【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】令和3年10月14日(2021.10.14)

【公表番号】特表2020-536426(P2020-536426A)
【公表日】令和2年12月10日(2020.12.10)
【年通号数】公開・登録公報2020-050
【出願番号】特願2020-518458(P2020-518458)
【国際特許分類】
Ｈ０４Ｗ　12/04　(2021.01)
Ｈ０４Ｗ　76/10　(2018.01)
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｗ　12/04
Ｈ０４Ｗ　76/10
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】令和3年9月6日(2021.9.6)
【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)によるワイヤレス通信のための方法であって、
ネットワークとのセキュアな接続を確立するために第1のメッセージを受信するステップであって、前記第1のメッセージはネットワークポリシー情報を含む、ステップと、
前記ネットワークポリシー情報に部分的に基づいて第1の鍵を生成するステップと、
前記第1の鍵を使用して前記ネットワークポリシー情報を検証するステップとを含む、方法。
【請求項２】
前記第1のメッセージが、前記ネットワークポリシー情報が有効である時間量をさらに含む、請求項1に記載の方法。
【請求項３】
前記第1の鍵が、前記ネットワーク内の前記UEとセキュリティアンカー機能(SEAF)との間で共有されるアンカー鍵、または前記ネットワークポリシー情報が有効である前記時間量のうちの少なくとも1つにさらに基づいて生成される、請求項2に記載の方法。
【請求項４】
前記第1のメッセージを受信する前に、前記SEAFとの認証手順または登録手順のうちの少なくとも1つを実行するステップをさらに含み、前記アンカー鍵が、前記認証手順または前記登録手順のうちの少なくとも1つに基づいて確立される、請求項3に記載の方法。
【請求項５】
前記ネットワークポリシー情報が、前記ネットワークとの通信セッションを確立するときに、前記UEがセッション管理トークンを前記ネットワーク内のセッション管理機能(SMF)から受信することになるかどうかの指示を含む、請求項1に記載の方法。
【請求項６】
前記第1のメッセージが、前記ネットワーク内のアクセスおよびモビリティ管理機能(AM

F)から受信される、請求項1に記載の方法。
【請求項７】
ネットワークとのセキュアな接続を確立するために第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のメッセージはネットワークポリシー情報を含む、手段と、
前記ネットワークポリシー情報に部分的に基づいて第1の鍵を生成するための手段と、
前記第1の鍵を使用して前記ネットワークポリシー情報を検証するための手段と
を備える、ユーザ機器(UE)。
【請求項８】
セキュリティアンカー機能(SEAF)によるワイヤレス通信のための方法であって、
ネットワークポリシー情報に少なくとも部分的に基づいてネットワークノードに対する鍵を生成するステップであって、前記鍵は、ユーザ機器(UE)と前記ネットワークノードとの間のセキュアな接続を確立するために使用される、ステップと、
前記鍵を前記ネットワークノードに送るステップとを含む、方法。
【請求項９】
前記鍵を生成する前に、前記UEとの認証手順または登録手順のうちの少なくとも1つに関与するステップをさらに含み、前記関与するステップが、前記UEと前記SEAFとの間で共有されるべきアンカー鍵を確立するステップを含む、請求項8に記載の方法。
【請求項１０】
前記鍵が、前記アンカー鍵または前記ネットワークポリシー情報が有効である時間量のうちの少なくとも1つにさらに基づいて生成される、請求項9に記載の方法。
【請求項１１】
前記ネットワークポリシー情報または前記ネットワークポリシー情報が有効である前記時間量のうちの少なくとも1つを前記ネットワークノードに送るステップをさらに含む、請求項10に記載の方法。
【請求項１２】
前記ネットワークポリシー情報が、ネットワーク内のセッション管理機能(SMF)が前記UEと前記ネットワークとの間の通信セッションに対するセッション管理トークンを生成して、前記セッション管理トークンを前記UEに送信することになっているかどうかの指示を含む、請求項8に記載の方法。
【請求項１３】
前記UEのポリシー情報を含むメッセージを受信するステップをさらに含み、UEポリシー情報は、UE能力情報またはUEセキュリティ情報のうちの少なくとも1つを含む、請求項8に記載の方法。
【請求項１４】
ネットワークポリシー情報に少なくとも部分的に基づいてネットワークノードに対する鍵を生成するための手段であって、前記鍵は、ユーザ機器(UE)と前記ネットワークノードとの間のセキュアな接続を確立するために使用される、手段と、
前記鍵を前記ネットワークノードに送るための手段と
を備える、セキュリティアンカー機能(SEAF)。
【請求項１５】
コンピュータによる実行時に、請求項1～6あるいは8～13のいずれか一項に記載の方法を前記コンピュータに実行させる命令を備えたコンピュータプログラム。