(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2016-519367
(P2016-519367A)
(43)公表日　平成28年6月30日(2016.6.30)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/33	(2013.01)	G06F	21/33	350	5J104
H04L 9/32	(2006.01)	H04L	9/00	673A	
		H04L	9/00	673D	

審査請求 有　予備審査請求 有　（全 39 頁）

(21)出願番号　特願2016-505564 (P2016-505564)
(86)(22)出願日　平成26年3月27日 (2014.3.27)
(85)翻訳文提出日　平成27年11月26日 (2015.11.26)
(86)国際出願番号　PCT/US2014/031998
(87)国際公開番号　WO2014/160853
(87)国際公開日　平成26年10月2日 (2014.10.2)
(31)優先権主張番号　61/805,851
(32)優先日　平成25年3月27日 (2013.3.27)
(33)優先権主張国　米国 (US)

(71)出願人　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　ヴィノッド　ケー．チョーイ
アメリカ合衆国　１９４０３　ペンシルベニア州　ノリスタウン　ミニットメン　レーン　１２０１

最終頁に続く

(54)【発明の名称】複数のエンティティにまたがるシームレスな認証

(57)【要約】
ユーザは、アイデンティティプロバイダ（ＩｄＰ）および結果を生成する認証エージェントにより認証される。例えば、チケットのような、認証の証明は、サービスプロバイダ（ＳＰ）へ提供される。ユーザ装置（ＵＥ）は別のＩｄＰおよび関連した結果を生成する認証エージェントで認証される。例えば、別のチケットのような、認証の証明は、上記ＳＰへ提供される。１つまたは複数の認証エージェントはＵＥから離れた認証エンティティに存在することができる。多要素認証プロキシ（ＭＦＡＰ）は認証エージェントをトリガして認証プロトコルを実行し、ＭＦＡＰはＵＥのクライアントエージェントへディケットを提供する。ユーザは、認証を活用して、同じＵＥのクライアントエージェント間を、または異なるＵＥのクライアントエージェント間を移行することができる。

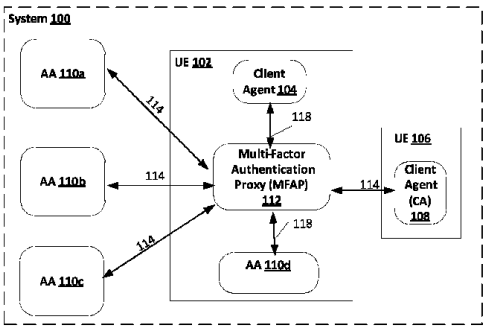


Fig. 1

【特許請求の範囲】
【請求項１】
多要素認証プロキシ（ＭＦＡＰ）を備えたユーザ機器（ＵＥ）であって、前記ＭＦＡＰは、
サービスプロバイダ（ＳＰ）によって提供されるサービスにアクセスするために、複数の認証要素が前記ＵＥのユーザを認証するために要求されていることを判定し、
前記要求された認証要素のうちの１つを利用して、認証を遂行するために、前記ＵＥとは異なるデバイス上の認証エージェント（ＡＡ）を特定し、
前記異なるデバイスへのローカルリンクを確立し、
前記認証を遂行するように前記ＡＡをトリガして
前記ローカルリンクを介して、前記ＡＡによる成功した認証を表すアサーションを受信する、
ように動作する、ＵＥ。
【請求項２】
前記ＭＦＡＰは、前記要求された認証要素のうちの少なくともう１つを利用して、認証を遂行するために、前記ＵＥの１つまたは複数の付加的な認証エージェントを特定する、ようにさらに動作する、請求項１に記載のＵＥ。
【請求項３】
前記ＭＦＡＰは、前記要求された認証要素のうちの少なくともう１つを利用する認証を遂行するために、前記ＵＥとは異なる第２のデバイス上の１つまたは複数の付加的な認証エージェントを特定する、ようにさらに動作し、前記ＭＦＡＰは、ローカルリンクまたはリモートリンクを介して、前記１つまたは複数の付加的な認証エージェントと通信する、請求項１に記載のＵＥ。
【請求項４】
前記ＭＦＡＰは、前記ＳＰへ直接、成功した認証を表す前記アサーションを送信する、ようにさらに動作する、請求項１に記載のＵＥ。
【請求項５】
第１のユーザ機器（ＵＥ）と、サービスプロバイダ（ＳＰ）と、多要素認証プロキシ（ＭＦＡＰ）とを備えたシステムにおいて前記ＭＦＡＰにより実行される方法であって、
前記ＳＰのポリシーに基づいて、前記第１のＵＥのユーザが前記ＳＰによって提供されるサービスにアクセスするために、多要素認証が要求されていることを判定することと、
第１の要素認証を遂行するために、第１の認証エージェントを特定することと、
第１のチケットが生じる前記第１の要素認証をトリガすることと、
第２の要素認証を遂行するために、第２の認証エージェントを特定することと、
第２のチケットが生じる記第２の要素認証をトリガすることと、
前記第１のＵＥの第１のクライアントエージェントへ、前記第１のチケットおよび前記第２のチケットを送信することであり、前記第１のＵＥが前記ＳＰによって提供される前記サービスにアクセスすることを可能にすることと、
を備える、方法。
【請求項６】
前記第１のＵＥの前記ユーザは、前記第１のクライアントエージェントの認証を活用することにより、第２のクライアントエージェントへ移行する、請求項６に記載の方法。
【請求項７】
前記第２のクライアントエージェントは、前記第１のＵＥまたは前記第１のＵＥと異なる第２のＵＥ上に存在する、請求項６に記載の方法。
【請求項８】
前記第１のチケットは、前記第１の要素認証を表すセッションアイデンティティにバインドされる、請求項５に記載の方法。
【請求項９】
前記ＭＦＡＰは前記第１のＵＥ上にある、請求項５に記載の方法。

【請求項１０】
前記ＭＦＡＰは、ローカルリンクまたはリモートリンクを介して、第２のＵＥの第２のクライアントエージェントと通信する、請求項９に記載の方法。
【請求項１１】
前記ＭＦＡＰは第２のＵＥ上に存在し、前記ＭＦＡＰは、ローカルリンクまたはリモートリンクを介して前記第１のＵＥの前記第１のクライアントエージェントと通信する、請求項５に記載の方法。
【請求項１２】
前記第１のチケットおよび前記第２のチケットはそれぞれ、デジタル署名、暗号値、ランダム値、または一時的アイデンティティのうちの少なくとも１つを備える、請求項５に記載の方法。
【請求項１３】
前記第１の認証エージェントおよび前記第２の認証エージェントの少なくとも１つは、第２のＵＥ上に存在する、請求項５に記載の方法。
【請求項１４】
前記ＳＰの前記ポリシーは前記多要素認証の要求される保証レベルを備え、前記第１の認証エージェント及び前記第２の認証エージェントは、前記多要素認証の前記要求される保証レベルに基づいて、特定される、請求項５に記載の方法。
【請求項１５】
前記第１のチケットの保証レベルおよび前記第２のチケットの保証レベルに基づき、集約保証レベルを判定すること、をさらに備える、請求項５に記載の方法。
【請求項１６】
第３の要素認証を遂行ために、第３の要素認証エージェントを特定することと、
第３のチケットが生じる前記第３の要素認証をトリガすることと、
をさらに備える、請求項５に記載の方法。
【請求項１７】
前記第１の認証エージェントおよび前記第２の認証エージェントはそれぞれ第１のアイデンティティプロバイダおよび第２のアイデンティティプロバイダと関連付けられている、請求項５に記載の方法。
【請求項１８】
通信ネットワークにおけるユーザ装置（ＵＥ）であって、
実行可能なメモリと、
実行可能命令を実行すると、
サービスプロバイダ（ＳＰ）によって提供されるサービスにアクセスするために、複数の認証要素が前記ＵＥのユーザを認証するために要求されていることを判定することと、
前記要求された認証要素のうちの１つを利用して、認証を遂行するために、前記ＵＥとは異なるデバイス上の認証エージェント（ＡＡ）を特定することと、
前記異なるデバイスへのローカルリンクを確立することと、
前記認証を遂行するように前記ＡＡをトリガすることと、
前記ローカルリンクを介して、前記ＡＡによる成功した認証を表すアサーションを受信することと
を実行するプロセッサと、
を備えた、ＵＥ。
【請求項１９】
前記プロセッサは、前記要求された認証要素のうちの少なくともう１つを利用して、認証を遂行するために、前記ＵＥ上の１つまたは複数の付加的な認証エージェントを特定することをさらに実行する、請求項１８に記載のＵＥ。
【請求項２０】
前記プロセッサは、前記要求された認証要素のうちの少なくともう１つを利用する認

証を遂行するために、前記ＵＥとは異なる第２のデバイスの１つまたは複数の付加的な認証エージェントを特定することをさらに実行する、請求項１８に記載のＵＥ。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、認証に関する。

【０００２】

（関連出願の相互参照）

本出願は、２０１３年3月２７日に出願された米国特許仮出願シリアルナンバー６１／８０５，８５１号明細書の利益を主張し、その開示内容は、あたかも本明細書にすべて記載されているかの如く、参照により本明細書に組み込まれる。

【背景技術】

【０００３】

多数のインターネットサービス（例えば、銀行取引、マルチメディア、ゲーム等）は、そのサービスがアクセスされる前にデバイスのユーザの認証を要求する。例えば、企業および「オーバーザトップの」アプリケーションサービスプロバイダは、ユーザを承認させるユーザのアイデンティティをアサートすることができる。サービスプロバイダ（ＳＰ）は、ユーザに各サービスプロバイダ（ＳＰ）によって提供されるサービスにアクセスするための個別の登録プロファイルを作成するように要求することが多い。従って、ユーザは、さまざまなサービスにアクセスするために種々のパスワードおよびユーザ名を有することが多く、ユーザにとってかなりの負担が生じている。

【０００４】

二要素認証を使用して、ユーザの認証を強化することができる。例示的な二要素認証は、ユーザのアイデンティティ（ＩＤ）およびパスワードを第１の認証要素として、ハードウェア／ソフトウェアベースのトークンを第２の認証要素とすることを基礎としている。ユーザＩＤおよびパスワードは、ユーザの存在を認証し、そしてトークンは、トークンの機能性が存在するデバイスのユーザの所有権を確認する。多要素認証は、２以上の要素を使用する任意の認証を指す。例示的な認証要素は、対応するパスワード、トークン、およびユーザの生体認証／行動的側面を有するユーザアイデンティティを含む。

【発明の概要】

【０００５】

多要素認証に対する現在のアプローチは、複数のデバイスの能力を活用していない。本明細書で説明されるさまざまな実施形態は、ユーザのユーザ機器（ＵＥ）に加え、多要素認証の所望のレベルを実現する認証エージェントとして機能する１つまたは複数のデバイスの能力を活用する。

【０００６】

ユーザおよび／またはユーザ機器（ＵＥ）を認証するためのシステム、方法および装置が本明細書で説明される。例として、ユーザ機器（ＵＥ）は、サービスプロバイダ（ＳＰ）によって提供されるサービスにアクセスするために、複数の認証要素がＵＥのユーザを認証するために要求されていることを判定するように動作する多要素認証プロキシ（ＭＦＡＰ）を含むことができる。ＭＦＡＰは、要求された認証要素のうちの１つを利用して、認証を遂行するために、ＵＥ以外の異なるデバイスの認証エージェント（ＡＡ）を特定することができる。さらに、ＭＦＡＰは、ＵＥとは異なるデバイスである、異なるデバイスへのローカルリンクを確立することができる。ＭＦＡＰは、認証を遂行するように認証エージェント（ＡＡ）をトリガすることができる。従って、ＭＦＡＰは、ローカルリンク経由で、ＡＡによる成功した認証を表すアサーションを受信することができる。ＭＦＡＰは、要求された認証要素のうちの少なくともう１つを利用して、認証を遂行するために、ＵＥの１つまたは複数の付加的な認証エージェントを特定するようにさらに動作することができる。あるいは、ＭＦＡＰは、要求された認証要素のうちの少なくともう１つを利用して、認証を遂行するために、ＵＥとは異なる第２のデバイスの１つまたは複数の付加

的な認証エージェントを特定するように動作することができる。

【０００７】

例示的な一実施形態において、ＵＥを操作するユーザは、サービスプロバイダ（ＳＰ）によって制御されるサービスへのアクセスを要求する。ユーザは、結果を出す、認証エージェント（ＡＡ）による、アイデンティティプロバイダ（ＩｄＰ）によって認証され得る。例えば、チケットなどの、認証の証拠は、ＳＰに提供され得る。チケットは、乱数値であってもよいし、またはチケットは、認証を遂行するセッションに接続される暗号で生成された値であってもよい。ＵＥは、別の結果を出す、別の認証エージェントによる、別のＩｄＰを用いて認証され得る。例えば、別のチケットなどの、認証の証拠は、ＳＰに提供され得る。認証エージェントのうちの１または複数は、ＵＥ以外のエンティティにあるものとすることができる。多要素認証プロキシ（ＭＦＡＰ）は、認証エージェントをトリガして、認証プロトコルを実行することができ、そしてＭＦＡＰは、チケットを、例えば、ＵＥのブラウザまたはアプリケーションなどの、第１のクライアントエージェントに提供できる。ＭＦＡＰはまた、同じユーザによって使用される別個のＵＥまたは第１のクライアントエージェントと同じＵＥにある、別のクライアントエージェントの認証も提供できる。例えば、別のクライアントエージェントを使用して、有効な新鮮度レベルを有するすでに発生した認証を活用することができる。従って、複数のエンティティを用いるシームレスな認証は、ＭＦＡＰによって可能にすることができる。例えば、複数のエンティティは、同じＵＥにある複数のクライアントエージェント（例えば、ブラウザ、アプリケーション）、または異なるＵＥにある複数のクライアントエージェントであってよい。従って、エンティティは、例えば、ＵＥにあるアプリケーションまたはＵＥ自体を指す。

【０００８】

別の例示的な実施形態により、認証システムは、第１のユーザ機器（ＵＥ）、サービスプロバイダ（ＳＰ）、および多要素認証プロキシ（ＭＦＡＰ）を備える。ＳＰのポリシーに基づいて、ＭＦＡＰは、第１のＵＥのユーザがＳＰによって提供されるサービスにアクセスするために多要素認証が要求されていることを判定する。ＭＦＡＰは、第１の要素認証を遂行するために第１の認証エージェントを特定し、そして第１の要素認証をトリガし、その結果、ＭＦＡＰに送信される第１のチケットが生じる。同様に、ＭＦＡＰは、第２の要素認証を遂行するために第２の認証エージェントを特定し、そして第２の要素認証をトリガし、その結果、ＭＦＡＰに送信される第２のチケットが生じる。第２の認証エージェントは、第１の認証エージェントとは異なるデバイスにあるものとすることができる。ＭＦＡＰは、第１および第２のチケットを、例えば、第１のＵＥのブラウザなどの、第１のクライアントエージェントに送信し、それによって、第１のＵＥがＳＰによって提供されるサービスにアクセスすることが可能となる。一実施形態により、ＭＦＡＰは、第１のＵＥにあるものとすることができる。あるいは、ＭＦＡＰは、第２のＵＥにあるものとすることができ、そしてＭＦＡＰは、ローカルリンク（例えば、Ｂｌｕｅｔｏｏｔｈ）またはリモートリンク経由で第１のＵＥの第１のクライアントエージェントと通信できる。認証エージェントのうちの少なくとも１つは、第１のＵＥにあるものとすることができる。あるいは、第１および第２の認証エージェントのうちの少なくとも１つは、第１のＵＥとは異なる第２のＵＥにあるものとすることができる。さらに別の実施形態により、ユーザが第１のクライアントエージェントを使用していて、第２のクライアントエージェントの使用に切り替えたいのであれば、ＭＦＡＰは、ＩｄＰによりまたはＭＦＡＰによるプロキシ方法（例えば、第１のクライアントエージェントを使用して実行される認証を活用して）により、単一の要素または複数の要素を使用して、第２のクライアントエージェントを使用するユーザがシームレスに認証されるように、認証を容易にする。第１のクライアントエージェントおよび第２のクライアントエージェントは、同じＵＥにあるものとしてもよいし、または異なるＵＥにあるものとしてもよい。

【０００９】

例示的な実施形態において、ＳＰのポリシーは、多要素認証の要求された保証レベルを備え、そして第１および第２の認証エージェントを使用して、多要素認証の要求された保

証レベルを取得できる。認証の保証レベルを組み合わせて、集約された認証保証レベルを形成することができる。認証の任意の数の要素が所望通りに完了され得るというより、任意の数の認証エージェントが所望通りに利用され得ることが認識されよう。各認証エージェントは、対応するアイデンティティプロバイダと関連付けられ得る。例えば、第１の認証エージェントは、第１のチケットを生成することができ、そしてそれに関連付けられるＩｄＰは、第１のチケットと比較されるチケットを生成することができる。チケットがマッチすれば、第１の認証エージェントに対応する認証の要素は、成功である。例示的な代替的実施形態において、ＩｄＰは、ＩｄＰによって、関連付けられた認証エージェントに送信されるチケットを生成することができ、そしてそのチケットは、サービスへのアクセスを取得するために認証エージェントによってクライアントエージェントに提示される。サービスを取得するためにクライアントエージェントによって提示されるチケットが、ＩｄＰがマスターＩｄＰに提供されるチケットにマッチすれば、認証は、成功である。

【図面の簡単な説明】

【００１０】

添付図面と共に例として与えられた、以下の説明からより詳細な理解を得ることができる。

【図１】例示的な実施形態による複数の認証エンティティを用いる例示的な認証システムのブロックシステム図である。

【図２】認証要素対認証保証レベルのマッピングの例を示す表である。

【図３】実施形態による複数の認証エンティティを使用する多要素認証のフロー図である。

【図４Ａ】例示的な実施形態によるＯｐｅｎＩＤ（ＯＩＤ）－汎用ブートストラッピングアーキテクチャ（ＧＢＡ）（ＯＩＤ－ＧＢＡ）を使用する三要素認証のフロー図である。

【図４Ｂ】例示的な実施形態によるＯＩＤ－ＧＢＡに基づく二要素認証のフロー図である。

【図４Ｃ】ブラウザがＵＥとは別個である、別の実施形態による、ＯＩＤ－ＧＢＡに基づく二要素認証の別のフロー図である。

【図４Ｄ】例示的な実施形態によるＧＢＡプロセスを通じてユーザ認証がループされる間に生成される三要素認証のフロー図である。

【図４Ｅ】付加的な詳細が描かれた、図４Ｄに示した三要素認証のフロー図である。

【図４Ｆ】図４Ｅに描かれている呼フローの圧縮バージョンである。

【図５Ａ】例示的な実施形態による、新鮮な認証結果がアサートされる多要素認証のフロー図である。

【図５Ｂ】例示的な実施形態による、複数の新鮮な認証結果がアサートされる多要素認証のフロー図である。

【図６Ａ】開示された１つまたは複数の実施形態が実装され得る例示的な通信システムのシステム図である。

【図６Ｂ】６Ａに図示された通信システム内で使用され得る例示的なワイヤレス送信／受信ユニット（ＷＴＲＵ）のシステム図である。

【図６Ｃ】６Ａに図示された通信システム内で使用され得る例示的な無線アクセスネットワークおよび例示的なコアネットワークのシステム図である。

【発明を実施するための形態】

【００１１】

次の詳細な説明は、例示的な実施形態を図示するために与えられ、本発明の範囲、適用性、または構成を限定することを意図しない。本発明の精神および範囲から逸脱しない範囲で要素およびステップの機能および配置においてさまざまな変更が行われてもよい。

【００１２】

上述のように、多要素認証に対する現在のアプローチは、複数のデバイスの能力を活用していない。特に、現在のアプローチは、複数のデバイスのそれぞれの間でシームレスに切り替わっている間、強固な多要素認証を実現するために複数のデバイスを使用していな

い。本明細書で説明されるさまざまな実施形態は、ユーザのユーザ機器（ＵＥ）に加え、多要素認証の所望のレベルを実現する認証エージェントとして機能する１つまたは複数のデバイスの能力を活用する。例示的な一実施形態において、例えば、複数のデバイスなどの、複数の認証エンティティを使用して、強固な多要素認証を提供する。さらに、複数のデバイスは、複数の認証要素を提供するために互いにシームレスに通信できる。以下で説明するように、多要素認証は、さまざまな実施形態により分割端末のシナリオに実装され得る。分割シナリオと呼ぶこともできる、分割端末のシナリオは、ＵＥの認証のためにＵＥが２以上の部分に分割される、任意のシナリオを指す。例として提示される、１つの分割端末のシナリオにおいて、所与のＵＥは、所与のＵＥのＵＩＣＣおよび別個に、例えば、所与のＵＥとは異なるデバイスに配置されているブラウザを使用して認証される。分割端末シナリオはまた、多要素認証プロキシ（ＭＦＡＰ）が、ＵＳＢ接続、ＷｉＦｉ、赤外線、Ｂｌｕｅｔｏｏｔｈ／ＮＦＣ等といった、ローカルリンクを使用してＭＦＡＰとペアにされる他のローカル認証のサービスを使用する、シナリオを指すこともある。例示的なローカル認証デバイスは、限定されないが、スマートウォッチ、Ｇｏｏｇｌｅグラス、または他のウェアラブルコンピューティングデバイス、スタンドアロンの生体または行動センサ等を含む。例示的な実施形態において、多要素認証は、ＯｐｅｎＩＤ（ＯＩＤ）汎用ブートストラッピングアーキテクチャ（ＧＢＡ）（ＯＩＤ－ＧＢＡ）に基づく。多要素認証結果は、ユーザ／ユーザ機器（ＵＥ）がＳＰによって提供されるサービスへのアクセスを受信することができるように、組み合わされてサービスプロバイダ（ＳＰ）に配信される。例示的な実施形態において、認証バインディングは、複数の認証要素の結果を使用して作成される。以下で説明するように、多要素認証は、例えば、ＯｐｅｎＩＤ／ＧＢＡフレームワークなどの、ＧＢＡフレームワークを使用して遂行され得る。

【００１３】

サービスにアクセスするために、ユーザは、サービスを提供するＳＰの認証要件を満たさなければならないこともある。認証要件は、さまざまなサービスの認証ポリシーに基づくことができる。例えば、ＳＰのポリシーは、認証が、ＳＰによって提供されるサービスがアクセスされる前の、認証強度と呼ぶこともできる、所定の保証レベルを満たすことを要求できる。従って、図２を参照すると、保証レベルは、認証の強度を示すことができ、そして高い保証レベルは、認証の複数の要素を要求することができる。例示的な実施形態において、保証レベルは、ユーザが認証される保証のレベルを指す。保証レベルは、使用される認証プロトコル、認証のためのいくつかの要素、認証要素のタイプ（例えば、生体、デバイス、ユーザ）、認証の新鮮度、補足条件、またはそれらの任意の適切な組み合わせに基づくことができる。保証レベルは、外部のオーソリティによって規定され得る。例示的な実施形態において、所望の保証レベルは、例えば、米国国立標準技術研究所（ＮＩＳＴ）、第３世代パートナーシッププロジェクト（３ＧＰＰ）、ワールドワイドウェブコンソーシアム（Ｗ３Ｃ）等を含む、標準化団体のような、さまざまな外部のオーソリティによって指定され得る。例えば、外部のオーソリティは、例えば、アプリケーション自身のセキュリティ要件、リクエストされたサービスをホストする会社のセキュリティポリシー等といった、さまざまな基準に基づいて保証レベルを指定できる。さらなる例として、ＳＰは、ＳＰがリクエストされたサービスをユーザに提供するためにそのＳＰが要求する保証レベルを指定できる。

【００１４】

さらに図２を参照すると、ＳＰは、サービスへのアクセスを許可する前に認証新鮮度レベルが満たされることを要求できる。認証に対応する認証新鮮度レベルは、その認証が遂行された時間期間を示すことができる。限定せずに提示された、新鮮度レベルの例として、ＳＰは、認証が遅くとも３０秒以内に実行されることを要求できる。ある場合には、多要素認証は、ＳＰの認証ポリシーを順守するために調整されなければならないこともある。ＳＰのさまざまなポリシーに基づいて、例えば、複数の認証エージェントは、本明細書で説明されるさまざまな実施形態により、ユーザまたはＵＥを認証するために使用され得る。

【００１５】
図１は、例示的な実施形態により、例示的な認証システム１００を示している。図１を参照すると、図示された実施形態により、認証システム１００は、第１のクライアントエージェント１０４を含む第１のユーザ機器１０２を含む。クライアントエージェントという語は、一般に、ＵＥにあるブラウザまたはクライアントアプリケーションを指す。図示された実施形態により、第１のクライアントエージェント（ＣＡ）１０４は、第１のＵＥ１０２にあるラウザまたはクライアントアプリケーションを指す。ユーザ機器（ＵＥ）という語は、以下でさらに説明されるように、任意の適切なワイヤレス送信／受信ユニット（ＷＴＲＵ）を含むデバイスを指してよいことが理解されよう。例えば、ＷＴＲＵは、固定または移動加入者ユニット、ページャ、セルラー電話、携帯情報端末（ＰＤＡ）、スマートフォン、ラップトップ、タブレットコンピュータ、パーソナルコンピュータ、ワイヤレスセンサ、家電等を指す。本明細書で使用される際、特に指定のない限り、サービスを開始するＵＥは、一次ＵＥと呼ばれ、そして一次ＵＥによって開始された後のセッションを継続するＵＥは、二次ＵＥと呼ばれる。例えば、図１を参照すると、ＵＥ１０２は、サービスへのアクセスを開始することができ、そして例えば、第２のＵＥ１０６などの、別のＵＥは、ＵＥ１０２がサービスへのアクセスを開始した後にそのサービスへのアクセスを継続する。従って、第１のＵＥ１０２を一次ＵＥと呼ぶことができ、第２のＵＥ１０６を二次ＵＥと呼ぶことができる。図１は、２つのＵＥを描いているが、本明細書で説明されるさまざまな実施形態により、所望通りにサービスにアクセスするために任意の数のＵＥが使用されてよいことが理解されよう。

【００１６】
ＣＡは、一次ＵＥおよび二次ＵＥのうちの少なくとも１つ、例えば、両方にあるものとすることができる。図１を参照すると、第１のＣＡ１０４は、第１のＵＥ１０２にあるものとあり、第２のＣＡ１０８は、第２のＵＥ１０６にあるものとする。ユーザは、例えば、スマートフォン、タブレット、ラップトップ、またはデスクトップなどの、複数のＵＥを有することができ、そしてＣＡは、ＵＥのうちの少なくとも１つにあるものとすることができる。従って、図示された実施形態により、ユーザは、例えば、スマートフォンになり得る、第１のＵＥ１０２（一次ＵＥ）上でアプリケーションまたはサービスを始動することができ、その後ユーザは、第２のＵＥ１０６にある第２のＣＡ１０８を使用して、例えば、タブレットになり得る、第２のＵＥ１０６上でシームレスに同じアプリケーションまたはサービスの使用を継続できる。例えば、第１のＵＥ１０２のユーザは、第１のＣＡ１０４の認証を活用することによって第２のＣＡ１０８に移行することができる。第２のＣＡ１０８が第２のＵＥ１０６にあるように図示されているが、第２のＣＡ１０８は代替的に、第１のＵＥ１０２にあるものとできることが理解されよう。

【００１７】
図１について続けて参照すると、認証システム１００は、例えば、第１の認証エージェント（ＡＡ）１１０ａ、第２のＡＡ１１０ｂ、第３のＡＡ１１０ｃ、および第４のＡＡ１１０ｄなどの、１つまたは複数の認証エージェント（ＡＡ）１１０を含むことができる。４つの認証エージェントが図示されているが、任意の数の認証エージェントを認証システムに所望通りに含むことができることが理解されよう。認証エージェント１１０は、一般に、クライアント、認証のための機能性と呼ぶこともできる、第１のＵＥ１０２に提供するハードウェア／ソフトウェアを含むことができる。ある場合には、認証エージェントは、例えば、第１のＵＥ１０２によって実装される第４のＡＡ１１０ｄなどの、ＵＥに実装される。従って、認証エージェントのうちの少なくとも１つは、ＵＥ１０２の少なくとも一部になる。さらに、認証エージェントのうちの少なくとも１つは、第２のＵＥ１０６にあるものとすることができる。あるいは、認証エージェントは、スタンドアロンの認証デバイスまたはクライアント機能として実装され得る。図示された例示的な実施形態により、第１のＡＡ１１０ａは、例えば、モバイルデバイス（例えば、電話機）にある、加入者識別モジュール（ＳＩＭ）、ソフトウェアＳＩＭ、またはユニバーサル集積回路カード（ＵＩＣＣ）などの、アイデンティティモジュールによって実装される。第２のＡＡ１１０

ｂは、電子キーフォブによって実装され得る。第３のＡＡ１１０ｃは、スタンドアロンの生体認証クライアントによって実装され得る。例示的なスタンドアロンの生体認証クライアントは、指紋リーダー、脈拍を測定するあるいは人が生存していることを検証するスマートウォッチ、耳たぶを認識するヘッドフォン、虹彩走査または他の顔認識／目の検証に使用されるグラス、生体センサを含む他のウェアラブルデバイス等を含む。図示された認証エージェントは、例示目的で提示され、さまざまな代替的認証エージェントを本明細書のさまざまな実施形態において使用されてよいことが理解されよう。例えば、ＡＡは、ユーザまたはＵＥの資格を格納するアプリケーションで構成することができる。さらに以下に説明されるように、図示された実施形態により、認証エージェント１１０は、第１のＵＥ１０２および／または第１のＵＥ１０２のユーザの認証に参加することができる。第１のＣＡ１０４および認証エージェントＡＡ１１０は、例えば、内部通信、ローカルリンク（例えば、Ｂｌｕｅｔｏｏｔｈ）、またはリモートリンクなどの、さまざまな手段を経て互いに通信できる。ローカルリンクは、ＷｉＦｉ、赤外線等を介した通信を指す。ＭＦＡＰ１１２は、ローカルリンクを使用して所与のＡＡと通信できる。リモートリンクは、リンクがＭＦＡＰ１１２を経由する、２つのデバイス間の通信リンクを指す。本明細書で使用される際、内部通信は、単一のデバイス内で起こる通信を指す。

【００１８】

さらに図１を参照すると、図示された実施形態により、多要素認証プロキシ（ＭＦＡＰ）１１２は、第１のＵＥ１０２にある。ＭＦＡＰ１１２は、例えば、第１のＵＥ１０２などの、ユーザデバイスに配置され得る。ＭＦＡＰ１１２は、分割端末またはマルチデバイスのシナリオにおいて多要素認証およびアサーションを可能にする機構を提供できる。例示的な実施形態により、ＭＦＡＰ１１２は、リクエストされた保証レベルを判定するように構成される。ＭＦＡＰ１１２は、認証レベルリクエストを認証の要素に翻訳するようにさらに構成され得る。例えば、翻訳された認証の要素のそれぞれは、その要素と関連付けられたそれぞれの認証強度を有することができる。従って、ＭＦＡＰは、認証レベルリクエストを、リクエストされた保証レベルを実現する認証要素の組み合わせに翻訳することができる。ＭＦＡＰ１１２は、多要素認証のために認証要素を判定するサービスプロバイダのポリシーを翻訳するプロキシエンジンにコンタクトするようにさらに構成され得る。

【００１９】

例示的な実施形態において、認証要素が判定された後、ＭＦＡＰ１１２は、認証要素のそれぞれをトリガするために１つまたは複数の認証エージェント（ＡＡ）と通信する。ＭＦＡＰとＡＡとの間の通信は、ローカルリンクを介して、またはリモートリンクを介して同じエンティティ内で遂行され得る。図１を参照すると、図示された実施形態により、ＭＦＡＰ１１２は、ローカルリンク１１４を介して第２のＡＡ１１０ｂと通信する。ＭＦＡＰ１１２はさらに、ローカルリンクを介して、第１の認証エージェント１１０ａと第３の認証エージェント１１０ｃのそれぞれとも通信する。さらに、図示されたＭＦＡＰ１１２は、内部リンク１１８を介して第４のＡＡ１１０ｄと通信する。

【００２０】

さらに以下に説明されるように、ＭＦＡＰ１１２は、複数の認証要素を組み合わせ、そして複数の認証要素の組み合わせと関連付けられた集約保証レベルを計算するようにさらに構成され得る。さらに、所与のＭＦＡＰおよび所与のＡＡは、承認されたＭＦＡＰおよびＡＡのみが互いに通信することが可能になるように、そしてＭＦＡＰとＡＡとの間の通信がセキュアになるように、互いに認証することができる。さらに、所与のＭＦＡＰおよび所与のＣＡは、承認されたＭＦＡＰおよびＣＡのみが互いに通信することが可能になるように、そしてＭＦＡＰとＣＡとの間の通信がセキュアになるように、互いに認証することができる。

【００２１】

再度図１を参照すると、図示された実施形態により、ＭＦＡＰ１１２は、内部リンク１１８を介して認証の結果を第１のＣＡ１０４に伝達する。例えば、ＭＦＡＰ１１２は、各認証要素と関連付けられた新鮮度レベルおよび保証レベルを伝達できる。さらに、ＭＦＡ

Ｐは、遂行された各認証要素の組み合わされた保証レベルを表す、集約保証レベルをＣＡ１０４に伝達できる。ＭＦＡＰ１１２は、ローカルリンク１１４または内部リンク１１８などの、所望通りの手段を介してＣＡと通信できる。図示された実施形態により、ＭＦＡＰ１１２は、第１のＵＥ１０２内の内部リンク１１８を介して第１のＣＡ１０４と通信し、そしてＭＦＡＰ１１２は、ローカルリンク１１４を介して第２のＣＡ１０４と通信する。

【００２２】

従って、ＭＦＡＰ１１２は、サービスプロバイダ（ＳＰ）によって提供されるサービスにアクセスするために、複数の認証要素がＵＥ１０２のユーザを認証するために要求されていることを判定できる。ＭＦＡＰ１１２は、要求された認証要素のうちの１つを利用して、ＵＥ１０２とは異なるデバイス、例えば、ＵＥ１０６の認証エージェント（ＡＡ）を特定して認証を遂行できる。ＭＦＡＰ１１２は、異なるデバイス（例えば、ＵＥ１０６）へのローカルリンクを確立することができ、そしてＭＦＡＰ１１２は、ＡＡをトリガして特定されたＡＡが認証を遂行するようにできる。それに応じて、ＭＦＡＰ１１２は、そのローカルリンク経由で、そのＡＡによって、成功した認証を表すアサーションを受信できる。

【００２３】

例示的な実施形態において、ＭＦＡＰ１１２は、ネットワークに配置されているアイデンティティプロバイダ（ＩｄＰ）サーバのクライアントタイプの役割を担う。ＩｄＰは、ユーザの好適な識別子の判定によってマスターＩｄＰとして指定され得る。例示的な実施形態において、マスターＩｄＰは、ＳＰとの相互接続同意を通じて、ユーザおよび／またはデバイスを認証する責任を負う。例えば、マスターＩｄＰは、認証が一要素または多要素であるかどうかの、認証自体を遂行するための資産（assets）を備えることができる。あるいは、マスターＩｄＰは、その資産に加えまたはその代わりに、他のＩｄＰの資産を用いることができる。例えば、マスターＩｄＰは、認証エージェントによって出された結果に基づいてＩｄＰがアイデンティティをアサートすることができるように、他のＩｄＰをトリガしてコンテキストを作成できる。さらに、マスターＩｄＰは、ＭＦＡＰ１１２のサーバとして機能することができる。

【００２４】

ＭＦＡＰ１１２は、認証エージェントのサービスを呼び出すことを可能にする情報で構成される。例えば、構成された情報は、それぞれの認証エージェント、認証エージェントのＩＰアドレス、認証エージェントのＭＡＣアドレス、所与のＡＡから認証を開始するために所与のＡＡによって要求されるパラメータ等に対応するＵＲＬを含むことができる。図１に示した図示された実施形態により、ＭＦＡＰ１１２は、ブラウジングエージェント（ＣＡ１０４）およびＡＡ（第４のＡＡ１１０ｄ）をホストする同じデバイス（ＵＥ１０２）にある。あるいは、ＭＦＡＰ１１２は、ブラウジングエージェントをホストしないが、ＡＡをホストするエンティティにあるものとすることができる。さらに別の実施形態において、ＭＦＡＰ１１２は、ブラウジングも認証機能も遂行しないデバイスにあるものとすることができる。ＭＦＡＰ１１２の機能性は、ブラウザへのプラグインとして実装され得るか、またはアプリケーションに組み込まれ得る。ＭＦＡＰの機能を呼び出すためのアプリケーションプログラミングインタフェース（ＡＰＩ）は、複数のクライアントエージェント（例えば、ブラウザ、アプリケーション）がＭＦＡＰの機能を呼び出すことができるように、提供され得る。例えば、ＭＦＡＰ１１２は、他のアプリケーションからのＡＰＩコールを用いて呼び出されるスタンドアロンのアプリケーションとして存在し得る。ＭＦＡＰ１１２は、ブラウザのインタラクション、例えば、インテントを使用してトリガされるスタンドアロンのアプリケーションとして存在し得る。

【００２５】

次に図３を参照すると、例示的な認証システム３００は、１つまたは複数の認証エージェント、例えば、第１のＡＡ３１０ａおよび第２のＡＡ３１０ｂ、ＣＡ３０４、ＳＰ３０６、マスターＩｄＰ３０８、およびＭＦＡＰ１１２を含む。参照数字は、便宜上図全体を

通して繰り返され、２以上の図に現れる参照数字は、それらの数字が表れる各図の同じまたは同様の特徴を指すことが理解されよう。２つの認証エージェントが認証システム３００に図示されているが、認証システム３００の認証エージェントの数は、所望通りに変えてよいことが理解されよう。図示された実施形態により、第１の認証エージェント３１０ａと第２の認証エージェント３１０ｂはそれぞれ、第１のＩｄＰ３０９ａと第２のＩｄＰ３０９ｂに関連付けられる。さらに、ＣＡ３０４がＳＰ３０６によって提供されるサービスへのアクセスを提供することができるように、認証エージェント３１０ａと３１０ｂおよびアイデンティティプロバイダ３０９ａと３０９ｂは、二要素認証を可能にできる。ＳＰ３０６、マスターＩｄＰ３０８、第１のＩｄＰ３０９ａ、および第２のＩｄＰ３０９ｂをまとめて、ネットワーク側の認証システム３００と呼ぶことができる。ＳＰ３０６はまた、限定されないが、信頼するパーティー（ＲＰ）３０６と呼ぶこともできる。例示的な二要素認証が図３に図示されているが、図３に示した呼フローは、３以上の要素を使用する認証に拡張されてよいことが理解されよう。図示された実施形態により、ＭＦＡＰ１１２は、ＳＰ３０６のポリシー要件にアクセスし、そしてマスターＩｄＰ３０８は、そのポリシーを翻訳して、そのポリシー要件を満たす認証プロトコルのパラメータを判定する。

【００２６】

図３について続けて参照すると、ＣＡ３０４は、ＳＰ３０６によって提供される要件に基づいてＭＦＡＰ１１２のサービスを呼び出すことができる。例えば、ＭＦＡＰ１１２は、ポリシーを翻訳して、要求された認証要素、要求された認証強度（保証レベル）、および／または要求された認証の新鮮度レベルを判定できる。ＭＦＡＰ１１２は、要求された認証エージェントが判定された後、要求された認証エージェントのそれぞれにコンタクトすることによってさまざまな認証プロトコルの始動をトリガすることができる。図示された実施形態により、ＭＦＡＰ１１２は、トリガされた認証プロトコルの結果を組み合わせ、そしてその認証の結果をＣＡ３０４に提示する。マスターＩｄＰ３０８は、ＩｄＰ３０９ａおよび３０９ｂのそれぞれから、それぞれの保証レベルを有する認証要素のそれぞれの結果を収集できる。マスターＩｄＰ３０８は、ＣＡ３０４および／またはＣＡ３０４のユーザのアイデンティティをＳＰ３０６にアサートすることができる。アサーションは、マスターＩｄＰ３０８がＣＡ３０４から受信する多要素認証の証拠（例えば、チケット）に基づくことができる。さまざまな例示的な実施形態において、マスターＩｄＰ３０８は、そのマスターＩｄＰがＣＡ３０４から受信するチケットを、そのマスターＩｄＰがＩｄＰ３０９ａおよび３０９ｂのそれぞれのから受信するチケットと比較できる。本明細書で使用される際、チケットという語は、一般に、認証パラメータを指す。例えば、チケットは、ノンス、暗号値、または認証アサーションを表すことができる。

【００２７】

さらに図３を参照すると、図示された実施形態により、３１２において、ユーザリクエストは、ＣＡ３０４経由で（ＳＰ３０６によって提供される）サービスにアクセスする。ＣＡ３０４は、ＳＰ３０６と通信することができ、そしてその通信は、ユーザと関連付けられたユーザＩＤを含むことができる。ユーザＩＤに基づいて、３１４において、ＳＰ３０６は、ユーザＩＤと関連付けられたマスターＩｄＰ３０８の発見を遂行して関連付ける。マスターＩｄＰ３０８は、ＯｐｅｎＩＤアイデンティティＰｒｏｖｉｄｅｒ（ＯＰ）またはネットワークアクセス機能（ＮＡＦ）と関連付けられた機能性を遂行することができ、従って、マスターＩｄＰ３０８は、ＯＰ３０８またはＮＡＦ３０８とも呼ばれ得る。３１６において、図示された実施形態により、ＳＰ３０６は、例えば、ＳＰ３０６のポリシーに基づいて、ＳＰ３０６によって提供されるリクエストされたサービスにユーザがアクセスするために、多要素認証が要求されていることを判定する。ＳＰ３０６はまた、ＳＰ３０６によって提供されるリクエストされたサービスにユーザがアクセスするために要求される認証の保証のレベルを判定することもできる。３１８において、図示された実施形態により、ＳＰ３０６は、その保証レベル要件をＣＡ３０４に伝達する。３２０において、ＣＡ３０４は、ＭＦＡＰ１１２のサービスを呼び出す。

【００２８】

例示的な実施形態において、ＣＡ３０４およびＭＦＡＰ１１２は、ＭＦＡＰ１１２のサービスがセキュアに呼び出されるように、互いに認証する。相互認証は、認証されたＣＡのみがＭＦＡＰ１１２のサービスを呼び出すこと、および認証されたＭＦＡＰのみがＣＡ３０４にサーブすることを確保できる。さらに図３を参照すると、３２０において、ＣＡ３０４は、図１について説明したように、ローカルリンクまたは内部リンク経由でＡＰＩコールを使用することによってＭＦＡＰ１１２のサービスを呼び出すことができる。ＡＰＩコールは、所望通りに任意の通信リンクを介して送信され得ることが理解されよう。図示された実施形態により、ＣＡ３０４はまた、ＳＰ３０６によって要求される保証情報も提供する。３２２において、サービスにアクセスするために要求される保証のレベルに基づいて、例えば、ＭＦＡＰ１１２は、要求される保証レベルを実現するために遂行されることができる認証要素のタイプおよび強度を判定する。ＭＦＡＰ１１２はさらに、要求された認証を遂行することができる認証エージェントを特定できる。例えば、図示された実施形態により、ＭＦＡＰ１１２は、第１のＡＡ３１０ａおよび第２のＡＡ３１０が認証要素の判定されたタイプおよび強度と関連付けられていることを判定する。第１の認証エージェント３１０ａが特定された後、３２４において、ＭＦＡＰ１１２は、第１の認証エージェント３１０ａが認証プロトコルを開始するように、トリガを第１の認証エージェント３１０ａに送信する。３２６において、マスターＩｄＰ３０８は、第１の認証エージェント３１０ａによって開始される認証プロトコルのコンテキストが作成されるプロトコルをトリガする。例えば、マスターＩｄＰ３０８は、第１のＡＡ３１０ａと関連付けられた第１のＩｄＰ３０９ａと通信して、第１のＩｄＰ３０９ａが、第１のＡＡが開始した認証(the first AA-initiated authentication)のコンテキストを生成することをリクエストできる。３２４および３２６において遂行されるステップは、互いに並行して遂行され得る。

【００２９】

図３について続けて参照すると、図示された実施形態により、３２８において、第１のＡＡ３１０ａおよび第１のＩｄＰ３０９ａは、認証を実行する。その認証は、ＣＡ３０４のユーザの認証（例えば、ユーザの生体認証）、ＣＡ３０４の認証、ＣＡ３０４と関連付けられたデバイスの認証等を備えることができる。例えば、第１のチケットのような、チケットは、認証が成功すると、第１のＩｄＰ３０９ａによって生成され得る。図示された実施形態により、第１のチケットは、第１の認証エージェント３１０ａに送信される。第１のＩｄＰ３０９ａによって生成されるチケットは、セキュアな方法で第１のＡＡ３１０ａに送信され得る。あるいは、第１のチケットは、第１のＩｄＰ３１０ｂによって使用される第１のチケットを生成する同様の機構を使用して、第１のＡＡ３１０ａによって生成され得る。それにもかかわらず、認証の終了時に、第１のＡＡ３１０ａと第１のＩｄＰ３０９ａの両方は、認証の証拠を有することができ、その証拠は、図３により第１のチケットと呼ばれる。

【００３０】

３３０において、３２４において受信されたトリガに応答して、第１のＡＡ３１０ａは、第１のチケットを備えるトリガ応答を送信できる。トリガ応答は、ＭＦＡＰ１１２に送信されることができ、そしてそのトリガ応答は、成功した認証が遂行されたことを証明できる。３３２において、ネットワーク側において、第１のＩｄＰ３０９ａは、第１のチケットおよびそれに関連付けられた新鮮度（例えば、認証が実行された時の日付／時間）をマスターＩｄＰ３０８に送信できる。

【００３１】

３３４において、例えば、ポリシーに基づいて、ＭＦＡＰ１１２は、第２の認証要素を使用してトリガを第２のＡＡ３１０ｂに送信することによって第２の認証の始動を開始できる。３３６において、図示された実施形態により、マスターＩｄＰ３０８は、第２の認証コンテキストを作成するトリガを第２のＩｄＰ３０９ｂに送信する。トリガされる第２の認証コンテキストは、第２のＡＡ３１０ｂによって遂行される、第２の認証要素を使用して、第２の認証と関連付けられる。３３４および３３６におけるステップは、互いに並

行して遂行され得る。３３８において、図示された実施形態により、第２のＡＡ３１０ｂと第２のＩｄＰ３０９ｂとの間の第２の要素認証が実行される。第２の要素認証を遂行するために使用される第２の要素は、ユーザの生体認証、ユーザと関連付けられた別の要素、デバイスと関連付けられた要素、ユーザの行動分析と関連付けられた要素等であってよい。あるいは、例えば、第２のＡＡ３１０ｂとユーザとの間の第２の要素認証が実行され得る。このような認証は、例えば、生体認証、ユーザデバイスと関連付けられた要素の認証、またはユーザの行動分析と関連付けられた要素を含むことができる。第２の要素認証の終了時に、第２のＩｄＰ３０９ｂは、例えば、第２のチケットなどの、チケットを生成できる。第２のチケットは、ランダムノンスを含むことができ、および／またはそのチケットは、暗号化して生成され得る。第２のチケットは、第２のＡＡ３１０ｂに送信され得る。あるいは、例示的な実施形態において、第２のＡＡ３１０ｂは、第２のＩｄＰ３０９ｂによって使用される第２のチケットを生成する機構を使用して、第２のチケットを生成し、従って、その第２のチケットは、第２のＩｄＰ３０９ｂから第２のＡＡ３１０ｂに送信されない。３４０において、３３４において送信されたトリガに応答して、第２のＡＡ３１０ｂは、第２のチケットおよびそれに関連付けられた新鮮度をＭＦＡＰ１１２に送信する。同様に、３４２において、第２のＩｄＰ３０９ｂは、第２のチケットおよびそのチケットに関連付けられた認証の新鮮度をマスターＩｄＰ３０８に送信できる。あるいは、例えば、ローカル認証が第２のＡＡ３１０ｂによって実行されるのであれば、第２のＡＡ３１０は、第２のチケットを生成して、その第２のチケットをＭＦＡＰ１１２にフォワードすることができる。

【００３２】

図３について続けて参照すると、図示された実施形態により、３４４において、ＭＦＡＰ１１２は、第１のチケットと第２のチケットを統合する。ＭＦＡＰはさらに、ＣＡ３０４の集約が実現された保証レベルおよび新鮮度レベルを計算できる。一例において、集約保証レベルは、各認証要素と関連付けられた保証レベルを合算することによって計算される。別の例として、保証レベルは、両方の認証要素に対応する集約保証レベルにおいて一方の認証要素が他方の認証要素と比較してより重く重み付けされるように、重み付けされ得る。各認証要素のエッジを因数分解する、新鮮度減衰関数などの、付加的なパラメータは、集約された保証要素を計算する時に考慮され得る。別の実施形態において、ＭＦＡＰ１１２は、計算された集約保証レベルを送信しないが、その代わりに認証の要素のそれぞれに関係する情報をマスターＩｄＰに送信し、そしてそのマスターＩｄＰは、集約保証レベルを計算することができる。３４６において、ＣＡ３０４は、第１および第２のチケットをマスターＩｄＰ３０８に提示する。ＣＡ３０４はさらに、認証のそれぞれと関連付けられた実現された保証レベルおよび新鮮度をマスターＩｄＰ３０８に送信できる。３４８において、マスターＩｄＰ３０８は、そのマスターＩｄＰがＣＡ３０４から受信した第１のチケットと第２のチケットをそれぞれ、第１のＩｄＰ３１０ａと第２のＩｄＰ３１０ｂによってそのマスターＩｄＰに配信された第１のチケットと第２のチケットと比較する。３５０において、例えば、第１のチケットの両方が互いにマッチして、第２のチケットの両方が互いにマッチすれば、マスターＩｄＰ３０８は、アサーションを作成する。マスターＩｄＰ３０８は、そのアサーションをＳＰ３０６に送信する。送信されるアサーションは、遂行された多要素認証によって実現された保証レベルおよび新鮮度レベルを含むことができる。あるいは、例えば、ローカル認証が実行されたのであれば、ＭＦＡＰ１１２は、そのチケットおよびアサーションを直接ＳＰ３０６に提示できる。３５２において、図示された実施形態により、ＳＰ３０６は、アサーションを検証して、成功メッセージをＣＡ３０４に提供し、それによってＣＡ３０４およびＣＡ３０４のユーザにＳＰ３０６によって提供されるリクエストされたサービスへのアクセスを提供する。

【００３３】

図４Ａを参照すると、例示的な実施形態により、ＯＩＤ－ＧＢＡシステム４００ａは、三要素認証を提供するために使用される。ＯＩＤ－ＧＢＡシステム４００は、ＵＥ４０４、ＵＥ４０４にある第１のＡＡ４１０ａ、第２のＡＡ４１０ｂ、第３のＡＡ４１０ｃ、Ｕ

Ｅ４０４にあるＭＦＡＰ１１２、オーバーザトップ（ＯＴＴ）ＳＰ４０６（ＲＰ４０６と呼ぶこともできる）、第１のＩｄＰ４０９ａ（マスターＩｄＰと呼ぶことができる）、第２のＩｄＰ４０９ｂ、第３のＩｄＰ４１０ｂを含む。例えば、ブラウザなどの、クライアントエージェント（ＣＡ）もＵＥ４０４にあるものとすることができる。

【００３４】

４１２において、図示された実施形態により、ＵＥ４０４のユーザは、ＵＥ４０４、および特にＵＥ４０４のＣＡ経由で（ＳＰ４０４によって提供される）サービスへのアクセスをリクエストする。ＵＥ４０４は、ＳＰ４０６と通信することができ、そしてその通信は、ユーザと関連付けられたユーザが供給した識別子（ＩＤ）を含むことができる。ユーザＩＤに基づいて、４１４において、ＳＰ４０６は、発見を遂行し、そしてユーザＩＤと関連付けられた第１のＩｄＰ４０９ａと関連付ける。第１のＩｄＰ４０９ａは、ＯｐｅｎＩＤアイデンティティプロバイダ（ＯＰ）またはネットワークアプリケーション機能（ＮＡＦ）と関連付けられた機能性を遂行することができ、従って、第１のＩｄＰ４０９ａをＯＰ４０９ａまたはＮＡＦ４０９ａと呼ぶこともできる。４１６において、図示された実施形態により、ＳＰ４０６は、例えば、ＳＰ４０６のポリシーに基づいて、ＳＰ４０６によって提供されるリクエストされたサービスにユーザがアクセスするために要求される認証の保証のレベルを判定できる。保証のレベルに基づいて、例えば、ＳＰ４０６は、ＳＰ４０６によって提供されるリクエストされたサービスにユーザがアクセスするために、多要素認証が要求されていることを判定できる。ＳＰ４０６はまた、ＳＰ４０６によって提供されるリクエストされたサービスにユーザがアクセスするために、認証の適切な要素が実行されなければならないことも判定できる。４１８において、図示された実施形態により、ＵＥ４０４は、ＯｐｅｎＩＤ認証リクエストを経由する、ＯＰ４０９ａと呼ぶこともできる、第１のＩｄＰ４０９ａにリダイレクトされる。ＳＰ４０６はまた、そのＳＰの保証のレベル要件をＵＥ４０４に伝達することもできる。さらに、４１８において、ＭＦＡＰ１１２のサービスは、例えば、図１および図３に対して説明したように、呼び出される。４２０において、ＵＥ４０４、特に第１のＡＡ３１０ａ、および第１のＩｄＰ３０９ａは、第１の認証を実行する。第１の認証は、第１の認証要素を使用してユーザを認証することができる。第１の認証要素は、第１のＩｄＰ３０９ａと関連付けられたユーザ名およびパスワードを含むことができる。例えば、ユーザは、ＵＥ４０４においてユーザ名およびパスワードを入力することができ、そして第１のＩｄＰ３０９ａは、そのユーザ名およびパスワードを検証することができる。あるいは、ローカル認証が実行されていれば、例えば、ローカル認証エージェント（第１のＡＡ４１０ａ）は、ＩｄＰ４０９ａの関与を用いずにユーザ名およびパスワードを検証できる。ローカル認証は、ＵＥ４０４によって遂行される認証を指す。従って、図示された実施形態により、第１の認証は、ユーザの認証である。４２２において、第１の認証に応答して、第１のＩｄＰ４０９ａは、第１の認証が成功したのであれば、第１のチケットを生成する。例えば、第１のチケットは、第１の要素認証が成功したことを示すことができる。４２４において、図示された実施形態により、成功した認証が実行されたという証拠を表す、第１のチケットは、ＵＥ４０４に送信される。その第１のチケットは、そのチケットに関連付けられた新鮮度レベルを含むことができる。４２６において、ＵＥ４０４は、その第１のチケットを格納する。４２８において、第１のＩｄＰ４０９ａは、その第１のチケットを格納する。あるいは、ユーザがＡＡ４１０ａによってローカルに認証されるのであれば、そしてそのローカル認証が成功したのであれば、ＡＡ４１０ａは、第１のチケットを生成して第１のチケットをＭＦＡＰ１１２に送信して、その第１のチケットがＭＦＡＰ１１２のみに格納されるようにできることが理解されよう。従って、ＭＦＡＰ１１２は、例えば、ローカルリンク経由で、ＡＡ４１０ａによる成功した認証を表すアサーションを受信できる。

【００３５】

図４Ａについて続けて参照すると、４３０において、図示された実施形態により、第２のＡＡ４１０ｂおよび第２のＩｄＰ４０９ｂは、第２の認証を実行する。第２の認証は、ＵＥ４０４のユーザの認証（例えば、ユーザの生体認証）、ＵＥ４０４の認証。ユーザ４

０４のＣＡと関連付けられたデバイスの認証等を備えることができる。例えば、第２のチケットなどの、チケットは、認証が成功すると、４３２において、第２のＩｄＰ４０９ｂによって生成され得る。４３４において、図示された実施形態により、第２のチケットは、第２のＡＡ４１０ｂに送信される。第２のＩｄＰ４０９ｂによって生成されるチケットは、セキュアな方法で第２のＡＡ４１０ｂに送信され得る。あるいは、第２のチケットは、第２のＩｄＰ４１０ｂによって使用される第２のチケットを生成する同様の機構を使用して、第２のＡＡ４１０ｂによって生成され得る。それにもかかわらず、第２の認証の終了時に、第２のＡＡ４１０ｂと第２のＩｄＰ４０９ｂの両方は、第２の認証の証拠を有することができ、その証拠は、図４Ａによる第２のチケットと呼ばれる。あるいは、例えば、ローカル認証が第２のＡＡ４１０ｂによって実行されるのであれば、そのＡＡ４１０ｂは、第２のチケットを生成できる。４３６において、第２のＡＡ４１０ｂは、応答をＵＥ４０４に、特にＭＦＡＰ１１２に送信できる。その応答は、その第２のチケットを含むことができる。その応答は、例えば、ローカルリンク経由などの、第２のＡＡ４１０ｂをＵＥ４０４に接続する通信リンク経由で送信される。４３８において、ネットワーク側において、第２のＩｄＰ４０９ｂは、第２のチケットおよびそのチケットに関連付けられた新鮮度（例えば、認証が実行された時の日付／時間）を第１のＩｄＰ４０９ａに送信できる。４４０と４４２において、第２のチケットはそれぞれ、ＵＥ４０４と第１のＩｄＰ４０９ａに格納される。あるいは、例えば、ローカル認証が実行されると、実施形態により、第２のチケットは、ＭＦＡＰ１１２のみに格納される。

【００３６】

さらに図４Ａを参照すると、４４４において、図示された実施形態により、第３のＡＡ４１０ｃおよび第３のＩｄＰ４０９ｃは、第３の認証を実行する。第３の認証は、ＵＥ４０４のユーザの認証（例えば、ユーザの生体認証、ユーザの行動的特性）、ＵＥ４０４の認証、ＵＥ４０４のＣＡと関連付けられたデバイスの認証等を備えることができる。認証が成功すると、例えば、第３のチケットなどの、チケットは、４４６において、第３のＩｄＰ４０９ｃによって生成され得る。４４８において、図示された実施形態により、第３のチケットは、第３のＡＡ４１０ｃに送信される。第３のＩｄＰ４０９ｃによって生成されるチケットは、セキュアな方法で第３のＡＡ４１０ｃに送信され得る。あるいは、第３のチケットは、第３のＩｄＰ４１０ｃによって使用される第３のチケットを生成する同様の機構を使用して、第３のＡＡ４１０ｃによって生成され得る。それにもかかわらず、第３の認証の終了時に、第３のＡＡ４１０ｃと第３のＩｄＰ４０９ｃの両方は、第３の認証の証拠を有することができ、その証拠は、図４Ａによる第３のチケットと呼ばれる。あるいは、例えば、ローカル認証が実行されると、例示的な実施形態により、第３のチケットは、第３のチケットが生成される第３のＡＡ４１０ｃのみに格納されることが可能である。４５０において、第３のＡＡ４１０ｃは、応答をＵＥ４０４に、特にＭＦＡＰ１１２に送信できる。その応答は、その第３のチケットを含むことができる。従って、ＭＦＡＰ１１２は、例えば、ローカルリンク経由で、ＡＡ４１０ｃによって成功した認証を表すアサーションを受信できる。その応答は、例えば、ローカルリンク経由などの、第３のＡＡ４１０ｃをＵＥ４０４に接続する通信リンク経由で送信される。４５２において、ネットワーク側において、第３のＩｄＰ４０９ｂは、第３のチケットおよびそのチケットに関連付けられた新鮮度（例えば、認証が実行された時の日付／時間）を第１のＩｄＰ４０９ａに送信できる。あるいは、例えば、第３のＡＡ４１０ｃが第３のチケットを生成したのであれば、そのチケットは、第３のＩｄＰ４０９ｃからマスターＩｄＰ４０９ａに転送されないことが理解されよう。４５４および４５６において、第３のチケットはそれぞれ、ＵＥ４０４と第１のＩｄＰ４０９ａに格納される。代替的実施形態において、第３のチケットは、ＵＥ４０４のＭＦＡＰ１１２のみに格納され得る。

【００３７】

４５８において、ＵＥ４０４、例えば、ＵＥ４０４のＣＡは、第１、第２、および第３のチケットを第１のＩｄＰ４０９ａに送信する。ＵＥ４０４はさらに、保証レベルおよび認証のそれぞれと関連付けられた新鮮度を第１のＩｄＰ４０９ａに送信できる。４６０に

おいて、第１のＩｄＰ４０９ａは、それがＵＥ４０４から受信した第１、第２、および第３のチケットをそれぞれ、第１のＩｄＰ４０９ａに格納されている第１、第２、および第３のチケットと比較する。例えば、第１のチケットが互いにマッチし、第２のチケットが互いにマッチし、そして第３のチケットが互いにマッチすると、第１のＩｄＰ４０９ａは、図示された三要素認証を検証することができる。従って、４６２において、チケットが検証されると、第１のＩｄＰ４０９ａは、三要素アサーションを作成し、その三要素アサーションをＳＰ４０６に送信する。送信されるアサーションは、遂行された多要素認証によって実現された保証レベルおよび新鮮度レベルを含むことができる。ＳＰ４０６は、そのアサーションを検証して、ＵＥ４０４にリクエストしたサービスにアクセスさせることができる。あるいは、例えば、ローカル認証のみが実行されたのであれば、ＵＥ４０４のＭＦＡＰ１１２は、チケットおよびアサーションを直接ＳＰ４０６に送信できる。

【００３８】

図４Ｂは、ＯＩＤ－ＧＢＡシステム４００を使用する別の例を示す、別のフロー図である。図４Ｂにおいて、ＯＩＤ－ＧＢＡシステム４００を使用して、二要素認証を提供する。三要素認証の代わりに二要素認証を描いているのに加え、図４Ｂはまた、以下で説明されるように、図４Ａと比べて付加的な詳細も描いている。図示された実施形態により、ユーザ名および暗号値は、第１要素の認証の一部として取得され、そしてパスワードは、第２要素の認証のために取得される。例えば、モバイル端末であってよい、図示されたＵＥ４０４は、ＣＡ（ブラウザエージェント）およびＭＦＡＰ１１２を含む。図示された実施形態により、ＡＡ４１０ｂは、ＵＩＣＣによって実装され、そして第１のＡＡ４１０ａは、ユーザ入力を使用してＵＥ４０４のユーザを認証する。

【００３９】

図４Ｂを参照すると、４１２において、ＵＥ４０４を使用するユーザは、ＯＴＴ ＳＰ４０６によって提供されるサービスへのアクセスをリクエストする。図示された実施形態により、ユーザは、ＩｄＰ／ＯＰ４０９ａと関連付けられたユーザのアイデンティティを使用してアクセスをリクエストする。４１４において、ＳＰ４０６は、ユーザのアイデンティティに基づいて、ＩｄＰ／ＯＰ／ＮＡＦ４０９ａの発見および関連付けを遂行する。４１６において、例えば、ＳＰ４０６のポリシーおよびユーザによってリクエストされたサービスに基づいて、ＳＰ４０６は、ユーザがリクエストしたサービスにアクセスするための適切な保証レベルを判定する。例えば、４１６において、ＳＰ４０６は、適切な保証レベルを実現するために、複数の認証要素が遂行されなければならないことを判定できる。４１８において、図示された実施形態により、ＵＥ４０４は、ＯｐｅｎＩＤ認証リクエストを経由する、ＯＰ４０９ａまたはＮＡＦ４０９ａと呼ぶこともできる、第１のＩｄＰ４０９ａにリダイレクトされる。ＳＰ４０６はまた、その保証レベル要件をＵＥ４０４に伝達することもできる。保証レベルは、ＭＦＡＰ１１２に格納され得る。４１９ａにおいて、ＵＥ４０４は、ＨＴＴＰＳ ＧｅｔリクエストをＯＰ４０９ａに送信する。そのリクエストは、多要素認証が要求されているという表示を含む。４１９ｂにおいて、ＯＰ４０９ａは、ＨＴＴＰＳ応答をＵＥ４０４に提供する。その応答は、ＵＥのユーザを認証することができる認証エージェントの識別子に対するリクエストを含む。あるいは、例えば、識別子がユーザによって以前にＳＰ４０６に提示されていたのであれば、前述のステップはスキップされる。ある場合には、４１９ｂにおいて、二次識別子は、ユーザまたはＵＥ４０４によってＩｄＰ／ＯＰ／ＮＡＦ４０９ａに提供され得る。その応答はさらに、ユーザパスワードに対するリクエストを含むことができる。図示された実施形態により、ユーザを認証できるＡＡは、ＵＥ４０４にあるものとすることができる、第１のＡＡ４１０ａである。４２１において、ＵＥ４０４は、第１のＡＡ４１０ａの識別子、パスワードのダイジェスト、およびパスワードと関連付けられた新鮮度値を含むことができるＨＴＴＰＳ Ｇｅｔリクエストを提供する。あるいは、例えば、ローカル認証が実行されていれば、ユーザは、ユーザ名およびパスワードをＵＥ４０４上のＡＡ４１０ａに提供できる。この場合、ステップ４１９から４２４までがスキップされる。４２２において、図４Ｂに示した図示された実施形態により、ＯＰ４０９ａは、認証されているユーザに応答して第１の

チケットを生成する。例えば、第１のチケットは、第１の要素認証が成功したことを示すことができる。４２４において、図示された実施形態により、成功した認証が実行された証拠を表す、第１のチケットは、ＵＥ４０４に送信される。あるいは、例えば、ローカル認証が実行されると、第１のチケットは、ＡＡ４１０ａによって発行される。チケットは、その後、ＭＦＡＰ１１２に格納され、関連付けられた新鮮度またはタイムスタンプ情報もＭＦＡＰ１１２によって格納され得る。４２４において、図４Ｂに示した図示された実施形態により、第２の認証要素を使用する第２の認証の識別子をリクエストするＨＴＴＰＳ応答メッセージを有する第１のチケットが送信される。第１のチケットは、それに関連付けられた新鮮度レベルを含むことができる。

【００４０】

さらに図４Ｂを参照すると、４２５において、ＭＦＡＰ１１２は、認証の第２の要素と関連付けられた識別子をＩｄＰ／ＯＰ／ＮＡＦ４０９ａに送信できる。その識別子は、ＵＥアイデンティティ（ＩＤ）、生体ＩＤ、または第２の要素と関連付けられたその他のアイデンティティを表すことができる。あるいは、ローカル認証が実行されていれば、ＭＦＡＰ１１２は、第２のＡＡ４１０ｂとして図示されている、適切なローカル認証エージェントを用いてローカル認証を開始する。４２７において、ＵＥ４０４のクライアントエージェントのアイデンティティは、第２のＡＡ４１０ｂとして図示されている、認証エージェントにマップされる。このマッピングは、ユーザと関連付けられた適切なＡＡおよび４２５においてＭＦＡＰによって提供された第２の要素識別子を判定するデータベースクエリを遂行することによって達成され得る。４２９において、ＩｄＰ／ＯＰ／ＮＡＦ４０９ａは、適切なＡＡ４１０ｂを使用してＧＢＡ認証をトリガするために、プッシュメッセージを開始する。あるいは、プッシュメッセージは、ＵＥ４０４上のＭＦＡＰ１１２に送信されことができ、ＭＦＡＰは、その後、ＭＦＡＰ１１２とＡＡ４１０ｂとの間のセキュアなトンネルリンクを設置できる（ステップ４２９ｂ）。４２９ｂにおいて、ＵＥ４０４は、ＩｄＰ／ＯＰ／ＮＡＦ４０９ａのＵＲＬを第２のＡＡ４１０ｂに書き込むことができる。４３１において、第２のＡＡ４１０ｂは、ＮＡＦ４０９ａを用いてＧＢＡ認証プロセスを開始する。４３３において、ＩｄＰ／ＯＰ／ＮＡＦ４０９ａは、ＧＢＡチャレンジを第２のＡＡ４１０ｂに発行する。４３５において、第２のＡＡ４１０ｂブートストラッピングサーバ機能（ＢＳＦ）４１１との間でＧＢＡブートストラッピングが遂行される。４３７において、第２のＡＡ４１０ｂは、ブートストラッピングアイデンティティを用いてチャレンジに応答する。４３９において、ＮＡＦ４０９ａは、ＢＳＦ４１１を用いて鍵を読み出して、ユーザを認証する。

【００４１】

図４Ｂについて続けて参照すると、ひとたび成功した認証がＡＡ４１０ｂによって実行されると、ＡＡ４１０ｂは、ＮｏｎｃｅＡＡとして図示されている、ノンス、およびセッションＩＤを生成する。ＮｏｎｃｅＡＡは、例えば、暗号鍵、デジタル署名、または一時的アイデンティティなどの、暗号値であってよい。一時的アイデンティティは、認証またはドメインと関連付けられることができる。例示的な一時的アイデンティティは、Ｂ－ＴＩＤ、ワンラウンドトリップ認証（ＯＲＴＡ）ＩＤ、拡張型マスターセッション鍵（ＭＳＫ）名等を含む。セッションＩＤは、チャネルまたはフローまたはセッションを特定する固有のアイデンティティであってよい。例えば、セッションＩＤは、ＴＬＳチャネルＩＤ、ＨＴＴＰセッションＩＤ、ＥＡＰセッションＩＤ等であってよい。４４３ａにおいて、図示された実施形態により、ＡＡ４１０ｂは、ＨＴＴＰセッション内でセッションＩＤとＮｏｎｃｅＡＡをそれぞれ、「ユーザ名」フィールドと「パスワード」フィールドにコピーすることによって、セッションＩＤとＮｏｎｃｅＡＡをＵＥ４０４のＣＡに送信する。ＨＴＴＰに加えて他のプロトコルが使用されてもよいし、その他のプロトコルは、ユーザ名およびパスワードを使用しなくてもよいことが理解されよう。従って、４４３ｂにおいて、ＮｏｎｃｅＡＡおよびパスワードは、第２のＡＡ４１０ｂからＣＡに送信される。ＭＦＡＰ１１２は、第１のＡＡ４１０ａによって発行された第１のチケットを格納する。ＭＦＡＰ１１２は、ＡＡ４１０ｂによって発行されたＮｏｎｃｅＡＡおよびセッションＩＤ

を格納できる。従って、第１の要素認証は、第１の要素認証と関連付けられたセッションＩＤにバインドされ、例えば、暗号化してバインドされ得る。例示的な実施形態において、認証の各要素、例えば、認証の各要素の結果として生じる各チケットは、多要素認証においてそれぞれのセッションＩＤにバインドされる。例えば、第１のチケットは、第１の要素認証を表すセッションアイデンティティ（ＩＤ）にバインドされることができ、第２のチケットは、第２の要素認証を表すセッションＩＤにバインドされることができ、第３のチケットは、第３の要素認証を表すセッションＩＤにバインドされることができる。４４５において、図示された実施形態により、ＭＦＡＰ１１２は、第１のチケットをＩｄＰ／ＯＰ／ＮＡＦ４０９ａに送信する。４４７において、ＩｄＰ／ＯＰ／ＮＡＦ４０９ａは、ＵＥ４０４のユーザおよびＣＡを認証するために、チケット、ＮｏｎｃｅＡＡ、およびセッションＩＤを検証する。例えば、ＩｄＰ／ＯＰ／ＮＡＦ４０９ａは、チケットに基づいてＮｏｎｃｅＡＡおよびセッションＩＤを生成することができ、そしてＩｄＰ／ＯＰ／ＮＡＦは、それがＧＢＡプロセスの一部として取得したＮｏｎｃｅＡＡおよびセッションＩＤを、生成されたＮｏｎｃｅＡＡおよびセッションＩＤと比較できる。４４９および４５１において、ユーザ／ＣＡが認証されると、ＩｄＰ／ＯＰ／ＮＡＦ４０９ａは、ＨＴＴＰリダイレクトメッセージを使用してアサーションをＵＥ４０４経由でＳＰ４０６に送信する。あるいは、例えば、ローカル認証のみが実行されたのであれば、ＭＦＡＰ１１２は、チケット、ＮｏｎｃｅＡＡ、およびセッションＩＤをＳＰ４０６に送信できる。他の場合では、すべての認証結果を組み合わせる組み合わせアサーションは、ＭＦＡＰ１１２によってＳＰ４０６に送信される。組み合わせアサーションは、１つまたは複数のセッションアイデンティティ（ＩＤ）のそれぞれをまとめて暗号化してバインドできる。さらに、組み合わせアサーションは、その組み合わせアサーションに対応する保証レベルおよび新鮮度値を含むことができる。４５３において、ＳＰ４０６が受信するアサーションは、ＳＰ４０６によって検証される。例えば、アサーションが少なくとも、ＳＰ４０６の認証要件（例えば、保証レベル）を満たすならば、そのユーザは、リクエストしたサービスへのアクセスを許可される。

【００４２】

図４Ｃを参照すると、ＯＩＤ－ＧＢＡシステム４００は、ブラウザエージェント（ＢＡ）４０５と呼ぶこともできる、クライアントエージェント（ＣＡ）４０５がＵＥ４０４とは別個である、例示的な実施形態従って二要素認証を提供するために使用される。従って、図４Ｃに図示された呼フローは、例示的な分割端末の実装を表す、ＯＩＤ－ＧＢＡシステム４００である。

【００４３】

さらに図４Ｃを参照すると、４１９ａにおいて、開始ＨＴＴＰＳリクエストは、ＯｐｅｎＩＤリダイレクトの後に送信される。４１９ｂにおいて、ＨＴＴＰＳ Ｕｎａｕｔｈｏｒｉｚｅｄ Ｒｅｓｐｏｎｓｅは、ＣＡ４０５に送信される。４２０において、図示された実施形態により、ユーザは、（例えば、ユーザＩＤおよびパスワードを使用して）ＯＰ４０９ａに対する第１の要素認証を進める。パスワードの許容できる新鮮度は、ＯＰ４０９ａのポリシーによって対処され得る。例えば、ＯＰポリシーは、どのくらい長くパスワードがブラウザ、例えば、ＣＡ４０５にキャッシュされるかを示すことができる。例示的な実施形態において、例えば、修正されたＵＩＣＣなどの、信頼のある実行環境は、このようなポリシーを強制する。４２７において、第１の要素認証が成功すると、ＯＰ４０９ａは、ＵＥ４０４、特にＡＡ４１０ａをＣＡ４０５にマップする。４２２において、図示された実施形態により、ＯＰ４０９ａは、ユーザの成功した認証を表す第１のチケットと呼ぶことができる、チケットを生成する。４２４において、第１のチケットは、ＣＡ４０５にフォワードされる。４２４において送信されるメッセージは、ＨＴＴＰＳによって保護され得る。４２９において、ＧＢＡは、メッセージによってトリガされる。４３１において、ＨＴＴＰＳリクエストは、ＧＢＡ認証を始動する。４３３において、ＨＴＴＰＳ ＧＢＡチャレンジは、ＵＥ４０４に送信される。４３７において、ブートストラッピングアイデンティティ（Ｂ－ＴＩＤ）を有するＨＴＴＰＳ ＧＢＡチャレンジＲｅｓｐｏｓｅ

は、ＵＥ４０４、例えば、第１のＡＡ４１０ａからＮＡＦ／ＯＰ４０９ａに送信される。４３９ａにおいて、ＮＡＦ／ＯＰ４０９ａは、例えば、$Nonce_{NAF}$などの、ノンスで応答する。４４１において、ＡＡ４１０ａは、$Nonce_{NAF}$を使用して、パスワードを生成する。４４３ａにおいて、図示された実施形態により、パスワードは、ローカルリンクを介してＣＡ４０５にコピーされる。４４３ａにおいて、第１のチケットは、ユーザ名にコピーされ、そしてローカルリンクを介して受信されたパスワードは、ＨＴＭＬ形式にコピーされる。４４５において、承認ヘッダを有するＨＴＴＰゲットリクエスト(get request)は、ＩｄＰ４０９ａに送信される。ＩｄＰ４０９ａは、認証アサーションを有するリダイレクトを適切なＳＰに送信する。例示的な実施形態において、４４９においてそのメッセージが送信された後、ＵＥ４０４は、ＯｐｅｎＩＤプロトコルの実装を継続することができる。

【００４４】

図４Ｄは、例示的な実施形態により、ユーザ認証中に生成されるチケットがＧＢＡプロセスを通じてループされる三要素認証のフロー図である。図４Ｄに示した図示された実施形態において遂行される多くのステップは、上記の図４Ａに対して説明される。図４Ｄを参照すると、生成されるチケットは、ＭＦＡＰ１１２によって完了された認証の終了時に４５８において、ＩｄＰ４０９ａに提示される。しかし各認証要素の後にチケットを送信する代わりに、チケットは、図示されているように、三要素認証が完了した後に送信され得る。あるいは、認証要素のそれぞれが、例えば、ＵＥ４０４上でローカルに実行されると、ＭＦＡＰ１１２は、そのチケットおよびアサーションを直接ＳＰ４０６に送信できる。例示的な実施形態において、チケットのそれぞれがループされ、それによって３つの認証プロトコルのそれぞれがバインドされるために、第３のチケットは、三要素認証が完了した後に送信される。図４Ｅは、付加的な詳細が描かれている、図４Ｄに示した三要素認証のフロー図である。図４Ｆは、図４Ｄで描かれた例示的な呼フローの圧縮バージョンである。

【００４５】

図４Ｅを参照すると、図示された実施形態により、４１２から４２１におけるメッセージは、ユーザ認証が遂行される、図４Ｄに対して上述した対応するメッセージと実質的に同じである。ユーザ認証が遂行された後、４２２において、第１のチケットは、ＩｄＰ／ＯＰ／ＮＡＦ４０９ａによって生成される。さらに、第２の要素認証は、ＭＦＡＰ１１２に送出される。４２５において、ＭＦＡＰ１１２は、第２の認証要素ＩＤを用いてＩｄＰ／ＯＰ／ＮＡＦ４０９ａに応答する。第２の認証要素ＩＤを使用して、４２７において、ＯＰ４０９ａは、クライアントエージェントを第２のＡＡ４１０ｂにマップする。ユーザ認証からのセッションまたはチャネルＩＤも第２のＡＡ４１０ｂにマップされ得る。４２９ａにおいて、ＩｄＰ／ＯＰ／ＮＡＦ４０９ａは、ＧＢＡ認証を始動するために、第２のＡＡ４１０ｂを用いてＧＢＡ認証プロセスを開始する。ＩｄＰ／ＯＰ／ＮＡＦ４０９ａによって第２のＡＡ４１０ｂに送信されるメッセージの一部を、４２９ａにおいて、４２２において実行された成功した第１の要素認証の一部として生成された第１のチケットにすることができる。あるいは、ＧＢＡ認証トリガメッセージ（４２９ｂおよび４２９ｃを参照のこと）は、ＭＦＡＰ１１２によって開始されることができ、従って、第１のチケットは、４２９ｂまたは４２９ｃのメッセージの一部としてＭＦＡＰ１１２から第２のＡＡ４１０ｂに渡されることができる。

【００４６】

４３９において、図示された実施形態により、ＮＡＦ鍵は、ＧＢＡプロセスの一部として得られ、そして第１のチケットは、ＧＢＡ－専用鍵と呼ぶこともできる、ＮＡＦ鍵にバインドされ得る。ＩｄＰ／ＮＡＦ４０９ａは、ＢＳＦ４１１からＮＡＦ鍵をＧＢＡプロセスの一部として読み出す。４４１において、第２のＡＡ４１０ｂは、任意のランダム値または暗号を表すことができる、ＮｏｎｃｅＡＡを生成し、ＧＢＡプロセスの一部として生成されたＮＡＦ鍵を使用してパスワードを生成する。第２のＡＡ４１０ｂは、例えば、第２のＡＡ４１０ｂをＵＥ４０４と接続するローカルリンクを使用して、ＮｏｎｃｅＡＡお

よびパスワードをＵＥ４０４上のＣＡに送信する（４４３ｂを参照のこと）。４４３ａにおいて、例えば、ＡＡ４１０ｂがＵＥ４０４上にあったならば、ＮｏｎｃｅＡＡおよびパスワードは、ユーザによってＣＡ上のＨＴＴＰ形式のページにコピーされ得る。４４５において、ＮｏｎｃｅＡＡおよびパスワードは、ＩｄＰ／ＯＰ／ＮＡＦ４０９ａに提示され得る。４３９において取得されたＧＢＡ ＮＡＦ鍵を使用して、および第１のチケットから生成されたＮｏｎｃｅＡＡおよびパスワードを使用して、ＩｄＰ／ＮＡＦ４０９ａは、ＵＥ４０４のＣＡによって送信されたパスワードを検証する（４４７を参照のこと）。例えば、マッチが存在すれば、認証アサーションを包含するメッセージは、ＩｄＰ／ＮＡＦ／ＯＰ４０９ａによってＵＥ４０４に送信され、そしてメッセージは、ＳＰ４０６にリダイレクトされる（４４９および４５１を参照のこと）。ローカル認証のみが実行されたのであれば、例えば、ＭＦＡＰ１１２は、アサーションがＩｄＰ／ＮＡＦ／ＯＰ４０９ａに送信されずに、アサーションを直接ＳＰ４０６に送信できる。そのアサーションは、多要素認証に対応する保証および新鮮度レベル情報を包含するまたは示すことができる。

【００４７】

図４Ｆを参照すると、４１９ａにおいて、開始ＨＴＴＰＳリクエストは、ＯｐｅｎＩＤリダイレクトの後に送信される。４１９ｂにおいて、ＨＴＴＰＳ Ｕｎａｕｔｈｏｒｉｚｅｄ Ｒｅｓｐｏｓｅは、ＣＡ４０５に送信される。４２０において、図示された実施形態により、ユーザは、（例えば、ユーザＩＤおよびパスワードを使用して）ＯＰ４０９ａに対する第１の要素認証を進める。パスワードの許容できる新鮮度は、ＯＰ４０９ａのポリシーによって対処され得る。例えば、ＯＰポリシーは、どのくらい長くパスワードがブラウザ、例えば、ＣＡ４０５にキャッシュされるかを示すことができる。例示的な実施形態において、例えば、修正されたＵＩＣＣなどの、信頼のある実行環境は、このようなポリシーを強制する。４２７において、第１の要素認証が成功すると、ＯＰ４０９ａは、ＵＥ４０４、特にＡＡ４１０ａをＣＡ４０５にマップする。４２２において、図示された実施形態により、ＯＰ４０９ａは、ユーザの成功した認証を表す第１のチケットと呼ぶことができる、チケットを生成する。上述のように、チケットという語は、本明細書で使用される際、ランダム値、暗号値、アサーション等を指す。例えば、チケットは、デジタル署名、暗号鍵、または一時的アイデンティティを表すことができる。４２４において、第１のチケットは、ＣＡ４０５にフォワードされる。４２４において送信されるメッセージは、ＨＴＴＰＳによって保護され得る。４２９において、ＧＢＡは、メッセージによってトリガされる。４３１において、ＨＴＴＰＳリクエストは、ＧＢＡ認証を始動する。４３３において、ＨＴＴＰＳ ＧＢＡチャレンジは、ＵＥ４０４に送信される。４３７において、ブートストラッピングアイデンティティ（Ｂ－ＴＩＤ）を有する第１のチケットを搬送するＨＴＴＰＳ ＧＢＡチャレンジＲｅｓｐｏｓｅは、ＵＥ４０４、例えば、第１のＡＡ４１０ａからＮＡＦ／ＯＰ４０９ａに送信される。さらに、４３７において、図４Ｆで示した図示された実施形態により、ＮＡＦ／ＯＰ４０９ａは、第１のチケットを受信して、第２の要素認証（例えば、ＵＩＣＣベースの認証）がステップ４２０から第１の要素認証（例えば、ユーザ認証）にバインドしていることを検証する。４３９ａにおいて、ＮＡＦ／ＯＰ４０９ａは、例えば、$Nonce_{NAF}$などの、ノンスで応答する。$Nonce_{NAF}$は、例えば、デジタル署名、暗号鍵、または一時的アイデンティティなどの、ランダムまたは暗号値であってよいことが認識されよう。４４１において、ＡＡ４１０ａは、パスワードおよび$Nonce_{NAF}$を生成する。４４３ａにおいて、図示された実施形態により、パスワードは、ローカルリンクを介してＣＡ４０５にコピーされる。４４３ａにおいて、第１のチケットは、ユーザ名にコピーされ、そしてローカルリンクを介して受信されたパスワードは、ＨＴＭＬ形式にコピーされる。４４５において、承認ヘッダを有するＨＴＴＰゲットリクエスト(get request)は、ＩｄＰ４０９ａに送信される。ＩｄＰ４０９ａは、認証アサーションを有するリダイレクトを適切なＳＰに送信する。例示的な実施形態において、４４９においてそのメッセージが送信された後、ＵＥ４０４は、ＯｐｅｎＩＤプロトコルの実装を継続することができる。

【００４８】

図５Ａは、例示的な実施形態により、新鮮な認証結果がアサートされるフロー図である。図５Ａを参照すると、例示的な認証システム５００ａは、１つまたは複数の認証エージェント、例えば、第１のＡＡ５１０ａおよび第２のＡＡ５１０ｂ、ＣＡ５０４、ＳＰ５０６、マスターＩｄＰ５０８、およびＭＦＡＰ１１２を含む。２つの認証エージェントが認証システム５００に図示されているが、認証システム３００の認証エージェントの数は、所望通りに変えてもよいことが理解されよう。図示された実施形態により、第１の認証エージェント５１０ａと第２の認証エージェント５１０ｂはそれぞれ、第１のＩｄＰ５０９ａと第２のＩｄＰ５０９ｂに関連付けられる。さらに、ＣＡ５０４がＳＰ５０６によって提供されるサービスへのアクセスを提供することができるように、認証エージェント５１０ａおよび５１０ｂとアイデンティティプロバイダ５０９ａおよび５０９ｂは、二要素認証を可能にすることができる。ＳＰ５０６、マスターＩｄＰ５０８、第１のＩｄＰ５０９ａ、および第２のＩｄＰ５０９ｂをまとめて、ネットワーク側の認証システム５００と呼ぶことができる。ＳＰ５０６を、限定されないが、信頼するパーティー（ＲＰ）５０６と呼ぶこともできる。例示的な二要素認証が図５Ａに図示されているが、図５Ａに示した呼フローは、３以上の要素を使用する認証に拡張され得ることが理解されよう。図示された実施形態により、ＳＰ５０６におけるポリシー、およびＳＰ５０６によってＣＡ５０４およびＭＦＡＰ１１２に提供された結果として生じる要件は、第２の要素が新鮮であったので、再度実行される必要がなかったと見なす。例えば、第２の要素認証を実行する代わりに、以前の認証の結果を使用して、第２の要素が認証されていることをアサートする。第１の要素が古くなったと見なされた場合もあり、従って図示された実施形態により実行される。

【００４９】

さらに図５Ａを参照すると、５１２において、ユーザリクエストは、ＣＡ５０４経由で（ＳＰ３０６によって提供される）サービスにアクセスする。ＣＡ５０４は、ＳＰ５０６と通信することができ、そしてその通信は、ユーザと関連付けられたユーザＩＤを含むことができる。ユーザＩＤに基づいて、５１４において、ＳＰ５０６は、ユーザＩＤと関連付けられたマスターＩｄＰ５０８の発見を遂行して関連付ける。マスターＩｄＰ５０８は、ＯｐｅｎＩＤアイデンティティＰｒｏｖｉｄｅｒ（ＯＰ）またはネットワークアクセス機能（ＮＡＦ）と関連付けられた機能性を遂行することができ、従って、マスターＩｄＰ５０８をＯＰ５０８またはＮＡＦ５０８と呼ぶこともできる。５１６において、図示された実施形態により、ＳＰ５０６は、例えば、ＳＰ５０６のポリシーに基づいて、ＳＰ５０６によって提供されるリクエストされたサービスにユーザがアクセスするために、多要素認証が要求されていることを判定する。ＳＰ５０６はまた、ＳＰ５０６によって提供されるリクエストされたサービスにユーザがアクセスするために要求される認証の保証のレベルを判定することもできる。５１８において、図示された実施形態により、ＳＰ５０６は、その認証レベル要件をＣＡ５０４に伝達する。５２０において、ＣＡ５０４は、ＭＦＡＰ５１２のサービスを呼び出す。あるいは、ＳＰ５０６は、ユーザがＳＰ５０６によって提供されるサービスにアクセスするために要求される保証レベルをＩｄＰ／ＯＰ／ＮＡＦ５０８に伝達できる。ＩｄＰ／ＯＰ／ＮＡＦ５０８は、要求保証レベルに基づいて実行されなければならないであろう対応する認証要素を判定できる。ＣＡ５０４は、ＵＥ上のアプリケーションになり得る、ＭＦＡＰ１１２をトリガすることができる。例えば、そのアプリケーションは、例えば、Ａｎｄｒｏｉｄプラットフォームなどの、プラットフォームを有するインテントとしてトリガされ得る。ＣＡ５０４は、認証要素のリストをＭＦＡＰ１１２に提供できる。

【００５０】

５２２において、サービスにアクセスするために要求される保証のレベルに基づいて、例えば、ＭＦＡＰ１１２は、要求された保証レベルを実現するために遂行することができる認証要素のタイプおよび強度を判定する。ＭＦＡＰ１１２はさらに、要求された認証を遂行することができる認証エージェントを特定できる。例えば、図示された実施形態により、ＭＦＡＰ１１２は、第１のＡＡ５１０ａおよび第２のＡＡ５１０が認証要素の判定さ

れたタイプおよび強度と関連付けられていることを判定する。第１の認証エージェント５１ａが特定された後、５２４において、ＭＦＡＰ１１２は、第１の認証エージェント５１０ａが認証プロトコルを開始するように、トリガを第１の認証エージェント５１０ａに送信する。５２６において、マスターＩｄＰ５０８は、第１の認証エージェント５１０ａによって開始される認証プロトコルのコンテキストが作成されるプロセスをトリガする。例えば、マスターＩｄＰ５０８は、第１のＡＡ５１０ａと関連付けられた第１のＩｄＰ５０９ａと通信して、第１のＩｄＰ３０９ａが、第１のＡＡが開始した認証(the first AA-initiated authentication)のコンテキストを作成することをリクエストできる。５２４および５２６において遂行されるステップは、互いに並行して遂行され得る。

【００５１】

図５Ａについて続けて参照すると、５２８において、図示された実施形態により、第１のＡＡ５１０ａおよび第１のＩｄＰ５０９ａは、認証を実行する。その認証は、ＣＡ５０４のユーザの認証（例えば、ユーザの生体認証）、ＣＡ５０４の認証、ＣＡ３０４と関連付けられたデバイスの認証等を備えることができる。例えば、第１のチケットなどの、チケットは、認証が成功すると、第１のＩｄＰ５０９ａによって生成され得る。図示された実施形態により、第１のチケットは、第１の認証エージェント５１０ａに送信される。第１のＩｄＰ５０９ａによって生成されるチケットは、セキュアな方法で第１のＡＡ５１０ａに送信され得る。あるいは、第１のチケットは、第１のＩｄＰ５１０ｂによって使用される第１のチケットを生成する同様の機構を使用して、第１のＡＡ５１０ａによって生成され得る。それにもかかわらず、認証の終了時に、第１のＡＡ５１０ａと第１のＩｄＰ５０９ａの両方は、認証の証拠を有することができ、その証拠は、図５Ａによる第１のチケットと呼ばれる。

【００５２】

５３０において、５２４において受信されたトリガに応答して、第１のＡＡ５１０ａは、第１のチケットを備えるトリガ応答を送信できる。トリガ応答は、ＭＦＡＰ１１２に送信されることができ、そしてトリガ応答は、成功した認証が遂行されたことを証明できる。５３２において、ネットワーク側において、第１のＩｄＰ３０９ａは、第１のチケットおよびそのチケットに関連付けられた新鮮度（例えば、認証が実行された時の日付／時間）をマスターＩｄＰ３０８に送信できる。

【００５３】

５３４において、図示された例示的な実施形態により、例えば、ポリシーに基づいて、ＭＦＡＰ１１２は、第２の要素認証に対応する新鮮なチケットが使用可能であることを判定する。例えば、ＭＦＡＰ１１２は、チケット、例えば、第２のチケットの期限が満了しておらず、従って、第２の要素が認証されていることをアサートするために使用され得ることを判定できる。例えば、ＭＦＡＰは、チケットのタイムスタンプを特定して、そのタイムスタンプがＳＰの要件を順守することを判定できる。従って、ＭＦＡＰ１１２は、第２のＡＡ５１０ｂにコンタクトしない。５３６において、マスターＩｄＰ５０８は、第２の要素に対応する新鮮なチケット（例えば、第２のチケット）が使用可能であることを判定する。５３８において、ＭＦＡＰ１１２は、第１のチケットと第２のチケットを統合する。ＭＦＡＰはさらに、ＣＡ５０４の集約が実現された保証レベルおよび新鮮度レベルを計算できる。５４０において、ＣＡ５０４は、第１および第２のチケットをマスターＩｄＰ５０８に提示できる（図５Ｂを参照のこと）。ＣＡ５０４はさらに、認証のそれぞれと関連付けられた実現された保証レベルおよび新鮮度をマスターＩｄＰ５０８に送信できる。あるいは、再度図５Ａを参照すると、ＣＡ５０４は、チケットを直接ＳＰ５０６に提示できる。５４２において、マスターＩｄＰ５０８（またはＳＰ５０６）は、そのマスターＩｄＰがＣＡ５０４から受信した第１および第２のチケットを、そのマスターＩｄＰが以前に所有した第１および第２のチケットと比較する。５４４において、例えば、第１のチケットの両方が互いにマッチして、第２のチケットの両方が互いにマッチすれば、マスターＩｄＰ５０８（またはＳＰ５０６）は、アサーションを作成する。そのアサーションは、ＳＰ５０６に送信される。送信されるアサーションは、遂行された多要素認証によって

実現された保証レベルおよび新鮮度レベルを含むことができる。５４６において、図示された実施形態により、ＳＰ６０６は、アサーションを検証して、成功メッセージをＣＡ５０４に提供し、それによってＣＡ５０４およびＣＡ５０４のユーザにＳＰ５０６によって提供されるリクエストされたサービスへのアクセスを提供する。

【００５４】

あるいは、ある場合には、ＳＰ５０６によってリクエストされた保証レベルのみがＭＦＡＰ１１２に提供される。従って、５２２において、ＭＦＡＰは、要求された保証レベルを実現するために呼び出され得る要素および対応する認証エージェントを判定する。５２４において、図示された実施形態により、ＭＦＡＰ１１２は、第１の認証をトリガするために、ローカル認証を遂行する理由によりローカル要素ＡＡと呼ぶことができる、第１のＡＡ５１０ａと通信する。例えば、ＡＡがローカル要素ＡＡであれば、そのＡＡは、ユーザとインタラクトしてユーザ名／パスワードを取得できる。さらに、ローカル要素ＡＡは、ユーザに指紋リーダーを使用するように命令することができ、またはローカル要素ＡＡは、ユーザの行動的特性を分析し、ユーザによって所有されたデバイスを認証する等ができる。あるいは、例えば、ＩｄＰ５０９ａのサービスを使用することによって、認証の一部をネットワーク側で実行できる。ローカル要素認証のシナリオにおいて、第１のチケットは、ＡＡ５１０ａによって生成されて、ＭＦＡＰ１１２に送信される。あるいは、第１のチケットは、ＩｄＰ５０９ａによって生成されて、ＩｄＰ／ＮＡＦ／ＯＰ５０８に送信され得る。ひとたび第１の認証要素を使用する第１の認証が実行されると、図示された実施形態により、ＭＦＡＰ１１２は、古いと判定されていないタイムスタンプを用いて実行された既存の新鮮な第２の要素認証が存在するので、第２の要素を実行する必要がないことを判定する。５３０において取得された認証の第１の要素と関連付けられた第１のチケットに加え、５３８において、第２の要素と関連付けられた第２のチケットは、ＭＦＡＰ１１２によってリリースされる。５４０において、チケットと署名されたアサーションの両方は、（ＣＡ５０４経由で）ＭＦＡＰ１１２によってセキュアな方法でＳＰ５０６にリリースされ得る。５４２において、チケットは、暗号手段を使用するＳＰ５０６によって検証され、５４４においてアクセスがユーザに提供される。あるいは、５４０において、チケットは、ＣＡ５０４によってＩｄＰ／ＯＰ５０８に提示され得る。このような場合、ＩｄＰ／ＮＡＦ／ＯＰ５０８は、チケットを検証して、ＳＰ５０６によってＩｄＰ／ＮＡＦ／ＯＰ５０８に送信されるアサーションを作成する。ＳＰ５０６は、署名されたアサーションを検証して、サービスへのアクセスを提供できる。

【００５５】

図５Ｂについても参照すると、例示的な実施形態により、複数の新鮮な認証結果は、例示的なシステム５００ｂにおいてアサートされることができる。図５Ｂにおいて、ＳＰ５０６におけるポリシー、およびＳＰ５０６によってＣＡ５０４およびＭＦＡＰ１１２に提供された結果として生じる要件は、実行された以前の認証（第１および第２の要素）およびＭＦＡＰ１１２に格納された結果（第１および第２のチケット）は、５０６にとって十分に新鮮であると見なす。従って、その認証プロトコルは、実行されず、代わりに以前の認証要素の結果を使用して、認証をＳＰ５０６にアサートする。

【００５６】

例えば、５２７において、図示された例示的な実施形態により、第１の要素認証がトリガされた後、第１のＡＡ５１０ａは、第１の要素認証に対応する新鮮なチケットが使用可能であることを判定する。例えば、第１のＡＡ５１０ａは、チケット、例えば、第１のチケットの期限が満了しておらず、従って、第１の要素が認証されていることをアサートするために使用され得ることを判定できる。５２９において、第１のＩｄＰ５０９ａは、第１のチケットが新鮮であることを判定する。５３０において、第１のＡＡ５１０ａは、新鮮である、その第１のチケットを含む、トリガ応答を用いてトリガに応答する。従って、第１の新鮮なチケットは、ＭＦＡＰ１１２に送信される。５３２において、図示された実施形態により、第１のＩｄＰ５０９ａは、第１の新鮮なチケットをマスターＩｄＰ５０８に送信する。５２３において、ＭＦＡＰ１１２は、第２の認証エージェント５１０ｂが認

証プロトコルを開始することができるように、トリガを第２の認証エージェント５１０ｂに送信する。５３５において、マスターＩｄＰ５０８は、第２の認証エージェント５１０ｂによって開始されることができる認証プロトコルのコンテキストが作成されるプロセスをトリガする。５３３および５３５において遂行されるステップは、互いに並行して遂行され得る

【００５７】

図５Ｂについて続けて参照すると、５３７において、図示された実施形態により、第２のＡＡ５１０ｂは、第２の要素認証に対応する新鮮なチケットが使用可能であることを判定する。例えば、第２のＡＡ５１０ｂは、チケット、例えば、第２のチケットの期限が満了しておらず、従って、第２の要素が認証されていることをアサートするために使用され得ることを判定できる。５３９において、第２のＩｄＰ５０９ｂは、第２の要素に対応する新鮮なチケット（例えば、第２のチケット）が使用可能であることを判定する。５４１において、第２のＡＡ５１０ｂは、（５３３における）認証トリガに応答して、第２のチケットをＭＦＡＰ１１２に送信する。５４３において、第２のＩｄＰ５０９ｂは、（５３５における）認証トリガに応答して、新鮮である、第２のチケットをマスターＩｄＰ５０８に送信する。５４１において、ＭＦＡＰ１１２は、第１のチケットと第２のチケットを統合する。ＭＦＡＰはさらに、ＣＡ５０４の集約が実現された保証レベルおよび新鮮度レベルを計算できる。５４０において、ＣＡ５０４は、第１および第２のチケットをマスターＩｄＰ５０８に提示する。ＣＡ５０４はさらに、認証のそれぞれと関連付けられた実現された保証レベルおよび新鮮度をマスターＩｄＰ５０８に送信する。５４２において、マスターＩｄＰ５０８は、そのマスターＩｄＰがＣＡ５０４から受信した第１および第２のチケットをそれぞれ、そのマスターＩｄＰが第１および第２のＩｄＰから受信しているチケットと比較する。５４４において、例えば、第１のチケットの両方が互いにマッチして、第２のチケットの両方が互いにマッチすれば、マスターＩｄＰ５０８は、アサーションを作成する。マスターＩｄＰ５０８は、そのアサーションをＳＰ５０６に送信する。送信されるアサーションは、遂行された多要素認証によって実現された保証レベルおよび新鮮度レベルを含むことができる。５４６において、図示された実施形態により、ＳＰ６０６は、アサーションを検証して、成功メッセージをＣＡ５０４に提供し、それによってＣＡ５０４およびＣＡ５０４のユーザにＳＰ５０６によって提供されるリクエストされたサービスへのアクセスを提供する。

【００５８】

図６Ａは、開示された１つまたは複数の実施形態を実装できる例示的な通信システム５０の図である。通信システム５０は、音声、データ、ビデオ、メッセージング、ブロードキャストなどのコンテンツを複数の無線ユーザに提供する、多元接続システムであってよい。通信システム５０は、複数の無線ユーザが、無線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できる。例えば、通信システム５０は、符号分割多元接続（ＣＤＭＡ）、時分割多元接続（ＴＤＭＡ）、周波数分割多元接続（ＦＤＭＡ）、直交ＦＤＭＡ（ＯＦＤＭＡ）、シングルキャリアＦＤＭＡ（ＳＣ－ＦＤＭＡ）などの、１つまたは複数のチャネルアクセス方法を用いることができる。

【００５９】

図６Ａに示すように、通信システム５０は、無線送信／受信ユニット（ＷＴＲＵ）５２ａ、５２ｂ、５２ｃ、５２ｄ、無線アクセスネットワーク（ＲＡＮ）５４、コアネットワーク５６、公衆交換電話網（ＰＳＴＮ）５８、インターネット６０、および他のネットワーク６２を含むことができるが、開示された実施形態は、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を企図することが認識されよう。ＷＴＲＵ５２ａ、５２ｂ、５２ｃ、５２ｄのそれぞれは、無線環境で動作するおよび／または通信するように構成された任意のタイプのデバイスであってよい。例として、ＷＴＲＵ５２ａ、５２ｂ、５２ｃ、５２ｄは、無線信号を送信および／または受信するように構成されてもよく、ユーザ機器（ＵＥ）、移動局、固定式または移動式加入者ユニット、ページャ、セルラー電話、携帯情報端末（ＰＤＡ）、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、無線センサ、家電製品などを含むことができる。

【００６０】

通信システム５０はまた、基地局６４ａと基地局６４ｂを含むこともできる。基地局６４ａ、６４ｂのそれぞれは、ＷＴＲＵ５２ａ、５２ｂ、５２ｃ、５２ｄのうちの少なくとも１つとワイヤレスにインタフェースして、コアネットワーク５６、インターネット６０、および／またはネットワーク６２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ように構成された任意のタイプのデバイスであってよい。例として、基地局６４ａ、６４ｂは、ベーストランシーバ基地局（ＢＴＳ）、ノードＢ、ｅノードＢ、ホームノードＢ、ホームｅノードＢ、サイトコントローラ、アクセスポイント（ＡＰ）、無線ルータなどであってよい。基地局６４ａ、６４ｂはそれぞれ、単一要素として描かれているが、基地局６４ａ、６４ｂは、相互接続された任意の数の基地局および／またはネットワーク要素を含むことができることが認識されよう。

【００６１】

基地局６４ａは、基地局コントローラ（ＢＳＣ）、無線ネットワークコントローラ（ＲＮＣ）、中継ノードなどの、他の基地局および／またはネットワーク要素（図示せず）を含むこともできる、ＲＡＮ５４の一部にすることができる。基地局６４ａおよび／または基地局６４ｂは、セル（図示せず）と呼ばれてもよい、特定の地理的領域内で無線信号を送信および／または受信するように構成され得る。セルは、セルセクタにさらに分割され得る。例えば、基地局６４ａと関連付けられたセルを３つのセクタに分割できる。従って、一実施形態において、基地局６４ａは、３つのトランシーバ、即ち、セルの各セクタに１トランシーバを含むことができる。実施形態において、基地局６４ａは、ＭＩＭＯ(multiple-input multiple output)テクノロジーを用いることができ、従って、セルの各セクタに複数のトランシーバを利用できる。

【００６２】

基地局６４ａ、６４ｂは、適した任意の無線通信リンク（例えば、無線周波数（ＲＦ）、マイクロ波、赤外線（ＩＲ）、紫外線（ＵＶ）、可視光線など）であってよい、エアインタフェース６６を介してＷＴＲＵ５２ａ、５２ｂ、５２ｃ、５２ｄのうちの１または複数と通信できる。エアインタフェース６６は、適した任意の無線アクセステクノロジー（ＲＡＴ）を使用して確立できる。

【００６３】

より詳細には、上述のように、通信システム５０は、多元接続システムであってよく、ＣＤＭＡ、ＴＤＭＡ、ＦＤＭＡ、ＯＦＤＭＡ、ＳＣ－ＦＤＭＡなどの、１つまたは複数のチャネルアクセススキームを用いることができる。例えば、ＲＡＮ５４内の基地局６４ａおよびＷＴＲＵ５２ａ、５２ｂ、５２ｃは、ＷＣＤＭＡ(登録商標)（広域帯ＣＤＭ）を使用してエアインタフェース８１６を確立できる、ＵＴＲＡ(ユニバーサル移動体通信システム（ＵＭＴＳ）地上波無線アクセス）などの無線テクノロジーを実装できる。ＷＣＤＭＡは、高速パケットアクセス（ＨＳＰＡ）および／または発展型ＨＳＰＡ（ＨＳＰＡ＋）などの通信プロトコルを含むことができる。ＨＳＰＡは、高速ダウンリンクパケットアクセス（ＨＳＤＰＡ）および／または高速アップリンクパケットアクセス（ＨＳＵＰＡ）を含むことができる。

【００６４】

実施形態において、基地局６４ａおよびＷＴＲＵ５２ａ、５２ｂ、５２ｃは、ＬＴＥ（ロングタームエボリューション）および／またはＬＴＥ－Ａ（ＬＴＥアドバンスト）を使用してエアインタフェース６６を確立できる、Ｅ－ＵＴＲＡ（発展型ＵＭＴＳ地上波無線アクセス）などの無線テクノロジーを実装できる。

【００６５】

他の実施形態において、基地局６４ａおよびＷＴＲＵ５２ａ、５２ｂ、５２ｃは、ＩＥＥＥ８０２．１６（即ち、ＷｉＭＡＸ(Worldwide Interoperability for Microwave Access)、ＣＤＭＡ２０００、ＣＤＭＡ２０００１Ｘ、ＣＤＭＡ２０００ＥＶ－ＤＯ、ＩＳ－２０００(Interim Standard 2000)、ＩＳ－９５(Interim Standard 95)、ＩＳ－８５６(I

nterim Standard 856)、ＧＳＭ(登録商標)(Global System for Mobile communications)、ＥＤＧＥ(Enhanced Data rates for GSM Evolution)、ＧＥＲＡＮ(GSM EDGE)などの無線テクノロジーを実装できる。

【００６６】

図６Ａの基地局６４ｂは、例えば、無線ルータ、ホームノードＢ、ホームｅノードＢ、フェムト基地局、またはアクセスポイントであってよく、職場、住居、車、キャンパスなどの、ローカルエリアで無線接続性を容易にするために適した任意のＲＡＴを利用できる。実施形態において、基地局６４ｂおよびＷＴＲＵ５２ｃ、５２ｄは、無線ローカルエリアネットワーク（ＷＬＡＮ）を確立するＩＥＥＥ８０２．１１などの、無線テクノロジーを実装できる。実施形態において、基地局６４ｂおよびＷＴＲＵ５２ｃ、５２ｄは、無線パーソナルエリアネットワーク（ＷＰＡＮ）を確立するＩＥＥＥ８０２．１５などの、無線テクノロジーを実装できる。さらなる実施形態において、基地局６４ｂおよびＷＴＲＵ５２ｃ、５２ｄは、セルベースのＲＡＴ（例えば、ＷＣＤＭＡ、ＣＤＭＡ２０００、ＧＳＭ、ＬＴＥ、ＬＴＥ－Ａなど）を利用して、ピコセルまたはフェムトセルを確立できる。図６Ａに示すように、基地局６４ｂは、インターネット６０に直接接続できる。従って、基地局６４ｂは、コアネットワーク５６経由でインターネット６０へのアクセスを要求されない。

【００６７】

ＲＡＮ５４は、音声、データ、アプリケーション、および／またはＶｏＩＰ（ボイスオーバーインターネットプロトコル）サービスをＷＴＲＵ５２ａ、５２ｂ、５２ｃ、５２ｄのうち１または複数に提供するように構成された任意のタイプのネットワークであってよい、コアネットワーク５６と通信できる。例えば、コアネットワーク５６は、呼制御、課金サービス、モバイル位置情報に基づくサービス、プリペイド電話、インターネット接続性、ビデオ分散などを提供でき、および／またはユーザ認証などのハイレベルのセキュリティ機能を遂行できる。図６Ａに示していないが、ＲＡＮ５４および／またはコアネットワーク５６は、ＲＡＮ５４と同じＲＡＴまたは異なるＲＡＴを用いる、他のＲＡＴとの直接または間接通信であってよいことが認識されよう。例えば、Ｅ－ＵＴＲＡ無線テクノロジーを利用できるＲＡＮ５４に接続されることに加えて、コアネットワーク５６はまた、ＧＳＭ無線テクノロジーを用いた別のＲＡＮ（図示せず）と通信することもできる。

【００６８】

コアネットワーク５６はまた、ＷＴＲＵ５２ａ、５２ｂ、５２ｃ、５２ｄがＰＳＴＮ５８、インターネット６０、および／または他のネットワーク６２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。ＰＳＴＮ５８は、旧来の音声電話サービス（ＰＯＳＴ）を提供する回線交換電話網を含むことができる。インターネット６０は、ＴＣＰ／ＩＰインターネットプロトコルスイートにおける伝送制御プロトコル（ＴＣＰ）、ユーザデータグラムプロトコル（ＵＤＰ）およびインターネットプロトコル（ＩＰ）などの、共通の通信プロトコルを使用して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のグローバルシステムを含むことができる。ネットワーク６２は、他のサービスプロバイダによって所有および／または運用される有線または無線通信ネットワークを含むことができる。例えば、ネットワーク６２は、ＲＡＮ５４と同じＲＡＴまたは異なるＲＡＴを用いることができる、１つまたは複数のＲＡＮに接続された別のコアネットワークを含むことができる。

【００６９】

通信システム８００内のＷＴＲＵ５２ａ、５２ｂ、５２ｃ、５２ｄの一部またはすべては、マルチモード能力を含むことができる。即ち、ＷＴＲＵ５２ａ、５２ｂ、５２ｃ、５２ｄは、異なる無線リンクを介して異なる無線ネットワークと通信する複数のトランシーバを含むことができる。例えば、図６Ａに示したＷＴＲＵ５２ｃは、セルベースの無線テクノロジーを用いることができる基地局６４ａと、ＩＥＥＥ８０２無線テクノロジーを用いることができる基地局６４ｂとの通信を行うように構成され得る。

【００７０】

図６Ｂは、例示的なＷＴＲＵ５２のシステム図である。図６Ｂに示すように、ＷＴＲＵ５２は、プロセッサ６８、トランシーバ７０、送信／受信要素７２、スピーカ／マイクロフォン７４、キーパッド７６、ディスプレイ／タッチパッド７８、ノンリムーバブルメモリ８０、リムーバブルメモリ８２、電源８４、全地球測位システム（ＧＰＳ）チップセット８６、および他の周辺機器８８を含むことができる。ＷＴＲＵ５２は、実施形態と整合性を保った上で、上述の要素の任意の組み合わせを含むことができることが認識されよう。

【００７１】

プロセッサ６８は、汎用プロセッサ、専用プロセッサ、従来型プロセッサ、デジタル信号プロセッサ（ＤＳＰ）、複数のマイクロプロセッサ、ＤＳＰコアと連動する１つまた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、特定用途向け集積回路（ＡＳＩＣ）、現場プログラム可能ゲートアレイ（ＦＰＧＡ）回路、その他のタイプの集積回路（ＩＣ）、ステートマシンなどであってよい。プロセッサ６８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ＷＴＲＵ５２が無線環境で動作可能にさせるその他の機能性を遂行できる。プロセッサ６８は、送信／受信要素７２に結合され得る、トランシーバ７０に結合され得る。図６Ｂは、プロセッサ６８とトランシーバ７０とを個別のコンポーネントとして示しているが、プロセッサ６８とトランシーバ７０とを電子パッケージまたはチップ内にまとめることができることが認識されよう。プロセッサ６８は、アプリケーションレイヤプログラム（例えば、ブラウザ）および／または無線アクセスレイヤ（ＲＡＮ）プログラムおよび／または通信を遂行できる。プロセッサ６８は、例えば、アクセスレイヤおよび／またはアプリケーションレイヤにおけるような、認証、セキュリティ鍵同意、および／または暗号化動作などの、セキュリティ動作を遂行できる。

【００７２】

送信／受信要素７２は、エアインタフェース６６を介して基地局（例えば、基地局６４ａ）に信号を送信する、または基地局から信号を受信するように構成され得る。例えば、実施形態において、送信／受信要素７２は、ＲＦ信号を送信および／または受信するように構成されたアンテナであってよい。実施形態において、送信／受信要素７２は、例えば、ＩＲ、ＵＶ、または可視光線信号を送信および／または受信するように構成されたエミッタ／検出器であってよい。さらなる実施形態において、送信／受信要素７２は、ＲＦ信号と光信号との両方を送受信するように構成され得る。送信／受信要素７２は、無線信号の任意の組み合わせを送信および／または受信するように構成され得ることが認識されよう。

【００７３】

さらに、送信／受信要素７２を単一要素として図６Ｂに示しているが、ＷＴＲＵ５２は、任意の数の送信／受信要素７２を含むことができる。より詳細には、ＷＴＲＵ５２は、ＭＩＭＯテクノロジーを用いることができる。従って、実施形態において、ＷＴＲＵ５２は、エアインタフェース６６を介して無線信号を送受信する２または３以上の送信／受信要素７２（例えば、複数のアンテナ）を含むことができる。

【００７４】

トランシーバ７０は、送信／受信要素７２によって送信される信号を変調して、送信／受信要素７２によって受信された信号を復調するように構成され得る。上述のように、ＷＴＲＵ５２は、マルチモード能力を有することができる、従って、トランシーバ７０は、ＷＴＲＵ５２が、例えば、ＵＴＲＡおよびＩＥＥＥ８０２．１１などの、複数のＲＡＴ経由で通信することを可能にする複数のトランシーバを含むことができる。

【００７５】

ＷＴＲＵ５２のプロセッサ６８は、スピーカ／マイクロフォン７４、キーパッド７６、および／またはディスプレイ／タッチパッド７８（例えば、液晶ディスプレイ（ＬＣＤ）表示ユニットまたは有機発光ダイオード（ＯＬＥＤ）表示ユニット）に結合されて、それらからユーザ入力データを受信できる。プロセッサ６８はまた、スピーカ／マイクロフォ

ン７４、キーパッド７６、および／またはディスプレイ／タッチパッド７８にユーザデータを出力することもできる。さらに、プロセッサ８１８は、ノンリムーバブルメモリ８０および／またはリムーバブルメモリ８２などの、適した任意のタイプのメモリからの情報にアクセスして、それらのメモリにデータを記憶できる。ノンリムーバブルメモリ８０は、ランダムアクセスメモリ（ＲＡＭ）、リードオンリーメモリ（ＲＯＭ）、ハードディスク、またはその他のタイプのメモリ記憶デバイスを含むことができる。リムーバブルメモリ８２は、契約者識別モジュール（ＳＩＭ）カード、メモリスティック、セキュアデジタル（ＳＤ）メモリカードなどを含むことができる。他の実施形態において、プロセッサ８１８は、サーバまたはホームコンピュータ（図示せず）などの、物理的にＷＴＲＵ５２に配置されていないメモリからの情報にアクセスして、それらのメモリにデータを記憶できる。

【００７６】

プロセッサ６８は、電源８４から電力を受け取ることができ、その電力をＷＴＲＵ５２内の他のコンポーネントに分散および／または制御するように構成され得る。電源８４は、ＷＴＲＵ５２に電力供給するのに適した任意のデバイスであってよい。例えば、電源８４は、１つまたは複数の乾電池（例えば、ニッケルカドミウム（ＮｉＣｄ）、ニッケル亜鉛（ＮｉＺｎ）、ニッケル水素（ＮｉＭＨ）、リチウムイオン（Ｌｉ－ｉｏｎ）など）、太陽電池、燃料電池などを含むことができる。

【００７７】

プロセッサ６８はまた、ＧＰＳチップセット８６を、ＷＴＲＵ５２の現在の位置に関する位置情報（例えば、経緯度）を提供するように構成され得る、ＧＰＳチップセット８６にも結合され得る。追加または代替として、ＧＰＳチップセット８６からの情報により、ＷＴＲＵ５２は、基地局（例えば、基地局６４ａ、６４ｂ）からエアインタフェース８１６を介して位置情報を受信し、および／または２または３以上の近隣の基地局から受信される信号のタイミングに基づいてＷＴＲＵの位置を判定できる。ＷＴＲＵ５２は、実施形態と整合性を保った上で、適した任意の位置判定方法によって位置情報を獲得できることが認識されよう。

【００７８】

プロセッサ６８は、付加的な特徴、機能性および／または有線または無線接続性を提供する、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、他の周辺機器８８にさらに結合され得る。例えば、周辺機器８８は、加速度計、電子コンパス、衛星トランシーバ、デジタルカメラ（写真またはビデオ用）、ユニバーサルシリアルバス（ＵＳＢ）ポート、振動デバイス、テレビトランシーバ、ハンズフリーヘッドセット、Ｂｌｕｅｔｏｏｔｈ（登録商標）モジュール、周波数変調（ＦＭ）無線ユニット、デジタル音楽プレーヤ、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。

【００７９】

図６Ｃは、実施形態に従うＲＡＮ５４およびコアネットワーク８０６のシステム図である。上述のように、ＲＡＮ５４は、ＵＴＲＡ無線テクノロジーを用いて、エアインタフェース６６を介してＷＴＲＵ５２ａ、５２ｂ、５２ｃと通信できる。ＲＡＮ５４はさらに、コアネットワーク８０６とも通信できる。図６Ｃに示すように、ＲＡＮ５４は、エアインタフェース６６を介してＷＴＲＵ５２ａ、５２ｂ、５２ｃと通信するための１つまたは複数のトランシーバを含むことができる、ノードＢ９０ａ、９０ｂ、９０ｃを含むことができる。ノードＢ９０ａ、９０ｂ、９０ｃのそれぞれをＲＡＮ５４内の特定のセル（図示せず）と関連付けることができる。ＲＡＮ５４はさらに、ＲＮＣ９２ａ、９２ｂを含むこともできる。ＲＡＮ５４は、実施形態と整合性を保った上で、任意の数のノードＢおよびＲＮＣを含むことができることが認識されよう。

【００８０】

図６Ｃに示すように、ノードＢ９０ａ、９０ｂは、ＲＮＣ９２ａと通信できる。あるいは、ノードＢ９０ｃは、ＲＮＣ９２ｂと通信できる。ノードＢ９０ａ、９０ｂ、９０ｃは

、Ｉｕｂインタフェース経由でそれぞれＲＮＣ９２ａ、９２ｂと通信できる。ＲＮＣ９２ａ、９２ｂは、Ｉｕｒインタフェース経由で互いに通信できる。９２ａ、９２ｂのそれぞれは、接続されているノードＢ９０ａ、９０ｂ、９０ｃのそれぞれを制御するように構成され得る。さらに、ＲＮＣ９２ａ、９２ｂのそれぞれは、外ループ電力制御、読み込み制御、許可制御、パケットスケジューリング、ハンドオーバー制御、マクロダイバーシティ、セキュリティ関数、データ暗号化などの、他の機能性を実行するおよび／またはサポートするように構成され得る。

【００８１】

図６Ｃに示したコアネットワーク８０６は、メディアゲートウェイ（ＭＧＷ）８４４、モバイル交換センター（ＭＳＣ）９６、サービングＧＰＲＳサポートノード（ＳＧＳＮ）９８、および／またはゲートウェイＧＰＲＳサポートノード（ＧＧＳＮ）９９を含むことができる。上述した要素のそれぞれをコアネットワーク５６の一部として示しているが、これらの要素のいずれも、コアネットワーク通信業者以外のエンティティによって所有および／または運用可能であることが認識されよう。

【００８２】

ＲＡＮ５４内のＲＮＣ９２ａをＩｕＣＳインタフェース経由でコアネットワーク５６内のＭＳＣ９６に接続できる。ＭＳＣ９６をＭＧＷ９４に接続できる。ＭＳＣ９６およびＭＧＷ９４は、ＷＴＲＵ５２ａ、５２ｂ、５２ｃにＰＳＴＮ５８などの回路交換ネットワークへのアクセスを提供して、ＷＴＲＵ５２ａ、５２ｂ、５２ｃと従来の固定電話回線による通信デバイスとの間の通信を容易にすることができる。

【００８３】

ＲＡＮ５４内のＲＮＣ９２ａはまた、ＩｕＰＳインタフェース経由でコアネットワーク８０６内のＳＧＳＮ９８にも接続され得る。ＳＧＳＮ９８をＧＣＳＮ９９に接続できる。ＳＧＳＮ９８およびＧＣＳＮ９９は、ＷＴＲＵ５２ａ、５２ｂ、５２ｃにインターネット６０などの、パケット交換ネットワークへのアクセスを提供して、ＷＴＲＵ５２ａ、５２ｂ、５２ｃとＩＰ対応(IP-enabled)デバイスとの間の通信を容易にすることができる。

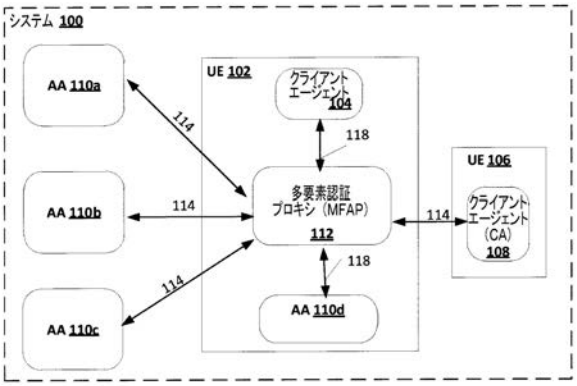
【００８４】

上述のように、コアネットワーク５６はまた、他のサービスプロバイダによって所有および／または運用される他の有線または無線ネットワークを含むことができる、ネットワーク６２にも接続され得る。

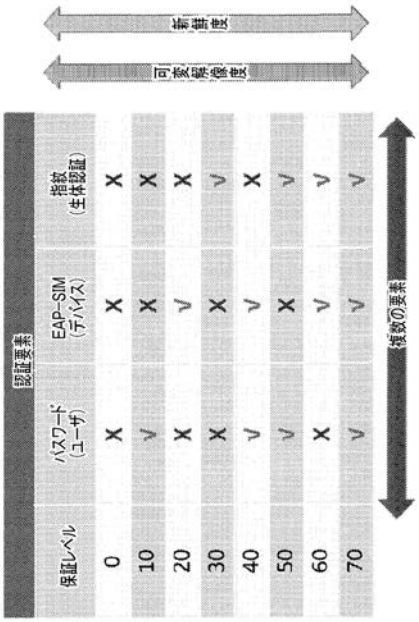
【００８５】

特定の組み合わせにおいて特徴および要素を上述しているが、各特徴または要素は、単独で、または他の特徴および要素との任意の組み合わせにおいて使用されることができる。さらに、本明細書で説明される実施形態は、例示目的としてのみ提供される。例えば、実施形態は、ＯｐｅｎＩＤおよび／またはＳＳＯ認証エンティティおよび機能を使用して説明され得るが、他の認証エンティティおよび機能を使用して同様の実施形態が実装され得る。さらに、本明細書で説明される実施形態は、コンピュータまたはプロセッサによって実行するためのコンピュータ可読媒体に組み込まれ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に実装され得る。コンピュータ可読媒体の例は、（有線および／または無線接続を介して送信される）電子信号および／またはコンピュータ可読記憶媒体を含む。コンピュータ可読記憶媒体の例は、限定されるわけではないが、リードオンリーメモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、レジスタ、キャッシュメモリ、半導体メモリデバイス、内部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媒体、光磁気媒体、およびＣＤ－ＲＯＭディスク、およびデジタル多用途ディスク（ＤＶＤ）などの光媒体を含む。ソフトウェアと連動するプロセッサを使用して、ＷＴＲＵ、ＵＥ、端末機、基地局、ＲＮＣ、および／または任意のホストコンピュータで使用するための無線周波数トランシーバを実装することができる。

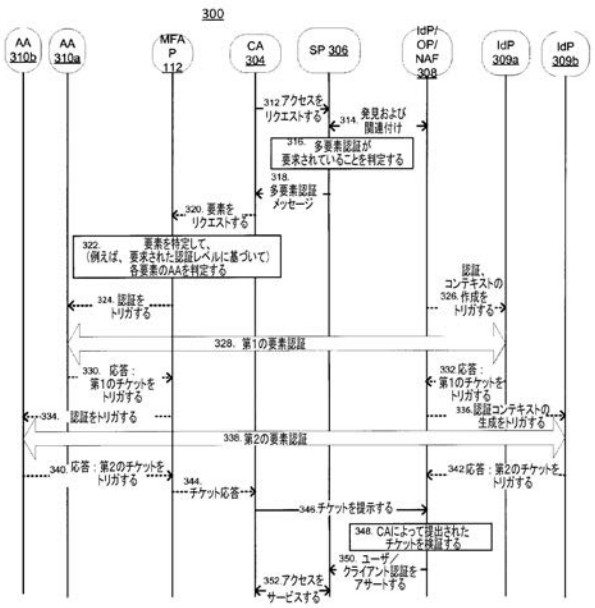
【図１】


システム 100
AA 110a
AA 110b
AA 110c
AA 110d
UE 102
クライアント エージェント 104
多要素認証 プロキシ（MFAP） 112
UE 106
クライアント エージェント （CA） 108
114
118

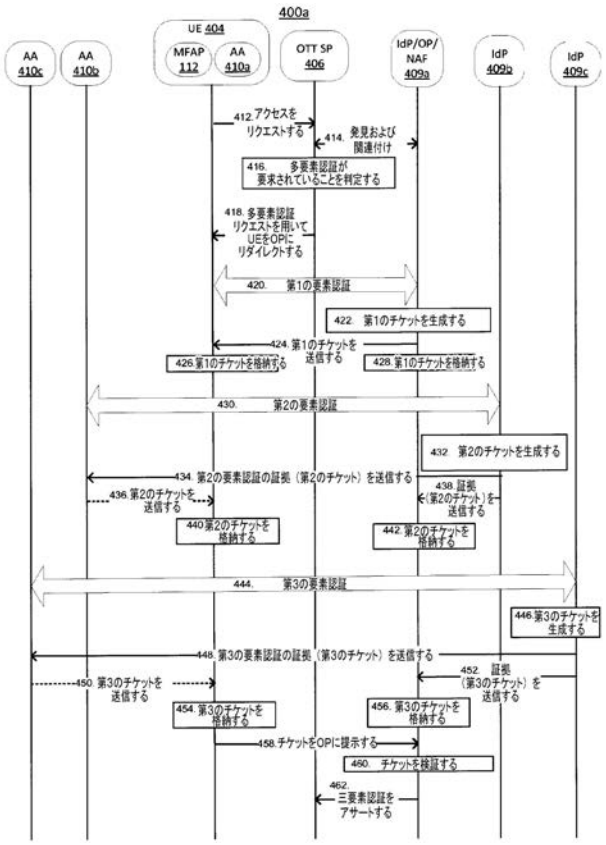
【図２】


認証要素
保証レベル
パスワード（ユーザ）
EAP-SIM（デバイス）
指紋（生体認証）
0
10
20
30
40
50
60
70
増加の要素

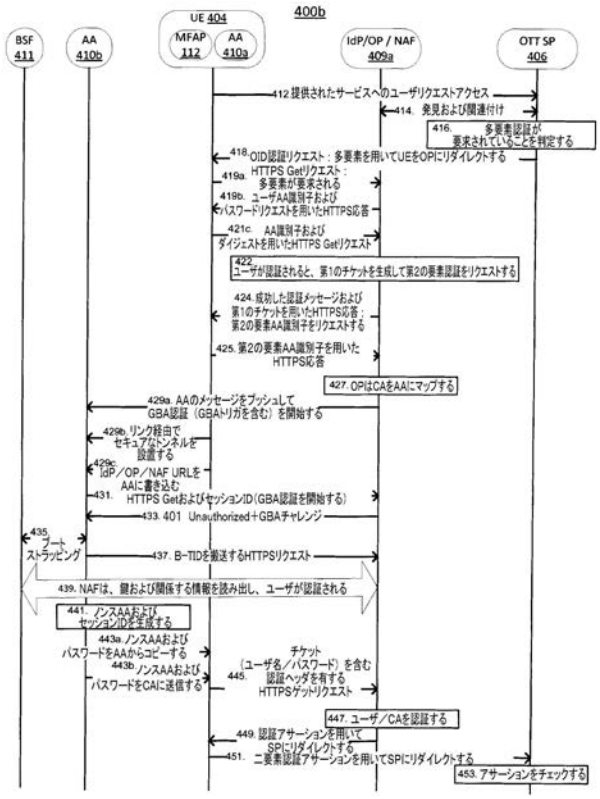
【図３】


300
AA 310b
AA 310a
MFAP 112
CA 304
SP 306
IdP/OP/NAF 308
IdP 309a
IdP 309b
312. アクセスをリクエストする
314. 発見および関連付け
316. 多要素認証が要求されていることを判定する
318. 多要素認証メッセージ
320. 要素をリクエストする
322. 要素を特定して、（例えば、要求された認証レベルに基づいて）各要素のAAを判定する
324. 認証をトリガする
326. 認証、コンテキストの作成をトリガする
328. 第1の要素認証
330. 応答：第1のチケットをトリガする
332. 応答：第1のチケットをトリガする
334. 認証をトリガする
336. 認証コンテキストの生成をトリガする
338. 第2の要素認証
340. 応答：第2のチケットをトリガする
342. 応答：第2のチケットをトリガする
344. チケット応答
346. チケットを提示する
348. CAによって提出されたチケットを検証する
350. ユーザ／クライアント認証をアサートする
352. アクセスをサービスする

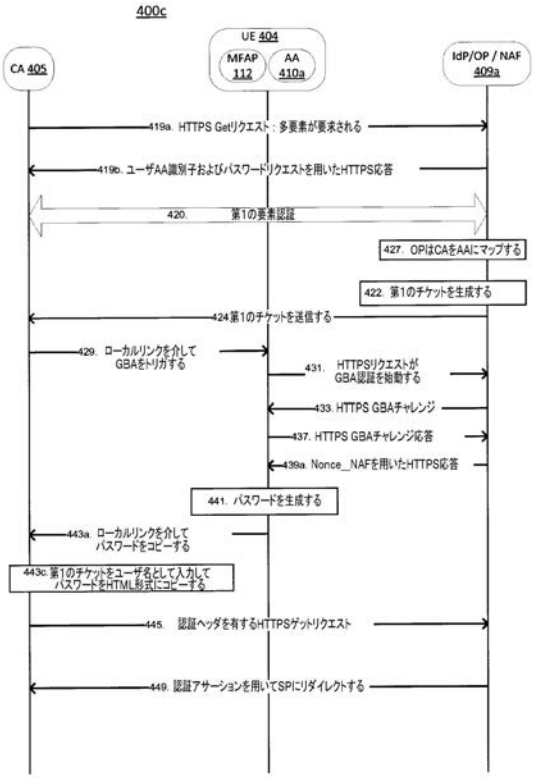
【図４Ａ】


400a
AA 410c
AA 410b
UE 404
MFAP 112
AA 410a
OTT SP 406
IdP/OP/NAF 409a
IdP 409b
IdP 409c
412. アクセスをリクエストする
414. 発見および関連付け
416. 多要素認証が要求されていることを判定する
418. 多要素認証リクエストを用いてUEをOPにリダイレクトする
420. 第1の要素認証
422. 第1のチケットを生成する
424. 第1のチケットを送信する
426. 第1のチケットを格納する
428. 第1のチケットを格納する
430. 第2の要素認証
432. 第2のチケットを生成する
434. 第2の要素認証の証拠（第2のチケット）を送信する
436. 第2のチケットを送信する
438. 証拠（第2のチケット）を送信する
440. 第2のチケットを格納する
442. 第2のチケットを格納する
444. 第3の要素認証
446. 第3のチケットを生成する
448. 第3の要素認証の証拠（第3のチケット）を送信する
450. 第3のチケットを送信する
452. 証拠（第3のチケット）を送信する
454. 第3のチケットを格納する
456. 第3のチケットを格納する
458. チケットをOPに提示する
460. チケットを検証する
462. 三要素認証をアサートする

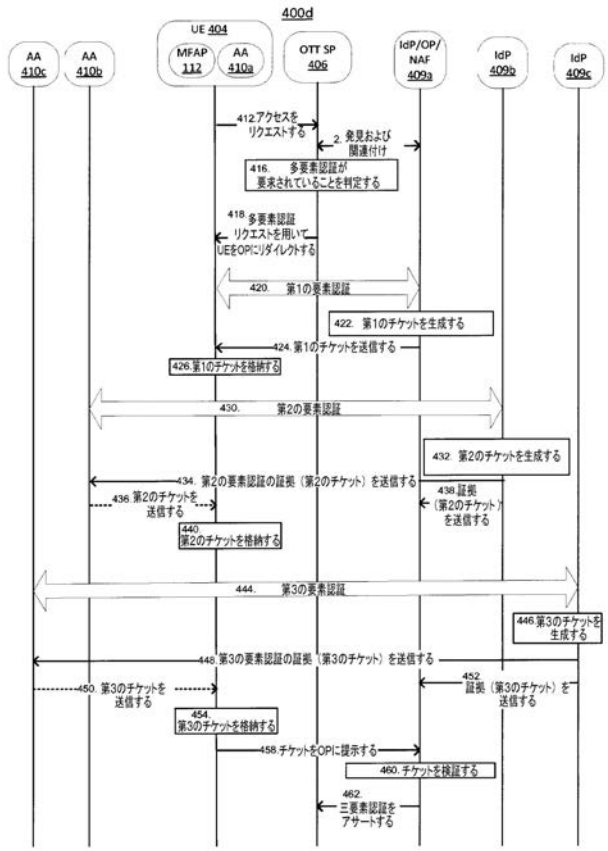
【図４Ｂ】



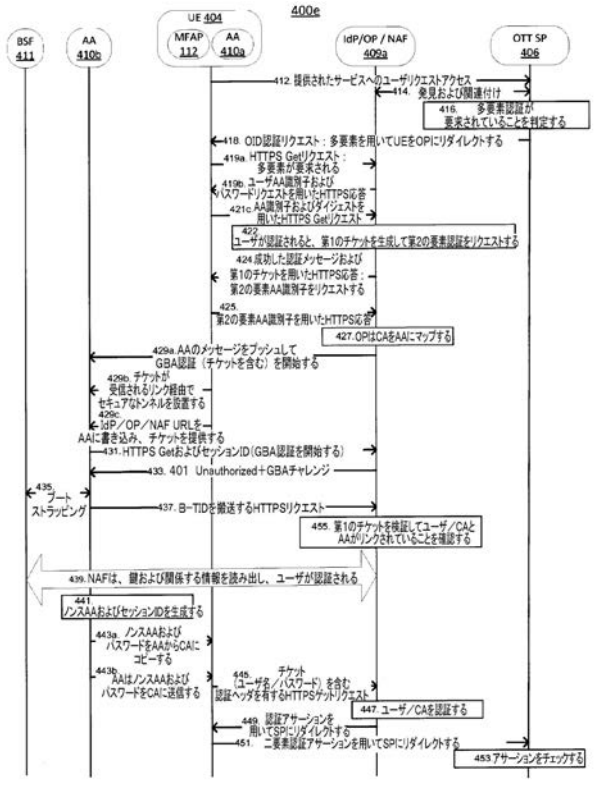
【図４Ｃ】



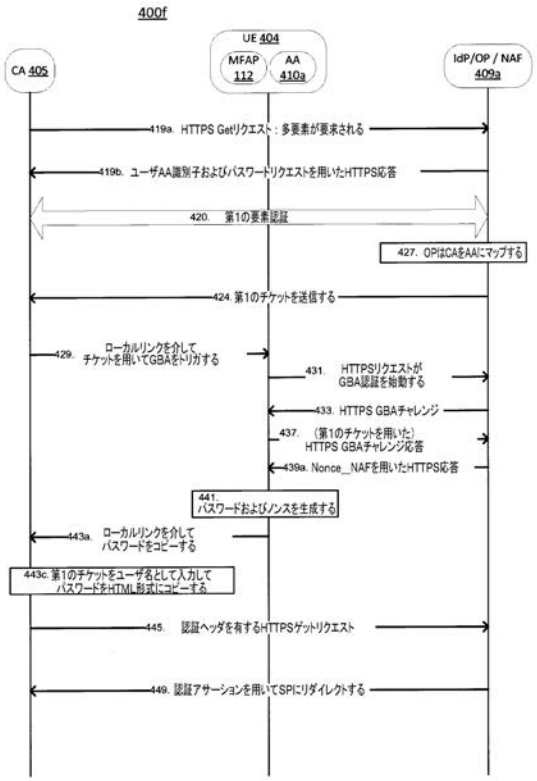
【図４Ｄ】



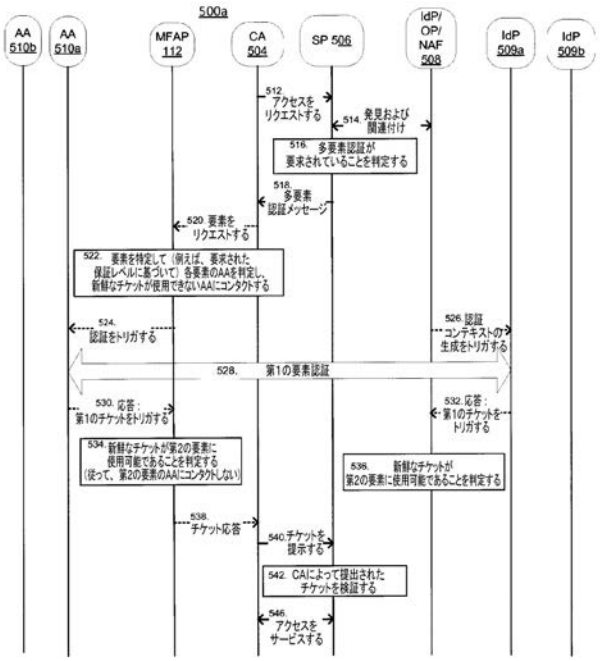
【図４Ｅ】



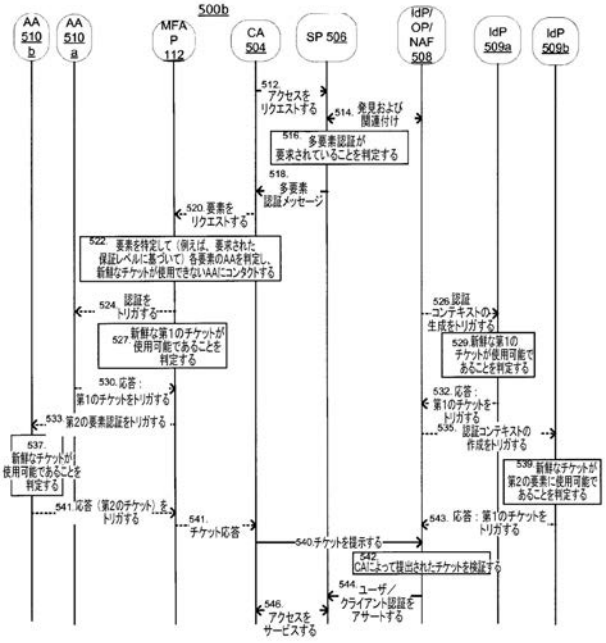
【図４Ｆ】



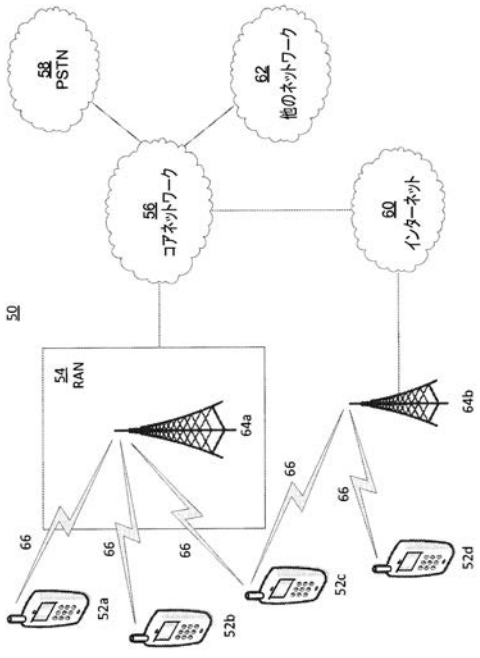
【図５Ａ】



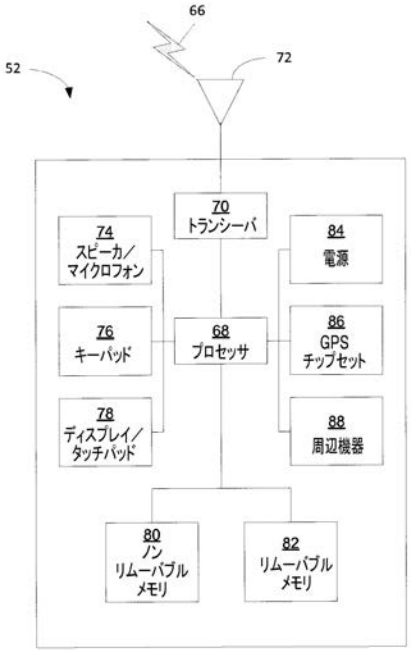
【図５Ｂ】



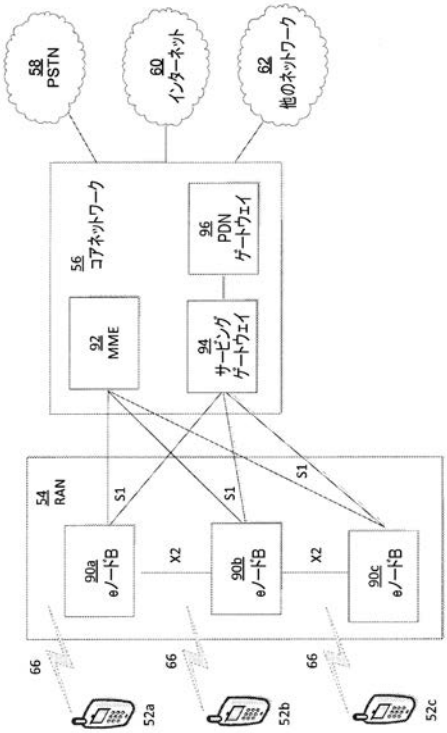
【図６Ａ】



【図６Ｂ】



【図６Ｃ】



【手続補正書】
【提出日】平成27年1月23日(2015.1.23)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
多要素認証プロキシ（ＭＦＡＰ）を備えたユーザ機器（ＵＥ）であって、前記ＭＦＡＰは、
サービスプロバイダ（ＳＰ）によって提供されるサービスにアクセスするために、複数の認証要素が前記ＵＥのユーザを認証するために要求されていることを判定し、
前記要求された認証要素のうちの１つを利用して、認証を遂行するために、前記ＵＥとは異なるデバイス上の認証エージェント（ＡＡ）を特定し、
前記異なるデバイスへのローカルリンクを確立し、
前記認証を遂行するように前記ＡＡをトリガして
前記ローカルリンクを介して、前記ＡＡによる成功した認証を表すアサーションを受信する、
ように動作する、ＵＥ。
【請求項２】
前記ＭＦＡＰは、前記要求された認証要素のうちの少なくともう１つを利用して、認証を遂行するために、前記ＵＥの１つまたは複数の付加的な認証エージェントを特定する、ようにさらに動作する、請求項１に記載のＵＥ。
【請求項３】

前記ＭＦＡＰは、前記要求された認証要素のうちの少なくともう１つを利用する認証を遂行するために、前記ＵＥとは異なる第２のデバイス上の１つまたは複数の付加的な認証エージェントを特定する、ようにさらに動作し、前記ＭＦＡＰは、ローカルリンクまたはリモートリンクを介して、前記１つまたは複数の付加的な認証エージェントと通信する、請求項１に記載のＵＥ。

【請求項４】

前記ＭＦＡＰは、前記ＳＰへ直接、成功した認証を表す前記アサーションを送信する、ようにさらに動作する、請求項１に記載のＵＥ。

【請求項５】

第１のユーザ機器（ＵＥ）と、サービスプロバイダ（ＳＰ）と、多要素認証プロキシ（ＭＦＡＰ）とを備えたシステムにおいて前記ＭＦＡＰにより実行される方法であって、

前記ＳＰのポリシーに基づいて、前記第１のＵＥのユーザが前記ＳＰによって提供されるサービスにアクセスするために、多要素認証が要求されていることを判定することと、

第１の要素認証を遂行するために、第１の認証エージェントを特定することと、

第１のチケットが生じる前記第１の要素認証を遂行するように前記第１の認証エージェントをトリガすることと、

第２の要素認証を遂行するために、前記第１の認証エージェントとは異なる第２の認証エージェントを特定することと、

第２のチケットが生じる記第２の要素認証を遂行するように前記第２の認証エージェントをトリガすることと、

前記第１のＵＥの第１のクライアントエージェントへ、前記第１のチケットおよび前記第２のチケットを送信することであり、前記第１のＵＥが前記ＳＰによって提供される前記サービスにアクセスすることを可能にすることと、

を備える、方法。

【請求項６】

前記第１のＵＥの前記ユーザは、前記第１のクライアントエージェントの認証を活用することにより、第２のクライアントエージェントへ移行する、請求項５に記載の方法。

【請求項７】

前記第２のクライアントエージェントは、前記第１のＵＥまたは前記第１のＵＥと異なる第２のＵＥ上に存在する、請求項６に記載の方法。

【請求項８】

前記第１のチケットは、前記第１の要素認証を表すセッションアイデンティティにバインドされる、請求項５に記載の方法。

【請求項９】

前記ＭＦＡＰは前記第１のＵＥ上にある、請求項５に記載の方法。

【請求項１０】

前記ＭＦＡＰは、ローカルリンクまたはリモートリンクを介して、第２のＵＥの第２のクライアントエージェントと通信する、請求項９に記載の方法。

【請求項１１】

前記ＭＦＡＰは第２のＵＥ上に存在し、前記ＭＦＡＰは、ローカルリンクまたはリモートリンクを介して前記第１のＵＥの前記第１のクライアントエージェントと通信する、請求項５に記載の方法。

【請求項１２】

前記第１のチケットおよび前記第２のチケットはそれぞれ、デジタル署名、暗号値、ランダム値、または一時的アイデンティティのうちの少なくとも１つを備える、請求項５に記載の方法。

【請求項１３】

前記第１の認証エージェントおよび前記第２の認証エージェントの少なくとも１つは、第２のＵＥ上に存在する、請求項５に記載の方法。

【請求項１４】

前記ＳＰの前記ポリシーは前記多要素認証の要求される保証レベルを備え、前記第１の認証エージェント及び前記第２の認証エージェントは、前記多要素認証の前記要求される保証レベルに基づいて、特定される、請求項５に記載の方法。

【請求項１５】

前記第１のチケットの保証レベルおよび前記第２のチケットの保証レベルに基づき、集約保証レベルを判定すること、をさらに備える、請求項５に記載の方法。

【請求項１６】

第３の要素認証を遂行ために、第３の要素認証エージェントを特定することと、

第３のチケットが生じる前記第３の要素認証をトリガすることと、

をさらに備える、請求項５に記載の方法。

【請求項１７】

前記第１の認証エージェントおよび前記第２の認証エージェントはそれぞれ第１のアイデンティティプロバイダおよび第２のアイデンティティプロバイダと関連付けられている、請求項５に記載の方法。

【請求項１８】

通信ネットワークにおけるユーザ装置（ＵＥ）であって、

実行可能なメモリと、

実行可能命令を実行すると、

サービスプロバイダ（ＳＰ）によって提供されるサービスにアクセスするために、複数の認証要素が前記ＵＥのユーザを認証するために要求されていることを判定することと、

前記要求された認証要素のうちの１つを利用して、認証を遂行するために、前記ＵＥとは異なるデバイス上の認証エージェント（ＡＡ）を特定することと、

前記異なるデバイスへのローカルリンクを確立することと、

前記認証を遂行するように前記ＡＡをトリガすることと、

前記ローカルリンクを介して、前記ＡＡによる成功した認証を表すアサーションを受信することと

を実行するプロセッサと、

を備えた、ＵＥ。

【請求項１９】

前記プロセッサは、前記要求された認証要素のうちの少なくともう１つを利用して、認証を遂行するために、前記ＵＥ上の１つまたは複数の付加的な認証エージェントを特定することをさらに実行する、請求項１８に記載のＵＥ。

【請求項２０】

前記プロセッサは、前記要求された認証要素のうちの少なくともう１つを利用する認証を遂行するために、前記ＵＥとは異なる第２のデバイス上の１つまたは複数の付加的な認証エージェントを特定することをさらに実行する、請求項１８に記載のＵＥ。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/031998

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/06 G06F21/34
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011/225625 A1 (WOLFSON BRUCE [US] ET AL) 15 September 2011 (2011-09-15) abstract; figures 1, 2, 3 paragraphs [0011], [0012] paragraphs [0015] - [0026] paragraphs [0034], [0044], [0045]	1-20
X	US 2012/167187 A1 (SMITH NED M [US] ET AL) 28 June 2012 (2012-06-28) abstract; figures 1-4; table 1 paragraphs [0019], [0020], [0025] paragraphs [0026], [0029], [0034] paragraphs [0037] - [0045]	1-20

-/--

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 July 2014	01/08/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Schossmaier, Klaus

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/031998

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/118745 A1 (BUER MARK [US]) 24 May 2007 (2007-05-24) abstract; figures 1, 2 paragraphs [0017] - [0022] paragraphs [0027], [0031] paragraphs [0044] - [0055] -----	1-20
X	Luís Miranda ET AL: "Context-aware multi-factor authentication", Repositorio Institucional da FCT-UNL, 24 September 2010 (2010-09-24), XP055091109, PT Retrieved from the Internet: URL:http://hdl.handle.net/10362/4111 [retrieved on 2014-07-17] paragraph [044-]; figures 3.2, 3.3, 3.4, 3.5, 4.3, 5.1; table 2.1 section 3 section 4.2 sections 5.4, 5.5 -----	1-20
E	WO 2014/093613 A1 (INTERDIGITAL PATENT HOLDINGS [US]) 19 June 2014 (2014-06-19) abstract; claim 14; figures 1,2 paragraphs [0022] - [0027] paragraphs [0030], [0031], [0037] paragraphs [0046], [0047] -----	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/031998

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011225625 A1	15-09-2011	NONE	
US 2012167187 A1	28-06-2012	NONE	
US 2007118745 A1	24-05-2007	US 2007118745 A1	24-05-2007
		US 2012272307 A1	25-10-2012
WO 2014093613 A1	19-06-2014	NONE	

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

（特許庁注：以下のものは登録商標）
１．ＡＮＤＲＯＩＤ

(72)発明者 アレック ブルシロフスキー
アメリカ合衆国 １９３３５ ペンシルベニア州 ダウニングタウン オーク ホロー ドライブ １１２２

Ｆターム(参考) 5J104 AA07 KA01 KA16 NA05