＳＮおよび／または別々のコアネットワークの間においてローミングすることを可能にすることができる。ＭＩＰ－ＨＡ１３７２は、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃと、ＩＰ対応デバイスとの間における通信を容易にするために、インターネット１３１０などのパケット交換ネットワークへのアクセスをＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃに提供することができる。ＡＡＡサーバ１３７４は、ユーザ認証と、ユーザサービスをサポートすることとを担当することができる。ゲートウェイ１３７６は、その他のネットワークと相互作用することを

容易にすることができる。たとえば、ゲートウェイ１３７６は、ＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃと、従来の地上通信線の通信デバイスとの間における通信を容易にするために、ＰＳＴＮ１３０８などの回路交換ネットワークへのアクセスをＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃに提供することができる。加えて、ゲートウェイ１３７６は、ネットワーク１３１２へのアクセスをＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃに提供することができ、ネットワーク１３１２は、その他のサービスプロバイダによって所有および／または運営されているその他の有線またはワイヤレスのネットワークを含むことができる。

【０１６８】

図１３Ｅにおいては示されていないが、ＲＡＮ１３０４は、その他のＡＳＮに接続されることが可能であり、コアネットワーク１３０６は、その他のコアネットワークに接続されることが可能であるということがわかるであろう。ＲＡＮ１３０４と、その他のＡＳＮとの間における通信リンクは、Ｒ４リファレンスポイントとして定義されることが可能であり、このＲ４リファレンスポイントは、ＲＡＮ１３０４と、その他のＡＳＮとの間においてＷＴＲＵ１３０２ａ、１３０２ｂ、１３０２ｃのモビリティーをコーディネートするためのプロトコルを含むことができる。コアネットワーク１３０６と、その他のコアネットワークとの間における通信リンクは、Ｒ５リファレンスとして定義されることが可能であり、このＲ５リファレンスは、ホームコアネットワークと、訪問先コアネットワークとの間における相互作用を容易にするためのプロトコルを含むことができる。

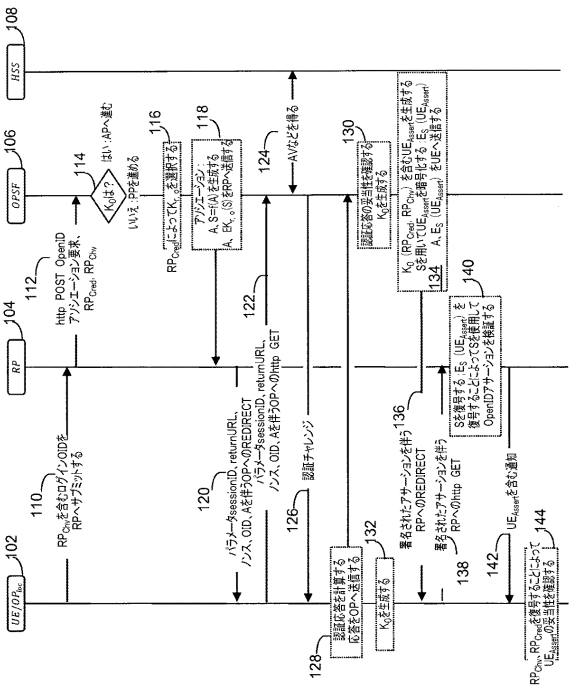
【０１６９】

本明細書に記載されている方法は、コンピュータまたはプロセッサによって実行するためにコンピュータ可読メディア内に組み込まれているコンピュータプログラム、ソフトウェア、またはファームウェアで実装されることが可能である。コンピュータ可読メディアの例は、（有線接続またはワイヤレス接続を介して伝送される）電子信号、およびコンピュータ可読ストレージメディアを含む。コンピュータ可読ストレージメディアの例は、ＲＯＭ（ｒｅａｄ ｏｎｌｙ ｍｅｍｏｒｙ）、ＲＡＭ（ｒａｎｄｏｍ ａｃｃｅｓｓ ｍｅｍｏｒｙ）、レジスタ、キャッシュメモリ、半導体メモリデバイス、内蔵ハードディスクおよびリムーバブルディスクなどの磁気メディア、光磁気メディア、ならびに、ＣＤ－ＲＯＭディスクおよびＤＶＤ（ｄｉｇｉｔａｌ ｖｅｒｓａｔｉｌｅ ｄｉｓｋ）などの光学メディアを含むが、それらには限定されない。ソフトウェアと関連付けられているプロセッサは、ＷＴＲＵ、ＵＥ、端末、基地局、ＲＮＣ、または任意のホストコンピュータにおいて使用するための無線周波数トランシーバを実装するために使用されることが可能である。

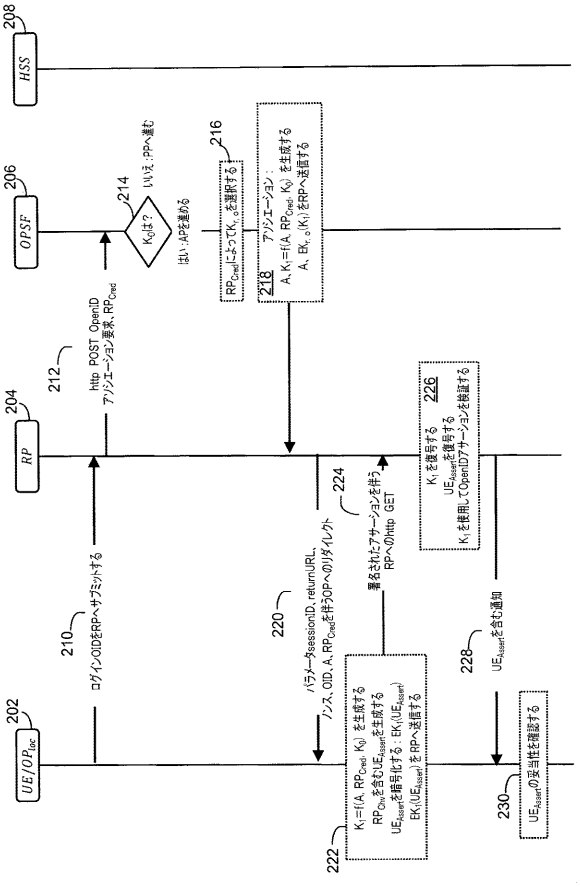
【０１７０】

上記では特徴および要素が特定の組合せで説明されているが、それぞれの特徴または要素は、単独で、またはその他の特徴および要素との任意の組合せで使用されることが可能である。たとえば、本明細書において説明されているプロトコルフローステップは、それらのプロトコルフローステップが説明されている順序には限定されない。加えて、本明細書において説明されている実施形態は、ＯｐｅｎＩＤ認証を使用して説明されているかもしれないが、その他の形態の認証が実施されることも可能である。同様に、本明細書において説明されている実施形態は、ＯｐｅｎＩＤ通信またはエンティティーに限定されないことが可能である。たとえば、ＲＰは、任意のサービスプロバイダを含むことができ、ＯＰ／ＯＰＳＦは、任意の（１つもしくは複数の）ＩＤおよび／もしくはアサーションプロバイダを含むことができ、ならびに／またはＯＰ$_{loc}$は、任意のローカルＩＤおよび／もしくはアサーションプロバイダであることが可能である。さらに、本明細書において説明されているＵＥのいかなる認証も、ＵＥおよび／またはＵＥに関連付けられているユーザの認証を含むことができる。

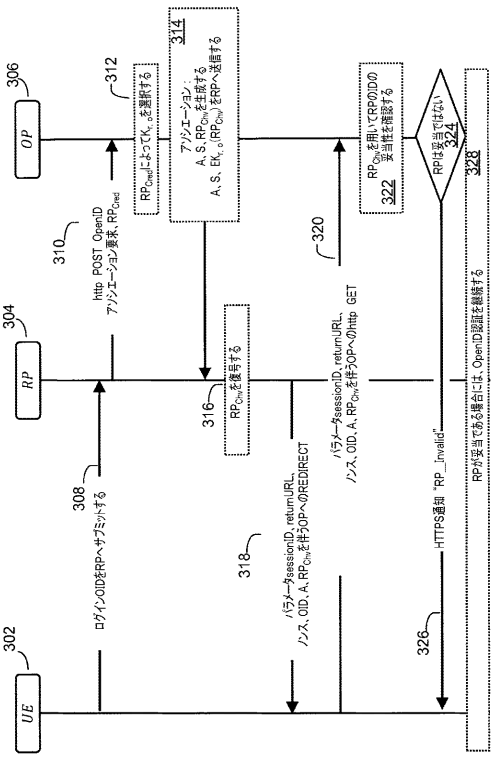
【図１】



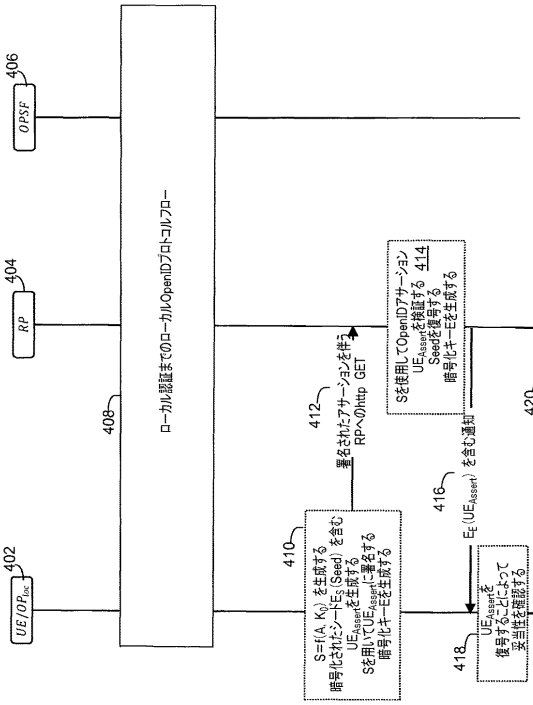
【図２】



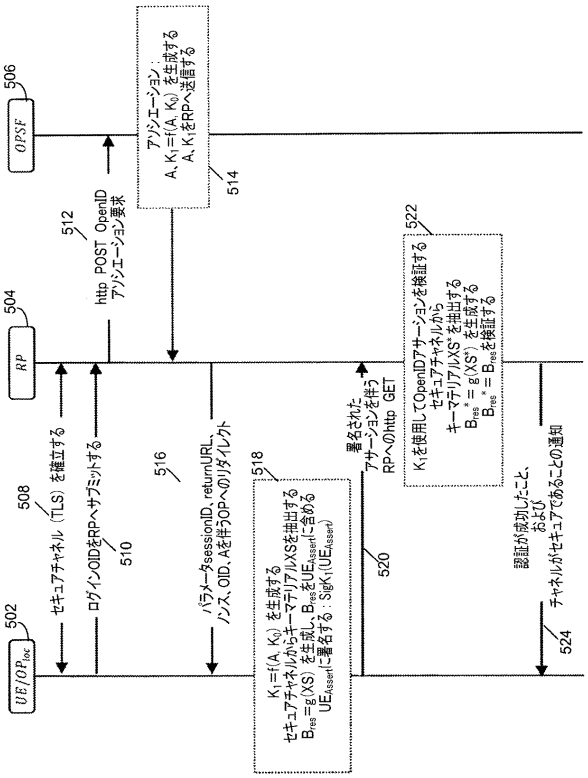
【図３】



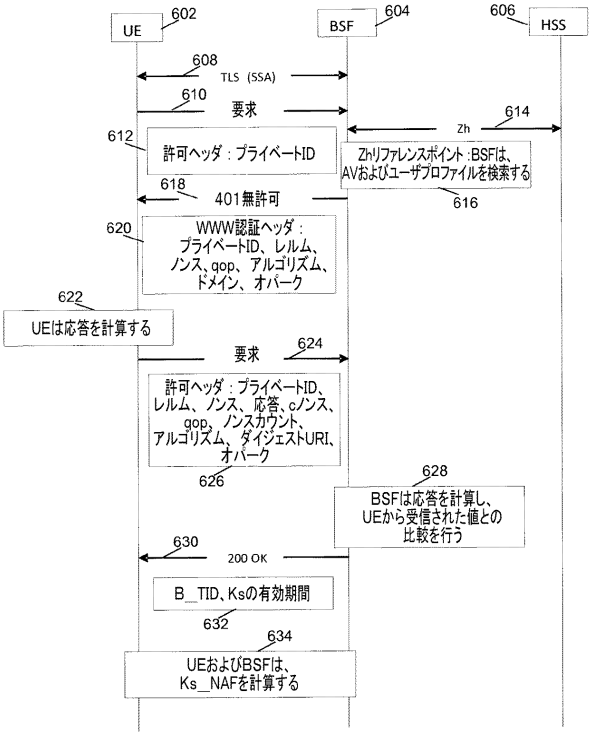
【図４】



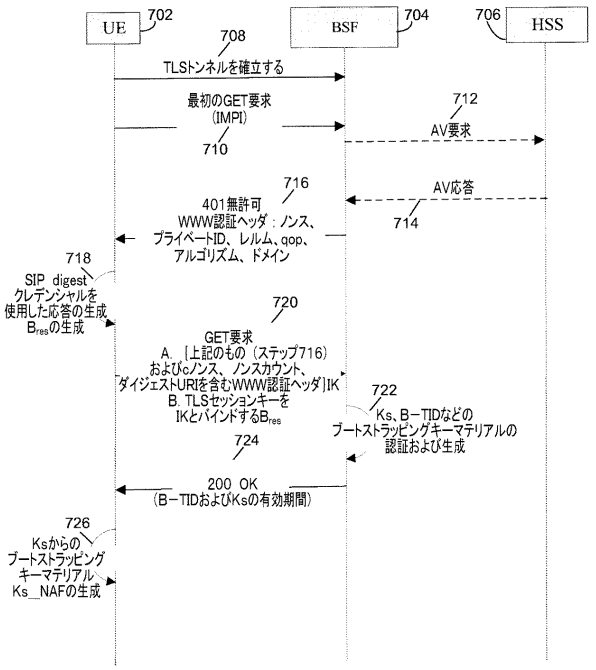
【図５】


OPSF
506
RP
504
UE/OPorc
502
アソシエーション：
A、K1=f(A、K0)を生成する
A、K1をRPへ送信する
514
512
http POST OpenID
アソシエーション要求
セキュアチャネル（TLS）を確立する
508
ログインOIDをRPへサブミットする
510
516
パラメータsessionID、returnURL、
ノンス、OID、Aを伴うOPへのリダイレクト
518
K1=f(A、K0)を生成する
セキュアチャネルからキーマテリアルXSを抽出する
Bres=g(XS)を生成し、BresをUEAssertに含める
UEAssertに署名する：Sig(K1(UEAssert))
520
署名されたアサーションを伴うRPへのhttp GET
522
K1を使用してOpenIDアサーションを検証する
セキュアチャネルからキーマテリアルXSを抽出する
Bres＊＝g(XS')を生成する
Bres＊＝Bresを検証する
524
認証が成功したこと、および
チャネルがセキュアであることの通知

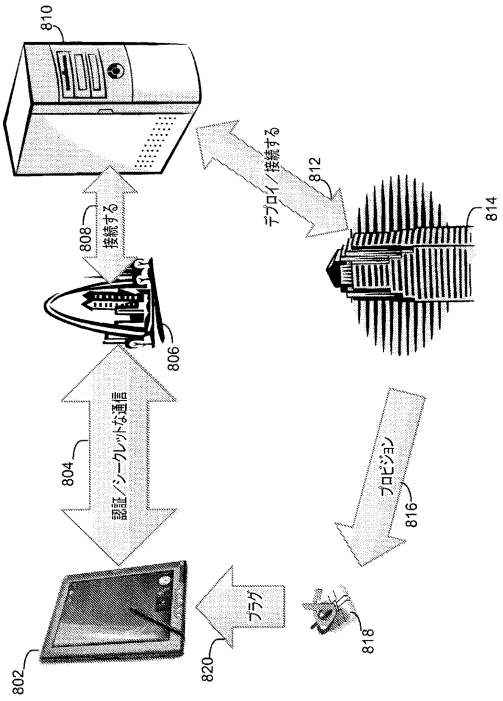
【図６】


UE
602
BSF
604
606
HSS
608
TLS（SSA）
610
要求
614
Zh
612
許可ヘッダ：プライベートID
Zhリファレンスポイント：BSFは、
AVおよびユーザプロファイルを検索する
618
401無許可
616
620
WWW認証ヘッダ：
プライベートID、レルム、
ノンス、qop、アルゴリズム、
ドメイン、オパーク
622
UEは応答を計算する
要求
624
許可ヘッダ：プライベートID、
レルム、ノンス、応答、cノンス、
qop、ノンスカウント、
アルゴリズム、ダイジェストURI、
オパーク
626
628
BSFは応答を計算し、
UEから受信された値との
比較を行う
630
200 OK
B_TID、Ksの有効期間
632
634
UEおよびBSFは、
Ks_NAFを計算する

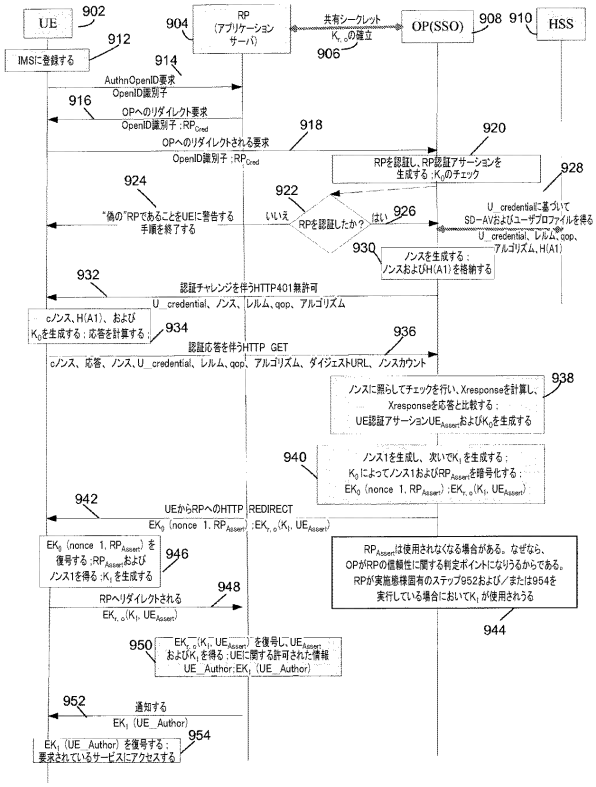
【図７】


UE
702
BSF
704
706
HSS
708
TLSトンネルを確立する
最初のGET要求
（IMPI）
710
712
AV要求
AV応答
714
716
401無許可
WWW認証ヘッダ：ノンス、
プライベートID、レルム、qop、
アルゴリズム、ドメイン
718
SIP digest
クレデンシャルを
使用した応答の生成
Bresの生成
720
GET要求
A.［上記のもの（ステップ716）
およびcノンス、ノンスカウント、
ダイジェストURIを含むWWW認証ヘッダ］IK
B. TLSセッションキーを
IKとバインドするBres
722
Ks、B－TIDなどの
ブートストラッピングキーマテリアルの
認証および生成
724
200 OK
（B－TIDおよびKsの有効期間）
726
Ksからの
ブートストラッピング
キーマテリアル
Ks_NAFの生成

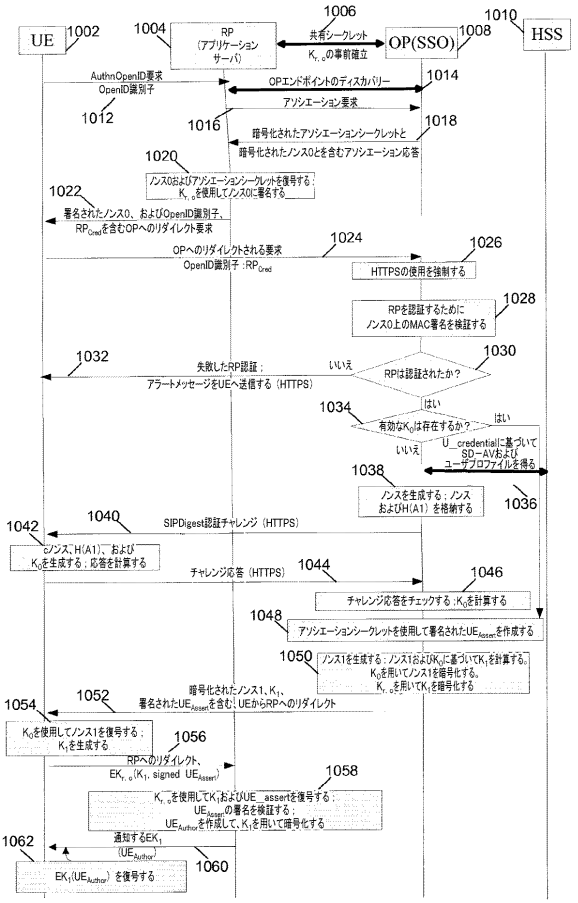
【図８】


810
デプロイ／接続する
812
814
接続する
808
806
804
認証／シークレットの通信
プロビジョン
816
802
プラグ
820
818

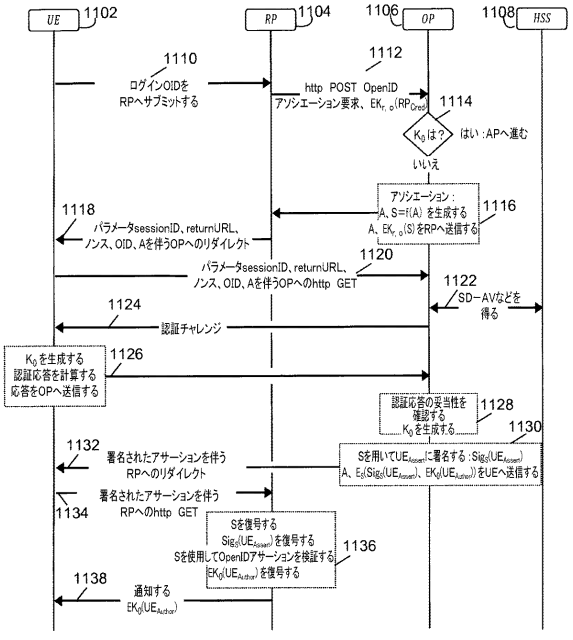
【図９】



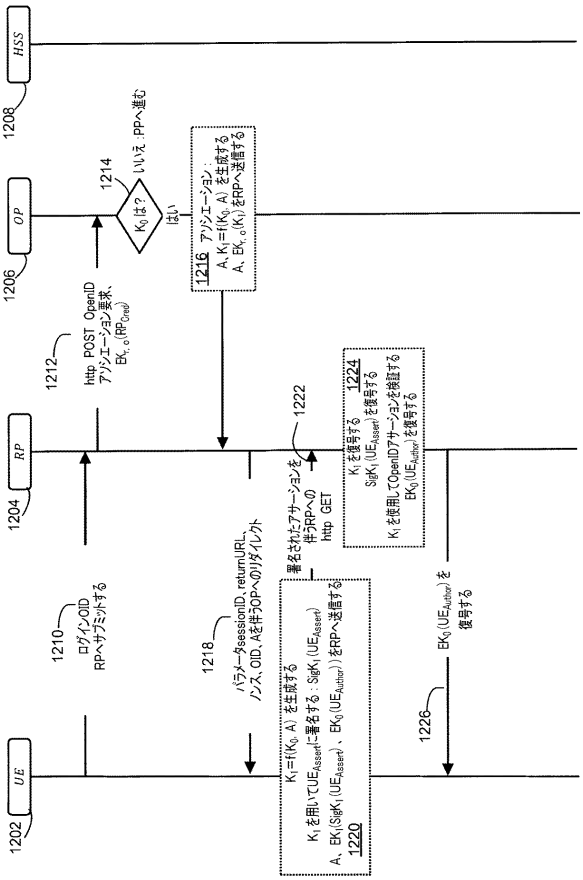

【図１０】



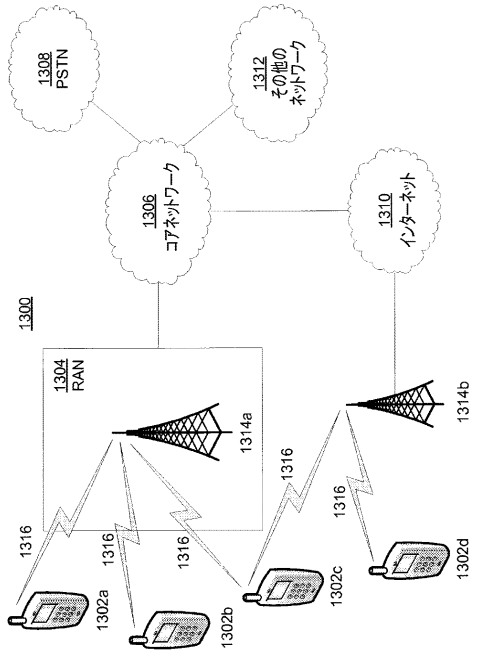

【図１１】



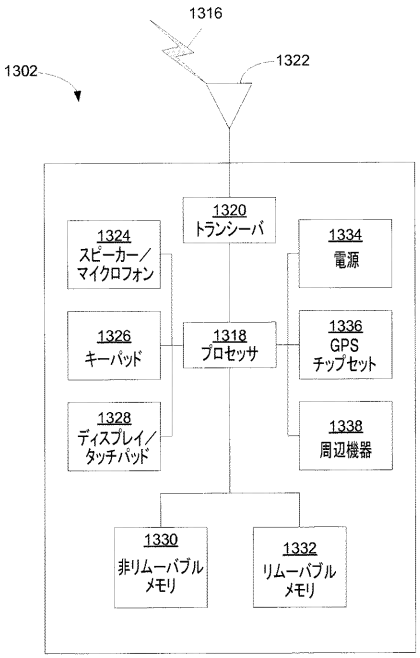

【図１２】



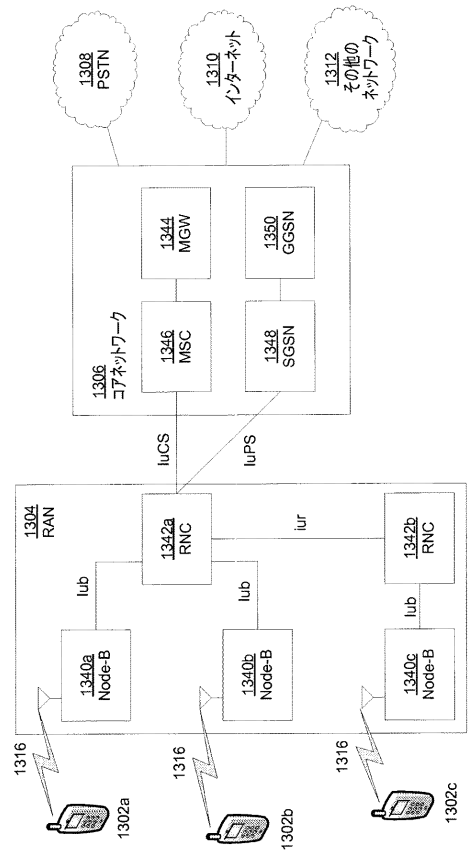
【図１３Ａ】



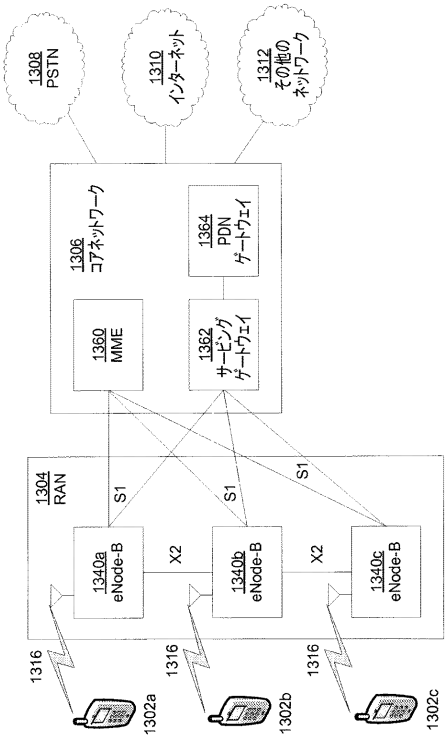

【図１３Ｂ】



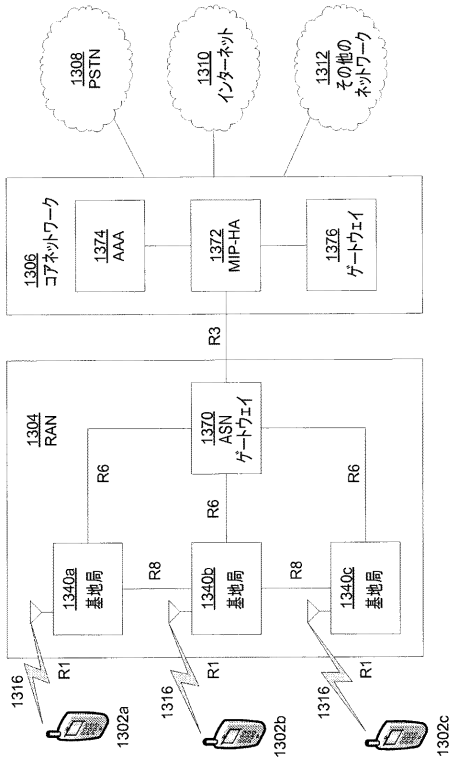

【図１３Ｃ】




【図１３Ｄ】



【図１３Ｅ】


1308
PSTN
1310
インターネット
1312
その他の
ネットワーク
1306
コアネットワーク
1374
AAA
1372
MIP-HA
1376
ゲートウェイ
R3
1304
RAN
1370
ASN
ゲートウェイ
R6
R6
R6
R8
R8
1340a
基地局
1340b
基地局
1340c
基地局
R1
R1
R1
1316
1316
1316
1302a
1302b
1302c

フロントページの続き

(31)優先権主張番号　61/466,662
(32)優先日　　平成23年3月23日(2011.3.23)
(33)優先権主張国　　米国(US)

(72)発明者　ルイス　ジェイ．グッチョーネ
アメリカ合衆国　１０７０９　ニューヨーク州　イースト　チェスター　リンカーン　プレイス　２１１
(72)発明者　アンドレアス　シュミット
ドイツ　６５９２９　フランクフルト　アム　マイン　チュートネンウェグ　３７
(72)発明者　アンドレアス　レイチェル
ドイツ　６０３８５　フランクフルト　ハイデシュトラッセ　１３１
(72)発明者　ヨゲンドラ　シー．シャー
アメリカ合衆国　１９３４１　ペンシルベニア州　エクストン　リージェンシー　コート　１０

審査官　青木　重徳

(56)参考文献　特表２００５－５３６１５４（ＪＰ，Ａ）
特開２００６－０５０５３５（ＪＰ，Ａ）
特開２００５－１６０００５（ＪＰ，Ａ）
特表２００８－５４６３３３（ＪＰ，Ａ）
特表２００５－５３５００６（ＪＰ，Ａ）
米国特許出願公開第２００６／００２０７９１（ＵＳ，Ａ１）
渡辺　龍、田中　俊昭，“携帯電話を用いた連携認証手法の提案”，コンピュータセキュリティシンポジウム２００８　論文集　［第一分冊］，日本，社団法人情報処理学会，２００８年１０月　８日，第２００８巻、第８号，ｐ．６１－６６
鍛　忠司、高田　治、星野　和義、藤城　孝宏、手塚　悟，“セキュアサービスプラットフォームにおけるセキュア通信確立モデル”，情報処理学会研究報告，日本，社団法人情報処理学会，２００５年　３月２３日，Ｖｏｌ．２００５、Ｎｏ．３３，ｐ．１５１－１５６
Andreas U. Schmidt, Andreas Leicher, Yogendra Shahm Inhyok Cha, and Louis Guccione, “SENDER SCORECARDS”, IEEE VEHICULAR TECHNOLOGY MAGAZINE, 米国, IEEE, ２０１１年　3月　4日, Volume:6, Issue:1, p.52-59

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｆ　２１／４４
Ｈ０４Ｗ　１２／０６