

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7414816号
(P7414816)

(45)発行日 令和6年1月16日(2024.1.16)

(24)登録日 令和6年1月5日(2024.1.5)

(51)国際特許分類		F I	
H O 4 W	8/02 (2009.01)	H O 4 W	8/02
H O 4 W	12/069 (2021.01)	H O 4 W	12/069
H O 4 W	12/40 (2021.01)	H O 4 W	12/40
H O 4 W	12/03 (2021.01)	H O 4 W	12/03
請求項の数 16 (全38頁)			
(21)出願番号	特願2021-518763(P2021-518763)	(73)特許権者	515076873
(86)(22)出願日	令和1年10月4日(2019.10.4)		ノキア テクノロジーズ オサケユイチア
(65)公表番号	特表2022-511606(P2022-511606		フィンランド国, 0 2 6 1 0 エスプー
	A)		, カラカーリ 7
(43)公表日	令和4年2月1日(2022.2.1)	(74)代理人	100094569
(86)国際出願番号	PCT/US2019/054883		弁理士 田中 伸一郎
(87)国際公開番号	WO2020/073014	(74)代理人	100103610
(87)国際公開日	令和2年4月9日(2020.4.9)		弁理士 ▲吉▼田 和彦
審査請求日	令和3年5月26日(2021.5.26)	(74)代理人	100109070
(31)優先権主張番号	62/742,341		弁理士 須田 洋之
(32)優先日	平成30年10月6日(2018.10.6)	(74)代理人	100067013
(33)優先権主張国・地域又は機関	米国(US)		弁理士 大塚 文昭
		(74)代理人	100086771
			弁理士 西島 孝喜
		(74)代理人	100109335
		最終頁に続く	

(54)【発明の名称】 ユーザ機器に供給された構成パラメータのセキュアな更新のためのシステム及び方法

(57)【特許請求の範囲】

【請求項1】

ユーザ機器（UE）であって、
前記UE用のUE構成パラメータを記憶する汎用加入者識別モジュール（USIM）と、
少なくとも1つのプロセッサと、
命令を記憶した少なくとも1つのメモリと、
を備える、UEであり、前記命令は、前記少なくとも1つのプロセッサによって実行され
たときに、前記UEに少なくとも、
非アクセス層（NAS）トランスポート手順の間、アクセス及びモビリティ管理機能（
AMF）要素から、前記UE用のUE構成パラメータ更新を含むコンテナを有するダウン
リンクNASトランスポートメッセージを受信することであって、前記UE構成パラメ
ータ更新は、前記ダウンリンクNASトランスポートメッセージの前記コンテナ内のセキュ
ア化パケット内にカプセル化され、前記ダウンリンクNASトランスポートメッセージの
前記セキュア化パケット内にカプセル化された前記UE構成パラメータ更新はルーティン
グインジケータパラメータを含むことと、
前記ダウンリンクNASトランスポートメッセージの前記コンテナ内の前記セキュア化パ
ケットを検証するために第1のセキュリティチェックを前記UEのモバイル機器（ME）
ドメインによって実行することと、
前記第1のセキュリティチェックが成功したとき、前記セキュア化パケットを前記US
IMに転送することと、

前記UEのNASセキュリティコンテキストを使用して前記ダウンリンクNASトランスポートメッセージの前記コンテナ内の前記セキュア化パケット内にカプセル化された前記UE構成パラメータ更新の完全性を検証するために第2のセキュリティチェックを実行することと、

前記第2のセキュリティチェックが成功したとき、前記ダウンリンクNASトランスポートメッセージの前記コンテナ内の前記セキュア化パケット内にカプセル化された前記UE構成パラメータ更新に基づいて、前記USIMを使用して、前記USIM内の前記UE構成パラメータのうちの1つ以上を更新することと、
を行わせる、UE。

【請求項2】

前記USIMは、前記UE内の汎用集積回路カード（UICC）上に存在する、請求項1に記載のUE。

【請求項3】

前記命令は、前記少なくとも1つのプロセッサによって実行されたときに、前記UEに、前記ダウンリンクNASトランスポートメッセージがUE確認応答インジケータを含む場合に、前記UEによって前記UE構成パラメータ更新が受信されたことを示す前記UEからのUE確認応答を含むコンテナを有するアップリンクNASトランスポートメッセージを前記AMF要素に送信すること、をさらに行わせる、請求項1に記載のUE。

【請求項4】

前記命令は、前記少なくとも1つのプロセッサによって実行されたときに、前記UEに、前記ダウンリンクNASトランスポートメッセージが再登録インジケータを含む場合に、前記UEの前記USIM上で更新された前記更新されたUE構成パラメータを使用して前記UEを再登録するためにNAS登録手順を開始させること、をさらに行わせる、請求項1に記載のUE。

【請求項5】

方法であって、

非アクセス層（NAS）トランスポート手順の間、ユーザ機器（UE）において、アクセス及びモビリティ管理機能（AMF）要素から、前記UE用のUE構成パラメータ更新を含むコンテナを有するダウンリンクNASトランスポートメッセージを受信することであって、前記UE構成パラメータ更新は、前記ダウンリンクNASトランスポートメッセージの前記コンテナ内のセキュア化パケット内にカプセル化され、前記ダウンリンクNASトランスポートメッセージの前記コンテナ内の前記セキュア化パケット内にカプセル化された前記UE構成パラメータ更新はルーティングインジケータパラメータを含むことと、前記ダウンリンクNASトランスポートメッセージの前記コンテナ内の前記セキュア化パケットを検証するために第1のセキュリティチェックを前記UEのモバイル機器（ME）ドメインによって実行することと、

前記第1のセキュリティチェックが成功したとき、前記セキュア化パケットを、前記UEと動作可能に通信する汎用加入者識別モジュール（USIM）に転送することと、

前記UEのNASセキュリティコンテキストを使用して前記ダウンリンクNASトランスポートメッセージの前記コンテナ内の前記セキュア化パケット内にカプセル化された前記UE構成パラメータ更新の完全性を検証するために第2のセキュリティチェックを実行することと、

前記第2のセキュリティチェックが成功したとき、前記ダウンリンクNASトランスポートメッセージの前記コンテナ内の前記セキュア化パケット内にカプセル化された前記UE構成パラメータ更新に基づいて、前記USIMを使用して、前記USIM内の前記UE構成パラメータのうちの1つ以上を更新することと、
を備える、方法。

【請求項6】

前記USIMは、前記UE内の汎用集積回路カード（UICC）上に存在する、請求項5に記載の方法。

10

20

30

40

50

【請求項 7】

前記ダウンリンク N A S トランスポートメッセージが U E 確認応答インジケータを含む場合に、前記 U E によって前記 U E 構成パラメータ更新が受信されたことを示す前記 U E からの U E 確認応答を含むコンテナを有するアップリンク N A S トランスポートメッセージを前記 U E から前記 A M F 要素に送信すること
をさらに備える、請求項 5 に記載の方法。

【請求項 8】

前記ダウンリンク N A S トランスポートメッセージが再登録インジケータを含む場合に、前記 U E を使用して、前記更新された U E 構成パラメータを使用して前記 U E を再登録するために N A S 登録手順を開始させること、をさらに備える、請求項 5 に記載の方法。

【請求項 9】

アクセス及びモビリティ管理機能（A M F）要素であって、
少なくとも 1 つのプロセッサと、
命令を記憶した少なくとも 1 つのメモリと、を備える、A M F 要素であって、前記命令は、
前記少なくとも 1 つのプロセッサによって実行されたときに、前記 A M F 要素に少なくとも、

第 1 の非アクセス層（N A S）トランスポート手順の間、U E 用の U E 構成パラメータ更新を含むコンテナを有するダウンリンク N A S トランスポートメッセージを生成することであって、前記 U E 構成パラメータ更新は、前記ダウンリンク N A S トランスポートメッセージの前記コンテナ内のセキュア化パケット内にカプセル化され、前記ダウンリンク N A S トランスポートメッセージの前記コンテナ内の前記セキュア化パケット内にカプセル化された前記 U E 構成パラメータ更新はルーティングインジケータパラメータを含む、生成することと、

前記ダウンリンク N A S トランスポートメッセージをユーザ機器（U E）に送信することと、実行させ、

前記ダウンリンク N A S トランスポートメッセージは、（i）前記 U E のモバイル機器（M E）ドメインに、前記ダウンリンク N A S トランスポートメッセージの前記コンテナ内の前記セキュア化パケットを検証するために、第 1 のセキュリティチェックを実行させる、（i i）前記第 1 のセキュリティチェックが成功したとき、前記 U E の前記 M E ドメインに、前記セキュア化パケットを、前記 U E と動作可能に通信する汎用加入者識別モジュール（U S I M）に転送させる、（i i i）前記 U E の N A S セキュリティコンテキストを使用して前記ダウンリンク N A S トランスポートメッセージの前記コンテナ内の前記セキュア化パケット内にカプセル化された前記 U E 構成パラメータ更新の完全性を検証するために前記 U S I M に第 2 のセキュリティチェックを実行させる、（i v）前記第 2 のセキュリティチェックが成功したとき、前記ダウンリンク N A S トランスポートメッセージの前記コンテナ内の前記セキュア化パケット内にカプセル化された前記 U E 構成パラメータ更新に基づいて、前記 U S I M 内の前記 U E 構成パラメータのうちの 1 つ以上を前記 U S I M が更新するように動作可能である、A M F 要素。

【請求項 10】

前記ダウンリンク N A S トランスポートメッセージが U E 確認応答インジケータを含む場合に、前記ダウンリンク N A S トランスポートメッセージは、前記 U E に、前記 U E によって前記 U E 構成パラメータ更新が受信されたことを示す前記 U E からの U E 確認応答を含むコンテナを有するアップリンク N A S トランスポートメッセージを前記 A M F 要素に送信させるようにさらに動作可能である、請求項 9 に記載の A M F 要素。

【請求項 11】

前記ダウンリンク N A S トランスポートメッセージが再登録インジケータを含む場合に、前記ダウンリンク N A S トランスポートメッセージは、前記 U E に、前記更新された U E 構成パラメータを使用して前記 U E を再登録するために N A S 登録手順を開始させるようにさらに動作可能である、請求項 9 に記載の A M F 要素。

【請求項 12】

前記少なくとも1つのメモリに記憶された前記命令は、前記少なくとも1つのプロセッサによって実行されたときに、前記AMF要素に、

統合データ管理(UDM)要素から、前記UE用のUE構成パラメータ更新を含む制御プレーンメッセージを受信することと、

前記UE構成パラメータ更新を前記ダウンリンクNASトランスポートメッセージのコンテンツ内に挿入することと、

をさらに行わせるように構成される、請求項9に記載のAMF要素。

【請求項13】

方法であって、

第1の非アクセス層(NAS)トランスポート手順の間、UE用のUE構成パラメータ更新を含むコンテンツを有するダウンリンクNASトランスポートメッセージを生成することであって、前記UE構成パラメータ更新は、前記ダウンリンクNASトランスポートメッセージの前記コンテンツ内のセキュア化パケット内にカプセル化され、前記ダウンリンクNASトランスポートメッセージの前記セキュア化パケット内にカプセル化された前記UE構成パラメータ更新はルーティングインジケータパラメータを含むことと、

前記ダウンリンクNASトランスポートメッセージをユーザ機器(UE)に送信することと、を備え、

前記ダウンリンクNASトランスポートメッセージは、(i)前記UEのモバイル機器(ME)ドメインに、前記ダウンリンクNASトランスポートメッセージの前記コンテンツ内の前記セキュア化パケットを検証するために第1のセキュリティチェックを実行させる、(ii)前記第1のセキュリティチェックが成功したとき、前記UEの前記MEドメインに、前記セキュア化パケットを、前記UEと動作可能に通信する汎用加入者識別モジュール(USIM)に転送させる、(iii)前記UEのNASセキュリティコンテキストを使用して前記ダウンリンクNASトランスポートメッセージの前記コンテンツ内の前記セキュア化パケット内にカプセル化された前記UE構成パラメータ更新の完全性を検証するために前記USIMに第2のセキュリティチェックを実行させる、(iv)前記第2のセキュリティチェックが成功したとき、前記ダウンリンクNASトランスポートメッセージの前記コンテンツ内の前記セキュア化パケット内にカプセル化された前記UE構成パラメータ更新に基づいて、前記USIM内の前記UE構成パラメータのうちの1つ以上を前記USIMが更新するように動作可能である、

方法。

【請求項14】

前記ダウンリンクNASトランスポートメッセージがUE確認応答インジケータを含む場合に、

前記UEに、前記UEによって前記UE構成パラメータ更新が受信されたことを示す前記UEからのUE確認応答を含むコンテンツを有するアップリンクNASトランスポートメッセージを前記AMF要素に送信させること

をさらに備える、請求項13に記載の方法。

【請求項15】

前記ダウンリンクNASトランスポートメッセージが再登録インジケータを含む場合に、前記方法は、

前記UEに、前記更新されたUE構成パラメータを使用して前記UEを再登録するためにNAS登録手順を開始させること

をさらに備える、請求項13に記載の方法。

【請求項16】

統合データ管理(UDM)要素から、前記UE用のUE構成パラメータ更新を含む制御プレーンメッセージを受信することと、

前記UE構成パラメータ更新を前記ダウンリンクNASトランスポートメッセージのコンテンツ内に挿入することと、

をさらに備える、請求項13に記載の方法。

10

20

30

40

50

【発明の詳細な説明】

【技術分野】

【0001】

関連出願の相互参照

本非仮特許出願は、2018年10月6日に出願された米国仮特許出願62/742,341号の優先権を主張し、引用により本明細書に完全に提供されているかのように組み込まれている。

【0002】

本開示は通信システムの分野に関し、詳細にはモバイルデバイスの更新に関する。

【背景技術】

【0003】

サービスプロバイダまたはキャリアは、一般にユーザ機器（UE）と呼ばれる、携帯電話またはその他のモバイルデバイス／端末のエンドユーザに多数の音声及びデータサービスを提供するモバイルネットワークを実装している。音声サービスのいくつかの例は、音声通話、通話転送、通話中着信などである。データサービスのいくつかの例は、インターネットアクセス、ストリーミングオーディオ、ストリーミングビデオ、オンラインゲーム、インターネットプロトコルテレビ（IPTV）などである。モバイルネットワークは、エンドユーザへの最後のリンクがワイヤレスであるタイプのネットワークである。モバイルネットワークは、一般に、コアネットワークと、無線インターフェースを介してUEとシグナリング及びデータを交換する1つまたは複数の無線アクセスネットワーク（RAN）とを含む。

【0004】

UEは、典型的には、サブスクライバの国際移動体加入者識別番号（IMSI）、セキュリティ認証、暗号化情報、及びその他の構成パラメータが供給される。UEのホームネットワークがUEの構成パラメータのうちの1つまたは複数を更新する必要がある場合があり得る。たとえば、UEのホームネットワークは、サブスクリプションの変更が発生したとき、新しいサービスの割り当てがあったとき、モバイルネットワークがロングタームエボリューション（LTE）から次世代ネットワークに移行したときなどに、構成パラメータを更新し得る。したがって、UEにおける構成パラメータを更新するための強化された手順を特定することは有益である。

【発明の概要】

【0005】

本明細書に記載の実施形態は、非アクセス層（NAS）メッセージを使用したUE構成パラメータの更新を提供する。概説として、次世代ネットワークに移行するモバイルネットワークは、統合データ管理（UDM）と、アクセス及びモビリティ管理機能（AMF）とを含み得る。UEのホームネットワーク内にあるUDMは、セキュリティ保護（たとえば、セキュア化パケット（secured packet）、完全性保護など）がなされたUE用のUE構成パラメータ更新をアセンブルするように構成される。UDMは、セキュリティ保護がなされたUE構成パラメータ更新をAMFに送信する。次いで、AMFは、NASメッセージを使用してUE構成パラメータ更新をUEに透過的に送信するように構成される。この場合も、UE構成パラメータ更新はNASメッセージ内でセキュリティ保護される。UEは、NASメッセージを受信すると、NASメッセージで提供された更新に基づいて自身のUE構成パラメータを更新するように構成される。この手順の技術的な利点の1つは、UE構成パラメータ更新に対してエンドツーエンドのセキュリティが提供されることである。他の技術的な利点は、UE構成パラメータを更新するために、ネイティブの制御プレーンの機能が使用され得ることである。したがって、UEに更新を提供するために、専用のネットワーク要素が配備される必要はない。

【0006】

一実施形態は、モバイルネットワークのAMF要素を備える。AMF要素は、プロセッサ（複数可）と、プロセッサによって実行可能なコンピュータプログラムコードを含むメ

10

20

30

40

50

モリと、を含む。プロセッサは、AMF要素に、UDM要素から、UE用のUE構成パラメータ更新を含む制御プレーンメッセージを受信させるように構成される。UE構成パラメータ更新は、保護メカニズムに従ってセキュリティ保護される。プロセッサは、AMF要素に、セキュリティ保護されたUE構成パラメータ更新を第1のNASメッセージのコンテナに挿入させるようにさらに構成され、コンテナはUE構成パラメータ更新用に設計(designate)される。プロセッサは、AMF要素に、セキュリティ保護されたUE構成パラメータ更新を含むコンテナを有する第1のNASメッセージをUEに送信させるようにさらに構成される。

【0007】

他の実施形態では、UE構成パラメータ更新は、保護メカニズムに従ってセキュア化パケット内にカプセル化される。

【0008】

他の実施形態では、UE構成パラメータ更新は、保護メカニズムに従ってUEのNASセキュリティコンテキストを使用して完全性保護される。

【0009】

他の実施形態では、UE構成パラメータ更新は、セキュア化パケット内にカプセル化され、セキュア化パケットは、保護メカニズムに従ってUEのNASセキュリティコンテキストを使用して完全性保護される。

【0010】

他の実施形態では、第1のNASメッセージは、NAS登録手順中にUEに送信されるNAS登録受諾メッセージを備える。プロセッサは、AMF要素に、NAS登録手順中にUEから、UE構成パラメータ更新が受信されたというUE確認応答を含むコンテナを有する第2のNASメッセージを受信させ、UE確認応答を有する他の制御プレーンメッセージをUDM要素に送信させるようにさらに構成される。UEから受信された第2のNASメッセージは、NAS登録完了メッセージまたはアップリンクNASトランスポートメッセージを備え得る。

【0011】

他の実施形態では、第1のNASメッセージは、NAS登録手順の後に実行されるNASトランスポート手順のダウンリンクNASトランスポートメッセージを備える。プロセッサは、AMF要素に、UE構成パラメータ更新が受信されたというUEからのUE確認応答を含むコンテナを有する第2のNASメッセージをUEから受信させ、UE確認応答を有する他の制御プレーンメッセージをUDM要素に送信させるようにさらに構成される。第2のNASメッセージは、アップリンクNASトランスポートメッセージを備える。

【0012】

他の実施形態は、UEに供給されたUE構成パラメータを更新するための更新手順を実行する方法を備える。この方法は、AMF要素においてUDM要素から、UE用のUE構成パラメータ更新を含む制御プレーンメッセージを受信することを備える。UE構成パラメータ更新は、保護メカニズムに従ってセキュリティ保護される。この方法は、AMF要素において、セキュリティ保護されたUE構成パラメータ更新を第1のNASメッセージのコンテナに挿入することであって、コンテナはUE構成パラメータ更新用に設計される、挿入することをさらに備える。この方法は、セキュリティ保護されたUE構成パラメータ更新を含むコンテナを有する第1のNASメッセージをAMF要素からUEに送信することをさらに備える。

【0013】

他の実施形態では、UE構成パラメータ更新は、保護メカニズムに従ってセキュア化パケット内にカプセル化される。

【0014】

他の実施形態では、UE構成パラメータ更新は、保護メカニズムに従ってUEのNASセキュリティコンテキストを使用して完全性保護される。

【0015】

10

20

30

40

50

他の実施形態では、UE構成パラメータ更新は、セキュア化パケット内にカプセル化され、セキュア化パケットは、保護メカニズムに従ってUEのNASセキュリティコンテキストを使用して完全性保護される。

【0016】

他の実施形態では、第1のNASメッセージは、NAS登録手順中にAMF要素からUEに送信されるNAS登録受諾メッセージを備える。

【0017】

他の実施形態では、この方法は、NAS登録手順中にAMF要素においてUEから、UE構成パラメータ更新が受信されたというUE確認応答を含むコンテナを有する第2のNASメッセージを受信することと、UE確認応答を有する他の制御プレーンメッセージをAMF要素からUDM要素に送信することと、をさらに備える。第2のNASメッセージは、NAS登録完了メッセージまたはアップリンクNASトランスポートメッセージを備え得る。

【0018】

他の実施形態では、第1のNASメッセージは、NAS登録手順の後に実行されるNASトランスポート手順のダウンリンクNASトランスポートメッセージを備える。

【0019】

他の実施形態では、この方法は、UE構成パラメータ更新が受信されたというUEからのUE確認応答を含むコンテナを有する第2のNASメッセージを、AMF要素においてUEから受信することと、UE確認応答を有する他の制御プレーンメッセージをAMF要素からUDM要素に送信することと、をさらに備える。第2のNASメッセージは、アップリンクNASトランスポートメッセージを備える。

【0020】

他の実施形態では、この方法は、UEにおいてAMF要素から、セキュリティ保護されたUE用のUE構成パラメータ更新を含むコンテナを有する第1のNASメッセージを受信することと、UEにおいてUE構成パラメータ更新を検証するためにセキュリティチェックを実行することと、UE構成パラメータ更新が検証されたときに、UE構成パラメータ更新に基づいてUE構成パラメータのうちの1つまたは複数を更新することと、をさらに備える。

【0021】

他の実施形態では、第1のNASメッセージが再登録インジケータを含むとき、この方法は、UEにおいて更新されたUE構成パラメータを使用して再登録するためにNAS登録手順を開始することをさらに備える。

【0022】

他の実施形態は、汎用加入者識別モジュール（USIM）をホストする汎用集積回路カード（UICC）と、プロセッサと、プロセッサによって実行可能なコンピュータプログラムコードを含むメモリと、を含むUEを備える。UICC及びメモリの少なくとも1つは、UE用のUE構成パラメータを記憶する。プロセッサは、UEに、AMF要素から、保護メカニズムに従ってセキュリティ保護されたUE用のUE構成パラメータ更新を含むコンテナを有する第1のNASメッセージを受信させるように構成される。UICC及び／またはプロセッサは、UEに、UE構成パラメータ更新を検証するためにセキュリティチェックを実行することと、UE構成パラメータ更新が検証されたときに、UE構成パラメータ更新に基づいてUE構成パラメータのうちの1つまたは複数を更新することと、を行わせるように構成される。

【0023】

他の実施形態では、UE構成パラメータ更新は、第1のNASメッセージのコンテナ内のセキュア化パケット内にカプセル化される。

【0024】

他の実施形態では、UE構成パラメータ更新は、UEのNASセキュリティコンテキストを使用して完全性保護される。

【0025】

他の実施形態では、UE構成パラメータ更新は、第1のNASメッセージのコンテナ内のセキュア化パケット内にカプセル化され、セキュア化パケットは、UEのNASセキュリティコンテキストを使用して完全性保護される。

【0026】

他の実施形態では、第1のNASメッセージは、NAS登録手順中にUEに送信されるNAS登録受諾メッセージを備える。

【0027】

他の実施形態では、NAS登録受諾メッセージがUE確認応答インジケータを含むとき、プロセッサは、UEに、UE構成パラメータ更新が受信されたというUEからのUE確認応答を含むコンテナを有する第2のNASメッセージをAMF要素に送信させるようにさらに構成される。第2のNASメッセージは、NAS登録完了メッセージまたはアップリンクNASトランスポートメッセージを備え得る。

10

【0028】

他の実施形態では、第1のNASメッセージは、NAS登録手順の後に実行されるNASトランスポート手順のダウンリンクNASトランスポートメッセージを備える。

【0029】

他の実施形態では、ダウンリンクNASトランスポートメッセージがUE確認応答インジケータを含むとき、プロセッサは、UEに、UE構成パラメータ更新が受信されたというUEからのUE確認応答を含むコンテナを有するアップリンクNASトランスポートメッセージをAMF要素に送信させるようにさらに構成される。

20

【0030】

他の実施形態では、第1のNASメッセージが再登録インジケータを含むとき、プロセッサは、UEに、更新されたUE構成パラメータを使用して再登録させるためにNAS登録手順を開始させるようにさらに構成される。

【0031】

他の実施形態は、UDM要素から、UE用のUE構成パラメータ更新を含む制御プレーンメッセージを受信するための手段を含むAMF要素を含む。UE構成パラメータ更新は、保護メカニズムに従ってセキュリティ保護される。AMF要素は、セキュリティ保護されたUE構成パラメータ更新を第1のNASメッセージのコンテナに挿入するための手段と、セキュリティ保護されたUE構成パラメータ更新を含むコンテナを有する第1のNASメッセージをUEに送信するための手段と、をさらに含む。

30

【0032】

他の実施形態は、UE用のUE構成パラメータを記憶するための手段を含むUEを備える。UEは、AMF要素から、保護メカニズムに従ってセキュリティ保護されたUE用のUE構成パラメータ更新を含むコンテナを有する第1のNASメッセージを受信するための手段と、UE構成パラメータ更新を検証するためにセキュリティチェックを実行するための手段と、UE構成パラメータ更新が検証されたときに、UE構成パラメータ更新に基づいてUE構成パラメータのうちの1つまたは複数を更新するための手段と、をさらに含む。

40

【0033】

上記の概要は、本明細書のいくつかの態様の基本的な理解を提供する。本概要は、本明細書の広範な概説ではない。本明細書の主要または重要な要素を特定することも、本明細書の特定の実施形態の範囲または特許請求の範囲を線引きすることも意図していない。その唯一の目的は、後述するさらに詳細な説明の前置きとして、本明細書のいくつかの概念を簡略化した形で提示することである。

【0034】

以下、本発明のいくつかの実施形態を、単なる例として添付の図面を参照しながら説明する。全ての図面において、同じ参照番号は同じ要素または同じタイプの要素を表す。

【図面の簡単な説明】

50

【0035】

【図1】例示的な実施形態におけるモバイルネットワークを示す。

【図2】進化型パケットコア（EPC）ネットワークを示す。

【図3】次世代ネットワークの非ローミングアーキテクチャを示す。

【図4】次世代ネットワークのローミングアーキテクチャを示す。

【図5】無線プロトコルスタックを示す。

【図6】例示的な実施形態におけるUEのブロック図である。

【図7】例示的な実施形態におけるUEの機能モデルの図である。

【図8】例示的な実施形態におけるAMF要素のブロック図である。

【図9】例示的な実施形態におけるUDM要素のブロック図である。

【図10】例示的な実施形態における、UDM要素において更新手順を実行する方法を示すフローチャートである。

【図11】例示的な実施形態における、AMF要素において更新手順を実行する方法を示すフローチャートである。

【図12】例示的な実施形態における、UEにおいて更新手順を実行する方法を示すフローチャートである。

【図13】例示的な実施形態における登録中の更新手順を示すメッセージ図である。

【図14】例示的な実施形態における登録後の更新手順を示すメッセージ図である。

【図15】例示的な実施形態における登録中の更新手順を示すメッセージ図である。

【図16】例示的な実施形態における登録後の更新手順を示すメッセージ図である。

【図17】例示的な実施形態における登録中の更新手順を示すメッセージ図である。

【図18】例示的な実施形態における登録後の更新手順を示すメッセージ図である。

【発明を実施するための形態】

【0036】

図及び以下の説明は、特定の例示的な実施形態を示している。したがって、当業者であれば、本明細書では明示的に説明も図示もしていないが、実施形態の原理を具現化し、実施形態の範囲内に含まれる様々な構成を考案できるであろうことは理解されよう。さらに、本明細書に記載の全ての実施例は、実施形態の原理を理解するのを助けることを意図したものであり、そのような具体的に記述した実施例及び条件に限定されないものとして解釈されるべきである。結果として、本発明の概念（複数可）は、以下に記載する特定の実施形態にも実施例にも限定されず、特許請求の範囲及びそれらの均等物によって限定される。

【0037】

図1は、例示的な実施形態におけるモバイルネットワーク100を示している。モバイルネットワーク100（セルラーネットワークとも呼ばれる）は、最後のリンクがワイヤレスであるタイプのネットワークであり、複数のデバイスに音声及び／またはデータサービスを提供する。モバイルネットワーク100は、第3世代（3G）、第4世代（4G）、及び／または次世代ネットワーク（たとえば、第5世代（5G））であり得る。

【0038】

モバイルネットワーク100は、UE110に（図示していない他のUEにも）通信サービスを提供するものとして図示している。UE110は、音声サービス、データサービス、マシンツーマシン（M2M）もしくはマシンタイプ通信（MTC）サービス、モノのインターネット（IoT）サービス、及び／またはその他のサービスが可能になり得る。UE110は、携帯電話（たとえば、スマートフォン）、タブレットまたはPDA、モバイルブロードバンドアダプタを有するコンピュータなどのエンドユーザデバイスであり得る。

【0039】

モバイルネットワーク100は、無線インターフェース122を介してUE110と通信する1つまたは複数の無線アクセスネットワーク（RAN）120を含む。RAN120は、進化型UMTS地上無線アクセスネットワーク（E-UTRAN）アクセス、ワイ

10

20

30

40

50

ヤレスローカルエリアネットワーク（WLAN）アクセス、固定アクセス、衛星無線アクセス、新しい無線アクセス技術（RAT）などをサポートし得る。一例として、RAN 120は、地理的エリアにわたって分散された1つまたは複数の基地局124を含むE-UTRANまたは次世代RAN（NG-RAN）を含み得る。基地局124は、無線通信技術を使用して、ライセンスされたスペクトルでUEと通信し、UEをコアネットワークとインターフェースするエンティティを含み得る。E-UTRAN内の基地局124は、進化型NodeB（eNodeB）と呼ばれる。NG-RAN内の基地局124は、gNodeB（NR基地局）、及び／またはng-eNodeB（5GコアネットワークをサポートするLTE基地局）と呼ばれる。他の例として、RAN 120は、1つまたは複数のワイヤレスアクセスポイント（WAP）125を含むWLANを含み得る。WLANは、UEがワイヤレス（無線）接続を介してローカルエリアネットワーク（LAN）に接続できるネットワークである。WAP 125は、無線通信技術を使用して、ライセンスされていないスペクトルを介してUEと通信し、UEにコアネットワークへのアクセスを提供するノードである。WAP 125の一例は、2.4 GHzまたは5 GHzの無線帯域で動作するWi-Fiアクセスポイントである。本明細書で使用する「基地局」という用語は、eNodeB、gNodeB、ng-eNodeB、WAPなどを指し得る。

【0040】

UE 110は、RAN 120のセル126に接続して、コアネットワーク130にアクセスすることができる。したがって、RAN 120は、UE 110とコアネットワーク130との間の無線インターフェースを表す。コアネットワーク130は、RAN 120によって接続された顧客に様々なサービスを提供するモバイルネットワーク100の中心部である。コアネットワーク130の一例は、3GPPによってLTE用に提案された進化型パケットコア（EPC）ネットワークである。コアネットワーク130の他の例は、3GPPによって提案された5Gコアネットワークである。コアネットワーク130は、UE 110にサービスを提供するサーバ、デバイス、装置、または機器（ハードウェアを含む）を含み得るネットワーク要素132を含む。EPCネットワークにおけるネットワーク要素132は、モビリティ管理エンティティ（MME）、サービングゲートウェイ（S-GW）、パケットデータネットワークゲートウェイ（P-GW）などを含み得る。5Gネットワークにおけるネットワーク要素132は、アクセス及びモビリティ管理機能（AMF）、セッション管理機能（SMF）、ポリシー制御機能（PCF）、アプリケーション機能（AF）、ユーザプレーン機能（UPF）などを含み得る。

【0041】

図2は、LTEのコアネットワークである進化型パケットコア（EPC）ネットワーク200を示している。EPCネットワーク200は、モビリティ管理エンティティ（MME）214、サービングゲートウェイ（S-GW）215、パケットデータネットワークゲートウェイ（P-GW）216、ホームサブスクリバサーバ（HSS）217、ならびにポリシー及び課金ルール機能（PCRF）218を含むが、図示していない他の要素、たとえば、IPマルチメディアサブシステム（IMS）アプリケーションサーバなどを含み得る。EPCネットワーク200内では、ユーザデータ（「ユーザプレーン」とも呼ばれる）及びシグナリング（「制御プレーン」とも呼ばれる）は分離されている。MME 214は、EPCネットワーク200内の制御プレーンを処理する。たとえば、MME 214は、E-UTRANアクセスのモビリティ及びセキュリティに関連するシグナリングを処理する。MME 214は、アイドルモードのUE 110の追跡及びページングを担当する。S-GW 215及びP-GW 216はユーザプレーンを処理する。S-GW 215及びP-GW 216は、UE 110と外部データネットワーク240（DNまたはパケットデータネットワーク（PDN））との間でデータトラフィックを転送する。S-GW 215は、無線側とEPCネットワーク200との間の相互接続点であり、着信及び発信IPパケットをルーティングすることによってUE 110にサービスを提供する。S-GW 215は、LTE内のモビリティのための（すなわち、eNodeB間のハンドオーバーの場合）、また、LTEと他の3GPPアクセスとの間のアンカーポイントでもある。P

ーGW216は、EPCネットワーク200と外部データネットワーク240との間の相互接続点（すなわち、データネットワーク240の入口または出口のポイント）であり、データネットワーク240との間でパケットをルーティングする。HSS217は、ユーザ関連及びサブスクリバ関連の情報を記憶するデータベースである。PCRF218は、EPCネットワーク200においてポリシー及び課金制御（PCC）ソリューションを提供し、エンドユーザによって要求されるサービスのためのPCC規則を策定するEPCネットワーク200のノードまたはエンティティである。

【0042】

MME214はS1-MMEインターフェースを介してRAN120（すなわち、eNodeB）に接続し、S-GW215はS1-Uインターフェースを介してRAN120に接続する。MME214は、S11インターフェースを介してS-GW215に接続し、S6aインターフェースを介してHSS217に接続する。PCRF218は、Gxインターフェースを介してP-GW216に接続し、これにより、PCRF218からP-GW216内のポリシー及び課金施行機能（PCEF）へのポリシー及び課金ルールの転送が提供される。PCRF218はGxxインターフェースを介してS-GW215に接続し、S-GW215はS5インターフェースを介してP-GW216に接続する。

【0043】

図3は、次世代ネットワークの非ローミングアーキテクチャ300を示している。図3のアーキテクチャは参照点表現であり、これは、引用により本明細書に完全に含まれているかのように組み込まれている3GPP TS 23.501（v15.3.0）にさらに記載されている。アーキテクチャ300は、コアネットワークのネットワーク機能（NF）から構成されており、制御プレーンのネットワーク機能は、ユーザプレーンから分離されている。コアネットワークの制御プレーンは、認証サーバ機能（AUSF）310、統合データ管理（UDM）312、ネットワークスライス選択機能（NSSF）313、アクセス及びモビリティ管理機能（AMF）314、セッション管理機能（SMF）316、ポリシー制御機能（PCF）318、ならびにアプリケーション機能（AF）320を含む。コアネットワークのユーザプレーンは、データネットワーク240と通信する1つまたは複数のユーザプレーン機能（UPF）324を含む。UE110は、（R）AN120を介してコアネットワークの制御プレーン及びユーザプレーンにアクセスすることができる。

【0044】

AUSF310は、UE110の認証をサポートするように構成される。UDM312は、UE110のサブスクリプションデータ／情報を記憶するように構成される。UDM312は、サブスクリプション、ポリシー、及びセッション関連のコンテキスト（たとえば、UEの位置）の3つのタイプのユーザデータを記憶し得る。AMF314は、UEベースの認証、認可、モビリティ管理などを提供するように構成される。SMF316は以下の機能、すなわち、セッション管理（SM）、UEインターネットプロトコル（IP）アドレスの割り当て及び管理、UPF（複数可）の選択及び制御、PCF318へのインターフェースの終端、ポリシー施行及びサービス品質（QoS）の制御部分、合法的傍受、NASメッセージのSM部分の終端、ダウンリンクデータ通知（DNN）、ローミング機能、サービスレベル合意（SLA）のQoSを適用するためのローカルな施行の処理、課金データ収集及び課金インターフェースなどを提供するように構成される。UE110が複数のセッションを有する場合、各セッションに異なるSMFを割り当てて個別に管理し、場合によってはセッションごとに異なる機能を提供し得る。PCF318は、ネットワークの挙動を管理するための統一されたポリシーフレームワークをサポートし、QoS施行、課金、アクセス制御、トラフィックルーティングなどのための制御プレーン機能にポリシールールを提供するように構成される。AF320はパケットフローに関する情報をPCF318に提供する。この情報に基づいて、PCF318は、AMF314及びSMF316を適切に動作させるために、モビリティ及びセッション管理に関するポリシールールを決定するように構成される。

【0045】

UPF324は、様々なユーザプレーン動作及び機能、たとえば、パケットルーティング及び転送、トラフィック処理（たとえば、QoS施行）、RAT内／RAT間モビリティのためのアンカーポイント（該当する場合）、パケット検査及びポリシールール施行、合法的傍受（UP収集）、トラフィックアカウンティング及びレポートなどをサポートする。データネットワーク240はコアネットワークの一部ではなく、インターネットアクセス、事業者サービス、サードパーティサービスなどを提供する。たとえば、国際電気通信連合（ITU）は、5Gモバイルネットワークサービスを、高速大容量（eMBB）、超高信頼低遅延通信（uRLLC）、大規模マシンタイプ通信（mMTC）または大規模なモノのインターネット（MIoT）の3つのカテゴリに分類している。eMBBは、HDビデオ、仮想現実（VR）、拡張現実（AR）など、高い帯域幅の要件を有するサービスに重点を置いている。uRLLCは、自動運転及びリモート管理など、遅延の影響を受けやすいサービスに重点を置いている。mMTC及びMIoTは、スマートシティ及びスマート農業など、接続密度に関する高い要件を含むサービスに重点を置いている。データネットワーク240は、これら及び他のサービスを提供するように構成され得る。

10

【0046】

アーキテクチャ300は、以下の参照点を含む。N1参照点は、UE110とAMF314との間に実装される。N2参照点は、（R）AN120とAMF314との間に実装される。N3参照点は、（R）AN120とUPF324との間に実装される。N4参照点は、SMF316とUPF324との間に実装される。N5参照点は、PCF318とAMF320との間に実装される。N6参照点は、UPF324とデータネットワーク240との間に実装される。N7参照点は、SMF316とPCF318との間に実装される。N8参照点は、UDM312とAMF314との間に実装される。N9参照点は、2つのUPF324の間に実装される。N10参照点は、UDM312とSMF316との間に実装される。N11参照点は、AMF314とSMF316との間に実装される。N12参照点は、AMF314とAUSF310との間に実装される。N13参照点は、UDM312とAUSF310との間に実装される。N14参照点は、2つのAMFの間に実装される。N15参照点は、非ローミングシナリオの場合に、PCF318とAMF314との間に実装される。N22参照点は、NSSF313とAMF314との間に実装される。

20

30

【0047】

図4は、次世代ネットワークのローミングアーキテクチャ400を示す。図4のアーキテクチャは、3GPP TS23.501（v15.3.0）にさらに記載されている、参照点表現でのローカルブレイクアウトシナリオである。ローミングシナリオでは、訪問先公衆陸上移動体ネットワーク（VPLMN）402及びホームPLMN（HPLMN）404が示されている。HPLMN404は、モバイルサブスクライバのプロファイルが保持されているPLMNを識別する。VPLMNは、モバイルサブスクライバがHPLMNを離れるときにローミングしているPLMNである。他のネットワークにローミングしているユーザは、HPLMN404からサブスクリプション情報を受信する。ローカルブレイクアウトシナリオでは、PCF318（hPCF）、UDM312、及びAUSF310がUE110のHPLMN404内に存在する。訪問先PCF（vPCF）418を含む他のネットワーク機能が、VPLMN402内に存在する。

40

【0048】

図5は、無線インターフェース122などの無線プロトコルスタック500を示している。本明細書に記載のように、ユーザプレーン512は、ネットワークを介して実際のユーザデータを転送するために使用されるプロトコルのセットを含み、制御プレーン514は、ネットワーク内のユーザ接続及びベアラを制御及び確立するために使用されるプロトコルを含む。ユーザプレーン512及び制御プレーン514に関して、無線プロトコルスタック500は、物理（PHY）レイヤ501、媒体アクセス制御（MAC）レイヤ502、無線リンク制御（RLC）レイヤ503、及びパケットデータコンバージェンスプロ

50

トコル（PDCP）レイヤ504を含む。制御プレーン514は、無線リソース制御（RC）レイヤ505と、非アクセス層（NAS）レイヤ506とをさらに含む。

【0049】

物理レイヤ501は、無線インターフェースを介してMACトランスポートチャネルからの全ての情報を伝達する。データ及びシグナリングメッセージは、物理レイヤ501の異なるレベルの間の物理チャネル上で伝達される。物理チャネルは、物理データチャネルと物理制御チャネルとに分けられる。物理データチャネルは、物理ダウンリンク共有チャネル（PDSCH）、物理ブロードキャストチャネル（PBCH）、物理マルチキャストチャネル（PMCH）、物理アップリンク共有チャネル（PUSCH）、及び物理ランダムアクセスチャネル（PRACH）を含み得る。物理制御チャネルは、物理制御フォーマットインジケータチャネル（PCFICH）、物理ハイブリッドARQインジケータチャネル（PHICH）、物理ダウンリンク制御チャネル（PDCCH）、及び物理アップリンク制御チャネル（PUCCH）を含み得る。

【0050】

MACレイヤ502は、論理チャネルとトランスポートチャネルとの間のマッピング、1つのまたは異なる論理チャネルからのMACサービスデータユニット（SDU）をトランスポートチャネル上で物理レイヤに配信されるトランスポートブロック（TB）に多重化すること、トランスポートチャネル上で物理レイヤから配信されたトランスポートブロックから1つのまたは異なる論理チャネルからのMAC SDUを逆多重化すること、スケジューリング情報のレポート、ハイブリッド自動再送要求（HARQ）による誤り訂正、動的スケジューリングによるUE間の優先処理、1つのUEの論理チャネル間の優先処理、及び論理チャネルの優先順位付けを担当する。RLCレイヤ503は、上位レイヤのプロトコルデータユニット（PDU）の転送、ARQによる誤り訂正、ならびにRLC SDUの連結、セグメンテーション、及び再構築を担当する。RLCレイヤ503はまた、RLCデータPDUの再セグメンテーション、RLCデータPDUの並べ替え、重複検出、RLC SDUの破棄、RLCの再確立、及びプロトコルエラーの検出を担当する。PDCPレイヤ504は、IPデータのヘッダ圧縮及び復元、データの転送（ユーザプレーンまたは制御プレーン）、PDCPシーケンス番号（SN）の維持、下位レイヤの再確立時の上位レイヤPDUの順序通りの配信、RLC確認応答モード（AM）でマッピングされた無線ベアラの下位レイヤの再確立時の下位レイヤSDUの重複排除、ユーザプレーンデータ及び制御プレーンデータの暗号化及び復号、制御プレーンデータの完全性保護及び完全性検証、タイマーに基づく破棄、重複破棄などを担当する。RRCレイヤ505は、NASに関連するシステム情報のブロードキャスト、アクセス層（AS）に関連するシステム情報のブロードキャスト、UEとRANとの間のRRC接続のページング、確立、維持、及び解放、キー管理を含むセキュリティ機能、ポイントツーポイント無線ベアラ（RB）の確立、構成、維持、及び解放を担当する。NASレイヤ506は、UEとコアネットワーク（たとえば、MME／AMF）との間の制御プレーン514の最上位層を表し、UEのモビリティ及びセッション管理手順をサポートして、UE及びコアネットワークの間のIP接続を確立及び維持する。

【0051】

モバイルネットワークからサービスを受ける各UE 110は、構成パラメータが供給される。ホームネットワーク（すなわち、HPLMN）は、UE内の構成パラメータのうちの1つまたは複数を更新することを望み得る。以前のモバイルネットワークでは、構成パラメータの更新はオーバー・ジ・エア（OTA：Over-The-Air）メカニズムを使用して実行されていた。OTAメカニズムでは、OTAゲートウェイと呼ばれる専用のネットワーク要素を配備する必要があった。構成パラメータの更新が実行されるとき、ネットワーク事業者のバックエンドシステムは、サービス要求をOTAゲートウェイに送信した。様々なOTA「ベアラ」がたとえば、ショートメッセージサービス（SMS）、非構造付加サービスデータ（USSD）、ハイパーテキスト転送プロトコル（HTTP）などのサービス要求をUEに送信するように指定された。OTAゲートウェイは、サービ

ス要求がUEに送信されるように、サービス要求をOTA「ベアラ」にマッピングした。たとえば、SMSベアラが使用されるとき、OTAゲートウェイは更新された構成パラメータを1つまたは複数のSMSメッセージ内にカプセル化した。次に、OTAゲートウェイはSMSメッセージをSMSセンター（SMSC）に送信し、SMSセンターはSMSメッセージをUEに送信した。OTAゲートウェイなどの専用ネットワーク要素を配備する必要なく、UE構成パラメータを更新するためにネットワーク事業者が使用し得るネイティブの制御プレーンのソリューションを提供することが望ましい。また、UE構成パラメータがセキュリティ保護されるソリューションを提供することが望ましい。

【0052】

本明細書に記載の実施形態では、ネットワークは、制御プレーンNASメッセージを介して、セキュリティ保護されたUE構成パラメータ更新をUEに透過的に送信する。たとえば、UE構成パラメータ更新は、セキュア化パケットを使用して、NASセキュリティコンテキストの完全性保護キーを使用して、またはその両方を使用して、セキュリティ保護され得る。UEは、NASメッセージでのUE構成パラメータ更新を受信すると、自身のUE構成パラメータを更新し得る。本明細書で提供するソリューションは次世代ネットワーク（たとえば、5G）に関連して説明するが、同様のソリューションが前世代または後世代のネットワークで提供され得る。実施形態のさらなる詳細を以下に示す。

【0053】

図6は、例示的な実施形態におけるUE110のブロック図である。UE110は、無線インターフェースコンポーネント602、1つまたは複数のプロセッサ604、メモリ606、ユーザインターフェースコンポーネント608、及びバッテリー610を含む。無線インターフェースコンポーネント602は、無線または「オーバー・ジ・エア」信号を介した基地局（たとえば、基地局124）とのワイヤレス通信に使用される、RFユニット620（たとえば、トランシーバ）及び1つまたは複数のアンテナ622などの、UE110のローカル無線リソースを表すハードウェアコンポーネントである。プロセッサ604は、UE110の機能を提供する内部回路、ロジック、ハードウェア、ソフトウェアなどを表す。プロセッサ604は、メモリ606にロードされたソフトウェアの命令640を実行するように構成され得る。プロセッサ604は、特定の実施態様に応じて、1つまたは複数のプロセッサのセットを含み得、またはマルチプロセッサコアを含み得る。プロセッサ604は、1つまたは複数のアプリケーション630を実行し得る。これらのアプリケーション630は、RAN120及びコアネットワーク130を介してダウンリンク（DL）データにアクセスし得、また、RAN120及びコアネットワーク130を介して宛先に転送するためのアップリンク（UL）データを生成し得る。メモリ606は、データ、命令640、アプリケーションなどのためのコンピュータ可読記憶媒体であり、プロセッサ604によってアクセス可能である。メモリ606は、一時的及び／または永続的に情報を記憶することが可能なハードウェア記憶デバイスである。メモリ606は、ランダムアクセスメモリ（RAM）、または他の任意の揮発性もしくは不揮発性記憶デバイスを含み得る。ユーザインターフェースコンポーネント608は、エンドユーザとやりとりするためのハードウェアコンポーネントである。たとえば、ユーザインターフェースコンポーネント608は、ディスプレイ650、スクリーン、タッチスクリーンなど（たとえば、液晶ディスプレイ（LCD）、発光ダイオード（LED）ディスプレイなど）を含み得る。ユーザインターフェースコンポーネント608は、キーボードまたはキーパッド652、トラッキングデバイス（たとえば、トラックボールまたはトラックパッド）、スピーカー、マイクロフォンなどを含み得る。

【0054】

UE110はまた、汎用集積回路カード（UICC）660を含み、これは、UE110にセキュリティ及び完全性機能を提供するハードウェアデバイスである。図6には示していないが、UICC660は、プロセッサ（すなわち、中央処理装置（CPU））、メモリ（たとえば、読み取り専用メモリ（ROM）、RAM、電氣的消去可能プログラム可能読み取り専用メモリ（EEPROM））、及び入力／出力（I/O）回路を含み得る。

10

20

30

40

50

UICC 660は、国際移動体加入者識別番号（IMSI）、セキュリティ認証及び暗号化情報、ならびにその他のホーム事業者構成情報などの情報を記憶する汎用加入者識別モジュール（USIM）662をホストまたは記憶し得る。

【0055】

UICC 660及び／またはメモリ606は、UE 110を構成するために使用されるホーム事業者情報を記憶し得、これを本明細書ではUE構成パラメータ664と呼ぶ。UE構成パラメータ664のうちの1つまたは複数は、UICC 660によって排他的に使用され得、UE構成パラメータ664のうちの1つまたは複数は、プロセッサ604によって使用され得る。UE構成パラメータ664は、ルーティングインジケータ、ホームネットワーク識別子（たとえば、PLMN識別情報及びMCC/MNC情報）、ホームネットワーク保護スキーム識別子、ホームネットワーク公開鍵識別子、ホームネットワーク公開証明書、ネットワーク選択情報（たとえば、アクセス技術を使用した事業者制御のPLMNセレクトのリスト）、ならびに／あるいはその他の情報を含み得る。UE構成パラメータ664は、ネットワーク事業者によって事前 to 供給されたデータ、または以下で論じる更新手順などを通じてネットワークによって供給されるデータを表し得る。UE 110は、図6に具体的に示していない他の様々なコンポーネントを含み得る。

【0056】

図7は、例示的な実施形態におけるUE 110の機能モデルである。UE 110は、モバイル機器（ME）702及びUSIM 662などのドメインに細分化され得る。上述のように、USIM 662の機能は、UICC 660上のプロセッサ及びメモリによって実行され得る。ME 702の機能は、プロセッサ604及びメモリ606によって実行され得る。ME 702は無線伝送を実行し、アプリケーションを含む。USIM 662は、それ自体を一義的かつセキュアに識別するデータ及び手順を含む。これらの機能は、典型的には、UICC 660などのスタンドアロンのスマートカードに組み込まれる。上記のように、UE構成パラメータ664のうちの1つまたは複数は、UICC 660内で使用または処理するためにUSIM 662に排他的に記憶され得、UE構成パラメータ664のうちの1つまたは複数は、ME 702内で使用または処理するためにME 702に排他的に記憶され得る。

【0057】

図8は、例示的な実施形態におけるAMF要素314のブロック図である。上述のように、AMF要素314は、UEベースの認証、認可、モビリティ管理などを提供するように構成される。この実施形態では、AMF要素314は、1つまたは複数のプラットフォームで動作する以下のサブシステム、すなわち、ネットワークインターフェースコンポーネント802及び更新マネージャ804を含む。ネットワークインターフェースコンポーネント802は、他のネットワーク要素及び／またはUEと（たとえば、RAN 120を介して）制御プレーンメッセージまたはシグナリングを交換するように構成される回路、ロジック、ハードウェア、手段などを含み得る。ネットワークインターフェースコンポーネント802は、様々なプロトコル（NASプロトコルを含む）または参照点を使用して動作し得る。更新マネージャ804は、UEでのUE構成パラメータの更新を処理するように構成される回路、ロジック、ハードウェア、手段などを含み得る。AMF要素314のサブシステムのうちの1つまたは複数は、アナログ及び／またはデジタル回路から構成されるハードウェアプラットフォーム上に実装され得る。AMF要素314のサブシステムのうちの1つまたは複数は、メモリ832に記憶された命令を実行するプロセッサ830上に実装され得る。プロセッサ830は、命令を実行するように構成される統合ハードウェア回路を含み、メモリ832は、データ、命令、アプリケーションなどのための非一時的コンピュータ可読記憶媒体であり、プロセッサ830によってアクセス可能である。AMF要素314は、図8に具体的に示していない他の様々なコンポーネントを含み得る。

【0058】

図9は、例示的な実施形態におけるUDM要素312のブロック図である。上述のように、UDM要素312は、UEのアクセス及びモビリティサブスクリプションデータを記

10

20

30

40

50

憶するように構成される。この実施形態では、UDM要素312は、1つまたは複数のプラットフォーム上で動作する以下のサブシステム、すなわち、ネットワークインターフェースコンポーネント902、サブスクリバデータリポジトリ904、及び更新マネージャ906を含む。ネットワークインターフェースコンポーネント902は、他のネットワーク要素と制御プレーンメッセージまたはシグナリングを交換するように構成される回路、ロジック、ハードウェア、手段などを含み得る。ネットワークインターフェースコンポーネント902は、様々なプロトコルまたは参照点を使用して動作し得る。サブスクリバデータリポジトリ904は、アクセス及びモビリティサブスクリプションデータを記憶するように構成される回路、ロジック、ハードウェア、手段などを含み得る。更新マネージャ906は、UEでのUE構成パラメータの更新を処理するように構成される回路、ロジック、ハードウェア、手段などを含み得る。UDM要素312のサブシステムのうちの1つまたは複数は、アナログ及び／またはデジタル回路から構成されるハードウェアプラットフォーム上に実装され得る。UDM要素312のサブシステムのうちの1つまたは複数は、メモリ932に記憶された命令を実行するプロセッサ930上に実装され得る。UDM要素312は、図9に具体的に示していない他の様々なコンポーネントを含み得る。

【0059】

UEがネットワークに登録するとき、またはUEがネットワークに登録した後に、更新手順が実行され得、または呼び出され得る。図10～図12は、UDM要素312、AMF要素314、及びUE110によって実行される一般的な更新手順を示している。更新手順のさらなる詳細については、以下の例示的なメッセージ図で説明する。したがって、本明細書で提供するフローチャートは、メッセージ図に関連して説明する更新手順によって補われ得る。

【0060】

図10は、例示的な実施形態における、UDM要素312において更新手順を実行する方法1000を示すフローチャートである。方法1000のステップは、図9のUDM要素312を参照して説明するが、当業者は、方法1000が他のネットワーク要素またはデバイスで実行され得ることを理解するであろう。また、本明細書に記載のフローチャートのステップは、全てを包括するものではなく、図示していない他のステップを含み得、ステップは代替の順序で実行され得る。

【0061】

この実施形態では、UE110はNAS登録手順を介してネットワークに登録しており、または既にネットワークに登録されていると想定し得る。UDM要素312の更新マネージャ906は、UE110内のUE構成パラメータ664のうちの1つまたは複数を更新するための更新手順を開始する（ステップ1002）。たとえば、更新マネージャ906は、サブスクリバデータリポジトリ904に記憶されたUE構成情報を処理し、UE構成パラメータ664の更新が必要または望ましいと判定し得る。更新マネージャ906は、UE110用のUE構成パラメータ更新をアセンブルする（ステップ1004）。UE構成パラメータ更新は、UE110においてUE構成パラメータ664の更新を実行するために使用される情報、コマンド、命令などを含む。たとえば、UE構成パラメータ更新は、UE110の1つまたは複数の更新されたUE構成パラメータを、アクセス及びモビリティサブスクリプションデータの一部として含み得る。

【0062】

更新マネージャ906は、1つまたは複数の保護メカニズムに従って、UE構成パラメータ更新にセキュリティ保護を適用する（ステップ1006）。一実施形態では、保護メカニズムは、セキュア化パケットであり得る。したがって、更新マネージャ906は、セキュリティ保護を適用するために、UE構成パラメータ更新をセキュア化パケット内に構成またはカプセル化し得る（任意選択のステップ1008）。一般に、セキュア化パケットは、特定のメカニズムが適用されたアプリケーションメッセージを含む。アプリケーションメッセージは、ネットワーク要素とUE110との間で交換されるコマンドまたはデータである。送信機は、セキュリティヘッダ（コマンドヘッダ）をアプリケーションメッセ

10

20

30

40

50

ージの先頭に付加し、そして、要求されたセキュリティをコマンドヘッダの一部と、アプリケーションメッセージの全体とに適用する。結果として得られる構造は、セキュア化されたデータをペイロードとして含む（セキュア化された）コマンドパケットと呼ばれる。更新マネージャ 906 は、ローカルのセキュア化パケットライブラリまたはリモートのセキュア化パケットライブラリにアクセスして、UE 構成パラメータ更新をセキュア化パケット内に構成またはカプセル化し得る。他の実施形態では、保護メカニズムは完全性保護であり得る。したがって、更新マネージャ 906 は、UE 110 の NAS セキュリティコンテキストを使用して、UE 構成パラメータ更新に完全性保護を適用し得る（任意選択のステップ 1010）。NAS セキュリティは、NAS セキュリティキーを使用して制御プレーンにおいて UE 110 と AMF 要素 314 との間で NAS シグナリングメッセージをセキュアに配信するために使用される。NAS セキュリティコンテキストは、NAS メッセージを保護するために使用される NAS セキュリティキー及びパラメータの集合体である。UE 110 がネットワークに認証されたときに、NAS セキュリティキーが生成される。したがって、認証後、更新マネージャ 906 は、NAS セキュリティコンテキストの完全性保護キーを使用して、UE 構成パラメータ更新に完全性保護を適用し得る。さらに他の実施形態では、更新マネージャ 906 は、セキュア化パケットと NAS セキュリティコンテキストとの両方を使用して、UE 構成パラメータ更新を保護し得る（任意選択のステップ 1012）。次に、更新マネージャ 906 は、セキュリティ保護された UE 構成パラメータ更新を制御プレーンメッセージに挿入するか、または別の方法で含め得る（ステップ 1014）。

【0063】

更新マネージャ 906 はまた、UE 確認応答インジケータを制御プレーンメッセージに挿入するか、または別の方法で含め得る（任意選択のステップ 1016）。UE 構成パラメータ更新のセキュリティチェックの成功についての UE 110 からの確認応答をホームネットワークが望むとき、UE 確認応答インジケータが含まれ得る。更新マネージャ 906 はまた、再登録インジケータを制御プレーンメッセージに挿入するか、または別の方法で含め得る（任意選択のステップ 1016）。UE 110 が更新された UE 構成パラメータを使用してネットワークに再登録することをホームネットワークが望むとき、再登録インジケータが含まれ得る。次に、更新マネージャ 906 は、ネットワークインターフェースコンポーネント 902 を介して、セキュリティ保護された UE 構成パラメータ更新と、UE 確認応答インジケータ及び／または再登録インジケータ（要求された場合）とを含む制御プレーンメッセージを AMF 要素 314 に送信する（ステップ 1018）。

【0064】

図 11 は、例示的な実施形態における、AMF 要素 314 において更新手順を実行する方法 1100 を示すフローチャートである。方法 1100 のステップは、図 8 の AMF 要素 314 を参照して説明するが、当業者は、方法 1100 が他のネットワーク要素またはデバイスで実行され得ることを理解するであろう。

【0065】

AMF 要素 314 の更新マネージャ 804 は、ネットワークインターフェースコンポーネント 802 を介して、セキュリティ保護された UE 構成パラメータ更新を含む制御プレーンメッセージを UDM 要素 312 から受信する（ステップ 1102）。更新マネージャ 804 は、セキュリティ保護された UE 構成パラメータ更新を NAS メッセージのコンテナに挿入する（ステップ 1104）。セキュリティ保護された UE 構成パラメータ更新の伝送は、AMF 要素 314 にとって「透過的」と考えられる。したがって、更新マネージャ 804 は、UE 構成パラメータ更新を修正も変更もせずに、セキュリティ保護された UE 構成パラメータ更新を転送するようにプログラムされる。そのため、更新マネージャ 804 は、UDM 要素 312 から制御プレーンメッセージで受信したセキュリティ保護された UE 構成パラメータ更新を、UE 構成パラメータ更新用に設計された「透過的」なコンテナに挿入し得る。このような透過的なコンテナの一例について、以下でより詳細に説明する。

【0066】

セキュリティ保護されたUE構成パラメータ更新を転送するためにAMF要素314によって使用されるNASメッセージのタイプは、実行されているNAS手順に依存し得る。たとえば、NAS登録手順が実行されているとき、NASメッセージは、NAS登録受諾メッセージを含み得る。NASトランスポート手順が実行されているとき、NASメッセージはDL NASトランスポートメッセージを含み得る。次に、更新マネージャ804は、ネットワークインターフェースコンポーネント802を介してNASメッセージをUE110に送信する（ステップ1106）。

【0067】

図12は、例示的な実施形態における、UE110において更新手順を実行する方法1200を示すフローチャートである。方法1200のステップは、図6及び図7のUE110を参照して説明するが、当業者は、方法1200が他のデバイスで実行され得ることを理解するであろう。

【0068】

UE110は（たとえば、ME702を介して）、AMF要素314からNASメッセージを受信する（ステップ1202）。ME702またはUSIM662は、NASメッセージのコンテナに含まれるセキュリティ保護されたUE構成パラメータ更新が、UE110のホームネットワーク（すなわち、HPLMN）によって提供されたことを検証するためにセキュリティチェックを実行する（ステップ1204）。たとえば、ME702またはUSIM662は、チェックサムを計算して、受信したセキュリティ保護されたUE構成パラメータ更新が、UDM要素312によって送信されたセキュリティ保護されたUE構成パラメータ更新と一致するか否かを判定し得る。セキュリティチェックが成功しなかったとき、ME702またはUSIM662は、セキュリティ保護されたUE構成パラメータ更新を破棄する（ステップ1206）。セキュリティチェックが成功したとき、ME702またはUSIM662は、UE構成パラメータ更新に基づいて、UE110に供給された1つまたは複数のUE構成パラメータ664を更新する（ステップ1208）。上述のように、UE構成パラメータ更新は、セキュア化パケット内にカプセル化され得る。このシナリオでは、USIM662は、セキュア化パケットライブラリを使用して、セキュア化パケットからUE構成パラメータ更新を復号またはアンパックするように構成される。次に、USIM662は、UE構成パラメータ更新に基づいて、USIM662にとってローカルな1つまたは複数のUE構成パラメータ664を更新する。

【0069】

NASメッセージがUE確認応答インジケータを含むとき、ME702またはUSIM662は、UE確認応答を含むコンテナを有するNASメッセージをAMF要素314に送信する（任意選択のステップ1210）。UE確認応答の伝送は、AMF要素314にとって「透過的」であると考えられる。したがって、ME702またはUSIM662は、UE確認応答用に設計された「透過的」なコンテナにUE確認応答を挿入するようにプログラムされる。このような透過的なコンテナの一例について、以下でより詳細に説明する。

【0070】

NASメッセージのタイプは、実行されているNAS手順に依存し得る。たとえば、NAS登録手順が実行されているとき、NASメッセージは、NAS登録完了メッセージまたはUL NASトランスポートメッセージを含み得る。NASトランスポート手順が実行されているとき、NASメッセージは、UL NASトランスポートメッセージを含み得る。

【0071】

図11において、AMF要素314の更新マネージャ804は、ネットワークインターフェースコンポーネント802を介して、UE確認応答を含むコンテナを有するNASメッセージをUE110から受信する（任意選択のステップ1108）。次に、更新マネージャ804は、ネットワークインターフェースコンポーネント802を介して、UE確認

10

20

30

40

50

応答を有する制御プレーンメッセージをUDM要素312に送信する（任意選択のステップ1110）。図10において、UDM要素312の更新マネージャ906は、ネットワークインターフェースコンポーネント902を介してAMF要素314からUE確認応答を有する制御プレーンメッセージを受信する（任意選択のステップ1020）。次に、更新マネージャ906は、UE確認応答がUE110によって提供されたことを検証する（任意選択のステップ1022）。

【0072】

図12において、AMF要素314からのNASメッセージが再登録インジケータを含むとき、UE110は（たとえば、ME702を介して）、NAS登録手順を開始して、更新されたUE構成パラメータを使用して再登録する（任意選択のステップ1212）。その後、更新手順は終了し得る。

【0073】

以下、さらなる実施形態における、更新手順を実行する例を提供する。

【0074】

例1：セキュア化パケットを使用した登録中の更新手順

図13は、例示的な実施形態における登録中の更新手順を示すメッセージ図である。この実施形態では、UE110はアイドルモード（たとえば、RRC_IDLE）にある。UE110は、NAS登録要求をAMF要素314に送信することによって、NAS登録手順を開始する（S1）。AMF要素314は、（タイプ「新規」の）NAS登録要求に回答して、UE110を認証するための認証手順を開始し得る（S2）。認証手順のために、AMF要素314は、AUSF要素310及びUDM要素312とやりとりし得る。たとえば、AMF要素314は、認証要求（すなわち、Nausf__UEAuthentication__Authenticate要求）をAUSF要素310に送信し得る。AUSF要素310は、認証要求を受信することに応じて、認証要求（すなわち、Nudm__UEAuthentication__Get要求）をUDM要素312に送信し得る。UDM要素312は、認証方法を選択し、（必要な場合に）AUSF要素310の認証データ及びキー素材（たとえば、トークン）を計算する認証資格証明リポジトリ及び処理機能（ARPF）に関連する機能をホストする。UDM要素312は、認証ベクトル（AV）及び他の情報を含む認証応答（すなわち、Nudm__UEAuthentication__Get応答）をAUSF要素310に送信し得る。次に、AUSF要素310は、AV及び他の情報を含む認証応答（すなわち、Nausf__UEAuthentication__Authenticate応答）をAMF要素314に送信し得る。AMF要素314は、UDM/AUSFによって提供された情報を使用して、UE110との認証手順を実行するように構成される。たとえば、AMF要素314は、認証要求をAVからの認証トークンと共にUE110に送信し得、UE110は認証トークンの検証を試みる。成功した場合、UE110は応答トークンを計算し、応答トークンを有する認証応答を送信し、これはAMF要素314によって受信される。AMF要素314は、他の認証要求（すなわち、Nausf__UEAuthentication__Authenticate要求）をフォーマットまたは生成し、UE110からの応答トークンを他の情報と共に認証要求に挿入し得る。次に、AMF要素314は、認証要求をAUSF要素310に送信し得る。AUSF要素310は、UE110からの応答トークンが予期された応答トークンと一致するか否かを検証し、認証の成功/失敗を示す認証応答（すなわち、Nausf__UEAuthentication__Authenticate応答）をAMF要素314に送信し得る。

【0075】

認証後、AMF要素314は、NASセキュリティコンテキストを確立するためのNASセキュリティ手順を開始し得る（S3）。NASセキュリティ手順の一部として、AMF要素314は、暗号化及び完全性保護のためのNASセキュリティアルゴリズム（または複数のアルゴリズム）を選択する。次に、AMF要素314は、NASセキュリティアルゴリズム（複数可）、ngKSI、及び他の情報を示すセキュリティモードコマンドメ

10

20

30

40

50

ッセージをUE110に送信する。UE110は、ngKSI及びNASセキュリティアルゴリズムを使用して、後続のNASメッセージを保護するための対応するキーを導出する。その結果、NASセキュリティコンテキストが、UE110とAMF要素314との間に確立される。次に、UE110は、セキュリティモード完了メッセージをAMF要素314に送信する。

【0076】

NAS登録手順のさらなる部分として、AMF要素314は、サブスクリプションデータ要求（たとえば、Nudm__SDM__Getメッセージ）をHPLMNのUDM要素312に送信して、他の情報の中でもとりわけ、UE110のアクセス及びモビリティサブスクリプションデータを取得する（S4）。ユーザサブスクリプション情報がUE構成パラメータ更新（たとえば、ルーティングID更新）を開始することを示すとき、UDM要素312は更新手順を開始する。UDM要素312は、1つまたは複数の更新されたUE構成パラメータを含むUE構成パラメータ更新をアセンブルする。次に、UDM要素312は、セキュア化パケットライブラリにアクセスしてUE構成パラメータ更新をセキュア化パケット内にカプセル化することによって、UE構成パラメータ更新にセキュリティ保護を適用する。セキュア化パケット及びセキュア化パケット構造の一例が、3GPP TS131.115（v.9.0.0）に開示されており、これは引用により本明細書に完全に含まれているかのように組み込まれている。次に、UDM要素312は、セキュア化パケットを含むサブスクリプションデータ応答（たとえば、Nudm__SDM__Get応答）をAMF要素314に送信する（S5）。UDM要素312はまた、UE確認応答インジケータ及び／または再登録インジケータをサブスクリプションデータ応答に含め得る。

【0077】

登録手順のさらに他の部分として、AMF要素314はまた、サブスクライブメッセージ（たとえば、Nudm__SDM__Subscribe）をUDM要素312に送信して、UE構成パラメータの変更の通知をサブスクライブし得る（図13には示していない）。

【0078】

AMF要素314は、更新手順の一部として、セキュア化パケットをUE110に透過的に送信するように構成される。したがって、AMF要素314は、NAS登録受諾メッセージをフォーマットまたは生成し、セキュア化パケットをNAS登録受諾メッセージのコンテナに挿入する。AMF要素314はまた、UE確認応答インジケータ及び／または再登録インジケータ（該当する場合）をNAS登録受諾メッセージのコンテナに挿入し得る。次に、AMF要素314は、NAS登録受諾メッセージをUE110に送信する（S6）。

【0079】

この実施形態では、NAS登録受諾メッセージのコンテナは、UE構成パラメータ更新用に設計される。表1は、NAS登録受諾メッセージのメッセージ内容の一例を示している。

【0080】

10

20

30

40

50

【表 1】

表 1 :

I E I	情報要素	タイプ／参照	存在	フォー マット	長さ
	拡張プロトコル弁別子	拡張プロトコル弁別子	M	V	1
	セキュリティヘッダタイプ	セキュリティヘッダタイプ	M	V	1 / 2
	予備の半オクテット	予備の半オクテット	M	V	1 / 2
	登録受諾メッセージ識別 情報	メッセージタイプ	M	V	1
	...				
x x	UE 構成パラメータ更新 コンテナ	UE 構成パラメータ更新 コンテナ	O	T L V - E	2 0 - 2 0 4 8
	...				

10

【 0 0 8 1】

この例では、NAS 登録受諾メッセージは、新しく定義されたUE 構成パラメータ更新コンテナ情報要素 (IE) を含む。NAS プロトコルのさらなる説明は、3 G P P T S 2 4 . 3 0 1 (v 1 5 . 4 . 0) で見つけられ得、これは引用により本明細書に完全に含まれているかのように組み込まれている。表 2 は、UE 構成パラメータ更新コンテナ IE の一例である。AMF 要素 3 1 4 がセキュア化パケットを修正せずにセキュア化パケットをコンテナに挿入するので、このコンテナは透過的であると考えられる。

20

【 0 0 8 2】

【表 2】

表 2 :

8 7 6 5 4 3 2 1

UE 構成パラメータ更新コンテナ IE I	オクテット 1
UE 構成パラメータ更新コンテナ内容長	オクテット 2 オクテット 3
UE 構成パラメータ更新ヘッダ	オクテット 4
セキュア化パケット [UE 構成パラメータ更新]	オクテット 5 - 2 0 4 8 *

30

【 0 0 8 3】

表 3 は、UE 構成パラメータ更新コンテナ IE のUE 構成パラメータ更新ヘッダの一例を示している。

【 0 0 8 4】

【表 3】

表 3 :

8	7	6	5	4	3	2	1	
0	0	0	0	0	R R R	U E	デー タ	オク テ ット 4
予備	予備	予備	予備	予備		A C K	タイ プ	

40

【 0 0 8 5】

ヘッダにおいて、R R Rビットは、再登録インジケータとして使用され得る。U E A C Kビットは、UE 確認応答インジケータとして使用され得る。データタイプビットは、コンテナが、ネットワークからUE に送信されるNAS メッセージで使用されているのか

50

(たとえば、値＝０)、ＵＥからネットワークに送信されるＮＡＳメッセージで使用されているのか(たとえば、値＝１)を示すために使用され得る。

【００８６】

ＭＥ７０２は、ＮＡＳ登録受諾メッセージを受信すると、プロトコル識別子が「ＳＩＭデータダウンロード」に設定され、データ符号化方式が「クラス２メッセージ」に設定され、ＳＭＳペイロードがセキュア化パケットであるＳＭＳメッセージが受信されたかのように動作し得る。ＭＥ７０２は、セキュア化パケットをＵＳＩＭ６６２にルーティングまたはアップロードする（Ｓ７）。ＵＳＩＭ６６２は、セキュリティチェックを実行して、セキュア化パケットがホームネットワークのＵＤＭ要素３１２によって送信されたことを検証する。セキュリティチェックが成功しなかった場合、ＵＳＩＭ６６２はＵＥ構成パラメータ更新を破棄し、登録手順を続行する。セキュリティチェックが成功した場合、ＵＳＩＭ６６２は、セキュア化パケットライブラリを使用して、セキュア化パケットからＵＥ構成パラメータ更新をアンパックする。セキュア化パケットの完全性／リプレイ保護が検証された後、ＵＳＩＭ６６２は、ＵＥ構成パラメータ更新に基づいてＵＥ構成パラメータ６６４のうちの１つまたは複数を更新する。

【００８７】

ネットワークがＵＥ１１０からの確認応答を要求しており、セキュリティチェックが成功した場合、ＵＳＩＭ６６２は、ＵＥ確認応答をＭＥ７０２に送信し得る（Ｓ８）。ＭＥ７０２は、他のＮＡＳメッセージをフォーマットまたは生成して、ＵＥ確認応答をＡＭＦ要素３１４に転送する。図１３に示す例では、ＭＥ７０２は、ＮＡＳ登録完了メッセージをフォーマットし、ＵＥ確認応答をＮＡＳ登録完了メッセージのコンテナに挿入する。ＮＡＳ登録完了メッセージのコンテナは、ＵＥ確認応答用に設計される。表４は、ＮＡＳ登録完了メッセージのメッセージ内容の一例を示している。

【００８８】

【表４】

表４：

ＩＥＩ	情報要素	タイプ／参照	存在	フォーマット	長さ
	拡張プロトコル弁別子	拡張プロトコル弁別子	M	V	1
	セキュリティヘッダタイプ	セキュリティヘッダタイプ	M	V	1／2
	予備の半オクテット	予備の半オクテット	M	V	1／2
	登録受諾メッセージ識別情報	メッセージタイプ	M	V	1
	...				
x x	ＵＥ確認応答コンテナ	ＵＥ確認応答コンテナ	O	T L V - E	2 0 - 2 0 4 8

【００８９】

この例では、ＮＡＳ登録完了メッセージは、新しく定義されたＵＥ確認応答コンテナＩＥを含む。表５は、ＵＥ確認応答コンテナＩＥの一例である。

【００９０】

10

20

30

40

50

【表 5】

表 5 :

8 7 6 5 4 3 2 1

UE 確認応答コンテナ I E I	オクテット 1
UE 確認応答コンテナ内容長	オクテット 2 オクテット 3
UE 確認応答ヘッダ	オクテット 4
UE 確認応答	オクテット 5 – 2 0

10

【 0 0 9 1】

表 6 は、UE 確認応答ヘッダの一例を示している。

【 0 0 9 2】

【表 6】

表 6 :

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	データ	オクテット 4
予備	予備	予備	予備	予備	予備	予備	タイプ	

20

【 0 0 9 3】

他の例では、USIM662 は、セキュア化パケットライブラリにアクセスして UE 確認応答をセキュア化パケット内にカプセル化することによって、UE 確認応答にセキュリティ保護を適用し得る。したがって、ME702 は、セキュア化パケットを UE 確認応答コンテナ I E に挿入し得る。

【 0 0 9 4】

次に、ME702 は、UE 確認応答を含むコンテナを有する NAS 登録完了メッセージを AMF 要素 314 に送信する (S9)。AMF 要素 314 は、UE 確認応答を有する情報メッセージ (たとえば、Nudm_SDM_Info メッセージ) を UDM 要素 312 に送信する (S10)。次に、UDM 要素 312 は、UE 確認応答が UE110 によって提供されたことを検証し得る。

30

【 0 0 9 5】

図 13 に示す代替例では、ME702 は、他のタイプの NAS メッセージを使用して、UE 確認応答を AMF 要素 314 に送信し得る。この代替例では、ME702 は UL NAS トランスポートメッセージをフォーマットし、UE 確認応答を UL NAS トランスポートメッセージのコンテナに挿入する。UL NAS トランスポートメッセージのペイロードコンテナ I E において、ペイロードコンテナタイプ値は、UE 確認応答用に設計され得る。次に、ME702 は、UE 確認応答を含むコンテナを有する UL NAS トランスポートメッセージを AMF 要素 314 に送信する (S9a)。次いで、AMF 要素 314 は、UE 確認応答を有する情報メッセージ (たとえば、Nudm_SDM_Info メッセージ) を UDM 要素 312 に送信する (S10a)。

40

【 0 0 9 6】

UE110 の再登録が必要なことをネットワークが示しており、セキュリティチェックが成功した場合、UE110 は登録解除し、更新された UE 構成パラメータを使用して、新しい NAS 登録手順を再度開始する (S11)。

【 0 0 9 7】

例 2 : セキュア化パケットを使用した登録後の更新手順

図 14 は、例示的な実施形態における登録後の更新手順を示すメッセージ図である。この実施形態では、UE110 は、既にネットワークに登録しており、接続モード (すなわち、RRC-CONNECTED) にある。登録後のある時点で、UDM 要素 312 は、

50

命令を受信するか、またはローカルポリシーを処理して、UE 110内のUE構成パラメータが更新される必要があると判定し得る。したがって、UDM要素312は、更新手順を開始し、UE構成パラメータ更新をアセンブルする。次に、UDM要素312は、セキュア化パケットライブラリにアクセスしてUE構成パラメータ更新をセキュア化パケット内にカプセル化することによって、UE構成パラメータ更新にセキュリティ保護を適用する。次に、UDM要素312は、セキュア化パケットを含む更新通知（たとえば、Nudm_SDM_UpdateNotification）をAMF要素314に送信する（S1）。UDM要素312はまた、UE確認応答インジケータ及び／または再登録インジケータを更新通知に含め得る。

【0098】

AMF要素314は、更新手順の一部として、セキュア化パケットをUE 110に透過的に送信するように構成される。したがって、AMF要素314は、ダウンリンク（DL）NASトランスポートメッセージをフォーマットまたは生成し、セキュア化パケットをDL NASトランスポートメッセージのコンテナに挿入する。AMF要素314はまた、UE確認応答インジケータ及び／または再登録インジケータ（該当する場合）をDL NASトランスポートメッセージのコンテナに挿入し得る。この実施形態では、DL NASトランスポートメッセージのコンテナは、UE構成パラメータ更新用に設計される。AMF要素314は、ペイロードコンテナタイプIEを「UE構成パラメータコンテナ」に設定し、ペイロードコンテナIEをセキュア化パケットに設定し得る。次に、AMF要素314は、DL NASトランスポートメッセージをUE 110に送信する（S2）。

【0099】

ME702は、DL NASトランスポートメッセージを受信すると、プロトコル識別子が「SIMデータダウンロード」に設定され、データ符号化方式が「クラス2メッセージ」に設定され、SMSペイロードがセキュア化パケットであるSMSメッセージが受信されたかのように動作し得る。ME702は、セキュア化パケットをUSIM662にルーティングまたはアップロードする（S3）。USIM662は、セキュア化パケットがホームネットワークのUDM要素312によって送信されたことを検証するためにセキュリティチェックを実行する。セキュリティチェックが成功しなかった場合、USIM662はUE構成パラメータ更新を破棄する。セキュリティチェックが成功した場合、USIM662は、セキュア化パケットライブラリを使用して、セキュア化パケットからUE構成パラメータ更新をアンパックする。セキュア化パケットの完全性／リプレイ保護が検証された後、USIM662は、UE構成パラメータ更新に基づいてUE構成パラメータ664のうちの1つまたは複数を更新する。

【0100】

ネットワークがUE 110からの確認応答を要求しており、セキュリティチェックが成功した場合、USIM662は、UE確認応答をME702に送信し得る（S4）。ME702はUL NASトランスポートメッセージをフォーマットまたは生成し、UE確認応答をUL NASトランスポートメッセージのコンテナに挿入する。UL NASトランスポートメッセージのコンテナは、UE確認応答用に設計される。次に、ME702は、UE確認応答を含むコンテナを有するUL NASトランスポートメッセージをAMF要素314に送信する（S5）。AMF要素314は、UE確認応答を有する情報メッセージ（たとえば、Nudm_SDM_Infoメッセージ）をUDM要素312に送信する（S6）。次に、UDM要素312は、UE確認応答がUE 110によって提供されたことを検証し得る。

【0101】

UE 110の再登録が必要なことをネットワークが示しており、セキュリティチェックが成功した場合、UE 110は登録解除し、更新されたUE構成パラメータを使用して、新しいNAS登録手順を再度開始する（図示せず）。

【0102】

例3：セキュリティキーを使用した登録中の更新手順

10

20

30

40

50

図15は、例示的な実施形態における登録中の更新手順を示すメッセージ図である。この実施形態では、UE110は、NAS登録要求をAMF要素314に送信することによって、NAS登録手順を開始する(S1)。AMF要素314は、(タイプ「新規」の)NAS登録要求に応答して、UE110を認証するための認証手順を開始し得る(S2)。UE110がネットワークに認証されたとき、AMF要素314は、NASセキュリティコンテキストを確立するためのNASセキュリティ手順を開始し得る(S3)。UE110が認証され、NASセキュリティコンテキストが確立された状態で、AMF要素314は、サブスクリプションデータ要求(たとえば、Nudm__SDM__Getメッセージ)をHPLMNのUDM要素312に送信して、他の情報の中でもとりわけ、UE110のアクセス及びモビリティサブスクリプションデータを取得する(S4)。ユーザサブスクリプション情報が、UE構成パラメータ更新(たとえば、ルーティングID更新)を開始することを示すとき、UDM要素312は、更新手順を開始する。UDM要素312は、UE構成パラメータ更新をアセンブルし、UE110のNASセキュリティコンテキストを使用して、UE構成パラメータ更新に完全性保護を適用する。そうするために、UDM要素312は、UE構成パラメータ更新を有する保護要求(たとえば、Nausf__ParameterProtectionRequest)をAUSF要素310に送信する(S5)。AUSF要素310は、(NASシーケンス番号から構築された)NASカウン트를特定し、UE110のNASセキュリティコンテキスト、たとえば、UE構成パラメータ更新のAUSFメッセージ認証コード(MAC)及びNASカウンなどに基づいて完全性保護情報を計算する。AUSF要素310はまた、UE110から期待されるMAC(X-UE-MAC)を計算し得る。次に、AUSF要素310は、完全性保護情報(すなわち、AUSF-MAC、NASカウン、及びX-UE-MAC)を有する保護応答(たとえば、Nausf__ParameterProtectionResponse)をUDM要素312に送信する(S6)。次に、UDM要素312は、UE構成パラメータ更新及び完全性保護情報(すなわち、AUSF-MAC及びNASカウン)を含むサブスクリプションデータ応答(たとえば、Nudm__SDM__Get応答)をAMF要素314に送信する(S7)。UDM要素312はまた、UE確認応答インジケータ及び／または再登録インジケータをサブスクリプションデータ応答に含め得る。

【0103】

AMF要素314は、更新手順の一部として、UE構成パラメータ更新をUE110に透過的に送信するように構成される。したがって、AMF要素314は、NAS登録受諾メッセージをフォーマットまたは生成し、UE構成パラメータ更新を、完全性保護情報(たとえば、AUSF-MAC及びNASカウン)と共に、NAS登録受諾メッセージのコンテナに挿入する。AMF要素314はまた、UE確認応答インジケータ及び／または再登録インジケータ(該当する場合)をNAS登録受諾メッセージのコンテナに挿入し得る。次に、AMF要素314は、NAS登録受諾メッセージをUE110に送信する(S8)。

【0104】

この例では、NAS登録受諾メッセージは、新しく定義されたUE構成パラメータ更新コンテナIEを含む。表7は、UE構成パラメータ更新コンテナIEの一例である。

【0105】

10

20

30

40

50

【表 7】

表 7 :

8 7 6 5 4 3 2 1	
UE 構成パラメータ更新コンテナ I E I	オクテット 1
UE 構成パラメータ更新コンテナ内容長	オクテット 2 オクテット 3
UE 構成パラメータ更新ヘッダ	オクテット 4
A U S F - M A C	オクテット 5 - 2 0
N A S カウント	オクテット 2 1 - 2 2
UE 構成パラメータ更新	オクテット 2 3 * - 2 0 4 8 *

10

【0106】

このコンテナは、AMF 要素 314 が、UE 構成パラメータ更新を修正することなく、UE 構成パラメータ更新をコンテナに挿入するので、透過的であると考えられる。例 1 に記載したように、UE 構成パラメータ更新ヘッダの UE ACK ビットは、ネットワークが UE からの確認応答を要求していることを示すために使用され得、RRR ビットは、ネットワークが再登録を要求することを示すために使用され得る。

【0107】

UE 110 の ME 702 は、NAS 登録受諾メッセージを受信することに応答して、UE 構成パラメータ更新がホームネットワークの UDM 要素 312 によって送信されたことを検証するためにセキュリティチェックを実行する。たとえば、ME 702 は、UE 構成パラメータ更新及び NAS カウントに対する UE-MAC を計算し、UE-MAC を AUSF-MAC と比較する。MAC が一致する場合、UE 構成パラメータ更新がホームネットワークからのものであることが検証され、セキュリティチェックが成功する。セキュリティチェックが成功しなかった場合、ME 702 は UE 構成パラメータ更新を破棄し、登録手順を続行する。セキュリティチェックが成功した場合、ME 702 及び／または USIM 662 は、UE 構成パラメータ更新に基づいて、UE 構成パラメータ 664 のうちの 1 つまたは複数を更新する。

20

【0108】

ネットワークが UE 110 からの確認応答を要求しており、セキュリティチェックが成功した場合、ME 702 は NAS 登録完了メッセージをフォーマットし、UE-MAC を NAS 登録完了メッセージのコンテナに挿入する。NAS 登録完了メッセージのコンテナは、UE 確認応答用に設計される。この例では、NAS 登録完了メッセージは、新しく定義された UE 確認応答コンテナ I E を含む。表 8 は、UE 確認応答コンテナ I E の一例である。

30

【0109】

【表 8】

表 8 :

8 7 6 5 4 3 2 1	
UE 構成パラメータ更新コンテナ I E I	オクテット 1
UE 構成パラメータ更新コンテナ内容長	オクテット 2 オクテット 3
UE 構成パラメータ更新コンテナヘッダ	オクテット 4
UE-MAC	オクテット 5 - 2 0

40

【0110】

次に、ME 702 は、UE-MAC を含むコンテナを有する NAS 登録完了メッセージを AMF 要素 314 に送信する (S9)。AMF 要素 314 は、UE-MAC を有する情

50

報メッセージ（たとえば、`Nu dm__S DM__I n f o`メッセージ）をUDM要素312に送信する（S10）。次に、UDM要素312は、UE110によって計算されたUE-MACをAUSF要素310によって計算されたX-UE-MACと比較して、UE確認応答がUE110によって提供されたことを検証し得る。

【0111】

UE110の再登録が必要なことをネットワークが示しており、セキュリティチェックが成功した場合、UE110は登録解除し、更新されたUE構成パラメータを使用して、新しいNAS登録手順を再度開始する（図示せず）。

【0112】

例4：セキュリティキーを使用した登録後の更新手順

図16は、例示的な実施形態における登録後の更新手順を示すメッセージ図である。この実施形態では、UE110は、既にネットワークに登録しており、接続モードにある。登録後のある時点で、UDM要素312は、UE110内のUE構成パラメータが更新される必要があると判定するために命令を受信するか、またはローカルポリシーを処理し得る。したがって、UDM要素312は、更新手順を開始し、UE構成パラメータ更新をアセンブルする。UDM要素312はまた、UE110のNASセキュリティコンテキストを使用して、UE構成パラメータ更新に完全性保護を適用する。そうするために、UDM要素312は、UE構成パラメータ更新を有する保護要求（たとえば、`Na us f__Pa r a m e t e r P r o t e c t i o n R e q u e s t`）をAUSF要素310に送信する（S1）。AUSF要素310は、NASカウンタを特定し、UE110のNASセキュリティコンテキスト、たとえば、UE構成パラメータ更新のAUSF-MAC及びNASカウンタなどに基づいて完全性保護情報を計算する。AUSF要素310はまた、UE110から期待されるMAC（X-UE-MAC）を計算し得る。次に、AUSF要素310は、完全性保護情報（すなわち、AUSF-MAC、NASカウンタ、及びX-UE-MAC）を有する保護応答（たとえば、`Na us f__Pa r a m e t e r P r o t e c t i o n R e s p o n s e`）をUDM要素312に送信する（S2）。次に、UDM要素312は、UE構成パラメータ更新及び完全性保護情報（すなわち、AUSF-MAC及びNASカウンタ）を含む更新通知（たとえば、`Nu dm__S DM__U p d a t e N o t i f i c a t i o n`）をAMF要素314に送信する（S3）。UDM要素312はまた、UE確認応答インジケータ及び／または再登録インジケータを更新通知に含め得る。

【0113】

AMF要素314は、更新手順の一部として、UE構成パラメータ更新をUE110に透過的に送信するように構成される。したがって、AMF要素314は、DL NASトランスポートメッセージをフォーマットまたは生成し、UE構成パラメータ更新を、完全性情報（たとえば、AUSF-MAC及びNASカウンタ）と共に、DL NASトランスポートメッセージのコンテナに挿入する。AMF要素314はまた、UE確認応答インジケータ及び／または再登録インジケータ（該当する場合）をDL NASトランスポートメッセージのコンテナに挿入し得る。この実施形態では、DL NASトランスポートメッセージのコンテナは、UE構成パラメータ更新用に設計される。次に、AMF要素314は、DL NASトランスポートメッセージをUE110に送信する（S4）。

【0114】

UE110のME702は、DL NASトランスポートメッセージを受信することに応答して、UE構成パラメータ更新がホームネットワークのUDM要素312によって送信されたことを検証するためにセキュリティチェックを実行する。セキュリティチェックが成功しなかった場合、ME702はUE構成パラメータ更新を破棄する。セキュリティチェックが成功した場合、ME702及び／またはUSIM662は、UE構成パラメータ更新に基づいて、UE構成パラメータ664のうちの1つまたは複数を更新する。

【0115】

ネットワークがUE110からの確認応答を要求しており、セキュリティチェックが成功した場合、ME702はUL NASトランスポートメッセージをフォーマットし、U

10

20

30

40

50

E-MACをUL NASTransportメッセージのコンテナに挿入する。UL NASTransportメッセージのコンテナは、UE確認応答に設計される。次に、ME702は、UE-MACを含むコンテナを有するUL NASTransportメッセージをAMF要素314に送信する(S5)。AMF要素314は、UE-MACを有する情報メッセージ(たとえば、Nudm__SDM__Infoメッセージ)をUDM要素312に送信する(S6)。次に、UDM要素312は、UE110によって計算されたUE-MACをAUSF要素310によって計算されたX-UE-MACと比較して、UE確認応答がUE110によって提供されたことを検証し得る。

【0116】

UE110の再登録が必要なことをネットワークが示しており、セキュリティチェックが成功した場合、UE110は登録解除し、更新されたUE構成パラメータを使用して、新しいNAS登録手順を再度開始する(図示せず)。

【0117】

例5:セキュア化パケット及びセキュリティキーを使用した登録中の更新手順

図17は、例示的な実施形態における登録中の更新手順を示すメッセージ図である。この実施形態では、UE110は、NAS登録要求をAMF要素314に送信することによって、NAS登録手順を開始する(S1)。AMF要素314は、(タイプ「新規」の)NAS登録要求に回答して、UE110を認証するための認証手順を開始し得る(S2)。UE110の認証後、AMF要素314は、NASセキュリティコンテキストを確立するためのNASセキュリティ手順を開始し得る(S3)。UE110が認証され、NASセキュリティコンテキストが確立された状態で、AMF要素314は、サブスクリプションデータ要求(たとえば、Nudm__SDM__Getメッセージ)をHPLMNのUDM要素312に送信して、他の情報の中でもとりわけ、UE110のアクセス及びモビリティサブスクリプションデータを取得する(S4)。ユーザサブスクリプション情報が、UE構成パラメータ更新(たとえば、ルーティングID更新)を開始することを示すとき、UDM要素312は、更新手順を開始する。UDM要素312は、1つまたは複数の更新されたUE構成パラメータを含むUE構成パラメータ更新をアセンブルする。次に、UDM要素312は、セキュア化パケットライブラリにアクセスしてUE構成パラメータ更新をセキュア化パケット内にカプセル化することによって、UE構成パラメータ更新にセキュリティ保護を適用する。

【0118】

UDM要素312はまた、UE110のNASセキュリティコンテキストを使用して、セキュア化パケットに完全性保護を適用する。そうするために、UDM要素312は、セキュア化パケットを有する保護要求(たとえば、Nausf__ParameterProtectionRequest)を、AUSF要素310に送信する(S5)。AUSF要素310は、NASカウンタを特定し、UE110のNASセキュリティコンテキスト、たとえば、セキュア化パケットのAUSF-MAC及びNASカウンタなどに基づいて完全性保護情報を計算する。AUSF要素310はまた、UE110から期待されるMAC(X-UE-MAC)を計算し得る。次に、AUSF要素310は、完全性保護情報(すなわち、AUSF-MAC、NASカウンタ、及びX-UE-MAC)を有する保護応答(たとえば、Nausf__ParameterProtectionResponse)をUDM要素312に送信する(S6)。次に、UDM要素312は、セキュア化パケット及び完全性保護情報(すなわち、AUSF-MAC及びNASカウンタ)を含むサブスクリプションデータ応答(たとえば、Nudm__SDM__Get応答)をAMF要素314に送信する(S7)。UDM要素312はまた、UE確認応答インジケータ及び/または再登録要求をサブスクリプションデータ応答に含め得る。

【0119】

AMF要素314は、更新手順の一部として、セキュア化パケットをUE110に透過的に送信するように構成される。したがって、AMF要素314は、NAS登録受諾メッセージをフォーマットまたは生成し、セキュア化パケットをNAS登録受諾メッセージの

10

20

30

40

50

コンテナに挿入する。AMF要素314はまた、UE確認応答インジケータ及び／または再登録要求（該当する場合）を、AUSF-MAC及びNASカウントと共に、NAS登録受諾メッセージのコンテナに挿入し得る。この例では、NAS登録受諾メッセージは、新しく定義されたUE構成パラメータ更新コンテナIEを含む。表9は、UE構成パラメータ更新コンテナIEの一例である。

【0120】

【表9】

表9：

8 7 6 5 4 3 2 1	
UE構成パラメータ更新コンテナIE I	オクテット1
UE構成パラメータ更新コンテナ内容長	オクテット2 オクテット3
UE構成パラメータ更新ヘッダ	オクテット4
AUSF-MAC	オクテット5-20
NASカウント	オクテット21-22
セキュア化パケット [UE構成パラメータ更新]	オクテット23*-2048*

10

【0121】

AMF要素314がセキュア化パケットを修正せずにセキュア化パケットをコンテナに挿入するので、このコンテナは透過的であると考えられる。次に、AMF要素314は、NAS登録受諾メッセージをUE110に送信する（S8）。UE110のME702は、NAS登録受諾メッセージを受信することに対応して、セキュア化パケットがホームネットワークのUDM要素312によって送信されたことを検証するためにセキュリティチェックを実行する。セキュリティチェックが成功しなかった場合、ME702はセキュア化パケットを破棄し、登録手順を続行する。セキュリティチェックが成功した場合、ME702はセキュア化パケットをUSIM662にルーティングまたはアップロードする（S9）。USIM662はまた、セキュア化パケットがホームネットワークのUDM要素312によって送信されたことを検証するためにセキュリティチェックを実行する。セキュリティチェックが成功しなかった場合、USIM662はUE構成パラメータ更新を破棄する。セキュリティチェックが成功した場合、USIM662は、セキュア化パケットライブラリを使用して、セキュア化パケットからUE構成パラメータ更新をアンパックする。次に、USIM662は、UE構成パラメータ更新に基づいて、UE構成パラメータ664のうちの1つまたは複数を更新する。

20

【0122】

ネットワークがUE110からの確認応答を要求しており、セキュリティチェックが成功した場合、ME702はNAS登録完了メッセージをフォーマットし、UE-MACをNAS登録完了メッセージのコンテナに挿入する。次に、ME702は、NAS登録完了メッセージをAMF要素314に送信する（S11）。AMF要素314は、UE-MACを有する情報メッセージ（たとえば、Nudm_SDM_Infoメッセージ）をUDM要素312に送信する（S10）。次に、UDM要素312は、UE110によって計算されたUE-MACをAUSF要素310によって計算されたX-UE-MACと比較して、UE確認応答がUE110によって提供されたことを検証し得る。

30

40

【0123】

UE110の再登録が必要なことをネットワークが示しており、セキュリティチェックが成功した場合、UE110は登録解除し、更新されたUE構成パラメータを使用して、新しいNAS登録手順を再度開始する（図示せず）。

【0124】

例6：セキュア化パケット及びセキュリティキーを使用した登録後の更新手順

図18は、例示的な実施形態における登録後の更新手順を示すメッセージ図である。こ

50

の実施形態では、UE 110は、既にネットワークに登録しており、接続モードにある。登録後のある時点で、UDM要素312は、UE 110内のUE構成パラメータが更新される必要があると判定するために命令を受信するか、またはローカルポリシーを処理し得る。したがって、UDM要素312は、更新手順を開始し、UE構成パラメータ更新をアセンブルする。次に、UDM要素312は、セキュア化パケットライブラリにアクセスしてUE構成パラメータ更新をセキュア化パケット内にカプセル化することによって、UE構成パラメータ更新にセキュリティ保護を適用する。

【0125】

UDM要素312はまた、UE 110のNASセキュリティコンテキストを使用して、セキュア化パケットに完全性保護を適用する。そうするために、UDM要素312は、セキュア化パケットを有する保護要求（たとえば、Nausf__ParameterProtectionRequest）を、AUSF要素310に送信する（S1）。AUSF要素310は、NASカウントを特定し、UE 110のNASセキュリティコンテキスト、たとえば、セキュア化パケットのAUSF-MAC及びNASカウントなどに基づいて完全性保護情報を計算する。AUSF要素310はまた、UE 110から予期されたMAC（X-UE-MAC）を計算し得る。次に、AUSF要素310は、完全性保護情報（すなわち、AUSF-MAC、NASカウント、及びX-UE-MAC）を有する保護応答（たとえば、Nausf__ParameterProtectionResponse）をUDM要素312に送信する（S2）。次に、UDM要素312は、セキュア化パケット及び完全性保護情報（すなわち、AUSF-MAC及びNASカウント）を含む更新通知（たとえば、Nudm__SDM_UpdateNotification）をAMF要素314に送信する（S3）。UDM要素312はまた、UE確認応答インジケータ及び／または再登録要求を更新通知に含め得る。

【0126】

AMF要素314は、更新手順の一部として、セキュア化パケットをUE 110に透過的に送信するように構成される。したがって、AMF要素314は、DL NASトランスポートメッセージをフォーマットまたは生成し、セキュア化パケットをDL NASトランスポートメッセージのコンテナに挿入する。AMF要素314はまた、UE確認応答インジケータ及び／または再登録インジケータ（該当する場合）を、AUSF-MAC及びNASカウントと共に、DL NASトランスポートメッセージのコンテナに挿入し得る。次に、AMF要素314は、DL NASトランスポートメッセージをUE 110に送信する（S4）。

【0127】

UE 110のME 702は、DL NASトランスポートメッセージを受信することに応答して、セキュア化パケットがホームネットワークのUDM要素312によって送信されたことを検証するためにセキュリティチェックを実行する。セキュリティチェックが成功しなかった場合、ME 702はセキュア化パケットを破棄する。セキュリティチェックが成功した場合、ME 702はセキュア化パケットをUSIM 662にルーティングまたはアップロードする（S5）。USIM 662はまた、セキュア化パケットがホームネットワークのUDM要素312によって送信されたことを検証するためにセキュリティチェックを実行する。セキュリティチェックが成功しなかった場合、USIM 662はUE構成パラメータ更新を破棄する。セキュリティチェックが成功した場合、USIM 662は、セキュア化パケットライブラリを使用して、セキュア化パケットからUE構成パラメータ更新をアンパックする。次に、USIM 662は、UE構成パラメータ更新に基づいて、UE構成パラメータ664のうちの1つまたは複数を更新する。USIM 662はまた、UE確認応答をME 702に送信する（S6）。

【0128】

ネットワークがUE 110からの確認応答を要求しており、セキュリティチェックが成功した場合、ME 702はUL NASトランスポートメッセージをフォーマットし、UE-MACをUL NASトランスポートメッセージのコンテナに挿入する。次に、ME

10

20

30

40

50

702は、UL NASトランスポートメッセージをAMF要素314に送信する(S7)。AMF要素314は、UE-MACを有する情報メッセージ(たとえば、Nudm_SDM_Infoメッセージ)をUDM要素312に送信する(S8)。次に、UDM要素312は、UE110によって計算されたUE-MACをAUSF要素310によって計算されたX-UE-MACと比較して、UE確認応答がUE110によって提供されたことを検証し得る。

【0129】

UE110の再登録が必要なことをネットワークが示しており、セキュリティチェックが成功した場合、UE110は登録解除し、更新されたUE構成パラメータを使用して、新しいNAS登録手順を再度開始する(図示せず)。

【0130】

図示または本明細書に記載した様々な要素またはモジュールはいずれも、ハードウェア、ソフトウェア、ファームウェア、またはこれらの何らかの組み合わせとして実装され得る。たとえば、要素は専用ハードウェアとして実装され得る。専用のハードウェア要素は、「プロセッサ」、「コントローラ」、または何らかの類似の用語と呼ばれ得る。機能は、プロセッサによって提供される場合、単一の専用プロセッサ、単一の共有プロセッサ、または一部が共有され得る複数の個別のプロセッサによって提供され得る。さらに、「プロセッサ」または「コントローラ」という用語の明示的な使用は、ソフトウェアを実行可能なハードウェアのみを指すものと解釈されるべきではなく、限定はしないが、デジタルシグナルプロセッサ(DSP)ハードウェア、ネットワークプロセッサ、特定用途向け集積回路(ASIC)もしくはその他の回路、フィールドプログラマブルゲートアレイ(FPGA)、ソフトウェアを記憶するための読み取り専用メモリ(ROM)、ランダムアクセスメモリ(RAM)、不揮発性ストレージ、ロジック、またはその他の何らかの物理ハードウェアコンポーネントもしくはモジュールを暗黙的に含み得る。

【0131】

また、ある要素は、その要素の機能を実行するための、プロセッサまたはコンピュータによって実行可能な命令として実装され得る。命令のいくつかの例は、ソフトウェア、プログラムコード、ファームウェアである。命令は、プロセッサによって実行されたときに、プロセッサに要素の機能を実行するように指示するよう動作可能である。命令は、プロセッサによって読み取り可能な記憶デバイスに記憶され得る。記憶デバイスのいくつかの例は、デジタルもしくはソリッドステートメモリ、磁気記憶媒体、たとえば、磁気ディスク及び磁気テープ、ハードドライブ、または光学的に読み取り可能なデジタルデータ記憶媒体である。

【0132】

「回路」という用語は、本明細書で使用する場合、以下のうちの1つまたは複数あるいは全てを指し得る：

(a) ハードウェアのみの回路の実施態様(たとえば、アナログ及び／またはデジタル回路のみの実施態様)、

(b) ハードウェア回路とソフトウェアとの組み合わせ、たとえば、以下である(適用可能な場合)：

(i) アナログ及び／またはデジタルハードウェア回路(複数可)と、ソフトウェア／ファームウェアとの組み合わせ、

(ii) 携帯電話またはサーバなどの装置に様々な機能を実行させるように協働する、ソフトウェアを使用するハードウェアプロセッサ(複数可)(デジタルシグナルプロセッサ(複数可)を含む)、ソフトウェア、及びメモリ(複数可)の任意の部分、

(c) 動作のためにソフトウェア(たとえば、ファームウェア)を必要とするが、動作に不要な場合はソフトウェアは存在しない場合がある、ハードウェア回路(複数可)及び／またはプロセッサ(複数可)、たとえば、マイクロプロセッサ(複数可)またはマイクロプロセッサ(複数可)の一部。

【0133】

この回路の定義は、任意の請求項を含めて、本出願におけるこの用語の全ての使用に適用される。さらなる例として、回路という用語は、本出願で使用する場合、単なるハードウェア回路またはプロセッサ（もしくは複数のプロセッサ）、あるいはハードウェア回路またはプロセッサの一部、ならびにそれに（またはそれらに）付随するソフトウェア及び／またはファームウェアの一実施態様も包含する。回路という用語はまた、たとえば、特定の請求項の要素に該当する場合、モバイルデバイス用のベースバンド集積回路またはプロセッサ集積回路、あるいはサーバ、セルラーネットワークデバイス、または他のコンピューティングデバイスもしくはネットワークデバイス内の同様の集積回路も包含する。

【 0 1 3 4 】

特定の実施形態を本明細書に記載したが、本開示の範囲はそれらの特定の実施形態に限定されるものではない。本開示の範囲は、以下の特許請求の範囲及びそれらの任意の均等物によって定められる。

10

20

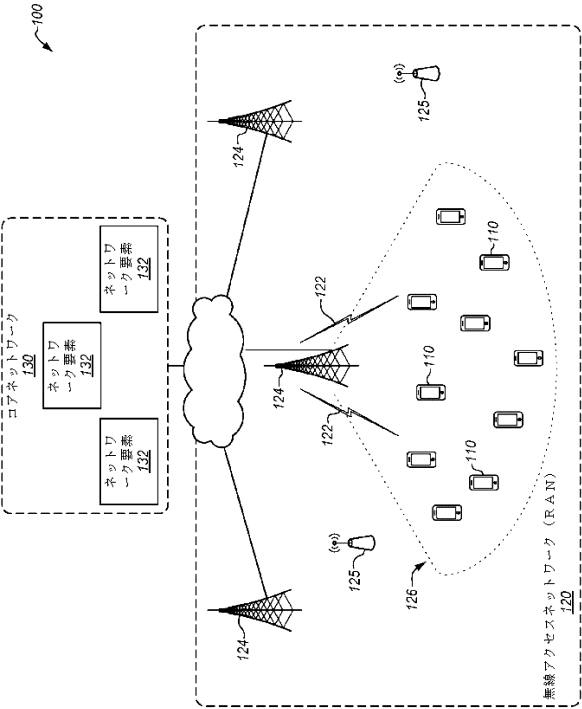
30

40

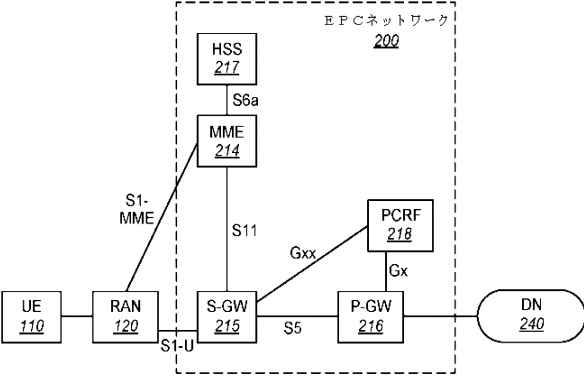
50

【図面】

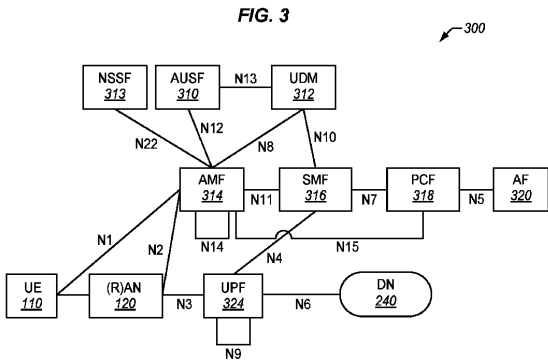
【図 1】



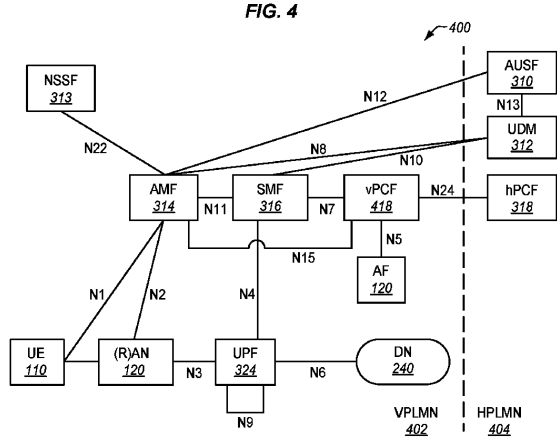
【図 2】



【図 3】



【図 4】



10

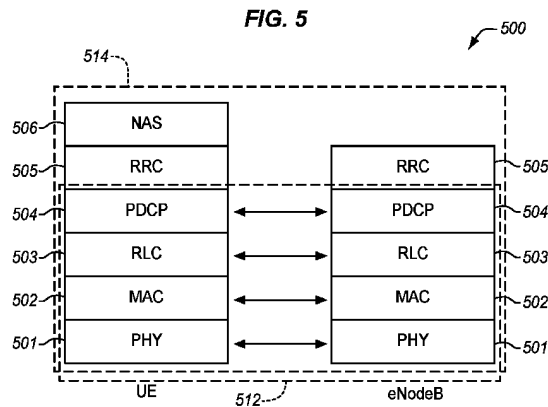
20

30

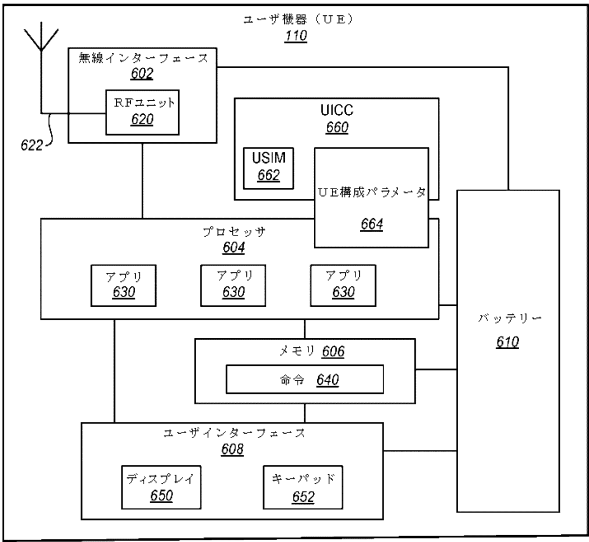
40

50

【図 5】

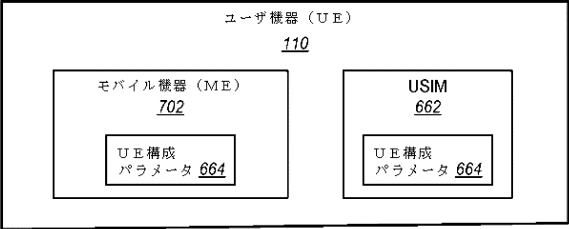


【図 6】

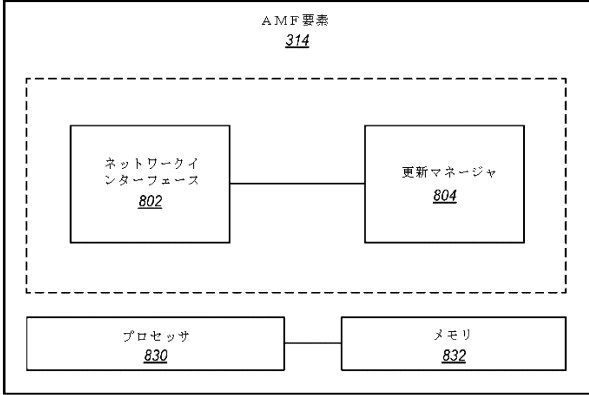


10

【図 7】



【図 8】



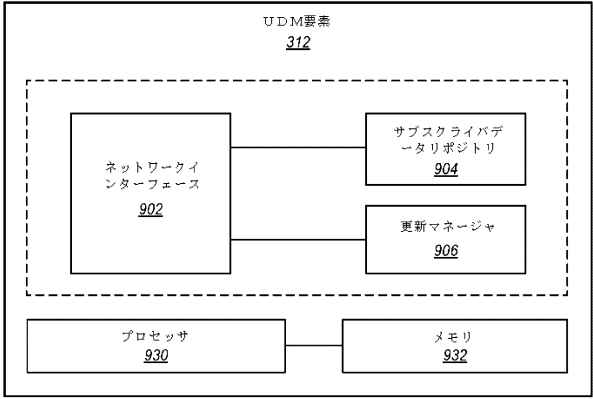
20

30

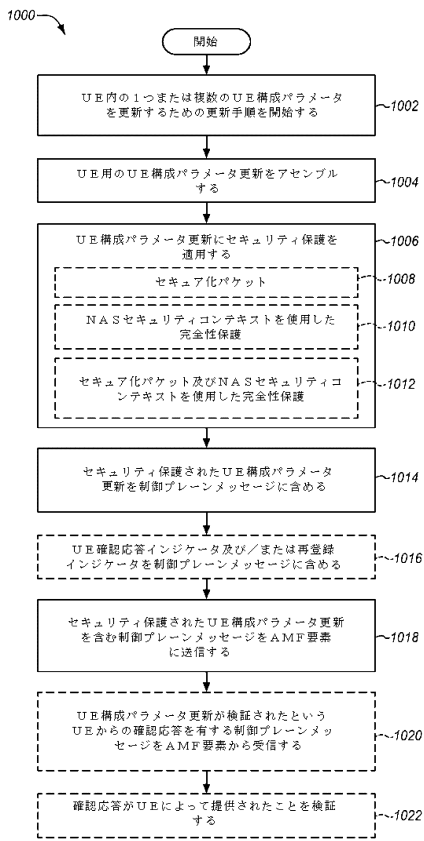
40

50

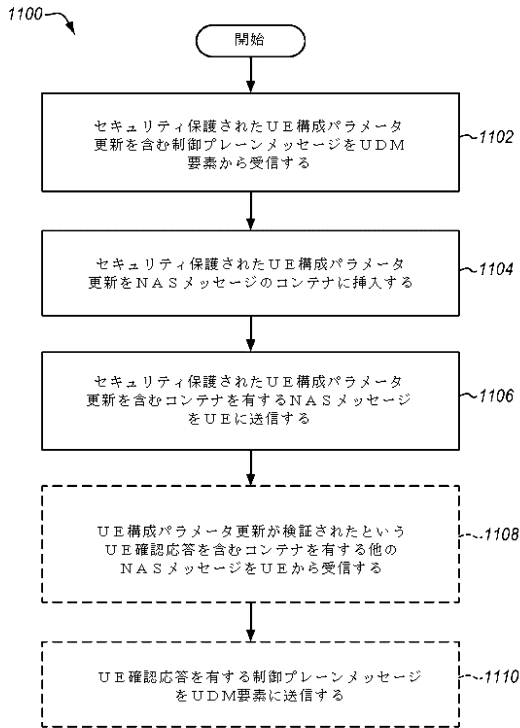
【図 9】



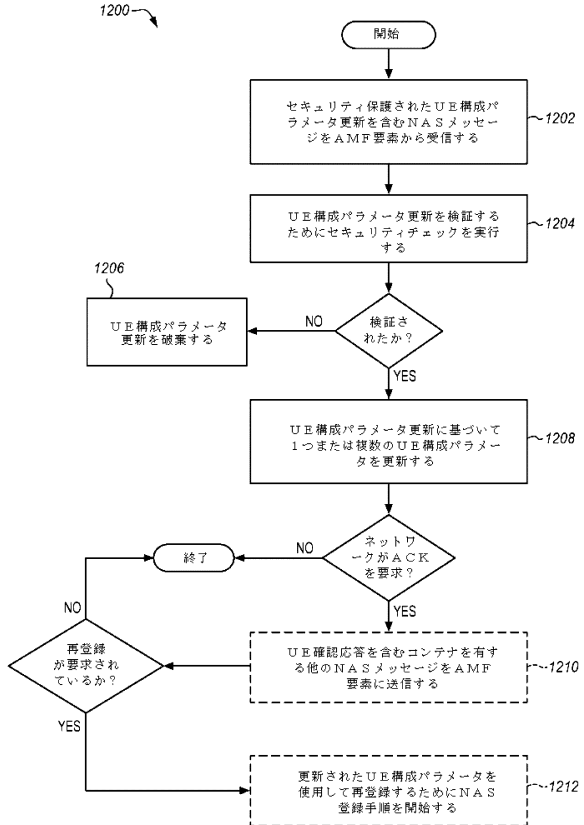
【図 10】



【図 11】



【図 12】



10

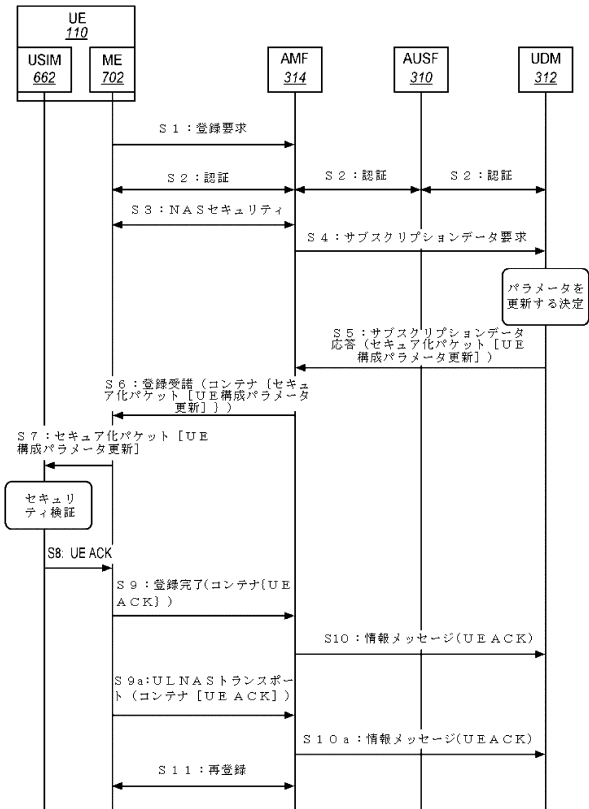
20

30

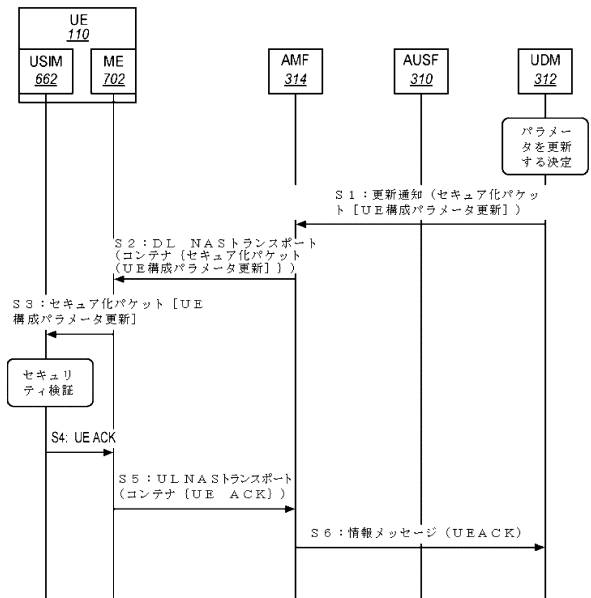
40

50

【図 13】



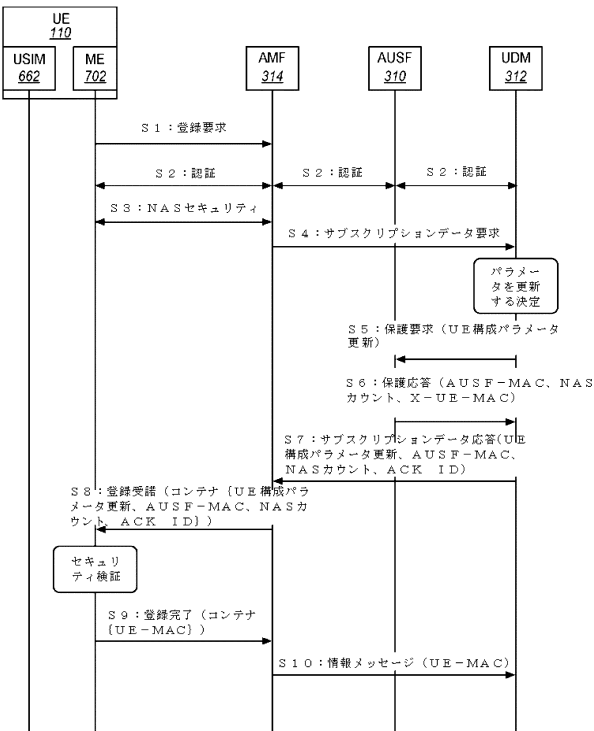
【図 14】



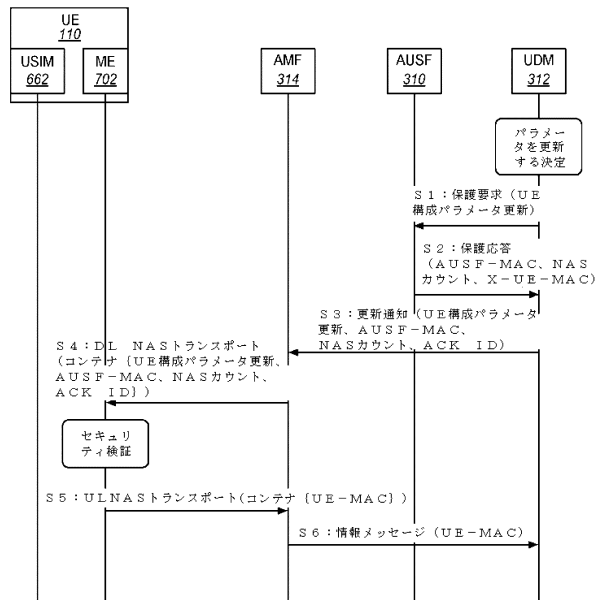
10

20

【図 15】



【図 16】

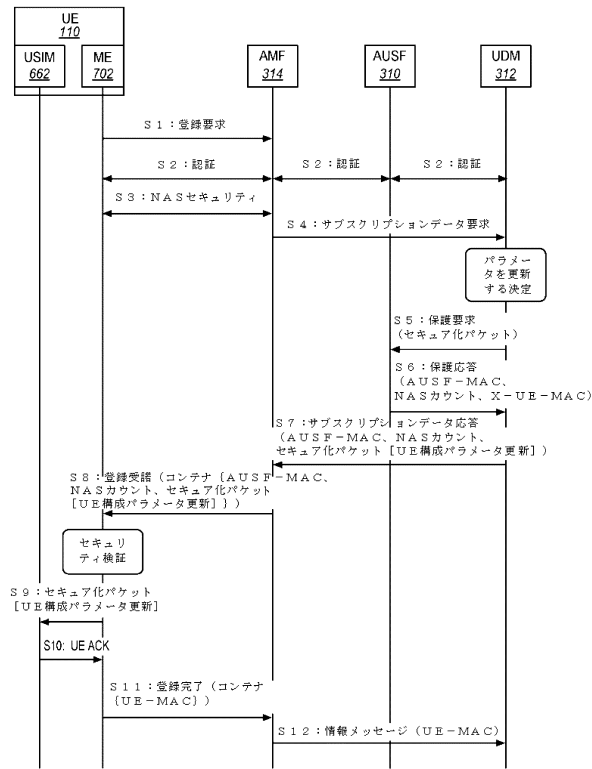


30

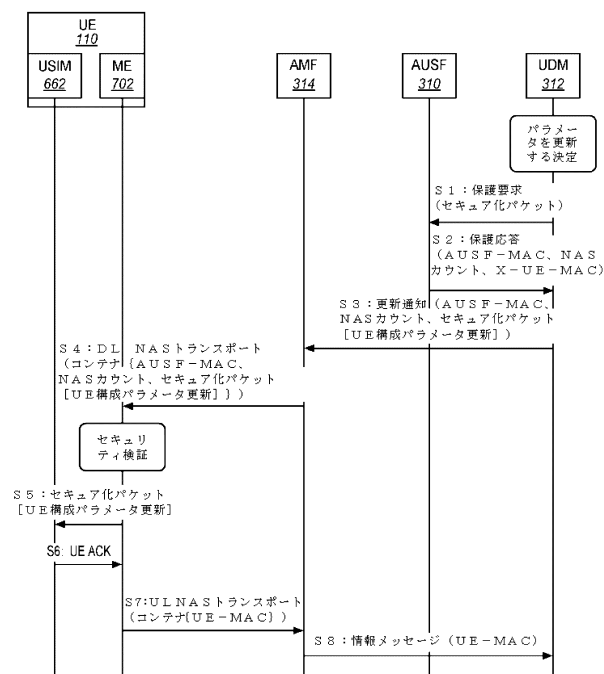
40

50

【図 17】



【図 18】



10

20

30

40

50

フロントページの続き

- 弁理士 上杉 浩
(74)代理人 100120525
弁理士 近藤 直樹
(74)代理人 100139712
弁理士 那須 威夫
(72)発明者 リウ, ジェニファー
アメリカ合衆国, テキサス州 75025, プラーノ, 3104 オーク スプリングス ドライブ
審査官 永田 義仁
(56)参考文献 国際公開第2018/097601 (WO, A1)
Intel, “ SoR Living Doc: Secure Packet Solution for Steering of Roaming ”, 3GPP TSG SA WG3(Security) Meeting #91-Bis S3-181703, [online], 2018年05月14日, インターネット <URL:https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_91Bis_LaJolla/Docs/S3-181703.zip>, [検索日2022年5月16日]
SA3, “ Reply LS on Routing ID ”, 3GPP TSG CT WG1 Meeting #112bis C1-186338, [online], 2018年10月05日, インターネット <URL:https://www.3gpp.org/ftp/tsg_ct/WG1_mm-c-c-sm_ex-CN1/TSGC1_112bis_Vilnius/docs/C1-186338.zip>, [検索日2022年5月16日]
“ 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) inidle mode (Release 15) ”, 3GPP TS 23.122 V15.5.0 (2018-09), [online], 2018年09月19日, p.51-55, インターネット <URL:https://www.3gpp.org/ftp//Specs/archive/23_series/23.122/23122-f50.zip>, [検索日2022年5月16日]
(58)調査した分野 (Int.Cl., DB名)
H04B7/24-7/26
H04W4/00-99/00
3GPP TSG RAN WG1-4
SA WG1-4
CT WG1、4