(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2013-534754
(P2013-534754A)
(43)公表日　平成25年9月5日(2013.9.5)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601B	5J104
G09C 1/00	(2006.01)	H04L	9/00	601E	5K067
H04W 12/06	(2009.01)	G09C	1/00	640E	
H04L 9/32	(2006.01)	H04W	12/06		
		H04L	9/00	675A	

審査請求 有　予備審査請求 未請求　（全 32 頁）

(21)出願番号　特願2013-515526 (P2013-515526)
(86)(22)出願日　平成23年6月16日 (2011.6.16)
(85)翻訳文提出日　平成24年12月20日 (2012.12.20)
(86)国際出願番号　PCT/US2011/040777
(87)国際公開番号　WO2011/159952
(87)国際公開日　平成23年12月22日 (2011.12.22)
(31)優先権主張番号　13/161,336
(32)優先日　平成23年6月15日 (2011.6.15)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/355,423
(32)優先日　平成22年6月16日 (2010.6.16)
(33)優先権主張国　米国 (US)

(71)出願人　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　エイドリアン・エドワード・エスコット
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】通信システムにおいて加入者認証とデバイス認証とをバインドするための方法および装置

(57)【要約】
デバイス(たとえば、クライアントデバイスまたはアクセス端末)とネットワークエンティティとの間の認証方法を提供する。リムーバブルストレージデバイスがデバイスに結合され得、加入者認証のために使用され得る加入者固有鍵を記憶する。セキュアストレージデバイスがデバイスに結合され得、デバイス認証のために使用されるデバイス固有鍵を記憶する。デバイスとネットワークエンティティとの間で加入者認証が実行され得る。また、ネットワークエンティティとのデバイスのデバイス認証が実行され得る。次いで、加入者認証とデバイス認証とをバインドするセキュリティ鍵が生成され得る。セキュリティ鍵は、デバイスとサービングネットワークとの間の通信をセキュアにするために使用され得る。

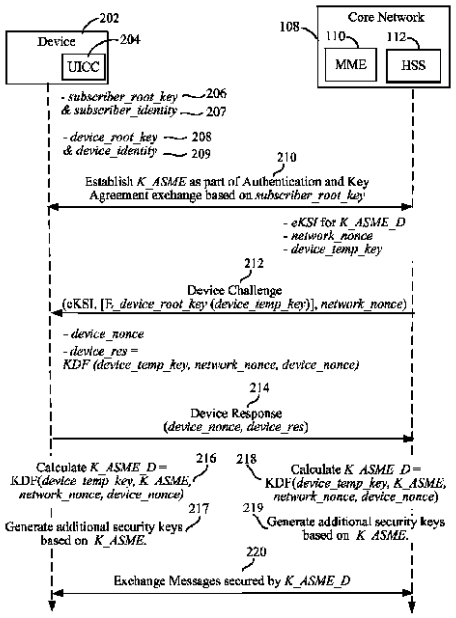


FIG. 2

【特許請求の範囲】
【請求項１】
デバイスにおいて動作可能な方法であって、
ネットワークエンティティとの加入者認証を実行するステップと、
ネットワークエンティティとの前記デバイスのデバイス認証を実行するステップと、
前記加入者認証と前記デバイス認証とをバインドするセキュリティ鍵を生成するステップと、
前記デバイスとサービングネットワークとの間の通信をセキュアにするために前記セキュリティ鍵を使用するステップと
を含む、方法。
【請求項２】
加入者認証が、前記デバイスと前記ネットワークエンティティとの間の認証鍵一致交換に基づく、請求項1に記載の方法。
【請求項３】
デバイス認証が、前記デバイスと前記ネットワークエンティティとの間の質問応答交換に基づく、請求項1に記載の方法。
【請求項４】
加入者認証が、前記ネットワークエンティティの一部である第1の認証サーバによって実行され、デバイス認証が、前記ネットワークエンティティの一部である第2の認証サーバによって実行される、請求項1に記載の方法。
【請求項５】
デバイス認証が、
前記ネットワークエンティティから、前記デバイスの公開鍵で暗号化されたデータを受信するステップと、
前記暗号化データを解読するために、対応する秘密鍵を使用するステップと、
その後、前記デバイスが前記データの知識を有することを前記ネットワークエンティティに証明するステップと
によって実行される、請求項1に記載の方法。
【請求項６】
前記デバイスから前記ネットワークエンティティに接続要求を送るステップであって、前記接続要求が前記デバイスのデバイス認証能力の指示を含む、送るステップ
をさらに含む、請求項1に記載の方法。
【請求項７】
デバイス認証が、前記加入者認証中に生成された少なくとも1つの鍵によってセキュアにされる、請求項1に記載の方法。
【請求項８】
加入者認証とデバイス認証とが複合メッセージ交換において同時に実行される、請求項1に記載の方法。
【請求項９】
加入者認証が、前記デバイス認証とは別の、早期のセキュリティ交換において実行される、請求項1に記載の方法。
【請求項１０】
前記セキュリティ鍵が、少なくとも、加入者認証から取得された第1の鍵と、デバイス認証から取得された第2の鍵とに応じて生成される、請求項1に記載の方法。
【請求項１１】
前記セキュリティ鍵がネットワークナンスとデバイスナンスとの関数でもある、請求項10に記載の方法。
【請求項１２】
前記デバイスが、前記ネットワークエンティティにはアクセス端末のように見え、1つまたは複数のアクセス端末にはネットワークデバイスのように見えるリレーノードである

、請求項1に記載の方法。
【請求項１３】
前記セキュリティ鍵が、前記デバイスと前記ネットワークエンティティとによって別々に生成される、請求項1に記載の方法。
【請求項１４】
サービス契約の一部として加入者固有鍵をプロビジョニングするステップであって、前記加入者固有鍵が前記加入者認証のために使用される、プロビジョニングするステップと、
製造中に前記デバイスにおいてデバイス固有鍵をプロビジョニングするステップであって、前記デバイス固有鍵が前記デバイス認証のために使用される、プロビジョニングするステップと
をさらに含む、請求項1に記載の方法。
【請求項１５】
通信インターフェースと、
前記通信インターフェースに結合された処理回路であって、
ネットワークエンティティとの加入者認証を実行することと、
ネットワークエンティティとの前記デバイスのデバイス認証を実行することと、
前記加入者認証と前記デバイス認証とをバインドするセキュリティ鍵を生成することと、
前記デバイスとサービングネットワークとの間の通信をセキュアにするために前記セキュリティ鍵を使用することと
を行うように適応された処理回路と
を含む、デバイス。
【請求項１６】
加入者認証が、前記デバイスと前記ネットワークエンティティとの間の認証鍵一致交換に基づく、請求項15に記載のデバイス。
【請求項１７】
デバイス認証が、前記デバイスと前記ネットワークエンティティとの間の質問応答交換に基づく、請求項15に記載のデバイス。
【請求項１８】
デバイス認証が、
前記ネットワークエンティティから、前記デバイスの公開鍵で暗号化されたデータを受信するステップと、
前記暗号化データを解読するために、対応する秘密鍵を使用するステップと、
その後、前記デバイスが前記データの知識を有することを前記ネットワークエンティティに証明するステップと
によって実行される、請求項15に記載のデバイス。
【請求項１９】
前記デバイスから前記ネットワークエンティティに接続要求を送るステップであって、前記接続要求が前記デバイスのデバイス認証能力の指示を含む、送るステップ
をさらに含む、請求項15に記載のデバイス。
【請求項２０】
デバイス認証が、前記加入者認証中に生成された少なくとも1つの鍵によってセキュアにされる、請求項15に記載のデバイス。
【請求項２１】
加入者認証とデバイス認証とが複合メッセージ交換において同時に実行される、請求項15に記載のデバイス。
【請求項２２】
加入者認証が、前記デバイス認証とは別の、早期のセキュリティ交換において実行される、請求項15に記載のデバイス。

【請求項２３】
前記セキュリティ鍵が、少なくとも、加入者認証から取得された第1の鍵と、デバイス認証から取得された第2の鍵とに応じて生成される、請求項15に記載のデバイス。
【請求項２４】
前記デバイスが、前記ネットワークエンティティにはアクセス端末のように見え、1つまたは複数のアクセス端末にはネットワークデバイスのように見えるリレーノードである、請求項15に記載のデバイス。
【請求項２５】
前記処理回路に結合されたリムーバブルストレージデバイスであって、前記加入者認証のために使用される加入者固有鍵を記憶するリムーバブルストレージデバイスと、
前記処理回路に結合されたセキュアストレージデバイスであって、前記デバイス認証のために使用されるデバイス固有鍵を記憶するセキュアストレージデバイスと
をさらに含む、請求項15に記載のデバイス。
【請求項２６】
ネットワークエンティティとの加入者認証を実行するための手段と、
ネットワークエンティティとの前記デバイスのデバイス認証を実行するための手段と、
前記加入者認証と前記デバイス認証とをバインドするセキュリティ鍵を生成するための手段と、
前記デバイスとサービングネットワークとの間の通信をセキュアにするために前記セキュリティ鍵を使用するための手段と
を含む、デバイス。
【請求項２７】
前記加入者認証のために使用される加入者固有鍵を記憶するための手段と、
前記デバイス認証のために使用されるデバイス固有鍵を記憶するための手段と
をさらに含む、請求項26に記載のデバイス。
【請求項２８】
デバイス上で動作可能な命令であって、プロセッサによって実行されたとき、前記プロセッサに、
ネットワークエンティティとの加入者認証を実行することと、
ネットワークエンティティとの前記デバイスのデバイス認証を実行することと、
前記加入者認証と前記デバイス認証とをバインドするセキュリティ鍵を生成することと、
前記デバイスとサービングネットワークとの間の通信をセキュアにするために前記セキュリティ鍵を使用することと
を行わせる命令を含むプロセッサ可読媒体。
【請求項２９】
ネットワークエンティティにおいて動作可能な方法であって、
デバイスとの加入者認証を実行するステップと、
前記デバイスのデバイス認証を実行するステップと、
前記加入者認証と前記デバイス認証とをバインドするセキュリティ鍵を生成するステップと、
前記ネットワークエンティティと前記デバイスとの間の通信をセキュアにするために前記セキュリティ鍵を使用するステップと
を含む、方法。
【請求項３０】
加入者認証が、前記ネットワークエンティティと前記デバイスとの間の認証鍵一致交換に基づく、請求項29に記載の方法。
【請求項３１】
デバイス認証が、前記ネットワークエンティティと前記デバイスとの間の質問応答交換に基づく、請求項29に記載の方法。

【請求項３２】
デバイス認証が、
前記デバイスから証明書を受信するステップと、
前記デバイスに関連する前記証明書が取り消されていないことを検証するステップと
を含む、請求項29に記載の方法。
【請求項３３】
前記デバイスから接続要求を受信するステップであって、前記接続要求が前記デバイスのデバイス認証能力の指示を含む、受信するステップ
をさらに含む、請求項29に記載の方法。
【請求項３４】
デバイス認証が、前記加入者認証中に生成された少なくとも1つの鍵によってセキュアにされる、請求項29に記載の方法。
【請求項３５】
加入者認証とデバイス認証とが複合メッセージ交換において同時に実行される、請求項29に記載の方法。
【請求項３６】
加入者認証が、前記デバイス認証とは別の、早期のセキュリティ交換において実行される、請求項29に記載の方法。
【請求項３７】
前記セキュリティ鍵が、少なくとも、加入者認証から取得された第1の鍵と、デバイス認証から取得された第2の鍵とに応じて生成される、請求項29に記載の方法。
【請求項３８】
前記セキュリティ鍵が、前記デバイスと前記ネットワークエンティティとによって別々に生成される、請求項29に記載の方法。
【請求項３９】
サービス契約の一部として加入者固有鍵を取得するステップであって、前記加入者固有鍵が前記加入者認証のために使用される、取得するステップと、
前記デバイスのためのデバイス固有鍵を取得するステップであって、前記デバイス固有鍵が前記デバイス認証のために使用される、取得するステップと
をさらに含む、請求項29に記載の方法。
【請求項４０】
ネットワークエンティティであって、
通信インターフェースと、
前記通信インターフェースに結合された処理回路であって、
デバイスとの加入者認証を実行することと、
前記デバイスのデバイス認証を実行することと、
前記加入者認証と前記デバイス認証とをバインドするセキュリティ鍵を生成することと、
前記ネットワークエンティティと前記デバイスとの間の通信をセキュアにするために前記セキュリティ鍵を使用することと
を含む、ネットワークエンティティ。
【請求項４１】
加入者認証が、前記ネットワークエンティティと前記デバイスとの間の認証鍵一致交換に基づく、請求項40に記載のネットワークエンティティ。
【請求項４２】
デバイス認証が、前記ネットワークエンティティと前記デバイスとの間の質問応答交換に基づく、請求項40に記載のネットワークエンティティ。
【請求項４３】
前記処理回路が、
前記デバイスから接続要求を受信することであって、前記接続要求が前記デバイスのデ

バイス認証能力の指示を含む、受信すること
を行うようにさらに適応された、請求項40に記載のネットワークエンティティ。
【請求項４４】
デバイス認証が、前記加入者認証中に生成された少なくとも1つの鍵によってセキュアにされる、請求項40に記載のネットワークエンティティ。
【請求項４５】
加入者認証とデバイス認証とが複合メッセージ交換において同時に実行される、請求項40に記載のネットワークエンティティ。
【請求項４６】
加入者認証が、前記デバイス認証とは別の、早期のセキュリティ交換において実行される、請求項40に記載のネットワークエンティティ。
【請求項４７】
前記セキュリティ鍵が、少なくとも、加入者認証から取得された第1の鍵と、デバイス認証から取得された第2の鍵とに応じて生成される、請求項40に記載のネットワークエンティティ。
【請求項４８】
サービス契約の一部として加入者固有鍵を取得するステップであって、前記加入者固有鍵が前記加入者認証のために使用される、取得するステップと、
前記デバイスのためのデバイス固有鍵を取得するステップであって、前記デバイス固有鍵が前記デバイス認証のために使用される、取得するステップと
をさらに含む、請求項40に記載のネットワークエンティティ。
【請求項４９】
ネットワークエンティティであって、
デバイスとの加入者認証を実行するための手段と、
前記デバイスのデバイス認証を実行するための手段と、
前記加入者認証と前記デバイス認証とをバインドするセキュリティ鍵を生成するための手段と、
前記ネットワークエンティティと前記デバイスとの間の通信をセキュアにするために前記セキュリティ鍵を使用するための手段と
を含む、ネットワークエンティティ。
【請求項５０】
ネットワークエンティティ上で動作可能な命令であって、プロセッサによって実行されたとき、前記プロセッサに、
デバイスとの加入者認証を実行することと、
前記デバイスのデバイス認証を実行することと、
前記加入者認証と前記デバイス認証とをバインドするセキュリティ鍵を生成することと、
前記ネットワークエンティティと前記デバイスとの間の通信をセキュアにするために前記セキュリティ鍵を使用することと
を行わせる命令を含むプロセッサ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
米国特許法第119条に基づく優先権の主張
本特許出願は、本出願の譲受人に譲渡され、参照により本明細書に明確に組み込まれる、2010年6月16日に出願された「Apparatus and Method for Device Authentication in 3GPP Systems」と題する米国仮出願第61/355,423号の優先権を主張する。
【０００２】
様々な特徴は、通信システムに関し、より詳細には、ワイヤードおよび/またはワイヤレス通信システムにおいて採用される、リレーノードおよびマシンツーマシンデバイスな

ど、デバイスの認証に関する。

【背景技術】

【０００３】

現代のワイヤレスネットワークは、ここではまとめてデバイスと呼ぶリレーノードおよび/またはアクセス端末を含み得る。そのようなデバイスが適切に機能するために、デバイスが動作させられる前に、デバイスは、しばしば、使用可能な(operational)加入者セキュリティ証明をプロビジョニングされ、それらで構成される。そのような加入者セキュリティ証明は、たとえば、ワイヤレスサービスまたはアクセスを与えるより前にデバイスを認証するために使用され得、場合によっては、モジュールのホストデバイスに着脱不可能に結合したモジュールに記憶され得る。加入者セキュリティ証明が認証されたデバイスから削除され、無許可デバイスに入れられ得るという危険が存在する。リレーノードの場合、これは、無許可リレーノードが、たとえば、アクセスノードと1つまたは複数のアクセス端末との間の送信に不正にアクセスすること、および/またはネットワークサービスへのフリーアクセスを取得することを可能にし得る。フリーネットワークアクセスを獲得するためにマシンツーマシン(M2M)デバイス中の有効な加入者証明(たとえば、リムーバブルユニバーサル集積回路カード(UICC)中の認証および鍵一致(AKA)パラメータ)が別のデバイスに転送され得るので、この危険または脆弱性はM2Mデバイスの場合にも存在する。M2Mデバイス自体への物理的アクセスを有する必要がないので、関連する脆弱性が存在する。M2Mデバイスインターフェース(たとえば、ホストデバイス対UICCインターフェース)を横断しているデータ(たとえば、認証から生じるセキュリティ鍵)へのアクセスは、セキュリティ鍵へのアクセスを獲得し、前記鍵によってセキュアにされたデータを露出するのに十分である。

【０００４】

事業者が、どのデバイスがそれらのネットワークにアクセスすることを可能にされるかを制御することを望む場合、同様の問題が存在する。

【発明の概要】

【発明が解決しようとする課題】

【０００５】

したがって、これらおよび他の脆弱性および危険に対処するために、追加のセキュリティをデバイスに与える必要がある。

【課題を解決するための手段】

【０００６】

セキュリティ鍵を生成するために加入者認証とデバイス認証とをバインドすることによってデバイスをセキュアにするための方法および装置を提供する。

【０００７】

第1の態様によれば、加入者認証とデバイス認証とをバインドする、デバイスにおいて動作可能な方法が提供される。デバイスは、ネットワークエンティティに接続要求を送ることによって開始し得、接続要求はデバイスのデバイス認証能力の指示を含む。ネットワークエンティティとの加入者認証がデバイスによって実行され得る。たとえば、加入者認証は、デバイスとネットワークエンティティとの間の認証鍵一致交換に基づき得る。デバイスはまた、ネットワークエンティティとのデバイス認証を実行し得る。たとえば、デバイス認証は、デバイスとネットワークエンティティとの間の質問応答交換に基づき得る。

【０００８】

次いで、加入者認証とデバイス認証とをバインドするセキュリティ鍵が生成され得る。セキュリティ鍵は、少なくとも、加入者認証から取得された第1の鍵と、デバイス認証から取得された第2の鍵とに応じて生成され得る。さらに、セキュリティ鍵は、ネットワークナンスとデバイスナンスとの関数でもあり得る。セキュリティ鍵は、次いで、デバイスとサービングネットワークとの間の通信をセキュアにするために使用され得る。セキュリティ鍵は、デバイスとネットワークエンティティとによって別々に生成され得、したがって、オーバージエアで送信されないことに留意されたい。

【０００９】
一実装形態によれば、加入者認証は、ネットワークエンティティの一部である第1の認証サーバによって実行され得、デバイス認証は、ネットワークエンティティの一部である第2の認証サーバによって実行され得る。
【００１０】
一例では、デバイス認証は、デバイスとネットワークエンティティとの間のいくつかの交換を暗号化/解読するために共有秘密鍵を使用することによって実行され得る。別の例では、デバイス認証は、(a)ネットワークエンティティから、デバイスの公開鍵で暗号化されたデータを受信すること、(b)暗号化データを解読するために、対応する秘密鍵を使用すること、および/または(c)その後、デバイスがデータの知識を有することをネットワークエンティティに証明することによって実行され得る。
【００１１】
一態様によれば、デバイス認証は、加入者認証中に生成された少なくとも1つの鍵によってセキュアにされ得る。
【００１２】
様々な実装形態では、加入者認証とデバイス認証とは、複合メッセージ交換において同時に実行され得るか、または加入者認証は、デバイス認証とは別の、早期のセキュリティ交換において実行され得る。
【００１３】
1つの特徴によれば、加入者固有鍵は、サービス契約の一部としてデバイス上にプロビジョニングされ得、加入者固有鍵は加入者認証のために使用される。同様に、デバイス固有鍵は、製造中にデバイスにおいてプロビジョニングされ得、デバイス固有鍵はデバイス認証のために使用される。
【００１４】
一実装形態では、デバイスは、ネットワークエンティティにはアクセス端末のように見え、1つまたは複数のアクセス端末にはネットワークデバイスのように見えるリレーノードであり得る。別の実装形態では、デバイスはアクセス端末であり得る。
【００１５】
一例によれば、デバイスは、処理回路に結合された通信インターフェースを含み得る。処理回路は、(a)ネットワークエンティティとの加入者認証を実行すること、(b)ネットワークエンティティとのデバイスのデバイス認証を実行すること、(c)加入者認証とデバイス認証とをバインドするセキュリティ鍵を生成すること、および/または(d)デバイスとサービングネットワークとの間の通信をセキュアにするためにセキュリティ鍵を使用することを行うように適応され得る。
【００１６】
さらに別の例によれば、デバイス上で動作可能な命令を含むプロセッサ可読媒体が提供され得る。プロセッサによって実行されたとき、これらの命令は、プロセッサに、(a)ネットワークエンティティとの加入者認証を実行すること、(b)ネットワークエンティティとのデバイスのデバイス認証を実行すること、(c)加入者認証とデバイス認証とをバインドするセキュリティ鍵を生成すること、および/または(d)デバイスとサービングネットワークとの間の通信をセキュアにするためにセキュリティ鍵を使用することを行わせ得る。
【００１７】
別の態様によれば、ネットワークエンティティにおいて動作可能な方法が提供される。ネットワークエンティティはデバイスから接続要求を受信し得、接続要求はデバイスのデバイス認証能力の指示を含む。ネットワークエンティティはデバイスとの加入者認証を実行し得る。同様に、ネットワークエンティティはデバイスのデバイス認証を実行し得る。次いで、加入者認証とデバイス認証とをバインドするセキュリティ鍵がネットワークエンティティによって生成され得る。セキュリティ鍵は、次いで、ネットワークエンティティとデバイスとの間の通信をセキュアにするために使用され得る。セキュリティ鍵のオーバージエア送信を防ぐために、セキュリティ鍵は、デバイスとネットワークエンティティと

によって別々に生成され得ることに留意されたい。

【００１８】

一例では、加入者認証は、ネットワークエンティティとデバイスとの間の認証鍵一致交換に基づき得る。デバイス認証は、ネットワークエンティティとデバイスとの間の質問応答交換に基づき得る。

【００１９】

一実装形態では、デバイス認証は、(a)デバイスから証明書を受信することと、(b)デバイスに関連する証明書が取り消されていないことを検証することとを含み得る。

【００２０】

一実装形態では、デバイス認証プロセス中のスヌーピングを防ぐために、デバイス認証は、早期の加入者認証中に生成された少なくとも1つの鍵によってセキュアにされ得る。

【００２１】

様々な例によれば、加入者認証とデバイス認証とは、複合メッセージ交換において同時に実行され得るか、または加入者認証は、デバイス認証とは別の、早期のセキュリティ交換において実行される。

【００２２】

別の例では、セキュリティ鍵は、少なくとも、加入者認証から取得された第1の鍵と、デバイス認証から取得された第2の鍵とに応じて生成され得る。

【００２３】

一実装形態では、ネットワークエンティティは、サービス契約の一部として加入者固有鍵を取得し得、加入者固有鍵は加入者認証のために使用される。同様に、ネットワークエンティティは、デバイスのためのデバイス固有鍵を取得し得、デバイス固有鍵はデバイス認証のために使用される。

【００２４】

一実装形態では、ネットワークエンティティは、処理回路に結合された通信インターフェースを含み得る。処理回路は、(a)デバイスとの加入者認証を実行すること、(b)デバイスのデバイス認証を実行すること、(c)加入者認証とデバイス認証とをバインドするセキュリティ鍵を生成すること、および/または(d)ネットワークエンティティとデバイスとの間の通信をセキュアにするためにセキュリティ鍵を使用することを行うように適応され得る。

【００２５】

一実装形態では、ネットワークエンティティ上で動作可能な命令を含むプロセッサ可読媒体が提供される。プロセッサによって実行されたとき、これらの命令は、プロセッサに、(a)デバイスとの加入者認証を実行すること、(b)デバイスのデバイス認証を実行すること、(c)加入者認証とデバイス認証とをバインドするセキュリティ鍵を生成すること、および/または(d)ネットワークエンティティとデバイスとの間の通信をセキュアにするためにセキュリティ鍵を使用することを行わせ得る。

【図面の簡単な説明】

【００２６】

【図１】様々なタイプのワイヤレスデバイスがサービスを取得するためにコアネットワークによって認証され得るワイヤレス通信システムを示すブロック図である。

【図２】デバイス認証と加入者認証とをバインドすることの一般的な手法を示す図である。

【図３Ａ】加入者認証に基づく鍵階層がデバイス認証を追加するためにどのように変更され得るかの一例を示す図である。

【図３Ｂ】加入者認証に基づく鍵階層がデバイス認証を追加するためにどのように変更され得るかの一例を示す図である。

【図４】パケット交換ネットワークにおいて動作するデバイス中に実装され得る例示的なプロトコルスタックを示す図である。

【図５】図3および図4に示した様々な認証および/またはセキュリティ鍵が生成され得る

ネットワークシステムを示すブロック図である。
【図６】加入者認証とデバイス認証とをバインドするように適応され得るワイヤレスデバイスの選択構成要素を示すブロック図である。
【図７】加入者認証とデバイス認証とをバインドするセキュリティ鍵を生成するための、ワイヤレスデバイスにおいて動作可能な方法の一例を示す流れ図である。
【図８】加入者認証とデバイス認証とをバインドするように適応され得るネットワークエンティティの選択構成要素を示すブロック図である。
【図９】加入者認証とデバイス認証とをバインドするセキュリティ鍵を生成するための、ネットワークエンティティにおいて動作可能な方法の一例を示す流れ図である。
【図１０】加入者認証とデバイス認証とをバインドすることによってセキュリティ鍵を生成するための第1の例示的な方法を示す図である。
【図１１】加入者認証とデバイス認証とをバインドすることによってセキュリティ鍵を生成するための第2の例示的な方法を示す図である。
【図１２】加入者認証とデバイス認証とをバインドすることによってセキュリティ鍵を生成するための第3の例示的な方法を示す図である。
【発明を実施するための形態】
【００２７】
以下の説明では、説明した実装形態を完全に理解することができるように具体的な詳細を与える。ただし、様々な実装形態はこれらの具体的な詳細なしに実施され得ることを当業者は理解されよう。たとえば、実装形態を不要な詳細で不明瞭にしないように回路をブロック図で示すことがある。他の場合には、説明した実装形態を不明瞭にしないように、よく知られている回路、構造および技法を詳細に示すことがある。
【００２８】
「例示的」という単語は、本明細書では、「例、事例、または例示の働きをすること」を意味するために使用する。本明細書に「例示的」と記載されたいかなる実装形態または実施形態も、必ずしも他の実施形態または実装形態よりも好ましいまたは有利であると解釈されるべきではない。同様に、「実施形態」という用語は、すべての実施形態が、論じられた特徴、利点または動作モードを含むことを必要としない。
【００２９】
概観
デバイス(たとえば、クライアントデバイスまたはアクセス端末)とネットワークエンティティとの間の認証方法を提供する。リムーバブルストレージデバイスがデバイスに結合され得、加入者認証のために使用され得る加入者固有鍵を記憶する。セキュアストレージデバイスがデバイスに結合され得、デバイス認証のために使用されるデバイス固有鍵を記憶する。デバイスとネットワークエンティティとの間で加入者認証が実行され得る。また、ネットワークエンティティとのデバイスのデバイス認証が実行され得る。次いで、加入者認証とデバイス認証とをバインドするセキュリティ鍵が生成され得る。すなわち、加入者認証プロセスからの鍵、データ、および/または情報と、デバイス認証プロセスからの鍵、データ、および/または情報とが、(複合)セキュリティ鍵を生成するために組み合わされ得る。セキュリティ鍵は、デバイスとサービングネットワークとの間の通信をセキュアにするために使用され得る。
【００３０】
例示的なネットワーク環境
図1は、様々なタイプのワイヤレスデバイスがサービスを取得するためにコアネットワークによって認証され得るワイヤレス通信システムを示すブロック図である。このワイヤレス通信システムは、たとえば、Universal Mobile Telecommunications System(UMTS)対応ネットワークまたは互換ネットワークあるいはGlobal System for Mobile communication(GSM（登録商標）)互換ネットワークまたはGlobal System for Mobile communication(GSM（登録商標）)互換ネットワークであり得る。本明細書で説明する例のいくつかはLong Term Evolution(LTE)ネットワークに関し得るが、本明細書で説明する様々な特徴は他の

ネットワークにおいても実装され得る。

【００３１】

システムは、アクセスノード106と通信する、アクセス端末103/104およびリレーノード102などの1つまたは複数のデバイス101を含み得る。リレーノード102は、ワイヤレス通信ネットワーク106/108と1つまたは複数のアクセス端末104との間のワイヤレス送信を可能にし得る。ワイヤレス通信システム(たとえば、Long Term Evolution(LTE)ネットワーク、LTE-Advancedネットワークなど)は、コアネットワーク108と1つまたは複数のアクセスノード106とを含み得る。アクセスノード106は、バックホールリンク(たとえば、ワイヤード接続)を介してコアネットワーク108に結合され得る。コアネットワーク108は、たとえば、モバイル管理エンティティ(MME)110、ホーム加入者サーバ(HSS)112および/または他の構成要素を含み得る。

【００３２】

一例では、モバイル管理エンティティ(MME)110は、(以下で総称的に「デバイス」と呼ぶ)デバイス101、リレーノード102、および/またはアクセス端末103/104のためのベアラアクティブ化/非アクティブ化と、ホーム加入者サーバ(HSS)112と対話することによって認証を支援することとに関与し得る。MME110はまた、一時識別情報を生成し、および/またはそれをデバイス(たとえば、デバイス101、リレーノード102、アクセス端末103/104など)に割り振り得る。MME110は、サービスプロバイダのパブリックランドモバイルネットワーク(PLMN)にキャンプオンする(たとえば、そこからサービスを取得する、それに接続する、それとの通信リンクをセットアップする)ためのデバイスの許可を検査し得、デバイスのローミング制限をエンフォースし得る。MME110は、非アクセス層(NAS)シグナリングの暗号化/完全性保護のためのネットワーク中の終端点であり得、セキュリティ鍵管理を扱う。MME110はまた、コアネットワーク108に結合されたデバイスのために、(再送信を含む)トラックおよび/またはページングプロシージャを実行し得る。

【００３３】

ホーム加入者サーバ(HSS)112は、デバイスを実際に扱うネットワークエンティティをサポートするマスタ加入者データベースである。HSS112は、サブスクリプション関係情報(加入者プロファイル)を含み得、サブスクリプションの認証および許可を実行するのを助け得、加入者のロケーションに関する情報を提供することができる。HSS112は、GSM（登録商標）ホームロケーションレジスタ(HLR)および認証センター(AuC)と同様である。ホームロケーションレジスタ(HLR)は、コアネットワークを使用することを許可される各加入者の詳細を含んでいるデータベースであり得る。HLRは、AuCが加入者(すなわち、ユーザ端末を使用する加入者)を認証するのを支援し得る。

【００３４】

リレーノード102は、アクセス端末104とアクセスノード106との間の信号を増幅および/または反復するように適応され得る。概して、リレーノード102は、アクセス端末104にはアクセスノード(AN)のように見え得、アクセスノード106にはアクセス端末(AT)のように見え得る。たとえば、リレーノード102は、アクセスノード106と通信するためのアクセス端末インターフェース105を含み得、アクセス端末104と通信するためのアクセスノードインターフェース107をも含み得る。すなわち、アクセス端末インターフェース105は、リレーノードをアクセスノード106にはアクセス端末のように見えるようにし得る。同様に、アクセスノードインターフェース107は、リレーノード102をアクセス端末104にはアクセスノードのように見えるようにし得る。いくつかの実装形態では、リレーノード102は、アクセス端末インターフェース105とアクセスノードインターフェース107との間で第1のフォーマットから第2のフォーマットに信号を変換し得る。リレーノード102は、アクセス端末104がアクセスノード106と直接通信するのではなく、リレーノード102と通信することができるように、セルのエッジの近くに配置され得る。

【００３５】

無線システムにおいて、セルは、受信および送信カバレージの地理的エリアである。セルは互いと重複することができる。典型的な例では、各セルに関連する1つのアクセスノ

ードがある。セルのサイズは、周波数帯域、電力レベル、およびチャネル状態などのファクタによって判断される。リレーノード102などのリレーノードは、セル内のまたはセルの近くのカバレージを向上させるため、またはセルのカバレージのサイズを拡張するために使用され得る。さらに、アクセス端末104は、アクセス端末104がセルのためのアクセスノード106と直接通信するときに使用し得るよりも高いデータレートまたは低い送信電力でリレーノード102にアクセスすることができるので、リレーノード102の使用は、そのセル内の信号のスループットを向上させることができる。より高いデータレートでの送信は、より高いスペクトル効率を生じ、より低い電力での送信は、たとえば、バッテリー電力をより少なく消費することによってアクセス端末104に利益を与える。

【００３６】

いくつかの例では、リレーノード102は、レイヤ1リレーノード、レイヤ2リレーノード、および/またはレイヤ3リレーノードの3つのリレータイプのうちの1つとして実装され得る。レイヤ1リレーノードは、本質的に、増幅およびわずかな遅延以外の変更なしに送信を再送信することができるリピータである。レイヤ2リレーノードは、それが受信した送信を復号し、復号の結果を再符号化し、次いで、再符号化されたデータを送信することができる。レイヤ3リレーノードは、完全な無線リソース制御能力を有することができ、したがって、アクセスノードと同様に機能することができる。リレーノードによって使用される無線リソース制御プロトコルは、アクセスノードによって使用されるものと同じであり得、リレーノードは、一般にアクセスノードによって使用される一意のセル識別情報を有し得る。本開示では、リレーノード102は、リレーノード102が電気通信システム(たとえば、ネットワーク108)中の他の構成要素にアクセスするために少なくとも1つのアクセスノード106(およびそのアクセスノードに関連するセル)または他のリレーノードの存在に依拠し得ることによって、アクセスノード106と区別される。すなわち、リレーノード102は、ネットワークには加入者デバイス、クライアントデバイス、またはアクセス端末のように見え得、したがって、リレーノード102は、ネットワーク108上で通信するためにアクセスノードに接続する。しかしながら、他の加入者デバイス、ユーザデバイス、および/またはアクセス端末104には、リレーノード102はネットワークデバイス(たとえば、アクセスノード)のように見え得る。したがって、リレーノード102は、アクセスノードならびに/あるいは1つまたは複数のアクセス/加入者/ユーザ端末と通信するための1つまたは複数の通信インターフェースを実装し得る。一例では、リレーノード102は、それのアクセスノードならびに/あるいは1つまたは複数のアクセス端末と通信するために、(たとえば、1つまたは複数のワイヤレスチャネルにおける)同じ送信機/受信機を使用し得る。別の例では、リレーノード102は、アクセスノードならびに/あるいは1つまたは複数のアクセス端末と通信するために、2つ以上の異なる送信機/受信機を利用し得る。

【００３７】

ネットワークサービスにアクセスするためのサブスクリプションの悪用を低減するために、デバイスは、デバイス認証を加入者認証とバインドし得る。デバイス認証は、たとえば、デバイスに着脱可能に結合されたユニバーサル集積回路カード(UICC)109、111、113、および116またはユニバーサル加入者識別情報モジュール(たとえば、USIM)に記憶された(加入者ルート鍵Kなどの)証明に基づく標準3GPP AKA(認証および鍵一致)アクセス認証に関連して動作し得る。いくつかの実施形態では、デバイス認証は、AKA認証のために使用される同じ非アクセス層(NAS)メッセージ中で行われ得る。このようにして、デバイス(たとえば、リレーノード102、アクセス端末103/104など)は、他者が無許可デバイスにおいてそれの加入者証明(すなわち、サブスクリプションサービスのための加入者証明)を使用することを防ぐために、それのサブスクリプション(すなわち、コアネットワーク108とのサービスサブスクリプション)にバインドされ得る。

【００３８】

加入者証明の無許可使用の危険への1つのソリューションは、デバイス(たとえば、デバイス101、リレーノード102またはアクセス端末103/104)とUICC109とが(たとえば、ホストデバイスとUICCとの間のセキュアなチャネルを使用して)互いを相互に認証することであ

るが、それは、UICC109、111、113、および116および/またはホストデバイス(たとえば、デバイス101、リレーノード102またはアクセス端末103/104)に、そのような相互認証を実行するための情報を事前プロビジョニングすることを必要とし得る。

【００３９】

別のソリューションは、ネットワークアクセスのために使用される鍵(たとえば、デバイスとネットワークとの間のトラフィックを保護するために使用される鍵)が、UICC109、111、113、および116に記憶された証明、ならびにデバイス(たとえば、デバイス101、リレーノード102またはアクセス端末103/104)に記憶された証明の両方に依存することを必要とすることであり得る。これは、何らかの方法でAKA認証鍵をデバイス認証とバインドすることによって達成され得る。このソリューションは、(たとえば、事業者が、それらのネットワークに無許可デバイスが接続するのを阻止することを可能にし得る)国際モバイル機器識別情報(IMEI)認証の場合にも有用である。これは、ネットワークアクセスのために使用されるAKA認証から生じる鍵を、デバイス認証のために使用される鍵とバインドすることによって、デバイスからネットワーク108に発信するすべてのメッセージが、認証されたデバイスから実際発信することが保証されるからである。バインドされた鍵(および、バインドされた鍵から導出されたすべての他の後続の鍵)がデバイス(たとえば、デバイス101、リレーノード102、またはアクセス端末103/104)にセキュアに記憶されるという仮定の下で、AKA認証からの鍵とデバイス認証とのバインディングは、デバイス認証のために質問/応答ベースの機構を単独で使用するよりも強いセキュリティを与える。デバイス認証のために質問/応答機構を単独で使用することは、デバイスが認証応答を生成するために存在したことを証明するにすぎず、デバイスがその後の時間に存在したままであることは証明しない。

【００４０】

図2に、デバイス認証と加入者認証とをバインドすることの一般的な手法を示す。デバイス202(たとえば、デバイス101、リレーノード102またはアクセス端末103/104)は、コアネットワーク108とのサブスクリプションを認証すること、および/またはデバイス202に送られた暗号化トラフィックにアクセスするために使用されるセキュリティ鍵を生成することのために使用され得るsubscriber_root_key206および/またはsubscriber_identity207をプロビジョニングされ得る。subscriber_root_key206は、subscriber_identity207に一意に関連し得る。一例では、subscriber_root_key206および/またはsubscriber_identity207はUICC204に記憶され得、および/または加入者認証はUICC204によって処理され得る。同様に、デバイス202は、コアネットワーク108に関してデバイスを認証するために使用され得るdevice_root_key208および/またはdevice_identity209をプロビジョニングされ得る(またはそれらを記憶する)。device_root_key208は、device_identity209に一意に関連し得る。

【００４１】

一例では、device_identity209は、デバイス202(たとえば、デバイス101、リレーノード102またはアクセス端末103/104)の国際モバイル機器識別情報(IMEI)であり得るが、デバイスに関連する他の形態の識別情報(たとえば、EUI-48またはEUI-64などのIEEEハードウェアアドレス)も使用され得る。

【００４２】

いくつかの実装形態では、device_root_key208は、デバイス202によってコアネットワーク108のみと共有され、オーバージエアで送信されない秘密鍵であり得る。device_identity209は、デバイス202がデバイス認証において使用すべき正しいdevice_root_keyを取得することができるように、デバイス202によってコアネットワーク108に送信され得る。代替的に、device_root_key208は、デバイス認証のために証明書が使用される場合、公開/秘密鍵ペアの公開鍵であり得る。たとえば、デバイスは、ネットワークから、公開鍵で暗号化された何らかのデータを受信し得る。次いで、デバイスは、それの秘密鍵を使用して暗号化データを解読し、その後、デバイスがデータの知識を有することをネットワークに証明し得る。証明書(たとえば、device_credentials)はコアネットワーク108によって

検証され得る。デバイス202の関連する秘密鍵は、デバイス202にセキュアに記憶され得る。device_credentialsは、デバイス証明書またはそれへのポインタのいずれかを参照し得る。これらのdevice_credentialsは、関係するネットワークエンティティがdevice_challengeを形成することと、デバイス202の取消しステータスを検査する(たとえば、デバイスに関連する秘密鍵または共有鍵などの証明が損なわれたかどうかを検査する)こととを可能にし得る。さらに、(3GPP技術仕様33.320において定義されている信頼環境またはTrEなどの)デバイスのセキュアな部分が、証明書に関連するdevice_root_keyおよび/または秘密鍵などの機密性の高いデバイス鍵を記憶すると仮定する。さらに、これらの鍵を利用するすべての暗号動作をTrEが実行すると仮定する。

【００４３】

初めに、デバイス202とネットワーク108との間で加入者認証が行われ得る。たとえば、デバイス202とネットワーク108との間の認証および鍵一致(AKA)交換210は、鍵K_ASMEを確立することを生じ得る。そのようなAKA交換210は、たとえば、デバイス202に関連する加入者を認証するために、subscriber_root_key206および/またはsubscriber_identity207に基づき得る。たとえば、そのようなサブスクリプション情報または証明は、ホストデバイス202に着脱可能に結合されたUICC204にセキュアに記憶され得る。

【００４４】

ネットワーク108はまた、デバイス202に対してデバイス認証を実行し得る。コアネットワーク108が正しい対応するdevice_root_key208をルックアップまたは取得することができるように、デバイス202によってdevice_identity209がコアネットワーク108に与えられ得る。ネットワーク108はdevice_challenge212を作成し得、それを(たとえば、関係するNASメッセージの一部として)デバイス202に送る。それに応答して、デバイス202は、(たとえば、device_challengeとdevice_root_key208またはそれの導関数とに基づいて)device_response214を計算し、それをネットワーク108に返信する。デバイス202は、device_challengeおよびdevice_response中のデータを使用して、複合セキュリティ鍵K_ASME_D216を計算し得る。デバイス202の場合、複合セキュリティ鍵K_ASME_D216は、device_response214が送られる前または後のいずれかに生成され得ることに留意されたい。一例では、複合セキュリティ鍵K_ASME_Dは、device_identity209と、K_ASME鍵などのAKA認証から生じる鍵とにバインドされることを除いて、3GPP技術仕様33.401において定義されているEvolved Universal Terrestrial Radio Access Network(E-UTRAN)において定義されているセキュリティ鍵K_ASMEに等価な鍵であり得る。ネットワーク108が有効なdevice_responseを受信した場合、ネットワーク108も複合セキュリティ鍵K_ASME_D218を計算する。

【００４５】

device_challenge212、device_response214および複合セキュリティ鍵K_ASME_Dの計算は、以下の通りであり得る。device_challenge212は、次のように計算され得る。

device_challenge=eKSI,[E_device_root_key(device_temp_key)],network_nonce

上式で、eKSIは、K_ASME_Dに関連することになる発展/拡張型鍵セット識別子であり、[..]は、随意のパラメータを示し、E_k(データ)は、鍵kで暗号化されたデータを意味し、network_nonceは、ネットワークによって選定された好適なサイズ(たとえば、128ビット)の乱数である。暗号化アルゴリズムは、非対称(device_root_keyがデバイス証明書に関連する公開鍵である場合)または対称(device_root_keyが共有鍵である場合)のいずれかであり得る。device_temp_keyは、デバイス認証の一部として取得または生成される鍵であり得る。一例では、device_temp_keyは、ネットワーク108によって(たとえば、ランダムに)選定され得、暗号化形態でデバイス202に送られ、適切な長さ(たとえば、256または128ビット値)である。

【００４６】

デバイス202とネットワーク108の両方は、最適化目的でネットワークアクセス間にdevice_temp_keyを保持し得る。そうでない場合、device_challenge212中の第2のパラメータ([E_device_root_key(device_temp_key)])は随意ではない。

【００４７】

device_response214は、次のように計算され得る。
device_response=device_nonce,device_res
上式で、device_nonceは、デバイスによって選定された好適なサイズ(たとえば、128ビット)の乱数であり、
device_res=KDF(device_temp_key,network_nonce,device_nonce)であり、
ただし、KDFは、応答device_resを生成するのに好適な暗号関数である。

【００４８】

(たとえば、AKA交換210の一部として)認証鍵K_ASMEを前もって取得した後、複合セキュリティ鍵K_ASME_D216および218の計算(すなわち、デバイス認証と加入者認証とをバインドすること)は、次のように行われ得る。
K_ASME_D=KDF(device_temp_key,K_ASME,network_nonce,device_nonce)
上式で、K_ASMEは、(AKA認証交換210の結果として)デバイスとネットワークとの間の加入者認証中に取得された鍵または値であり得る。一例では、K_ASME鍵は、デバイス202とネットワーク108との間で前に生成および/または使用された鍵であり得る。代替的に、デバイス認証プロセス212および214が、AKAプロシージャ210のために使用されるNASメッセージと同じNASメッセージを使用して実行されている場合、K_ASME鍵は、新たにまたは同時に生成され得る。同様に、device_temp_keyは、デバイス202とネットワーク108との間のデバイス認証中に取得された鍵または値であり得る。

【００４９】

複合セキュリティ鍵は、次いで、追加のセキュリティ鍵217および219を計算するための基礎および/またはルートとして使用され得る。追加のセキュリティ鍵は、たとえば、NASレベルおよび/またはASレベル通信をセキュアにするのに役立ち得る。

【００５０】

複合セキュリティ鍵K_ASME_D、関連するセキュリティパラメータ、およびK_ASME_Dから導出されたすべての鍵は、デバイス202上にセキュアに保持され得、UICC204には記憶されない。複合セキュリティ鍵K_ASME_Dは、次いで、デバイス202とコアネットワーク108との間で交換されるメッセージ220をセキュアにするために使用され得る。

【００５１】

(図3Aと図3Bとからなる)図3に、加入者認証に基づく鍵階層がデバイス認証をも含むためにどのように変更され得るかの一例を示す。鍵階層は、デバイスとネットワークとの間の通信を暗号化/解読する際に使用するセキュリティパラメータ(たとえば、セキュリティ鍵)を確立するために実装され得る。この例では、加入者およびデバイス認証は、デバイス322とネットワークエンティティ324との間で実行され得る。デバイス322は、たとえば、アクセス端末(AT)、ユーザ機器(UE)、モバイルフォン、および/またはリレーノードであり得る。ネットワークエンティティ324は、モビリティ管理エンティティ(MME)および/またはホーム加入者サーバ(HSS)などの1つまたは複数のネットワークデバイスであり得る。

【００５２】

この例は、加入者認証に基づく第1の鍵階層300が、加入者認証とデバイス認証の両方に基づく第2の鍵階層300'を取得するためにどのように変更されるかを示す。

【００５３】

第1の鍵階層300に示す加入者認証のために、ユニバーサル集積回路カード(デバイス322中のUICC)およびネットワークエンティティ324(たとえば、図1におけるMME110、HSS112、または他のネットワークエンティティ)は、マスタ鍵K302を使用して、暗号鍵(CK)304と完全性鍵(IK)306とを生成し得る。次いで、デバイス322およびネットワークエンティティ324は、認証および鍵一致(AKA)交換の一部として暗号鍵(CK)304と完全性鍵(IK)306とを使用して、(本明細書では加入者認証鍵とも呼ぶ)アクセスセキュリティ管理エンティティ鍵K_ASME308を生成し得る。デバイス202のセキュリティアクティブ化は、認証および鍵一致プロシージャ(AKA)、非アクセス層(NAS)セキュリティモード構成(NAS SMC)プロシージャおよびアクセス層(AS)セキュリティモード構成(AS SMC)プロシージャを通して達成され得る

。

【００５４】

この例では、加入者認証は、K_ASME308を生じるAKA交換326を含み得る。AKA交換326は、加入者認証要求340と加入者認証応答342とを含み得る。この例では、K_ASME鍵308を生成する加入者認証プロセスは、関連するNASレベル鍵(たとえば、K_NAS-enc305およびK_NAS-int311)および/またはASレベル鍵(たとえば、K_UP-enc315、K_RRC-enc317、およびK_RRC-int319)をも生成し得る。いくつかの実装形態では、NASレベル鍵およびASレベル鍵のこれらのバージョンが使用されない場合、これらの鍵の生成は、加入者認証中に控えられ得ることに留意されたい。

【００５５】

第2の鍵階層300'は、NASレベルおよびASレベルセキュリティ鍵を生成するために、デバイス認証が加入者認証にどのようにバインドされ得るかを示す。加入者認証(およびそれの対応するK_ASME鍵308の生成)と同時に、それより前に、またその後に、デバイス認証328は、デバイス固有ルート鍵に少なくとも部分的に基づいて実行され得る。デバイス認証328は、デバイス認証要求344とデバイス認証応答346とを含み得る。一実装形態では、デバイス認証307は加入者認証とは無関係であり得、加入者認証とデバイス認証の両方が満たされる場合のみ、複合セキュリティ鍵K_ASME_D309が生成される。代替実装形態では、デバイス認証は加入者認証より前に実行され得る。

【００５６】

複合セキュリティ鍵K_ASME_D309は、たとえば、NAS(非アクセス層)鍵310および312と、AS(アクセス層)鍵314、316、318、および320との計算のためのベース鍵として使用され得る。すなわち、デバイス322およびネットワークエンティティ324は、次いで、K_ASME_D鍵309を使用して、1つまたは複数のセキュリティ鍵を生成し得る。

【００５７】

パケット交換ネットワークは複数の階層プロトコルレイヤで構造化され得、下位プロトコルレイヤは上位レイヤにサービスを提供し、各レイヤは異なるタスクを受け持つ。たとえば、図4に、パケット交換ネットワークにおいて動作するデバイス中に実装され得る例示的なプロトコルスタックを示す。この例では、プロトコルスタック402は、物理(PHY)レイヤ404と、媒体アクセス制御(MAC)レイヤ406と、無線リンク制御(RLC)レイヤ408と、パケットデータコンバージェンスプロトコル(PDCP)レイヤ410と、無線リソース制御(RRC)レイヤ412と、非アクセス層(NAS)レイヤ414と、アプリケーション(APP)レイヤ416とを含む。

【００５８】

NASレイヤ414の下のレイヤは、しばしばアクセス層(AS)レイヤ418と呼ばれる。RLCレイヤ408は、1つまたは複数のチャネル420を含み得る。RRCレイヤ412は、接続状態とアイドル状態とを含む、アクセス端末のための様々な監視モードを実装し得る。非アクセス層(NAS)レイヤ414は、通信デバイスのモビリティ管理コンテキスト、パケットデータコンテキストおよび/またはそれのIPアドレスを維持し得る。プロトコルスタック402中に(たとえば、図示のレイヤの上、下、および/または中間に)他のレイヤが存在し得るが、説明のために省略されていることに留意されたい。

【００５９】

図4を参照すると、たとえばRRCレイヤ412および/またはNASレイヤ414において無線/セッションベアラ422が確立され得る。したがって、NASレイヤ414は、図3に示したセキュリティ鍵K_NAS-enc310とK_NAS-int312とを生成するために、デバイス202およびコアネットワーク108によって使用され得る。同様に、RRCレイヤ412は、アクセス層(AS)セキュリティ鍵K_UP-enc316とK_RRC-enc318とK_RRC-int320とを生成するために、デバイス202およびアクセスノード108によって使用され得る。セキュリティ鍵K_UP-enc316、K_RRC-enc318、およびK_RRC-int320はRRCレイヤ412において生成され得るが、これらの鍵は、シグナリングおよび/またはユーザ/データ通信をセキュアにするためにPDCPレイヤ410によって使用され得る。たとえば、鍵K_UP-enc316は、ユーザ/データプレーン(UP)通信をセキュアにす

るためにPDCPレイヤ410によって使用され得、鍵K_RRC-enc318およびK_RRC-int320は、PDCPレイヤ410においてシグナリング(すなわち、制御)通信をセキュアにするために使用され得る。

【００６０】

暗号化および完全性アルゴリズムのために使用されるこれらのセキュリティ鍵の導出において、AS(ユーザプレーンおよびRRC)とNASの両方は、個々のアルゴリズム識別情報が入力のうちの1つとして与えられることを必要とする。ASレベルにおいて、使用されるべきアルゴリズムは、無線リソース制御(RRC)セキュリティモードコマンドによって与えられる。

【００６１】

図5は、図3および図4に示した様々な認証および/またはセキュリティ鍵が生成され得るネットワークシステムを示すブロック図である。ここで、デバイス322は、様々なレイヤ(たとえば、APP、NAS、RRC、RLC、MAC、およびPHY)を含む通信スタックを実装し得る。アクセスネットワーク504(たとえば、図1におけるアクセスノード106)は、デバイス322がネットワーク108と通信し得るように、デバイス322にワイヤレス接続性を与え得る。ホーム加入者サーバ506およびデバイス322は、両方とも、暗号鍵(CK)および/または完全性鍵(IK)を生成または取得するために使用され得るルート鍵(K)を知っているかまたはそれへのアクセスを有し得る。デバイス322および/またはHSS506は、次いで、暗号鍵(CK)および/または完全性鍵(IK)を使用して、アクセスセキュリティ管理エンティティ鍵K_ASMEを生成し得る。また、デバイス認証を実行し、K_ASME鍵と組み合わせてまたはそれに基づいて複合セキュリティ鍵K_ASME_Dを生成し、それにより、加入者認証とデバイス認証とを組み合わせて1つの鍵にし得る。K_ASME_D鍵を使用して、デバイス322およびモビリティ管理エンティティ(MME)510は、次いで、鍵K_NAS-encとK_NAS-intとを生成し得る。デバイス322およびMME510はまた、アクセスネットワーク固有鍵K_eNB/NHを生成し得る。このアクセスネットワーク固有鍵K_eNB/NHを使用して、デバイス322およびアクセスネットワーク504は、鍵K_UP-encとK_RRC-encとK_RRC-intとを生成し得る。

【００６２】

これらの鍵の導出に関する詳細は、参照により本明細書に組み込まれる、(3GPP TS33.401として知られる)3GPP STD-T63-33.401「System Architecture Evolution (SAE): Security Architecture」リリース8において与えられている。図3～図5では、デバイスおよび加入者認証とバインディングとが実装され得る特定の環境/コンテキストについて説明しているが、これは、様々な他のタイプのネットワークにおいて実装され得るこの特徴を限定するものではないことに留意されたい。

【００６３】

例示的なワイヤレスデバイス

図6は、加入者認証とデバイス認証とをバインドするように適応され得るワイヤレスデバイス600の選択構成要素を示すブロック図である。ワイヤレスデバイス600は、概して、1つまたは複数のワイヤレス通信インターフェース604に結合された処理回路602を含む。たとえば、ワイヤレスデバイス600はリレーノードおよび/またはアクセス端末であり得る。

【００６４】

処理回路602は、データを取得し、処理しおよび/または送ることと、データアクセスおよびストレージを制御することと、コマンドを発行することと、他の所望の動作を制御することとを行うように構成され得る。処理回路602は、少なくとも1つの実施形態では、適切なメディアによって与えられる所望のプログラミングを実装するように構成された回路を含み得る。たとえば、処理回路602は、たとえば、ソフトウェアおよび/またはファームウェア命令、および/またはハードウェア回路を含む実行可能命令を実行するように構成された、プロセッサ、コントローラ、複数のプロセッサおよび/または他の構造のうちの1つまたは複数として実装され得る。処理回路602の実施形態は、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲー

トアレイ(FPGA)または他のプログラマブル論理構成要素、個別ゲートまたはトランジスタ論理、個別ハードウェア構成要素、あるいは本明細書で説明する機能を実行するように設計されたそれらの任意の組合せを含み得る。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、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、または状態機械であり得る。プロセッサは、DSPとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つまたは複数のマイクロプロセッサ、あるいは任意の他のそのような構成など、コンピューティング構成要素の組合せとしても実装され得る。処理回路602のこれらの例は説明のためのものであり、本開示の範囲内の他の好適な構成も企図される。

【００６５】

ワイヤレス通信インターフェース604は、ワイヤレスデバイス600のワイヤレス通信を可能にするように構成され得る。たとえば、通信インターフェース604は、アクセス端末、アクセスノード、他のリレーノードなど、他のワイヤレスデバイスに対して情報を双方向に通信するように構成され得る。通信インターフェース604はアンテナ(図示せず)に結合され得、ワイヤレス通信のための少なくとも1つの送信機および/または少なくとも1つの受信機(たとえば、1つまたは複数の送信機/受信機チェーン)を含むワイヤレストランシーバ回路を含み得る。

【００６６】

処理回路602は、加入者およびデバイス認証バインディングモジュール610を含み得る。加入者およびデバイス認証モジュール610は、加入者セキュリティ証明(たとえば、ユニバーサル集積回路カード608に記憶された加入者固有鍵607および/または加入者識別情報609)を使用して加入者認証プロシージャを実行するように適応され、デバイス固有証明(たとえば、デバイス固有鍵605および/またはデバイス識別情報611)を使用して(信頼環境606内で)デバイス認証プロシージャを実行し、加入者認証とデバイス認証とを互いにバインドするように適応された、回路および/またはプログラミングを含むことができる。そのような「バインディング」は、加入者認証とデバイス認証の両方からのいくつかの結果を組み合わせることに関与し得る。たとえば、第3の(複合)セキュリティ鍵を取得するために、加入者認証から取得された第1のセキュリティ鍵が、デバイス認証から取得された第2のセキュリティ鍵と組み合わされ得る。

【００６７】

いくつかの実施形態では、ワイヤレスデバイス600は信頼環境(TrE)606を含み得る。信頼環境606は、TS33.320の3GPP仕様詳細における信頼環境のための仕様を満たすように適応され得る。信頼環境606は、少なくともいくつかのセキュリティ証明(たとえば、デバイス固有鍵605および/またはデバイス識別情報611)を事前プロビジョニングされ得る(またはセキュアに組み込まれ得る)。たとえば、信頼環境606は、デバイス認証に関係するセキュリティ証明を有し得る。

【００６８】

いくつかの実施形態では、ワイヤレスデバイス600は、ユニバーサル集積回路カード(UICC)608内でのセキュアな処理を含み得る。UICC608は、ワイヤレスデバイス600に着脱可能に結合され得る。UICC608は、初期認証および鍵一致(AKA)証明などの加入者セキュリティ証明(たとえば、加入者固有鍵607および/または加入者識別情報609)を事前プロビジョニングされ得る。代替的に、セキュアな処理は、汎用加入者識別モジュール(USIM)内で実行され得る。

【００６９】

ワイヤレスデバイス600の1つまたは複数の特徴によれば、処理回路602は、図2～図5、図7、図10、図11、および図12に示す、関係するプロセス、機能、ステップおよび/またはルーチンのいずれかまたはすべてを実行するように適応され得る。処理回路602に関して本明細書で使用する「適応される」という用語は、処理回路602が、本明細書で説明する様々な特徴に従って特定のプロセス、機能、ステップおよび/またはルーチンを実行するように構成、採用、実装、および/またはプログラムされることを指すことがある。

【００７０】
図7は、加入者認証とデバイス認証とをバインドするセキュリティ鍵を生成するための、ワイヤレスデバイスにおいて動作可能な方法の一例を示す流れ図である。ワイヤレスデバイスにデバイス固有鍵を事前プロビジョニングする(702)。たとえば、そのようなデバイス固有鍵は、チップ中に組み込まれるか、またはワイヤレスデバイスの製造中に構成され得る。ワイヤレスデバイスはまた、デバイス固有鍵に関連するデバイス識別子を含み得る。さらに、ワイヤレスデバイスに加入者固有鍵を事前プロビジョニングする(704)。たとえば、そのような加入者固有鍵は、加入者に割り当てられたルート鍵であり得、ワイヤレスデバイスに結合された固定またはリムーバブルモジュール(たとえば、UICCまたはUSIM)内に記憶され得る。ワイヤレスデバイスはまた、加入者固有鍵に関連するサブスクリプション識別情報を含み得る。ワイヤレスデバイスは、(たとえば、加入者固有鍵を使用して)ネットワークエンティティとの加入者認証を実行する(706)。これは、たとえば、ネットワークエンティティとの認証および鍵一致交換を含み得る。ワイヤレスデバイスはまた、(たとえば、デバイス固有鍵を使用して)ネットワークエンティティとのデバイス認証を実行する(708)。同じまたは異なる時間に、同じネットワークエンティティとのまたは異なるネットワークエンティティとの加入者認証とデバイス認証とが実行され得る。次いで、ワイヤレスデバイスはセキュリティ鍵(たとえば、K_ASME_Dなど)を生成し、そのようなセキュリティ鍵は、加入者認証とデバイス認証とをバインドする(710)。たとえば、一例では、デバイス認証からのデータ(たとえば、1つまたは複数の得られた鍵、証明書、識別子など)と、加入者認証からのデータ(たとえば、1つまたは複数の得られた鍵、証明書、識別子など)とが、セキュリティ鍵を生成するために組み合わされ得る。たとえば、図2において、加入者認証210からのK_ASME鍵と、図2におけるデバイス認証からのdevice_temp_keyとは、セキュリティ鍵K_ASME_Dを生成するために組み合わされ得る。次いで、ワイヤレスデバイスとネットワークエンティティとの間のワイヤレス通信をセキュアにするためにセキュリティ鍵を使用する(712)。たとえば、セキュリティ鍵は、ワイヤレスデバイスとネットワークとの間の通信(たとえば、データおよびシグナリング)を暗号化/解読するのに役立ち得る他の鍵および/または証明書(たとえば、NASレベルおよび/またはASレベルセキュリティ鍵)を生成するために使用され得る。

【００７１】
例示的なネットワークエンティティ
図8は、加入者認証とデバイス認証とをバインドするように適応され得るネットワークエンティティ800の選択構成要素を示すブロック図である。ネットワークエンティティ800は、通信インターフェース804に結合された処理回路802を含み得る。処理回路802は、データを取得し、処理しおよび/または送ることと、データアクセスおよびストレージを制御することと、コマンドを発行することと、他の所望の動作を制御することとを行うように構成される。処理回路802は、少なくとも1つの実施形態では、適切なメディアによって与えられる所望のプログラミングを実装するように構成された回路を含み得る。たとえば、処理回路802は、たとえば、ソフトウェアおよび/またはファームウェア命令、および/またはハードウェア回路を含む実行可能命令を実行するように構成された、プロセッサ、コントローラ、複数のプロセッサおよび/または他の構造のうちの1つまたは複数として実装され得る。処理回路802の実施形態は、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)または他のプログラマブル論理構成要素、個別ゲートまたはトランジスタ論理、個別ハードウェア構成要素、あるいは本明細書で説明する機能を実行するように設計されたそれらの任意の組合せを含み得る。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、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、または状態機械であり得る。プロセッサは、DSPとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つまたは複数のマイクロプロセッサ、あるいは任意の他のそのような構成など、コンピューティング構成要素の組合せとしても実装され得る。処理回路802のこれらの例は説明のためのものであり、本開示の範囲内の他の好適な構成

も企図される。

【００７２】

処理回路802は、加入者およびデバイス認証バインディングモジュール806を含む。加入者およびデバイス認証バインディングモジュール806は、加入者セキュリティ証明(たとえば、加入者固有鍵および/または加入者識別子)に基づいてサブスクリプションを認証するための加入者認証プロシージャを実行することと、デバイス固有証明(たとえば、デバイス固有鍵および/またはデバイス識別子)に基づいてデバイスを認証するためのデバイス認証プロシージャを実行することと、セキュリティ鍵を生成するために、デバイス認証と加入者認証とからのデータ(たとえば、鍵、値、証明書など)をバインドすることとを行うように適応された回路および/またはプログラミングを含むことができる。

【００７３】

通信インターフェース804は、リレーノードおよびアクセス端末などの他のデバイスと直接または(たとえば、1つまたは複数の他のネットワークエンティティを通して)間接的に通信するために、ネットワークエンティティ800の通信を可能にするように構成される。

【００７４】

ネットワークエンティティ800の1つまたは複数の特徴によれば、処理回路802は、モバイル管理エンティティ(MME)110およびホーム加入者サーバ(HSS)112などの様々なネットワークエンティティに関係するプロセス、機能、ステップおよび/またはルーチンのいずれかまたはすべてを実行するように適応され得る。さらに、ネットワークエンティティ800は、単一のエンティティ、またはネットワークの2つ以上のエンティティの組合せを含み得る。限定ではなく例として、ネットワークエンティティ800は、特に、モバイル管理エンティティ(MME)、ホーム加入者サーバ(HSS)、デバイス認証サーバを含み得る。処理回路802に関して本明細書で使用する「適応される」という用語は、処理回路802が、本明細書で説明する様々な特徴に従って特定のプロセス、機能、ステップおよび/またはルーチンを実行するように構成、採用、実装、またはプログラムされることのうちの1つまたは複数を指すことがある。

【００７５】

図9は、加入者認証とデバイス認証とをバインドするセキュリティ鍵を生成するための、ネットワークエンティティにおいて動作可能な方法の一例を示す流れ図である。ネットワークエンティティは、ワイヤレスデバイスのためのデバイス固有鍵を取得する(902)。たとえば、そのようなデバイス固有鍵は、チップ中に組み込まれるか、またはワイヤレスデバイスの製造中に構成され得、この情報は、ネットワークエンティティがアクセスすることができるデータベースに記憶され得る。デバイス識別子はデバイス固有鍵に関連し得、デバイスとそれの鍵とを識別するために使用され得る。さらに、ネットワークエンティティは、ワイヤレスデバイスのためのサブスクリプションに関連する加入者固有鍵を取得する(904)。たとえば、そのような加入者固有鍵は、加入者に割り当てられたルート鍵であり得、ワイヤレスデバイスに結合された固定またはリムーバブルモジュール(たとえば、UICCまたはUSIM)内に記憶され得る。ネットワークエンティティは、(たとえば、加入者固有鍵を使用して)ワイヤレスデバイスとの加入者認証を実行する(906)。これは、たとえば、ネットワークエンティティとの認証および鍵一致交換を含み得る。ネットワークエンティティはまた、(たとえば、デバイス固有鍵を使用して)ワイヤレスデバイスとのデバイス認証を実行する(908)。加入者認証とデバイス認証とは、同じまたは異なる時間に実行され得る。次いで、ネットワークエンティティは(複合)セキュリティ鍵(たとえば、K_ASME_Dなど)を生成し、そのようなセキュリティ鍵は、加入者認証とデバイス認証とをバインドする(910)。たとえば、一例では、デバイス認証からのデータ(たとえば、1つまたは複数の得られた鍵、証明書、識別子など)と、加入者認証からのデータ(たとえば、K_ASMEなど)とが、セキュリティ鍵を生成するために組み合わされ得る。次いで、ネットワークエンティティとワイヤレスデバイスとの間のワイヤレス通信をセキュアにするためにセキュリティ鍵を使用する(912)。たとえば、セキュリティ鍵は、ワイヤレスデバイスとネット

ワークとの間の通信を暗号化/解読するのに役立ち得る他の鍵および/または証明書を生成するために使用され得る。

【００７６】

加入者デバイス認証の第1の例示的な方法

図10に、加入者認証とデバイス認証とをバインドすることによってセキュリティ鍵を生成するための第1の例示的な方法を示す。この例では、デバイス1002は、たとえば、リレーノードまたはアクセス端末であり得る。デバイス1102が(たとえば、MME1004とHSS1006とを含む)ワイヤレスネットワークに接続しようとする接続段階中に、デバイス識別情報または他の関係するデバイス情報をオーバージエアであらわにすることは、(たとえば、デバイス1002についての)セキュリティ懸念であり得る。したがって、本方法では、デバイス1002は、デバイス識別情報に対するパッシブ攻撃を防ぐために、ネットワークによってセキュアに要求されるまで、それのデバイス証明(たとえば、国際モバイル機器識別情報(IMEI)などのデバイス固有識別子など)をオーバージエアで提示しない。

【００７７】

デバイスは、デバイス認証が可能であるという指示を含む接続要求1010をネットワークに送ることによって開始し得る。接続要求1010を受信すると、モビリティ管理エンティティ(MME)1004は、(たとえば、デバイス1002のサブスクリプションベースのアカウントまたはユーザに関連する)サブスクリプションおよび認証情報1012をホームサブスクリプションサーバ(HSS)1006に要求し、受信し得る。MME1004は、次いで、AKA認証を実行するために、AKA質問を含む認証要求1014を送る。AKA認証要求1014を受信すると、デバイス1002は、AKA応答を含む認証応答1016を送る。AKA認証要求1014および応答1016は、サブスクリプション認証を実行するのに役立つ。そのようなAKA認証プロシージャにより、加入者認証鍵(たとえば、K_ASME)がデバイス1002およびMMEによって生成されることになり得る。

【００７８】

デバイス認証は、このセキュリティアクティブ化プロセス中の様々な段階において実行され得る。この例では、デバイス認証は、NASレベルセキュリティメッセージ上にピギーバックされ得る。たとえば、MME1004は、デバイス識別情報についての要求(たとえば、IMEIソフトウェアバージョン(IMEISV)についての要求および/またはdevice_credentialsについての要求)を含むNASセキュリティモードコマンド1018を送り得る。それに応答して、デバイス1002は、セキュリティモード完了1020メッセージ内で、デバイス認証が実行されるべきデバイス識別情報または証明を与え得る。送信中にデバイス識別情報または証明をオーバージエアで露出することを回避するために、セキュリティモード完了1020中のデバイス識別情報または証明は、前に計算された加入者認証鍵(たとえば、K_ASME)によってセキュアにされ得ることに留意されたい。デバイス識別情報または証明を受信すると、MME1004は、発展/拡張型鍵セット識別子(eKSI)およびdevice_challengeをもつ識別情報要求1022メッセージを送り得る。eKSIは、生成されるべきK_ASME_Dに関連し得る。したがって、識別情報要求1022中で使用されるeKSIは、たとえば、AKA(すなわち、加入者認証)のために使用された可能性のある他のeKSIとは異なるかまたは別個であり得る。識別情報要求1022メッセージを受信すると、デバイス1002は、device_challengeに基づいてdevice_responseを生成し得、これを識別情報応答1024メッセージの一部として送る。device_responseは、device_challengeとデバイス識別情報または証明とに基づき得る。デバイス1002は、次いで、認証鍵(たとえば、K_ASME)とデバイス認証データ(たとえば、デバイス応答など)とに基づいて、(複合)セキュリティ鍵(K_ASME_D)1025を計算し得る。MME1004は、たとえば、デバイス1002のデバイス識別情報または証明書を使用することと、device_challengeを使用することとによって、device_responseを検査する。デバイス1002がMME1004によって正常に認証された場合、MME1004もセキュリティ鍵(K_ASME_D)1027を生成する。この時点で、デバイス1002とMME1004とは、セキュリティ鍵(K_ASME_D)とそれの関連する識別子eKSIとを共有する。

【００７９】

MME1004は、次いで、セキュリティ鍵(K_ASME_D)に関連する発展/拡張型鍵セット識別子

eKSIをもつセキュリティモードコマンド1026を送り得る。これは、デバイス1002がセキュリティ鍵(K_ASME_D)に基づいて1つまたは複数のセキュリティ鍵を計算することを可能にする。デバイス1002は、セキュリティモード完了1028メッセージをMME1004に送り、それにより、MME1004は、接続完了1030メッセージを送ることが可能になり得る。

【００８０】

加入者デバイス認証の第2の例示的な方法

図11に、加入者認証とデバイス認証とをバインドすることによってセキュリティ鍵を生成するための第2の例示的な方法を示す。この例では、オーバージエア送信におけるデバイス識別情報または証明書(または他の関係する証明情報)をあらわにすることは、セキュリティ懸念ではない。図10の方法とは異なり、この場合、デバイス識別情報をアップフロントで提示することはプライバシー問題または危険につながらないと仮定する。

【００８１】

デバイスは、MMEが受け付けるデバイス識別子または証明(たとえば、IMEI)はすでに有するが、MMEが使用することを望むE-UTRANセキュリティコンテキストは有しない。

【００８２】

デバイス1102は、それのデバイス識別子または証明を含む接続要求1108をMME1104に送る。MME1104は、HSS1106からサブスクリプションおよび認証情報1110を取得し得、たとえば、(サブスクリプション認証のための)AKA質問および/または(デバイス認証のための)デバイス質問を含む認証要求1112を送る。デバイス1102は、AKA応答および/またはデバイス応答を含み得る認証応答1114を送ることによって応答し得ることに留意されたい。AKA応答は、加入者識別子に少なくとも部分的に基づき得る。デバイス応答は、デバイス識別子および/または証明とデバイス質問とに基づき得る。デバイス1104は、次いで、加入者認証情報とデバイス認証情報とを組み合わせることによって(複合)セキュリティ鍵K_ASME_Dを生成し得る。同様に、AKA応答およびデバイス応答の検証が成功すると、MME1104も、加入者認証情報とデバイス認証情報とを組み合わせることによってセキュリティ鍵K_ASME_Dを生成し得る。

【００８３】

MMEは、セキュリティ鍵K_ASME_Dに基づくセキュリティコンテキストを使用して開始するために、セキュリティモードコマンド1116メッセージを送る。デバイス1102は、セキュリティモード完了1118メッセージで応答する。すなわち、デバイス1102およびMME1104は、セキュリティ鍵K_ASME_Dを使用して、1つまたは複数の追加のセキュリティ鍵を生成し得る(あるいは、デバイス1102とMME1104との間の通信をセキュアにし得る)。MME1104は、次いで、接続完了1120メッセージをデバイス1102に送り得る。

【００８４】

ここで、デバイス識別子および/または証明(または前に取得/生成されたデバイス鍵)がサブスクリプション識別子とともにネットワーク中のHSS1106または別のサーバに記憶された場合、デバイス1102は、このフローを使用して接続を実行することができることがわかる。これをそこで行うために、デバイス1102は、それのデバイス識別子および/または証明がHSS1106または他のネットワークサーバから取得され得ることを(たとえば、接続要求1108中で)示し得る。代替的に、MME1104は、(たとえば、何らかの形態のdevice_challengeとともに、IMEIなどのデバイス識別子を含めることによって)device_challengeが特定のデバイス識別子に関連することをデバイス1102に示し得る。このようにして、デバイス1102は、(認証要求1112中の)デバイス質問がそれのデバイス識別子に関連することを知ることができる。

【００８５】

加入者デバイス認証の第3の例示的な方法

図12に、加入者認証とデバイス認証とをバインドすることによってセキュリティ鍵を生成するための第3の例示的な方法を示す。この例では、加入者認証は前に実行されており、したがって、加入者セキュリティコンテキスト1206(たとえば、K_ASME鍵)はすでに存在する。既存のセキュリティコンテキストを置き換えるために、組み合わされた加入者およ

びデバイス認証がネットワークによって開始され得る。この実施形態は、事業者から完全な(full fledged)または使用可能な証明を取得するために、初期AKAベースセキュリティコンテキストを確立することを必要とし得るデバイスにとって有益であり得る。

【００８６】

この手法は、MMEがデバイス識別子(たとえば、IMEI)および/またはdevice_credentialsをすでに知っていると仮定する。

【００８７】

MME1204は、device_challengeを含む認証要求1208をデバイス1202に送る。それに応答して、デバイス1202は、device_responseを含む認証応答1210をMME1204に送る。device_responseは、device_challengeとデバイス識別子および/または証明書とに基づき得る。この時点で、デバイス1202とMME1204の両方は、(たとえば、AKAベースセキュリティコンテキストとデバイス認証情報とに基づいて)(複合)セキュリティ鍵K_ASME_Dを計算するために十分な情報を有し得る。

【００８８】

MME1204は、既存のセキュリティコンテキスト1206を、(たとえば、加入者認証とデバイス認証の両方を組み込む)新しいセキュリティ鍵K_ASME_Dに基づくセキュリティコンテキストと置き換えるために、NASセキュリティモードコマンド1212をデバイス1202に送り得る。それに応答して、デバイス1202は、セキュリティ鍵K_ASME_Dに基づいて新しいセキュリティコンテキストを生成し得、それに応答してNASセキュリティモード完了1214メッセージを送り得る。

【００８９】

本明細書の様々な例は、加入者認証とデバイス認証の両方がMMEを介して実行され得ることを示しているが、MMEとの組合せでまたはMMEの代わりに他のネットワークエンティティがこれらの機能のいくつかを実行し得ることに留意されたい。

【００９０】

図1、図2、図3、図4、図5、図6、図7、図8、図9、図10、図11、および/または図12に示した構成要素、ステップ、特徴および/または機能のうちの1つまたは複数は、単一の構成要素、ステップ、特徴または機能に再構成され、および/または組み合わされ、あるいは、いくつかの構成要素、ステップ、または機能で実施され得る。また、本開示から逸脱することなく追加の要素、構成要素、ステップ、および/または機能が追加され得る。図1、図5、図6および/または図8に示した装置、デバイス、および/または構成要素は、図2、図3、図4、図7および/または図9～図12で説明した方法、特徴、またはステップのうちの1つまたは複数を実行するように構成され得る。本明細書で説明する新規のアルゴリズムは、ソフトウェアでも効率的に実装され得、および/またはハードウェアにも組み込まれ得る。

【００９１】

また、少なくともいくつかの実装形態を、フローチャート、流れ図、構造図、またはブロック図として示されるプロセスとして説明したことに留意されたい。フローチャートは動作を逐次プロセスとして説明することがあるが、動作の多くは並行してまたは同時に実行され得る。さらに、動作の順序は並び替えられ得る。プロセスは、それの動作が完了したときに終了する。プロセスは、方法、関数、プロシージャ、サブルーチン、サブプログラムなどに対応し得る。プロセスが関数に対応するとき、それの終了は呼出し関数またはメイン関数への関数の復帰に対応する。

【００９２】

さらに、実施形態は、ハードウェア、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、またはそれらの任意の組合せによって実装され得る。ソフトウェア、ファームウェア、ミドルウェアまたはマイクロコードで実装されるとき、必要なタスクを実行するためのプログラムコードまたはコードセグメントは、記憶媒体または他のストレージなどの機械可読媒体に記憶され得る。プロセッサは必要なタスクを実行し得る。コードセグメントは、プロシージャ、関数、サブプログラム、プログラム、ルーチン、サブルー

チン、モジュール、ソフトウェアパッケージ、クラス、または命令、データ構造、もしくはプログラムステートメントの任意の組合せを表し得る。コードセグメントは、情報、データ、引数、パラメータ、またはメモリ内容をパスおよび/または受信することによって、別のコードセグメントまたはハードウェア回路に結合され得る。情報、引数、パラメータ、データなどは、メモリ共有、メッセージパッシング、トークンパッシング、ネットワーク送信などを含む好適な手段を介してパス、フォワーディング、または送信され得る。

【００９３】

「機械可読媒体」、「コンピュータ可読媒体」、および/または「プロセッサ可読媒体」という用語は、限定はしないが、ポータブルまたは固定ストレージデバイス、光ストレージデバイス、ならびに命令および/またはデータを記憶、含有または搬送することが可能な様々な他の非一時的媒体を含み得る。したがって、本明細書で説明する様々な方法は、「機械可読媒体」、「コンピュータ可読媒体」、および/または「プロセッサ可読媒体」に記憶され、1つまたは複数のプロセッサ、機械および/またはデバイスによって実行され得る命令および/またはデータによって部分的にまたは完全に実装され得る。

【００９４】

本明細書で開示する例に関して説明した方法またはアルゴリズムは、ハードウェアで、プロセッサによって実行可能なソフトウェアモジュールで、または両方の組合せで、処理ユニット、プログラム命令、または他の指示の形態で直接実施され得、単一のデバイスに含まれるかまたは複数のデバイスにわたって分散され得る。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、または当技術分野で知られている任意の他の形態の記憶媒体中に常駐し得る。記憶媒体は、プロセッサがその記憶媒体から情報を読み取り、その記憶媒体に情報を書き込むことができるようにプロセッサに結合され得る。代替として、記憶媒体はプロセッサと一体であり得る。

【００９５】

さらに、本明細書で開示する実施形態に関して説明する様々な例示的な論理ブロック、モジュール、回路、およびアルゴリズムステップは、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実装され得ることを当業者は諒解されよう。ハードウェアとソフトウェアのこの互換性を明確に示すために、様々な例示的な構成要素、ブロック、モジュール、回路、およびステップについて、上記では概してそれらの機能に関して説明した。そのような機能をハードウェアとして実装するか、ソフトウェアとして実装するかは、特定の適用例および全体的なシステムに課せられた設計制約に依存する。

【００９６】

本明細書で説明する本発明の様々な特徴は、本発明から逸脱することなく様々なシステムで実装され得る。上記の実施形態は例にすぎず、本発明を限定するものと解釈すべきではないことに留意されたい。実施形態の説明は、例示的なものであり、本開示の範囲を限定するものではない。したがって、本教示は、他のタイプの装置、ならびに多くの代替形態、変更形態、および変形形態に容易に適用され得ることが当業者には明らかであろう。

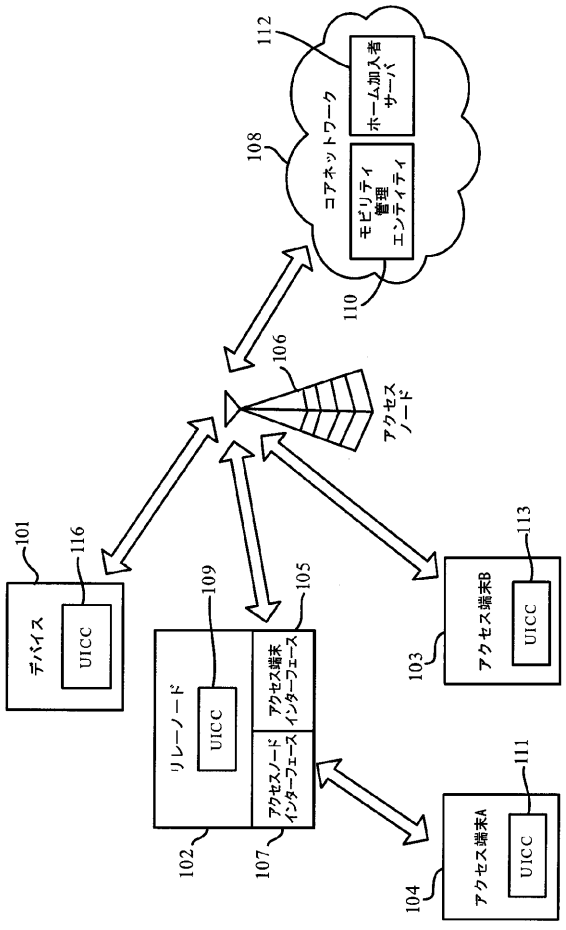
【符号の説明】

【００９７】

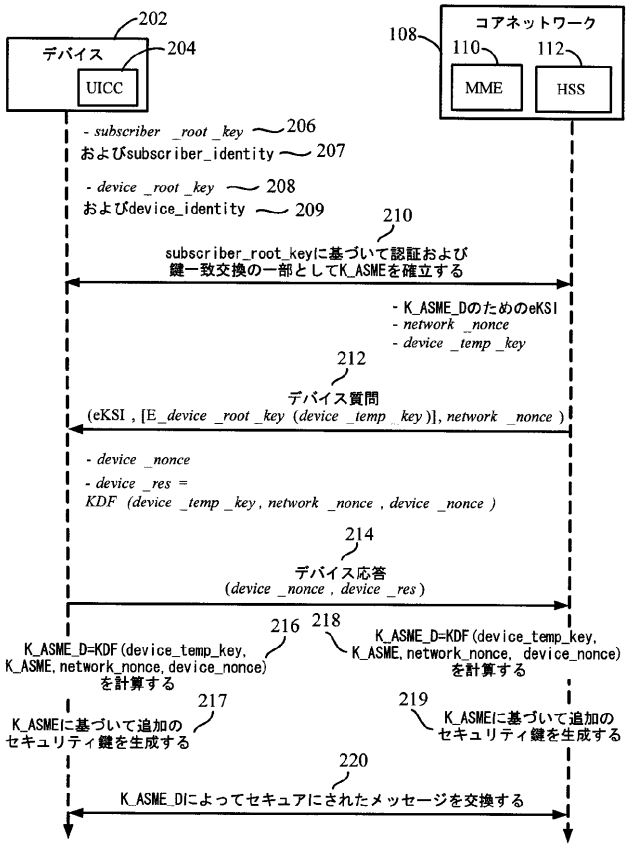
101　デバイス
102　リレーノード
103　アクセス端末A
104　アクセス端末B
105　アクセス端末インターフェース
106　アクセスノード
106　ワイヤレス通信ネットワーク
107　アクセスノードインターフェース
108　コアネットワーク
108　ワイヤレス通信ネットワーク

109　ユニバーサル集積回路カード(UICC)
110　モバイル管理エンティティ(MME)
110　モビリティ管理エンティティ
111　ユニバーサル集積回路カード(UICC)
112　ホーム加入者サーバ(HSS)
113　ユニバーサル集積回路カード(UICC)
116　ユニバーサル集積回路カード(UICC)

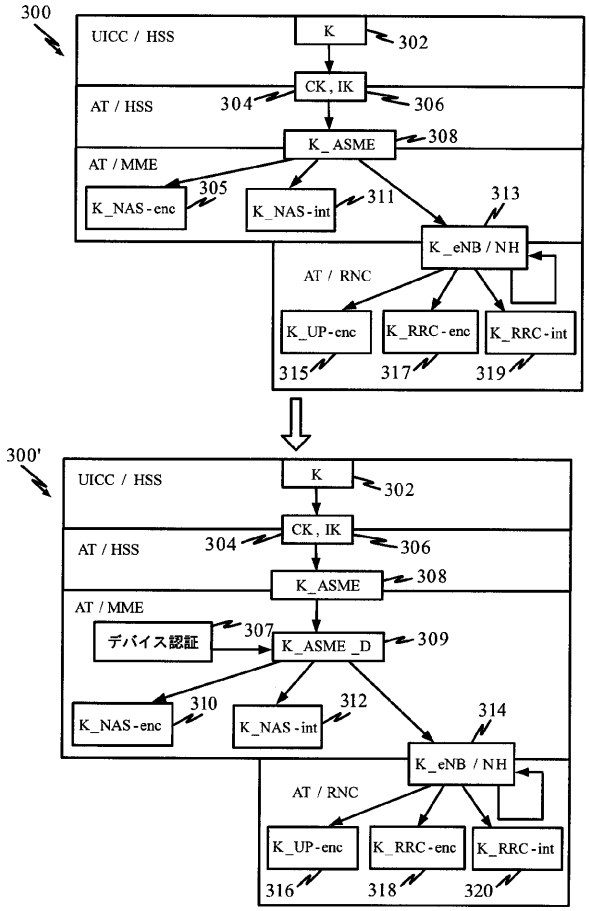
【図１】



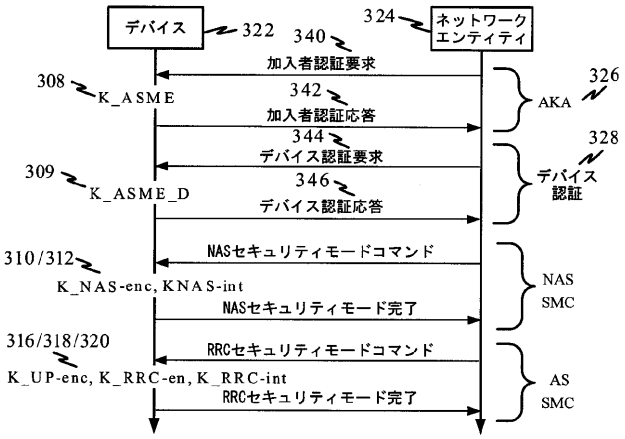
【図２】



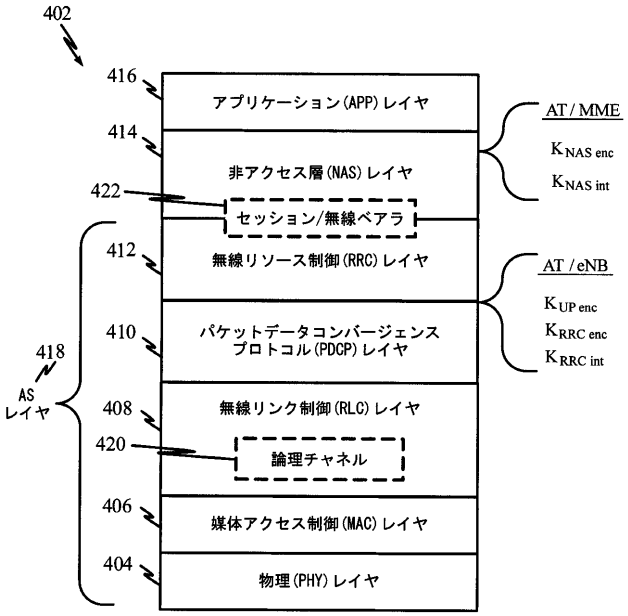
【図３Ａ】


300
UICC / HSS
K
302
CK, IK
AT / HSS
304
306
K_ASME
308
AT / MME
K_NAS-enc
305
K_NAS-int
311
313
K_eNB / NH
AT / RNC
K_UP-enc
K_RRC-enc
K_RRC-int
315
317
319
300'
UICC / HSS
K
302
CK, IK
AT / HSS
304
306
K_ASME
308
AT / MME
デバイス認証
307
K_ASME _D
309
K_NAS-enc
310
K_NAS-int
312
314
K_eNB / NH
AT / RNC
K_UP-enc
K_RRC-enc
K_RRC-int
316
318
320

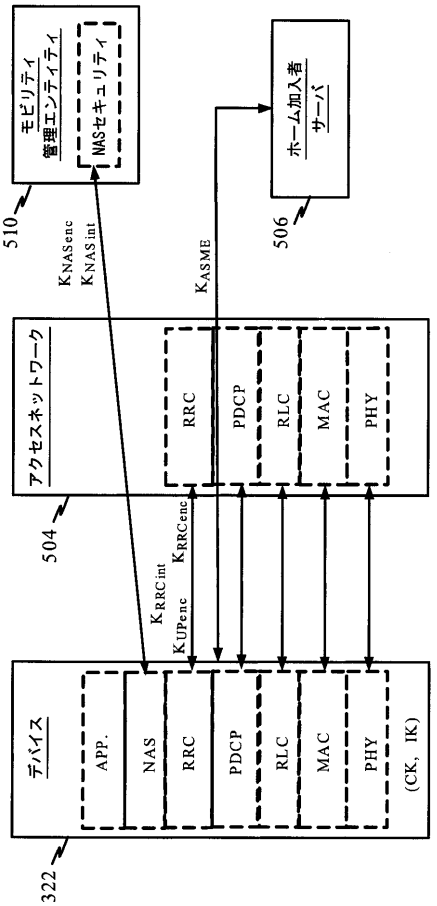
【図３Ｂ】


デバイス
322
340
324
ネットワーク
エンティティ
加入者認証要求
308
K_ASME
342
加入者認証応答
326
AKA
344
デバイス認証要求
328
デバイス
認証
309
K_ASME_D
346
デバイス認証応答
NASセキュリティモードコマンド
310/312
K_NAS-enc, KNAS-int
NAS
SMC
NASセキュリティモード完了
316/318/320
RRCセキュリティモードコマンド
K_UP-enc, K_RRC-en, K_RRC-int
AS
SMC
RRCセキュリティモード完了

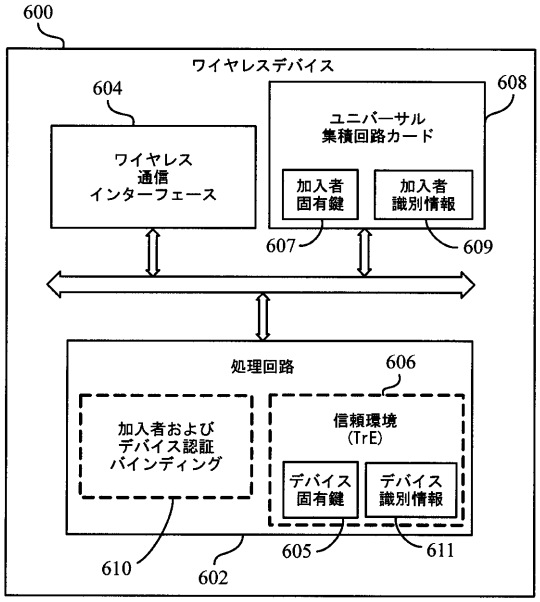
【図４】


402
416
アプリケーション(APP)レイヤ
414
非アクセス層(NAS)レイヤ
422
セッション/無線ベアラ
412
無線リソース制御(RRC)レイヤ
410
パケットデータコンバージェンス
プロトコル(PDCP)レイヤ
418
AS
レイヤ
408
無線リンク制御(RLC)レイヤ
420
論理チャネル
406
媒体アクセス制御(MAC)レイヤ
404
物理(PHY)レイヤ
AT / MME
KNAS enc
KNAS int
AT / eNB
KUP enc
KRRC enc
KRRC int

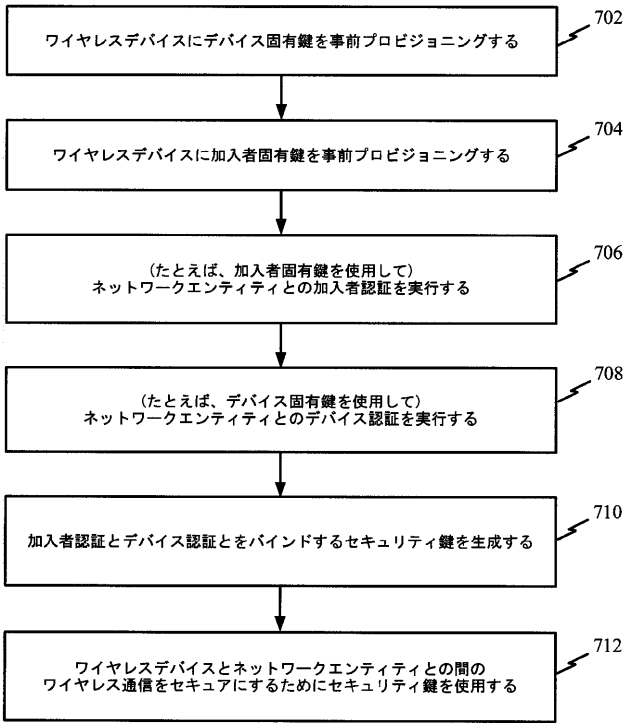
【図５】


モビリティ
管理エンティティ
NASセキュリティ
510
ホーム加入者
サーバ
506
KNASenc
KNASint
KASME
アクセスネットワーク
RRC
PDCP
RLC
MAC
PHY
504
KRRCenc
KRRCint
KUPenc
デバイス
APP.
NAS
RRC
PDCP
RLC
MAC
PHY
(CK, IK)
322

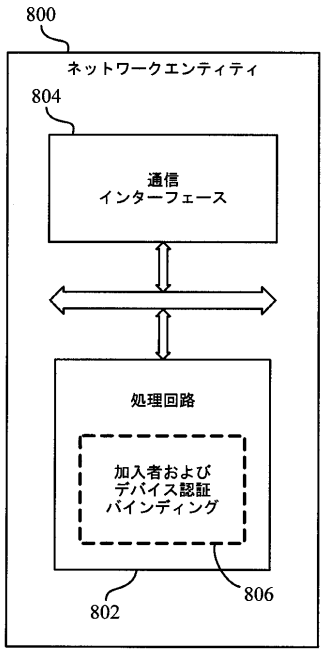
【図６】


600
ワイヤレスデバイス
604
608
ワイヤレス
通信
インターフェース
ユニバーサル
集積回路カード
加入者
固有鍵
加入者
識別情報
607
609
処理回路
606
加入者および
デバイス認証
バインディング
信頼環境
(TrE)
デバイス
固有鍵
デバイス
識別情報
610
602
605
611

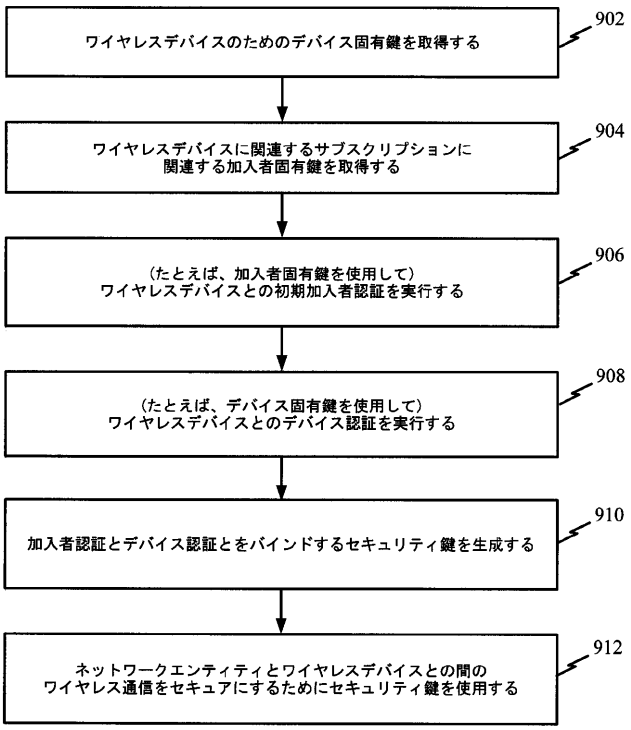
【図７】


ワイヤレスデバイスにデバイス固有鍵を事前プロビジョニングする
702
ワイヤレスデバイスに加入者固有鍵を事前プロビジョニングする
704
(たとえば、加入者固有鍵を使用して)
ネットワークエンティティとの加入者認証を実行する
706
(たとえば、デバイス固有鍵を使用して)
ネットワークエンティティとのデバイス認証を実行する
708
加入者認証とデバイス認証とをバインドするセキュリティ鍵を生成する
710
ワイヤレスデバイスとネットワークエンティティとの間の
ワイヤレス通信をセキュアにするためにセキュリティ鍵を使用する
712

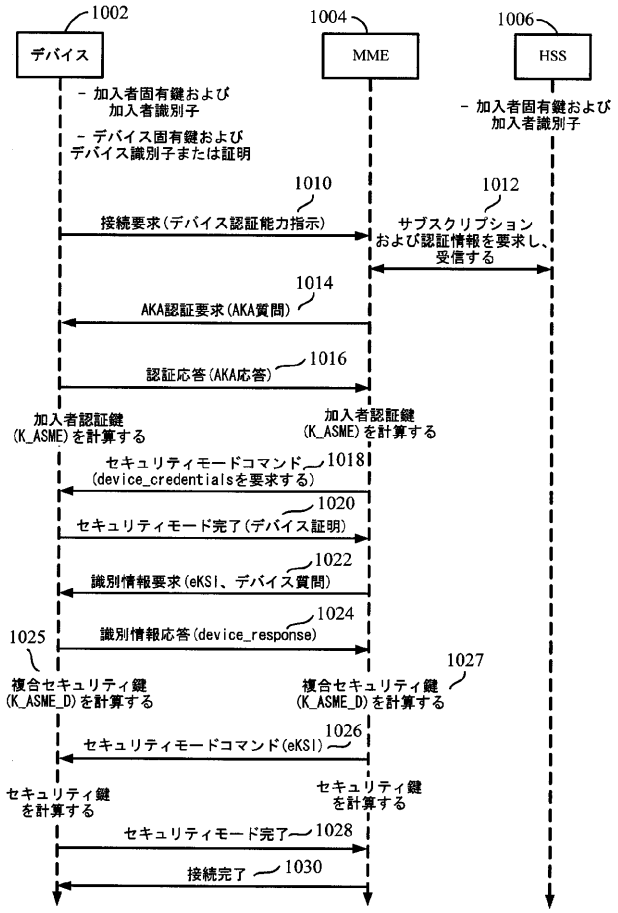
【図８】


800
ネットワークエンティティ
804
通信
インターフェース
処理回路
加入者および
デバイス認証
バインディング
802
806

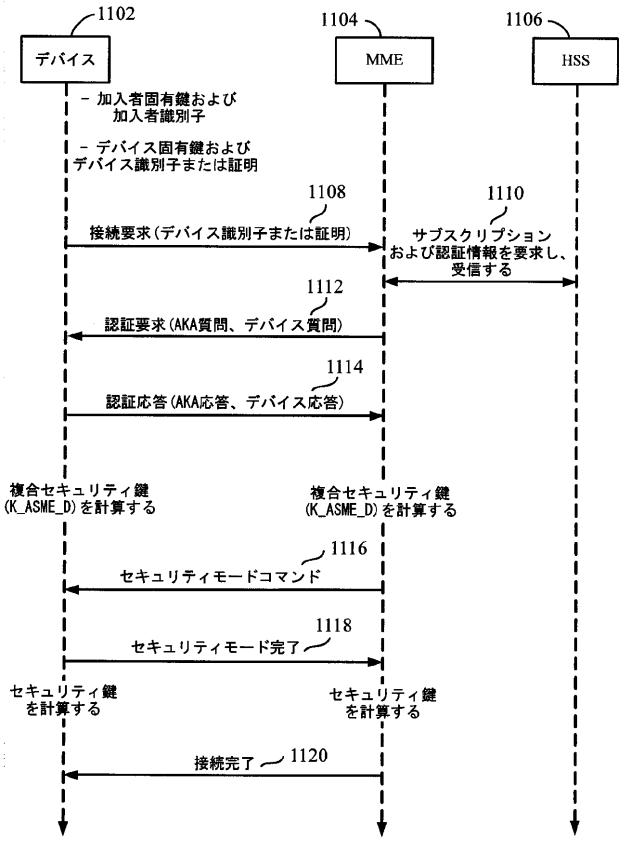
【図９】


ワイヤレスデバイスのためのデバイス固有鍵を取得する
902
ワイヤレスデバイスに関連するサブスクリプションに
関連する加入者固有鍵を取得する
904
(たとえば、加入者固有鍵を使用して)
ワイヤレスデバイスとの初期加入者認証を実行する
906
(たとえば、デバイス固有鍵を使用して)
ワイヤレスデバイスとのデバイス認証を実行する
908
加入者認証とデバイス認証とをバインドするセキュリティ鍵を生成する
910
ネットワークエンティティとワイヤレスデバイスとの間の
ワイヤレス通信をセキュアにするためにセキュリティ鍵を使用する
912

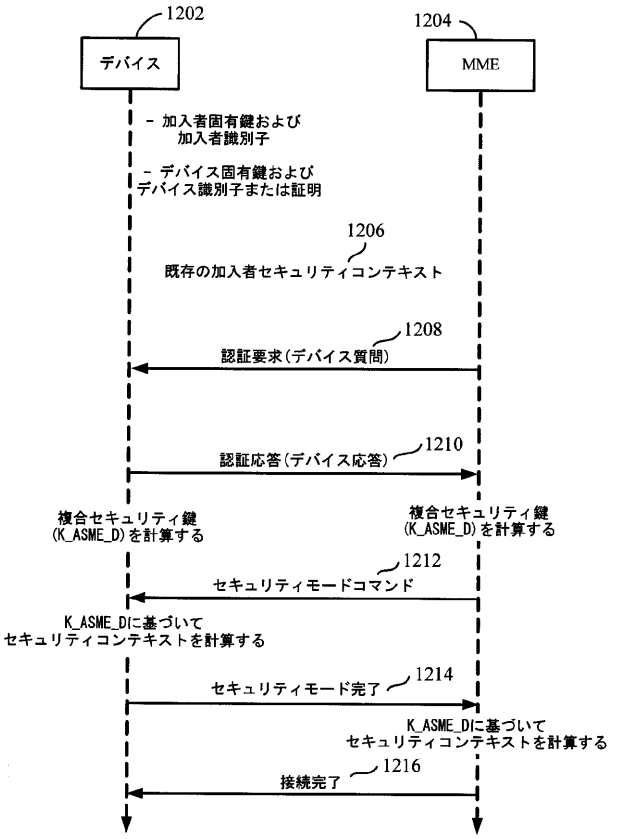
【図１０】


1002
デバイス
1004
MME
1006
HSS
- 加入者固有鍵および
加入者識別子
- デバイス固有鍵および
デバイス識別子または証明
- 加入者固有鍵および
加入者識別子
1010
接続要求(デバイス認証能力指示)
1012
サブスクリプション
および認証情報を要求し、
受信する
1014
AKA認証要求(AKA質問)
1016
認証応答(AKA応答)
加入者認証鍵
(K_ASME)を計算する
加入者認証鍵
(K_ASME)を計算する
セキュリティモードコマンド
(device_credentialsを要求する)
1018
1020
セキュリティモード完了(デバイス証明)
1022
識別情報要求(eKSI、デバイス質問)
1024
識別情報応答(device_response)
1025
複合セキュリティ鍵
(K_ASME_D)を計算する
1027
複合セキュリティ鍵
(K_ASME_D)を計算する
1026
セキュリティモードコマンド(eKSI)
セキュリティ鍵
を計算する
セキュリティ鍵
を計算する
セキュリティモード完了
1028
接続完了
1030

【図１１】


1102
デバイス
1104
MME
1106
HSS
- 加入者固有鍵および
加入者識別子
- デバイス固有鍵および
デバイス識別子または証明
1108
接続要求(デバイス識別子または証明)
1110
サブスクリプション
および認証情報を要求し、
受信する
1112
認証要求(AKA質問、デバイス質問)
1114
認証応答(AKA応答、デバイス応答)
複合セキュリティ鍵
(K_ASME_D)を計算する
複合セキュリティ鍵
(K_ASME_D)を計算する
1116
セキュリティモードコマンド
1118
セキュリティモード完了
セキュリティ鍵
を計算する
セキュリティ鍵
を計算する
接続完了
1120

【図１２】


1202
デバイス
1204
MME
- 加入者固有鍵および
加入者識別子
- デバイス固有鍵および
デバイス識別子または証明
1206
既存の加入者セキュリティコンテキスト
1208
認証要求(デバイス質問)
1210
認証応答(デバイス応答)
複合セキュリティ鍵
(K_ASME_D)を計算する
複合セキュリティ鍵
(K_ASME_D)を計算する
1212
セキュリティモードコマンド
K_ASME_Dに基づいて
セキュリティコンテキストを計算する
1214
セキュリティモード完了
K_ASME_Dに基づいて
セキュリティコンテキストを計算する
1216
接続完了

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/040777

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

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

B. FIELDS SEARCHED

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

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 practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2007/121190 A2 (QUALCOMM INC [US]; DONDETI LAKSHMINATH REDDY [US]; NARAYANAN VIDYA [US) 25 October 2007 (2007-10-25) paragraph [0003] - paragraph [0007] paragraph [0038] - paragraph [0060] paragraph [0070] - paragraph [0072] figure 4 ----- -/--	1-50

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

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document 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
19 October 2011	28/10/2011

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	Olaechea, Javier

3

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/040777

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	3GPP: "3rd Generation Partnership Project; Technical Specification Group Service and Systems Aspects: Security of H(e)NB; (Release 8)", 3GPP TR 33.820 V8.3.0, , vol. 33.820, no. V8.3.0 1 December 2009 (2009-12-01), pages 1-99, XP002650893, Retrieved from the Internet: URL:http://www.quintillion.co.jp/3GPP/Specs/33820-830.pdf Sections 6 and 7	1-50
X	EP 1 739 903 A1 (SAMSUNG ELECTRONICS CO LTD [KR]) 3 January 2007 (2007-01-03) paragraph [0003] - paragraph [0014] paragraph [0030] - paragraph [0032] paragraph [0034] - paragraph [0047] figures 1,4	1-50

3

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2011/040777

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2007121190 A2	25-10-2007	CN 101395887 A	25-03-2009
		EP 2005706 A2	24-12-2008
		JP 2009533771 A	17-09-2009
		KR 20080108130 A	11-12-2008
		TW 200810487 A	16-02-2008
		US 2008040606 A1	14-02-2008
EP 1739903 A1	03-01-2007	AU 2006266651 A1	11-01-2007
		BR PI0612566 A2	23-11-2010
		CA 2608261 A1	11-01-2007
		CN 101208901 A	25-06-2008
		JP 4647689 B2	09-03-2011
		JP 2008547350 A	25-12-2008
		WO 2007004824 A1	11-01-2007
		KR 20070003484 A	05-01-2007
		RU 2367098 C1	10-09-2009
		US 2007016780 A1	18-01-2007

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,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,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,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,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,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PE,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 アナンド・パラニゴウンダー
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

Ｆターム(参考) 5J104 AA07 EA23 KA02 KA04 PA01
5K067 AA35 HH22 HH36