(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6371644号
(P6371644)
(45)発行日　平成30年8月8日(2018.8.8)　(24)登録日　平成30年7月20日(2018.7.20)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675A
G06F 21/30	(2013.01)	G06F	21/30	
G06F 21/33	(2013.01)	G06F	21/33	

請求項の数 10　(全 28 頁)

(21)出願番号	特願2014-179883(P2014-179883)
(22)出願日	平成26年9月4日(2014.9.4)
(62)分割の表示	特願2013-514245(P2013-514245)の分割
原出願日	平成23年6月6日(2011.6.6)
(65)公開番号	特開2015-29288(P2015-29288A)
(43)公開日	平成27年2月12日(2015.2.12)
審査請求日	平成26年10月3日(2014.10.3)
審判番号	不服2016-16768(P2016-16768/J1)
審判請求日	平成28年11月9日(2016.11.9)
(31)優先権主張番号	12/813,153
(32)優先日	平成22年6月10日(2010.6.10)
(33)優先権主張国	米国(US)

(73)特許権者　504326572
ジエマルト・エス・アー
フランス国、９２１２０・ムドン、リユ・ドウ・ラ・ベレリー・６
(74)代理人　110001173
特許業務法人川口國際特許事務所
(72)発明者　イオアニス・ブロウステイス
アメリカ合衆国、ニユー・ジヤージー・０７０４１、ミルバーン、メイン・ストリート・１６３、アパートメント・３・ビー
(72)発明者　ガナパシイ・エス・サンダラム
アメリカ合衆国、ニユー・ジヤージー・０８８４４、ヒルズボロー、ヒツコリー・ヒル・ロード・１０

最終頁に続く

(54)【発明の名称】単一の登録手順を使用するクライアントのグループの安全な登録

(57)【特許請求の範囲】
【請求項１】
通信ネットワークにおいて通信デバイスのグループを登録するための方法であって、
ネットワークデバイスから通信デバイスのグループにグループチャレンジメッセージを送信するステップと、
ネットワークデバイスにおいて、それぞれグループ内の少なくとも２つの通信デバイスからグループチャレンジに対する少なくとも２つの応答メッセージを受信するステップであって、応答メッセージのそれぞれはグループに対応する同じグループ資格情報を備えるステップと、
ネットワークデバイスにおいて、グループチャレンジに対する応答メッセージを集約するステップと、
前記少なくとも２つの通信デバイスをグループとして、相互に認証させるために、集約メッセージをネットワークデバイスから通信ネットワーク内のオーセンティケータに送信するステップとを備え、
前記グループに対応する同じグループ資格情報が、グループ内の少なくとも２つの通信デバイスによって、グループチャレンジをグループ内の通信デバイスに共通な鍵と組み合わせることによって、それぞれ計算される、方法。
【請求項２】
グループ内のすべての通信デバイスがグループとしてオーセンティケータと相互に認証されるように、集約メッセージが通信ネットワーク内のオーセンティケータに送信される

、請求項１に記載の方法。
【請求項３】
オーセンティケータが通信ネットワーク内のアプリケーションサーバである、請求項２に記載の方法。
【請求項４】
ネットワークデバイスがグループ内の通信デバイスを認証する、請求項１に記載の方法。
【請求項５】
ネットワークデバイスにおいて、２つ以上の通信デバイスのグループに対するアドレス割り当てを取得するステップをさらに備える、請求項１に記載の方法。
【請求項６】
グループ内の通信デバイスのうちの所与の１つが認証されると、所与の通信デバイスがアプリケーションサーバとのデータセッションを確立する、請求項１に記載の方法。
【請求項７】
通信ネットワークにおいて通信デバイスのグループを登録する際に使用するための装置であって、
メモリと、
メモリに結合されたプロセッサであって、通信デバイスのグループにグループチャレンジメッセージを送信し、それぞれグループ内の少なくとも２つの通信デバイスからグループチャレンジに対する少なくとも２つの応答メッセージを受信し、グループチャレンジに対する応答メッセージを集約し、前記少なくとも２つの通信デバイスをグループとして、相互に認証させるために、集約メッセージを通信ネットワーク内のオーセンティケータに送信するように構成され、応答メッセージのそれぞれがグループに対応する同じグループ資格情報を備えるプロセッサとを備え、
前記グループに対応する同じグループ資格情報が、グループ内の少なくとも２つの通信デバイスによって、グループチャレンジをグループ内の通信デバイスに共通な鍵と組み合わせることによって、それぞれ計算される、装置。
【請求項８】
通信ネットワークにおいて通信デバイスのグループを登録するための方法であって、
グループの通信デバイスの所与の１つにおいて、ネットワークデバイスにより通信デバイスのグループに送信されたグループチャレンジメッセージを受信するステップと、
所与の通信デバイスからネットワークデバイスに、グループチャレンジに対する応答メッセージを送信するステップであって、応答メッセージが、グループ内の少なくとも１つの他の通信デバイスからネットワークデバイスに送信される、グループチャレンジに対する応答メッセージと、グループに対応する同じグループ資格情報を備えるステップと、
ネットワークデバイスからオーセンティケータに送信された集約メッセージを使用して、所与の通信デバイスを、グループ内の前記少なくとも１つの他の通信デバイスとともにグループとして、通信ネットワーク内のオーセンティケータと相互に認証させるステップであって、集約メッセージが、所与の通信デバイスからの応答メッセージと、前記少なくとも１つの他の通信デバイスからネットワークデバイスにおいて受信した、グループチャレンジに対する応答メッセージとを含むステップとを備え、
前記グループに対応する同じグループ資格情報が、所与の通信デバイスと、前記少なくとも１つの他の通信デバイスとによって、グループチャレンジをグループ内の通信デバイスに共通な鍵と組み合わせることによって、それぞれ計算される、方法。
【請求項９】
通信ネットワークにおいて通信デバイスのグループを登録する際に使用するための装置であって、
グループの通信デバイスの所与の１つに関連付けられたメモリと、
所与の通信デバイスに関連付けられ、メモリに結合されたプロセッサであって、ネットワークデバイスにより通信デバイスのグループに送信されたグループチャレンジメッセー

ジを受信し、ネットワークデバイスに、グループチャレンジに対する応答メッセージを送信し、ネットワークデバイスからオーセンティケータに送信された集約メッセージを使用して、所与の通信デバイスを、グループ内の少なくとも１つの通信デバイスとともにグループとして、通信ネットワーク内のオーセンティケータと相互に認証させるように構成され、応答メッセージが、グループ内の前記少なくとも１つの他の通信デバイスからネットワークデバイスに送信される、グループチャレンジに対する応答メッセージと、グループに対応する同じグループ資格情報を備え、集約メッセージが、所与の通信デバイスからの応答メッセージと、前記少なくとも１つの他の通信デバイスからネットワークデバイスにおいて受信した、グループチャレンジに対する応答メッセージとを含む、プロセッサとを備え、

前記グループに対応する同じグループ資格情報が、所与の通信デバイスと、前記少なくとも１つの他の通信デバイスとによって、グループチャレンジをグループ内の通信デバイスに共通な鍵と組み合わせることによって、それぞれ計算される、装置。

【請求項１０】

通信ネットワークにおいてユーザのグループを登録するための方法であって、

ネットワークデバイスからユーザのグループにグループチャレンジメッセージを送信するステップと、

ネットワークデバイスにおいて、それぞれグループ内の少なくとも２つのユーザからグループチャレンジに対する少なくとも２つの応答メッセージを受信するステップであって、応答メッセージのそれぞれがグループに対応する同じグループ資格情報を備えるステップと、

ネットワークデバイスにおいて、グループチャレンジに対する応答メッセージを集約するステップと、

前記少なくとも２つのユーザをグループとして、相互に認証させるために、集約メッセージをネットワークデバイスから通信ネットワーク内のオーセンティケータに送信するステップとを備え、

前記グループに対応する同じグループ資格情報が、グループ内の少なくとも２つのユーザによって、グループチャレンジをグループ内のユーザに共通な鍵と組み合わせることによって、それぞれ計算される、方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は一般に、通信セキュリティに関し、さらに詳細には、単一の登録手順を使用して通信ネットワークにおいて通信デバイスのグループを登録するための技法に関する。

【背景技術】

【０００２】

従来の安全な登録プロトコルは、サーバ（またはネットワーク）で認証するクライアント（またはデバイス）に依存している。たとえば、（クライアントまたはデバイスの）ユーザがサーバにログオンすることがあるか、またはモバイルデバイスがネットワークに登録することもある。多くの場合、登録プロトコルは、サーバ／ネットワークへのクライアント／デバイスの認証、または相互の認証プロトコルを含む。さらに近年、（アクセスだけにとどまらず）セッション全体を保護することを目的として、それらの認証プロトコルは、セッション全体を保護するためにクライアント／デバイスおよびサーバ／ネットワークが鍵のセットを合意できるようにする鍵合意手順を含めるように増強された。

【０００３】

一方向認証プロトコルの例は、Ｗ．Ｓｉｍｐｓｏｎ、「ＰＰＰ Ｃｈａｌｌｅｎｇｅ Ｈａｎｄｓｈａｋｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ（ＣＨＡＰ）」、ＲＦＣ１９９４において説明されるＣＨＡＰ、Ｂ．Ｌｌｏｙｄ、「ＰＰＰ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌｓ」、ＲＦＣ１３３４において説明されるＰＡＰ、Ｅｕｒｏｐｅａｎ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｓｔａｎｄａｒｄｓ Ｉ

nstitute、GSM（登録商標） Technical Specification GSM 03.20（ETS 300 534）：Digital Cellular Telecommunication System（Phase 2）；Security Related Network Functions、August 1997において説明されるGSM triplet based authentication protocolsを含み、それらの開示を引用により全体として本願に援用する。

【0004】

相互認証プロトコルの例は、3GPP TS 33.102、Technical Specification Group Services and System Aspects；3G Security；Security Architecture（Release 9）において説明される3rd Generation Partnership Projects（3GPP）Authentication and Key Agreement（AKA）protocol、およびB. AbobaおよびD. Simon、「PPP EAP TLS Authentication Protocol」、RFC2716において説明されるEAP－TLS（EAPトランスポート層セキュリティ）のようなさまざまな拡張認証プロトコル（EAP：Extensible Authentication Protocol）ベースの相互認証プロトコルを含み、それらの開示を引用により全体として本願に援用する。

【0005】

それらの安全な登録プロトコルは、「シングルサインオン（single sign－on）」プロトコルと一般に称されるものを使用して、複数のサーバに登録するクライアントを含むように拡張された。シングルサインオンにより、ユーザは、1度ログインすると、各システムで再度ログインするようプロンプトで要求されることなくすべてのシステムにアクセスすることができる。それらのプロトコルは、ユーザが複数のサーバにアクセスする許可を有し、同時に複数のサーバにアクセスしようとするような、エンタープライズ環境において極めて有用である。シングルサインオンプロトコルの一例は、R. Cox、E. GrosseおよびR. Pike、「Security in Plan 9」、USENIX、2002年において説明されるFactotumであり、その開示を引用により全体として本願に援用する。

【先行技術文献】

【非特許文献】

【0006】

【非特許文献1】W. Simpson、「PPP Challenge Handshake Authentication Protocol（CHAP）」、RFC1994

【非特許文献2】B. Lloyd、「PPP Authentication Protocols」、RFC1334

【非特許文献3】European Telecommunications Standards Institute、GSM Technical Specification GSM 03.20（ETS 300 534）：Digital Cellular Telecommunication System（Phase 2）；Security Related Network Functions、August 1997

【非特許文献4】3GPP TS 33.102、Technical Specification Group Services and System Aspects；3G Security；Security Architecture（Release 9）

【非特許文献5】B. AbobaおよびD. Simon、「PPP EAP TLS Authentication Protocol」、RFC2716

【非特許文献６】Ｒ．Ｃｏｘ、Ｅ．ＧｒｏｓｓｅおよびＲ．Ｐｉｋｅ、「Ｓｅｃｕｒｉｔｙ ｉｎ Ｐｌａｎ ９」、ＵＳＥＮＩＸ、２００２年
【非特許文献７】３ＧＰＰ ＴＳ ３３．４０１、Ｔｅｃｈｎｉｃａｌ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｇｒｏｕｐ Ｓｅｒｖｉｃｅｓ ａｎｄ Ｓｙｓｔｅｍ Ａｓｐｅｃｔｓ；３ＧＰＰ Ｓｙｓｔｅｍ Ａｒｃｈｉｔｅｃｔｕｒｅ Ｅｖｏｌｕｔｉｏｎ（ＳＡＥ）；Ｓｅｃｕｒｉｔｙ Ａｒｃｈｉｔｅｃｔｕｒｅ（Ｒｅｌｅａｓｅ ９）
【非特許文献８】３ＧＰＰ ＴＳ ２２．３６８、Ｔｅｃｈｎｉｃａｌ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｇｒｏｕｐ Ｓｅｒｖｉｃｅｓ ａｎｄ Ｓｙｓｔｅｍ Ａｓｐｅｃｔｓ；Ｓｅｒｖｉｃｅ Ｒｅｑｕｉｒｅｍｅｎｔｓ ｆｏｒ Ｍａｃｈｉｎｅ Ｔｙｐｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ（ＭＴＣ）；Ｓｔａｇｅ１（Ｒｅｌｅａｓｅ １０）
【非特許文献９】ｈｔｔｐ：／／ｗｗｗ．ｚｉｇｂｅｅ．ｏｒｇ
【非特許文献１０】Ｕ．ＢｌｕｍｅｎｔｈａおよびｌＰ．Ｇｏｅｌ、「Ｐｒｅｓｈａｒｅｄ Ｋｅｙ（ＰＳＫ） Ｃｉｐｈｅｒｓｕｉｔｅｓ ｗｉｔｈ ＮＵＬＬ Ｅｎｃｒｙｐｔｉｏｎ ｆｏｒ Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ（ＴＬＳ）」、ＲＦＣ ４７８５
【非特許文献１１】Ｊ．ＡｒｋｋｏおよびＨ．Ｈａｖｅｒｉｎｅｎ、「Ｅｘｔｅｎｓｉｂｌｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ Ｍｅｔｈｏｄ ｆｏｒ ３ｒｄ Ｇｅｎｅｒａｔｉｏｎ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ａｇｒｅｅｍｅｎｔ（ＥＡＰ－ＡＫＡ）」

【発明の概要】

【発明が解決しようとする課題】

【０００７】

しかし、既存の登録の手法のいずれも、複数のクライアントが安全かつ効率的な方法で１つのシステムにアクセスすることができる「リバースシングルサインオン（ｒｅｖｅｒｓｅ ｓｉｎｇｌｅ ｓｉｇｎ－ｏｎ）」を可能にするメカニズムを提供することはない。複数のクライアントが安全かつ効率的な方法で１つのシステムにアクセスできるようにする課題に対処するための技法、ひいては「リバースシングルサインオン」の課題の解決策を提供することが望ましい。

【課題を解決するための手段】

【０００８】

本発明の実施形態は、複数のクライアントが安全かつ効率的な方法で１つのシステムにアクセスできるようにする課題に対処する通信デバイスのための自動安全登録技法を提供し、ひいては「リバースシングルサインオン」の課題ならびに既存の登録手法のその他の欠点に解決策を提供する。

【０００９】

たとえば、１つの態様において、通信ネットワークにおいて２つ以上の通信デバイスのグループを登録するための方法は、以下のステップを備える。ネットワークデバイスから２つ以上の通信デバイスのグループにグループチャレンジメッセージが送信される。ネットワークデバイスは、それぞれ２つ以上の通信デバイスのグループの１つまたは複数からグループチャレンジに対する１つまたは複数の応答メッセージを受信し、グループ内の各々の応答通信デバイスからの応答メッセージはグループに対応するグループ資格情報を備える。

【００１０】

登録方法の一環として、グループの通信デバイスは次いで、グループとして認証されてもよい。その後、登録方法の一環として、認証された通信デバイスのグループは次いで、１つまたは複数のアプリケーションについてそれぞれのデータセッションをセットアップすることができる。

【００１１】

ネットワークデバイスが、特定の実施形態に応じて通信ネットワーク内の異なるエンティティであってもよいことを理解されたい。たとえば、１つの実施形態において、ネット

ワークデバイスは、認証サーバであってもよい。別の実施形態において、ネットワークデバイスは、ゲートウェイエンティティであってもよい。さらに別の実施形態において、ネットワークデバイスは、基地局であってもよい。

【００１２】

有利なことに、本発明の登録の技法は、複数のクライアントが安全かつ効率的な方法で１つのシステムにアクセスすることができる「リバースシングルサインオン」を達成するためのフレームワークおよび手順を提供する。言い換えれば、クライアントのグループは、１つの登録手順を使用して同一システムに安全に登録することができる。これにより、クライアント登録プロセスに関連する信号伝達の大幅な減少が可能になる。さらに、例示的な実施形態において、本発明の技法の１つの重要な特徴は、クライアントまたはデバイスのグループを安全に認証するために１つの登録手順が使用されるが、登録の結果として生成されるセッション鍵はクライアントにわたって同一とならないよう保証されることである。これにより、各クライアントは、グループ内のプライバシーを危険にさらすことなく、サーバ／ネットワークと安全に通信することができる。

【００１３】

本発明の上記ならびにその他の目的、特徴、および利点は、添付の図面と併せて本発明の例示的な実施形態の以下の詳細な説明を読むことで明らかとなろう。

【図面の簡単な説明】

【００１４】

【図１】本発明の複数の実施形態による安全な登録の技法が実施されうる通信ネットワークの一部を示すブロック図である。

【図２】本発明の１つの実施形態によるネットワークフレームワークを示すブロック図である。

【図３】本発明の１つの実施形態によるゲートウェイデバイスとネットワーク間の相互の認証手順を示す流れ図である。

【図４Ａ】本発明の第１の実施形態によるグループ認証プロトコルを示す流れ図である。

【図４Ｂ】本発明の第２の実施形態によるグループ認証プロトコルを示す流れ図である。

【図４Ｃ】本発明の第３の実施形態によるグループ認証プロトコルを示す流れ図である。

【図４Ｄ】本発明の第４の実施形態によるグループ認証プロトコルを示す流れ図である。

【図５】本発明の１つの実施形態によるＩＰアドレス割り当て手順を示す流れ図である。

【図６Ａ】本発明の１つの実施形態によるグループ登録、認証、および鍵合意プロトコルを示す流れ図である。

【図６Ｂ】本発明の１つの実施形態による鍵階層を示すブロック図である。

【図６Ｃ】本発明の１つの実施形態によるサービスレイヤグループ登録プロトコルを示す流れ図である。

【図７】本発明の複数の実施形態による１つまたは複数のプロトコルを実施するための適するデータネットワークおよび通信デバイスの汎用ハードウェアアーキテクチャを示すブロック図である。

【発明を実施するための形態】

【００１５】

以下の説明は、本発明を、マシン通信（ＭＴＣ：ｍａｃｈｉｎｅ－ｔｙｐｅ－ｃｏｍｍｕｎｉｃａｔｉｏｎｓ）としても知られている、例示的なマシン間通信（Ｍ２Ｍ：ｍａｃｈｉｎｅ－ｔｏ－ｍａｃｈｉｎｅ）環境のコンテキストにおいて例示する。しかし、本発明の原理はＭ２ＭまたはＭＴＣのような環境に特に適しているが、本発明がそのような環境で使用することに限定されないことを理解されたい。つまり、本発明の原理は一般に、単一の登録手順を使用してデバイス（ユーザ）のグループの安全な登録機能を提供することが望ましい任意の通信環境に適用可能である。

【００１６】

本発明の原理との使用に特に適する通信デバイスの１つのタイプは、「オープンデバイス（ｏｐｅｎ　ｄｅｖｉｃｅ）」と呼ばれる。「オープンデバイス」という語句は一般に

、ネットワーク事業者による事前の承認なしにそのネットワーク事業者以外の任意のプロバイダからアプリケーション（たとえば、ファームウェアまたはソフトウェア）を実行することができるネットワーク内で動作する通信デバイスとして定義されうる。それらのタイプのデバイスの例は、センサー、ロケーションタグ、マシン、モニタ、およびメータを含むが、これらに限定されることはない。そのようなデバイスが使用可能にすることができるアプリケーションのタイプは、考え得る限りでは無限である。ほんの一例として、そのようなアプリケーション固有のデバイスは、ヘルスモニター、公益事業設備管理メータ、車両管理タグ、自動販売機、およびＰＯＳ（ｐｏｉｎｔ－ｏｆ－ｓａｌｅ：売り場）端末を含むことができる。

【００１７】

したがって、セルラーネットワーク事業者（ほんの一例として、Ｖｅｒｉｚｏｎ、ＡＴ＆Ｔ、またはＳｐｒｉｎｔ）により運用されるセルラーネットワークのような、公的にアクセス可能なワイドエリア通信ネットワークを介して安全に動作する、Ｍ２Ｍデバイスのような、オープンデバイスの環境は、本発明の例示的な実施形態が実施されうる環境である。

【００１８】

本発明の例示的な実施形態によれば、フレームワークおよびプロトコルは、複数のクライアントが１つのシステムにアクセスすることができる「リバースシングルサインオン」と考えられうるものを達成するために提供される。前述のように、クライアントのグループは、１つの登録手順を使用して同一システムに安全に登録することができる。これにより、以下において詳細に説明されるように、クライアント登録プロセスに関連する信号伝達の大幅な減少が可能になる。本発明のフレームワークおよびプロトコルの１つの重要な特徴は、クライアントまたはデバイスのグループを安全に認証するために１つの登録手順が使用されるが、登録の結果として生成されるセッション鍵はクライアントにわたって同一とならないよう保証されることである。これにより、各クライアントは、グループ内のプライバシーを危険にさらすことなく、サーバ／ネットワークと安全に通信することができる。既存の手法は、グループ認証の課題への対処を試みてきたが、それらは、以下で詳細に説明されるように、すべてのデバイスを同一の認証エンティティ（オーセンティケータ：ａｕｔｈｅｎｔｉｃａｔｏｒ）のグループとして認証するのではなく、デバイス（またはユーザ）がグループのメンバーであることを確認するメカニズムに重点を置いていたことに留意されたい。

【００１９】

以下の本発明の例示的な詳細にわたる説明は、Ｍ２ＭまたはＭＴＣへのアプリケーションでグループ認証および鍵合意を実行するための安全なフレームワークについて述べているが、フレームワークは、グループ登録が道理にかなうようなその他のアプリケーションに対処するために実施されてもよいことを理解されたい。一例として、ＭＴＣに適用される本発明のフレームワークにより、ＮＯ（ネットワーク事業者）および／またはＭ２ＭＯ（Ｍ２Ｍ事業者）は、グループ化ポリシーに従ってグループ分けされるデバイスのセットを認証することができるようになる。したがって、各Ｍ２Ｍデバイスを個々に認証するために、Ｍ２Ｍデバイスごとに個別のセッションを確立する必要はない。対照的に、本発明のフレームワークは、特定のグループに属するデバイスを一度に認証し、それによりかなりの程度まで認証手順の複雑さおよび帯域幅要件を軽減する。

【００２０】

参照を容易にするため、詳細な説明のこれ以降の部分は、以下のように分割される。セクションＩでは、本発明の例示的な実施形態によるグループ登録フレームワークの概略を説明する。セクションＩＩでは、本発明の例示的な実施形態に関連付けられている設計の前提を説明する。セクションＩＩＩでは、本発明の例示的な実施形態による安全なグループ登録プロトコルの詳細を説明する。セクションＩＶでは、本発明の例示的な実施形態による１つまたは複数の安全なグループ登録プロトコルを実施するための例示的なコンピューティングシステムを説明する。

【００２１】
Ｉ．　グループ登録フレームワークの概要
Ｎ個の（通信）デバイスの配置、ならびに認証エンティティ（オーセンティケータ）が、それらのデバイスの１つまたは複数のサービスへのアクセスを許可する前に、それらのデバイスの各々を認証する必要があることを検討する。既存のプロトコルでは、オーセンティケータは、個々のセッションを確立して、各デバイスと固定数の認証メッセージを交換する必要がある。したがって、配置がＮ個のデバイスを含む場合、およびオーセンティケータと各デバイス間でｋ個のメッセージが交換される必要がある場合、それらのデバイスすべてが認証されるためには、合計Ｎ＊ｋ個のメッセージが無線で伝送される必要がある。
【００２２】
一例として、Ｎ＝１００、０００とし、オーセンティケータがＡＫＡ相互認証プロトコル（それらの開示を引用により全体として本願に援用する、３ＧＰＰ　ＴＳ　３３．１０２、Ｔｅｃｈｎｉｃａｌ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ　Ｇｒｏｕｐ　Ｓｅｒｖｉｃｅｓ　ａｎｄ　Ｓｙｓｔｅｍ　Ａｓｐｅｃｔｓ；３Ｇ　Ｓｅｃｕｒｉｔｙ；Ｓｅｃｕｒｉｔｙ　Ａｒｃｈｉｔｅｃｔｕｒｅ（Ｒｅｌｅａｓｅ　９）、および３ＧＰＰ　ＴＳ　３３．４０１、Ｔｅｃｈｎｉｃａｌ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ　Ｇｒｏｕｐ　Ｓｅｒｖｉｃｅｓ　ａｎｄ　Ｓｙｓｔｅｍ　Ａｓｐｅｃｔｓ；３ＧＰＰ　Ｓｙｓｔｅｍ　Ａｒｃｈｉｔｅｃｔｕｒｅ　Ｅｖｏｌｕｔｉｏｎ（ＳＡＥ）；Ｓｅｃｕｒｉｔｙ　Ａｒｃｈｉｔｅｃｔｕｒｅ（Ｒｅｌｅａｓｅ　９）において説明されるように）を使用すると仮定する。ＡＫＡプロトコルに従って、オーセンティケータはユーザ認証要求をクライアントに送信するが、このユーザ認証要求はランダムチャレンジ（ＲＡＮＤ）および認証トークン（ＡＵＴＮ）を含み、したがってこの場合ｋ＝２である。その結果、既存の手法では、２００、０００の個々のメッセージが全体として必要となる。この全プロセスの最後に、Ｎ個のデバイスの各々はセッション鍵を生成する、すなわち、既存の手法では、合計１００、０００個のセッション鍵がオーセンティケータと各デバイス間で相互に生成されることになる。
【００２３】
１つのオーセンティケータの代わりに、異なるタイプのサービスを各々許可する複数のオーセンティケータが存在しうることに留意されたい。そのような場合、既存の手法では、すべてのデバイスは、オーセンティケータの各々と個別の認証処理を独立して保持することが必要になる。幸いなことにそのようなシナリオでは、「シングルサインオン」という概念が使用されてもよく、デバイスは（その開示内容が引用により全体として本明細書に援用される、Ｒ．Ｃｏｘ、Ｅ．ＧｒｏｓｓｅおよびＲ．Ｐｉｋｅ、「Ｓｅｃｕｒｉｔｙ　ｉｎ　Ｐｌａｎ　９」、ＵＳＥＮＩＸ、２００２年において説明されるように）資格情報の単一のセットを使用して多種多様なオーセンティケータで認証することができる。しかし、多数のクライアントが単一のオーセンティケータにより認証される必要がある場合には、個々のデバイスデータの機密性が保持される必要があるので、登録中にすべてのデバイスが異なるセキュリティ資格情報を生成する必要があり、シングルサインオンは好ましくない。
【００２４】
上記の説明を考慮して、本発明の例示的な登録の技法は、Ｎ個のデバイスのグループが単一登録手順を使用してどのように認証されうるかの問題に対処する。具体的には、この問題に対処する解決策の目標は、「リバースシングルサインオン」メカニズムを設計することであり、このメカニズムにより、Ｎ個のデバイスを「グループ」として認証し（それによりＮ個の相互セッション鍵を生成し）、同時に以下の事項に適合することができる：
（１）　個々のデバイスの認証の場合と同じセキュリティの強さを確保する。
（２）　デバイスデータが他のデバイス（たとえ同一グループに属するものであっても）から引き起こされた潜在的な攻撃に対して保護されるように、デバイスごとに個別な一意の鍵を確立する。
（３）　より少ない数の認証メッセージを使用する、好ましくは、単一認証処理の場合

と同様に多くのメッセージを同じ帯域幅を使用してオーセンティケータと交換する。

【００２５】

本明細書において説明される本発明のフレームワークおよびプロトコルは、前述の目標を達成する。この解決策の１つの実施形態において、アーキテクチャ設計の主な態様は、以下の通りである：

（１） ＧＷ（ＧａｔｅＷａｙ）と称する新しいネットワークエンティティを導入する。ＧＷはアグリゲータであり、グループに属するすべてのデバイス（本明細書において「ユーザ機器」またはＵＥとも称される）からの認証応答を収集する。通常、ＧＷは、グループのデバイスに比較的接近して配置される。

（２） グループ認証の目的で、グループのすべてのデバイスは、認証メッセージをＧＷとのみ交換する。ＧＷはさらに、グループ内の各デバイスの資格情報を確認するためにオーセンティケータとのネゴシエーションを実行する責任を負う。１つの実施形態において、フレームワークはまた、ＧＷがオーセンティケータとなることを可能にする。このために、ＧＷは、グループ内のすべてのデバイスを認証するために使用される必要な情報を受信する必要がある。この後者の実施形態が、帯域幅を節約するため、および全体として必要な信号伝達を大幅に低減するために好ましいことに留意されたい、

（３） デバイスのグループを認証するために、登録に先立ち（特にグループ鍵の）グループ資格情報がプロビジョニングされ、それらはグループ内のすべてのデバイスに対して同一である。フレームワークの設計は、異なる代替のグループ認証手順を含み、手順は各々、ネットワーク事業者のプリファレンスに基づいて適用されてパラメータ化されてもよい。選択される実際の手順に応じて、グループ資格情報は、各デバイスまたはＧＷのいずれかに提供されてもよい。グループ認証処理は、グループチャレンジに基づき、ＧＷはグループチャレンジメッセージをグループ内のすべてのデバイスにブロードキャストする。デバイスは、ＧＷへのメッセージでこのチャレンジに個別に応答する。グループ資格情報はグループ認証に使用されるが、それらの資格情報および個々の資格情報は共に、以下において説明されるように、一意の暗号および完全性保護鍵素材を生成するために各デバイスによって使用される。

（４） ＧＷとグループ内の各デバイス間の通信は、好ましくは、無認可の帯域幅（たとえば、ＺｉｇＢｅｅ、ＷｉＦｉなどに割り振られた帯域幅）を使用する。この手法により、ネットワーク事業者に割り振られる認可帯域幅を使用するアクセスネットワークとＧＷとの間に必要とされる信号伝達は、はるかに少なくなる。

【００２６】

本発明の解決策の異なる１つの実施形態において、グループ認証操作は、ＧＷがない場合に適用される。そのような場合、グループチャレンジをブロードキャストして、各デバイスから個々の応答を受信することが、基地局の責任である。ここでは、基地局が個々の一意のチャレンジを各デバイスに送信するのではなく、単に１つのメッセージをブロードキャストする必要があるので、グループ認証が引き続き有益である。しかし、チャレンジ応答はアクセスネットワーク事業者の帯域幅でデバイスにより伝送されるので、グループ認証に起因する利点は、ＧＷを使用する場合のように大きくはない。

【００２７】

有利なことに、本発明のグループ認証フレームワークが先例のないネットワークパフォーマンスの利点をもたらすことができることは明らかである。このことは、多数のデバイスが１つまたは複数のネットワークエンティティに登録する必要があるようなシナリオにおいて、特に当てはまると予想される。

【００２８】

ＩＩ． 設計の前提事項

本明細書において説明される本発明の例示的なフレームワークは、以下の前提に基づいて設計される：

（１） デバイスは、特定のポリシーに基づいてグループ化され、デバイスの属するグループ（複数可）を認識する。ポリシー作成手順およびそのようなポリシーの展開に関与

するネットワークエンティティの機能は、このフレームワーク設計の範囲を超える。言い換えれば、このフレームワークは、それに基づいてクライアントデバイスのグループが形成されるポリシーに非依存である。

（２） Ｎ個のデバイスのグループは、グループ識別子または識別情報（ＩＤ）によって表され、これはグループ認証処理に関与するすべてのネットワークエンティティに知られており、ネットワークエンティティは個々のデバイスを認証するために使用されるエンティティと同一のエンティティである。それらのエンティティはまた、そのようなグループに属するすべてのデバイスの識別情報を認識している。そのような情報は、ルックアップテーブルの形態ですべてのエンティティにローカルに格納されてもよい。エンティティがそれらのローカルに格納されたルックアップテーブルのコンテンツに関して同期されると仮定する。

（３） グループに属する各通信デバイス（以下の詳細な説明において「ユーザ機器」またはＵＥとも称される）は、無認可のスペクトル（たとえば、ＺｉｇＢｅｅ）を使用して、ローカルゲートウェイ（ＧＷ）とのワイヤレス接続を保持する。始めに、ＵＥが、登録の目的で３ＧＰＰ対応のインターフェイスを装備していないと仮定する。したがって、グループ認証および鍵合意を目的とするＵＥとネットワーク間の任意の制御またはデータトラフィックは、ＧＷを経由する。ＵＥが３ＧＰＰ（もしくは３ＧＰＰ２またはＷＩＭＡＸ）対応のインターフェイスを装備している場合、基地局はＧＷの役割を果たす。

（４） 場合によっては、ＵＥは特定の資格情報（グループ鍵と称され、以下で説明される）を事前にプロビジョニングされており、ＵＥはグループ認証中に認証および鍵素材を生成するために使用する。別の場合では、ＧＷのみがグループ鍵を認識するが、ＵＥは認識しない。

（５） ＧＷが接続される３ＧＰＰネットワークは、ＵＭＴＳ（Ｕｎｉｖｅｒｓａｌ Ｍｏｂｉｌｅ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｓｙｓｔｅｍ）ネットワークである。

（６） ＵＥグループ認証の１つの利点は、リモートアプリケーションサーバとデータセッションをさらに確立することにある。このサーバがすでに３ＧＰＰネットワークと相互に認証していると仮定する。

（７） ＵＥとＧＷ間のリンクがリンク層において保護されていると仮定する。したがって、ＵＥとＧＷ間の任意の通信は、リンク層資格情報を使用して暗号化される可能性がある。

【００２９】

図１は、そのような本発明によるフレームワークおよびプロトコルを提供するための１つのシステムを示す。通信ネットワーク１００の一部に示されるように、グループ１０２を構成する複数の通信デバイスまたはユーザ機器（ＵＥ）１０１－１、１０１－２、．．．、１０１－Ｎは、ゲートウェイデバイス（ＧＷ）１０４と称されるネットワークデバイスに動作可能に結合される。グループは、これより多くのＵＥまたはこれより少ないＵＥを含むことができる。ＧＷ１０４は、Ｎｏｄｅ Ｂ１０６と称される基地局およびアプリケーションサーバ１０８に動作可能に結合される。知られているように、Ｎｏｄｅ Ｂは、ＵＭＴＳの用語による基地局であり、ＧＳＭ（Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ）の用語で使用されるＢＴＳ（送受信基地局：ｂａｓｅ ｔｒａｎｓｃｅｉｖｅｒ ｓｔａｔｉｏｎ）と等価である。したがって、ネットワーク要素１０６は、Ｎｏｄｅ ＢまたはＢＴＳ、もしくはアクセスされる通信ネットワークに応じた任意の形態の基地局であってもよい。ＵＥが携帯電話であるアプリケーションにおいて、Ｎｏｄｅ Ｂは、携帯電話ネットワークに接続され、通常携帯ハンドセットと直接通信するネットワークデバイスである。しかし、図１の実施形態において、ＧＷ１０４は、ＵＥと直接通信する。Ｎｏｄｅ Ｂは通常、エアインターフェイス技術としてＷＣＤＭＡ（登録商標）／ＴＤ－ＳＣＤＭＡ（広帯域符号分割多元接続／時分割同期符号分割多元接続：Ｗｉｄｅｂａｎｄ Ｃｏｄｅ Ｄｉｖｉｓｉｏｎ Ｍｕｌｔｉｐｌｅ Ａｃｃｅｓｓ／Ｔｉｍｅ Ｄｉｖｉｓｉｏｎ Ｓｙｎｃｈｒｏｎｏｕｓ Ｃｏｄｅ Ｄ

ｉｖｉｓｉｏｎ Ｍｕｌｔｉｐｌｅ Ａｃｃｅｓｓ）を使用する。
【００３０】
Ｎｏｄｅ Ｂ１０６は、サービス提供ＧＰＲＳサポートノード（ＳＧＳＮ：Ｓｅｒｖｉｎｇ ＧＰＲＳ Ｓｕｐｐｏｒｔ Ｎｏｄｅ）１１０に動作可能に結合される。ＳＧＳＮは、汎用パケット無線サービス（ＧＰＲＳ：Ｇｅｎｅｒａｌ Ｐａｃｋｅｔ Ｒａｄｉｏ Ｓｅｒｖｉｃｅ）ネットワークの主コンポーネントであり、通常は、たとえばモビリティ管理およびユーザの認証など、ネットワーク内のすべてのパケット交換データを処理する。しかし、以下で説明されるように、認証はＧＷ１０４に従って実行される。
【００３１】
ＳＧＳＮ１１０は、ホームロケーションレジスタ（ＨＬＲ：Ｈｏｍｅ Ｌｏｃａｔｉｏｎ Ｒｅｇｉｓｔｅｒ）としても知られているホーム加入者サーバ（ＨＳＳ：Ｈｏｍｅ Ｓｕｂｓｃｒｉｂｅｒ Ｓｅｒｖｅｒ）１１２に動作可能に結合される。ＨＳＳ１１２は、移動加入者（ユーザ）からの情報が格納されるデータベースである。ＨＳＳは通常、加入者の識別情報に関する情報、電話番号、関連サービス、および加入者の位置に関する一般情報を含む。加入者の正確な位置は、通常ビジターロケーションレジスタ（ＶＬＲ：Ｖｉｓｉｔｏｒ Ｌｏｃａｔｉｏｎ Ｒｅｇｉｓｔｅｒ、図示せず）に保持される。
【００３２】
ＩＩＩ． グループ認証フレームワークおよびアプリケーション
本発明の１つの実施形態によれば、グループ認証フレームワークは、５つの主要ネットワークフレームワークモジュールから成る。本明細書において使用される「モジュール」という用語は、図１に示されるネットワークコンポーネント（すなわち、ＵＥ１０１、ＧＷ１０４、Ｎｏｄｅ Ｂ１０６、アプリケーションサーバ１０８、ＳＧＳＮ１１０、およびＨＳＳ１１２）の１つまたは複数に従って実行される主要機能を指すことが意図されることを理解されたい。図２は、ネットワークフレームワーク２００のモジュールを示す。ネットワークフレームワークモジュールの各々はさらに、以下のサブセクションＡからＥにおいてそれぞれ説明される。
【００３３】
示されているように、３ＧＰＰネットワークによるＧＷ登録、およびＭ２Ｍアプリケーションサーバによる接続確立のためのフレームワークモジュール２０２（以下のサブセクションＡにおいて説明される）が提供される。
【００３４】
次の認証に関してＵＥのグループに通知するためのフレームワークモジュール２０４（以下のサブセクションＢにおいて説明される）が提供される。
【００３５】
グループ認証プロトコル動作を実行するフレームワークモジュール２０６（以下のサブセクションＣにおいて説明される）が提供される。
【００３６】
ＩＰ（インターネットプロトコル）アドレスをグループに属するＵＥに提供するフレームワークモジュール２０８（以下のサブセクションＤにおいて説明される）が提供される。
【００３７】
３ＧＰＰネットワークによるグループ認証が正常に完了した後、Ｍ２Ｍアプリケーションサーバ（図１の１０８）にデバイスのグループを登録するためのフレームワークモジュール２１０（以下のサブセクションＥにおいて説明される）が提供される。
【００３８】
次いで、例示的な実施形態において、図２の各フレームワークモジュールの機能の一部が、図１のネットワークコンポーネントのうちの２つまたはそれ以上において実行されることを理解されたい。このことは、各々のサブセクションＡからＥにおける説明から明らかとなろう。しかし、また、本発明が、以下において例示的に説明されるモジュール機能の分散に限定されることを意図するものではないことも理解されたい。むしろ、１つのコ

ンポーネントで実行されるように示される１つの機能は、たとえばＳＧＳＮ１１０で実行されるように示されるフレームワークモジュールの機能が代替としてＧＷ１０４で実行されてもよい、というように、代替として別のコンポーネントで実行されてもよい。

【００３９】

これ以降、例示的なグループ認証フレームワークのモジュラー設計を詳細に示す。説明を分かりやすくするため、特定数（Ｎ）のＭ２Ｍデバイスの配置を仮定する（その開示内容が引用により全体として本明細書に援用される、３ＧＰＰ　ＴＳ　２２．３６８、Ｔｅｃｈｎｉｃａｌ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ　Ｇｒｏｕｐ　Ｓｅｒｖｉｃｅｓ　ａｎｄ　Ｓｙｓｔｅｍ　Ａｓｐｅｃｔｓ；Ｓｅｒｖｉｃｅ　Ｒｅｑｕｉｒｅｍｅｎｔｓ　ｆｏｒ　Ｍａｃｈｉｎｅ　Ｔｙｐｅ　Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ（ＭＴＣ）；Ｓｔａｇｅ　１（Ｒｅｌｅａｓｅ　１０）において説明されるように）。上記の説明に沿って、ＮＯ（ネットワーク事業者）および／またはＭ２ＭＯ（Ｍ２Ｍ事業者）は、グループ化ポリシーに従ってグループ分けされるＮ個のＭ２Ｍデバイスのセットを認証することができるようになる。したがって、各Ｍ２Ｍデバイスを個々に認証するために、Ｍ２Ｍデバイスごとに個別のセッションを確立する必要はない。対照的に、本発明のフレームワークは、特定のグループに属するＭ２Ｍデバイスを一度に認証し、それによりかなりの程度まで認証手順の複雑さおよび帯域幅要件を軽減する。本発明のフレームワークの５つの主要モジュールの各々について、以下のサブセクションＡからＥにおいてそれぞれ説明する。

【００４０】

Ａ．　ＧＷと３ＧＰＰネットワーク間の相互認証（図２のフレームワークモジュール２０２）

ＵＥ１０１－１、１０１－２、．．．、１０１－Ｎを認証する前に、ＧＷ１０４が最初に認証される必要がある。加えて、ＧＷは、ネットワークも信頼できることを確認する必要がある。「ネットワーク」という用語は本明細書において、ゲートウェイがＵＥのアクセスポイントとしての機能を果たすＵＭＴＳネットワーク（３ＧＰＰ）を意味する（たとえば、Ｎｏｄｅ　Ｂ１０６、アプリケーションサーバ１０８、ＳＧＳＮ１１０、ＨＳＳ１１２など）。この認証のために、１つの実施形態において、認証および鍵合意（ＡＫＡ：Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　Ｋｅｙ　Ａｇｒｅｅｍｅｎｔ）手順が採用される。たとえば、ＵＭＴＳネットワークが考慮される限りは、ＧＷ１０４を３ＧＰＰクライアントＵＥとして処理して、開示を引用により全体として本願に援用する３ＧＰＰ　ＴＳ　３３．１０２において説明されるＡＫＡ手順が採用されてもよい。

【００４１】

図３は、このＧＷおよび３ＧＰＰネットワークの相互認証手順のステップを示す。示されているように、相互認証手順３００は、以下のステップを含む：

１．　ＧＷ１０４は、登録要求をＳＧＳＮ１１０に送信する（ステップ３０２）。

２．　ＳＧＳＮ１１０は、ＧＷ１０４に代わって認証要求をＨＳＳ１１２に送信する（ステップ３０４）。

３．　ＨＳＳ１１２は、１つまたは複数の認証ベクトルを含む認証応答をＳＧＳＮ１１０に送信する（ステップ３０６）。

４．　ＳＧＳＮ１１０は、ベクトルの１つを使用して、乱数ＲＡＮＤおよび認証トークンＡＵＴＮを含むチャレンジをＧＷ１０４に送信する（ステップ３０８）。

５．　ＧＷ１０４は、チャレンジを受信して、ＡＵＴＨを確認し、成功すると応答ＲＥＳをＳＧＳＮ１１０に送信する（ステップ３１０）。

６．　ＳＧＳＮ１１０は、ＲＥＳを受信して、ＲＥＳを、使用される特定の認証ベクトルに含まれているＸＲＥＳと比較する（ステップ３１２）。

７．　ＲＥＳ＝ＸＲＥＳである場合、ＧＷ１０４はその正統性を確認され、ＳＧＳＮ１１０は、認証結果をＧＷ１０４に送信し、確認の成功についてＧＷ１０４に知らせる（ステップ３１４）。

８．　ＧＷ１０４は、ＡＵＴＮを使用して、３ＧＰＰ　ＴＳ　３３．１０２に従って、ネットワークを認証する（ステップ３１６）。

【００４２】
ＳＧＳＮ１１０がＸＲＥＳ＝ＲＥＳであると仮定し、ＧＷ１０４もまたＡＵＴＮの正統性を確認すると仮定すると、このプロセスの最後に、３ＧＰＰ　ＴＳ３３．１０２に従って、相互認証が成功したと見なされ、ＧＷ１０４およびＲＡＮＤとの両方によりサポートされる暗号化アルゴリズムを使用して、暗号鍵（CK_i）および完全性鍵（IK_i）が生成され、後続のパケット交換を暗号化および完全性保護するために使用される。加えて、ＧＷ１０４が正常に認証されることを所与として、ＰＤＰ（パケットデータプロトコル：Ｐａｃｋｅｔ　Ｄａｔａ　Ｐｒｏｔｏｃｏｌ）コンテキストはＧＷ１０４とＧＧＳＮ／ＳＧＳＮ１１０間で確立され、それによりＧＷ１０４はリモートＭ２Ｍアプリケーションサーバ１０８との（潜在的に安全な）セッションを確立することができる。そのようなセッションが確立される１つの手段は、以下において説明される。

【００４３】
Ｂ．　次の認証に関してＵＥのグループを通知する（図２のフレームワークモジュール２０４）
（図１におけるような）Ｍ２Ｍデバイス１０１－１、１０１－２、．．．、１０１－Ｎのグループ１０２が認証されるために、グループのすべてのデバイスは、同時にアクティブ（アライブ）である必要がある、すなわちＧＷ１０４とアクティブな接続を保持する必要がある。しかし、各デバイスのアプリケーションおよびソフトウェア構成に応じて、グループ内の一部のデバイスがスリープモードにある可能性もある。たとえば、一部のＭ２Ｍアプリケーション（スマートメータアプリケーションなど）では、Ｍ２Ｍデバイスが所定の時間間隔でウェイクアップして、Ｍ２Ｍアプリケーションサーバ１０８への接続を確立し、それらのデータをアップロードすることを必要とする。そのようなデバイスのグループを認証するため、グループのすべてのデバイスがアライブ状態である必要がある。本発明のフレームワークは、認証のためにグループのデバイスを「準備させる」４つの例示的な手段を提供する。以下のサブセクションにおいて、それらの手段について説明する。ＧＷ１０４とＵＥ１０１－１、１０１－２、．．．、１０１－Ｎ間を通過するメッセージが、以下で説明されるように、図１のＵＥとＧＷを接続することが示されるリンクを介して渡されることを理解されたい。

【００４４】
Ｂ１．　Ｍ２Ｍアプリケーションサーバ発信の「ウェイクアップ」信号伝達
この手法により、Ｍ２Ｍアプリケーションサーバ１０８またはＨＳＳ１１２は、特殊な「ウェイクアップ」（アクティブ化）メッセージをＧＷ１０４に通信する。このウェイクアップメッセージは、認証されるべきグループのＩＤを含む。ＧＷ１０４は、このメッセージを受信すると直ちに、そのローカルに格納されているルックアップテーブルを使用して、特定のグループに属するＵＥのセットを導き出す。その後、ＧＷ１０４は、ブロードキャストメッセージ（たとえば、ＺｉｇＢｅｅメッセージ）を、特定のＩＤを持つグループのデバイスのすべてに伝送する。

【００４５】
本発明の原理は任意の特定の通信規格を使用することに限定されないが、本明細書において説明される一部の例示的な実施形態において、使用される通信規格はＺｉｇＢｅｅ規格であることを理解されたい。知られているように、ＺｉｇＢｅｅは、ＩＥＥＥ８０２．１５．４－２００３規格に基づく小型の低電力の通信デバイスを使用する高水準通信プロトコルのスイート向けの仕様である。用語は、ＺｉｇＢｅｅ仕様（２００６年バージョン）により定義され、その開示は引用により全体として本明細書において援用する。ＺｉｇＢｅｅ　Ａｌｌｉａｎｃｅは、ＺｉｇＢｅｅ規格を保持し公開する企業のグループである（ｈｔｔｐ：／／ｗｗｗ．ｚｉｇｂｅｅ．ｏｒｇを参照）。

【００４６】
ＵＥは、このメッセージを受信すると直ちに、それが特定のグループの一部であるかどうかを決定する。グループの一部である場合、ＧＷ１０４との接続（たとえば、ＺｉｇＢｅｅ接続）をさらに確立（または復元）する。このプロセスの最後に、グループのすべて

のデバイスは認証処理に参加できる状態になり、共通暗号鍵（たとえば、ＺｉｇＢｅｅ鍵K_{ZB}）が確立される。

【００４７】

Ｂ２．　所定の時間間隔でスケジュールされる登録

ウェイクアップメッセージを使用してデバイス（１０１－１、１０１－２、．．．、１０１－Ｎ）のグループに通知する代わりに、デバイスは、認証処理に参加するために特定の時間間隔で（自発的に）ウェイクアップするようにスケジュールされてもよい。そのような手順には、デバイスとＧＷ１０４との間で緩い時間同期化が必要となる。スケジュールされるウェイクアップの時間は、製造時において事前にプロビジョニングされるか、または無線によりプロビジョニングされてもよい。ＵＥは、ウェイクアップすると直ちに、前述のサブセクションＢ１において説明されるように、ＧＷとのＺｉｇＢｅｅ接続を確立する。そのような手順により、グループは、ＵＥとＭ２Ｍアプリケーションサーバ１０８との間にトラフィックがほとんどないか、または全くないときに認証されてもよいことに留意されたい。したがって、ＵＥのグループが認証され、それらのＩＰアドレスを割り当てられる限りにおいて、ＵＥのグループはスリープモードに戻ることができ、ウェイクアップしたとき、ＵＥのグループはそれらの割り当てられているＩＰアドレスを使用してＭ２Ｍアプリケーションサーバ１０８へのデータ接続を確立することができる。

【００４８】

Ｂ３．　ＧＷにおける認証素材のキャッシング

上記の２つの手法は、すべてのＵＥが一度にウェイクアップし、ＧＷとのＺｉｇＢｅｅ接続を同時に確立することを規定する。しかし、そのような手順は、特にグループが多数のＵＥで構成されるような場合（センサーネットワーク配置の場合など）、各ＵＥ１０１とＧＷ１０４との間のリンクに特別な制御信号伝達のオーバーヘッドを課す。（同一グループに属す）多数のＭ２Ｍデバイスがそれらのデータをサーバ（ＧＷ１０４）に送信することをＭ２Ｍサーバが要求するようなシナリオにおいて、そのようなデバイスは同時にそろってウェイクアップするようにスケジュールされるのではなく、それらのスケジュールに何らかの遅延を伴うことになることが予想される。そのため、ＧＷ１０４は過負荷状態にはならない。一方、グループを認証するために、グループに属するすべてのデバイスがアライブ状態である必要があることに再度言及する。このため、このフレームワークは、ＧＷ１０４において認証素材をキャッシュに入れるオプションを提供する。特に、グループ１０２からの第１のＵＥ１０１がウェイクアップして、（グループ認証の目的のため）ＧＷ１０４とのＺｉｇＢｅｅ接続を確立すると直ちに、ＧＷ１０４はコアネットワークに認証素材を要求する（この手順は以下のサブセクションＣにおいて説明される）。加えて、ＧＷ１０４は、グループ認証処理が開始されうるように、グループのすべてのＵＥがアライブ状態になるまでこの素材をキャッシュに入れる。キャッシュに入れられたパラメータ（Ｇ＿ＡＵＴＮおよびＧ＿ＲＡＮＤ）ならびにこれらがＧＷ１０４により使用される手段は、以下のサブセクションＣにおいて説明される。

【００４９】

Ｂ４．　認証素材のキャッシングおよびＧＷにおけるローカルなグループ認証

このフレームワークはまた、ＧＷ１０４が意図されるデバイスのグループを認証するためのメカニズムを、ＧＷがそのようなタスクを実行できる限りにおいて提供する。言い換えれば、ＧＷ１０４はこれ以降、（ｉ）デバイスのグループが正統であることを確認すること、および（ｉｉ）認証の結果を３ＧＰＰコアネットワークエンティティ（Ｎｏｄｅ Ｂ１０６、ＳＧＳＮ１１０、ＨＳＳ１１２など）、およびＭ２Ｍアプリケーションサーバ１０８にレポートすることに責任を負うことになる。同様に、サブセクションＢ３において上記で説明されるように、ＧＷ１０４は、認証パラメータのセットを受信してキャッシュに入れる。しかし、ここでＧＷ１０４は、認証処理をローカルに実行するために、追加のパラメータ（Ｇ＿ＸＲＥＳと呼ばれる）をキャッシュに入れる必要がある。そのようなプロセスがどのように実行されるのかを、以下のサブセクションにおいて説明する。

【００５０】

Ｃ．　グループ認証プロトコル（図２のフレームワークモジュール２０６）
　グループ認証プロトコルは、対象となるグループ内のすべてのＵＥがアライブ状態であり、アクティブなＺｉｇＢｅｅセッションを確立していることをＧＷ１０４が確認すると、直ちに開始される。以下において、このプロトコルの５つの例示的な実施形態を提示する。
【００５１】
　Ｃ１．　ＳＧＳＮがグループ内のデバイスの正統性を確認する
　この手法は、図４Ａに示される。プロトコル４００により、ＧＷ１０４は、グループのすべてのデバイスから認証応答を収集して、それらの応答を確認のためにＳＧＳＮ１１０に転送する。特に、プロトコルのステップは以下のとおりである：
　１．　ＧＷ１０４は、グループ登録要求をＳＧＳＮ１１０に送信する（ステップ４０２）。
　２．　ＳＧＳＮ１１０は、この要求をＨＳＳ１１２に転送する（ステップ４０４）。
　３．　ＨＳＳ１１２は、１つまたは複数の「グループベクトル」Ｖを生成して、ＳＧＳＮ１１０に送信する（ステップ４０６）。そのようなベクトルは、以下のような形態をとる。
$V = \{G\_AUTN, G\_RAND, [XRES_1, CK_1, IK_1], [XRES_2, CK_2, IK_2], \ldots, [XRES_N, CK_N, IK_N]\}$
これらのパラメータは、３ＧＰＰ　ＴＳ　３３．１０２の場合と同様に定義される。
　４．　ＳＧＳＮ１１０は、Ｇ＿ＲＡＮＤおよびＧ＿ＡＵＴＮを含むグループ認証応答をＧＷ１０４に送信する（ステップ４０８）。ＧＷ１０４が、上記のセクションＢ３およびＢ４で説明されるように、Ｇ＿ＲＡＮＤおよびＧ＿ＡＵＴＮをキャッシュに入れることができることに留意されたい。
　５．　ＧＷ１０４は、「グループ鍵」K_Gを使用して作成されたＧ＿ＡＵＴＮを確認する（ステップ４１０）。この鍵は、ＵＥには知られておらず、すでにＧＷに提供されている。
　６．　ＧＷ１０４は、Ｇ＿ＲＡＮＤを含むＺｉｇＢｅｅブロードキャストメッセージをＵＥに送信する（ステップ４１２）。このメッセージは、上記で言及したＺｉｇＢｅｅ規格に従って、K_{ZB}で暗号化される。
　７．　各ＵＥ１０１は、このメッセージを受信し、RES_iを計算して、このRES_iをＧＷ１０４に送信する（ステップ４１４）。
　８．　ＧＷ１０４は、すべてのRES_i応答をＵＥ１０１から収集して、それらをＳＧＳＮ１１０に送信する（ステップ４１６）。ここで、ＧＷ１０４は、ＵＥ１０１からの個々の応答を転送するか、またはより少ない、より大きいメッセージにその応答を集約してＳＧＳＮ１１０に転送することができる。
　９．　ＳＧＳＮ１１０はグループベクトルを使用して各応答を確認し、次いでＳＧＳＮ１１０は、グループ認証結果をＧＷ１０４に送信する（ステップ４１８）。このメッセージは、各ＵＥの認証結果を含む。
　１０．　すべてのＵＥ１０１が正常に認証された場合、ＧＷ１０４は単に「成功」メッセージをすべてのＵＥにブロードキャストする。それ以外の場合、ＧＷ１０４は、（ｉ）どのＵＥが正常に認証されたかに関する情報を含む成功メッセージをブロードキャストする、および（ｉｉ）どのＵＥが確認されなかったかに関する情報を含むエラーメッセージを、失敗の原因と共にブロードキャストする（ステップ４２０）。あるいは、「成功」メッセージは省略されてもよく、正常に認証されたＵＥ１０１は、それらのＩＤがエラーブロードキャストメッセージに含まれているかどうかを検査することにより、認証の成功を認識することができる。各ＵＥ１０１は、ブロードキャストメッセージの受信をＧＷ１０４に個々に通知し、ＧＷ１０４は共通の確認応答メッセージをＳＧＳＮ１１０に転送する。
　１１．　正常に認証されたＵＥ１０１は、個々のK_i鍵を使用して、CK_iおよびIK_i鍵を計算する（ステップ４２２）（３ＧＰＰ　ＴＳ　３３．１０２を参照）。

【００５２】
Ｃ２．　ＨＳＳがグループ内のデバイスの正統性を確認する
この手法は、図４Ｂに示される。ＨＳＳ１１２が、上記のサブセクションＣ１のステップ９に従って、ＵＥ１０１の応答を確認するために認証ベクトル（複数可）をＳＧＳＮ１１０に提供する代わりに、ＨＳＳ１１２は代替として、$ＲＥＳ_i$応答の確認を実行することができる。この場合、ＳＧＳＮ１１０は、［$ＸＲＥＳ_1$，$ＣＫ_1$，$ＩＫ_1$］を認識している必要はない。この場合明らかなように、ＧＷ１０４は、ＳＧＳＮ１１０を通じて、ＵＥ１０１からＨＳＳ１１２に$ＲＥＳ_i$応答を送信する。さらに具体的には、この場合のプロトコル４３０のステップは以下のとおりである：
１．　ＧＷ１０４は、グループ登録要求をＳＧＳＮ１１０に送信する（ステップ４３２）。
２．　ＳＧＳＮ１１０は、この要求をＨＳＳ１１２に転送する（ステップ４３４）。
３．　ＨＳＳ１１２は、「グループベクトル」ＶをＳＧＳＮ１１０に送信する（ステップ４３６）。このベクトルは、Ｖ＝｛Ｇ＿ＡＵＴＮ，Ｇ＿ＲＡＮＤ｝の形態をとる。これらのパラメータは、３ＧＰＰ　ＴＳ　３３．１０２の場合と同様に定義される。
４．　ＳＧＳＮ１１０は、Ｇ＿ＲＡＮＤおよびＧ＿ＡＵＴＮを含むグループ認証応答をＧＷ１０４に送信する（ステップ４３８）。ＧＷ１０４が、上記のセクションＢ３およびＢ４で説明されるように、Ｇ＿ＲＡＮＤおよびＧ＿ＡＵＴＮをキャッシュに入れることができることに留意されたい。
５．　ＧＷ１０４は、「グループ鍵」$Ｋ_G$を使用して作成されたＧ＿ＡＵＴＮを確認する（ステップ４４０）。この鍵は、ＵＥには知られておらず、すでにＧＷに提供されている。
６．　ＧＷ１０４は、Ｇ＿ＲＡＮＤを含むＺｉｇＢｅｅブロードキャストメッセージをＵＥ１０１に送信する（ステップ４４２）。このメッセージは、ＺｉｇＢｅｅ規格に従って、$Ｋ_{ＺＢ}$で暗号化される。
７．　各ＵＥ１０１は、このメッセージを受信し、$ＲＥＳ_i$を計算して、この$ＲＥＳ_i$をＧＷ１０４に送信する（ステップ４４４）。
８．　ＧＷ１０４は、すべての$ＲＥＳ_i$応答をＵＥ１０１から収集して、それらをＳＧＳＮ１１０に送信する（ステップ４４６）。ここで、ＧＷ１０４は、ＵＥ１０１からの個々の応答を転送するか、またあるいはより少ない、より大きいメッセージにその応答を集約してＳＧＳＮ１１０に転送することができる。
９．　ＳＧＳＮ１１０は、これらの応答をＨＳＳ１１２に転送する（ステップ４４８）。
１０．　ＨＳＳ１１２は各応答を確認するために選択されたグループベクトルを使用し、次いで、ＨＳＳ１１２はグループ認証結果をＳＧＳＮ１１０に送信し、ＳＧＳＮ１１０はこのメッセージをさらにＧＷ１０４に転送する（ステップ４５０）。このメッセージは、各ＵＥ１０１の認証結果を含む。
１１．　すべてのＵＥ１０１が正常に認証された場合、ＧＷ１０４は単に「成功」メッセージをすべてのＵＥ１０１にブロードキャストする。それ以外の場合、ＧＷ１０４は、（ｉ）どのＵＥが正常に認証されたかに関する情報を含む成功メッセージをブロードキャストする、および（ｉｉ）どのＵＥが確認されなかったかに関する情報を含むエラーメッセージを、失敗の原因と共にブロードキャストする（ステップ４５２）。あるいは、「成功」メッセージは省略されてもよく、正常に認証されたＵＥ１０１は、それらのＩＤがエラーブロードキャストメッセージに含まれているかどうかを検査することにより、認証の成功を認識することができる。各ＵＥ１０１は、ブロードキャストメッセージの受信をＧＷ１０４に個々に通知し、ＧＷ１０４は共通の確認応答メッセージをＨＳＳ１１２に転送する。
１２．　正常に認証されたＵＥ１０１は、個々の$Ｋ_i$鍵を使用して、$ＣＫ_i$および$ＩＫ_i$鍵を計算する（ステップ４５４）（３ＧＰＰ　ＴＳ　３３．１０２を参照）。
【００５３】

Ｃ３．　ＵＥはグループ鍵を認識するが、ＧＷはグループ鍵を認識せず、ＳＧＳＮはグループ内のデバイスの正統性を確認する。

【００５４】

手順Ｃ１およびＣ２は、ＧＷ１０４が個々のＲＥＳ$_i$値をＳＧＳＮ１１０（Ｃ１により）またはＨＳＳ１１２（Ｃ２により）にも送信する必要があるので、オーバーヘッドが増大する。（数千のデバイスがＧＷと通信しうる可能性もあるセンサーの場合のように）グループが多数のデバイスから成るシナリオにおいて、ＧＷと３ＧＰＰネットワーク間のリンクは過剰に使用されることになる。代替のプロトコル４６０は、図４Ｃにおいて説明される。ここでは、すべてのＵＥが共通のＫ$_G$鍵を認識すると仮定される。

【００５５】

１．　ＧＷ１０４は、グループ登録要求をＳＧＳＮ１１０に送信する（ステップ４６２）。

２．　ＳＧＳＮ１１０は、この要求をＨＳＳ１１２に転送する（ステップ４６４）。

３．　ＨＳＳ１１２は、１つまたは複数の「グループベクトル」を生成して、ＳＧＳＮ１１０に送信する（ステップ４６６）。そのようなベクトルは、以下のような形態をとる：

Ｖ＝｛Ｇ＿ＡＵＴＮ，Ｇ＿ＲＡＮＤ，Ｇ＿ＸＲＥＳ，［ＭＴＣ＿ＣＫ$_1$，ＭＴＣ＿ＩＫ$_1$］，．．．，［ＭＴＣ＿ＣＫ$_N$，ＭＴＣ＿ＩＫ$_N$］｝

４．　ＳＧＳＮ１１０は、Ｇ＿ＲＡＮＤおよびＧ＿ＡＵＴＮを含むグループ認証応答をＧＷ１０４に送信する（ステップ４６８）。ＧＷ１０４が、上記のセクションＢ３およびＢ４で説明されるように、Ｇ＿ＲＡＮＤおよびＧ＿ＡＵＴＮをキャッシュに入れることができることに留意されたい。

５．　ＧＷ１０４は、Ｇ＿ＡＵＴＮおよびＧ＿ＲＡＮＤを含むＺｉｇＢｅｅブロードキャストメッセージをすべてのＵＥ１０１に送信する（ステップ４７０）。この場合、Ｋ$_G$を提供されていないので、ＧＷがＧ＿ＡＵＴＮを確認できないことに留意されたい。

６．　各ＵＥ１０１は、個々にＧ＿ＡＵＴＮを確認する（ステップ４７２）。

７．　各ＵＥ１０１は、Ｇ＿ＲＥＳを含むメッセージで応答する（ステップ４７４）。Ｇ＿ＲＥＳの値は、提供されたＫ$_G$鍵を使用して計算される。この鍵はＵＥ１０１およびＨＳＳ１１２にのみ知られており、ＧＷ１０４には知られていないことを再度言及する。また、各ＵＥ１０１が同じＧ＿ＲＡＮＤを受信し、Ｋ$_G$を有するので、各正規のＵＥ１０１はＧ＿ＲＥＳの同じ値を計算すべきであることにも留意されたい。

８．　ＧＷ１０４は、ＵＥ１０１からの応答をＳＧＳＮ１１０に送信する（ステップ４７６）。明らかに、このメッセージは、ＧＷ１０４が同じＧ＿ＲＥＳ値を提供したＵＥ識別情報をグループ化できるので、Ｃ１およびＣ２の場合よりもはるかに少ない帯域幅を占有するものと予想される。

９．　ＳＧＳＮ１１０はグループベクトルを使用して応答を確認し、すべてのＧ＿ＲＥＳ値について、ＳＧＳＮ１１０は、Ｇ＿ＲＥＳ＝Ｇ＿ＸＲＥＳであるかどうかを検査する。その後、ＳＧＳＮ１１０は、グループ認証結果をＧＷ１０４に送信する（ステップ４７８）。

１０．　ＧＷ１０４は、認証の結果を各ＵＥ１０１に知らせる（ステップ４８０）。すべてのＵＥ１０１が正常に認証された場合、ＧＷ１０４は単に「成功」メッセージをすべてのＵＥ１０１にブロードキャストする。それ以外の場合、ＧＷ１０４は、（ｉ）どのＵＥ１０１が正常に認証されたかに関する情報を含む成功メッセージをブロードキャストする、および（ｉｉ）どのＵＥ１０１が確認されなかったかに関する情報を含むエラーメッセージを、失敗の原因と共にブロードキャストする。あるいは、「成功」メッセージは省略されてもよく、正常に認証されたＵＥ１０１は、それらのＩＤがエラーブロードキャストメッセージに含まれているかどうかを検査することにより、認証の成功を認識することができる。各ＵＥ１０１は、ブロードキャストメッセージの受信をＧＷ１０４に個々に通知し、ＧＷ１０４は共通の確認応答メッセージをＳＧＳＮ１１０に転送する。

１１．　正常に認証された各ＵＥ１０１は、個々のＫ$_i$鍵（Ｋ$_G$とは異なる）を使用し

て、CK_iおよびIK_i鍵を計算し、加えて、MTC_CK_iおよびMTC_IK_iが以下のように計算される（ステップ４８２）：

$MTC\_CK_i = CK_i \ XOR \ CK_G$

$MTC\_IK_i = IK_i \ XOR \ IK_G$

ただし、

$CK_G = f_3(K_G, G\_RAND)$，$IK_G = f_4(K_G, G\_RAND)$

$CK_i = f_3(K_i, G\_RAND)$，$IK_i = f_4(K_i, G\_RAND)$

サブセクションＣ２の場合と同様に、ＨＳＳ１１２は、このタスクをＳＧＳＮ１１０に割り当てるのではなく、ＵＥの応答を確認することを決定することができる。この場合、Ｇ＿ＡＵＴＮおよびＧ＿ＲＡＮＤのみが、サブセクションＣ２に従って、ＳＧＳＮ１１０に送信される。

【００５６】

Ｃ４．　ＧＷがグループ内のデバイスの正統性を確認し、結果をレポートする。

グループ認証プロトコルの帯域幅要件をさらに低減するため、３ＧＰＰネットワークは、グループの正統性の確認をＧＷ１０４に割り当てることができる。ＧＷ１０４は、そのようなタスクを実行できるようにするため、ＵＥ１０１からの応答が正しく計算されたＧ＿ＲＥＳ値を含むかどうかを検査できる必要がある。したがって、ＧＷ１０４は、すでにＧ＿ＸＲＥＳパラメータを含む認証ベクトルを受信する必要がある。上記のＣ３の場合と同様に、ここでは、すべてのＵＥ１０１が共通のK_G鍵を認識すると仮定される。さらに具体的には、この場合のプロトコル４８５のステップは図４Ｄに示され、以下のとおりである：

１．　ＧＷ１０４は、グループ登録要求をＳＧＳＮ１１０に送信する（ステップ４８６）。

２．　ＳＧＳＮ１１０は、この要求をＨＳＳ１１２に転送する（ステップ４８８）。

３．　ＨＳＳ１１２は、１つまたは複数の「グループベクトル」を生成して、ＳＧＳＮ１１０に送信する（ステップ４９０）。そのようなベクトルは、以下のような形態をとる：

$V = \{G\_AUTN, G\_RAND, G\_XRES, [MTC\_CK_1, MTC\_IK_1], \ldots, [MTC\_CK_N, MTC\_IK_N]\}$

４．　ＳＧＳＮ１１０は、Ｇ＿ＲＡＮＤ、Ｇ＿ＡＵＴＮ、およびＧ＿ＸＲＥＳを含むグループ認証応答をＧＷに送信する（ステップ４９１）。ＧＷ１０４が、上記のセクションＢ３およびＢ４で説明されるように、それらのパラメータをキャッシュに入れることができることに留意されたい。

５．　ＧＷ１０４は、Ｇ＿ＡＵＴＮおよびＧ＿ＲＡＮＤを含むＺｉｇＢｅｅブロードキャストメッセージをすべてのＵＥ１０１に送信する（ステップ４９２）。この場合、K_Gをプロビジョニングされていないので、ＧＷ１０４がＧ＿ＡＵＴＮを確認できないことに留意されたい。

６．　各ＵＥ１０１は、個々にＧ＿ＡＵＴＮを確認する（ステップ４９３）。

７．　各ＵＥ１０１は、Ｇ＿ＲＥＳを含むメッセージで応答する（ステップ４９４）。Ｇ＿ＲＥＳの値は、プロビジョニングされたK_G鍵を使用して計算される。この鍵はＵＥ１０１およびＨＳＳ１１２にのみ知られており、ＧＷ１１０には知られていないことを再度言及する。また、各ＵＥ１０１が同じＧ＿ＲＡＮＤを受信し、K_Gを有するので、各正規のＵＥ１０１はＧ＿ＲＥＳの同じ値を計算すべきであることにも留意されたい。

８．　ＧＷ１０４は、すべての受信したＧ＿ＲＥＳを、ローカルに格納されているＧ＿ＸＲＥＳと比較する。さらに、ＧＷ１０４は、正常に認証されたＵＥ１０１のリスト、および正常に認証されなかったＵＥ１０１のリストをコンパイルする（ステップ４９５）。

９．　ＧＷ１０４は、２つのリストをＳＧＳＮ１１０に送信する（ステップ４９６）。明らかに、このメッセージは、ＧＷによって配信された２つのリストのサイズが小さくなっているので、Ｃ１、Ｃ２、およびＣ３の場合よりもはるかに少ない帯域幅を占有するものと予想される。代替として、ＧＷ１０４は、リストの１つを送信することを省略するこ

とができる。リストのうちの１つのみを検査することにより、ＳＧＳＮ１１０は、どのＵＥ１０１が正常に認証されたかについての結果を導き出すことができる。

１０．　ＧＷ１０４は、認証の結果を各ＵＥ１０１に知らせる（ステップ４９７）。すべてのＵＥ１０１が正常に認証された場合、ＧＷ１０４は単に「成功」メッセージをすべてのＵＥ１０１にブロードキャストする。それ以外の場合、ＧＷ１０４は、（ｉ）どのＵＥ１０１が正常に認証されたかに関する情報を含む成功メッセージをブロードキャストする、および（ｉｉ）どのＵＥ１０１が確認されなかったかに関する情報を含むエラーメッセージを、失敗の原因と共にブロードキャストする。あるいは、「成功」メッセージは省略されてもよく、正常に認証されたＵＥ１０１は、それらのＩＤがエラーブロードキャストメッセージに含まれているかどうかを検査することにより、認証の成功を認識することができる。各ＵＥ１０１は、ブロードキャストメッセージの受信をＧＷ１０４に個々に通知し、ＧＷ１０４は共通の確認応答メッセージをＳＧＳＮ１１０に転送する。

１１．　正常に認証された各UE_i１０１は、個々のK_i鍵（K_Gとは異なる）を使用して、CK_iおよびIK_iを計算し、加えて、ＭＴＣ＿CK_iおよびＭＴＣ＿IK_iが以下のように計算される（ステップ４９８）：

$MTC\_CK_i = CK_i \ XOR \ CK_G$

$MTC\_IK_i = IK_i \ XOR \ IK_G$

ただし、

$CK_G = f_3(K_G, G\_RAND)$，$IK_G = f_4(K_G, G\_RAND)$

$CK_i = f_3(K_i, G\_RAND)$，$IK_i = f_4(K_i, G\_RAND)$

Ｃ５．　ＧＷがデバイスを信頼し、デバイスをグループとして登録する。

【００５７】

認証プロトコルの帯域幅要件は、ＧＷが関連付けられたデバイスをすでに信頼している場合、すなわちデバイスおよびＧＷが共通の相互に信頼される環境内で動作する場合、いっそうさらに軽減される。たとえば、ＧＷと各デバイス間の通信リンクは、信頼されるローカルエリアネットワークの一部である。加えて、ＧＷはK_Gを認識しており、ＳＧＳＮ／ＨＳＳにより信頼される。したがって、この場合、ＧＷは、Ｇ＿ＲＡＮＤ（ＳＧＳＮ／ＨＳＳによりＧＷに送信された）およびK_Gを使用して計算された、Ｇ＿ＲＥＳを含むメッセージでＳＧＳＮ／ＨＳＳに応答する。Ｇ＿ＲＥＳを送信することにより、ＧＷは、特定のグループに属するすべてのデバイスが正常に認証されたことをＳＧＳＮ／ＨＳＳに知らせる。ＳＧＳＮ／ＨＳＳが＜デバイスＩＤ－グループＩＤ＞の形式のマッピングテーブルを保持するのであれば、ＳＧＳＮ／ＨＳＳは、特定のグループ内の各デバイスの認証の成功について通知される。ＨＳＳはK_GおよびK_iを認識しているので、ＭＴＣ＿CK_iおよびＭＴＣ＿IK_iはサブセクションＣ４に従って生成されてもよい。ＳＧＳＮ／ＨＳＳは、グループ登録確認メッセージをＧＷに送信する。ＧＷは、Ｇ＿ＲＡＮＤをこのメッセージに含め、メッセージをグループのすべてのデバイスにブロードキャストする。これにより、各デバイスは、Ｇ＿ＲＡＮＤ、K_G、およびK_iを使用して、ＭＴＣ＿CK_iおよびＭＴＣ＿IK_iをサブセクションＣ４に従って計算する。

【００５８】

Ｄ．　対象のグループに属するＵＥへの個々およびマルチキャストのＩＰアドレス割り当て（図２のフレームワークモジュール２０８）

ＵＥ１０１がＭ２Ｍアプリケーションサーバ１０８とのトラフィックセッション（複数可）を確立できるようにするため、ルーティング可能ＩＰアドレスは最初にＵＥ１０１に割り当てられる必要がある。そのために、ＵＥ１０１は、ＧＧＳＮ１１０とのＰＤＰ（パケットデータプロトコル）コンテキストを確立する必要がある。非常に多数のＵＥ１０１が単一のＧＷ１０４に接続されうることを考慮すれば、各ＵＥ１０１に３ＧＰＰコアネットワークとのＰＤＰコンテキストをネゴシエートさせることはオーバーヘッドの観点から過度な増大をまねく。したがって、このフレームワークでは、ＧＷ１０４は、ＵＥ１０１に代わってそれらのネゴシエーションを実行する責任を負う。さらに具体的には、ＩＰアドレス割り当て手順５００のステップは図５に示され、以下のとおりである：

１．　ＧＷ１０４は、「ＰＤＰコンテキストアクティブ化（ａｃｔｉｖａｔｅ　ＰＤＰ　ｃｏｎｔｅｘｔ）」メッセージをＳＧＳＮ１１０に送信する（ステップ５０２）。このメッセージは、グループＩＤおよびＰＤＰタイプを含む。このメッセージはまた、ＵＭＴＳにおいて個々の３ＧＰＰ　ＵＥのＰＤＰアクティブ化のために使用されるパラメータと同じパラメータを含む。

２．　ＳＧＳＮ１１０は、前述のパラメータを含む「ＰＤＰコンテキスト作成（ｃｒｅａｔｅ　ＰＤＰ　ｃｏｎｔｅｘｔ）」メッセージをゲートウェイＧＰＲＳサポートノード（ＧＧＳＮ：Ｇａｔｅｗａｙ　ＧＰＲＳ　Ｓｕｐｐｏｒｔ　Ｎｏｄｅ）に送信する（ステップ５０４）。ＧＧＳＮは図１に具体的に示されていないが、ＧＧＳＮがＳＧＳＮに接続され、ＧＰＲＳネットワークと、インターネットのような外部パケット交換ネットワークとの間の相互作用に責任を負うことが知られていることに留意されたい。

３．　ＧＧＳＮはＰＤＰコンテキストのインターフェイス識別子を選択し、アドレススペースを作成して、「ＰＤＰコンテキスト作成応答（ｃｒｅａｔｅ　ＰＤＰ　ｃｏｎｔｅｘｔ　ｒｅｓｐｏｎｓｅ）」メッセージでＳＧＳＮ１１０に応答する（ステップ５０６）。このメッセージは、（ａ）ＧＷ１０４に接続されるすべてのＵＥ１０１のＰＤＰアドレス、および（ｂ）グループＩＤに対応するグループマルチキャストアドレスを含む。

４．　ＳＧＳＮ１１０は、すべてのＵＥ１０１の割り当てられたＩＰアドレス、およびグループに対応するマルチキャストアドレスを含む「ＰＤＰコンテキストアクティブ化確定（ａｃｔｉｖａｔｅ　ＰＤＰ　ｃｏｎｔｅｘｔ　ａｃｃｅｐｔ）」メッセージをＧＷ１０４に送信する（ステップ５０８）。

５．　ＧＷ１０４は、このメッセージをすべてのＵＥ１０１にブロードキャストする（ステップ５１０）。このメッセージは、CK_Gを使用して暗号化され、IK_Gを使用して完全性保護される。

６．　各ＵＥ１０１は、確認メッセージでＧＷに個々に応答する（ステップ５１２）。ＵＥ１０１は、ＧＷ１０４がそのような情報をすでに認識しているので、ルータ要請メッセージをＧＧＳＮに送信することはない。同様に、ＧＧＳＮは、任意のルータアドバタイズメントをＵＥ１０１のグループに送信することはない。そのようなアドバタイズメントは、後者の登録中にＧＧＳＮによりＧＷ１０４に送信された。

７．　ＧＷ１０４は、すべてのＵＥ１０１からの応答を収集する（ステップ５１４）。その後、ＧＷ１０４は、単一確認応答メッセージをＧＧＳＮに送信する。

【００５９】

Ｅ．　グループ登録、認証、およびＭ２Ｍアプリケーションサーバとの鍵合意（図２のフレームワークモジュール２１０）

すべてのＵＥ１０１がそれらのＩＰアドレスを割り当てられた後、ＵＥ１０１は、ルーティング可能パスを介して、場合によってはインターネット経由で、Ｍ２Ｍアプリケーションサーバ１０８に到達することができる。デバイスは、Ｍ２Ｍアプリケーションサービスにアクセスする前に、サービスレイヤにおいてこのサーバに最初に登録する必要がある。本発明の技法の１つの目的は、デバイスのグループを、単純な方法で、すなわち各デバイスを個々に登録する必要なく、Ｍ２Ｍアプリケーションサーバに登録するためのメカニズムを提供することである。さまざまなネットワークおよびセキュリティプロトコルがサービスレイヤにおけるＭ２Ｍデバイスの登録に採用されてもよいが（ＡＫＡ、ＴＬＳ－ＰＳＫなど）、このフレームワークは、わずかな調整を行なうだけでそれらのプロトコルのいずれにも採用することができるか、またさらにはいかなる変更も行なわずに適用されてもよい。

【００６０】

１つの実施形態において、サービスレイヤ登録のための本発明の技法は、（ａ）Ｍ２Ｍサーバ１０８がクライアントエンティティとしてＭ２Ｍデバイス１０１を認証する必要があること、および（ｂ）Ｍ２Ｍサーバ１０８が複数のＭ２Ｍアプリケーションを容易にできることを考慮すれば、Ｍ２Ｍデバイス１０１でローカルに実行し、ネットワークサービスにアクセスしようとする各アプリケーションは、他のすべてのアプリケーションとは異

なるセキュリティ資格情報を使用する必要があること、という２つのサービスレイヤセキュリティ要件に動機付けられている。それらの要件を考慮すれば、本発明のフレームワークは、図６Ａに示される以下の汎用ステップを使用して、グループ登録、認証、および鍵合意プロトコル６００を実行する：

１．　手順は、ＵＥ１０１の正統性を確認するＧＷ１０４または認証エンティティ（たとえば、Ｍ２Ｍアプリケーションサーバ１０８）により開始される（ステップ６０２）。

２．　認証エンティティは、グループを構成するデバイスを識別し、ＵＥ１０１にチャレンジするために認証パラメータのセットをＧＷ１０４に送信する（ステップ６０４）。

３．　ＧＷ１０４は、チャレンジをすべてのＵＥ１０１にブロードキャストし、それらの応答を受信する。さらに、ＧＷ１０４は、応答を認証エンティティに転送する（ステップ６０６）。この場合も同様に、認証エンティティは、Ｍ２Ｍアプリケーションサーバ１０８であってもよいか、または応答を確認する別のオーセンティケータであってもよい。

４．　確認後、個々のセッション鍵および共通グループセッション鍵は、すべての関与するエンティティにより確立される（ステップ６０８）。

５．　アプリケーションレイヤ鍵素材は、それらのセッション鍵から生成される（ステップ６１０）。そのようなアプリケーションレイヤ鍵は、事前に合意された鍵の存在を必要とする、ＴＬＳ－ＰＳＫによるＨＴＴＰＳの場合のように、各アプリケーションに関与するデータトラフィックを安全にするために使用されてもよい（開示を引用により全体として本明細書において援用する、Ｕ．ＢｌｕｍｅｎｔｈａｌおよびＰ．Ｇｏｅｌ、「Ｐｒｅｓｈａｒｅｄ　Ｋｅｙ（ＰＳＫ）　Ｃｉｐｈｅｒｓｕｉｔｅｓ　ｗｉｔｈ　ＮＵＬＬ　Ｅｎｃｒｙｐｔｉｏｎ　ｆｏｒ　Ｔｒａｎｓｐｏｒｔ　Ｌａｙｅｒ　Ｓｅｃｕｒｉｔｙ（ＴＬＳ）」、ＲＦＣ　４７８５を参照）。

【００６１】

明らかに、これらのステップは、登録／認証プロトコルに容易に組み入れられうる。１つの一般的な方式では、アクセスネットワーク登録の場合のサブセクションＣと同様に、各Ｍ２Ｍ　ＵＥが一意の永久ルート鍵K_R、および共通グループルート鍵K_{GR}をすでにプロビジョニングされていると仮定する。上記で説明されるように、これらの鍵は次いで、図６Ｂに示される鍵階層６１２に従って、セッションおよびアプリケーション鍵を生成するために使用される。一例として、永久ルート鍵および共通グループルート鍵は共に、初期サービスグループ登録に先立ってＭ２Ｍ　ＵＥにプロビジョニングされる。すべてのサービス登録手順において、Ｍ２Ｍ　ＵＥは、それらの鍵の知識を提供することによって認証される。個々の登録中に、Ｍ２Ｍ　ＵＥを認証するためにルート鍵K_Rのみが使用されるが、グループ認証にはグループルート鍵K_{GR}が使用されることに留意されたい。サービスセッション鍵（K_S）は、K_RおよびK_{GR}の両方の使用を通じて、認証成功の結果として生成される。サービスセッション鍵は、新しく登録されるごとに更新される。そのような鍵はさらに、アプリケーション鍵（K_A）を導き出すために使用されるが、この鍵は、アプリケーションデータトラフィックの完全性保護および暗号化のためにセキュリティ機能によって使用される。

【００６２】

以下において、ＥＡＰ－ＡＫＡが使用される場合にこのサービスレイヤグループ登録プロトコルがどのように実現されうるかの例（ユースケース）を示す。ここで、認証エンティティ（オーセンティケータ）が、バックエンドＥＡＰサーバと通信する別個のエンティティであると仮定する。簡潔にするため、ここではそれらの対話については説明されない。図６Ｃのプロトコル６２０は、以下のステップを含む：

１．　オーセンティケータは、ＥＡＰ－要求／識別情報をＧＷ１０４に送信する（ステップ６２２）。

２．　すべてのＵＥ１０１がアライブ状態であり、ＧＷ１０４へのＺｉｇＢｅｅ接続を確立していると仮定して、ＧＷ１０４は、グループＩＤを含むＥＡＰ－応答／識別情報メッセージでオーセンティケータに応答する（ステップ６２４）。

３．　ＥＡＰサーバは、そのローカルデータベースを使用して、特定のグループに属す

るデバイスを識別する（ステップ６２６）。続いて、ＥＡＰサーバは、（ａ）各ＵＥ１０１の提供された個々のルート鍵K_R、および（ｂ）各ＵＥ１０１にも知られている共通グループルート鍵K_{GR}に基づいて認証ベクトルを取得する。取得された各ベクトルは、Ｖ＝｛Ｇ＿ＡＵＴＮ$_S$，Ｇ＿ＲＡＮＤ$_S$，Ｇ＿ＸＲＥＳ$_S$，［ＭＴＣ＿ＣＫ$_{S1}$，ＭＴＣ＿ＩＫ$_{S1}$］，．．．，［ＭＴＣ＿ＣＫ$_{SN}$，ＭＴＣ＿ＩＫ$_{SN}$］｝のような形態をとる。

４．　ＥＡＰサーバは、オーセンティケータを通じて、ＥＡＰ－グループ要求メッセージをＧＷ１０４に送信する（ステップ６２８）。このメッセージは、Ｇ＿ＲＡＮＤ$_S$、Ｇ＿ＡＵＴＮ$_S$、およびＧ＿ＭＡＣ$_S$、すなわちＥＡＰパケットをカバーするメッセージ認証コードを含む（たとえば、開示を引用により全体として本明細書において援用する、Ｊ．ＡｒｋｋｏおよびＨ．Ｈａｖｅｒｉｎｅｎ、「Ｅｘｔｅｎｓｉｂｌｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ Ｍｅｔｈｏｄ ｆｏｒ ３ｒｄ Ｇｅｎｅｒａｔｉｏｎ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ａｇｒｅｅｍｅｎｔ（ＥＡＰ－ＡＫＡ）」を参照）。

５．　ＧＷ１０４は、上記の３つのパラメータを含むＺｉｇＢｅｅブロードキャストメッセージをグループのすべてのＵＥ１０１に送信する（ステップ６３０）。このメッセージは、ＺｉｇＢｅｅ規格に従って、K_{ZB}で暗号化される。

６．　このブロードキャストメッセージを受信した後、各ＵＥ１０１は、Ｇ＿ＡＵＴＮ$_S$を個々に確認するためにＡＫＡアルゴリズムを実行する（ステップ６３２）。

７．　各ＵＥ１０１は、Ｇ＿ＲＥＳ$_S$を含むメッセージでＧＷ１０４に応答する（ステップ６３４）。Ｇ＿ＲＥＳ$_S$の値は、提供されたK_{GR}鍵を使用して計算される。この鍵はＵＥおよびＥＡＰサーバにのみ知られていることを再度言及する。さらに、各ＵＥ１０１が同じＧ＿ＲＡＮＤ$_S$を受信し、K_{GR}を有するので、各正規のＵＥ１０１はＧ＿ＲＥＳ$_S$の同じ値を計算すべきである。

８．　ＧＷ１０４は、すべての応答を収集し、それらをＥＡＰ－グループ応答メッセージで（オーセンティケータを通じて）ＥＡＰサーバに送信する（ステップ６３６）。このメッセージはまた、Ｇ＿ＭＡＣ$_S$も含む。

９．　ＥＡＰサーバは、Ｇ＿ＲＥＳ$_S$をＧ＿ＸＲＥＳ$_S$と比較することにより、Ｇ＿ＲＥＳ$_S$をＵＥ１０１ごとに検査する。サーバはまた、Ｇ＿ＭＡＣ$_S$も確認する（ステップ６３８）。

１０．　ＥＡＰサーバは、応答を認証の結果と共にＧＷ１０４に送信する（ステップ６４０）。

１１．　ＧＷ１０４は、認証の結果を各ＵＥ１０１に知らせる（ステップ６４２）。すべてのＵＥが正常に認証された場合、ＧＷは単に「成功」メッセージをすべてのＵＥにブロードキャストする。それ以外の場合、ＧＷは、（ｉ）どのＵＥが正常に認証されたかに関する情報を含む成功メッセージをブロードキャストする、および（ｉｉ）どのＵＥが確認されなかったかに関する情報を含むエラーメッセージを、失敗の原因と共にブロードキャストする。あるいは、「成功」メッセージは省略されてもよく、正常に認証されたＵＥは、それらのＩＤがエラーブロードキャストメッセージに含まれているかどうかを検査することにより、認証の成功を認識することができる。各ＵＥは、ブロードキャストメッセージの受信をＧＷに個々に通知し、ＧＷは共通の確認応答メッセージをオーセンティケータに転送する。

１２．　正常に認証された各UE_i１０１は、個々のK_i鍵（K_Gとは異なる）を使用して、CK_{Si}およびIK_{Si}を計算し、加えて、ＭＴＣ＿CK_{Si}およびＭＴＣ＿IK_{Si}が以下のように計算される（ステップ６４４）：

$MTC\_CK_{Si} = CK_{Si}\ XOR\ CK_{GR}$

$MTC\_IK_{Si} = IK_{Si}\ XOR\ IK_{GR}$

ただし、

$CK_{GR} = f_3(K_G, G\_RAND_S)$，$IK_{GR} = f_4(K_{GR}, G\_RAND_S)$

$CK_{Ri} = f_3(K_R, G\_RAND_S)$，$IK_{Si} = f_4(K_R, G\_RAND_S)$

１３．　MTC_CK_{Si}は、グループ登録が有効を維持する限り、特定のUE_iのセ

ッション鍵K_{S_i}として使用されてもよい（ステップ６４６）。この鍵から、３ＧＰＰＴＳ３３．１０２に従って、ＵＥおよびオーセンティケータの両方により、任意の数のアプリケーション鍵K_A（ＵＥでローカルに実行する）が導き出されてもよい（たとえば図６Ｂを参照）。新しく登録されるたびに新しいセッション鍵が導き出されるので、すべてのアプリケーションレイヤ鍵は、新しいグループ登録ごとに更新される。

【００６３】

Ｆ．　設計の前提事項（７）の緩和

サブセクションＩＩにおいて、ＵＥとＧＷ間のリンクが暗号化される可能性があるという前提事項（７）を示した。この前提事項は、Ｇ＿ＲＥＳが、K_Gに加えてＵＥの一意の識別子（たとえば、ＵＭＴＳの場合ＩＭＳＩ）を使用して各ＵＥにより計算されると仮定することにより緩和されてもよい。これにより、Ｇ＿ＲＥＳの値は、ＵＥごとに異なる。

ＩＶ．　例示的なコンピューティングシステム

【００６４】

図７は、本発明による複数のエンティティ（Ｍ２Ｍデバイス１０１のようなオープンデバイス、およびＧＷ１０４のようなゲートウェイサーバ）間の安全な登録プロトコルを実施するのに適したコンピューティングシステムの形態で、ネットワーク環境および通信デバイス（ユーザ）の汎用ハードウェアアーキテクチャ７００を示す。図に示されるように、Ｍ２Ｍデバイス（通信デバイス）はコンピューティングシステム７０２を備え、ゲートウェイサーバ（ネットワークデバイス）はコンピューティングシステム７０４を備える。２つのコンピューティングシステム７０２および７０４は、ネットワーク７０６を介して結合される。ネットワークは、Ｍ２ＭデバイスおよびＧＷサーバが通信することができる任意のネットワークであってもよく、たとえば、上記で説明される実施形態におけるように、ネットワーク７０６は、ネットワーク事業者（たとえば、Ｖｅｒｉｚｏｎ、ＡＴ＆Ｔ、Ｓｐｒｉｎｔ）により運用されるセルラー通信ネットワークのような、公的にアクセス可能なワイドエリア通信ネットワークを含むことができる。しかし、本発明は、特定のタイプのネットワークに限定されることはない。通常、Ｍ２Ｍデバイスはクライアントマシンであってもよく、ＧＷサーバはサーバマシンであってもよい。また、共にクライアントであってもよく、または共にサーバであってもよい。さらに、クライアントは、ユーザとインターフェイスをとることができる。したがって、本発明の通信プロトコルは、コンピューティングシステムがそれぞれクライアントおよびサーバである事例に限定されることはなく、むしろ２つのネットワーク要素を備える任意のコンピューティングデバイスに適用可能であることを理解されたい。

【００６５】

したがって、図７のアーキテクチャが、図４Ａから図６Ｃのプロトコルの２つの関与要素を示すことを理解されたい。類似するコンピューティングシステム（通信デバイスおよびネットワークデバイス）が、たとえばＮｏｄｅ　Ｂ１０６、アプリケーションサーバ１０８、ＳＧＳＮ１１０、ＨＳＳ１１２などのプロトコルのその他の関与要素の実施を実現するために使用されることを理解されたい。簡潔にするため、本発明のプロトコルに関与しうるすべてのコンピューティングシステム（通信デバイスおよびネットワークデバイス）が、図７に示されているわけではない。

【００６６】

当業者には容易に理解されるように、サーバおよびクライアントは、プログラムコードの制御の下で動作するプログラムされたコンピューティングシステムとして実施されてもよい。プログラムコードは、コンピュータ可読ストレージ媒体（たとえば、メモリ）に格納され、コードは、コンピューティングシステムのプロセッサにより実行される。あるいは、サーバおよびクライアントはそれぞれ、１つまたは複数の特殊用途向け集積回路（ＡＳＩＣ）として実施されてもよい。ＡＳＩＣはプログラムコードにアクセスしてロードすることができるか、またはプログラムコードはＡＳＩＣに格納されてもよい。本発明のこの開示を踏まえ、当業者は、本明細書において説明されるプロトコルを実施するために、適切なプログラムコードを容易に作成することができるであろう。

【００６７】
しかし、図７では、ネットワークを介して通信する各コンピューティングシステムのための例示的なアーキテクチャを全体的に示す。示されているように、Ｍ２Ｍデバイス７０２は、Ｉ／Ｏデバイス７０８－Ａ、プロセッサ７１０－Ａ、およびメモリ７１２－Ａを備える。ＧＷサーバ７０４は、Ｉ／Ｏデバイス７０８－Ｂ、プロセッサ７１０－Ｂ、およびメモリ７１２－Ｂを備える。本明細書において使用される「プロセッサ」という用語は、中央処理装置（ＣＰＵ）、または１つまたは複数の信号プロセッサ、１つまたは複数の集積回路などを含む（ただし、これらに限定されない）、その他の処理回路を含む、１つまたは複数の処理デバイスを含むことが意図されることを理解されたい。また、本明細書において使用される「メモリ」という用語は、ＲＡＭ、ＲＯＭ、固定メモリデバイス（たとえば、ハードドライブ）、または取り外し可能メモリデバイス（たとえば、ディスケットまたはＣＤＲＯＭ）のような、プロセッサまたはＣＰＵに関連付けられたメモリを含むことが意図される。加えて、本明細書において使用される「Ｉ／Ｏデバイス」という用語は、処理装置にデータを入力するための１つまたは複数の入力デバイス（たとえば、キーボード、マウス）、および処理装置に関連付けられた結果を提供するための１つまたは複数の出力デバイス（例えばＣＲＴディスプレイ）を含むことが意図される。

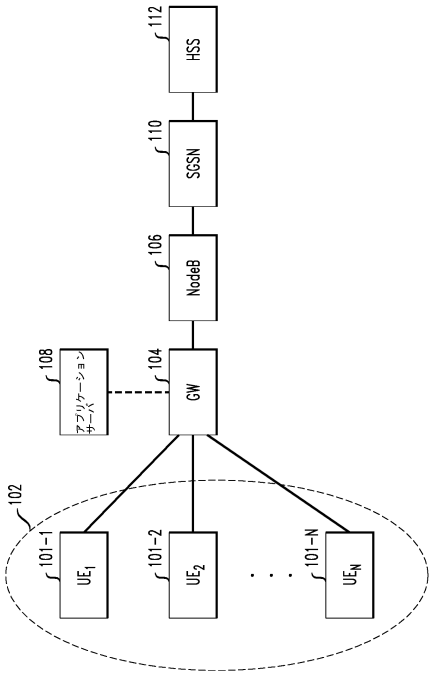
【００６８】
したがって、本明細書において説明される、本発明の方法を実行するためのソフトウェア命令またはコードは、たとえばＲＯＭ、固定式または取り外し可能メモリのような関連するメモリデバイスの１つまたは複数に格納されてもよく、使用される準備が整ったときにＲＡＭにロードされ、ＣＰＵにより実行されてもよい。

【００６９】
有利なことに、上記で例示的に説明してきたように、本発明の原理は、複数のクライアント／デバイス（ユーザ）が登録手順の１つのセットを使用して同一のサーバ／ネットワークで安全に登録できるようにするフレームワーク（および方法）を提供する。要するに、「リバースシングルサインオン」の問題を解決するためのフレームワークおよび詳細なプロトコルを開発する。このフレームワークの１つの主要な利点は、複数のクライアントデバイス（ユーザ）が「グループ」としてネットワークに登録できるようにし、しかもネットワークとの個々のセッション鍵を生成することができるようにすることである。これにより、多数のデバイス（ユーザ）を認証するプロセスは、大幅に簡略化され、認証手順の複雑さおよび帯域幅要件がかなりの程度まで軽減される。解説を簡略化することを目的として、このセキュリティフレームワークが、（マシンタイプ通信すなわちＭＴＣとしても知られている）マシン間通信（Ｍ２Ｍ）へのアプリケーションでグループ認証および鍵合意を実行するためにどのように適用されうるかについて説明する。Ｍ２Ｍはアプリケーションの１つの適切な分野であるが、このフレームワークは一般的であり、グループ登録が道理にかなうようなその他のアプリケーションにも十分に対処できる。

【００７０】
本発明の例示的な実施形態は、添付の図面を参照して、本明細書において説明されてきたが、本発明がそれらの厳密な実施形態に限定されることはなく、さまざまなその他の変更および修正が、本発明の範囲または趣旨を逸脱することなく当業者によって行なわれてもよいことを理解されたい。

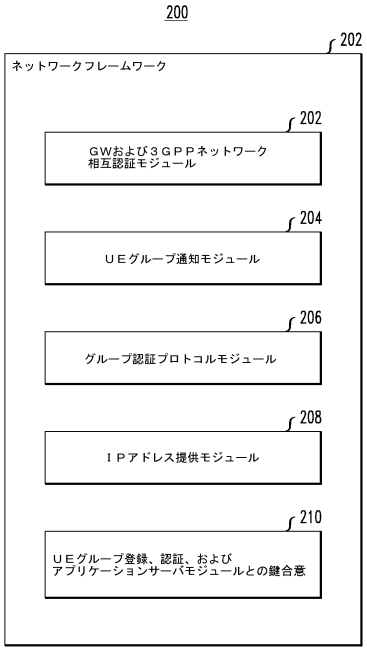
【図１】

FIG. 1



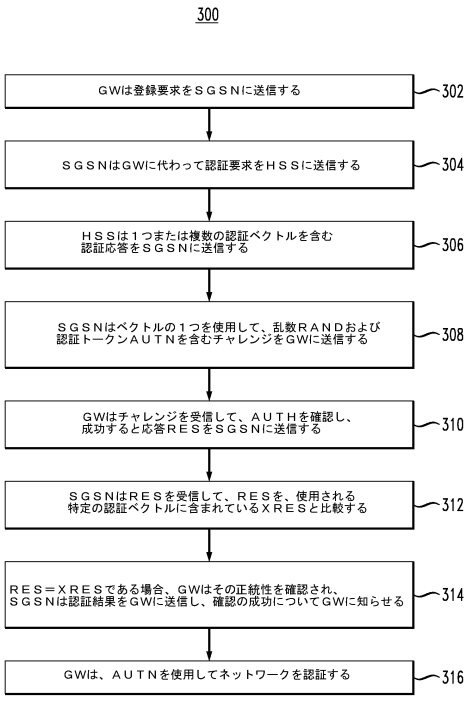
【図２】

FIG. 2



【図３】

FIG. 3

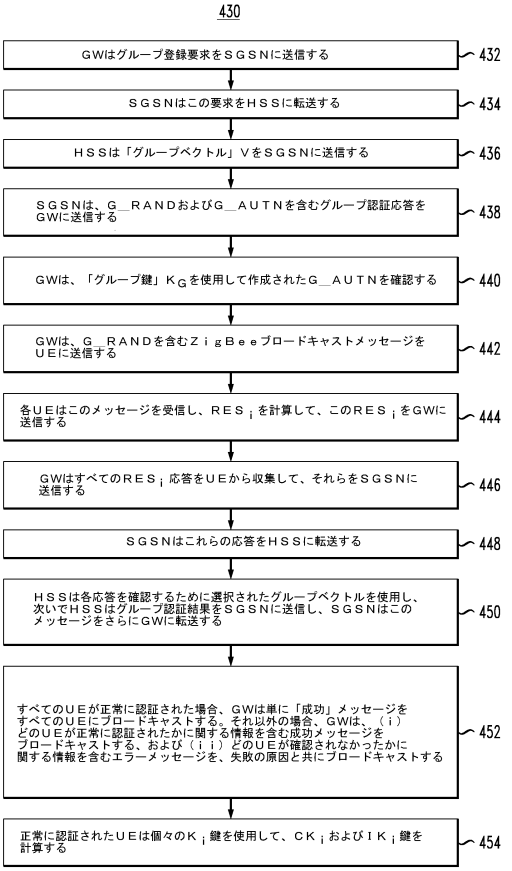


【図４Ａ】

FIG. 4A

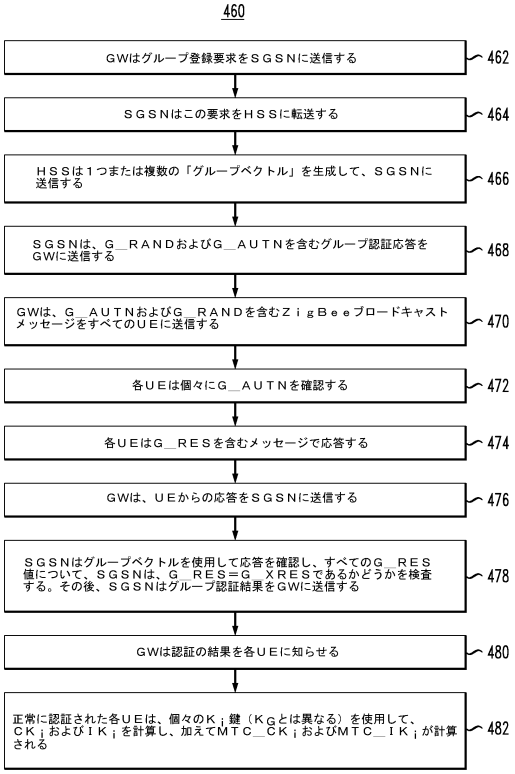
【図４Ｂ】

FIG. 4B



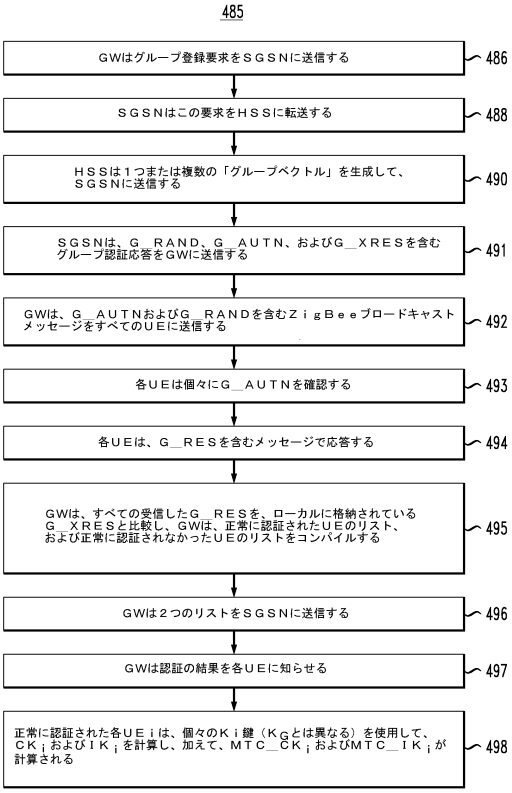
【図４Ｃ】

FIG. 4C



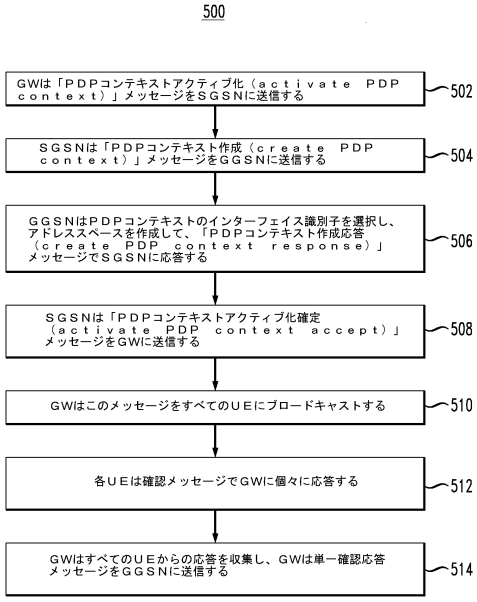
【図４Ｄ】

FIG. 4D



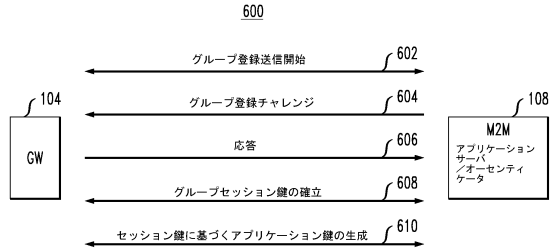
【図５】

FIG. 5



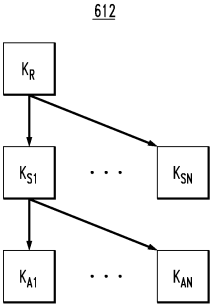
【図６Ａ】

FIG. 6A



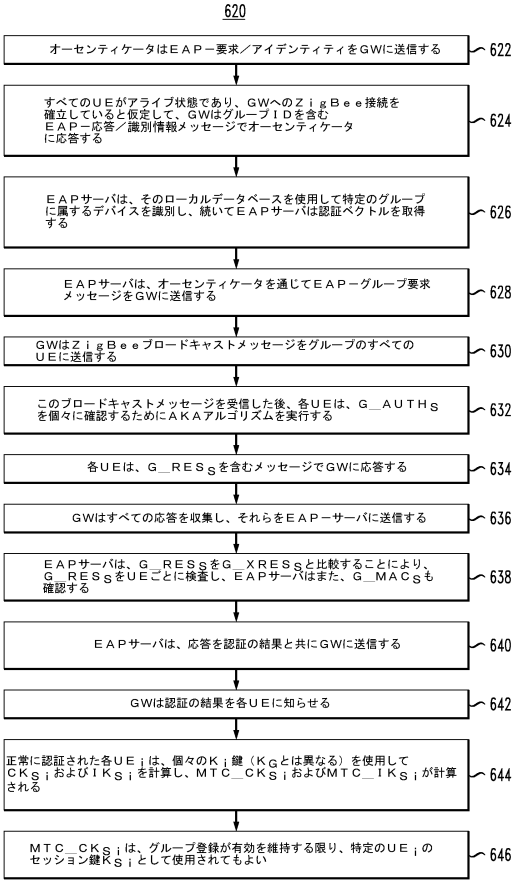
【図６Ｂ】

FIG. 6B



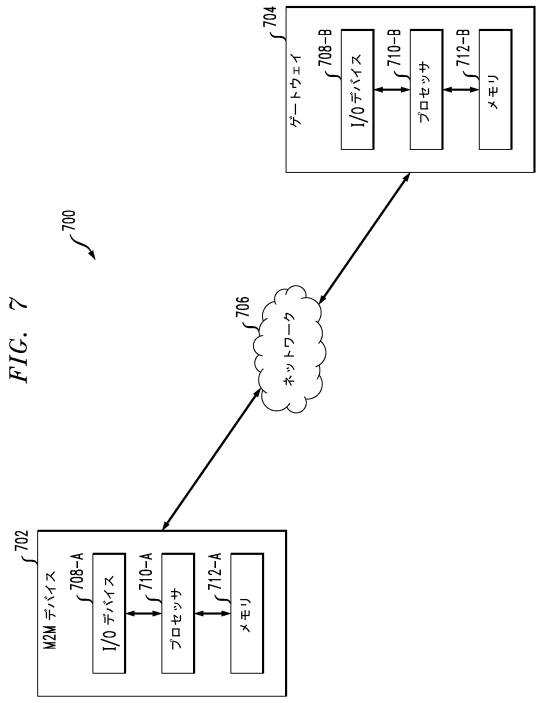
【図６Ｃ】

FIG. 6C



【図７】

FIG. 7



フロントページの続き

(72)発明者　ハリツシユ・ビスワナサン
アメリカ合衆国、ニユー・ジヤージー・０７９６０、モリスタウン、コツトンウツド・ロード・１７

合議体
審判長　石井　茂和
審判官　高木　進
審判官　須田　勝巳

(56)参考文献　特開２００２－１２４９４１（ＪＰ，Ａ）
国際公開第２００５／１０６６８１（WO，Ａ１）
特開２００２－１６３２１２（ＪＰ，Ａ）
特開２００６－１０９４１３（ＪＰ，Ａ）
特開２００１－２１１１４７（ＪＰ，Ａ）
熊谷恒治，ＮＴ管理者必見！！Ｗｉｎｄｏｗｓ２０００へのアップグレードに失敗しないためのＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙへの近道　第6回，Ｗｉｎｄｏｗｓ　ＮＴ　Ｗｏｒｌｄ，日本，株式会社ＩＤＧコミュニケーションズ，１９９９年7月1日，Ｖｏｌ．４，Ｎｏ．７，ｐ．２８８－２９１

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/00