【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20日(2018.9.20)

【公表番号】特表2017-535998(P2017-535998A)
【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2017-515932(P2017-515932)
【国際特許分類】
Ｈ０４Ｗ　12/06　(2009.01)
Ｈ０４Ｗ　12/04　(2009.01)
Ｈ０４Ｗ　12/08　(2009.01)
Ｈ０４Ｌ　 9/32　(2006.01)
Ｇ０９Ｃ　 1/00　(2006.01)
Ｈ０４Ｍ　11/00　(2006.01)
【ＦＩ】
Ｈ０４Ｗ　12/06
Ｈ０４Ｗ　12/04
Ｈ０４Ｗ　12/08
Ｈ０４Ｌ　 9/00　６７５Ｂ
Ｇ０９Ｃ　 1/00　６４０Ｅ
Ｈ０４Ｍ　11/00　３０２

【手続補正書】
【提出日】平成30年8月7日(2018.8.7)
【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】
ユーザ機器(UE)とサービングネットワークとの間のワイヤレス通信をセキュアにする方法であって、
前記UEによって、前記UEに対するサービングネットワークを認証するために、前記UEとホーム加入者サーバの間のセキュリティアクティブ化交換を開始するステップと、
前記サービングネットワークが認証された後に、前記UEによって前記サービングネットワークにおけるネットワーク機能に要求を送信するステップであって、前記要求は、ナンスとシグネチャ要求とを含む、ステップと、
前記UEによって、前記サービングネットワークにおける信頼できる環境に維持された鍵を使用して生成された前記ネットワーク機能からの前記要求に対する応答を受信するステップであって、前記応答は、前記ネットワーク機能のシグネチャを含み、前記信頼できる環境は攻撃者が前記鍵を取得することを防止する、ステップと、
前記UEによって、前記ネットワーク機能の前記シグネチャと前記UEに維持される信頼できるネットワークのリスト中に提供された証明書とに基づいて、前記サービングネットワークを再認証するステップとを含む方法。
【請求項２】
前記シグネチャは、前記ネットワーク機能に対応する公開鍵証明書を使用して作成され、前記公開鍵証明書は、前記サービングネットワークに関連するネットワーク事業者によって供給される前記サービングネットワークの秘密鍵を使用して署名される、請求項1に

記載の方法。
【請求項３】
前記サービングネットワークを再認証する前記ステップは、
信頼できる第三者機関を使用して前記ネットワーク機能に対応する前記公開鍵証明書を検証するステップを含む、請求項2に記載の方法。
【請求項４】
前記シグネチャは、前記UEと前記ネットワーク機能との間で共有される鍵を使用して作成される、請求項1に記載の方法。
【請求項５】
前記UEに維持される前記信頼できるネットワークのリストは、前記信頼できるネットワークに対応する公開鍵または公開鍵証明書を識別し、
前記サービングネットワークを再認証する前記ステップは、前記UEによって信頼できるネットワークの前記リストを使用して前記ネットワーク機能の前記公開鍵および前記ネットワーク機能によって生成される前記シグネチャを検証するステップを含む、請求項1に記載の方法。
【請求項６】
前記サービングネットワークに送信される前記要求は、無線リソース制御メッセージ(RRCメッセージ)を含む、請求項1に記載の方法。
【請求項７】
前記RRCメッセージは、RRC接続要求、RRC接続再確立要求、またはRRC再構成完了メッセージを含む、請求項6に記載の方法。
【請求項８】
前記RRCメッセージは、アイドルモードからの遷移時に送信される、請求項6に記載の方法。
【請求項９】
前記サービングネットワークに送信される前記要求は、トラッキングエリア更新(TAU)要求を含む、請求項1に記載の方法。
【請求項１０】
前記サービングネットワークに証明書完全性情報要求を送信するステップと、
前記サービングネットワークから受信される第1の証明書完全性情報を、ホーム加入者サーバから受信される第2の証明書完全性情報を使用して検証するステップとをさらに含み、
前記証明書完全性情報要求は、前記第2の証明書完全性情報に対応する証明書オブザーバトリの識別子を含み、
前記証明書オブザーバトリは、1つまたは複数のネットワークに関する証明書のセットの完全性を維持するように構成される、請求項1に記載の方法。
【請求項１１】
前記証明書オブザーバトリの前記識別子は、インターネットプロトコル(IP)アドレスまたはユニバーサルリソースロケータ(URL)を含む、請求項10に記載の方法。
【請求項１２】
第1の証明書完全性情報を検証するステップは、
前記証明書オブザーバトリの公開鍵を使用して前記証明書完全性情報要求に対する応答を認証するステップを含む、請求項10に記載の方法。
【請求項１３】
第1の証明書完全性情報を検証するステップは、
前記第1の証明書完全性情報を前記第2の証明書完全性情報と比較するステップと、
前記第1の証明書完全性情報と前記第2の証明書完全性情報との間に違いがあると判定されたときに証明書サーバ機能(CSF)に証明書ステータス要求を送信するステップと、
前記CSFからの応答に基づいてネットワーク機能証明書のステータスを検証するステップとを含み、

前記証明書ステータス要求は、前記ネットワーク機能を識別する第1の識別情報と、前記ネットワーク機能証明書を識別する第2の識別情報と、前記ネットワーク機能証明書のバージョン番号とを含み、

CSFからの応答は、前記ネットワーク機能証明書のステータスと、前記ネットワークの公開鍵と、前記ネットワークの秘密鍵を使用して前記CSFによって作成される証明書ステータス応答のシグネチャとを含む証明書ステータス応答を含み、前記証明書ステータス応答の検証は、前記ネットワークの前記公開鍵を使用して実行される、請求項10に記載の方法。

【請求項１４】

ワイヤレストランシーバと、

前記トランシーバに結合されたプロセッサとを備える装置であって、前記プロセッサは、

前記装置に対するサービングネットワークを認証するために、前記装置とホーム加入者サーバの間のセキュリティアクティブ化交換を開始することと、

前記サービングネットワークが認証された後に、前記サービングネットワークにおけるネットワーク機能に要求を送信することであって、前記要求は、ナンスとシグネチャ要求とを含む、送信することと、

前記サービングネットワークにおける信頼できる環境に維持された鍵を使用して生成された前記ネットワーク機能からの前記要求に対する応答を受信することであって、前記応答は、前記ネットワーク機能のシグネチャを含み、前記信頼できる環境は攻撃者が前記鍵を取得することを防止する、受信することと、

前記ネットワークの前記シグネチャが、前記ネットワーク機能の前記シグネチャと前記装置に維持される信頼できるネットワークのリスト中に提供された証明書とに基づくとき、前記サービングネットワークを再認証することとを行うように構成される装置。

【請求項１５】

前記要求は、無線リソース制御接続要求またはトラッキングエリア要求を含み、前記プロセッサは、

前記装置がアイドルモードから遷移している間、前記無線リソース制御接続要求またはトラッキングエリア要求を前記サービングネットワークにおける前記ネットワーク機能に送信するように構成される、請求項14に記載の装置。

【請求項１６】

前記シグネチャは、UEと前記ネットワーク機能との間で共有される鍵を使用するか、または前記サービングネットワークに関連するネットワーク事業者によって供給されるサービングネットワークの秘密鍵を使用して署名された公開鍵証明書を使用して作成される、請求項14に記載の装置。

【請求項１７】

前記プロセッサは、

前記サービングネットワークに証明書完全性情報要求を送信することと、

前記サービングネットワークから受信される第1の証明書完全性情報とホーム加入者サーバから受信される第2の証明書完全性情報との間に違いがないと判定されたときに、前記第1の証明書完全性情報を前記第2の証明書完全性情報に基づいて検証することと、

前記第1の証明書完全性情報と前記第2の証明書完全性情報との間に違いがあると判定されたときに証明書サーバ機能(CSF)に証明書ステータス要求を送信することと、

前記CSFからの応答に基づいてネットワーク機能証明書のステータスを検証することとを行うように構成され、

前記証明書完全性情報要求は、前記第2の証明書完全性情報に対応する証明書オブザーバトリの識別子を含み、

前記証明書オブザーバトリは、1つまたは複数のネットワークに関する証明書のセットの完全性を維持するように構成され、

前記証明書ステータス要求は、前記ネットワーク機能の識別子と、前記ネットワーク機

能証明書の識別子と、前記ネットワーク機能証明書のバージョン番号とを含む、請求項14に記載の装置。

【請求項１８】

サービングネットワークのメンバーシップを証明する方法であって、

ユーザ機器(UE)がホームネットワークとのセキュアな接続を介して前記サービングネットワークを認証した後に前記UEから第1のメッセージを受信するステップであって、前記第1のメッセージが、前記サービングネットワークのネットワーク機能を対象とし、ナンスとシグネチャ要求とを含む、ステップと、

前記サービングネットワークにおける信頼できる環境に維持される事業者署名付き証明書を使用してシグネチャを生成するステップであって、前記信頼できる環境は攻撃者が鍵を取得することを防止する、ステップと、

前記UEに第2のメッセージを送信するステップであって、前記シグネチャが前記第2のメッセージに添付され、前記UEが、前記シグネチャを使用して、前記UEに維持される信頼できるネットワークのリストに基づいて前記サービングネットワークを再認証するように構成される、ステップとを含む方法。

【請求項１９】

前記事業者署名付き証明書は、前記サービングネットワークの事業者によって署名された公開鍵証明書である、請求項18に記載の方法。

【請求項２０】

前記事業者署名付き証明書に対応する秘密鍵が、セキュアなストレージまたはセキュアな実行環境に維持される、請求項18に記載の方法。

【請求項２１】

前記事業者署名付き証明書に対応する秘密鍵が、信頼できる環境に維持される、請求項18に記載の方法。

【請求項２２】

前記シグネチャは、前記UEと前記ネットワーク機能との間で共有されるセッション鍵を使用して作成されるメッセージ認証コード(MAC)を含み、前記第2のメッセージの署名に対称暗号が使用される、請求項18に記載の方法。

【請求項２３】

前記ネットワーク機能はモビリティ管理エンティティ(MME)を含み、前記セッション鍵はアクセスセキュリティ管理エンティティ鍵(K_{ASME})を備え、前記方法は、

前記MMEの公開鍵を使用して暗号化されたメッセージにおいて前記K_{ASME}をホーム加入者サーバ(HSS)から受信するステップと、

信頼できる環境内に記憶された秘密鍵を使用して前記K_{ASME}を解読するステップと、

前記K_{ASME}を前記信頼できる環境内に記憶するステップとをさらに含む、請求項22に記載の方法。

【請求項２４】

前記ネットワーク機能はeNodeBを含み、前記セッション鍵はKeNBを含み、前記方法は、

前記eNodeBの公開鍵を使用して暗号化されたメッセージにおいて前記KeNBをMMEから受信するステップと、

信頼できる環境内に記憶された秘密鍵を使用して前記KeNBを解読するステップと、

前記KeNBを前記信頼できる環境内に記憶するステップとをさらに含む、請求項22に記載の方法。

【請求項２５】

前記シグネチャは、前記ネットワーク機能の秘密鍵を使用して作成されたデジタルシグネチャを含み、前記第2のメッセージの署名に対称暗号が使用され、前記ネットワーク機能の前記秘密鍵は、信頼できる環境内に記憶され、前記シグネチャは、前記信頼できる環境内に作成される、請求項18に記載の方法。

【請求項２６】

前記ネットワーク機能はeNodeBを含み、前記第1のメッセージは無線リソース制御メッ

セージ(RRCメッセージ)を含み、前記第2のメッセージは前記RRCメッセージに対する応答を含む、請求項18に記載の方法。

【請求項２７】

前記RRCメッセージは、RRC接続確立要求、RRC接続再確立要求、またはRRC再構成完了メッセージである、請求項26に記載の方法。

【請求項２８】

前記ネットワーク機能はMMEを含み、前記第1のメッセージはトラッキングエリア更新(TAU)要求を含む、請求項18に記載の方法。

【請求項２９】

ユーザ機器(UE)がホームネットワークとのセキュアな接続を介してサービングネットワークを認証した後に前記UEから第1のメッセージを受信するための手段であって、前記第1のメッセージが、サービングネットワークのネットワーク機能を対象とし、ナンスとシグネチャ要求とを含む手段と、

前記サービングネットワークにおいて信頼できる環境に維持される事業者署名付き証明書を使用してシグネチャを生成するための手段であって、前記信頼できる環境は攻撃者が鍵を取得することを防止する、手段と、

前記UEに第2のメッセージを送信するための手段であって、前記シグネチャが前記第2のメッセージに添付される手段とを備え、

前記第2のメッセージに添付される前記シグネチャは、装置が前記サービングネットワークのメンバーであることを前記UEに対して証明するために生成され、前記事業者署名付き証明書は、前記サービングネットワークの事業者によって署名された公開鍵証明書であり、前記UEが、前記シグネチャを使用して、前記UEに維持される信頼できるネットワークのリストに基づいて前記サービングネットワークを再認証するように構成される、装置。

【請求項３０】

前記第1のメッセージは無線リソース制御(RRC)メッセージを含み、前記第2のメッセージは、前記ネットワーク機能がeNodeBを含むときに前記RRCメッセージに対する応答を含み、

前記第1のメッセージは、前記ネットワーク機能がモビリティ管理エンティティ(MME)を含むときにトラッキングエリア更新(TAU)要求を含む、請求項29に記載の装置。