【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成30年9月27日(2018.9.27)

【公表番号】特表2017-535989(P2017-535989A)
【公表日】平成29年11月30日(2017.11.30)
【年通号数】公開・登録公報2017-046
【出願番号】特願2017-514477(P2017-514477)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０９Ｃ　1/00　(2006.01)
Ｈ０４Ｗ　12/06　(2009.01)
Ｈ０４Ｗ　12/04　(2009.01)
Ｈ０４Ｍ　1/00　(2006.01)
Ｈ０４Ｍ　11/00　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｄ
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｇ０９Ｃ　1/00　６４０Ｅ
Ｈ０４Ｗ　12/06
Ｈ０４Ｗ　12/04
Ｈ０４Ｍ　1/00　Ｒ
Ｈ０４Ｍ　11/00　３０２

【手続補正書】
【提出日】平成30年8月13日(2018.8.13)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
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であって、前記デバイス証明書が前記デバイスを一意に識別し、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)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)のうちの少なくとも1つまたは組合せに基づく、ステップと、
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システム情報ブロードキャスト(SIB)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】

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３】
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2に記載の方法。
【請求項４】
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６】
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5に記載の方法。
【請求項７】
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5に記載の方法。
【請求項８】
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９】
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8に記載の方法。
【請求項１０】
前記ネットワーク証明書が失効しているかどうかを判断する前記ステップが、
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9に記載の方法。
【請求項１１】
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9に記載の方法。
【請求項１２】
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１３】
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１４】
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１５】
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１６】
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15に記載の方法。
【請求項１７】
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１８】
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17に記載の方法。
【請求項１９】
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17に記載の方法。
【請求項２０】
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、
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ように構成されたデバイス証明書生成器であって、前記デバイス証明書が前記デバイスを一意に識別し、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)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)のうちの少なくとも1つまたは組合せに基づく、デバイス証明書生成器と、
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システム情報ブロードキャスト(SIB)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２１】
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、
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ための手段であって、前記デバイス証明書が前記デバイスを一意に識別し、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)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)のうちの少なくとも1つまたは組合せに基づく、手段と、
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システム情報ブロードキャスト(SIB)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２２】
コンピュータに、
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ことであって、前記デバイス証明書が前記デバイスを一意に識別し、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)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)のうちの少なくとも1つまたは組合せに基づく、ことを行わせ、
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システム情報ブロードキャスト(SIB)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、コンピュータ可読記録媒体。
【請求項２３】
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、
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前記LTEネットワークが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システム情報ブロードキャスト(SIB)メッセージを送信するステップと、
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であって、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)メッセージを含み、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、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２４】
前記指示が添付メッセージ内で受信される、請求項23に記載の方法。
【請求項２５】
前記指示がEAPメッセージの一部として受信される、請求項23に記載の方法。
【請求項２６】
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23に記載の方法。
【請求項２７】
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23に記載の方法。
【請求項２８】

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23に記載の方法。
【請求項２９】
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28に記載の方法。
【請求項３０】
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28に記載の方法。
【請求項３１】
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30に記載の方法。
【請求項３２】
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31に記載の方法。
【請求項３３】
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30に記載の方法。
【請求項３４】
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23に記載の方法。
【請求項３５】
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23に記載の方法。
【請求項３６】
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23に記載の方法。

【請求項３７】
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23に記載の方法。
【請求項３８】
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、
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前記LTEネットワークが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システム情報ブロードキャスト(SIB)メッセージを送信し、
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であって、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)メッセージを含み、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、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３９】
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、
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前記LTEネットワークが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システム情報ブロードキャスト(SIB)メッセージを送信するための手段と、
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であって、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)メッセージを含み、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、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４０】
コンピュータに、
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前記LTEネットワークが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システム情報ブロードキャスト(SIB)メッセージを送信することと、
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することと、
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ことであって、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)メッセージを含み、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、ことと、

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ことと

を行わせるためのコードを含む、コンピュータ可読記録媒体。