(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2017-535989
(P2017-535989A)
(43)公表日　平成29年11月30日(2017.11.30)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675D	5J104
G09C 1/00	(2006.01)	H04L	9/00	675B	5K067
H04W 12/06	(2009.01)	G09C	1/00	640E	5K127
H04W 12/04	(2009.01)	H04W	12/06		5K201
H04M 1/00	(2006.01)	H04W	12/04		

審査請求 未請求　予備審査請求 未請求　（全 38 頁）　最終頁に続く

(21)出願番号　特願2017-514477 (P2017-514477)
(86)(22)出願日　平成27年9月17日 (2015.9.17)
(85)翻訳文提出日　平成29年3月14日 (2017.3.14)
(86)国際出願番号　PCT/US2015/050602
(87)国際公開番号　WO2016/048774
(87)国際公開日　平成28年3月31日 (2016.3.31)
(31)優先権主張番号　62/054,272
(32)優先日　平成26年9月23日 (2014.9.23)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　62/083,826
(32)優先日　平成26年11月24日 (2014.11.24)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　14/794,452
(32)優先日　平成27年7月8日 (2015.7.8)
(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　カレ・イルマリ・アフマヴァーラ
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】証明書ベースの認証

(57)【要約】
ロングタームエボリューション(LTE)ネットワークと通信するように構成されたデバイスにおいて動作可能な認証のための方法について説明する。この方法は、LTEネットワークが加入者識別モジュール(SIM)ベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートすることを指示する第1のメッセージをLTEネットワークから受信するステップを含む。この方法はまた、証明書ベースの認証を実行するための1つまたは複数のメッセージをLTEネットワークと通信するステップを含む。この方法は、証明書ベースの認証から導出された鍵に基づいてLTEセキュリティコンテキストを確立するステップをさらに含む。

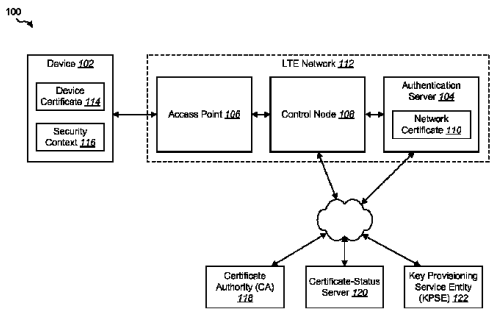


FIG. 1

【特許請求の範囲】
【請求項１】
ロングタームエボリューション(LTE)ネットワークと通信するように構成されたデバイスにおいて動作可能な認証のための方法であって、
前記LTEネットワークが加入者識別モジュール(SIM)ベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートすることを指示する第1のメッセージを前記LTEネットワークから受信するステップと、
前記証明書ベースの認証を実行するための1つまたは複数のメッセージを前記LTEネットワークと通信するステップと、
前記証明書ベースの認証から導出された鍵に基づいて前記LTEセキュリティコンテキストを確立するステップと
を含む、方法。
【請求項２】
LTEネットワークからの前記第1のメッセージが、システム情報ブロードキャスト(SIB)メッセージを含む、請求項1に記載の方法。
【請求項３】
前記LTEネットワークによってサポートされる1つまたは複数の認証方法および1つまたは複数のサービスプロバイダを指示する第2のメッセージを前記LTEネットワークから受信するステップをさらに含む、請求項1に記載の方法。
【請求項４】
デバイスから要求を送ることに応答して、前記第2のメッセージを受信するステップをさらに含む、請求項3に記載の方法。
【請求項５】
前記1つまたは複数のメッセージが、1つまたは複数のLTE非アクセス層(NAS)シグナリングメッセージを使用して通信される、請求項1に記載の方法。
【請求項６】
前記1つまたは複数のメッセージが、1つまたは複数の拡張認証プロトコル(EAP)メッセージを含む、請求項1に記載の方法。
【請求項７】
前記1つまたは複数のEAPメッセージが、1つまたは複数のLTE NASシグナリングメッセージを使用して通信される、請求項6に記載の方法。
【請求項８】
前記証明書ベースの認証が、EAPトランスポートレイヤセキュリティ(EAP-TLS)またはEAPトンネルトランスポートレイヤセキュリティ(EAP-TTLS)を使用して実行される、請求項6に記載の方法。
【請求項９】
前記証明書ベースの認証を実行するための前記1つまたは複数のメッセージを前記LTEネットワークと前記通信するステップが、
ネットワーク証明書を認証サーバから受信するステップと、
前記ネットワーク証明書を検証するステップと
を含む、請求項1に記載の方法。
【請求項１０】
前記ネットワーク証明書を前記検証するステップが、
前記ネットワーク証明書が信頼できる認証局によって署名されているかどうかを決定するステップ、
前記ネットワーク証明書が期限切れしているかどうかを決定するステップ、
前記ネットワーク証明書が失効しているかどうかを決定するステップ、または
前記認証サーバが前記ネットワーク証明書を所有しているかどうかを決定するステップのうちの1つまたは複数を含む、請求項9に記載の方法。
【請求項１１】

前記ネットワーク証明書が失効しているかどうかを前記判断するステップが、
前記ネットワーク証明書が証明書失効リスト(CRL)内にないことを検証するステップ、または
オンライン証明書状態プロトコル(OCSP)サーバに問い合わせるステップ
を含む、請求項10に記載の方法。

【請求項１２】

前記証明書ベースの認証を実行するための前記1つまたは複数のメッセージを前記LTEネットワークと前記通信するステップが、デバイス証明書を前記認証サーバに送るステップをさらに含み、前記デバイス証明書が、前記ネットワーク証明書内の情報に基づいて暗号化される、請求項10に記載の方法。

【請求項１３】

ユーザ資格に対する要求を受信するステップと、
前記ユーザ資格を前記LTEネットワークに送るステップと
をさらに含む、請求項1に記載の方法。

【請求項１４】

ペンネームを前記LTEネットワークから受信するステップと、
前記LTEネットワークへのアクセスを得るための後続の試みにおいてデバイス証明書の代わりに前記ペンネームを前記LTEネットワークに送るステップと
をさらに含む、請求項1に記載の方法。

【請求項１５】

サービス合意を受け入れるための要求を受信するステップと、
前記サービス合意を受け入れるメッセージを送るステップと
をさらに含む、請求項1に記載の方法。

【請求項１６】

前記デバイスが製造される時点で前記デバイスにデバイス証明書をプロビジョニングするステップをさらに含む、請求項1に記載の方法。

【請求項１７】

前記デバイス証明書が前記デバイスを一意に識別する、請求項16に記載の方法。

【請求項１８】

前記デバイス証明書が、シリアル番号、メディアアクセス制御(MAC)ID、国際モバイル機器識別情報(IMEI)、または国際モバイル加入者識別情報(IMSI)のうちの少なくとも1つまたは組合せに基づく、請求項17に記載の方法。

【請求項１９】

企業証明書登録プロセスを使用して、前記デバイスにデバイス証明書をプロビジョニングするステップをさらに含む、請求項1に記載の方法。

【請求項２０】

前記企業証明書登録プロセスが簡易証明書登録プロトコル(SCEP)を利用する、請求項19に記載の方法。

【請求項２１】

前記デバイスに固有の公開鍵と秘密鍵のペアを使用して前記デバイスに関する自己署名デバイス証明書を生成するステップをさらに含む、請求項1に記載の方法。

【請求項２２】

システムオンチップ(SoC)内にプログラムされた秘密鍵を使用して前記デバイスに関する前記公開鍵と秘密鍵のペアを生成するステップをさらに含み、前記秘密鍵が信頼できるエンティティと共有される、請求項21に記載の方法。

【請求項２３】

前記デバイスと信頼できるエンティティとの間で鍵プロビジョニングプロトコルを実行することによって、前記公開鍵と秘密鍵のペアを生成するステップをさらに含む、請求項21に記載の方法。

【請求項２４】

ロングタームエボリューション(LTE)ネットワークと通信するように構成された装置であって、
前記LTEネットワークがSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートすることを指示する第1のメッセージを前記LTEネットワークから受信し、
前記証明書ベースの認証を実行するための1つまたは複数のメッセージを前記LTEネットワークと通信する
ように構成されたトランシーバと、
前記証明書ベースの認証から導出された鍵に基づいて前記LTEセキュリティコンテキストを確立するように構成されたセキュリティコンテキスト確立器と
を含む、装置。
【請求項２５】
ロングタームエボリューション(LTE)ネットワークと通信するように構成された装置であって、
前記LTEネットワークがSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートすることを指示する第1のメッセージを前記LTEネットワークから受信するための手段と、
前記証明書ベースの認証を実行するための1つまたは複数のメッセージを前記LTEネットワークと通信するための手段と、
前記証明書ベースの認証から導出された鍵に基づいて前記LTEセキュリティコンテキストを確立するための手段と
を含む、装置。
【請求項２６】
コンピュータに、
LTEネットワークがSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートすることを指示する第1のメッセージを前記LTEネットワークから受信させ、
前記証明書ベースの認証を実行するための1つまたは複数のメッセージを前記LTEネットワークと通信させ、
前記証明書ベースの認証から導出された鍵に基づいて前記LTEセキュリティコンテキストを確立させる
ためのコードを含む、非一時的コンピュータ可読媒体。
【請求項２７】
ロングタームエボリューション(LTE)ネットワーク内で認証するための方法であって、
デバイスがSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートするという指示を前記デバイスから受信するステップと、
前記証明書ベースの認証を実行するための1つまたは複数のメッセージを前記デバイスと通信するステップと、
前記証明書ベースの認証から導出された鍵に基づいて前記LTEセキュリティコンテキストを確立するステップと
を含む、方法。
【請求項２８】
前記指示が添付メッセージ内で受信される、請求項27に記載の方法。
【請求項２９】
前記指示が拡張認証プロトコル(EAP)メッセージの一部として受信される、請求項27に記載の方法。
【請求項３０】
前記1つまたは複数のメッセージが、1つまたは複数のLTE非アクセス層(NAS)シグナリングメッセージを使用して通信される、請求項27に記載の方法。

【請求項３１】
前記1つまたは複数のメッセージが1つまたは複数のEAPメッセージを含む、請求項27に記載の方法。
【請求項３２】
前記1つまたは複数のEAPメッセージが、1つまたは複数のLTE NASシグナリングメッセージを使用して通信される、請求項31に記載の方法。
【請求項３３】
前記証明書ベースの認証が、EAPトランスポートレイヤセキュリティ(EAP-TLS)またはEAPトンネルトランスポートレイヤセキュリティ(EAP-TTLS)を使用して実行される、請求項31に記載の方法。
【請求項３４】
前記証明書ベースの認証を実行するための前記1つまたは複数のメッセージを前記デバイスと前記通信するステップが、
デバイス証明書を前記デバイスから受信するステップと、
前記デバイス証明書を検証するステップと
を含む、請求項27に記載の方法。
【請求項３５】
前記デバイス証明書を前記検証するステップが、
前記デバイス証明書が自己署名デバイス証明書であると決定するステップと、
信頼できるエンティティから前記デバイスに関する公開鍵を取得するステップと、
前記公開鍵に基づいて前記自己署名デバイス証明書が前記デバイスによって署名されていることを検証するステップと
を含む、請求項34に記載の方法。
【請求項３６】
前記デバイス証明書を前記検証するステップが、
前記デバイス証明書が信頼できる認証局によって署名されているかどうかを決定するステップ、
前記デバイス証明書が期限切れしているかどうかを決定するステップ、または
前記デバイスが前記デバイス証明書を所有しているかどうかを決定するステップ
のうちの1つまたは複数を含む、請求項34に記載の方法。
【請求項３７】
前記デバイス証明書を前記検証するステップが、前記デバイス証明書が失効しているかどうかを決定するステップをさらに含む、請求項36に記載の方法。
【請求項３８】
前記デバイス証明書が失効しているかどうかを前記決定するステップが、
前記デバイス証明書が証明書失効リスト(CRL)内にないことを検証するステップ、または
オンライン証明書状態プロトコル(OCSP)サーバに問い合わせるステップ
のうちの1つまたは組合せを含む、請求項37に記載の方法。
【請求項３９】
前記デバイス証明書を前記検証するステップが、
前記デバイスが前記LTEネットワークにアクセスすることが可能にされているデバイスのリスト内にあるかどうかを決定するステップ、または
前記デバイスが前記LTEネットワークにアクセスすることが可能にされていないデバイスのリスト内にないかどうかを決定するステップ
のうちの1つまたは組合せをさらに含む、請求項36に記載の方法。
【請求項４０】
ネットワーク証明書を前記デバイスに送るステップをさらに含む、請求項27に記載の方法。
【請求項４１】

ユーザ資格に対する要求を前記デバイスに送るステップと、
前記ユーザ資格を前記デバイスから受信するステップと、
前記ユーザ資格を検証するステップと、
前記ユーザ資格に基づいて、前記LTEネットワークへのアクセスを前記デバイスに付与するステップと
をさらに含む、請求項27に記載の方法。
【請求項４２】
ペンネームを前記デバイスに送るステップと、
前記LTEネットワークへのアクセスを得るための後続の要求においてデバイス証明書の代わりに前記ペンネームを前記デバイスから受信するステップと
をさらに含む、請求項27に記載の方法。
【請求項４３】
サービス合意を受け入れるための要求を前記デバイスに送るステップと、
前記サービス合意を受け入れるメッセージを前記デバイスから受信するステップと、
前記サービス合意を受け入れる前記メッセージに基づいて、前記LTEネットワークへのアクセスを前記デバイスに付与するステップと
をさらに含む、請求項27に記載の方法。
【請求項４４】
ロングタームエボリューション(LTE)ネットワーク内で認証するための装置であって、
デバイスがSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートするという指示を前記デバイスから受信し、
前記証明書ベースの認証を実行するための1つまたは複数のメッセージを前記デバイスと通信する
ように構成されたトランシーバと、
前記証明書ベースの認証から導出された鍵に基づいて前記LTEセキュリティコンテキストを確立するように構成されたセキュリティコンテキスト確立器と
を含む、装置。
【請求項４５】
ロングタームエボリューション(LTE)ネットワーク内で認証するための装置であって、
デバイスがSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートするという指示を前記デバイスから受信するための手段と、
前記証明書ベースの認証を実行するための1つまたは複数のメッセージを前記デバイスと通信するための手段と、
前記証明書ベースの認証から導出された鍵に基づいて前記LTEセキュリティコンテキストを確立するための手段と
を含む、装置。
【請求項４６】
コンピュータに、
デバイスがSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてロングタームエボリューション(LTE)セキュリティコンテキストの確立をサポートするという指示を前記デバイスから受信させ、
前記証明書ベースの認証を実行するための1つまたは複数のメッセージを前記デバイスと通信させ、
前記証明書ベースの認証から導出された鍵に基づいて前記LTEセキュリティコンテキストを確立させる
ためのコードを含む、非一時的コンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】

【０００１】
関連出願
本出願は、「Certificate-Based Authentication」に関して、2014年9月23日に出願した米国仮特許出願第62/054,272号に関し、その優先権を主張するものである。本出願はまた、「Certificate-Based Authentication」に関して、2014年11月24日に出願した米国仮特許出願第62/083,826号に関し、その優先権を主張するものである。
【０００２】
本開示は、一般に、通信の分野に関し、より詳細には、1つまたは複数の証明書を通信することによって、ネットワークに対してデバイスを認証するためのシステムおよび方法に関する。
【背景技術】
【０００３】
ワイヤレス通信システムは、たとえば、音声、データなどの、様々なタイプの通信コンテンツを提供するために、広く展開されている。典型的なワイヤレス通信システムは、利用可能なシステムリソース(たとえば、帯域幅、送信電力など)を共有することによって、複数のユーザとの通信をサポートすることが可能な多元接続システムであってよい。そのような多元接続システムの例は、符号分割多元接続(CDMA)システム、時分割多元接続(TDMA)システム、周波数分割多元接続(FDMA)システム、直交周波数分割多元接続(OFDMA)システムなどを含んでもよい。加えて、システムは、第3世代パートナーシッププロジェクト(3GPP)、3GPPロングタームエボリューション(LTE:long term evolution)、ウルトラモバイルブロードバンド(UMB:ultra mobile broadband)、エボリューションデータオプティマイズド(EV-DO:evolution data optimized)などの仕様に準拠することができる。
【０００４】
一般に、ワイヤレス多元接続通信システムは、複数のデバイスに関する通信を同時にサポートすることができる。各デバイスは、順方向リンクおよび逆方向リンク上の伝送を介して、1つまたは複数の基地局と通信することができる。順方向リンク(またはダウンリンク)は、基地局からデバイスまでの通信リンクを指し、逆方向リンク(またはアップリンク)は、デバイスから基地局までの通信リンクを指す。さらに、デバイスと基地局との間の通信は、単入力単出力(SISO)システム、多入力単出力(MISO)システム、多入力多出力(MIMO)システムなどを介して確立され得る。加えて、ピアツーピアワイヤレスネットワーク構成では、デバイスは他のデバイスと(および/または、基地局は他の基地局と)通信することができる。
【０００５】
ワイヤレス通信ネットワークにアクセスする前に、デバイスは認証することが要求される場合がある。多くのワイヤレス通信ネットワーク内で、認証はネットワークオペレータによって提供される加入者識別モジュール(SIM)カードを使用して実行することができる。ニュートラルホスト(NH:neutral-host)ネットワークなど、いくつかのワイヤレス通信ネットワークは、デバイスがSIMカードを使用せずに接続し、確実に認証することを可能にすることが必要な場合がある。したがって、1つまたは複数の証明書を交換することによってワイヤレス通信ネットワークに対してデバイスを認証するためのシステムおよび方法は有益であり得る。
【発明の概要】
【課題を解決するための手段】
【０００６】
ロングタームエボリューション(LTE)ネットワークと通信するように構成されたデバイスにおいて動作可能な認証のための方法について説明する。この方法は、LTEネットワークが加入者識別モジュール(SIM)ベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートすることを指示する第1のメッセージをLTEネットワークから受信するステップを含む。この方法はまた、証明書ベースの認証を実行するための1つまたは複数のメッセージをLTEネットワークと通信するス

テップを含む。この方法は、証明書ベースの認証から導出された鍵に基づいてLTEセキュリティコンテキストを確立するステップをさらに含む。

【０００７】

LTEネットワークからの第1のメッセージは、システム情報ブロードキャスト(SIB)メッセージを含み得る。この方法はまた、LTEネットワークによってサポートされる1つまたは複数の認証方法および1つまたは複数のサービスプロバイダを指示する第2のメッセージをLTEネットワークから受信するステップを含む。この方法は、デバイスから要求を送ることに応答して、第2のメッセージを受信するステップをさらに含む。

【０００８】

1つまたは複数のメッセージは、1つまたは複数のLTE非アクセス層(NAS)シグナリングメッセージを使用して通信され得る。1つまたは複数のメッセージは、1つまたは複数の拡張認証プロトコル(EAP)メッセージを含み得る。1つまたは複数のEAPメッセージは、1つまたは複数のNASシグナリングメッセージを使用して通信され得る。証明書ベースの認証は、EAPトランスポートレイヤセキュリティ(EAP-TLS:EAP-Transport Layer Security)またはEAPトンネルトランスポートレイヤセキュリティ(EAP-TTLS:EAP-Tunneled Transport Layer Security)を使用して実行され得る。

【０００９】

証明書ベースの認証を実行するための1つまたは複数のメッセージをLTEネットワークと通信するステップは、ネットワーク証明書を認証サーバから受信するステップを含み得る。ネットワーク証明書を検証することができる。

【００１０】

ネットワーク証明書を検証するステップは、ネットワーク証明書が信頼できる認証局によって署名されているかどうかを決定するステップ、ネットワーク証明書が期限切れしているかどうかを決定するステップ、ネットワーク証明書が失効しているかどうかを決定するステップ、または認証サーバがネットワーク証明書を所有しているかどうかを決定するステップのうちの1つまたは複数を含み得る。

【００１１】

ネットワーク証明書が失効しているかどうかを決定するステップは、ネットワーク証明書が証明書失効リスト(CRL)内にないことを検証するステップを含み得る。ネットワーク証明書が失効しているかどうかを決定するステップは、代替的に、オンライン証明書状態プロトコル(OCSP:Online Certificate Status Protocol)サーバに問い合わせるステップを含み得る。

【００１２】

証明書ベースの認証を実行するための1つまたは複数のメッセージをLTEネットワークと通信するステップは、デバイス証明書を認証サーバに送るステップをさらに含み得る。デバイス証明書は、ネットワーク証明書内の情報に基づいて暗号化され得る。

【００１３】

本方法はまた、ユーザ資格に対する要求を受信するステップを含み得る。ユーザ資格をLTEネットワークに送ることができる。

【００１４】

本方法はまた、ペンネームをLTEネットワークから受信するステップを含み得る。この方法は、LTEネットワークへのアクセスを得るための後続の試みにおいてデバイス証明書の代わりにペンネームをLTEネットワークに送るステップをさらに含み得る。

【００１５】

本方法はまた、サービス合意を受け入れるための要求を受信するステップを含み得る。本方法は、サービス合意を受け入れるメッセージを送るステップをさらに含み得る。

【００１６】

この方法はまた、デバイスが製造される時点でデバイスにデバイス証明書をプロビジョニングするステップを含み得る。デバイス証明書はデバイスを一意に識別することができる。デバイス証明書は、シリアル番号、メディアアクセス制御(MAC)ID、国際モバイル機

器識別情報(IMEI)、または国際モバイル加入者識別情報(IMSI)のうちの少なくとも1つまたは組合せに基づいてよい。

【００１７】

この方法はまた、企業証明書登録プロセスを使用して、デバイスにデバイス証明書をプロビジョニングするステップを含み得る。企業証明書登録プロセスは簡易証明書登録プロトコル(SCEP)を利用することができる。

【００１８】

この方法はまた、デバイスに固有の公開鍵と秘密鍵のペアを使用してデバイスに関する自己署名デバイス証明書を生成するステップを含み得る。この方法は、システムオンチップ(SoC)内にプログラムされた秘密鍵を使用してデバイスに関する公開鍵と秘密鍵のペアを生成するステップをさらに含み得る。秘密鍵は信頼できるエンティティと共有され得る。この方法は、デバイスと信頼できるエンティティとの間で鍵プロビジョニングプロトコルを実行することによって、公開鍵と秘密鍵のペアを生成するステップをさらに含み得る。

【００１９】

ロングタームエボリューション(LTE)ネットワークと通信するように構成された装置についても説明する。この装置は、LTEネットワークがSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートすることを指示する第1のメッセージをLTEネットワークから受信するように構成されたトランシーバを含む。このトランシーバはまた、証明書ベースの認証を実行するための1つまたは複数のメッセージをLTEネットワークと通信するように構成される。この装置はまた、証明書ベースの認証から導出された鍵に基づいてLTEセキュリティコンテキストを確立するように構成されたセキュリティコンテキスト確立器を含む。

【００２０】

ロングタームエボリューション(LTE)ネットワークと通信するように構成された別の装置についても説明する。この装置は、LTEネットワークがSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートすることを指示する第1のメッセージをLTEネットワークから受信するための手段を含む。この装置はまた、証明書ベースの認証を実行するための1つまたは複数のメッセージをLTEネットワークと通信するための手段を含む。この装置は、証明書ベースの認証から導出された鍵に基づいてLTEセキュリティコンテキストを確立するための手段をさらに含む。

【００２１】

コンピュータ可読媒体についても説明する。このコンピュータ可読媒体は、コンピュータに、LTEネットワークがSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートすることを指示する第1のメッセージをLTEネットワークから受信させるためのコードを含む。このコンピュータ可読媒体はまた、コンピュータに、証明書ベースの認証を実行するための1つまたは複数のメッセージをLTEネットワークと通信させるためのコードを含む。このコンピュータ可読媒体は、コンピュータに、証明書ベースの認証から導出された鍵に基づいてLTEセキュリティコンテキストを確立させるためのコードをさらに含む。

【００２２】

ロングタームエボリューション(LTE)ネットワーク内で認証するための方法についても説明する。この方法は、デバイスがSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートするという指示をデバイスから受信するステップを含む。この方法はまた、証明書ベースの認証を実行するための1つまたは複数のメッセージをデバイスと通信するステップを含む。この方法は、証明書ベースの認証から導出された鍵に基づいてLTEセキュリティコンテキストを確立するステップをさらに含む。

【００２３】

この指示は添付メッセージ内で受信され得る。この指示は拡張認証プロトコル(EAP)メ

ッセージの一部として受信され得る。1つまたは複数のメッセージは、LTE非アクセス層(NAS)シグナリングメッセージを使用して通信され得る。1つまたは複数のメッセージはEAPメッセージを含み得る。

【００２４】

証明書ベースの認証を実行するための1つまたは複数のメッセージをデバイスと通信するステップは、デバイス証明書をデバイスから受信するステップを含み得る。デバイス証明書を検証することができる。

【００２５】

デバイス証明書を検証するステップは、デバイス証明書が自己署名デバイス証明書であると決定するステップと、信頼できるエンティティからデバイスに関する公開鍵を取得するステップと、公開鍵に基づいて自己署名デバイス証明書がデバイスによって署名されていることを検証するステップとを含み得る。

【００２６】

デバイス証明書を検証するステップは、デバイス証明書が信頼できる認証局によって署名されているかどうかを決定するステップ、デバイス証明書が期限切れしているかどうかを決定するステップ、またはデバイスがデバイス証明書を所有しているかどうかを決定するステップのうちの1つまたは複数を含み得る。

【００２７】

デバイス証明書を検証するステップは、デバイス証明書が失効しているかどうかを決定するステップをさらに含み得る。デバイス証明書が失効しているかどうかを決定するステップは、デバイス証明書が証明書失効リスト(CRL)内にないことを検証するステップ、またはオンライン証明書状態プロトコル(OCSP)サーバに問い合わせるステップのうちの1つまたは組合せを含み得る。

【００２８】

デバイス証明書を検証するステップは、デバイスがLTEネットワークにアクセスすることが可能にされているデバイスのリスト内にあるかどうかを決定するステップ、またはデバイスがLTEネットワークにアクセスすることが可能されていないデバイスのリスト内にないかどうかを決定するステップのうちの1つまたは組合せをさらに含み得る。

【００２９】

この方法はまた、ネットワーク証明書をデバイスに送るステップを含み得る。

【００３０】

この方法はまた、ユーザ資格に対する要求をデバイスに送るステップを含み得る。この方法は、ユーザ資格をデバイスから受信するステップをさらに含み得る。この方法は、ユーザ資格を検証するステップをさらに含み得る。この方法はまた、ユーザ資格に基づいて、LTEネットワークへのアクセスをデバイスに付与するステップを含み得る。

【００３１】

この方法はまた、ペンネームをデバイスに送るステップを含み得る。この方法は、LTEネットワークへのアクセスを得るための後続の要求においてデバイス証明書の代わりにペンネームをデバイスから受信するステップをさらに含み得る。

【００３２】

この方法はまた、サービス合意を受け入れるための要求をデバイスに送るステップを含み得る。この本方法は、サービス合意を受け入れるメッセージをデバイスから受信するステップをさらに含み得る。この方法は、サービス合意を受け入れるメッセージに基づいて、LTEネットワークへのアクセスをデバイスに付与するステップをさらに含み得る。

【００３３】

ロングタームエボリューション(LTE)ネットワーク内で認証するための装置についても説明する。この装置は、デバイスがSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートするという指示をデバイスから受信するように構成されたトランシーバを含む。このトランシーバはまた、証明書ベースの認証を実行するための1つまたは複数のメッセージをデバイスと通信する

ように構成される。この装置はまた、証明書ベースの認証から導出された鍵に基づいてLTEセキュリティコンテキストを確立するように構成されたセキュリティコンテキスト確立器を含む。

【００３４】

ロングタームエボリューション(LTE)ネットワーク内で認証するための別の装置についても説明する。この装置は、デバイスがSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートするという指示をデバイスから受信するための手段を含む。この装置はまた、証明書ベースの認証を実行するための1つまたは複数のメッセージをデバイスと通信するための手段を含む。この装置は、証明書ベースの認証から導出された鍵に基づいてLTEセキュリティコンテキストを確立するための手段をさらに含む。

【００３５】

非一時的コンピュータ可読媒体についても説明する。このコンピュータ可読媒体は、コンピュータに、デバイスがSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてロングタームエボリューション(LTE)セキュリティコンテキストの確立をサポートするという指示をデバイスから受信させるためのコードを含む。このコンピュータ可読媒体はまた、コンピュータに、証明書ベースの認証を実行するための1つまたは複数のメッセージをデバイスと通信させるためのコードを含む。このコンピュータ可読媒体は、コンピュータに、証明書ベースの認証から導出された鍵に基づいてLTEセキュリティコンテキストを確立させるためのコードをさらに含む。

【図面の簡単な説明】

【００３６】

【図１】例示的なワイヤレス通信システムを示す図である。

【図２】例示的なデバイスを示すブロック図である。

【図３】例示的な認証サーバを示すブロック図である。

【図４】デバイスによって実行され得る認証のための方法の一構成を例示する流れ図である。

【図５】ロングタームエボリューション(LTE)ネットワークによって実行され得る認証のための方法の別の構成を例示する流れ図である。

【図６】証明書ベースの認証のための手順を示すシーケンス図である。

【図７】証明書ベースの認証のための別の手順を示すシーケンス図である。

【図８】証明書ベースの認証のための手順を示すさらに別のシーケンス図である。

【図９】デバイス内に含まれ得るいくつかの構成要素を示す図である。

【図１０】認証サーバ内に含まれ得るいくつかの構成要素を示す図である。

【発明を実施するための形態】

【００３７】

LTEネットワーク内で、現在、デバイスを認証するための唯一の方法は、特定のモバイルネットワークオペレータによって提供されるSIMカードを使用することである。しかしながら、ニュートラルホスト(NH)LTEネットワークの場合、任意のデバイスが任意のNH LTEネットワークに接続し、確実に自らを認証することを可能にする必要が存在する。これは、SIMカードに依存せず、かつNHネットワークに固有の資格をデバイスにプロビジョニングすることを要求せずに可能であることが必要である。

【００３８】

本明細書で説明するシステムおよび方法は、1つまたは複数の証明書を通信することによって、ネットワークに対してデバイスを認証することを可能にする。デバイスに一意のデバイス証明書を事前プロビジョニングすることができる。デバイス証明書をデバイスから受信するとすぐに、NH LTEネットワークは、(従来のSIMベースの認証の代わりに)証明書ベースの認証を実行することができる。NH LTEネットワークは、次いで、証明書ベースの認証から導出された鍵に基づいてデバイスに関するセキュリティコンテキストを確立することができる。したがって、NH対応LTEデバイスは、任意のNH対応LTEネットワークに接

続し、自らを確実に認証し、その後、接続されたNH LTEネットワークからサービスを獲得することができる。

【００３９】

図面に関して、ここで様々な態様につい説明する。以下の説明では、説明の目的で、1つまたは複数の態様を完全に理解できるように多数の具体的な詳細を記載する。そのような態様がこれらの具体的な詳細なしに実践される場合があることは明らかであろう。

【００４０】

様々な態様では、証明書ベースの認証のためのシステムおよび方法について説明する。説明はデバイスを参照する場合がある。デバイスは、システム、モバイルデバイス、加入者ユニット、加入者局、移動局、モバイル、遠隔局、モバイル端末、遠隔端末、アクセス端末、ユーザ端末、端末、通信デバイス、ユーザエージェント、ユーザデバイス、またはユーザ機器(UE)と呼ばれる場合もある。デバイスは、セルラー電話、衛星電話、コードレス電話、セッション開始プロトコル(SIP)電話、ワイヤレスローカルループ(WLL)局、携帯情報端末(PDA)、ワイヤレス接続機能を有するハンドヘルドデバイス、タブレット、コンピューティングデバイス、あるいはデバイスにセルラーアクセスまたはワイヤレスネットワークアクセスを与える1つまたは複数の基地局(BS)にワイヤレスモデムを介して接続された他の処理デバイスであってよい。

【００４１】

基地局(BS)は、デバイスと通信するために利用することができ、アクセスポイント106、フェムトノード、ピコノード、マイクロノード、ノードB、発展型ノードB(eNB)、H(e)NBと総称されるホームノードB(HNB)もしくはホーム発展型ノードB(HeNB)、または何らかの他の用語で呼ばれる場合もある。これらの基地局は低電力基地局と見なされ得る。たとえば、低電力基地局は、ワイヤレスワイドエリアネットワーク(WWAN)に関連するマクロ基地局と比較して、比較的低い電力で送信することができる。したがって、低電力基地局のカバレージエリアは、マクロ基地局のカバレージエリアよりも実質的に小さい可能性がある。

【００４２】

本明細書で説明する技法は、CDMA、TDMA、FDMA、OFDMA、SC-FDMA、Wi-Fiキャリア検知多重アクセス(CSMA:carrier sense multiple access)、およびその他のシステムなど、様々なワイヤレス通信システムに使用され得る。「システム」および「ネットワーク」という用語は、しばしば互換的に使用される。CDMAシステムは、ユニバーサル地上波無線アクセス(UTRA)、cdma2000などの無線技術を実装することができる。UTRAは、広帯域CDMA(W-CDMA)、およびCDMAの他の変形態を含む。さらに、cdma2000は、IS-2000規格、IS-95規格、およびIS-856規格を包含する。TDMAシステムは、移動体通信用グローバルシステム(GSM（登録商標）)のような無線技術を実装することができる。OFDMAシステムは、発展型UTRA(E-UTRA)、ウルトラモバイルブロードバンド(UMB:Ultra Mobile Broadband)、IEEE 802.11(Wi-Fi)、IEEE 802.16(WiMAX)、IEEE 802.20、Flash-OFDM(登録商標)などの無線技術を実装し得る。UTRAおよびE-UTRAは、ユニバーサルモバイルテレコミュニケーションシステム(UMTS)の一部である。3GPPロングタームエボリューション(LTE)は、ダウンリンクにおいてOFDMAを用い、アップリンクにおいてSC-FDMAを用いるE-UTRAを使用するUMTSのリリースである。UTRA、E-UTRA、UMTS、LTEおよびGSM（登録商標）は、「第3世代パートナーシッププロジェクト」(3GPP)と称する組織からの文書に記載されている。加えて、cdma2000およびUMBは、「第3世代パートナーシッププロジェクト2」(3GPP2)という名称の組織からの文書に記載されている。さらに、そのようなワイヤレス通信システムは、不対無認可スペクトル、802.xxワイヤレスローカルエリアネットワーク(LAN)、Bluetooth（登録商標）、および任意の他の短距離または長距離のワイヤレス通信技法をしばしば使用するピアツーピア(たとえば、モバイルツーモバイル)アドホックネットワークシステムをさらに含み得る。

【００４３】

様々な態様または特徴は、いくつかのデバイス、構成要素、モジュールなどを含むこと

ができるシステムに関して提示されることになる。様々なシステムは、追加のデバイス、構成要素、モジュール、などを含むことができ、および/または、諸図に関連して論じるデバイス、構成要素、モジュール、などのすべてを含まなくてもよいことが理解され、認識されるべきである。これらの手法の組合せも使用され得る。

【００４４】

図1は、例示的なワイヤレス通信システム100を示す。ワイヤレス通信システム100は、デバイス102と、LTEネットワーク112と、認証局(CA)118と、証明書状態サーバ120と、鍵プロビジョニングサービスエンティティ(KPSE)122とを含み得る。ワイヤレス通信システム100は、示されない他のデバイスまたはネットワークノードを含んでもよい。LTEネットワーク112は、アクセスポイント106、制御ノード(CN)108、認証サーバ104のうちの1つまたは複数を含み得る。デバイス102、アクセスポイント106、制御ノード108、認証サーバ104、認証局118、証明書状態サーバ120、およびKPSE122は、1つまたは複数のワイヤードリンクまたはワイヤレスリンク上で通信することができる。

【００４５】

ワイヤレス通信システム100における通信は、ワイヤレスリンク上の伝送を介して達成され得る。そのようなワイヤレスリンクは、単入力単出力(SISO)、多入力単出力(MISO)、または多入力多出力(MIMO)システムを介して確立され得る。MIMOシステムは、それぞれデータ送信用の複数の(N_T)送信アンテナおよび複数の(N_R)受信アンテナを備えた送信機および受信機を含む。いくつかの構成では、ワイヤレス通信システム100はMIMOを利用することができる。MIMOシステムは、時分割複信(TDD)システムおよび周波数分割複信(FDD)システムをサポートすることができる。

【００４６】

いくつかの構成では、ワイヤレス通信システム100は、1つまたは複数の規格に従って動作することができる。これらの規格の例には、Bluetooth（登録商標）(たとえば、米国電気電子技術者協会(IEEE)802.15.1)、IEEE802.11(Wi-Fi)、IEEE802.16(ワールドワイドインターオペラビリティフォーマイクロウェーブアクセス(WiMAX))、モバイル通信用グローバスシステム(GSM（登録商標）)、ユニバーサルモバイルテレコミュニケーションシステム(UMTS)、CDMA2000、ロングタームエボリューション(LTE)などがある。

【００４７】

いくつかの構成では、ワイヤレス通信システム100は、利用可能なシステムリソース(たとえば、帯域幅および送信電力)を共有することによって、複数のデバイスとの通信をサポートすることが可能な多元接続システムであってよい。そのような多元接続システムの例には、符号分割多元接続(CDMA)システム、広帯域符号分割多元接続(W-CDMA)システム、時分割多元接続(TDMA)システム、周波数分割多元接続(FDMA)システム、直交周波数分割多元接続(OFDMA)システム、エボリューションデータオプティマイズド(EV-DO)、シングルキャリア周波数分割多元接続(SC-FDMA)システム、汎用パケット無線サービス(GPRS)アクセスネットワークシステム、第3世代パートナーシッププロジェクト(3GPP)ロングタームエボリューション(LTE)システム、および空間分割多元接続(SDMA)システムなどがある。

【００４８】

LTEネットワーク112では、モバイルネットワークオペレータによって提供される加入者識別モジュール(SIM)カードを使用して、ネットワークに対してデバイス102を認証することができる。しかしながら、ニュートラルホスト(NH)LTEネットワークの場合、任意のデバイス102が、SIMカードなしで、かつネットワーク固有の資格の事前プロビジョニングなしで、任意のNH LTEネットワークに接続し、確実に認証することを可能にする必要が存在し得る。

【００４９】

NHネットワークは、NHネットワークサービスプロバイダによって管理されるか、またはNHネットワークサービスプロバイダとのローミング関係を有するNHアクセスネットワークのセットであってよい。NHアクセスネットワークは、ホットスポットとして、または住居内に、たとえば、ケーブルオペレータまたは企業によって局所的に所有され、操作され得

る。一例では、NHネットワークは、他のネットワークオペレータからデバイス102へのアクセスを可能にするフェムトセルネットワークであってよい。フェムトセルネットワークは、特定のベニュー(たとえば、モール、スタジアム、または事業所)に設置されてよく、拡張されたカバレージまたは容量を提供することができる。

【００５０】

本明細書で説明するLTEネットワーク112はNHネットワークであってよい。一構成では、LTEネットワーク112は、デバイス102がLTEネットワーク112上でサービスを使用することが許可される前に、デバイス102を認証することができる。たとえば、LTEネットワーク112は、デバイス証明書114に基づいてデバイス102を認証することができる。別の構成では、デバイス102およびLTEネットワーク112は、デバイス102がLTEネットワーク112上でサービスを使用することが許可される前に、互いを認証することができる。たとえば、デバイス102は、ネットワーク証明書110に基づいてLTEネットワーク112を認証することができ、LTEネットワーク112は、デバイス証明書114に基づいてデバイス102を認証することができる。

【００５１】

NH LTEネットワーク112の証明書ベースの認証は、LTEネットワーク112が別のネットワークになりすますことを防止することができる。証明書ベースの認証プロセスは、ユーザ識別プライバシー(すなわち、デバイス102識別)が標準LTEネットワークほど劣らないことを確実にすることができる。たとえば、プロセスは、疑われることなく、ユーザまたはデバイス102を識別するために使用され得る情報を送ることができる。言い換えれば、受動盗聴者またはNHアクセスLTEネットワーク112自体が、ユーザまたはデバイス102を追跡するために使用され得る情報に対するアクセスを有することはできない。

【００５２】

デバイス102に一意のデバイス証明書114をプロビジョニングすることができる。デバイス証明書114は、シリアル番号、メディアアクセス制御(MAC)アドレス、国際モバイル機器識別情報(IMEI)、または国際モバイル加入者識別情報(IMSI)など、一意の識別子(ID)を使用してデバイス102を一意に識別することができる。一例では、一意の識別子は、いかなる既存のモバイルネットワークオペレータにも関連付けられないグローバル一意IMSI値であってよい。デバイス証明書114は、特定のNHネットワークに固有でなくてよく、デバイス証明書114は、任意のNHネットワークに対してデバイス102を確実に認証するために使用され得る。

【００５３】

一構成では、デバイス102製造プロセスの一環として、デバイス102にデバイス証明書114をプロビジョニングすることができる。別の構成では、企業証明書登録プロセスを使用して、デバイス102にデバイス証明書114をプロビジョニングすることができる。たとえば、簡易証明書登録プロトコル(SCEP)を使用して、デバイス102にデバイス証明書114をプロビジョニングすることができる。

【００５４】

各デバイス102に関するデバイス証明書114は、認証局(CA)118によって生成され得る。CA118は、相手先商標製造会社(OEM)または第三者であってよい。一構成では、デバイス証明書114を発行することが許可されるルートCA118および1つまたは複数の中間CA118が存在し得る。デバイス証明書114のプロビジョニングは、デバイス証明書114をCA118から製造会社に転送するためのセキュアなチャネルを必要とし得る。

【００５５】

別の構成では、各デバイス102に関するデバイス証明書114は、デバイス固有の公開鍵と秘密鍵のペアを使用して、自己署名デバイス証明書114としてデバイス102自体に関して生成され得る。公開鍵と秘密鍵のペアは、システムオンチップ(SoC)内にプログラムされ、鍵プロビジョニングサービスエンティティ(KPSE)122と共有されるSoC固有の一意の秘密鍵を使用して、デバイス102上で生成され得る。秘密鍵および公開鍵の生成は、デバイス102とKPSE122との間で鍵プロビジョニングプロトコルを実行することを伴う場合がある。デ

バイス102の自己署名デバイス証明書114は、KPSE122から取得された公開鍵を使用して、認証サーバ104によって検証され得る。

【００５６】

NHネットワークサーバにネットワーク証明書110を発行することが許可される信頼できるCA118のリストをさらにデバイス102に提供することができる。このリストは、NHネットワークに接続されることが可能なすべてのデバイス102に関する共通のリストであってよい。

【００５７】

一構成では、証明書状態サーバ120のアドレスをデバイス102に提供することもできる。証明書状態サーバ120は、オンライン証明書状態プロトコル(OCSP)サーバであってよい。デバイス102は、証明書状態サーバ120のアドレスを使用して、証明書状態サーバ120に問い合わせて、ネットワーク証明書110が失効していないことを検証することができる。別の構成では、証明賞失効リスト(CRL)をデバイス102に提供することができる。CRLは失効しているネットワーク証明書110のリストであってよい。デバイス102は、CRLを使用して、ネットワーク証明書110が失効していないことを検証することができる。

【００５８】

デバイス102は、アクセスポイント106を介して制御ノード108と通信することができる。一構成では、制御ノード108は、モビリティ管理エンティティ(MME)であってよい。この構成では、LTE非アクセス層(NAS)シグナリングは、デバイス102と制御ノード108との間で拡張認証プロトコル(EAP)メッセージを搬送するように拡張され得る。デバイス102は、添付メッセージ内に証明書ベースの認証またはニュートラルホスト動作に対するサポートを指示することができる。制御ノード108は、次いで、この指示を使用して、デバイス102と認証サーバ104との間の証明書ベースの認証プロセスを開始することができる。EAPベースの認証をサポートするためのそのような拡張制御ノード108を備えたLTEネットワーク112は、ニュートラルホストLTEネットワークまたはNH LTEネットワークとして知られている場合がある。

【００５９】

一構成では、認証サーバ104は、認証、許可、およびアカウンティング(AAA)サーバであってよい。この構成では、制御ノード108(たとえば、MME)は、EAPを使用して認証サーバ104(たとえば、AAAサーバ)とインターフェースするように拡張され得る。たとえば、制御ノード108は、EAPを使用して認証サーバ104とインターフェースし、IETF RFC5216に定義されるようにトランスポートレイヤセキュリティ(EAP-TLS)を使用して、デバイス102を認証することができる。別の例では、制御ノード108は、EAPを使用して認証サーバ104とインターフェースし、IETF RFC5281に定義されるようにトンネルトランスポートレイヤセキュリティ(EAP-TTLS)を使用して、デバイス102を認証することができる。

【００６０】

一構成では、デバイス102のTLSクライアント認証は、(上で説明した)生成されたデバイス自己署名デバイス証明書114を使用して認証サーバ104(たとえば、AAAサーバ)によって実行される。EAP-TTLS方法では、デバイス自己署名デバイス証明書114を使用したデバイス102のTLSクライアント認証の後に、認証サーバ104によって、さらなるユーザ認証(たとえば、ユーザ名およびパスワード、セキュアなIDトークン、または別のよく知られているユーザ認証方法)を実行することができる。

【００６１】

EAPメッセージは、制御ノード108と認証サーバ104との間で遠隔認証ダイアルインユーザサービス(RADIUS:remote authentication dial-in user service)またはダイアメータプロトコルを介して搬送され得る。認証プロセスの最後に、認証サーバ104は、EAPマスタセッション鍵(MSK)を制御ノード108に送ることができる。制御ノード108は、MSKを使用して、3GPP TS33.401に定義されるようにLTE NASおよびアクセス層(AS)セキュリティのために使用され得る鍵K_{ASME}を導出することができる。

【００６２】

デバイス102は、証明書ベースの認証から導出された鍵に基づいてLTEセキュリティコンテキスト116を確立することができる。セキュリティコンテキスト116は、LTEネットワーク112、LTEネットワーク112のネットワーク証明書110、LTEネットワーク112に関連付けられるペンネーム、および/またはLTEネットワーク112に関する認証プロセスについての情報を記憶することができる。デバイス102がデバイス証明書114を使用してLTEネットワーク112に対して認証された後で、デバイス102はセキュリティコンテキスト116を生成することができる。デバイス102は、デバイス証明書114の代わりに、セキュリティコンテキスト116を使用して、LTEネットワーク112にアクセスする後続の試みにおいてLTEネットワーク112に再接続することができる。

【００６３】

デバイス102にデバイス証明書114を発行することが許可される信頼できるCA118のリストを認証サーバ104に提供することができる。別の構成では、認証サーバ104に、少なくともデバイス102識別子およびNH対応デバイス102の自己署名デバイス証明書114に関連付けられる公開鍵のリストを提供することができる。認証サーバ104は、デバイス102識別子に関連付けられる公開鍵を使用して、自己署名デバイス証明書114の認証を検証することができる。

【００６４】

一構成では、LTEネットワーク112上でサービスにアクセスすることが許可されるデバイス102のリスト(たとえば、ホワイトリスト)を認証サーバ104に提供することができる。LTEネットワーク112上でサービスにアクセスすることが許可されないデバイス102のリスト(たとえば、ブラックリスト)を認証サーバ104にさらに提供することができる。デバイス証明書114を使用したデバイス102の成功裏の認証の後で、認証サーバ104は、オプションで、ネットワークアクセスをデバイス102に付与する前に、このリストを使用してさらなる認証検査を実行することができる。

【００６５】

認証サーバ104は、デバイス証明書114が失効していないことを検証することができる。一構成では、証明書状態サーバ120(たとえば、OCSPサーバ)のアドレスを認証サーバ104に提供することができる。認証サーバ104は、証明書状態サーバ120のアドレスを使用して、証明書状態サーバ120に問い合わせて、デバイス証明書114が失効していないことを検証することができる。別の構成では、証明賞失効リスト(CRL)を認証サーバ104に提供することができる。この場合、CRLは失効しているデバイス証明書114のリストであってよい。認証サーバ104は、CRLを使用してデバイス証明書114が失効していないことを検証することができる。

【００６６】

サービス合意をさらに認証サーバ104に提供することができる。デバイス証明書114を検証した後で、またはそうでなく、LTEネットワーク112にアクセスするためのデバイス102の資格を検証した後で、認証サーバ104は、サービス合意をデバイス102に送ることができるか、またはそうでなく、デバイス102にLTEネットワーク112を介して完全なサービスを受信するために要求されるサービス合意についての情報を受信させることができる。これは、たとえば、ウェブアクセス要求をサービス合意ポータルにリダイレクトさせるようにLTEネットワーク112を構成して、認証サーバ104によって行われてよい。

【００６７】

デバイス102またはデバイス102のユーザは、LTEネットワーク112を通じてサービスにアクセスするためのサービス合意を受け入れることを要求される場合がある。一構成では、サービス合意は、LTEネットワーク112を使用するための条件を設定することができる。別の構成では、サービス合意は課金情報を含み得る。サービス合意に合意することによって、デバイス102のユーザは、デバイス102によってアクセスされるサービスを支払う責任を受け入れることができる。別の構成では、サービス合意は、複数のよく知られている支払方法のうちの任意の1つを使用して、課金金額を支払うことを伴う場合がある。

【００６８】

サービス合意の成功裏の実行時に、認証サーバ104は、一意のデバイスIDを、支払を受け持つユーザにリンクされたアカウントと関連付けることができる。LTEネットワーク112への後続の訪問の際に、認証サーバ104は、デバイス102がサービス合意を前に受け入れていることに基づいて、サービス合意を再度受け入れることをデバイス102、またはデバイス102のユーザに要求せずにアクセスを認証されたデバイス102に付与することができる。

【００６９】

デバイス102がLTEネットワーク112を認証するために使用することができるネットワーク証明書110を認証サーバ104に提供することもできる。ネットワーク証明書110はCA118によって提供され得る。一構成では、1つのルートCA118がすべてのNHネットワークに関するネットワーク証明書110を発行することができる。ルートCA118は、デバイス102が、ネットワーク証明書110が失効していないことを検証するために問い合わせることができる証明書状態サーバ120(たとえば、OCSPサーバ)を維持することもできる。単一のCA118にすべてのネットワーク証明書110を発行させることは、複雑さを低減し得る。これは、CA118またはネットワーク証明書110が損なわれた場合、NHネットワークになりすますリスクを高める可能性もある。

【００７０】

別の構成では、ルートCA118は1つまたは複数の中間CA118を許可することができる。中間CA118は、次いで、ネットワーク証明書110を発行することができる。この構成では、ルートCA118は、中間CA118の失効リストを維持することができる。さらに、中間CA118は、中間CA118が発行した証明書(たとえば、デバイス証明書114および/またはネットワーク証明書110)に関する失効リストを維持することができる。

【００７１】

図2は、例示的なデバイス202を示すブロック図である。デバイス202は、トランシーバ230と、ネットワーク証明書検証器236と、デバイス証明書生成器238と、セキュリティコンテキスト確立器240と、メモリ205とを含み得る。デバイス202は、LTEネットワーク112と通信することが可能であり得る。一構成では、LTEネットワーク112はニュートラルホスト(NH)LTEネットワークであってよい。

【００７２】

トランシーバ230は、送信機232と受信機234とを含み得る。送信機232は、デバイス202がワイヤレス通信システム100内でメッセージを送信することを可能にし得る。受信機234は、デバイス202がワイヤレス通信システム100内でメッセージを受信することを可能にし得る。

【００７３】

ネットワーク証明書検証器236は、デバイス202がネットワーク証明書110を検証することを可能にし得る。たとえば、デバイス202は、ネットワーク証明書110を認証サーバ104から受信することができる。一構成では、ネットワーク証明書検証器236は、ネットワーク証明書110が信頼できるCA118によって署名されているかどうか、ネットワーク証明書110が期限切れしているかどうか、ネットワーク証明書が110失効しているかどうか、および/または認証サーバ104がネットワーク証明書110の所有者であるかどうかを決定することによって、ネットワーク証明書110を検証することができる。

【００７４】

デバイス証明書生成器238は、デバイス202が自己署名デバイス証明書214を生成し、署名することを可能にし得る。セキュリティコンテキスト確立器240は、ネットワークとの証明ベースの認証を実行した後で、デバイス202がセキュリティコンテキスト216を確立することを可能にし得る。

【００７５】

デバイス202は、メモリ205内に記憶された、デバイス証明書214、証明書失効リスト(CRL)224、OCSPサーバアドレス226、ユーザ資格228、ネットワーク証明書110を発行するための信頼できるCA118のリスト242、1つまたは複数のセキュリティコンテキスト216、および1つまたは複数のペンネーム246をさらに含み得る。

【００７６】
デバイス202は、デバイス証明書214を使用して、LTEネットワーク112に対して認証することができる。たとえば、デバイス202は、デバイス証明書214を認証サーバ104に送ることができる。認証サーバ104は、デバイス証明書214が信頼できるCA118によって署名されているかどうか、デバイス証明書214が期限切れしているかどうか、デバイス証明書214が失効しているかどうか、および/またはデバイス202がデバイス証明書214の所有者であるかどうかを決定することができる。
【００７７】
ネットワーク証明書検証器236は、CRL224、OCSPサーバアドレス226、およびネットワーク証明書110を発行するための信頼できるCA118のリスト242を使用してネットワーク証明書110を検証することができる。たとえば、ネットワーク証明書検証器236は、CRL224を検査するか、またはOCSPサーバアドレス226においてOCSPサーバに問い合わせて、ネットワーク証明書110が失効しているかどうかを決定することができる。ネットワーク証明書検証器236は、ネットワーク証明書110を発行するための信頼できるCA118のリスト242を使用して、ネットワーク証明書110が信頼できるCA118によって署名されているかどうかを決定することができる。
【００７８】
デバイス202は、デバイス証明書214に加えて、またはその代わりに、ユーザ資格228を使用して、LTEネットワーク112に対して認証することができる。たとえば、企業によって操作されるNHネットワークは、追加のセキュリティ対策として、ユーザ資格228(たとえば、ユーザ名およびパスワードなど)を使用して認証することをデバイス202に要求する場合がある。
【００７９】
デバイス202は、1つまたは複数のペンネーム246を使用して、デバイス202がデバイス証明書214を使用して前に認証されていることをLTEネットワーク112に対して認証することができる。たとえば、ユーザのプライバシー強化するために、デバイス202がデバイス証明書214を使用して成功裏に認証した後で、LTEネットワーク112はデバイスにペンネーム246または他の再認証識別子を発行することができる。LTEネットワーク112へのアクセスを得る後続の試みにおいて、デバイス202は、デバイス証明書214を送るのではなく、ペンネーム246をLTEネットワーク112に提示することができる。これは、デバイス202が、LTEネットワーク112への後続の訪問の際に、疑われることなくデバイス証明書214を送るのを回避することを可能にし得る。
【００８０】
デバイス202は1つまたは複数のセキュリティコンテキスト216を記憶することができ、各セキュリティコンテキスト216は訪問したNHネットワークに関連付けられる。セキュリティコンテキスト216は、LTEネットワーク112、LTEネットワーク112のネットワーク証明書110、LTEネットワーク112に関連付けられるペンネーム246、およびLTEネットワーク112に関する認証プロセスについての情報を記憶することができる。デバイス202は、1つまたは複数のセキュリティコンテキスト216を使用して、前に訪問したNHネットワークに再接続することができる。デバイス202がデバイス証明書214を使用してLTEネットワーク112に対して認証された後で、セキュリティコンテキスト確立器240はセキュリティコンテキスト216を生成することができる。
【００８１】
図3は、例示的な認証サーバ304を示すブロック図である。認証サーバ304は、トランシーバ330と、デバイス証明書検証器348と、ユーザ証明書検証器350と、セキュリティコンテキスト確立器352と、メモリ305とを含み得る。
【００８２】
トランシーバ330は、送信機332と受信機334とを含み得る。送信機332は、認証サーバ304がワイヤレス通信システム100内でメッセージを送信することを可能にし得る。受信機334は、認証サーバ304がワイヤレス通信システム100内でメッセージを受信することを可能

にし得る。一構成では、認証サーバ304をLTEネットワーク112内に含めることが可能である。

【００８３】

デバイス証明書検証器348は、認証サーバ304がデバイス証明書114を検証することを可能にし得る。たとえば、認証サーバ304は、デバイス証明書114をデバイス102から受信することができる。一構成では、デバイス証明書検証器348は、デバイス証明書114が信頼できるCA118によって署名されているかどうか、デバイス証明書114が期限切れしているかどうか、および/またはデバイス102がデバイス証明書114の所有者であるかどうかを決定することによって、デバイス証明書114を検証することができる。別の構成では、デバイス証明書検証器348は、デバイス証明書114が失効しているかどうかを決定することもできる。

【００８４】

ユーザ資格検証器350は、認証サーバ304がユーザ資格228を検証することを可能にし得る。たとえば、ユーザ資格検証器350は、パスワードがユーザ名に関連付けられることを検証することができる。セキュアトークンまたはバイオメトリックの使用など、ユーザ資格228を検証するための他の方法を使用することも可能である。

【００８５】

セキュリティコンテキスト確立器352は、デバイス102がLTEネットワーク112に対して認証された後で、認証サーバ304がデバイス102に関するセキュリティコンテキスト116を確立するのを助けることを可能にし得る。セキュリティコンテキスト116は、LTEネットワーク112、LTEネットワーク112のネットワーク証明書310、LTEネットワーク112に関連付けられるペンネーム246、およびLTEネットワーク112に関する認証プロセスについての情報を記憶することができる。デバイス102は、後続の訪問の際に、セキュリティコンテキスト116を使用して、LTEネットワーク112に再度接続することができる。

【００８６】

認証サーバ304は、メモリ305内に記憶された、ネットワーク証明書310、CRL324、OCSPサーバアドレス326、サービス合意354、割り当てられたペンネーム246のリスト356、ネットワークにアクセスすることが可能にされているデバイス102のリスト358(たとえば、ホワイトリスト)、ネットワークにアクセスすることが可能にされていないデバイス102のリスト360(たとえば、ブラックリスト)、およびデバイス証明書114を発行するための信頼できるCA118のリスト362を含むことも可能である。

【００８７】

認証サーバ304は、ネットワーク証明書310を使用して、デバイス102に対して認証することができる。たとえば、認証サーバ304は、ネットワーク証明書310をデバイス102に送ることができる。デバイス102は、ネットワーク証明書310が信頼できるCA118によって署名されているかどうか、ネットワーク証明書310が期限切れしているかどうか、ネットワーク証明書310が失効しているかどうか、および/または認証サーバ304がネットワーク証明書310の所有者であるかどうかを決定することができる。

【００８８】

デバイス証明書検証器348は、CRL324、OCSPサーバアドレス326、およびデバイス証明書114を発行するための信頼できるCA118のリスト362を使用してデバイス証明書114を検証することができる。たとえば、デバイス証明書検証器348は、CRL324を検査するか、またはOCSPサーバアドレス326においてOCSPサーバに問い合わせて、デバイス証明書114が失効しているかどうかを決定することができる。デバイス証明書検証器348は、デバイス証明書114を発行するための信頼できるCA118のリスト362を使用して、デバイス証明書114が信頼できるCA118によって署名されているかどうかを決定することができる。

【００８９】

認証サーバ304は、認証サーバ304がデバイス102に発行した、割り当てられたペンネーム246のリスト356を維持することができる。認証サーバ304は、次いで、デバイス102がLTEネットワーク112に対して認証する後続の試みを行うとき、デバイス102からのペンネー

ム246を使用することができる。

【００９０】

認証サーバ304は、デバイス102がLTEネットワーク112にアクセスするのを許可する前に、課金についての情報を含めて、サービス合意354の条件を受け入れることをデバイス102に要求することができる。

【００９１】

認証サーバ304は、LTEネットワーク112にアクセスすることが可能にされているデバイス102のリスト358と、LTEネットワーク112にアクセスすることが可能にされていないデバイス102のリスト360とを使用して、デバイス102がLTEネットワーク112にアクセスすることが許可されるかどうかを決定することができる。たとえば、認証サーバ304は、デバイス102がLTEネットワーク112にアクセスすることが可能にされているデバイス102のリスト358内で識別される場合、有効なデバイス証明書114を用いてデバイス102を許可することができる。別の例では、認証サーバ304は、デバイス102が有効なデバイス証明書114を有するかどうかにかかわらず、デバイス102がLTEネットワーク112にアクセスすることが可能されていないデバイス102のリスト360内で識別される場合、デバイス102にアクセスを拒否することができる。

【００９２】

図4は、デバイス102によって実行され得る認証のための方法400の一構成を例示する流れ図である。デバイス102は、LTEネットワーク112と通信することが可能であり得る。一構成では、LTEネットワーク112はニュートラルホスト(NH)LTEネットワークであってよい。したがって、方法400はLTEアクセス認証のために実行され得る。

【００９３】

デバイス102は、LTEネットワークが、SIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキスト116の確立をサポートすることを指示する第1のメッセージをLTEネットワーク112から受信することができる(402)。一構成では、第1のメッセージは、LTEネットワーク112から送られたシステム情報ブロードキャスト(SIB)メッセージであってよい。

【００９４】

SIBメッセージは、LTEネットワーク112が証明書ベースの認証および/またはニュートラルホスト動作をサポートするという指示を含み得る。この指示は、ニュートラルホスト使用のために確保された特定のネットワーク識別子値、またはLTEネットワーク112が証明書ベースの認証をサポートすることを意味することをNH対応デバイス102が理解する別の指示であってよい。たとえば、この指示は、既存のSIBメッセージの既存のフィールド内の新しい値として、または新しいSIBメッセージの一部として、既存のSIBメッセージ内の新しいフィールド内に含まれてもよい。

【００９５】

一実装形態では、第1のメッセージをLTEネットワーク112から受信すること402に応答して、デバイス102は、LTEネットワーク112によってサポートされる認証方法およびサービスプロバイダに対する要求を送ることができる。デバイス102は、LTEネットワーク112によってサポートされる認証方法およびサービスプロバイダを指示する第2のメッセージをLTEネットワーク112から受信することができる。

【００９６】

デバイス102は、接続要求をLTEネットワーク112に送ることができる。この要求は、証明書ベースの認証に対するサポートを指示することができる。一構成では、デバイス102はLTEネットワーク112とネットワーク添付手順を実行することができる。添付手順の間、デバイス102は、デバイス102がニュートラルホスト動作および/または証明書ベースの認証をサポートすること、またはデバイス102がニュートラルホストLTEネットワーク112に接続することを意図していることをLTEネットワーク112に指示することができる。この指示は、それによって、デバイス102がニュートラルホスト対応であること、証明書ベースの認証をサポートすること、および/またはニュートラルホストLTEネットワーク112に接

続することを試みていることをデバイス102がLTEネットワーク112に知らせる、添付シグナリングまたは何らかの他の機構においてニュートラルホスト動作に関して確保されたネットワーク識別子値であってよい。

【００９７】

デバイス102は、証明書ベースの認証を実行するための1つまたは複数のメッセージをLTEネットワーク112と通信することができる(404)。本明細書で使用される場合、1つまたは複数のメッセージを通信することは、メッセージを送ること、メッセージを受信すること、またはメッセージを送ることとメッセージを受信することの組合せを含み得る。したがって、1つまたは複数のメッセージを通信することは、1つまたは複数のメッセージを交換することを含み得る。さらに、1つまたは複数のメッセージを通信することは、1つまたは複数のメッセージを送ると、または受信するとすぐに、1つまたは複数の活動を実行することを含み得る。

【００９８】

一構成では、1つまたは複数のメッセージは、LTE非アクセス層(NAS)シグナリングメッセージを使用して通信され得る。1つまたは複数のメッセージは、拡張認証プロトコル(EAP)メッセージを含み得る。

【００９９】

一構成では、LTE非アクセス層(NAS)シグナリングは、LTEネットワーク112内でデバイス102と制御ノード108(たとえば、MME)との間で拡張認証プロトコル(EAP)メッセージを搬送するように拡張され得る。デバイス102は、添付メッセージ内に証明書ベースの認証またはニュートラルホスト動作に関するサポートを指示することができる。制御ノード108は、次いで、この指示を使用して、デバイス102と認証サーバ104との間の証明書ベースの認証プロセスを開始することができる。

【０１００】

証明書ベースの認証を実行するために、デバイス102は、ネットワーク証明書110を認証サーバ104から受信することができる。デバイス102は、次いで、ネットワーク証明書110を検証することができる。検証プロセスの一環として、デバイス102は、ネットワーク証明書110が信頼できる認証局118によって署名されているかどうかを決定することができる。デバイス102はまた、ネットワーク証明書110が期限切れしているかどうかを決定することができる。デバイス102はさらに、認証サーバ104がネットワーク証明書110を所有しているかどうかを決定することができる。

【０１０１】

デバイス102はさらに、ネットワーク証明書110が失効したかどうかを決定することができる。これは、ネットワーク証明書110が証明書失効リスト(CRL)224内にないことをデバイス102が検証することによって達成され得る。代替的に、デバイス102は、証明書状態サーバ120(たとえば、OCSPサーバ)に問い合わせて、ネットワーク証明書110が失効しているかどうかを決定することができる。

【０１０２】

証明書ベースの認証の一環として、デバイス102は、デバイス証明書114を認証サーバ104に送ることもできる。デバイス証明書114は、ネットワーク証明書110内の情報に基づいて暗号化され得る。デバイス証明書114はデバイス102を一意に識別することができる。たとえば、デバイス証明書114は、シリアル番号、メディアアクセス制御(MAC)アドレス、国際モバイル機器識別情報(IMEI)、または国際モバイル加入者識別情報(IMSI)など、一意の識別子(ID)を使用してデバイス102を識別することができる。

【０１０３】

一構成では、デバイス102にデバイス証明書114をプロビジョニングすることができる。一実装形態では、デバイス102が製造される時点で、デバイス102にデバイス証明書114をプロビジョニングすることができる。別の実装形態では、企業証明書登録プロセスを使用して、デバイス102にデバイス証明書114をプロビジョニングすることができる。たとえば、企業証明書登録プロセスは、簡易証明書登録プロトコル(SCEP)を利用することができる

。

【０１０４】

別の構成では、デバイス102は、デバイス102に固有の公開鍵と秘密鍵のペアを使用して自己署名デバイス証明書114を生成することができる。デバイス102は、システムオンチップ(SoC)内にプログラムされた秘密鍵を使用して公開鍵と秘密鍵のペアを生成することができる。デバイス102はさらに、デバイス102と信頼できるエンティティ(たとえば、鍵プロビジョニングサービスエンティティ(KPSE)122)との間で鍵プロビジョニングプロトコルを実行することによって、公開鍵と秘密鍵のペアを生成することができる。デバイス102は信頼できるエンティティと公開鍵を共有することができる。デバイス102の自己署名デバイス証明書114は、KPSE122から取得された公開鍵を使用して、認証サーバ104によって検証され得る。

【０１０５】

デバイス102は、証明書ベースの認証から導出された鍵に基づいてLTEセキュリティコンテキスト116を確立することができる(406)。認証の最後に、デバイスは、EAP認証から生じたEAPマスタセッション鍵(MSK)を使用して鍵K_{ASME}を導出することができる。デバイスは、K_{ASME}を使用してさらなる鍵を導出し、LTE NASおよびアクセス層(AS)セキュリティのためにそれらの鍵を使用することができる。認証プロセスの最後に、認証サーバ104は、EAPマスタセッション鍵(MSK)を制御ノード108に送ることができる。制御ノード108は、MSKを使用して、さらなる鍵を導出するためにLTEネットワーク112によって使用され得るK_{ASME}を導出し、LTE NASおよびアクセス層(AS)セキュリティのためにそれらの鍵を使用することができる。

【０１０６】

セキュリティコンテキスト116は、LTEネットワーク112、LTEネットワーク112のネットワーク証明書110、LTEネットワーク112に関連付けられるペンネーム246、および/またはLTEネットワーク112に関する認証プロセスについての情報を記憶することができる。デバイス102は、1つまたは複数のセキュリティコンテキスト116を使用して、前に訪問したLTEネットワーク112に再接続することができる。デバイス102がデバイス証明書114を使用してLTEネットワーク112に対して認証された後で、デバイス102はセキュリティコンテキスト116を生成することができる。

【０１０７】

図5は、LTEネットワーク112によって実行され得る認証のための方法500の別の構成を例示する流れ図である。一構成では、方法500は、LTEネットワーク112内に含まれた1つまたは複数のネットワークノードによって実装され得る。たとえば、LTEネットワーク112は、アクセスポイント106と、制御ノード108と、認証サーバ104とを含み得る。デバイス102は、LTEネットワーク112と通信することが可能であり得る。一構成では、LTEネットワーク112はニュートラルホスト(NH)LTEネットワークであってよい。

【０１０８】

LTEネットワーク112は、デバイス102がSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキスト116の確立をサポートするという指示をデバイス102から受信することができる(502)。たとえば、この指示は添付メッセージ内で受信され得る。一構成では、この指示は、拡張認証プロトコル(EAP)メッセージ(たとえば、EAP識別メッセージ)の一部として受信され得る。

【０１０９】

LTEネットワーク112は、証明書ベースの認証を実行するための1つまたは複数のメッセージをデバイス102と通信することができる(504)。上で説明したように、1つまたは複数のメッセージは、LTE非アクセス層(NAS)シグナリングメッセージを使用して通信され得る。1つまたは複数のメッセージはEAPメッセージを含み得る。

【０１１０】

LTEネットワーク112は、ネットワーク証明書110をデバイス102に送ることができる。デバイス102は、ネットワーク証明書110が信頼できるCA118によって署名されているかどう

か、ネットワーク証明書110が期限切れしているかどうか、ネットワーク証明書110が失効しているかどうか、および/またはLTEネットワーク112がネットワーク証明書110の所有者であるかどうかを決定することができる。

【０１１１】

証明書ベースの認証を実行するための1つまたは複数のメッセージをデバイス102と通信することは、デバイス証明書114をデバイス102から受信することを含み得る。デバイス102は、ネットワーク証明書110を検証するとすぐに、デバイス証明書114を送ることができる。LTEネットワーク112は、次いで、デバイス証明書114を検証することができる。

【０１１２】

一構成では、LTEネットワーク112は、受信されたデバイス証明書114が自己署名デバイス証明書114であると決定することができる。この構成では、LTEネットワーク112は、信頼できるエンティティ(たとえば、鍵プロビジョニングサービスエンティティ(KPSE)122)からデバイス102に関する公開鍵を取得することによって、デバイス証明書114を検証することができる。LTEネットワーク112は、次いで、公開鍵に基づいて、自己署名デバイス証明書114がデバイス102によって署名されていることを検証することができる。

【０１１３】

別の構成では、デバイス証明書114を検証することは、デバイス証明書114が信頼できる認証局(CA)118によって署名されているかどうかを決定することを含み得る。LTEネットワーク112はまた、デバイス証明書114が期限切れしているかどうかを決定することができる。LTEネットワーク112はさらに、デバイス102がデバイス証明書114を所有しているかどうかを決定することができる。

【０１１４】

LTEネットワーク112はまた、デバイス証明書114が失効しているかどうかを決定することによって、デバイス証明書114を検証することができる。これは、LTEネットワーク112が、デバイス証明書114が証明書失効リスト(CRL)324内にないことを検証することによって達成され得る。代替的に、LTEネットワーク112は、証明書状態サーバ120(たとえば、OCSPサーバ)に問い合わせて、デバイス証明書114が失効しているかどうかを決定することができる。

【０１１５】

LTEネットワーク112はまた、デバイス102がLTEネットワーク112にアクセスすることが可能にされているデバイス102のリスト358(たとえば、ホワイトリスト)内にあるかどうかを決定することによって、デバイス証明書114を検証することができる。代替的に、LTEネットワーク112は、デバイス102がLTEネットワーク112にアクセスすることが可能にされていないデバイス102のリスト360(たとえば、ブラックリスト)内にないかどうかを決定することができる。

【０１１６】

LTEネットワーク112は、証明書ベースの認証から導出された鍵に基づいてLTEセキュリティコンテキスト116を確立することができる(506)。たとえば、認証プロセスの最後に、認証サーバ104は、EAPマスタセッション鍵(MSK)を制御ノード108に送ることができる。制御ノード108は、MSKを使用して、さらなる鍵を導出するためにLTEネットワーク112によって使用され得るK_{ASME}を導出して、LTE NASおよびアクセス層(AS)セキュリティのためにそれらの鍵を使用することができる。

【０１１７】

セキュリティコンテキスト116は、LTEネットワーク112、LTEネットワーク112のネットワーク証明書110、LTEネットワーク112に関連付けられるペンネーム、および/またはLTEネットワーク112に関する認証プロセスについての情報を記憶することができる。デバイス102は、LTEネットワーク112への後続の訪問の間に、セキュリティコンテキスト116を使用してLTEネットワーク112に接続することができる。

【０１１８】

図6は、証明書ベースの認証のための手順を示すシーケンス図である。デバイス602は、

LTEネットワーク612と通信することが可能であり得る。一構成では、LTEネットワーク612はニュートラルホスト(NH)LTEネットワークであってよい。

【０１１９】

LTEネットワーク612は、証明書ベースの認証をサポートすることを指示するメッセージを送ることができる(601)。たとえば、メッセージは、ニュートラルホストLTEネットワーク612内でアクセスポイント106(たとえば、基地局または発展型ノードB(eNB))によってブロードキャストされ得る。

【０１２０】

一構成では、メッセージはシステム情報ブロック(SIB)メッセージであってよい。SIBメッセージは、LTEネットワーク612が証明書ベースの認証および/またはニュートラルホスト動作をサポートするという指示を含み得る。この指示は、ニュートラルホスト使用のために確保された特定のネットワーク識別子値、またはLTEネットワーク612が証明書ベースの認証をサポートすることを意味することをNH対応デバイス602が理解する別の指示であってよい。たとえば、この指示は、既存のSIBメッセージの既存のフィールド内の新しい値として、または新しいSIBメッセージの一部として、既存のSIBメッセージ内の新しいフィールド内に含まれてもよい。

【０１２１】

デバイス602は、デバイス602が証明書ベースの認証をサポートすることを指示する接続要求をLTEネットワーク612に送ることができる(603)。一構成では、デバイス602はネットワーク添付手順を実行することができる。

【０１２２】

添付手順の間、デバイス602は、デバイス602がニュートラルホスト動作および/または証明書ベースの認証をサポートすること、またはデバイス602がニュートラルホストLTEネットワーク612に接続することを意図していることをLTEネットワーク612に指示することができる。この指示は、それによって、デバイス602がニュートラルホスト対応であること、証明書ベースの認証をサポートすること、および/またはニュートラルホストLTEネットワーク612に接続することを試みていることをデバイス602がLTEネットワーク612に知らせる、添付シグナリングまたは何らかの他の機構においてニュートラルホスト動作に関して確保されたネットワーク識別子値であってよい。

【０１２３】

図7は、証明書ベースの認証のための別の手順を示すシーケンス図である。図7では、デバイス702はLTEネットワーク712と通信することが可能であり得る。一構成では、LTEネットワーク712はニュートラルホスト(NH)LTEネットワークであってよい。

【０１２４】

LTEネットワーク712は、証明書ベースの認証をサポートすることを指示するメッセージを送ることができる(701)。たとえば、メッセージは、図6で説明した対応するメッセージと同様であってよい。

【０１２５】

証明書ベースの認証をサポートすることを指示するメッセージをLTEネットワーク712から受信した後で、デバイス702は、LTEネットワーク712がサポートする認証方法および/またはサービスプロバイダに対する要求をLTEネットワーク712送ることができる(703)。

【０１２６】

LTEネットワーク712は、LTEネットワーク712がサポートする認証方法および/またはサービスプロバイダを指示するメッセージを送ることができる(705)。このメッセージに基づいて、デバイス702はデバイス証明書114を使用して認証することを決定することができる(すなわち、証明書ベースの認証)。

【０１２７】

デバイス702は、証明書ベースの認証をサポートすることを指示する接続要求をLTEネットワーク712に送ることができる(707)。たとえば、デバイス702は、添付メッセージ内に証明書ベースの認証に関するサポートを指示することができる。

【０１２８】
図6または図7で説明したメッセージを交換した後で、デバイス702およびLTEネットワーク712は、証明書ベースの認証の実行を可能にするためのシグナリングメッセージを交換することができる。たとえば、従来のLTE認証を実行する代わりに、デバイス702およびLTEネットワーク712は、証明書ベースの認証を可能にするLTEシグナリングを交換することができる。
【０１２９】
LTEネットワーク712サイドで、認証サーバ104(たとえば、認証、許可、およびアカウンティング(AAA)サーバ)は、証明書ベースの認証をサポートするように適合された制御ノード108(たとえば、MME)と協調して、デバイス702とLTEシグナリングを交換することができる。LTEシグナリングは、AAAベースの認証に関するEAPシグナリングを転送するように設計された非アクセス層(NAS)メッセージを含み得る。LTEシグナリングは、あらかじめ確立されたLTEセキュリティコンテキスト116なしに、デバイス702と交換されることが可能である。
【０１３０】
成功裏の証明書ベースの認証の後で、デバイス702およびLTEネットワーク712は、証明書ベースの認証に基づいてキー材料(keying material)を導出することができる。認証プロセスの最後に、デバイス702は、EAP認証から生じたEAPマスタセッション鍵(MSK)を使用して鍵K_{ASME}を導出することができる。さらに、認証プロセスの最後に、AAAサーバは、EAPマスタセッション鍵(MSK)をMMEに送ることができる。MMEはMSKを使用して、鍵K_{ASME}を導出することができる。デバイス702およびMMEは、キー材料K_{ASME}を使用して、(たとえば、3GPP TS33.401定義されているように)デバイス702とLTEネットワーク712との間のLTEアクセス層(AS)およびASおよびNAS通信をさらに確保するために使用され得るNASセキュリティ鍵の明確なセットを含めて、NHネットワーク固有のLTEセキュリティコンテキスト116を導出することができる。
【０１３１】
図8は、証明書ベースの認証のためのさらに別の手順を示すシーケンス図である。図8では、デバイス802はLTEネットワーク112と通信することが可能であり得る。一構成では、LTEネットワーク112はニュートラルホスト(NH)LTEネットワークであってよい。LTEネットワーク112は認証サーバ804を含み得る。
【０１３２】
デバイス802は、LTEネットワーク112にアクセスするための要求を認証サーバ804に送ることができる(801)。認証サーバ804は、ネットワーク証明書110をデバイス802に送ることができる(803)。
【０１３３】
デバイス802は、ネットワーク証明書110を検証することができる(805)。ネットワーク証明書110を検証する(805)ために、デバイス802は、ネットワーク証明書110が信頼できるCA118によって署名されているかどうかを決定することができる。デバイス802は、ネットワーク証明書110を発行するための信頼できるCA118の記憶されたリスト242に基づいて、この決定を行うことができる。デバイス802はさらに、ネットワーク証明書110が期限切れしているかどうかを決定することができる。デバイス802は、ネットワーク証明書110の有効期限を現在の日付と比較することができる。現在の日付が有効期限よりも遅い場合、デバイス802はネットワーク証明書110が期限切れしていると決定することができる。
【０１３４】
ネットワーク証明書110を検証する(805)ために、デバイス802はまた、ネットワーク証明書110が失効しているかどうかを決定することができる。ネットワーク証明書110が失効しているかどうかを決定するために、デバイス802は、ネットワーク証明書110がCRL224内にないことを検証することができるか、またはデバイス802は証明書状態サーバ120(たとえば、OCSPサーバ)に問い合わせることができる。
【０１３５】

ネットワーク証明書110を検証する(805)ために、デバイス802はまたさらに、認証サーバ804がネットワーク証明書110を所有しているかどうかを決定することができる。認証サーバ804がネットワーク証明書110を所有しているかどうかを決定するために、デバイス802は、ネットワーク証明書110内の公開鍵を使用してメッセージを暗号化し、次いで、認証サーバ804がそのメッセージを正確に解読することができることを検証することができ、それによって、認証サーバ804がネットワーク証明書110に関連付けられる秘密鍵を所有していることを実証する。

【０１３６】

デバイス802は、次いで、デバイス証明書114を認証サーバ804に送ることができる(807)。一構成では、疑われることなく、デバイス証明書114を送ることを回避するために、デバイス802は、ネットワーク証明書110内の公開鍵を使用してデバイス証明書114を暗号化することができる。認証サーバ804は、必要な場合、デバイス証明書114を解読し、次いで、デバイス証明書114を検証することができる(809)。

【０１３７】

デバイス証明書114を検証する(809)ために、認証サーバ804は、デバイス証明書114が信頼できる認証局118によって署名されているかどうかを決定することができる。認証サーバ804は、デバイス証明書114を発行するための信頼できるCA118の記憶されたリスト362に基づいて、この決定を行うことができる。

【０１３８】

デバイス証明書114を検証する(809)ために、認証サーバ804はまた、デバイス証明書114が期限切れしているかどうかを決定することができる。認証サーバ804は、デバイス証明書114の有効期限を現在の日付と比較することができる。現在の日付が有効期限よりも遅い場合、認証サーバ804はデバイス証明書114が期限切れしていると決定することができる。

【０１３９】

デバイス証明書114を検証する(809)ために、認証サーバ804はまた、デバイス証明書114が失効しているかどうかを決定することができる。デバイス証明書114が失効しているかどうかを決定するために、認証サーバ804は、デバイス証明書114がCRL324内にないことを検証することができるか、または認証サーバ804はOCSPサーバに問い合わせることができる。

【０１４０】

デバイス証明書114を検証する(809)ために、認証サーバ804はまた、デバイス802がデバイス証明書114を所有しているかどうかを決定することができる。デバイス802がネットワーク証明書114を所有しているかどうかを決定するために、認証サーバ804は、デバイス証明書114内の公開鍵を使用してメッセージを暗号化することができ、次いで、デバイス802がそのメッセージを正確に解読することができることを検証することができ、それによって、デバイス802がデバイス証明書114に関連付けられる秘密鍵を所有していることを実証する。別の構成では、デバイス証明書114は自己署名デバイス証明書114であってよい。デバイス802の自己署名デバイス証明書114は、信頼できるエンティティ(たとえば、KPSE122)から取得されたデバイス802の公開鍵を使用して、認証サーバ804によって検証され得る。

【０１４１】

一構成では、認証サーバ804はさらに、デバイス802がネットワーク112にアクセスすることが可能にされているデバイス802のリスト358(すなわち、ホワイトリスト)内にあるかどうかを決定することによって、デバイス証明書114を検証することができる(809)。別の構成では、認証サーバ804は、デバイス802がネットワーク112にアクセスすることが可能にされていないデバイス802のリスト360(すなわち、ブラックリスト)内にあるかどうかを決定することができる。さらに別の構成では、認証サーバ804は、デバイス証明書114が失効しているかどうかを決定する代わりに、ホワイトリストまたはブラックリストを検査することができる。

【０１４２】
いくつかの構成では、認証サーバ804は、次いで、デバイス802からユーザ資格228を要求することができる(811)。デバイス802は、ユーザ資格228を送ることができる(813)。認証サーバ804はユーザ資格228を検証することができる(815)。たとえば、認証サーバ804は、パスワードがユーザ名に関連付けられることを検証することができる。セキュアトークンまたはバイオメトリックの使用など、ユーザ資格228を検証するための他の方法を使用することも可能である。認証サーバ804は、ユーザ資格228に基づいて、LTEネットワーク112へのアクセスをデバイス802に付与することができる。
【０１４３】
他の構成では、認証サーバ804は、サービス合意354を受け入れるための要求をデバイス802に送ることができる(817)。この要求はサービス合意354の複写を含み得る。サービス合意354はネットワークアクセスに関する条件を特定することができる。サービス合意354はまた、ネットワークアクセスに関連付けられる課金情報を含み得る。デバイス802は、サービス合意354を受け入れるメッセージを認証サーバ804に送ることができる(819)。
【０１４４】
さらに他の構成では、認証サーバ804は、ペンネーム246または他の再認証識別子をデバイス802に送ることができる(821)。ネットワーク112への後続の訪問の際に、デバイス802は、ネットワーク112を認証するために、デバイス証明書114の代わりにペンネーム246を使用することができる。デバイス証明書114の代わりにペンネーム246を使用することは、ユーザプライバシーを強化し得る。
【０１４５】
認証サーバ804は、次いで、ネットワーク112へのアクセスをデバイス802に付与することができる(823)。アクセスは、サービス合意354に記載されたサービスおよび課金条件によって管理され得る。
【０１４６】
図9は、デバイス902内に含まれ得るいくつかの構成要素を示す。図9に関して説明するデバイス902は、図1～図8のうちの1つまたは複数に関して説明したデバイス102、202、602、702、802のうちの1つまたは複数の例であり得る、かつ/またはそれらに従って実装され得る。
【０１４７】
デバイス902はプロセッサ903を含む。プロセッサ903は、汎用のシングルチップマイクロプロセッサまたはマルチチップマイクロプロセッサ(たとえば、アドバンスドRISC(縮小命令セットコンピュータ)マシン(ARM))、専用マイクロプロセッサ(たとえば、デジタル信号プロセッサ(DSP))、マイクロコントローラ、プログラマブルゲートアレイなどであってよい。プロセッサ903は中央処理装置(CPU)と呼ばれ得る。図9のデバイス902内に単一のプロセッサ903のみが示されているが、代替構成では、プロセッサの組合せ(たとえば、ARMとDSP)が使用され得る。
【０１４８】
デバイス902は、プロセッサと電子通信しているメモリ905も含む(すなわち、プロセッサはメモリから情報を読み取ること、および/またはメモリに情報を書き込むことができる)。メモリ905は、電子情報を記憶することができる任意の電子構成要素であってよい。メモリ905は、ランダムアクセスメモリ(RAM)、読取り専用メモリ(ROM)、磁気ディスク記憶媒体、光記憶媒体、RAM内のフラッシュメモリデバイス、プロセッサとともに含まれるオンボードメモリ、EPROMメモリ、EEPROMメモリ、レジスタなど、およびそれらの組合せとして構成され得る。
【０１４９】
データ907aおよび命令909aをメモリ905内に記憶することができる。命令は、1つまたは複数のプログラム、ルーチン、サブルーチン、機能、手順、コードなどを含み得る。命令は、単一のコンピュータ可読ステートメントまたは多数のコンピュータ可読ステートメントを含み得る。命令909aは、本明細書で開示する方法を実装するようにプロセッサ903に

よって実行可能であってよい。命令909aを実行することは、メモリ905に記憶されたデータ907aの使用を伴う場合がある。プロセッサ903が命令909を実行すると、命令の様々な部分909bがプロセッサ903上にロードされてよく、データの様々な断片907bがプロセッサ903上にロードされ得る。

【０１５０】

デバイス902は、アンテナ917を介したデバイス902との間の信号の送信および受信を可能にするための送信機932および受信機934も含み得る。送信機932および受信機934は、集合的にトランシーバ930と呼ばれ得る。デバイス902は、複数の送信機、複数のアンテナ、複数の受信機、および/または複数のトランシーバも含み得る(図示せず)。

【０１５１】

デバイス902は、デジタル信号プロセッサ(DSP)921を含み得る。デバイス902は、通信インターフェース923も含み得る。通信インターフェース923は、ユーザがデバイス902と対話することを可能にし得る。

【０１５２】

デバイス902の様々な構成要素は、1つまたは複数のバスによって互いに結合することができ、それらのバスとしては、電力バス、制御信号バス、ステータス信号バス、データバスなどを含むことができる。明確にするために、様々なバスはバスシステム919として図9に示される。

【０１５３】

図10は、認証サーバ1004内に含まれ得るいくつかの構成要素を示す図である。図10に関して説明する認証サーバ1004は、図1～図8のうちの1つまたは複数に関して説明した認証サーバ104、304、804またはネットワークノードのうちの1つまたは複数の例であり得る、かつ/またはそれらに従って実装され得る。

【０１５４】

認証サーバ1004はプロセッサ1003を含む。プロセッサ1003は、汎用のシングルチップマイクロプロセッサまたはマルチチップマイクロプロセッサ(たとえば、アドバンスドRISC(縮小命令セットコンピュータ)マシン(ARM))、専用マイクロプロセッサ(たとえば、デジタル信号プロセッサ(DSP))、マイクロコントローラ、プログラマブルゲートアレイなどであってよい。プロセッサ1003は中央処理装置(CPU)と呼ばれ得る。図10の認証サーバ1004には、1つのプロセッサ1003しか示されていないが、代替構成では、プロセッサの組合せ(たとえばARMとDSP)が使用されてもよい。

【０１５５】

認証サーバ1004は、プロセッサと電子通信しているメモリ1005も含む(すなわち、プロセッサはメモリから情報を読み取ること、および/またはメモリに情報を書き込むことができる)。メモリ1005は、電子情報を記憶することができる任意の電子構成要素であってよい。メモリ1005は、ランダムアクセスメモリ(RAM)、読取り専用メモリ(ROM)、磁気ディスク記憶媒体、光記憶媒体、RAM内のフラッシュメモリデバイス、プロセッサとともに含まれるオンボードメモリ、EPROMメモリ、EEPROMメモリ、レジスタなど、およびそれらの組合せとして構成され得る。

【０１５６】

データ1007aおよび命令1009aをメモリ1005内に記憶することができる。命令は、1つまたは複数のプログラム、ルーチン、サブルーチン、機能、手順、コードなどを含み得る。命令は、単一のコンピュータ可読ステートメントまたは多数のコンピュータ可読ステートメントを含み得る。命令1009aは、本明細書で開示する方法を実装するようにプロセッサ1003によって実行可能であってよい。命令1009aを実行することは、メモリ1005に記憶されたデータ1007aの使用を伴う場合がある。プロセッサ1003が命令1009を実行すると、命令の様々な部分1009bがプロセッサ1003上にロードされてよく、データの様々な断片1007bがプロセッサ1003上にロードされ得る。

【０１５７】

認証サーバ1004は、アンテナ1017を介した認証サーバ1004との間の信号の送信および受

信を可能にするための送信機1032および受信機1034も含み得る。送信機1032および受信機1034は、集合的にトランシーバ1030と呼ばれ得る。認証サーバ1004は、複数の送信機、複数のアンテナ、複数の受信機、および/または複数のトランシーバも含み得る(図示せず)。

【０１５８】

認証サーバ1004は、デジタル信号プロセッサ(DSP)1021を含み得る。認証サーバ1004は、通信インターフェース1023も含み得る。通信インターフェース1023は、ユーザが認証サーバ1004と対話することを可能にし得る。

【０１５９】

認証サーバ1004の様々な構成要素は、1つまたは複数のバスによって互いに結合することができ、それらのバスとしては、電力バス、制御信号バス、ステータス信号バス、データバスなどを含むことができる。明確にするために、様々なバスはバスシステム1019として図10に示される。

【０１６０】

上記の説明では、時として参照番号が様々な用語に関連して使用されている。用語が参照番号に関して使用されるとき、これは、諸図のうちの1つまたは複数において示される特定の要素を指すことを意味し得る。用語が参照番号なしで使用されるとき、これはいかなる特定の図にも限定せずに、一般にその用語を指すことを意味し得る。

【０１６１】

「決定する」という用語は多種多様な動作を包含し、したがって「決定する」ことは、計算すること、算出すること、処理すること、導出すること、調査すること、ルックアップすること(たとえば、テーブル、データベース、または別のデータ構造をルックアップすること)、確認することなどを含み得る。さらに、「決定する」ことは、受信すること(たとえば、情報を受信すること)、アクセスすること(たとえば、メモリ内のデータにアクセスすること)などを含み得る。また、「決定すること」は、解決すること、選択すること、選ぶこと、確立することなどを含むことができる。

【０１６２】

「に基づいて」という語句は、別段に明記されていない限り、「だけに基づいて」を意味するのではない。言い換えれば、「に基づいて」という語句は、「だけに基づいて」と「に少なくとも基づいて」の両方を記述する。

【０１６３】

「プロセッサ」という用語は、汎用プロセッサ、中央処理装置(CPU)、マイクロプロセッサ、デジタル信号プロセッサ(DSP)、コントローラ、マイクロコントローラ、ステートマシンなどを含むように、広く解釈されるものとする。いくつかの状況下では、「プロセッサ」は、特定用途向け集積回路(ASIC)、プログラマブル論理デバイス(PLD)、フィールドプログラマブルゲートアレイ(FPGA)などを指し得る。「プロセッサ」という用語は、たとえば、デジタル信号プロセッサ(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、デジタル信号プロセッサ(DSP)コアと連動する1つまたは複数のマイクロプロセッサ、または他の任意のそのような構成など、処理デバイスの組合せを指すことができる。

【０１６４】

「メモリ」という用語は、電子情報を記憶することができる任意の電子部品を含むように、広く解釈されるものとする。メモリという用語は、たとえばランダムアクセスメモリ(RAM)、読取り専用メモリ(ROM)、不揮発性ランダムアクセスメモリ(NVRAM)、プログラマブル読取り専用メモリ(PROM)、消去可能プログラマブル読取り専用メモリ(EPROM)、電気的消去可能PROM(EEPROM)、フラッシュメモリ、磁気または光学のデータストレージ、レジスタなどの様々なタイプのプロセッサ可読媒体を指し得る。メモリは、プロセッサがメモリから情報を読み取り、かつ/またはメモリに情報を書き込むことができる場合、プロセッサと電子通信すると言われる。プロセッサと一体のメモリは、プロセッサと電子的に通信している。

【０１６５】
「命令」および「コード」という用語は、任意のタイプのコンピュータ可読ステートメントを含むように、広く解釈されるべきである。たとえば、「命令」および「コード」という用語は、1つまたは複数のプログラム、ルーチン、サブルーチン、関数、手順などを指し得る。「命令」および「コード」は、単一のコンピュータ可読ステートメントまたは多数のコンピュータ可読ステートメントを含んでよい。
【０１６６】
本明細書で説明する構成のうちの任意の1つに関して説明した特徴、機能、手順、構成要素、要素、構造などのうちの1つまたは複数は、互換可能な場合、本明細書で説明した他の構成のいずれかに関して説明した機能、手順、構成要素、要素、構造などのうちの1つまたは複数と組み合わせられ得ることに留意されたい。言い換えると、本明細書に記載した、機能、プロシージャ、構成要素、要素などのどの互換可能な組合せも、本明細書で開示したシステムおよび方法に従って実装され得る。
【０１６７】
本明細書で説明される機能は、プロセッサ可読またはコンピュータ可読媒体上に1つまたは複数の命令として記憶され得る。「コンピュータ可読媒体」という用語は、コンピュータまたはプロセッサによってアクセスされ得る任意の利用可能な媒体を指す。限定ではなく、例として、そのような媒体は、ランダムアクセスメモリ(RAM)、読取り専用メモリ(ROM)、電気的消去可能プログラマブル読取り専用メモリ(EEPROM)、フラッシュメモリ、コンパクトディスク読取り専用メモリ(CD-ROM)もしくは他の光ディスクストレージ、磁気ディスクストレージデバイスもしくは他の磁気ストレージデバイス、あるいは所望のプログラムコードを命令またはデータ構造の形で記憶するために使用可能であり、かつコンピュータによってアクセス可能な任意の他の媒体を含み得る。本明細書で使用される場合、ディスク(disk)およびディスク(disc)は、コンパクトディスク(disc)(CD)、レーザーディスク（登録商標）(disc)、光ディスク(disc)、デジタル多用途ディスク(disc)(DVD)、フロッピーディスク(disk)、およびブルーレイ(登録商標)ディスク(disc)を含み、ディスク(disk)は、通常、磁気的にデータを再生し、ディスク(disc)は、レーザーで光学的にデータを再生する。コンピュータ可読媒体は、有形および非一時的であってよいことに留意されたい。「コンピュータプログラム製品」という用語は、コンピューティングデバイスまたはプロセッサによって実行、処理、または計算され得るコードまたは命令(たとえば、「プログラム」)と組み合わせて、コンピューティングデバイスまたはプロセッサを指す。本明細書で使用される場合、「コード」という用語は、コンピューティングデバイスまたはプロセッサによって実行可能な、ソフトウェア、命令、コード、またはデータを指し得る。
【０１６８】
ソフトウェアまたは命令はまた、送信媒体を介して送信することもできる。たとえば、ウェブサイト、サーバ、または他の遠隔ソースから、同軸ケーブル、光ファイバケーブル、より対線、デジタル加入者回線(DSL)、または赤外線、無線、およびマイクロ波などのワイヤレス技術を使用してソフトウェアが送信される場合、上記の同軸ケーブル、光ファイバケーブル、より対線、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、伝送媒体の定義に含まれる。
【０１６９】
本明細書で開示した方法は、説明した方法を達成するための1つまたは複数のステップまたは活動を含む。方法ステップおよび/または方法活動は、特許請求の範囲から逸脱することなく互いに交換され得る。言い換えると、ステップまたは活動の特定の順序が、説明される方法の正しい動作のために要求されない限り、特定のステップおよび/または活動の順序および/または使用は、特許請求の範囲から逸脱することなく変更され得る。
【０１７０】
さらに、たとえば図4～図8によって示したものなど、本明細書で説明した方法および技法を実行するためのモジュールおよび/または他の適切な手段は、ダウンロードされてよ

く、かつ/またはそうでなくデバイスによって取得され得ることを理解されたい。たとえば、本明細書で説明した方法を実行するための手段の転送を容易にするために、デバイスがサーバに結合され得る。あるいは、本明細書で説明した様々な方法は、記憶手段(たとえば、ランダムアクセスメモリ(RAM)、読取り専用メモリ(ROM)、コンパクトディスク(CD)またはフロッピーディスクなどの物理的記憶媒体など)をデバイスに結合または提供した後、デバイスが様々な方法を得ることができるように、記憶手段を介して提供され得る。その上、本明細書において説明した方法および技法をデバイスに提供するための任意の他の適切な技法を利用することができる。

【０１７１】

特許請求の範囲は、上で説明された厳密な構成および構成要素に限定されないことは理解されたい。様々な修正、変更、および変形は、特許請求の範囲から逸脱することなく、本明細書で説明したシステム、方法、および装置の構成、操作、および細部において行われ得る。

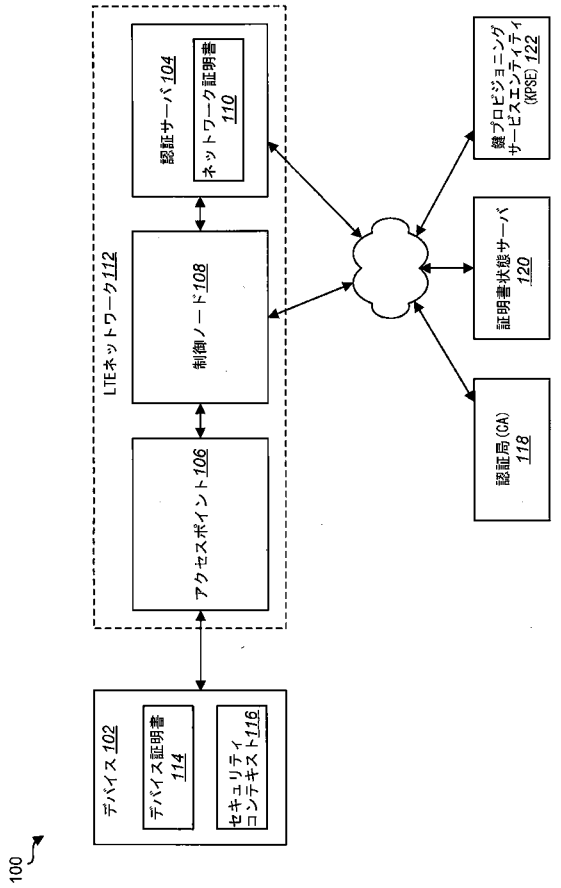
【符号の説明】

【０１７２】

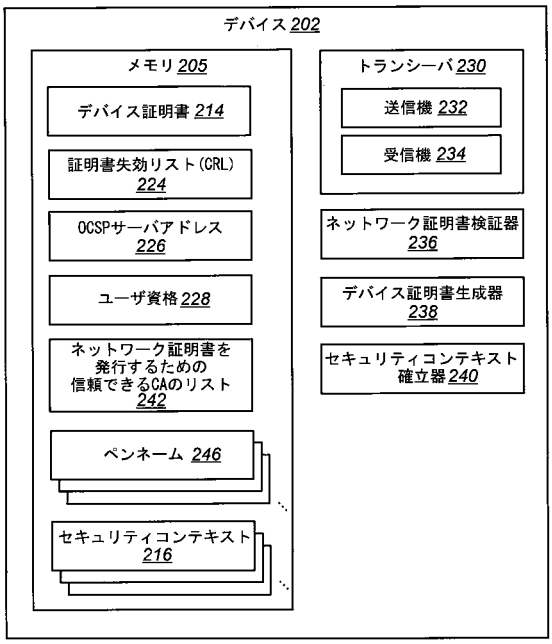
100 ワイヤレス通信システム
102 デバイス
104 認証サーバ
106 アクセスポイント
108 制御ノード(CN)
110 ネットワーク証明書
112 LTEネットワーク
114 デバイス証明書
116 セキュリティコンテキスト
118 認証局(CA)、ルートCA
120 証明書状態サーバ
122 鍵プロビジョニングサービスエンティティ(KPSE)
202 デバイス
205 メモリ
214 デバイス証明書
216 セキュリティコンテキスト
224 証明書失効リスト(CRL)
226 OCSPサーバアドレス
228 ユーザ資格
230 トランシーバ
232 送信機
234 受信機
236 ネットワーク証明書検証器
238 デバイス証明書生成器
240 セキュリティコンテキスト確立器
242 ネットワーク証明書を発行するための信頼できるCAのリスト
246 ペンネーム
304 認証サーバ
305 メモリ
310 ネットワーク証明書
324 CRL
326 OCSPサーバアドレス
330 トランシーバ
332 送信機
334 受信機

348 デバイス証明書検証器
350 ユーザ資格検証器
352 セキュリティコンテキスト確立器
354 サービス合意
356 割り当てられたペンネームのリスト
358 ネットワークにアクセスすることが可能にされているデバイスのリスト
360 ネットワークにアクセスすることが可能にされていないデバイスのリスト
362 デバイス証明書を発行するための信頼できるCAのリスト
400 方法
500 方法
602 デバイス
612 LTEネットワーク
702 デバイス
712 LTEネットワーク
802 デバイス
804 認証サーバ
902 デバイス
903 プロセッサ
905 メモリ
907a データ
907b データの様々な断片
909 命令
909a 命令
909b 命令の様々な部分
917 アンテナ
919 バスシステム
921 デジタル信号プロセッサ(DSP)
923 通信インターフェース
930 トランシーバ
932 送信機
934 受信機
1003 プロセッサ
1004 認証サーバ
1005 メモリ
1007a データ
1007b データの様々な断片
1009 命令
1009a 命令
1009b 命令の様々な部分
1017 アンテナ
1019 バスシステム
1021 デジタル信号プロセッサ(DSP)
1023 通信インターフェース
1030 トランシーバ
1032 送信機
1034 受信機

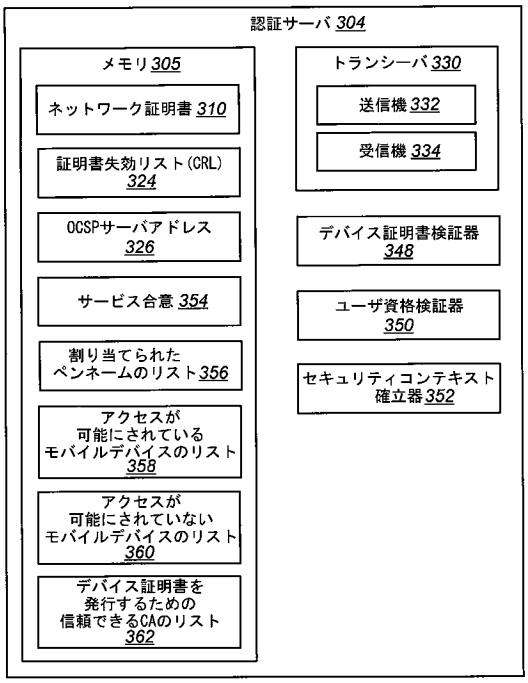
【図１】


認証サーバ 104
ネットワーク証明書 110
制御ノード 108
アクセスポイント 106
LTEネットワーク 112
鍵プロビジョニングサービスエンティティ (KPSE) 122
証明書状態サーバ 120
認証局 (CA) 118
デバイス 102
デバイス証明書 114
セキュリティコンテキスト 116
100

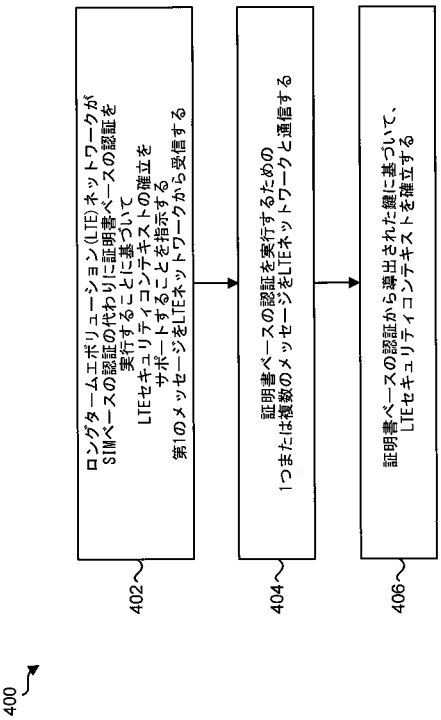
【図２】


デバイス 202
メモリ 205
デバイス証明書 214
証明書失効リスト (CRL) 224
OCSPサーバアドレス 226
ユーザ資格 228
ネットワーク証明書を発行するための信頼できるCAのリスト 242
ペンネーム 246
セキュリティコンテキスト 216
トランシーバ 230
送信機 232
受信機 234
ネットワーク証明書検証器 236
デバイス証明書生成器 238
セキュリティコンテキスト確立器 240

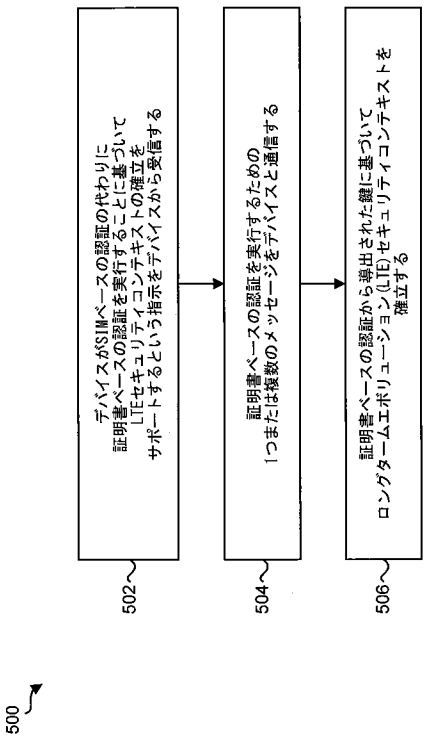
【図３】


認証サーバ 304
メモリ 305
ネットワーク証明書 310
証明書失効リスト (CRL) 324
OCSPサーバアドレス 326
サービス合意 354
割り当てられたペンネームのリスト 356
アクセスが可能にされているモバイルデバイスのリスト 358
アクセスが可能にされていないモバイルデバイスのリスト 360
デバイス証明書を発行するための信頼できるCAのリスト 362
トランシーバ 330
送信機 332
受信機 334
デバイス証明書検証器 348
ユーザ資格検証器 350
セキュリティコンテキスト確立器 352

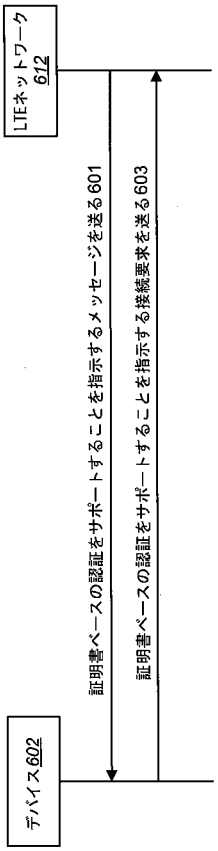
【図４】


ロングタームエボリューション (LTE) ネットワークがSIMベースの認証の代わりに証明書ベースの認証を実行することに基づいてLTEセキュリティコンテキストの確立をサポートすることを指示する第1のメッセージをLTEネットワークから受信する
402
証明書ベースの認証を実行するための1つまたは複数のメッセージをLTEネットワークと通信する
404
証明書ベースの認証から導出された鍵に基づいて、LTEセキュリティコンテキストを確立する
406
400

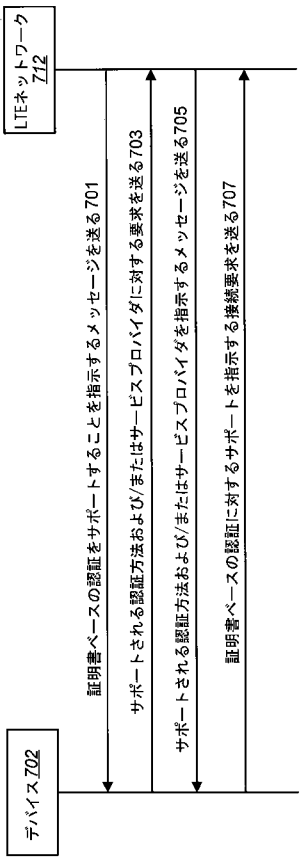
【図５】


デバイスがSIMベースの認証の代わりに
証明書ベースの認証を実行することに基づいて
LTEセキュリティコンテキストの確立を
サポートするという指示をデバイスから受信する
502
証明書ベースの認証を実行するための
1つまたは複数のメッセージをデバイスと通信する
504
証明書ベースの認証から導出された鍵に基づいて
ロングタームエボリューション(LTE)セキュリティコンテキストを
確立する
506
500

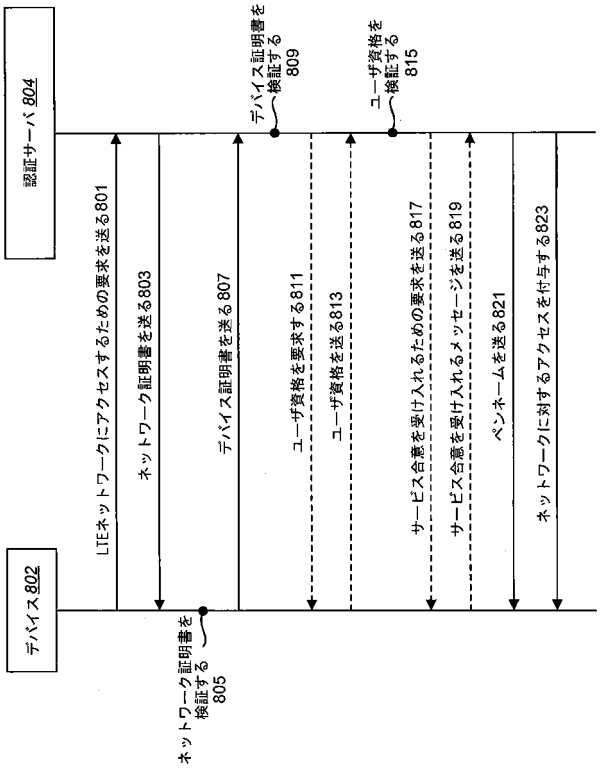
【図６】


LTEネットワーク
612
証明書ベースの認証をサポートすることを指示するメッセージを送る601
証明書ベースの認証をサポートすることを指示する接続要求を送る603
デバイス602

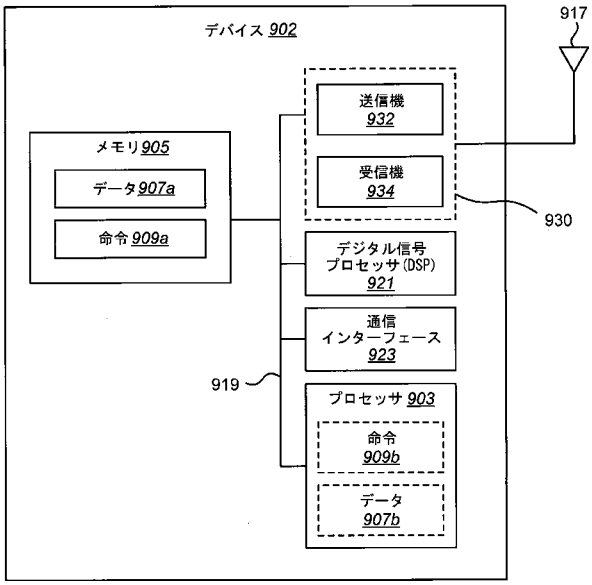
【図７】


LTEネットワーク
712
証明書ベースの認証をサポートすることを指示するメッセージを送る701
サポートされる認証方法および/またはサービスプロバイダに対する要求を送る703
サポートされる認証方法および/またはサービスプロバイダを指示するメッセージを送る705
証明書ベースの認証に対するサポートを指示する接続要求を送る707
デバイス702

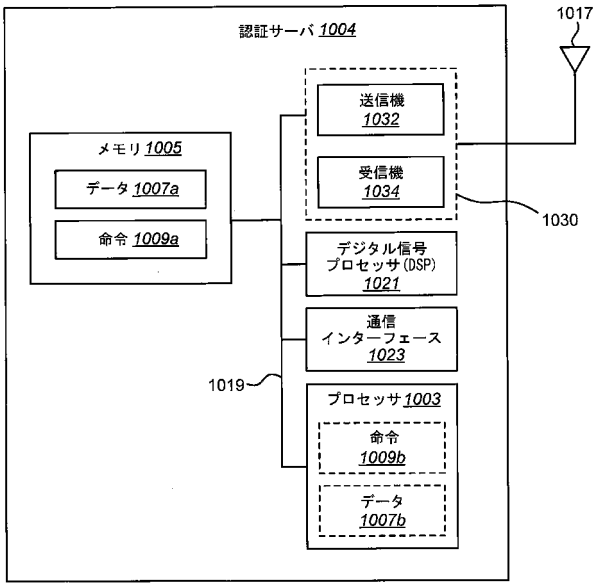
【図８】


認証サーバ804
デバイス証明書を
検証する
809
ユーザ資格を
検証する
815
LTEネットワークにアクセスするための要求を送る801
ネットワーク証明書を送る803
デバイス証明書を送る807
ユーザ資格を要求する811
ユーザ資格を送る813
サービス合意を受け入れるための要求を送る817
サービス合意を受け入れるメッセージを送る819
ペンネームを送る821
ネットワークに対するアクセスを付与する823
デバイス802
ネットワーク証明書を
検証する
805

【図９】


デバイス 902
917
送信機 932
受信機 934
930
メモリ 905
データ 907a
命令 909a
デジタル信号プロセッサ(DSP) 921
通信インターフェース 923
919
プロセッサ 903
命令 909b
データ 907b

【図１０】


認証サーバ 1004
1017
送信機 1032
受信機 1034
1030
メモリ 1005
データ 1007a
命令 1009a
デジタル信号プロセッサ(DSP) 1021
通信インターフェース 1023
1019
プロセッサ 1003
命令 1009b
データ 1007b

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/050602

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/06
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 practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/012165 A1 (POPOVICH GEORGE [US] ET AL) 10 January 2013 (2013-01-10) paragraphs [0030], [0041], [0042], [0044], [0048], [0050], [0052] claim 7 figures 1,3,4,5 -----	1-46
A	US 2010/017603 A1 (JONES MARK [CA]) 21 January 2010 (2010-01-21) paragraph [0029] -----	14,42

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 December 2015	11/12/2015

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	Pajatakis, Emmanouil

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/050602

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013012165 A1	10-01-2013	AU 2012283026 A1	30-01-2014
		CA 2841094 A1	17-01-2013
		EP 2730074 A1	14-05-2014
		US 2013012165 A1	10-01-2013
		WO 2013009508 A1	17-01-2013
US 2010017603 A1	21-01-2010	NONE	

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

フロントページの続き

(51)Int.Cl.		F I			テーマコード（参考）
Ｈ０４Ｍ 11/00	*(2006.01)*	Ｈ０４Ｍ	1/00	Ｒ	
		Ｈ０４Ｍ	11/00	３０２	

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

(72)発明者 アナンド・パラニグンダー
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 KA02 KA05 MA01 NA02 NA37 NA38 PA02
5K067 AA30 AA32 DD11 EE02 EE10 EE16
5K127 AA05 AA21 BA03 GE02 GE03 GE04 GE05
5K201 AA07 AA08 AA09 BB08 BC23 CB08 CB12 CB15 CC02 EA07
EC06 ED05