(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2017-534214
(P2017-534214A)
(43)公表日　平成29年11月16日(2017.11.16)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601B	5J104
		H04L	9/00	601E	

審査請求 未請求　予備審査請求 有　（全 36 頁）

(21)出願番号	特願2017-524993 (P2017-524993)
(86)(22)出願日	平成27年10月30日 (2015.10.30)
(85)翻訳文提出日	平成29年7月10日 (2017.7.10)
(86)国際出願番号	PCT/US2015/058364
(87)国際公開番号	WO2016/077087
(87)国際公開日	平成28年5月19日 (2016.5.19)
(31)優先権主張番号	62/078,162
(32)優先日	平成26年11月11日 (2014.11.11)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	14/926,791
(32)優先日	平成27年10月29日 (2015.10.29)
(33)優先権主張国	米国 (US)

(71)出願人　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100158805
弁理士　井関　守三
(74)代理人　100112807
弁理士　岡田　貴志

最終頁に続く

(54)【発明の名称】認証サーバとのワイヤレス局の再認証中のプライバシー

(57)【要約】
方法、システム、装置、およびデバイスは、第１のＡＰから第２のＡＰにハンドオーバを遂行する間、認証サーバとのワイヤレス局の再認証中のプライバシーのために説明される。ワイヤレス局は、再認証鍵およびシーケンス番号から第１の識別子を導出し得る。再認証鍵は、第１のセッション鍵から少なくとも部分的に導出され得る。ワイヤレス局は、第１の識別子およびドメイン名を認証者に送信し得る。第１の識別子およびドメイン名は、認証サーバとのワイヤレス局の第１の再認証中に送信され得る。第１のセッション鍵の名前の送信は、第１の再認証中、差し控えられ得る。

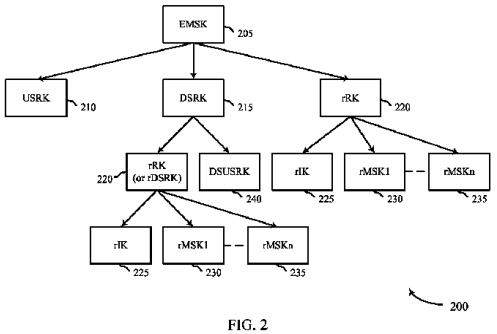


FIG. 2

【特許請求の範囲】
【請求項１】
ワイヤレス通信のための方法であって、
再認証鍵およびシーケンス番号からワイヤレス局において第１の識別子を導出することと、前記再認証鍵は、第１のセッション鍵から少なくとも部分的に導出される、
前記第１の識別子およびドメイン名を認証者に送信することと、前記第１の識別子および前記ドメイン名は、認証サーバとの前記ワイヤレス局の第１の再認証中に送信される、
前記第１の再認証中、前記第１のセッション鍵の名前の送信を差し控えることと
を備える、ワイヤレス通信のための方法。
【請求項２】
前記シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、
前記再認証鍵および前記次のシーケンス番号に少なくとも部分的に基づいて第２の識別子を導出することと
をさらに備える、請求項１に記載の方法。
【請求項３】
前記第２の識別子および前記ドメイン名を送信すること、前記第２の識別子および前記ドメイン名は、前記認証サーバとの前記ワイヤレス局の第２の再認証中に送信される、
をさらに備える、請求項２に記載の方法。
【請求項４】
再認証失敗メッセージを受信することと、
前記再認証失敗メッセージを受信することに応答して、前記第２の識別子および前記ドメイン名を送信することと
をさらに備える、請求項２に記載の方法。
【請求項５】
前記認証サーバとの前記ワイヤレス局の単一の再認証のために前記第１の識別子を使用すること
をさらに備える、請求項１に記載の方法。
【請求項６】
識別子ラベルに少なくとも部分的に基づいて前記第１の識別子を導出すること
をさらに備える、請求項１に記載の方法。
【請求項７】
前記第１の再認証は、拡張認証プロトコル（ＥＡＰ）再認証を備え、前記第１のセッション鍵は、拡張マスターセッション鍵（ＥＭＳＫ）を備え、前記再認証鍵は、再認証ルート鍵（ｒＲＫ）を備える、請求項１に記載の方法。
【請求項８】
前記第１の再認証は、前記認証サーバとの完全な認証を遂行した後に遂行される、請求項１に記載の方法。
【請求項９】
再認証失敗メッセージを受信することと、
前記再認証失敗メッセージを受信することに応答して、前記認証サーバとの完全な認証を遂行することと
をさらに備える、請求項１に記載の方法。
【請求項１０】
ワイヤレス通信のための装置であって、
プロセッサと、
前記プロセッサと電子通信しているメモリと、
前記メモリに記憶されている命令と
を備え、前記命令は、
再認証鍵およびシーケンス番号からワイヤレス局において第１の識別子を導出するこ

とと、前記再認証鍵は、第１のセッション鍵から少なくとも部分的に導出される、
　前記第１の識別子およびドメイン名を認証者に送信することと、前記第１の識別子および前記ドメイン名は、認証サーバとの前記ワイヤレス局の第１の再認証中に送信される、
　前記第１の再認証中、前記第１のセッション鍵の名前の送信を差し控えることと
を行うように前記プロセッサによって実行可能である、ワイヤレス通信のための装置。
【請求項１１】
前記シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、
前記再認証鍵および前記次のシーケンス番号に少なくとも部分的に基づいて第２の識別子を導出することと
を行うように前記プロセッサによって実行可能な命令をさらに備える、請求項１０に記載の装置。
【請求項１２】
前記第２の識別子および前記ドメイン名を送信することと、前記第２の識別子および前記ドメイン名は、前記認証サーバとの前記ワイヤレス局の第２の再認証中に送信される、
を行うように前記プロセッサによって実行可能な命令をさらに備える、請求項１１に記載の装置。
【請求項１３】
再認証失敗メッセージを受信することと、前記再認証失敗メッセージを受信することに応答して、前記第２の識別子および前記ドメイン名を送信することと
を行うように前記プロセッサによって実行可能な命令をさらに備える、請求項１１に記載の装置。
【請求項１４】
前記認証サーバとの前記ワイヤレス局の単一の再認証のために前記第１の識別子を使用すること
を行うように前記プロセッサによって実行可能な命令をさらに備える、請求項１０に記載の装置。
【請求項１５】
識別子ラベルに少なくとも部分的に基づいて前記第１の識別子を導出すること
を行うように前記プロセッサによって実行可能な命令をさらに備える、請求項１０に記載の装置。
【請求項１６】
前記第１の再認証は、拡張認証プロトコル（ＥＡＰ）再認証を備え、前記第１のセッション鍵は、拡張マスターセッション鍵（ＥＭＳＫ）を備え、前記再認証鍵は、再認証ルート鍵（ｒＲＫ）を備える、請求項１０に記載の装置。
【請求項１７】
前記第１の再認証は、前記認証サーバとの完全な認証を遂行した後に遂行される、請求項１０に記載の装置。
【請求項１８】
再認証失敗メッセージを受信することと、
前記再認証失敗メッセージを受信することに応答して、前記認証サーバとの完全な認証を遂行することと
を行うことを前記プロセッサによって実行可能な命令をさらに備える、請求項１０に記載の装置。
【請求項１９】
ワイヤレス通信のための方法であって、
再認証鍵およびシーケンス番号から、認証サーバにおいて、第１の識別子を導出することと、前記再認証鍵は、第１のセッション鍵から少なくとも部分的に導出される、
第２の識別子を前記認証サーバにおいて受信することと、前記第２の識別子は、前記認

証サーバとのワイヤレス局の第１の再認証中に受信される、
前記第１の識別子を前記第２の識別子と比較することと、
前記比較することに少なくとも部分的に基づいて前記ワイヤレス局の認証者に第２のセッション鍵を送信することと
を備える、ワイヤレス通信のための方法。
【請求項２０】
前記第１の識別子は、前記第２の識別子と一致する、請求項１９に記載の方法。
【請求項２１】
前記シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、
前記再認証鍵および前記次のシーケンス番号に少なくとも部分的に基づいて第３の識別子を導出することと
をさらに備える、請求項１９に記載の方法。
【請求項２２】
前記認証サーバとの前記ワイヤレス局の第２の再認証中に第４の識別子を受信することと、
前記第３の識別子を前記第４の識別子と比較することと、
前記比較することに少なくとも部分的に基づいて前記第２のセッション鍵を送信することと
をさらに備える、請求項２１に記載の方法。
【請求項２３】
前記第３の識別子は、前記第４の識別子と一致する、請求項２２に記載の方法。
【請求項２４】
識別子ラベルに少なくとも部分的に基づいて前記第１の識別子を導出すること、をさらに備える、請求項１９に記載の方法。
【請求項２５】
前記第１の識別子が前記第２の識別子と一致できないとき、再認証失敗メッセージを送信すること、をさらに備える、請求項１９に記載の方法。
【請求項２６】
前記再認証失敗メッセージは、前記第１の識別子と前記第２の識別子との間の不一致を示すタイプレングスバリュー（ＴＬＶ）要素を備える、請求項２５に記載の方法。
【請求項２７】
前記第１の再認証は、拡張認証プロトコル（ＥＡＰ）再認証を備え、前記第１のセッション鍵は、拡張マスターセッション鍵（ＥＭＳＫ）を備え、前記再認証鍵は、再認証ルート鍵（ｒＲＫ）を備え、前記第２のセッション鍵は、再認証マスターセッション鍵（ｒＭＳＫ）を備える、請求項１９に記載の方法。
【請求項２８】
ワイヤレス通信のための装置であって、
プロセッサと、
前記プロセッサと電子通信しているメモリと、
前記メモリに記憶されている命令と
を備え、前記命令は、
再認証鍵およびシーケンス番号から、認証サーバにおいて、第１の識別子を導出することと、前記再認証鍵は、第１のセッション鍵から少なくとも部分的に導出される、
第２の識別子を前記認証サーバにおいて受信することと、前記第２の識別子は、前記認証サーバとのワイヤレス局の第１の再認証中に受信される、
前記第１の識別子を前記第２の識別子と比較することと、
前記比較することに少なくとも部分的に基づいて前記ワイヤレス局の認証者に第２のセッション鍵を送信することと
を行うように前記プロセッサによって実行可能である、ワイヤレス通信のための装置。

【請求項２９】
前記第１の識別子は、前記第２の識別子と一致する、請求項２８に記載の装置。
【請求項３０】
前記シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、
前記再認証鍵および前記次のシーケンス番号に少なくとも部分的に基づいて第３の識別子を導出することと
を行うように前記プロセッサによって実行可能な命令をさらに備える、請求項２８に記載の装置。
【発明の詳細な説明】
【関連出願の相互参照】
【０００１】
[0001] 本特許出願は、各々が本出願の譲受人に譲渡される、２０１５年１０月２９日に出願された「Ｐｒｉｖａｃｙ Ｄｕｒｉｎｇ Ｒｅ－Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｏｆ ａ Ｗｉｒｅｌｅｓｓ Ｓｔａｔｉｏｎ ｗｉｔｈ ａｎ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｓｅｒｖｅｒ」と題するＬｅｅ他による米国特許出願第１４／９２６，７９１号、および２０１４年１１月１１日に出願された「Ｐｒｉｖａｃｙ Ｄｕｒｉｎｇ Ｒｅ－Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｏｆ ａ Ｗｉｒｅｌｅｓｓ Ｓｔａｔｉｏｎ ｗｉｔｈ ａｎ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｓｅｒｖｅｒ」と題するＬｅｅ他による米国仮特許出願第６２／０７８，１６２号に対する優先権を主張する。
【技術分野】
【０００２】
[0002] 本開示は、例えば、ワイヤレス通信システム、とりわけ、認証サーバとのワイヤレス局の再認証中のプライバシーに関する。
【背景技術】
【０００３】
[0003] ワイヤレス通信システムは、音声、映像、パケットデータ、メッセージング、ブロードキャスト、等のような様々なタイプの通信コンテンツを提供するために広く展開されている。これらのシステムは、利用可能なシステムリソース（例えば、時間、周波数、および電力）を共有することによって、複数のユーザとの通信をサポートすることが可能な多元接続システムであり得る。ワイヤレスネットワーク、例えばＷｉ－Ｆｉネットワーク（ＩＥＥＥ ８０２．１１）のようなワイヤレスローカルエリアネットワーク（ＷＬＡＮ）は、局（ＳＴＡ：station）または移動デバイスと通信し得るアクセスポイント（ＡＰ：access point）を含み得る。ＡＰは、インターネットのようなネットワークに結合され得、移動デバイスが、ネットワークを介して通信する（および／または、アクセスポイントに結合された他のデバイスと通信する）ことを可能にし得る。
【０００４】
[0004] ＡＰを介してアクセス可能なネットワークに対するプライバシーは、ＡＰおよび認証サーバによって、少なくとも部分的に、管理され得る。ワイヤレス局が最初にネットワークにアクセスするとき、ＡＰは、認証サーバとのワイヤレス局の認証を開始し得る。ワイヤレス局が第１のＡＰを介するネットワークへのアクセスから、第２のＡＰを介するネットワークへのアクセスに移行するとき、第２のＡＰは、認証サーバとのワイヤレス局の再認証を開始し得る。どちらの場合においても、ワイヤレス局は、認証サーバがワイヤレス局を認証（または再認証）しない場合、ネットワークへのアクセスを否定され得る。
【発明の概要】
【０００５】
[0005] 説明される特徴は概して、ワイヤレス通信のための様々な改善されたシステム、方法、および／または装置に関する。そのようなシステム、方法、および／または装置は、認証サーバとのワイヤレス局の再認証（例えば、局の移動性（mobility）および異な

るアクセスポイントを介したネットワークへのアクセスの結果として遂行される再認証）中のプライバシーを提供し得る。ワイヤレス局が、拡張アクセスプロトコル（ＥＡＰ）再認証プロトコル（ＥＡＰ－ＲＰ：Re-authentication Protocol）を使用して認証サーバと再認証をするとき、ワイヤレス局は、拡張マスターセッション鍵名（ＥＭＳＫ名：Extended Master Session Key name）を認証サーバに送信し得る。ＥＭＳＫ名は、再認証セッションおよび対応する再認証ルート鍵（ｒＲＫ：re-authentication Root Key）を識別するために使用され得る。しかしながら、ＥＭＳＫ名は、ワイヤレス局とアクセスポイントとの間で安全な関係（secure association）が確立される前に、ワイヤレスチャネルを通して（over）送信され得る（すなわち、ＥＭＳＫ名が暗号化されずに（例えば、プレーンテキストのように）送信される）。受動攻撃者（passive attacker）はそれゆえ、ＥＭＳＫ名を傍受し、ＥＭＳＫ名を、ワイヤレス局またはそのユーザに関する情報を追跡するために使用し得る。本開示は、ワイヤレス局が、認証サーバとのワイヤレス局の再認証中に、ＥＭＳＫ名の送信を差し控え得るシステム、方法、および装置について説明する。

【０００６】

[0006] 例示的な例の第１のセットでは、ワイヤレス通信のための方法が提供される。方法は、再認証鍵およびシーケンス番号からワイヤレス局において第１の識別子を導出することと、再認証鍵は、第１のセッション鍵から少なくとも部分的に導出され、第１の識別子およびドメイン名を認証者に送信することと、第１の識別子およびドメイン名は、認証サーバとのワイヤレス局の第１の再認証中に送信され、第１の再認証中、第１のセッション鍵の名前の送信を差し控えることと、を含み得る。

【０００７】

[0007] いくつかの態様では、方法は、シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、再認証鍵および次のシーケンス番号に少なくとも部分的に基づいて第２の識別子を導出することと、を含み得る。いくつかの態様では、方法は、第２の識別子およびドメイン名を送信することを含み得る。第２の識別子およびドメイン名は、認証サーバとのワイヤレス局の第２の再認証中に送信され得る。いくつかの態様では、方法は、再認証失敗メッセージを受信することと、再認証失敗メッセージを受信することに応答して、第２の識別子およびドメイン名を送信することと、を含み得る。

【０００８】

[0008] いくつかの態様では、方法は、認証サーバとのワイヤレス局の単一の再認証のために第１の識別子を使用することを含み得る。いくつかの実施形態では、方法は、識別子ラベルに少なくとも部分的に基づいて第１の識別子を導出することを含み得る。方法のいくつかの態様では、第１の再認証は、拡張認証プロトコル（ＥＡＰ：extensible authentication protocol）再認証を含み得、第１のセッション鍵は、拡張マスターセッション鍵（ＥＭＳＫ）を含み得、再認証鍵は、再認証ルート鍵（ｒＲＫ）を含み得る。

【０００９】

[0009] 方法のいくつかの態様では、第１の再認証は、認証サーバとの完全な（full）認証を遂行した後に遂行され得る。いくつかの態様では、方法は、再認証失敗メッセージを受信することと、再認証失敗メッセージを受信することに応答して、認証サーバとの完全な認証を遂行することと、を含み得る。

【００１０】

[0010] 例示的な例の第２のセットでは、ワイヤレス通信のための装置が提供される。装置は、プロセッサ、プロセッサと電子通信しているメモリ、およびメモリに記憶されている命令を含み得る。命令は、再認証鍵およびシーケンス番号からワイヤレス局における第１の識別子を導出することと、再認証鍵は、第１のセッション鍵から少なくとも部分的に導出され、第１の識別子およびドメイン名を認証者に送信することと、第１の識別子およびドメイン名は、認証サーバとのワイヤレス局の第１の再認証中に送信され、第１の再認証中、第１のセッション鍵の名前の送信を差し控えることと、を行うようにプロセッサによって実行可能であり得る。

【００１１】

[0011] いくつかの態様では、装置は、シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、再認証鍵および次のシーケンス番号に少なくとも部分的に基づいて第２の識別子を導出することと、を行うようにプロセッサによって実行可能な命令をさらに含み得る。いくつかの態様では、装置は、第２の識別子およびドメイン名を送信するようにプロセッサによって実行可能な命令を含み得る。第２の識別子およびドメイン名は、認証サーバとのワイヤレス局の第２の再認証中に送信され得る。いくつかの態様では、装置は、再認証失敗メッセージを受信することと、再認証失敗メッセージを受信することに応答して、第２の識別子およびドメイン名を送信することと、を行うようにプロセッサによって実行可能な命令を含み得る。

【００１２】

[0012] いくつかの態様では、装置は、認証サーバとのワイヤレス局の単一の再認証のために第１の識別子を使用するようにプロセッサによって実行可能な命令を含み得る。いくつかの態様では、装置は、識別子ラベルに少なくとも部分的に基づいて第１の識別子を導出するようにプロセッサによって実行可能な命令を含み得る。装置のいくつかの態様では、第１の再認証は、拡張ＥＡＰ再認証を含み得、第１のセッション鍵は、ＥＭＳＫを含み得、再認証鍵は、ｒＲＫを含み得る。

【００１３】

[0013] 装置のいくつかの態様では、第１の再認証は、認証サーバとの完全な認証を遂行した後に遂行され得る。いくつかの態様では、装置は、再認証失敗メッセージを受信することと、再認証失敗メッセージを受信することに応答して、認証サーバとの完全な認証を遂行することと、を行うことをプロセッサによって実行可能な命令を含み得る。

【００１４】

[0014] 例示的な例の第３のセットでは、ワイヤレス通信のための方法が提供される。方法は、認証サーバにおいて、再認証鍵およびシーケンス番号から第１の識別子を導出することと、再認証鍵は、第１のセッション鍵から少なくとも部分的に導出され、第２の識別子を認証サーバにおいて受信することと、第２の識別子は、認証サーバとのワイヤレス局の第１の再認証中に受信され、第１の識別子を第２の識別子と比較することと、比較することに少なくとも部分的に基づいて第２のセッション鍵をワイヤレス局の認証者に送信することと、を含み得る。

【００１５】

[0015] 方法のいくつかの態様では、第１の識別子は、第２の識別子と一致（match）し得る。いくつかの態様では、方法は、シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、再認証鍵および次のシーケンス番号に少なくとも部分的に基づいて第３の識別子を導出することと、を含み得る。いくつかの態様では、方法は、認証サーバとのワイヤレス局の第２の再認証中に第４の識別子を受信することと、第３の識別子を第４の識別子と比較することと、比較することに少なくとも部分的に基づいて第２のセッション鍵を送信することと、を含み得る。方法のいくつかの態様では、第３の識別子は、第４の識別子と一致し得る。

【００１６】

[0016] いくつかの態様では、方法は、識別子ラベルに少なくとも部分的に基づいて第１の識別子を導出することを含み得る。いくつかの態様では、方法は、第１の識別子が第２の識別子と一致できないとき、再認証失敗メッセージを送信することを含み得る。方法のいくつかの態様では、再認証失敗メッセージは、第１の識別子と第２の識別子との間の不一致を示すタイプレングスバリュー（ＴＬＶ：type-length value）要素を含み得る。方法のいくつかの態様では、第１の再認証は、ＥＡＰ再認証を含み得、第１のセッション鍵は、ＥＭＳＫを含み得、再認証鍵は、ｒＲＫを含み得、第２のセッション鍵は、ｒＭＳＫを含み得る。

【００１７】

[0017] 例示的な例の第４のセットでは、ワイヤレス通信のための装置が提供される。装置は、プロセッサと、プロセッサと電子通信しているメモリと、メモリに記憶されてい

る命令とを含み得る。命令は、認証サーバにおいて、再認証鍵およびシーケンス番号から第１の識別子を導出することと、再認証鍵は、第１のセッション鍵から少なくとも部分的に導出され、第２の識別子を認証サーバにおいて受信することと、第２の識別子は、認証サーバとのワイヤレス局の第１の再認証中に受信され、第１の識別子を第２の識別子と比較することと、比較することに少なくとも部分的に基づいて第２のセッション鍵をワイヤレス局の認証者に送信することと、を行うようにプロセッサによって実行可能であり得る。

【００１８】

[0018] 装置のいくつかの態様では、第１の識別子は、第２の識別子と一致し得る。いくつかの態様では、装置は、シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、再認証鍵および次のシーケンス番号に少なくとも部分的に基づいて第３の識別子を導出することと、を行うようにプロセッサによって実行可能な命令を含み得る。いくつかの態様では、装置は、認証サーバとのワイヤレス局の第２の再認証中に第４の識別子を受信することと、第３の識別子を第４の識別子と比較することと、比較することに少なくとも部分的に基づいて第２のセッション鍵を送信することと、を行うようにプロセッサによって実行可能な命令を含み得る。装置のいくつかの態様では、第３の識別子は、第４の識別子と一致し得る。

【００１９】

[0019] いくつかの態様では、装置は、識別子ラベルに少なくとも部分的に基づいて第１の識別子を導出するようにプロセッサによって実行可能な命令を含み得る。いくつかの態様では、装置は、第１の識別子が第２の識別子と一致できないとき、再認証失敗メッセージを送信するようにプロセッサによって実行可能な命令を含み得る。装置のいくつかの態様では、再認証失敗メッセージは、第１の識別子と第２の識別子との間の不一致を示すＴＬＶ要素を含み得る。装置のいくつかの態様では、第１の再認証は、ＥＡＰ再認証を含み得、第１のセッション鍵は、ＥＭＳＫを含み得、再認証鍵は、ｒＲＫを含み得、第２のセッション鍵は、ｒＭＳＫを含み得る。

【００２０】

[0020] 前述は、以下の詳細な説明がより良く理解され得るように、本開示による例の特徴および技術的利点をどちらかといえば広く概説している。追加の特徴および利点が以下に説明される。開示される概念および特定の例は、本開示と同じ目的を実行するための他の構造を修正または設計するための基礎として容易に利用され得る。このような等価な構造は、添付の特許請求の範囲の範囲から逸脱しない。本明細書で開示される概念の特徴は、それらの編成および動作の方法の両方に関して、関連する利点とともに、添付の図に関連して検討されたときに以下の説明からより良く理解されるであろう。図の各々は、例示および説明のみを目的として提供され、特許請求の範囲の限定の定義としては提供されない。

【図面の簡単な説明】

【００２１】

[0021] 本開示の性質および利点のさらなる理解は、以下の図面を参照することによって実現され得る。添付の図面では、同様のコンポーネントまたは特徴は、同じ参照ラベルを有し得る。さらに、同じタイプの様々なコンポーネントは、参照ラベルに、ダッシュと、同様のコンポーネント間を区別する第２のラベルとを後続させることによって区別され得る。本明細書中で第１の参照ラベルのみが使用される場合、その説明は、第２の参照ラベルに関わりなく同じ第１の参照ラベルを有する同様のコンポーネントのいずれか１つに適用可能である。

【図１】[0022] 図１は、本開示の様々な態様にしたがって、ワイヤレス通信システムのブロック図を示す。

【図２】[0023] 図２は、本開示の様々な態様にしたがって、認証サーバとのワイヤレス局の認証または再認証に使用可能な鍵階層（key hierarchy）を示す。

【図３】[0024] 図３は、本開示の様々な態様にしたがって、ワイヤレス通信に使用する

ための装置のブロック図を示す。
【図４】[0025] 図４は、本開示の様々な態様にしたがって、ワイヤレス通信に使用するための装置のブロック図を示す。
【図５】[0026] 図５は、本開示の様々な態様にしたがって、ワイヤレス通信に使用するためのワイヤレス局のブロック図を示す。
【図６】[0027] 図６は、本開示の様々な態様にしたがって、ワイヤレス通信に使用するための装置のブロック図を示す。
【図７】[0028] 図７は、本開示の様々な態様にしたがって、ワイヤレス通信に使用するための装置のブロック図を示す。
【図８】[0029] 図８は、本開示の様々な態様にしたがって、ワイヤレス通信に使用するための認証サーバのブロック図を示す。
【図９】[0030] 図９は、本開示の様々な態様にしたがって、ワイヤレス通信の態様を例示するスイムレーン図（swim lane diagram）を示す。
【図１０】[0031] 図１０は、本開示の様々な態様にしたがって、ワイヤレス通信の態様を例示するスイムレーン図を示す。
【図１１】[0032] 図１１は、本開示の様々な態様にしたがって、ワイヤレス通信の態様を例示するスイムレーン図を示す。
【図１２】[0033] 図１２は、本開示の様々な態様にしたがって、ワイヤレス通信のための方法の例を例示するフローチャートを示す。
【図１３】[0034] 図１３は、本開示の様々な態様にしたがって、ワイヤレス通信のための方法の例を例示するフローチャートを示す。
【図１４】[0035] 図１４は、本開示の様々な態様にしたがって、ワイヤレス通信のための方法の例を例示するフローチャートを示す。
【図１５】[0036] 図１５は、本開示の様々な態様にしたがって、ワイヤレス通信のための方法の例を例示するフローチャートを示す。
【発明を実施するための形態】
【００２２】
[0037] ワイヤレス局（ＳＴＡ）が（例えば、局の移動性および異なるアクセスポイントを介してネットワークにアクセスすることの結果として）、認証サーバと再認証するとき、情報は、ワイヤレス局と、ワイヤレス局が認証サーバと通信するときに介するアクセスポイントとの間に安全な関係が確立される前に、ワイヤレス局から認証サーバに送信され得る（例えば、情報は、暗号化されていないチャネルを通して送信され得る）。情報は、いくつかのケースにおいて、ＥＭＳＫ名を含み得る。ＥＭＳＫ名を傍受する受動攻撃者は、ワイヤレス局またはそのユーザに関する情報を追跡するためにＥＭＳＫ名を使用し得る。
【００２３】
[0038] 攻撃者の有益な追跡情報の傍受を軽減するために、本開示において説明される方法、システム、装置、およびデバイスは、ワイヤレス局が、認証サーバとの再認証中に、ＥＭＳＫ名のような識別子の送信を差し控えることを可能にする。再認証セッションを識別するためにＥＭＳＫ名を送信する代わりに、ワイヤレス局は、再認証鍵（例えば、ｒＲＫ）およびシーケンス番号から導出される識別子を送信し得る。シーケンス番号は、認証サーバとの相互の完全な認証中、またはその結果として導出され得る。第１の再認証セッションのための第１の識別子を生成すると、ワイヤレス局は、シーケンス番号を増加し、再認証鍵および次のシーケンス番号から第２の識別子を導出し得る。このやり方で、再認証セッションの各識別子は、認証サーバとのワイヤレス局の単一の再認証に使用される。再認証に使用される識別子はまた、ワイヤレス局が、ＥＭＳＫ名の中に見出され得る追跡情報を差し控えることを可能にする。そのような識別子を受信する認証サーバは、ワイヤレス局と認証サーバとの間の前の相互の完全な認証中にワイヤレス局と共有された情報から識別子を独立して導出し得る。認証サーバはそれから、識別子が一致するかどうかを決定するために、ワイヤレス局によって導出された識別子と認証サーバによって導出され

た識別子とを比較し得る。識別子が一致するとき、ワイヤレス局は、再認証され得、認証サーバは、ワイヤレス局がネットワークにアクセスし得るときに介するアクセスポイントにセッション鍵を提供し得る。識別子が一致しないとき、認証サーバは、再認証の失敗を示し得、少なくとも一時的に、アクセスポイントにネットワークへのワイヤレス局のアクセスを否認するように命令し得る。

【００２４】

[0039] 以下の説明は、例を提供しており、特許請求の範囲に記載されている範囲、適用可能性、または例を限定してはいない。変更が、本開示の範囲から逸脱することなく、論じられる要素の機能および配置において行われ得る。様々な例は、適宜、様々なプロシージャまたはコンポーネントを省略、代用、または追加し得る。例えば、説明される方法は、説明されるものとは異なる順序で遂行され得、様々なステップが追加、省略、または組み合わされ得る。また、いくつかの例に関して説明される特徴は、他の例において組み合され得る。

【００２５】

[0040] まず図１を参照すると、ブロック図は、例えば標準のＩＥＥＥ８０２．１１ファミリー（IEEE 802.11 family）の少なくとも１つを実装する（implementing）ネットワークのようなＷＬＡＮネットワーク１００の例を例示する。ＷＬＡＮネットワーク１００は、アクセスポイント（ＡＰ）１０５、および移動局、携帯情報端末（ＰＤＡ）、他のハンドヘルドデバイス、ネットブック、ノートブックコンピュータ、タブレットコンピュータ、ラップトップ、表示デバイス（例えば、ＴＶ、コンピュータモニタ、など）、プリンター、などのようなワイヤレスデバイスまたは局（ＳＴＡ）１１５を含み得る。１つのＡＰ１０５のみが例示されているが、ＷＬＡＮネットワーク１００は、複数のＡＰ１０５を有し得る。ワイヤレス局１１５の各々、それはまた移動局（ＭＳ）、移動デバイス、アクセス端末（ＡＴ）、ユーザ機器（ＵＥ）、加入者局（ＳＳ）、または加入者ユニットと呼ばれ得る、は、通信リンク１２０を介してＡＰ１０５と関連付け、通信し得る。各ＡＰ１０５は、そのエリア内のワイヤレス局１１５がＡＰ１０５と一般的に通信することが可能であるような地理的カバレージエリア（geographic coverage area）１１０を有する。ワイヤレス局１１５は、地理的カバレージエリア１１０全体にわたって分散され得る。各ワイヤレス局１１５は、固定式または移動式であり得る。

【００２６】

[0041] 図１に示されていないけれども、ワイヤレス局１１５は、２個以上のＡＰ１０５によってカバーされることが可能であり、それゆえ異なる時間に異なるＡＰ１０５に関連付けることが可能である。単一のＡＰ１０５および局の関連付けられたセットは、基本サービスセット（ＢＳＳ：basic service set）と呼ばれ得る。拡張サービスセット（ＥＳＳ：extended service set）は、接続されたＢＳＳのセットである。配信システム（ＤＳ：distribution system）（図示せず）は、拡張サービスセットにおいて、ＡＰ１０５を接続するために使用される。アクセスポイント１０５のための地理的カバレージエリア１１０は、カバレージエリアの一部分のみを構成するセクタ（図示せず）に分割され得る。ＷＬＡＮネットワーク１００は、カバレージエリアのサイズを変えることおよび異なる技術のためにカバレージエリアを重複すること（overlapping）とともに、異なるタイプのアクセスポイント１０５（例えば、大都市エリア（metropolitan area）、ホームネットワーク、など）を含み得る。図示されないけれども、他のワイヤレスデバイスは、ＡＰ１０５と通信可能である。

【００２７】

[0042] ワイヤレス局１１５は、通信リンク１２０を使用して、ＡＰ１０５を通じて互いに通信し得るが、各ワイヤレス局１１５はまた、ダイレクトワイヤレスリンク１２５を介して、他のワイヤレス局１１５と直接的に通信し得る。２つまたはそれより多いワイヤレス局１１５は、両方のワイヤレス局１１５がＡＰ地理的カバレージエリア１１０にあるとき、または１つまたはどちらのワイヤレス局１１５もＡＰ地理的カバレージエリア１１０内にないとき（図示せず）、ダイレクトワイヤレスリンク１２５を介して通信し得る。

ダイレクトワイヤレスリンク１２５の例は、Ｗｉ－Ｆｉダイレクト接続、Ｗｉ－Ｆｉトンネルドダイレクトリンクセットアップ（ＴＤＬＳ：Wi-Fi Tunneled Direct Link Setup）リンクを使用して確立された接続、および他のＰ２Ｐグループ接続を含み得る。これらの例のワイヤレス局１１５は、ＷＬＡＮ無線と、ＩＥＥＥ８０２．１１標準および８０２．１１ｂ、８０２．１１ｇ、８０２．１１ａ、８０２．１１ｎ、８０２．１１ａｃ、８０２．１１ａｄ、８０２．１１ａｈ、などを含む、但しこれらに限定されない、その様々なバージョンから物理レイヤおよびＭＡＣレイヤを含むベースバンドプロトコルと、にしたがって通信し得る。他の実装において、他のピアツーピア（peer-to-peer）接続および／またはアドホック（ad hoc）ネットワークは、ＷＬＡＮネットワーク１００内に実装され得る。

【００２８】

[0043] ＷＬＡＮネットワーク１００のためのプライバシーは、少なくとも部分的に、ＡＰ１０５のようなＡＰおよび認証サーバ１３５または再認証サーバ１４０によって、管理され得る。ワイヤレス局１１５がＷＬＡＮネットワーク１００に最初にアクセスするとき、ＡＰ１０５は、認証サーバ１３５とのワイヤレス局１１５の認証（例えば、完全な認証）を開始し得る。ワイヤレス局１１５が、第１のＡＰを介するＷＬＡＮネットワーク１００へのアクセスから、第２のＡＰ（例えば、ＡＰ１０５）を介するＷＬＡＮネットワーク１００へのアクセスに移行するとき、ＡＰ１０５は、再認証サーバ１４０とのワイヤレス局１１５の再認証を開始し得る。いつかの例では、認証サーバ１３５は、再認証サーバ１４０を含み得またはそれと通信し得、その再認証サーバ１４０は、認証サーバ１３５のための再認証プロトコルの一部または全てを実行し得る。本開示の目的のために、認証サーバ１３５および／または再認証サーバ１４０は、個々におよび集合的に、認証サーバ１３５と呼ばれる。

【００２９】

[0044] ワイヤレス局１１５は、ワイヤレス局１１５とＷＬＡＮネットワーク１００(例えば、ＡＰ１０５または認証サーバ１３５)との間のワイヤレス通信に対するプライバシーの態様を管理する局側再認証コンポーネント（station-side re-authentication component）１３０を含み得る。認証サーバ１３５は、ワイヤレス局１１５とＷＬＡＮネットワーク１００(例えば、ＡＰ１０５または認証サーバ１３５)との間のワイヤレス通信に対するプライバシーの態様を管理するサーバ側再認証コンポーネント（server-side re-authentication component）１４５を含み得る。いくつかの例では、ワイヤレス局１１５の局側再認証コンポーネント１３０および認証サーバ１３５のサーバ側再認証コンポーネント１４５は、認証サーバ１３５とのワイヤレス局１１５の再認証に参加し得る。いくつかの例では、再認証は、拡張認証プロトコル（ＥＡＰ）再認証を含み得る。

【００３０】

[0045] 図２を参照すると、そこには、本開示の様々な態様にしたがって、認証サーバとのワイヤレス局の認証または再認証に、あるいは他の目的に使用可能な例示的な鍵階層２００が示されている。いくつかの例では、鍵階層２００は、認証サーバとのワイヤレス局のＷｉ－Ｆｉ再認証に使用可能なＥＡＰ－ＲＰ鍵階層の例であり得る。いくつかの例では、ワイヤレス局または認証サーバは、図１に関して説明されたワイヤレス局１１５または認証サーバ１３５の態様の各々の例であり得る。

【００３１】

[0046] 鍵階層２００のルート（root）は、拡張マスターセッション鍵（ＥＭＳＫ）２０５を含む。インターネットエンジニアリングタスクフォース（ＩＥＴＦ：Internet Engineering Task Force）リクエストフォーコメント（ＲＦＣ：Request for Comments）３７４８（ＲＦＣ　３７４８）によると、ＥＭＳＫは、ワイヤレス局と認証サーバとの間の完全な相互認証の結果として導出され得、少なくとも６４バイトの長さを含み得る。ＥＭＳＫ２０５は、ＥＡＰセッションＩＤおよび二進または原文の表示（binary or textual indication）を使用して名づけられ得る。ＥＡＰセッションＩＤは、使用されるＥＡＰ方法（EAP method）に基づき得る。１つの例示的なＥＡＰ方法は、ＥＡＰトランスポートレ

イヤセキュリティ（ＥＡＰ－ＴＬＳ：EAP-Transport Layer Security）である。ＥＡＰ－ＴＬＳは、ＲＦＣ５２１６において定義される。ＥＡＰ－ＴＬＳによると、

【数１】

$$\text{Key\_Material} = \text{TLS-PRF-128(RK, “client EAP encryption”, client.random} \parallel \text{server random) (}i.e.\text{, a 1024 bit output),}$$

$$\text{MSK (Master Session Key)} = \text{Key\_Material(0, 63) (}i.e.\text{, higher 512 bits of Key\_Material),}$$

$$\text{EMSK} = \text{Key\_Material(64, 127) (}i.e.\text{, lower 512 bits of Key\_Material), and}$$

$$\text{Session-ID} = \text{0x0D} \parallel \text{clicnt.random} \parallel \text{server.random,}$$

であり、ここで、client.randomおよびserver.randomは、完全な相互認証中に、認証サーバ（ＡＳ）とワイヤレス局（ＳＴＡ）との間で交換される乱数（各々３２ビット）であり、ＴＬＳ－ＲＰＦ－Ｘは、ＲＦＣ４３４６において定義されるようにＸバイトの出力（すなわち、８Ｘビット）を作る。いくつかの例では、ＥＭＳＫは、期限満了時間（expiration time）に関連づけられ得る。

【００３２】

[0047] ＥＭＳＫから導出される鍵は、例外がシグナリングされるとともに、ＥＭＳＫの識別子（例えば、ＥＭＳＫ名）および派生鍵（descendant key）使用のコンテキスト（context）によって参照され得る。いくつかの例では、ＥＭＳＫ名は次のとおりに導出され得る。

【数２】

$$\text{EMSKname} = \text{KDF (EAP Session-ID, “EMSK”} \mid \text{“\0”} \mid \text{length),}$$

ここで、ＫＤＦは、鍵導出関数（Key Derivation Function）であり、lengthは、８バイト（６４ビット）であり得る。EMSKnameは、完全な相互ＥＡＰ認証中にまたはその結果として導出され得、次の完全な相互ＥＡＰ認証がワイヤレス局と認証サーバとの間で遂行されるまで、認証サーバとともに、ワイヤレス局の従来の再認証プロセスに使用され得る。

【００３３】

[0048] ＥＭＳＫ２０５から導出される鍵は、使用特定ルート鍵（ＵＳＲＫ：Usage Specific Root Key）２１０、ドメイン特定ルート鍵（ＤＳＲＫ：Domain Specific Root Key）２１５、または再認証ルート鍵（ｒＲＫ）２２０を含み得る。ｒＲＫ２２０（またはｒＤＳＲＫ）はまた、ＤＳＲＫ２１５から導出され得る。ドメイン特定使用特定ルート鍵（ＤＳＵＳＲＫ：Domain Specific Usage Specific Root Key）２４０はまた、ＤＳＲＫ２１５から導出され得る。ｒＲＫ２２０は次のとおりに導出され得る。

【数３】

$$\text{rRK} = \text{KDF (K, S),}$$

ここで、Ｋ＝ＥＭＳＫまたはＫ＝ＤＳＲＫであり、

【数４】

$$\text{S} = \text{rRK Label} \mid \text{“\0”} \mid \text{length}$$

であり、rRK Labelは、インターネットアサインドナンバーオーソリティ（ＩＡＮＡ：Internet Assigned Numbers Authority）が割り当てた８ビットの情報交換用米国標準コード（ＡＳＣＩＩ：American Standard Code for Information Exchange）ストリングであり得る：EAP Re-authentication Root Key@ietf.org.。

【００３４】

[0049] 再認証整合鍵（ｒＩＫ：re-authentication Integrity Key）２２５および再認証マスターセッション鍵（例えば、ｒＭＳＫ１ ２３０、・・・、ｒＭＳＫｎ ２３５）は、ｒＲＫ２２０（またはｒＤＳＲＫ）から導出され得る。ｒＩＫ２２５は次のとおり

導出され得る。
【数５】

$$rIK = KDF(K, S),$$

ここで、Ｋ＝ｒＲＫであり、
【数６】

$$S = rIK\ Label \mid \text{“\0”} \mid cryptosuite \mid length$$

であり、rIK Labelは８ビットのＡＳＣＩＩストリングであり得る：Re-authentication Integrity Key@ietf.org.。
【００３５】
[0050] ｒＭＳＫは、次のとおりに導出され得る。
【数７】

$$rMSK = KDF(K, S),$$

ここで、Ｋ＝ｒＲＫであり、
【数８】

$$S = rMSK\ Label \mid \text{“\0”} \mid SEQ \mid length$$

であり、rMSK Labelは、８ビットのＡＳＣＩＩストリングであり得：Re-authentication Master Session Key@ietf.org、ＳＥＱは、ＥＡＰ開始／再認証スタート（または、ＥＡＰ要求／識別）メッセージにおいて、ワイヤレス局によって送られるシーケンス番号であり得、再生保護に使用され得る。ＳＥＱは、再認証が遂行されるとき、１増加され得、新しいｒＲＫが導出されたとき、０に初期化され得る。
【００３６】
[0051] 上記の導出のいずれかにおいて、ＨＭＡＣ－ＳＨＡ－２５６は、デフォルトのＫＤＦとして使用され得る。
【００３７】
[0052] ワイヤレス局が、ネットワークにおいて第１のアクセスポイント（例えば、ＷＬＡＮネットワークにおける第１のアクセスポイント）を介する通信から、（例えば、局移動性の結果として）ネットワークにおいて第２のアクセスポイントを介する通信に移行するとき、ワイヤレス局は、それ自身を認証サーバと再認証し得る。ワイヤレス局は、第１のアクセスポイントから第２のアクセスポイントへのワイヤレス局のハンドオーバの結果として、または、他の理由のために、第１のアクセスポイントを介する通信から第２のアクセスポイントを介する通信に移行し得る。ワイヤレス局が、ＥＡＰ－ＲＰを使用して認証サーバと再認証するとき、ワイヤレス局は、そのＥＭＳＫ名を認証サーバに送信し得る。ＥＭＳＫ名は、再認証セッションおよび対応するｒＲＫ２２０を識別するために使用され得る。しかしながら、ＥＭＳＫ名は、安全な関係がワイヤレス局とアクセスポイントとの間で確立される前に、ワイヤレスチャネルを通して送信される（すなわち、ＥＭＳＫ名が（例えば、プレーンテキストのように）暗号化されずに送信される）。受動攻撃者はそれゆえ、ＥＭＳＫ名を傍受し、ワイヤレス局あるいはそのユーザに関する情報を追跡するためにＥＭＳＫ名を使用し得る。本開示は、ワイヤレス局が、認証サーバとのワイヤレス局の認証中に、ＥＭＳＫ名の送信を差し控え得るシステム、方法、および装置を説明する。
【００３８】
[0053] 図３は、本開示の様々な態様にしたがって、ワイヤレス通信のためにワイヤレス局で使用するための装置１１５－ａのブロック図３００を示す。いくつかの例では、装置１１５－ａは、図１に関連して説明されたワイヤレス局１１５の態様の例であり得る。装置１１５－ａはまた、プロセッサ（図示せず）であり得、またはそれを含み得る。装置１１５－ａは、受信機３０５、局側再認証コンポーネント３１０、および／または送信機３１５を含み得る。これらのコンポーネントの各々は、互いに通信し得る。
【００３９】

[0054] 装置１１５－ａは、受信機３０５、局側再認証コンポーネント３１０、および／または送信機３１５を通じて、本明細書に説明される機能を遂行し得る。例えば、装置１１５－ａは、認証サーバとの装置１１５－ａを含むワイヤレス局の再認証の態様を管理し得る。

【００４０】

[0055] 装置１１５－ａのコンポーネントは、個々にまたは集合的に、ハードウェアに適用可能な機能のいくつかまたは全てを遂行するように適合された特定用途向け集積回路（ＡＳＩＣ）を使用して実装され得る。代替として、機能は、集積回路上で、他の処理ユニット（またはコア）によって遂行され得る。他の例では、他のタイプの集積回路（例えば、構造化（structured）／プラットフォームＡＳＩＣ、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、および他のセミカスタムＩＣ）が使用され得、それらは、当該技術分野において知られている任意のやり方でプログラムされ得る。各コンポーネントの機能はまた、全体的にあるいは部分的に、メモリ中に具現化された命令とともに実装され得、それらの命令は、汎用あるいは特定用途向けプロセッサによって実行されるようにフォーマットされ得る。

【００４１】

[0056] 受信機３０５は、様々な情報チャネル（例えば、制御チャネル、データチャネル、など）に関連付けられたパケット、ユーザデータ、および／または制御情報のような情報を受信し得る。受信機３０５は、認証サーバとの装置１１５－ａを含むワイヤレス局の再認証中に、アクセスポイントから信号、メッセージ等を受信し得る。情報は、局側再認証コンポーネント３１０および装置１１５－ａの他のコンポーネントに渡され得る。

【００４２】

[0057] 局側再認証コンポーネント３１０は、認証サーバとの装置１１５－ａを含むワイヤレス局の再認証の態様に関する機能を監視し、管理し、またはそうでない場合は遂行し得る。局側再認証コンポーネント３１０は、再認証鍵及びシーケンス番号から（および、いくつかの場合においては、識別子ラベルから）、第１の識別子を導出し得る。再認証鍵は、第１のセッション鍵から少なくとも部分的に導出され得る。第１のセッション鍵は、装置１１５－ａを含むワイヤレス局と認証サーバとの間の相互の完全な認証中にあるいはその結果として導出され得る。

【００４３】

[0058] 局側再認証コンポーネント３１０はまた、第１の識別子およびドメイン名を、認証者(例えば、アクセスポイント)に送信し得る。第１の識別子およびドメイン名は、認証サーバとのワイヤレス局の第１の再認証中に送信され得、送信機３１５を介して送信され得る。第１のセッション鍵の名前の送信は、第１の再認証中、差し控えられ得る。いくつかの例では、第１の識別子は、認証サーバとの装置１１５－ａを含むワイヤレス局の単一の再認証に使用され得る。

【００４４】

[0059] いくつかの実施形態では、局側再認証コンポーネント３１０によって遂行される再認証（例えば、第１の再認証）は、Ｗｉ－Ｆｉ再認証を含み得る。これらの実施形態において、再認証は、ＥＡＰ再認証を含み得、第１のセッション鍵は、ＥＭＳＫを含み得、再認証鍵はｒＲＫを含み得る。

【００４５】

[0060] 送信機３１５は、装置１１５－ａの他のコンポーネントから受信した信号を送信し得る。送信機３１５は、認証サーバとの装置１１５－ａを含むワイヤレス局の再認証に関連付けられる様々な信号、メッセージ、などを送信し得る。いくつかの例では、送信機３１５は、トランシーバコンポーネント内に、受信機３０５とコロケートされ得る。送信機３１５は、単一のアンテナ、または複数のアンテナを含み得る。

【００４６】

[0061] 図４は、本開示の様々な態様にしたがって、ワイヤレス通信のためにワイヤレス局で使用するための装置１１５－ｂのブロック図４００を示す。装置１１５－ｂは、図

１に関連して説明されたワイヤレス局１１５の態様の例であり得る。それはまた、図３に関連して説明されたワイヤレス局１１５－ａの例であり得る。装置１１５－ｂは、受信機３０５－ａ、局側再認証コンポーネント３１０－ａ、および／または送信機３１５－ａを含み得、それらは、装置１１５－ａの対応するコンポーネントの例であり得る。装置１１５－ｂはまた、プロセッサ(図示せず)を含み得る。これらのコンポーネントの各々は、互いに通信し得る。局側再認証コンポーネント３１０－ａは、再認証開始管理コンポーネント４０５、識別子導出コンポーネント４１０、再認証情報送信コンポーネント４１５、または再認証失敗管理コンポーネント４２０を含み得る。受信機３０５－ａおよび送信機３１５－ａは、図３の受信機３０５および送信機３１５の機能をそれぞれ遂行し得る。

【００４７】

[0062] 再認証開始管理コンポーネント４０５は、ＥＡＰ再認証の開始に関する機能を監視し、管理し、またはそうでない場合は遂行し得る。ＥＡＰ再認証は、認証サーバとの装置１１５－ｂを含むワイヤレス局の再認証を含み得る。いくつかの態様では、再認証開始管理コンポーネント４０５は、装置１１５－ｂを含むワイヤレス局がハンドオーバしたアクセスポイントから（または、装置１１５－ｂを含むワイヤレス局がネットワークにアクセスしようと試みるときに介するアクセスポイントから）、ＥＡＰ開始／再認証スタート（または、ＥＡＰ要求／識別）メッセージを受信し得る。

【００４８】

[0063] いくつかの態様では、識別子導出コンポーネント４１０は、再認証に使用可能な識別子を導出することの態様を管理し得る。いくつかの例では、識別子導出コンポーネント４１０は、再認証鍵（例えば、ｒＲＫ）、シーケンス番号（ＳＥＱ）、および識別子ラベルから識別子（例えば、ｒＲＫ名）を導出し得る。例えば、識別子は、公式を使って導出され得る。

【数９】

$$rRKname = KDF\,(rRK,\ rRKname\ Label \mid "\backslash 0" \mid SEQ \mid length)$$

ここで、rRKname Label＝“鍵名”であり、ＳＥＱは、再生保護のためにｒＭＳＫの導出において定義されたシーケンス番号のようなシーケンス番号であり、length＝８バイト（すなわち、８オクテット（octets））である。ｒＲＫは、第１のセッション鍵（例えば、ＥＭＳＫ）から少なくとも部分的に導出され得る。第１のセッション鍵は、装置１１５－ｂを含むワイヤレス局と認証サーバとの間の相互の完全な認証中またはその結果として、導出され得る。第１の識別子は、第１のシーケンス番号（例えば、ＳＥＱ＝ＳＥＱ１）およびｒＲＫ名のためのＫＤＦを使用して導出され得る；第２の識別子は、第２のシーケンス番号（例えば、ＳＥＱ２＝ＳＥＱ１＋１）およびｒＲＫ名のためのＫＤＦを使用して導出され得る；など。

【００４９】

[0064] 再認証情報送信コンポーネント４１５は、認証サーバとの装置１１５－ｂを含むワイヤレス局の再認証中に、識別子およびドメイン名を認証者（例えば、アクセスポイント）に送信することに関する機能を管理し、またはそうでない場合は遂行し得る。例えば、再認証情報送信コンポーネント４１５は、認証サーバとのワイヤレス局の第１の再認証中に、第１の識別子およびドメイン名を認証者に送信し得、第１の再認証を完了するためのさらなる試み中に（または、認証サーバとのワイヤレス局の第２の再認証中に）、第２の識別子およびドメイン名を認証者に送信し得る。第１のセッション鍵の名前の送信は、第１の認証を完了するためのさらなる試み中、および／または第２の再認証中、差し控えられ得る。識別子導出コンポーネント４１０によって導出された各識別子は、再認証情報送信コンポーネント４１５によって一回送信され得る（例えば、認証サーバとの装置１１５－ｂを含むワイヤレス局の再認証をするための単一の試み中に使用される）。

【００５０】

[0065] 再認証失敗管理コンポーネント４２０は、単独で、または装置１１５－ｂの他のコンポーネントと協力して、再認証失敗を管理し得る。例えば、再認証失敗メッセージ

を受信することに応答して、再認証失敗管理コンポーネント４２０は、再認証情報送信コンポーネント４１５に、次のシーケンス番号（例えば、１増加されたシーケンス番号）に基づく識別子を送信させ得る。代替として、再認証失敗管理コンポーネント４２０は、認証サーバとの再認証ができないことを示し得、および／または認証サーバとの相互の完全な認証をトリガし得る。

【００５１】

[0066] 図５を参照すると、認証サーバとの再認証を遂行することが可能なワイヤレス局１１５－ｃを例示する図５００が示されている。ワイヤレス局１１５－ｃは、様々な構成を有し得、パーソナルコンピュータ（例えば、ラップトップコンピュータ、ネットブックコンピュータ、タブレットコンピュータ、など）、セルラ電話、ＰＤＡ、デジタルビデオレコーダ（ＤＶＲ）、インターネット家電（internet appliance）、ゲーム機（gaming console）、電子リーダ（e-reader）、などを含み得、またはその一部であり得る。ワイヤレス局１１５－ｃは、モバイル動作を容易にするために、小型バッテリのような、内部電源（図示せず）を有し得る。ワイヤレス局１１５－ｃは、図１、図３、および図４のワイヤレス局１１５および／または装置１１５の例であり得る。

【００５２】

[0067] ワイヤレス局１１５－ｃは、プロセッサ５０５、メモリ５１５、トランシーバ５３５、アンテナ５４０、局側再認証コンポーネント３１０－ｂ、および通信管理コンポーネント５１０を含み得る。局側再認証コンポーネント３１０－ｂは、図３または図４の局側再認証コンポーネント３１０の例であり得る。これらのコンポーネントの各々は、少なくとも１つのバス５４５を通して、直接的または間接的に、互いに通信し得る。

【００５３】

[0068] メモリ５１５は、ランダムアクセスメモリ（ＲＡＭ）またはリードオンリーメモリ（ＲＯＭ）を含み得る。メモリ５１５は、実行されるとき、プロセッサ５０５に、認証サーバとのワイヤレス局１１５－ｃの再認証のために本明細書で説明される様々な機能を遂行させる命令を含むコンピュータ可読、コンピュータ実行可能ソフトウェア（ＳＷ）コード５２０を記憶し得る。代替として、ソフトウェアコード５２０は、プロセッサ５０５によって直接的に実行可能であり得るのではなく、（例えば、コンパイルされ（compiled）、実行されるとき）コンピュータに、本明細書で説明される機能を遂行させ得る。

【００５４】

[0069] プロセッサ５０５は、インテリジェントハードウェアデバイス、例えば、中央処理ユニット（ＣＰＵ）、マイクロコントローラ、ＡＳＩＣ、などを含み得る。プロセッサ５０５は、トランシーバ５３５を通じて受信されるおよび／またはアンテナ５４０を通じた送信のためにトランシーバ５３５に送られるように情報を処理し得る。プロセッサ５０５は、単独で、または、局側再認証コンポーネント３１０－ｂと接続して、認証サーバとのワイヤレス局１１５－ｃの再認証の様々な態様を操作し（handle）得る。

【００５５】

[0070] トランシーバ５３５は、図１に示された少なくとも１つのＡＰ１０５と、または図１、図３、および図４に示された他のワイヤレス局１１５、移動デバイス、および／または装置と双方向に通信し得る。トランシーバ５３５は、いくつかの例では、少なくとも１つの送信機コンポーネントおよび少なくとも１つの別個の受信機コンポーネントとして実装され得る。トランシーバ５３５は、送信のためにパケットを変調し、変調されたパケットをアンテナ５４０に提供するために、およびアンテナ５４０から受信されるパケットを復調するために、モデムを含み得る。ワイヤレス局１１５－ｃは、単一のアンテナを含み得るが、ワイヤレス局１１５－ｃが複数のアンテナ５４０を含み得る態様が存在し得る。

【００５６】

[0071] 図５のアーキテクチャにしたがって、ワイヤレス局１１５－ｃは、通信管理コンポーネント５１０をさらに含み得る。通信管理コンポーネント５１０は、様々なアクセスポイント１０５－ａ、ワイヤレス局１１５－ｄ、などとの通信を管理し得る。通信管理

コンポーネント５１０は、少なくとも１つのバス５４５を通して、ワイヤレス局１１５－ｃの他のコンポーネントのいくつかまたは全てと通信するワイヤレス局１１５－ｃのコンポーネントであり得る。代替として、通信管理コンポーネント５１０の機能性は、トランシーバ５３５のコンポーネントとして、コンピュータプログラム製品として、および／または、プロセッサ５０５の少なくとも１つのコントローラ要素として、実装され得る。

【００５７】

[0072] ワイヤレス局１１５－ｃのコンポーネントは、図１、図３、および図４に関して上記で論じられた態様を実装し得、それらの態様は、簡潔さのために、本明細書では繰り返されないことがある。

【００５８】

[0073] 図６は、本開示の様々な態様にしたがって、認証サーバで使用するための装置１３５－ａのブロック図６００を示す。いくつかの例では、装置１３５－ａは、図１に関連して説明された認証サーバ１３５の態様の例であり得る。装置１３５－ａはまた、プロセッサ（図示せず）であり得、またはそれを含み得る。装置１３５－ａは、受信機６０５、サーバ側再認証コンポーネント６１０、および／または送信機６１５を含み得る。これらのコンポーネントの各々は、互いに通信し得る。

【００５９】

[0074] 装置１３５－ａは、受信機６０５、サーバ側再認証コンポーネント６１０、および／または送信機６１５を通じて、本明細書で説明される機能を遂行し得る。例えば、装置１３５－ａは、装置１３５－ａを含む認証サーバとのワイヤレス局の再認証の態様を管理し得る。

【００６０】

[0075] 装置１３５－ａのコンポーネントは、個々にまたは集合的に、ハードウェアに適用可能な機能のいくつかまたは全てを遂行するように適合されたＡＳＩＣを使用して実装され得る。代替として、機能は、集積回路上で、他の処理ユニット（またはコア）によって遂行され得る。他の例では、他のタイプの集積回路（例えば、ストラクチャード／プラットフォームＡＳＩＣ、ＦＰＧＡ、および他のセミカスタムＩＣ）が使用され得、それらは、当該技術において知られている任意のやり方でプログラムされ得る。各コンポーネントの機能はまた、全体的にあるいは部分的に、メモリ中に具現化された命令とともに実装され得、それらの命令は、汎用あるいは特定用途向けプロセッサによって実行されるようにフォーマットされ得る。

【００６１】

[0076] 受信機６０５は、様々な情報チャネル（例えば、制御チャネル、データチャネル、など）に関連付けられた、パケット、ユーザデータ、および／または制御情報のような情報を受信し得る。受信機６０５は、装置１３５－ａを含む認証サーバとのワイヤレス局の再認証中に、アクセスポイントから、信号、メッセージ等を受信し得る。情報は、サーバ側再認証コンポーネント６１０、および装置１３５－ａの他のコンポーネントに渡され得る。

【００６２】

[0077] サーバ側再認証コンポーネント６１０は、認証サーバとの装置１１５－ａを含むワイヤレス局の再認証の態様に関する機能を監視し、管理し、またはそうでない場合は遂行し得る。サーバ側再認証コンポーネント６１０は、再認証鍵およびシーケンス番号から（および、いくつかのケースでは、識別子ラベルから）第１の識別子を導出し得る。再認証鍵は、第１のセッション鍵から少なくとも部分的に導出され得る。第１のセッション鍵は、ワイヤレス局と装置１３５－ａを含む認証サーバとの間の相互の完全な認証中、またはその結果として導出され得る。

【００６３】

[0078] サーバ側再認証コンポーネント６１０はまた、第２の識別子を受信し得る。第２の識別子は、装置１３５－ａを含む認証サーバとのワイヤレス局の第１の再認証中に受信され得る。いくつかの例では、第２の識別子は、装置１３５－ａを含む認証サーバとの

ワイヤレス局の単一の再認証に使用され得る。いくつかの例では、第２の識別子は、認証者（例えば、アクセスポイント）を介して認証サーバにおいて受信され得る。

【００６４】

[0079] なお、さらに、サーバ側再認証コンポーネント６１０は、第１の識別子を第２の識別子と比較し得る。サーバ側再認証コンポーネント６１０はそれから、比較することに少なくとも部分的に基づいて第２のセッション鍵を送信し得る。例えば、第１の識別子が第２の識別子と一致するとき、サーバ側再認証コンポーネント６１０は、第２のセッション鍵を、第２の識別子がワイヤレス局から受信されたときに介する認証者（例えば、アクセスポイント）に送信し得る。

【００６５】

[0080] いくつかの実施形態では、サーバ側再認証コンポーネント６１０によって遂行される再認証（例えば、第１の再認証）は、Ｗｉ－Ｆｉ再認証を含み得る。これらの実施形態では、再認証は、ＥＡＰ再認証を含み得、第１のセッション鍵は、ＥＭＳＫを含み得、再認証鍵はｒＲＫを含み得、第２のセッション鍵は、ｒＭＳＫを含み得る。

【００６６】

[0081] 送信機６１５は、装置１３５－ａの他のコンポーネントから受信した信号を送信し得る。送信機６１５は、装置１３５－ａを含む認証サーバとのワイヤレス局の再認証に関連付けられる様々な信号、メッセージ、などを送信し得る。いくつかの例では、送信機６１５は、トランシーバコンポーネント内に受信機６０５とコロケートされ得る。送信機６１５は、単一のアンテナ、または複数のアンテナを含み得る。

【００６７】

[0082] 図７は、本開示の様々な態様にしたがって、ワイヤレス通信のために認証サーバで使用するための装置１３５－ｂのブロック図７００を示す。装置１３５－ｂは、図１に関連して説明された認証サーバ１３５の例であり得る。それはまた、図６に関連して説明された装置１３５－ａの例であり得る。装置１３５－ｂは、受信機６０５－ａ、サーバ側再認証コンポーネント６１０－ａ、および／または送信機６１５－ａを含み得、それらは、装置１３５－ａの対応するコンポーネントの例であり得る。装置１３５－ｂはまた、プロセッサ(図示せず)を含み得る。これらのコンポーネントの各々は、互いに通信し得る。サーバ側再認証コンポーネント６１０－ａは、識別子導出コンポーネント７０５、再認証情報受信コンポーネント７１０、再認証管理コンポーネント７１５、再認証情報送信コンポーネント７２０、または再認証失敗管理コンポーネント７２５を含み得る。受信機６０５－ａおよび送信機６１５－ａは、図６の受信機６０５および送信機６１５の機能をそれぞれ遂行し得る。

【００６８】

[0083] いくつかの態様では、識別子導出コンポーネント７０５は、再認証に使用可能な識別子を導出することの態様を管理し得る。いくつかの例では、識別子導出コンポーネント７０５は、再認証鍵（例えば、ｒＲＫ）、シーケンス番号（ＳＥＱ）、および識別子ラベルから識別子（例えば、ｒＲＫ名）を導出し得る。例えば、識別子は、図４に関して説明された、ｒＲＫ名の公式を使って導出され得る。再認証鍵（ｒＲＫ）は、第１のセッション鍵（例えば、ＥＭＳＫ）から少なくとも部分的に導出され得る。第１のセッション鍵は、ワイヤレス局と装置１１５－ｂを含む認証サーバとの間の相互の完全な認証中に、またはその結果として、導出され得る。第１の識別子は、第１のシーケンス番号（例えば、ＳＥＱ＝ＳＥＱ１）およびｒＲＫ名のためのＫＤＦを使用して導出され得る；第２の識別子は、第２のシーケンス番号（例えば、ＳＥＱ２＝ＳＥＱ１＋１）およびｒＲＫ名のためのＫＤＦを使用して導出される；など。

【００６９】

[0084] 再認証情報受信コンポーネント７１０は、装置１３５－ｂを含む認証サーバとのワイヤレス局の再認証中に、識別子を受信することに関する機能を管理し、またはそうでない場合は遂行し得る。例えば、再認証情報受信コンポーネント７１０は、認証サーバとのワイヤレス局の第１の再認証中にワイヤレス局から第１の識別子を受信し得、第１の

再認証を完了させるためのさらなる試み中に（または、認証サーバとのワイヤレス局の第２の再認証中に）、ワイヤレス局から第２の識別子を受信し得る。（１つまたは複数の）識別子は、認証者（例えば、アクセスポイント）を介してワイヤレス局から受信され得る。

【００７０】

[0085] いくつかの態様では、再認証管理コンポーネント７１５は、ワイヤレス局を再認証することに関する機能を管理し、またはそうでない場合は遂行し得る。例えば、再認証管理コンポーネント７１５は、ワイヤレス局から受信した識別子を装置１３５－ｂによって導出された識別子と比較し得る。ワイヤレス局および装置１３５－ｂは、ワイヤレス局と装置１３５－ｂを含む認証サーバとの間の相互の完全な認証中、またはその結果として、鍵情報を交換することに加えて、それらのシーケンス番号の生成を同時にし（synchronize）得る。ワイヤレス局から受信される識別子が装置１３５－ｂによって導出される識別子と一致するとき、再認証管理コンポーネント７１５は、再認証情報送信コンポーネント７２０に第２のセッション鍵を送信させ得る。第２のセッション鍵は、ワイヤレス局から受信される識別子が受信されるときに介する認証者（例えば、アクセスポイント）に送信され得る。

【００７１】

[0086] 再認証失敗管理コンポーネント７２５は、単独で、または装置１３５－ｂの他のコンポーネントと協力して、再認証の失敗を管理し得る。例えば、ワイヤレス局から受信される識別子が、装置１３５－ｂによって導出される識別子と一致できないとき、再認証失敗管理コンポーネント７２５は、（例えば、ＲＦＣ６６９６によって定義されるように）再認証失敗メッセージを送信し得る。再認証失敗メッセージは、識別子間の不一致を示すタイプレングスバリュー（ＴＬＶ）要素を含み得る。再認証失敗メッセージは、一致しない識別子（non-matching）が受信されるワイヤレス局に送信され得る。再認証失敗メッセージは、一致しない識別子が装置１３５－ｂによって受信されるときに通じるアクセスポイントを介してワイヤレス局に送信され得る。装置１３５－ｂが識別子を一致できないので、再認証失敗メッセージの送信は、完全には（integrity）保護されないことがある（例えば、装置１３５－ｂは、ｒＲＫに対応するｒＩＫを置く（locate）ことができないことがある）。

【００７２】

[0087] 図８を参照すると、ワイヤレス局の再認証を遂行することが可能な認証サーバ１３５－ｃを例示する図８００が示されている。認証サーバ１３５－ｃは、図１、図６、および図７の認証サーバ１３５および／または装置１３５の例であり得る。認証サーバ１３５－ｃは、プロセッサ８１０、メモリ８２０、トランシーバ８３０、アンテナ８４０、およびサーバ側再認証コンポーネント６１０－ｂを含み得る。サーバ側再認証コンポーネント６１０－ｂは、図６または図７のサーバ側再認証コンポーネント６１０の例であり得る。いくつかの例では、認証サーバ１３５－ｃはまた、ＡＰ／基地局通信コンポーネント８６０を含み得る。これらのコンポーネントの各々は、少なくとも１つのバス８０５を通して、直接的にまたは間接的に、互いに通信し得る。

【００７３】

[0088] メモリ８２０は、ＲＡＭまたはＲＯＭを含み得る。メモリ８２０はまた、実行されるとき、プロセッサ８１０に、認証サーバ１３５－ｃとのワイヤレス局の再認証のために本明細書で説明される様々な機能を遂行させる命令を含むコンピュータ可読、コンピュータ実行可能なＳＷコード８２５を記憶し得る。代替として、ソフトウェアコード８２５は、プロセッサ８１０によって直接的に実行可能であり得るのではなく、（例えば、コンパイルされ、実行されるとき）コンピュータに、本明細書で説明される機能を遂行させ得る。

【００７４】

[0089] プロセッサ８１０は、インテリジェントハードウェアデバイス、例えば、ＣＰＵ、マイクロコントローラ、ＡＳＩＣ、などを含み得る。プロセッサ８１０は、トランシ

ーバ８３０および／またはＡＰ／基地局通信コンポーネント８６０を通じて受信した情報を処理し得る。プロセッサ８１０はまた、アンテナ８４０および／またはＡＰ／基地局通信コンポーネント８６０を通じて、通信のためにトランシーバ８３０に送られるように情報を処理し得る。プロセッサ８１０は、単独で、またはサーバ側再認証コンポーネント６１０－ｂと接続して、ワイヤレス局の再認証に関する様々な態様を操作し得る。

【００７５】

[0090] トランシーバ８３０は、送信のためにパケットを変調し、変調されたパケットをアンテナ８４０に提供するために、およびアンテナ８４０から受信されるパケットを復調するために、モデムを含み得る。トランシーバ８３０は、少なくとも１つの送信機コンポーネントおよび少なくとも１つの別個の受信機コンポーネントとして実装され得る。トランシーバ８３０は、アンテナ８４０を介して、図１に関して説明されたアクセスポイント１０５のような少なくとも１つのアクセスポイント１０５と双方向に通信し得る。認証サーバ１３５－ｃは、典型的に、複数のアンテナ８４０（例えば、アンテナアレイ）を含み得る。認証サーバ１３５－ｃは、ＡＰ／基地局通信コンポーネント８６０を使用して、アクセスポイント／基地局１０５－ｂまたはアクセスポイント／基地局１０５－ｃのようなＡＰ／基地局と通信し得る。

【００７６】

[0091] 認証サーバ１３５－ｃのコンポーネントは、図１、図６、および図７に関して上記で論じられた態様を実装し得、それらの態様は、簡潔さのために、本明細書では繰り返されないことがある。

【００７７】

[0092] 図９は、本開示の様々な態様にしたがって、ワイヤレス通信の態様を例示するスイムレーン図９００である。図９００は、図１に関連して説明されたＷＬＡＮネットワーク１００の態様を例示し得る。図９００は、ワイヤレス局（ＳＴＡ）１１５－ｅ、アクセスポイント（ＡＰ）１０５－ｄ、および認証サーバ（ＡＳ）１３５－ｄを含む。ワイヤレス局１１５－ｅは、図１、および図３～図５に関して上記で説明されたワイヤレス局１１５および／または装置１１５の少なくとも１つの例であり得る。アクセスポイント１０５－ｄは、図１、図５、および図８に関して上記で説明されたアクセスポイント１０５の少なくとも１つの例であり得る。認証サーバ１３５－ｄは、図１および図６～図８に関して上記で説明された認証サーバ１３５および／または装置１３５の少なくとも１つの例であり得る。概して、図９００は、認証サーバ１３５－ｄとのワイヤレス局１１５－ｅの再認証の態様を例示する。いくつかの例では、ワイヤレス局１１５、装置１１５、アクセスポイント１０５、認証サーバ１３５、および／または、装置１３５の１つのようなシステムデバイスは、以下に説明される機能のいくつかまたは全てを遂行するようにデバイスの機能的要素を制御するためのコードのセットを実行し得る。

【００７８】

[0093] ブロック９０５において、ワイヤレス局１１５－ｅは、再認証鍵およびシーケンス番号からワイヤレス局において第１の識別子を導出し得る。再認証鍵は、第１のセッション鍵から少なくとも部分的に導出され得る。

【００７９】

[0094] ９１０において、ワイヤレス局１１５－ｅは、第１の識別子とドメイン名をアクセスポイント１０５－ｄ（例えば、認証者のタイプ）に送信し得る。第１の識別子およびドメイン名は、認証サーバ１３５－ｄとのワイヤレス局１１５－ｅの第１の再認証中に送信され得る。第１のセッション鍵の名前の送信は、第１の再認証中、差し控えられ得る。いくつかの例では、アクセスポイント１０５－ｄは、認証サーバ１３５－ｄを識別するためにドメイン名を使用し得、第１の識別子をラジアスアクセス要求（Radius-Access-Request）９１５の一部として認証サーバ１３５－ｄに送信し得る。いくつかの例では、第１の再認証は、Ｗｉ－Ｆｉ再認証を含み得る。

【００８０】

[0095] 図１０は、本開示の様々な態様にしたがって、ワイヤレス通信の態様を例示す

るスイムレーン図１０００である。図１０００は、図１に関連して説明されたＷＬＡＮネットワーク１００の態様を例示し得る。図１０００は、ワイヤレス局（ＳＴＡ）１１５－ｆ、アクセスポイント（ＡＰ）１０５－ｅ、および認証サーバ（ＡＳ）１３５－ｅを含む。ワイヤレス局１１５－ｆは、図１、図３～図５、および図９に関して上記で説明されたワイヤレス局１１５および／または装置１１５の少なくとも１つの例であり得る。アクセスポイント１０５－ｅは、図１、図５、図８、および図９に関して上記で説明されたアクセスポイント１０５の少なくとも１つの例であり得る。認証サーバ１３５－ｅは、図１および図６～図９に関して上記で説明された認証サーバ１３５および／または装置１３５の少なくとも１つの例であり得る。概して、図１０００は、認証サーバ１３５－ｅとのワイヤレス局１１５－ｆの再認証の態様を例示する。いくつかの例では、ワイヤレス局１１５、装置１１５、アクセスポイント１０５、認証サーバ１３５、および／または装置１３５の１つのようなシステムデバイスは、以下に説明される機能のいくつかまたは全てを遂行するようにデバイスの機能的要素を制御するためのコードのセットを実行し得る。

【００８１】

[0096] １００５において、アクセスポイント１０５－ｅは、ワイヤレス局１１５－ｆの識別（identity）を要求し得る。いくつかの例では、アクセスポイント１０５－ｅは、アクセスポイント１０５－ｅへのワイヤレス局１１５－ｆのハンドオーバの際に、またはワイヤレス局１１５－ｆがアクセスポイント１０５－ｅを介してネットワークまたはサービスにアクセスすることを試みる際に、ワイヤレス局１１５－ｆの識別を要求し得る。

【００８２】

[0097] ブロック１０１０において、ワイヤレス１１５－ｆは、第１の再認証鍵および第１のシーケンス番号からワイヤレス局において第１の識別子を導出し得る。第１の再認証鍵は、第１のセッション鍵から少なくとも部分的に導出され得る。

【００８３】

[0098] １０１５において、ワイヤレス局１１５－ｆは、第１の識別子およびドメイン名を、その識別のための要求に応答して、アクセスポイント１０５－ｅ（例えば、認証者のタイプ）に送信し得る。第１の識別子およびドメイン名は、認証サーバ１３５－ｅとのワイヤレス局１１５－ｆの第１の再認証中に送信され得る。第１のセッション鍵の名前の送信は、第１の認証中、差し控えられ得る。いくつかの例では、アクセスポイント１０５－ｅは、認証サーバ１３５－ｅを識別するためにドメイン名を使用し得、ラジアスアクセス要求メッセージの一部として、１０２０において、第１の識別子を認証サーバ１３５－ｅに送信し得る。

【００８４】

[0099] ブロック１０２５において、認証サーバ１３５－ｅは、第２の再認証鍵および第２のシーケンス番号から第２の識別子を導出し得る。第２の再認証鍵は、第２のセッション鍵から少なくとも部分的に導出され得る。ワイヤレス局１１５－ｆが認証サーバ１３５－ｅとの相互の完全な認証を前に完了していた場合、第１の再認証鍵および第２の再認証は同じになり、第１のセッション鍵および第２のセッション鍵は同じになり、第１のシーケンス番号および第２のシーケンス番号は同じになるであろう。

【００８５】

[0100] ブロック１０３０において、認証サーバ１３５－ｅは、第１の識別子を第２の識別子と比較し得、第１の識別子が第２の識別子と一致すると決定し得る。

【００８６】

[0101] １０３５において、認証サーバ１３５－ｅは、第３のセッション鍵をアクセスポイント１０５－ｅに送信し得る。いくつかの例では、認証サーバ１３５－ｅは、ラジアスアクセス受諾（Radius-Access-Accept）メッセージの一部として、第３のセッション鍵をアクセスポイント１０５－ｅに送信し得る。

【００８７】

[0102] ブロック１０４０および１０４５において、およびアクセスポイントの第３のセッション鍵の受領に少なくとも部分的に基づいて、アクセスポイント１０５－ｅおよび

ワイヤレス局１１５－ｆは、第１の再認証を終了し得る。

【００８８】

[0103] ブロック１０５０において、ワイヤレス局１１５－ｆは、第１のシーケンス番号に少なくとも部分的に基づいて次のシーケンス番号（例えば、第３のシーケンス番号）を生成し得る。ブロック１０５５において、ワイヤレス局１１５－ｆは、第１の再認証鍵および第３のシーケンス番号に少なくとも部分的に基づいて第３の識別子を導出し得る。第３の識別子およびドメイン名は、認証サーバ１３５－ｅとのワイヤレス局１１５－ｆの第２の再認証中に、認証サーバ１３５－ｅに送信され得る。いくつかの例では、第２の再認証は、アクセスポイント１０５－ｅ以外のアクセスポイントを介して遂行され得る。第１のセッション鍵の名前の送信はまた、第２の再認証中、差し控えられ得る。

【００８９】

[0104] ブロック１０６０において、認証サーバ１３５－ｅは、第２のシーケンス番号に少なくとも部分的に基づいて、次のシーケンス番号（例えば、第４のシーケンス番号）を生成し得る。ブロック１０６５において、認証サーバ１３５－ｅは、第２の再認証鍵および第４のシーケンス番号に少なくとも部分的に基づいて第４の識別子を導出し得る。第２の再認証が開始される場合、認証サーバ１３５－ｅは、第３の識別子をワイヤレス局１１５－ｆから受信し、第３の識別子を第４の識別子と比較し得る。

【００９０】

[0105] 図１１は、本開示の様々な態様にしたがって、ワイヤレス通信の態様を例示するスイムレーン図１１００である。図１１００は、図１に関連して説明されたＷＬＡＮネットワーク１００の態様を例示し得る。図１１００は、ワイヤレス局（ＳＴＡ）１１５－ｇ、アクセスポイント（ＡＰ）１０５－ｆ、および認証サーバ（ＡＳ）１３５－ｆを含む。ワイヤレス局１１５－ｇは、図１、図３～図５、図９、および図１０に関して上記で説明されたワイヤレス局１１５および／または装置１１５の少なくとも１つの例であり得る。アクセスポイント１０５－ｆは、図１、図５、図８～図１０に関して上記で説明されたアクセスポイント１０５の少なくとも１つの例であり得る。認証サーバ１３５－ｆは、図１および図６～図１０に関して上記に説明された認証サーバ１３５および／または装置１３５の少なくとも１つの例であり得る。概して、図１１００は、認証サーバ１３５－ｆとのワイヤレス局１１５－ｇの再認証の態様を例示する。いくつかの例では、ワイヤレス局１１５、装置１１５、アクセスポイント１０５、認証サーバ１３５、および／または装置１３５の１つのようなシステムデバイスは、以下に説明される機能のいくつかまたは全てを遂行するようにデバイスの機能的要素を制御するためのコードのセットを実行し得る。

【００９１】

[0106] １１０５において、アクセスポイント１０５－ｆは、ワイヤレス局１１５－ｇの識別を要求し得る。いくつかの例では、アクセスポイント１０５－ｆは、アクセスポイント１０５－ｆへのワイヤレス局１１５－ｇのハンドオーバの際に、またはワイヤレス局１１５－ｇがアクセスポイント１０５－ｆを介してネットワークまたはサービスにアクセスすることを試みる際に、ワイヤレス局１１５－ｆの識別を要求し得る。

【００９２】

[0107] ブロック１１１０において、ワイヤレス１１５－ｇは、第１の再認証鍵および第１のシーケンス番号からワイヤレス局において第１の識別子を導出し得る。第１の再認証鍵は、第１のセッション鍵から少なくとも部分的に導出され得る。

【００９３】

[0108] １１１５において、ワイヤレス局１１５－ｇは、第１の識別子およびドメイン名を、その識別のための要求に応答して、アクセスポイント１０５－ｆ（例えば、認証者のタイプ）に送信し得る。第１の識別子およびドメイン名は、認証サーバ１３５－ｆとのワイヤレス局１１５－ｇの第１の再認証中に送信され得る。第１のセッション鍵の名前の送信は、第１の認証中、差し控えられ得る。いくつかの例では、アクセスポイント１０５－ｆは、認証サーバ１３５－ｅを識別するためにドメイン名を使用し得、ラジアスアクセス要求メッセージの一部として、１１２０において、第１の識別子を認証サーバ１３５－

ｆに送信し得る。

【００９４】

[0109] ブロック１１２５において、認証サーバ１３５－ｆは、第２の再認証鍵および第２のシーケンス番号から第２の識別子を導出し得る。第２の再認証鍵は、第２のセッション鍵から少なくとも部分的に導出され得る。ワイヤレス局１１５－ｇが認証サーバ１３５－ｆとの相互の完全な認証を前に完了していた場合、第１の再認証鍵および第２の再認証は同じになり、第１のセッション鍵および第２のセッション鍵は同じになり、第１のシーケンス番号および第２のシーケンス番号は同じになるであろう。

【００９５】

[0110] ブロック１１３０において、認証サーバ１３５－ｆは、第１の識別子を第２の識別子と比較し、第１の識別子が第２の識別子と一致しないと決定し得る。

【００９６】

[0111] １１３５において、認証サーバ１３５－ｆは、再認証失敗メッセージを、アクセスポイント１０５－ｆを介して、ワイヤレス局１１５－ｇに送信し得る。再認証失敗メッセージは、第１の識別子と第２の識別子との間の不一致を示すＴＬＶ要素を含み得る。認証サーバ１３５－ｆが識別子を一致できないので、再認証失敗メッセージの送信は、完全には保護されないことがある（例えば、認証サーバ１３５－ｆは、ｒＲＫに対応するｒＩＫを置くことができないことがある）。

【００９７】

[0112] ブロック１１４０において、ワイヤレス局１１５－ｇは、第１のシーケンス番号に少なくとも部分的に基づいて、次のシーケンス番号（例えば、第３のシーケンス番号）を生成し得る。ブロック１１４５において、ワイヤレス局１１５－ｇは、第１の再認証鍵および第３のシーケンス番号に少なくとも部分的に基づいて、第３の識別子を導出し得る。１１５０において、ワイヤレス局１１５－ｇは、第１の再認証を遂行する第２の試みにおいて、第３の識別子およびドメイン名をアクセスポイント１０５－ｆに送信し得る。いくつかの例では、アクセスポイント１０５－ｆは、第２のラジアスアクセス要求メッセージの一部として、１１５５において、第３の識別子を認証サーバ１３５－ｆに送信し得る。代替として（例えば、１１４０、１１４５、１１５０、および１１５５の代替として）、ワイヤレス局１１５－ｇは、再認証ができないことを示し、および／または認証サーバ１３５－ｆとのワイヤレス局１１５－ｇの相互の完全な認証をトリガし得る。

【００９８】

[0113] ブロック１１６０において、認証サーバ１３５－ｆは、第３の識別子を第２の識別子と比較し得る。第３の識別子が第２の識別子と一致するとき、認証サーバ１３５－ｆは、第３のセッション鍵を１１６５におけるアクセスポイント１０５－ｆに送信し得る。いくつかの例では、認証サーバ１３５－ｆは、ラジアスアクセス受諾メッセージの一部として、第３のセッション鍵をアクセスポイント１０５－ｆに送信し得る。

【００９９】

[0114] ブロック１１７０および１１７５において、およびアクセスポイントの第３のセッション鍵の受領に少なくとも部分的に基づいて、アクセスポイント１０５－ｆおよびワイヤレス局１１５－ｇは、第１の再認証を終了し得る。

【０１００】

[0115] 第３の識別子が第２の識別子と一致しないとき、認証サーバ１３５－ｆは、第２の再認証失敗メッセージを、アクセスポイント１０５－ｆを介してワイヤレス局１１５－ｇに送信し得る。第２の再認証失敗メッセージは、第１の再認証を遂行する別の試みをトリガし得、または認証サーバ１３５－ｆとのワイヤレス局１１５－ｇの完全な認証の開始をトリガし得る。

【０１０１】

[0116] 図１２は、本開示の様々な態様にしたがって、ワイヤレス通信のための方法１２００の例を例示するフローチャートである。明確さのために、方法１２００は、図１、図５、および図９～図１１に関連して説明されたワイヤレス局の態様、または図３および

図４に関連して説明された装置の態様に関連して以下に説明される。いくつかの例では、ワイヤレス局は、以下に説明される機能を遂行するようにワイヤレス局の機能的要素を制御するためのコードのセットを実行し得る。加えてまたは代替として、ワイヤレス局は、専用（special-purpose）ハードウェアを使って以下に説明する機能を遂行し得る。

【０１０２】

[0117] ブロック１２０５において、方法１２００は、再認証鍵およびシーケンス番号からワイヤレス局において第１の識別子を導出することを含み得る。再認証鍵は、第１のセッション鍵から少なくとも部分的に導出され得る。ブロック１２１０において、方法１２００は、第１の識別子およびドメイン名を認証者（例えば、アクセスポイント）に送信することを含み得る。第１の識別子およびドメイン名は、認証サーバとのワイヤレス局の第１の再認証中に送信され得る。第１のセッション鍵の名前の送信は、第１の再認証中、差し控えられ得る。いくつかの例では、方法１２００は、認証サーバとのワイヤレス局の単一の再認証のために第１の識別子を使用することを含み得る。いくつかの例では、第１の再認証は、Ｗｉ－Ｆｉ再認証を含み得る。

【０１０３】

[0118] ブロック１２０５および１２１０における（１つまたは複数の）動作は、図３～図５に関連して説明された局側再認証コンポーネント３１０を使用して遂行され得る。

【０１０４】

[0119] したがって、方法１２００は、ワイヤレス通信を提供し得る。方法１２００は、単に１つの実装であり、方法１２００の動作は、他の実装が可能になるように、再配置され、またはそうでない場合は修正され得ることに留意されたい。

【０１０５】

[0120] 図１３は、本開示の様々な態様にしたがって、ワイヤレス通信のための方法１３００の例を例示するフローチャートである。明確さのために、方法１２００は、図１、図５、および図９～図１１に関連して説明されたワイヤレス局の態様、または、図３および図４に関連して説明された装置の態様に関連して以下に説明される。いくつかの例において、ワイヤレス局は、以下に説明される機能を遂行するようにワイヤレス局の機能的要素を制御するためのコードのセットを実行し得る。加えてまたは代替として、ワイヤレス局は、専用ハードウェアを使って、以下に説明する機能を遂行し得る。

【０１０６】

[0121] ブロック１３０５において、方法１３００は、再認証鍵およびシーケンス番号からワイヤレス局において第１の識別子を導出することを含み得る。再認証鍵は、第１のセッション鍵から少なくとも部分的に導出され得る。ブロック１３１０において、方法１３００は、第１の識別子およびドメイン名を認証者（例えば、アクセスポイント）に送信することを含み得る。第１の識別子およびドメイン名は、認証サーバとのワイヤレス局の第１の認証中に送信され得る。第１のセッション鍵の名前の送信は、第１の再認証中、差し控えられ得る。いくつかの例では、方法１３００は、認証サーバとのワイヤレス局の単一の再認証のために第１の識別子を使用することを含み得る。いくつかの例では、第１の再認証は、Ｗｉ－Ｆｉ再認証を含み得る。

【０１０７】

[0122] ブロック１３１５において、方法１３００は、シーケンス番号に少なくとも部分的に基づいて、次のシーケンス番号を生成することを含み得る。ブロック１３２０において、方法１３００は、再認証鍵および次のシーケンス番号に少なくとも部分的に基づいて、第２の識別子を導出することを含み得る。

【０１０８】

[0123] ブロック１３２５において、および第１のオプションのフローにおいて、方法１３００は、再認証失敗メッセージを受信することを含み得る。再認証失敗メッセージは、第１の再認証の失敗の際に受信され得る。ブロック１３３０において、方法１３００は、再認証失敗メッセージを受信することに応答して、第２の識別子およびドメイン名を送信することを含み得る。いくつかの例では、ブロック１３１５において生成された次のシ

ーケンス番号、またはブロック１３２０において導出された第２の識別子は、ブロック１３２５において、再認証失敗メッセージを受信した後に、生成され／導出され得る。

【０１０９】

[0124] ブロック１３３５において、および第２のオプションのフローにおいて、方法１３００は、認証サーバとのワイヤレス局の第２の再認証中に、第２の識別子およびドメイン名を送信することを含み得る。いくつかの例では、第１の再認証は、第１の識別子とドメイン名を、第１の認証者（例えば、第１のアクセスポイント）を介して認証サーバに送信することを伴い得、第２の再認証は、第２の識別子およびドメイン名を、第２の認証者（例えば、第２のアクセスポイント）を介して認証サーバに送信することを伴い得る。

【０１１０】

[0125] 第１のセッション鍵の名前の送信は、ブロック１３３０において、再認証失敗メッセージに応答するとき、またはブロック１３３５において、第２の再認証中、差し控えられ得る。いくつかの例では、方法１３００は、認証サーバとのワイヤレス局の再認証をするための単一の試みのために、第１の識別子および第２の識別子の各々を使用することを含み得る。

【０１１１】

[0126] ブロック１３０５、１３１０、１３１５、１３２０、１３２５、１３３０、および１３３５における（１つまたは複数の）動作は、図３～図５に関連して説明された局側再認証コンポーネント３１０を使用して遂行され得る。

【０１１２】

[0127] したがって、方法１３００は、ワイヤレス通信を提供し得る。方法１３００は、単に１つの実装であり、方法１３００の動作は、他の実装が可能になるように、再配置され、またはそうでない場合は修正され得ることに留意されたい。

【０１１３】

[0128] 図１４は、本開示の様々な態様にしたがって、ワイヤレス通信のための方法１４００の例を例示するフローチャートである。明確さのために、方法１４００は、図１および図８～図１１に関連して説明された認証サーバの態様、または、図５および図６に関連して説明された装置の態様に関連して以下に説明される。いくつかの例では、認証サーバは、以下に説明する機能を遂行するように認証サーバの機能的要素を制御するためのコードのセットを実行し得る。加えてまたは代替として、認証サーバは、専用ハードウェアを使用して以下に説明する機能を遂行し得る。

【０１１４】

[0129] ブロック１４０５において、方法１４００は、再認証鍵およびシーケンス番号から、認証サーバにおいて、第１の識別子を導出することを含み得る。再認証鍵は、第１のセッション鍵から少なくとも部分的に導出され得る。ブロック１４１０において、方法１４００は、第２の識別子を認証サーバにおいて受信することを含み得る。第２の識別子は、認証サーバとのワイヤレス局の第１の再認証中に受信され得る。ブロック１４１５において、方法１４００は、第１の識別子を第２の識別子と比較することを含み得る。ブロック１４２０において、方法１４００は、比較することに少なくとも部分的に基づいて第２のセッション鍵を送信することを含み得る。例えば、第１の識別子が第２の識別子と一致するとき、第２のセッション鍵は、第２の識別子が受信されるときに介する認証者（例えば、アクセスポイント）に送信され得る。いくつかの例では、再認証は、Ｗｉ－Ｆｉ再認証を含み得る。

【０１１５】

[0130] ブロック１４０５、１４１０、１４１５、および１４２０における（１つまたは複数の）動作は、図６～図８に関連して説明されたサーバ側再認証コンポーネント６１０を使用して遂行され得る。

【０１１６】

[0131] したがって、方法１４００は、ワイヤレス通信を提供し得る。方法１４００は、単に１つの実装であり、方法１４００の動作は、他の実装が可能になるように、再配置

され、またはそうでない場合は修正され得ることに留意されたい。

【０１１７】

[0132] 図１５は、本開示の様々な態様にしたがって、ワイヤレス通信のための方法１５００の例を例示するフローチャートである。明確さのために、方法１５００は、図１および図８～図１１に関連して説明された認証サーバの態様、または図６および図７に関連して説明された装置の態様に関連して以下に説明される。いくつかの例では、認証サーバは、以下に説明する機能を遂行するように認証サーバの機能的要素を制御するためのコードのセットを実行し得る。加えてまたは代替として、認証サーバは、専用ハードウェアを使用して以下に説明する機能を遂行し得る。

【０１１８】

[0133] ブロック１５０５において、方法１５００は、再認証鍵およびシーケンス番号から、認証サーバにおいて、第１の識別子を導出することを含み得る。再認証鍵は、第１のセッション鍵から少なくとも部分的に導出され得る。ブロック１５１０において、方法１５００は、第２の識別子を認証サーバにおいて受信することを含み得る。第２の識別子は、認証サーバとのワイヤレス局の第１の再認証中に受信され得る。ブロック１５１５において、方法１５００は、第１の識別子を第２の識別子と比較することを含み得る。いくつかの例では、再認証は、Ｗｉ－Ｆｉ再認証を含み得る。

【０１１９】

[0134] ブロック１５２０において、方法１５００は、第１の識別子が第２の識別子と一致するかどうかを決定することを含み得る。第１の識別子が第２の識別子と一致するとき、方法１５００は、ブロック１５２５を続け得る。第１の識別子が第２の識別子と一致しないとき、方法１５００は、ブロック１５５５を続け得る。

【０１２０】

[0135] ブロック１５２５において、方法１５００は、比較することに少なくとも部分的に基づいて、第２のセッション鍵を送信することを含み得る。第２のセッション鍵は、第２の識別子がワイヤレス局から受信されるときに介する認証者（例えば、アクセスポイント）に送信され得る。

【０１２１】

[0136] ブロック１５３０において、方法１５００は、シーケンス番号に少なくとも部分的に基づいて、次のシーケンス番号を生成することを含み得る。ブロック１５３５において、方法１５００は、再認証鍵および次のシーケンス番号に少なくとも部分的に基づいて、第３の識別子を導出することを含み得る。

【０１２２】

[0137] ブロック１５４０において、方法１５００は、認証サーバとのワイヤレス局の第２の再認証中に第４の識別子を受信することを含み得る。ブロック１５４５において、方法１５００は、第３の識別子を第４の識別子と比較することを含み得る。ブロック１５５０において、方法１５００は、比較することに少なくとも部分的に基づいて、第２のセッション鍵を送信することを含み得る。例えば、第３の識別子が第４の識別子と一致するとき、第２のセッション鍵は、第４の識別子がワイヤレス局から受信されるときに介する認証者（例えば、アクセスポイント）に送信され得る。いくつかの例では、第１の再認証は、第１のアクセスポイントを介してワイヤレス局から第２の識別子を受信することを伴い得、第２の再認証は、第２のアクセスポイントを介してワイヤレス局から第４の識別子を受信することを伴い得る。

【０１２３】

[0138] ブロック１５５５において、方法１５００は、第１の識別子が第２の識別子と一致できないとき、再認証失敗メッセージを送信することを含み得る。再認証失敗メッセージは、第１の識別子と第２の識別子との間の不一致を示すＴＬＶ要素を含み得る。ブロック１５６０において、方法１５００は、第１の再認証を遂行するためのワイヤレス局による第２の試み中に第４の識別子を受信することを含み得る。ブロック１５６５において、方法１５００は、第３の識別子を第４の識別子と比較することを含み得る。ブロック１

５７０において、方法１５００は、比較することに少なくとも部分的に基づいて、第２のセッション鍵を送信することを含み得る。例えば、第３の識別子が第４の識別子と一致するとき、第２のセッション鍵は、第４の識別子がワイヤレス局から受信されるときに介する認証者（例えば、アクセスポイント）に送信され得る。

【０１２４】

[0139] ブロック１５０５、１５１０、１５１５、１５２０、１５２５、１５３０、１５３５、１５４０、１５４５、１５５０、１５５５、１５６０、１５６５、および１５７０における（１つまたは複数の）動作は、図６～図８に関連して説明されたサーバ側再認証コンポーネント６１０を使用して遂行され得る。

【０１２５】

[0140] したがって、方法１５００は、ワイヤレス通信を提供し得る。方法１５００は、単に１つの実装であり、方法１５００の動作は、他の実装が可能になるように、再配置され、またはそうでない場合は修正され得ることに留意されたい。

【０１２６】

[0141] いくつかの例では、方法１２００および１３００からの態様は、組み合わされ得、または方法１４００および１５００からの態様は、組み合わされ得る。方法１２００、１３００、などは、単に実装の例であり、方法１２００～１５００の動作は、他の実行が可能になるように、再配置され、またはそうでない場合は修正され得ることに留意されたい。

【０１２７】

[0142] 添付された図面に関連して上述された詳細な説明は、例を説明しており、実装され得るまたは特許請求の範囲の範囲内にある唯一の例を表してはいない。「例（example）」、「例証的（exemplary）」という用語は、本説明中で使用されるとき、「例、事例、または例示としての役割を果たす」ことを意味し、「好ましい」または「他の例に対して有利である」ことを意味しない。詳細な説明は、説明された技法の理解を提供することを目的として特定の詳細を含む。これらの技法は、しかしながら、これらの特定の詳細なしに実施されうる。いくつかの事例において、良く知られている構造および装置は、説明された例の概念を曖昧にすることを避けるために、ブロック図形式で示される。

【０１２８】

[0143] 情報および信号は、多様な異なる技術および技法のうちの任意のものを使用して表わされ得る。例えば、上記の説明の全体にわたって参照され得る、データ、命令、コマンド、情報、信号、ビット、シンボル、およびチップは、電圧、電流、電磁波、磁場または磁性粒子、光場または光学粒子、あるいはそれらの任意の組み合わせによって表わされ得る。

【０１２９】

[0144] 本明細書での開示に関連して説明された様々な例示的なブロックおよびコンポーネントは、汎用プロセッサ、デジタルシグナルプロセッサ（ＤＳＰ）、ＡＳＩＣ、ＦＰＧＡまたは他のプログラマブルロジックデバイス、ディスクリート（discrete）ゲートまたはトランジスタロジック、ディスクリートハードウェアコンポーネント、あるいは本明細書で説明された機能を遂行するように設計されたそれらの任意の組み合わせを用いて実装されまたは遂行され得る。汎用プロセッサは、マイクロプロセッサであり得るが、代替として、このプロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、またはステートマシンであり得る。プロセッサはまた、コンピューティングデバイスの組み合わせ、例えば、ＤＳＰおよびマイクロプロセッサの組み合わせ、複数のマイクロプロセッサ、ＤＳＰコアと連携したマイクロプロセッサ、または任意の他のそのような構成として実装され得る。

【０１３０】

[0145] 本明細書で説明された機能は、ハードウェア、プロセッサによって実行されるソフトウェア、ファームウェア、またはそれらの任意の組み合わせにおいて実装され得る。プロセッサによって実行されるソフトウェアにおいて実装される場合、機能は、命令ま

たはコードとして、コンピュータ可読媒体上に記憶またはコンピュータ可読媒体を介して送信され得る。他の例および実装は、本開示および添付の特許請求の範囲内にある。例えば、ソフトウェアの性質により、上記に説明された機能は、プロセッサによって実行されるソフトウェア、ハードウェア、ファームウェア、ハードワイヤリング、またはこれらの任意の組み合わせを使用して実装されることができる。機能を実装する特徴はまた、機能の一部分が異なる物理的ロケーションにおいて実装されるように分散されることを含めて、様々な位置に物理的に置かれ得る。本明細書で使用される場合、特許請求の範囲を含み、「および／または」という用語は、２つまたはそれより多い項目からなるリストで使用されるとき、リストされた項目のうちの任意の１つが単独で採用されることが可能であること、または、リストされた項目のうちの２つまたはそれより多くからなる任意の組み合わせが採用されることが可能であることを意味する。例えば、ある構成が、コンポーネントＡ、Ｂ、および／またはＣを含むものとして説明されている場合、この構成は、Ａだけ、Ｂだけ、Ｃだけ、ＡとＢの組み合わせ、ＡとＣの組み合わせ、ＢとＣの組み合わせ、またはＡとＢとＣの組み合わせを含むことができる。また、本明細書で使用される場合、特許請求の範囲を含み、項目のリスト（例えば、「のうちの少なくとも１つ」または「のうちの１つまたは複数」のようなフレーズで始まる項目のリスト）において使用されるような「または（or）」は、例えば「Ａ、Ｂ、またはＣのうちの少なくとも１つ」のリストが、Ａ、またはＢ、またはＣ、またはＡＢ、またはＡＣ、またはＢＣ、またはＡＢＣ（すなわち、ＡおよびＢおよびＣ）を意味するような選言的なリスト（disjunctive list）を示す。

【０１３１】

[0146] コンピュータ可読媒体は、コンピュータ記憶媒体と、１つの場所から別の場所へのコンピュータプログラムの転送を容易にする任意の媒体を含む通信媒体との両方を含む。記憶媒体は、汎用または専用コンピュータによってアクセスされることができる任意の利用可能な媒体であり得る。限定ではなく例として、コンピュータ可読媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ（登録商標）、フラッシュメモリ、ＣＤ－ＲＯＭまたは他の光ディスク記憶装置、磁気ディスク記憶装置または他の磁気記憶デバイス、あるいは命令またはデータ構造の形態で所望のプログラムコード手段を搬送または記憶するために使用されることが可能であり、汎用または専用コンピュータ、あるいは汎用または専用プロセッサによってアクセスされることが可能である任意の他の媒体を備えることができる。また、任意の接続は、適切にコンピュータ可読媒体と称される。例えば、ソフトウェアが、同軸ケーブル、光ファイバーケーブル、ツイストペア、デジタル加入者回線（ＤＳＬ）、または赤外線、無線、およびマイクロ波のようなワイヤレス技術を使用して、ウェブサイト、サーバ、または他の遠隔ソースから送信される場合、同軸ケーブル、光ファイバーケーブル、ツイストペア、ＤＳＬ、あるいは赤外線、無線、およびマイクロ波のようなワイヤレス技術は、媒体の定義に含まれる。ディスク（disk）およびディスク（disc）は、本明細書で使用される場合、コンパクトディスク（ＣＤ）（disc）、レーザーディスク（登録商標）（disc）、光ディスク（disc）、デジタル多用途ディスク（ＤＶＤ）（disc）、フロッピー（登録商標）ディスク（disk）およびＢｌｕ－ｒａｙ（登録商標）ディスク（disc）を含み、ここで、ディスク（disk）は通常、磁気的にデータを再生し、その一方でディスク（disc）は、レーザーを用いて光学的にデータを再生する。上記の組み合わせもまた、コンピュータ可読媒体の範囲内に含まれる。

【０１３２】

[0147] 本開示の前の説明は、当業者が本開示を製造または使用することを可能にするために提供される。本開示への様々な修正は、当業者にとって容易に明らかであり、本明細書に定義された一般的な原理は、本開示の範囲から逸脱することなく、他の変形形態に適用され得る。本開示全体にわたって、「例」または「例示的」という用語は、例または事例を示すものであり、言及された例についてのいかなる選好を暗に示すものでも必要とするものでもない。したがって、本開示は、本明細書に説明された例および設計に限定されるべきではなく、本明細書に開示された原理および新規な特徴と一致する最も広い範囲

を与えられるべきである。

【図１】

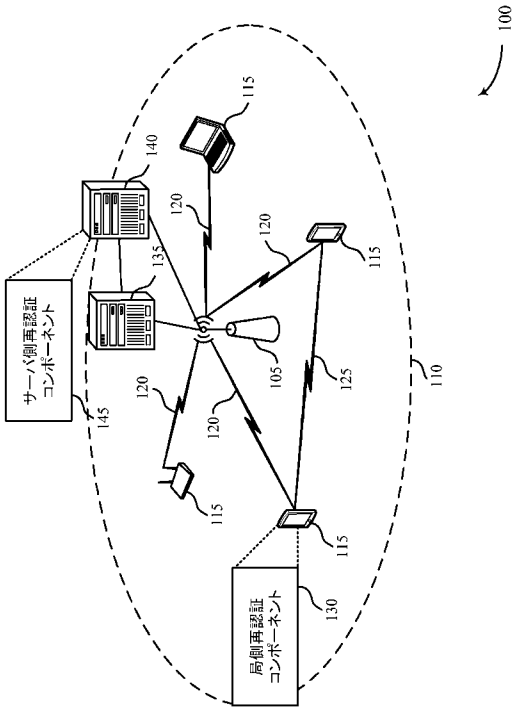


FIG. 1

【図２】

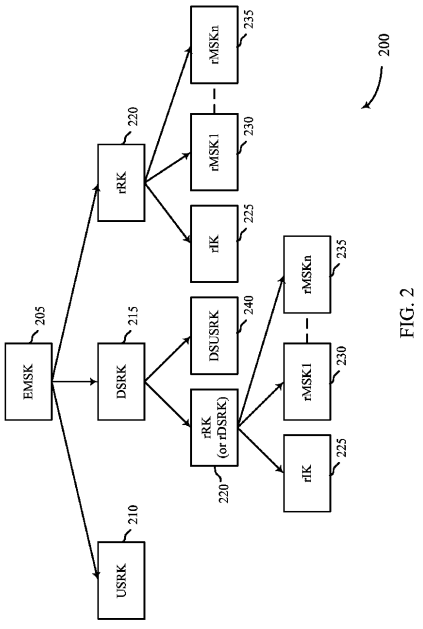


FIG. 2

【図３】

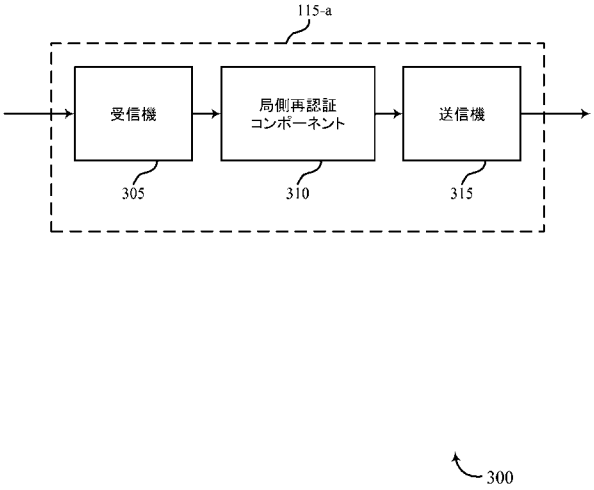


FIG. 3

【図４】

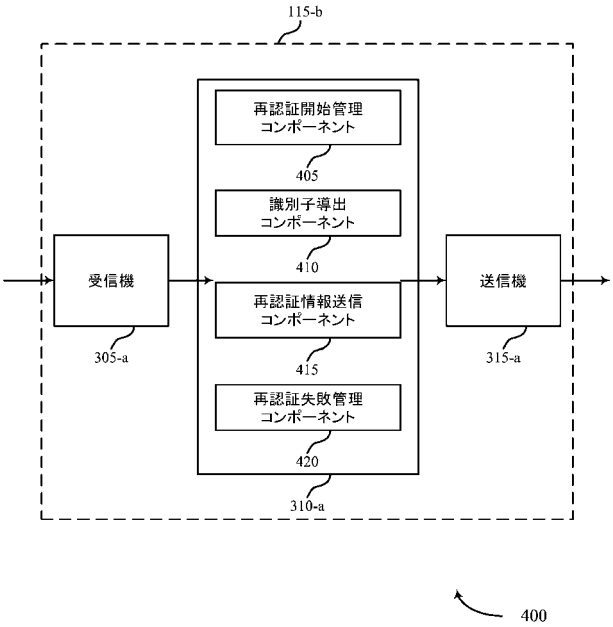


FIG. 4

【図５】

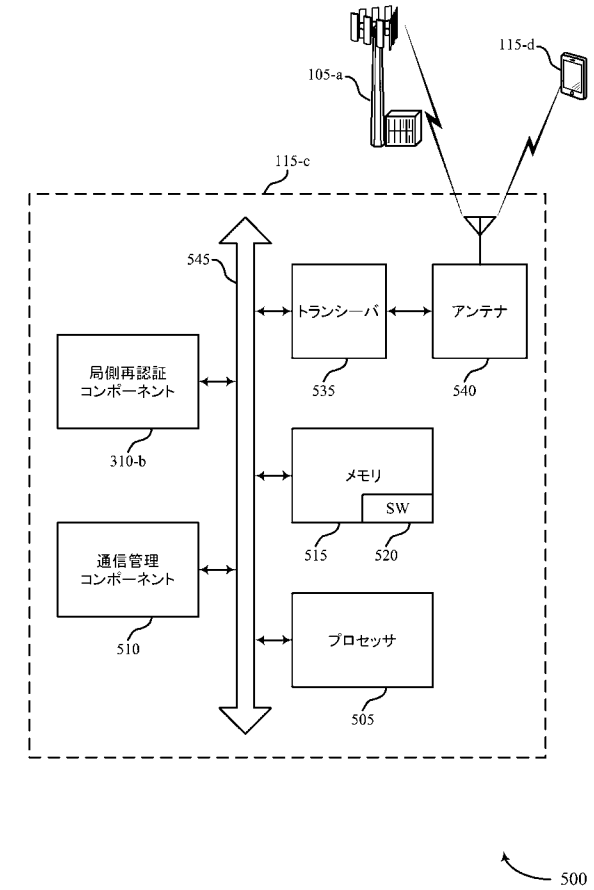


FIG. 5

【図６】

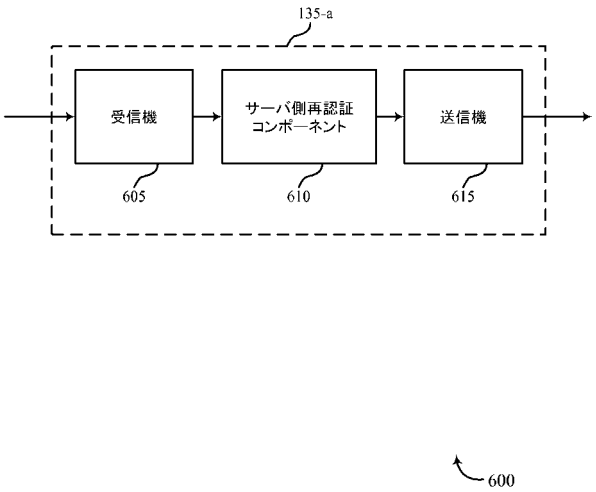


FIG. 6

【図７】

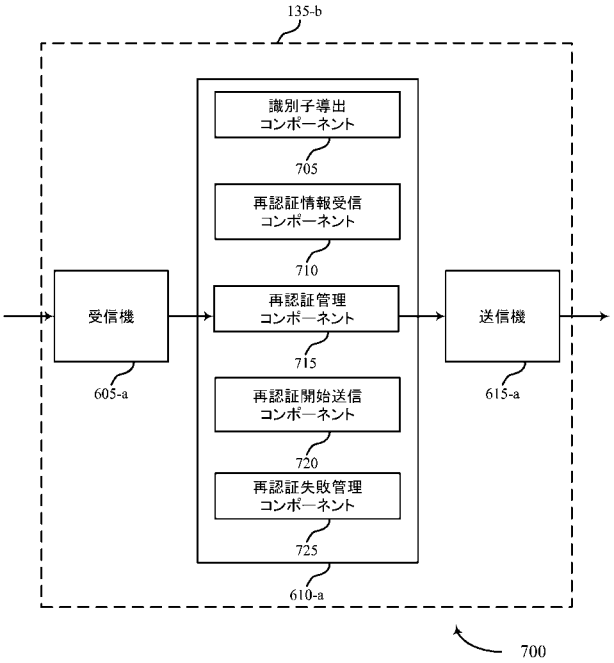


FIG. 7

【図８】

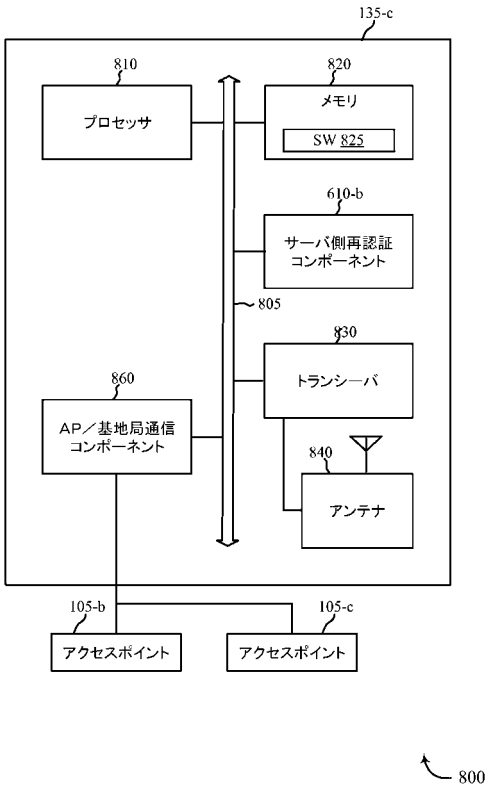


FIG. 8

【図９】

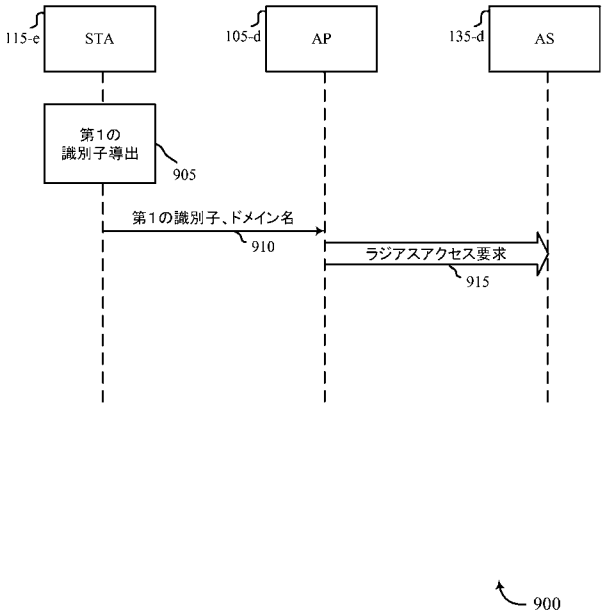


FIG. 9

【図１０】

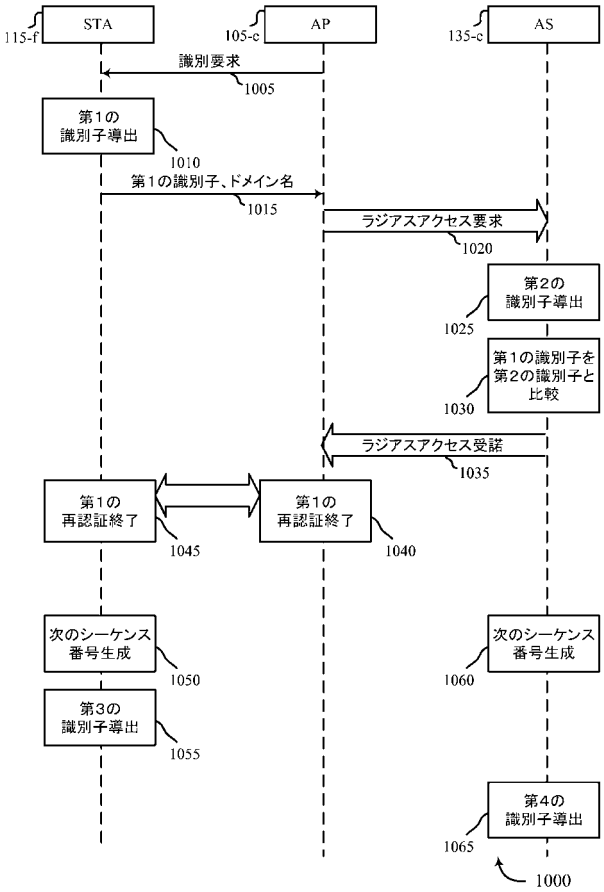


FIG. 10

【図１１】

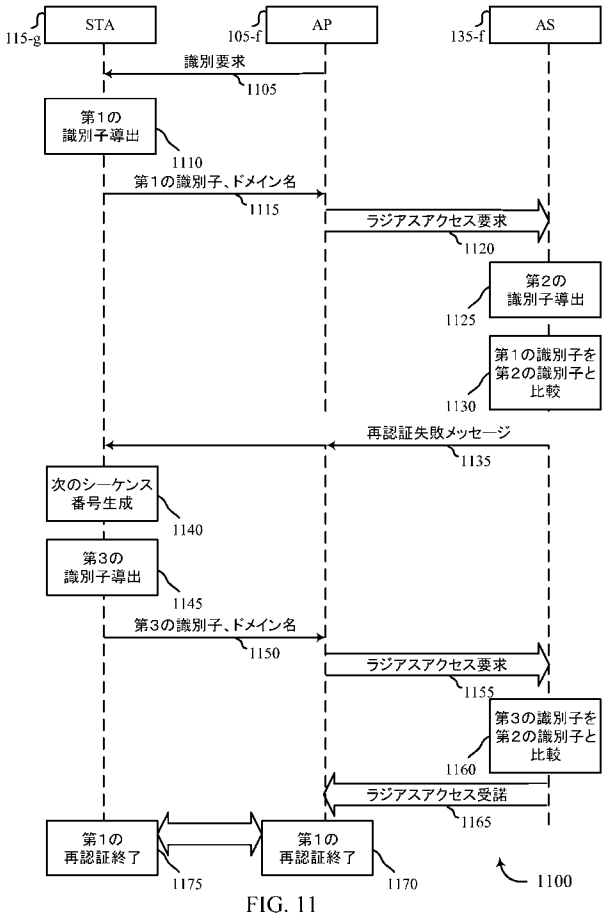
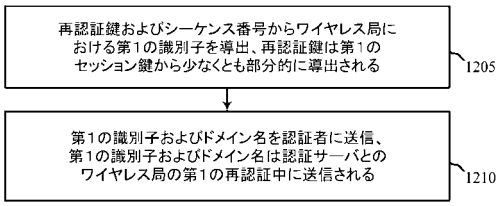


FIG. 11

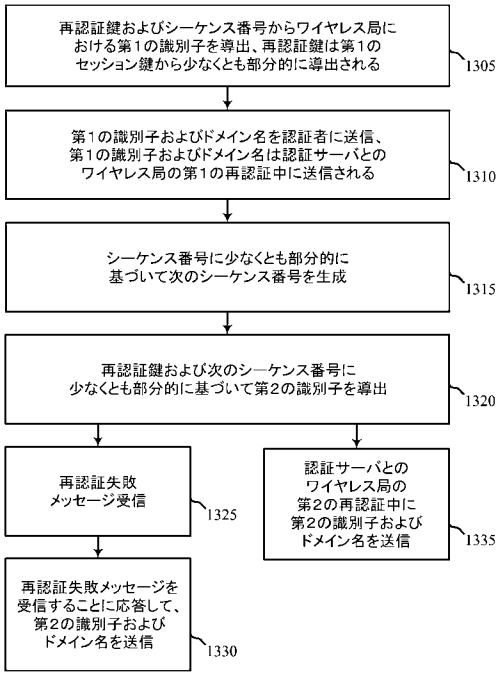
【図１２】



1200

FIG. 12

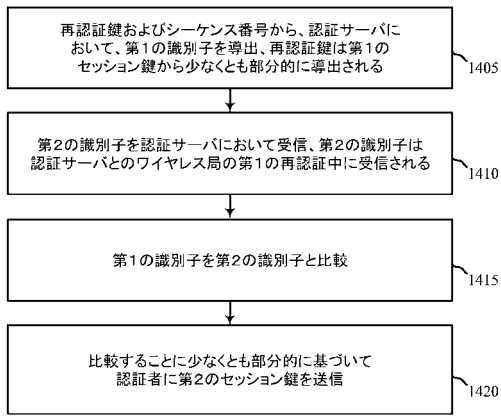
【図１３】



1300

FIG. 13

【図１４】



1400

FIG. 14

【図１５】

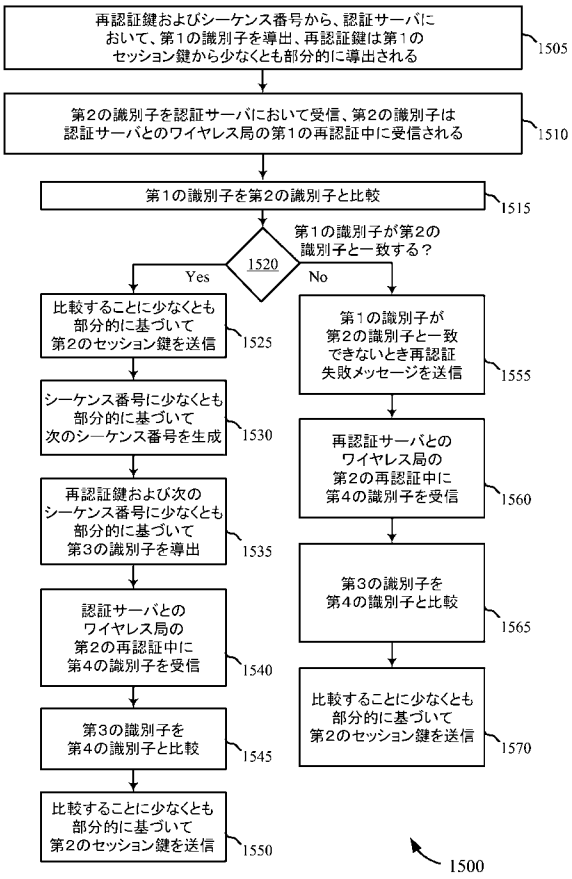

再認証鍵およびシーケンス番号から、認証サーバにおいて、第１の識別子を導出、再認証鍵は第１のセッション鍵から少なくとも部分的に導出される
1505
第２の識別子を認証サーバにおいて受信、第２の識別子は認証サーバとのワイヤレス局の第１の再認証中に受信される
1510
第１の識別子を第２の識別子と比較
1515
第１の識別子が第２の識別子と一致する？
1520
Yes
No
比較することに少なくとも部分的に基づいて第２のセッション鍵を送信
1525
シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成
1530
再認証鍵および次のシーケンス番号に少なくとも部分的に基づいて第３の識別子を導出
1535
認証サーバとのワイヤレス局の第２の再認証中に第４の識別子を受信
1540
第３の識別子を第４の識別子と比較
1545
比較することに少なくとも部分的に基づいて第２のセッション鍵を送信
1550
第１の識別子が第２の識別子と一致できないとき再認証失敗メッセージを送信
1555
再認証サーバとのワイヤレス局の第２の再認証中に第４の識別子を受信
1560
第３の識別子を第４の識別子と比較
1565
比較することに少なくとも部分的に基づいて第２のセッション鍵を送信
1570
1500

FIG. 15

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/058364

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W36/08 H04W12/02 H04L29/06
ADD. H04W12/04

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)
H04W H04L

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/298209 A1 (TARGALI YOUSIF [US] ET AL) 7 November 2013 (2013-11-07) paragraphs [0047] - [0051]; figure 1B paragraphs [0052] - [0056]; figure 2 paragraphs [0039] - [0040]; figure 12	1-30
A	ABOBA B ET AL: "Extensible Authentication Protocol (EAP) Key Management Framework; RFC 5247", INTERNET ENGINEERING TASK FORCE (IETF), August 2008 (2008-08), XP015060257, section 1.4.1 section 3.1	1-30

☐ Further documents are listed in the continuation of Box C.

☒ 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
20 January 2016	29/01/2016

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	Tabery, Peter

1

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/058364

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013298209 A1	07-11-2013	TW 201406118 A	01-02-2014
		US 2013298209 A1	07-11-2013
		WO 2013165605 A1	07-11-2013

Form PCT/ISA/210 (patent family annex) (April 2005)

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,ST,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,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

(72)発明者 リ、ス・ボム
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 チェリアン、ジョージ
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５

Ｆターム(参考) 5J104 AA16 EA06 EA18 NA02 NA37 PA01