(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2020-529754
(P2020-529754A)
(43)公表日　令和2年10月8日(2020.10.8)

(51)Int.Cl.		F I			テーマコード（参考）
H04M 15/00	(2006.01)	H04M	15/00	G	5K025
H04M 3/00	(2006.01)	H04M	3/00	D	5K067
H04M 15/34	(2006.01)	H04M	15/34		5K201
H04W 12/06	(2009.01)	H04W	12/06		
H04W 12/04	(2009.01)	H04W	12/04		

審査請求 未請求　予備審査請求 未請求　（全 13 頁）　最終頁に続く

(21)出願番号　特願2019-571008 (P2019-571008)
(86)(22)出願日　平成30年8月3日(2018.8.3)
(85)翻訳文提出日　令和2年1月30日(2020.1.30)
(86)国際出願番号　PCT/EP2018/071160
(87)国際公開番号　WO2019/025603
(87)国際公開日　平成31年2月7日(2019.2.7)
(31)優先権主張番号　17184733.8
(32)優先日　平成29年8月3日(2017.8.3)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)

(71)出願人　518144182
アイピーコム　ゲーエムベーハー　ウント　コー.　カーゲー
ドイツ国、プラッハ　８２０４９　ツーク　シュピッツシュトラーセ　１５
(74)代理人　110000877
龍華国際特許業務法人
(72)発明者　ルフト、アヒム
ドイツ国、プラッハ　８２０４９　ツーク　シュピッツシュトラーセ　１５　アイピーコム　ゲーエムベーハー　ウント　コー.　カーゲー内

最終頁に続く

(54)【発明の名称】サービス検証メッセージを送信するように適合されるＵＥ

(57)【要約】
本発明は、モバイル通信用のユーザ機器デバイス（ＵＥデバイス）によって実行されるトランザクションを認証する方法であって、ＵＥデバイスは、ＵＥデバイスと移動先ネットワークとの間でセキュアコンテキストを確立するべく、ＵＥデバイスと、移動先ネットワークのモバイル管理エンティティとの間で認証および鍵共有手順を実行済みである方法を提供し、本方法は、サービス検証メッセージをＵＥデバイスから移動先ネットワークまで送信する段階であって、サービス検証メッセージは、ＵＥデバイスとホームオペレータのネットワークとの間で共有される完全性保障鍵を使用して、ＵＥデバイスによってデジタル署名されている、段階と、サービス検証メッセージを移動先ネットワークからオペレータのホームネットワークまで転送する段階とを備える。

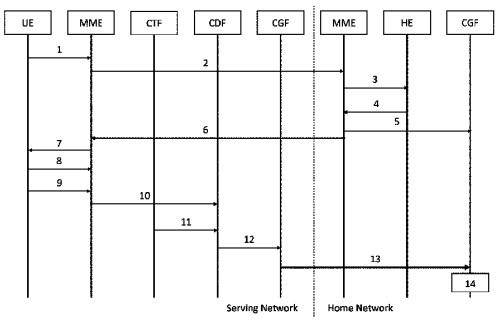


Fig. 3

【特許請求の範囲】
【請求項１】
モバイル通信用のユーザ機器デバイス（ＵＥデバイス）によって実行されるトランザクションを認証する方法であって、前記ＵＥデバイスは、前記ＵＥデバイスと移動先ネットワークとの間でセキュリティコンテキストを確立するべく、前記ＵＥデバイスと、前記移動先ネットワークのモバイル管理エンティティとの間で認証および鍵共有手順を実行済みであり、前記方法は、
サービス検証メッセージを前記ＵＥデバイスから前記移動先ネットワークまで送信する段階であって、前記サービス検証メッセージは、前記ＵＥデバイスとホームネットワークとの間で共有される完全性保障鍵を使用して、前記ＵＥデバイスによってデジタル署名されている、段階と、
前記サービス検証メッセージを前記移動先ネットワークから前記ホームネットワークまで転送する段階と
を備える方法。
【請求項２】
セッション鍵階層のルート、または完全性保障のセッション鍵のいずれも含まない認証ベクトルを前記ホームネットワークが提供する第２の認証および鍵共有手順を実行することによって、前記完全性保障鍵を得る、請求項１に記載の方法。
【請求項３】
チャレンジ、および前記チャレンジに対する期待される応答のみを前記ホームネットワークが前記移動先ネットワークに提供する第２の認証および鍵共有手順を実行することによって、前記完全性保障鍵を得る、請求項１または２に記載の方法。
【請求項４】
前記ホームネットワークにおける既存の鍵から得られる完全性保障鍵を使用して、前記ＵＥデバイスと前記移動先ネットワークとの間で前記セキュリティコンテキストを確立する、請求項１から３のいずれか一項に記載の方法。
【請求項５】
前記サービス検証メッセージがタイムスタンプおよびメッセージシーケンス番号のうち少なくとも１つを含む、請求項１から４のいずれか一項に記載の方法。
【請求項６】
要求に応答して前記サービス検証メッセージが送信される、請求項１から５のいずれか一項に記載の方法。
【請求項７】
前記要求が非アクセス層メッセージの一部として送信される、請求項６に記載の方法。
【請求項８】
前記サービス検証メッセージが前記ＵＥデバイスによって自律的に送信される、請求項１から請求項６のいずれか一項に記載の方法。
【請求項９】
前記サービス検証メッセージが前記移動先ネットワークによって課金データ記録と連結され、連結された前記サービス検証メッセージが前記ホームネットワークの課金ゲートウェイ機能に送信される、請求項１から８のいずれか一項に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、モバイル通信システム内のユーザ機器（ＵＥ）デバイスを介してサービス検証メッセージを送信することに関する。
【背景技術】
【０００２】
ＧＳＭ（登録商標）、ＵＭＴＳおよび進化型パケットコア（ＥＰＣ）ネットワークは、ベアラレベル、サブシステムレベル、およびサービスレベルでオフライン課金機構および

／またはオンライン課金機構を実装する機能を提供する。これらの課金機構をサポートするために、ネットワークは、上記３つのレベルでリアルタイムでのリソースの使用の監視を実行し、関連する課金可能イベントを検出する。

【０００３】

オフライン課金では、リソースの使用は、リソースの使用が生じた後にネットワークから課金ドメイン（ＢＤ）に報告される。オンライン課金では、要求されたネットワークリソースの使用の許可が与えられる前に、オンライン課金システム（ＯＣＳ）に配置される加入者アカウントに照会される。

【０００４】

ネットワークリソースの使用の典型的な例は、一定時間のボイスコール、一定のデータ量の伝送、または、一定のサイズのマルチメディアメッセージの送信である。ネットワークリソースの使用の要求は、ＵＥまたはネットワークを介して開始される場合がある。

【０００５】

オフライン課金は、ネットワークリソースの使用の課金情報がそのネットワークリソースの使用と同時に収集されるプロセスである。次いで、課金情報は一連の課金ロジック機能を通して渡される。本プロセスの最後で、課金データ記録（ＣＤＲ）ファイルがネットワークを介して生成され、次いで課金データ記録は加入者課金および／またはオペレータ間課金用のオペレータのネットワーク課金ドメイン（またはオペレータの自由裁量による追加関数、例えば統計）に転送される。ＢＤは一般的に、オペレータの課金システムまたは課金仲介デバイスなどの後処理モジュールシステムを含む。要するに、オフライン課金は、提供したサービスに課金情報がリアルタイムで影響を与えない機構である。

【０００６】

オンライン課金は、オフライン課金と同じように、ネットワークリソースの使用の課金情報がそのネットワークリソースの使用と同時に収集されるプロセスである。ただし、ネットワークリソースの使用の承認は、実際のリソースの使用が生じる前にネットワークを介して得られる必要がある。このネットワークリソースの使用の承認は、ネットワークから要求されたらすぐにＯＣＳによって与えられる。

【０００７】

ネットワークがネットワークリソースの使用の要求を受信すると、ネットワークは関連する課金情報を収集し、課金イベントをＯＣＳにリアルタイムで生成する。次いでＯＣＳは、リソースの適切な使用の承認を送り返す。リソースの使用の承認はその承認範囲（例えば、データ量または時間）が限定される場合があるため、ユーザがネットワークリソースの使用を持続する限り、リソースの使用の承認は随時更新しなければならない場合がある。

【０００８】

オンライン課金は、提供したサービスに課金情報がリアルタイムで影響を与える可能性があるため、課金機構をネットワークリソースの使用の制御と直接的に相互作用させることが必要となる機構である。

【０００９】

課金トリガ機能（ＣＴＦ）は、ネットワークリソースの使用を監視することによって課金イベントを生成する。課金データ機能（ＣＤＦ）は、いわゆるＲｆ基準点を介してＣＴＦから課金イベントを受信する。次いでＣＤＦは、課金イベントに含まれる情報を使用して課金データ記録（ＣＤＲ）を構築する。ＣＤＦによって作り出されたＣＤＲは、いわゆるＧａ基準点を介して直ちに課金ゲートウェイ機能（ＣＧＦ）に転送される。ＣＧＦは、３ＧＰＰネットワークとＢＤ間のゲートウェイの機能を果たす。ＣＧＦは、ＣＤＲファイルをＢＤに転送するのにいわゆるＢｘ基準点を使用する。ＯＣＦは、２つの異なるモジュール、すなわちセッションベース課金機能（ＳＢＣＦ）およびイベントベース課金機能（ＥＢＣＦ）から構成される。

【００１０】

ＳＢＣＦは、ネットワークのオンライン課金／ユーザセッション、例えば、ボイスコー

ル、ＩＰ　ＣＡＮベアラ、ＩＰ　ＣＡＮセッションまたはＩＭＳセッションを担う。

【００１１】

ＥＢＣＦは、ＳＩＰアプリケーションサーバを含む、任意のアプリケーションサーバまたはサービスＮＥと共にイベントベースオンライン課金を実行する。

【００１２】

レーティング機能（ＲＦ）は、ＯＣＦの代わりとなるネットワークリソースの使用値（ＯＣＦがネットワークから受信する課金イベント内に記載される）を決定する。

【００１３】

オフライン課金システム（ＯＦＣＳ）は、オフライン課金に使用される課金機能のグループ化である。ＯＦＣＳは、１または複数のＣＴＦから課金イベントを収集および処理し、続いて起こる下流のオフライン課金プロセスのＣＤＲを生成する。

【００１４】

加入者がローミングしている場合および移動先ネットワークによってサービスを提供される場合、（移動先ネットワークおよびホームネットワーク内の）両方の課金システムが別々に加入者に課金することになる。ローミング課金は一般的に、ボイスコール１分あたり（ボイスコールを発信した携帯電話と、終了した携帯電話とで課金が異なる）、ＳＭＳあたり、およびメガバイトデータ量あたりである。課金の理由により、両方のネットワークは、課金情報交換手続き（ＴＡＰ）を介して通信を行う。ＴＡＰの転送機構は、モバイルネットワーク拡張ロジック用カスタム化アプリケーション（ＣＡＭＥＬ）と呼ばれる機構である。

【００１５】

ホームネットワーク経由でルーティングされ、移動先ネットワークが提供する全てのサービス、例えば、ボイスコール、ＳＭＳ、ＩＭＳの場合、ホームネットワークのオペレータはＴＡＰを介してサービングネットワークから転送される全ての課金を検証することができる。ローカルブレイクアウトによるインターネットアクセス、または局所的にルーティングされるボイスオーバーＩＰ（ＶｏＩＰ）コールなど、ホームネットワーク経由では現時点でルーティングされない幾つかのサービスがすでに存在する。こうした局所的に提供されるサービスが、より一般的になる傾向にある。ホームオペレータは、局所的にルーティングされるサービス用のＴＡＰを介してサービングネットワークから転送される課金を検証する機構がない。現在、オペレータは、ローミング加入者に実際に提供される課金をサービングネットワークが送信するそうした局所的にルーティングされるサービスを互いに信頼しなければならない。ホームオペレータがローミング課金の検証を可能にする機構が必要である。

【００１６】

ＵＳ２００２／０１６１７２３Ａ１では、ＵＥの中に記憶される鍵および認証センターを使用して、従来のやり方でＵＥのアイデンティティを検証する技術を記載する。ＵＥがホームネットワークとは異なるローカルネットワークに接続される場合、ホームネットワークのオペレータおよびＵＥが共有する共有秘密鍵を使用して、ローカルネットワークのオペレータがＵＥを検証する。ＵＥのユーザがＵＥを使用して買い物をし、支払いを承認したい場合、異なる通信ネットワークを利用してメッセージが売り手と交換され、ＵＥが売り手からのメッセージに署名してトランザクションの了承の旨が知らされる。次いで、署名認証ネットワークサービスを使用して署名の確認が行われる。署名確認サービスは、ホームネットワークやローカルネットワークなどと区別される。上記のように、ＵＥおよび署名確認サービスには両方とも署名鍵が提供される。

【００１７】

ＷＯ２００５／００４４５６では、移動先ネットワークを使用してユーザのＵＥに課金する機構を記載しており、その機構では、ホームネットワークが、ＵＥに送信される課金証明書を発行することによってＵＥが課金証明書を移動先ネットワークのサービスプロバイダに提供することが可能となる。

【００１８】

本発明は、モバイル通信用のユーザ機器デバイス（ＵＥデバイス）によって実行されるトランザクションを認証する方法であって、ＵＥデバイスは、ＵＥデバイスと移動先ネットワークとの間でセキュリティコンテキストを確立するべく、ＵＥデバイスと、移動先ネットワークのモバイル管理エンティティとの間で認証および鍵共有手順を実行済みである方法を提供し、本方法は、サービス検証メッセージをＵＥデバイスから移動先ネットワークまで送信する段階であって、サービス検証メッセージは、ＵＥデバイスとホームネットワークとの間で共有される完全性保障鍵を使用して、ＵＥデバイスによってデジタル署名されている、段階と、サービス検証メッセージを移動先ネットワークからホームネットワークまで転送する段階とを備える。

【００１９】

本発明は、ＴＡＰを介して転送されるローミング課金に対してかなりの支配権をホームオペレータに与える機構を提供する。ユーザの同意は本機構の一部になり得る。本機構の一態様は、ＵＥとホームオペレータ間で共有秘密鍵を確立し、この共有秘密鍵を使用して完全性保障サービス検証メッセージを生成することである。共有秘密鍵はさらに、完全性保障サービス検証メッセージ（すなわち、例えば好ましい移動先ネットワークまたは許容移動先ネットワークが掲載されたリスト）をオペレータのホームネットワークからＵＥまで送信するのに使用することができる。これらの完全性保障サービス検証メッセージをＵＥからホームオペレータにどのように転送するかに関して幾つかの代替形態を提供する。最も有益な選択肢は移動先ネットワークにおけるＣＴＦを強化することである。その結果、ローミングＵＥ内で生成される完全性保障サービス検証メッセージがサービングネットワーク内の生成されたＣＤＲに追加され、ＴＡＰの課金メッセージでホームオペレータに転送される。ＵＥとホームネットワークとの間にあり、移動先ネットワークに知られていない秘密鍵を共有するのに幾つかの代替形態がさらに存在する。選択肢の１つは、認証および鍵共有機能（ＡＫＡ）を２回実行することであるが、２回目の実行では移動先ネットワークと完全性保障鍵を共有しない。本方法の利点は、既存のＳＩＭカードに与える影響は全くないという点である。将来の段階である５Ｇ標準化の段階において、ホームネットワークから移動先ネットワークまでの全てのセッション鍵を得るのに鍵導出機能（ＫＤＦ）を使用することが可能となる、すなわち、移動先ネットワークは、ホームネットワークの鍵を受信するのではなく、ホームネットワークの鍵から得られる移動先ネットワーク専用の鍵を受信する。この場合、現時点で移動先ネットワークに知られていないホームネットワークの完全性保障鍵を使用することができる。

【００２０】

本発明の特定の態様は、ローミング課金に対する支配権をオペレータに与える、および／またはより信頼できるローミング課金ビジネスの共有を確立することができる。本発明の実装は、信用ではなく技術的手段に基づくことができ、本発明により、ユーザはローミング課金に関連する詐欺を回避することが可能となる。

【００２１】

添付図面を参照しながら例示としてのみ本発明の好ましい実施形態をここで記載する。

【図面の簡単な説明】

【００２２】

【図１】ホーム環境から認証ベクトルを要求するモバイル管理エンティティの概略図である。

【図２】認証および鍵共有手順の概略図である。

【図３】本発明の一実施形態を示すメッセージフローチャートである。

【発明を実施するための形態】

【００２３】

第１の実施形態では、２つの異なる完全性鍵を生成するべく、セッション鍵が生成される「認証および鍵共有」（ＡＫＡ）と呼ばれる周知の最初のチャレンジ応答機構が２回実行される。従来のＬＴＥローミングシナリオでは、ＡＫＡが、ＵＥとサービングネットワークのモビリティ管理エンティティ（ＭＭＥ）との間で１回実行される。ＭＭＥはホーム

オペレータから認証ベクトルを要求し、認証ベクトルは、チャレンジと、ルートセッション鍵K_{ASME}と、チャレンジに対する期待される応答とを含む。ＭＭＥはチャレンジをＵＥに送信し、ＵＥは、このチャレンジへの応答および対応するルートセッション鍵を計算する。ＵＥは、当該応答をＭＭＥに返信する。ＭＭＥは、期待される応答を用いてこの応答を検証する。生成されたセッション鍵は、ＵＥおよびＭＭＥ内の識別子KSI_{ASME}と共に記憶され、ＵＥにセキュリティコンテキストを確立するのに使用される。ＡＫＡ手順は、３ＧＰＰ　ＴＳ３３．４０１　ｖ１５．０．０で説明される。

【００２４】

この実施形態では、ＡＫＡ手順を２回実行する。１回目の実行は上記で説明したとおりである。２回目の実行では、チャレンジおよび期待される応答のみをホームネットワークからサービングネットワークに転送する、すなわち、セッションルート鍵$K_{ASME}2$がホームネットワーク内に保持され、サービング（移動先）ネットワークには付与されない。サービングネットワークとＵＥとの間のセキュリティコンテキスト用のセッション鍵階層のルートは、$K_{ASME}1$であり、サービス確認メッセージ用の完全性保障鍵は、$K_{ASME}2$から得られる。サービングネットワークは$K_{ASME}2$の知識がないため、ＵＥおよびホームオペレータだけが互いに共有する完全性保障鍵で署名される完全性保障サービス検証メッセージは、サービングネットワークによって生成されるのではなく、ＵＥによってのみ生成することができる。サービングネットワークがサービス検証メッセージの中身を変える場合、ホームネットワーク内の完全性の確認は失敗することになる。

【００２５】

図１は、ホームオペレータのネットワークのホーム環境（ＨＥ）において、加入者データベースから１または複数の認証ベクトルを要求するＭＭＥを示す。ＡＫＡ手順が図２で示される（従来技術）。

【００２６】

その後の標準化リリースにおいて、ホームネットワークにおいて知られている現在のセッション鍵は、ホームオペレータからサービングネットワークに転送されないことがあり得る。したがって、第２の実施形態では、ホームオペレータのセッション鍵はホームオペレータのみに存在し、一方サービングネットワーク内で使用されるセッション鍵は、代わりにホームネットワークおよびＵＥにおける既存鍵から得られることになる。このケースでは、第２のＡＫＡ実行の上記手順は時代遅れである。なぜなら、ＵＥおよびホームオペレータはホームオペレータのセッション鍵によってその通信の完全性を保障できるからである。

【００２７】

ホームネットワークが要求している場合において、サービス検証メッセージがＵＥおよびサービングネットワークによってのみ実行されるオプション機能であるならば、ホームオペレータのネットワークからサービングネットワークに要求をシグナリングすることが必要となる。ＨＥからの認証要求に応答して情報をサービングネットワーク内のＭＭＥに加えることは有益である。第３の実施形態では、ホームオペレータのネットワークが１または複数の専用メッセージ内のサービス検証メッセージをサービングネットワークに要求する。第４の実施形態では、ＨＥは、要求だけではなく１つの認証ベクトルを用いて暗黙に応答することによって、サービングネットワークからサービス認証メッセージを要求する。

【００２８】

さらに、ＵＥは、サービス検証メッセージを生成する要求を受信する。この要求は、認証プロセスにおいてホームオペレータのネットワークまたはサービングネットワークから追加情報として、例えば、非アクセス層（ＮＡＳ）セキュリティモードコマンドメッセージで送信することができる。別の実施形態では、サービス検証メッセージは、サービングネットワークによって１または複数の専用メッセージでＵＥに要求される。一実施形態では、サービングネットワークは、接続手続き時、例えば認証プロセス時またはセキュリティコンテキストセットアップ時にサービス検証メッセージを要求する。別の実施形態では

、サービングネットワークは、ベアラセットアップ手続き時にベアラ単位に基づいてサービス検証メッセージを要求する。サービングネットワークが、ＵＥ内にサービス検証メッセージを生成するために対応する周期性を要求することは有益である。別の実施形態では、ＵＥは、ホームオペレータのネットワークが提供する記憶されたポリシー情報に基づいて周期性を決める。

【００２９】

サービス検証メッセージが要求されるか否か、およびＵＥがサービス検証メッセージを生成するように要求される周期性は、ホームオペレータの自由裁量による。それは、加入者ポリシーに基づくか、またはアクセスクラスポリシーに基づくか、またはＵＥの能力に基づいてよい。一実施形態では、サービス検証メッセージポリシーは、ホームオペレータのネットワークのＨＥ内に記憶される。別の実施形態では、サービス検証メッセージポリシーは、ポリシーコントロールおよび課金機能（ＰＣＣＦ）の一部である。

【００３０】

移動先ネットワークを介してＵＥからホームネットワークに送信されるサービス検証メッセージは、リプレーアタックから保護される必要がある。これは、タイムスタンプまたはメッセージシーケンス番号、またはこの両方を用いて実行することができる。第１のサービス検証メッセージは事前検証であり得る、すなわち、第１のサービス検証メッセージは、重要なサービス提供を検証することなく、サービスのセットアップ、またはセットアップの構成の受信を検証する。この第１のサービス検証メッセージは、例えば１分後、または１００キロバイトのローミングデータトラフィックで、または通話の終わりなど、第２の検証メッセージを予想できる場合に、タイムスタンプまたはメッセージシーケンス番号１を含む必要がある。第２のサービス検証メッセージ以降、（各サービスの）メッセージは、ボイスコールの直前の１分間のボイスコールの品質、または最後の１００キロバイトのローミングデータトラフィックのデータレートなど、直前のサービス期間に関する追加のフィードバック情報を含むことができる。

【００３１】

以下は、こうしたサービス検証メッセージの一例である。

【表１】

ID	Ver	SEQ	TS	P	SID	FB	MAC

ＩＤ：加入者ＩＤ、例えばＧＵＴＩ（グローバル一意一時ＩＤ）
Ｖｅｒ：プロトコルバージョン情報
ＳＥＱ：メッセージシーケンス番号、例えば１６ビット
ＴＳ：タイムスタンプ
Ｐ：このサービスのサービス検証メッセージの予想される周期性
ＳＩＤ：サービス識別子（例えば、ローカルブレイクアウトによるデータサービス、ボイスコール、ベアラまたはＰＤＵセッションＩＤ）
ＦＢ：現在のサービスのフィードバック情報
ＭＡＣ：共有セッション鍵による完全性保障としてのメッセージ認証コード

【００３２】

例示的なメッセージフローチャートが図３で示される。ユーザが外国で自分のＵＥを作動する。段階１で、ＵＥは、登録手続き中に、ホームオペレータがローミング契約を結ぶサービングネットワークを見つける。ホームオペレータが制御する許容ネットワークのリストがＳＩＭ内に記憶される。段階２で、サービングネットワークが、ローミングユーザのホームオペレータから認証ベクトルを要求する。段階３で、サービングネットワークのモビリティ管理エンティティ（ＭＭＥ）が、ホームネットワークのホーム環境（ＨＥ）から１または複数の認証ベクトル（ＡＶ）を要求する。段階４で、ＨＥが、要求された認証ベクトルおよび１つの追加認証ベクトルを用いて応答する。段階５で、ホームネットワークのＭＭＥが、追加認証ベクトルから得られる完全性保障セッション鍵を課金ゲートウェイ機能に転送する。段階６で、サービングネットワークが２つの認証ベクトル（ＡＶ）を

受信する。従来技術で知られるように１つ目の認証ベクトルは完全であり、本発明による２つ目のＡＶには、セッション鍵階層のルート（少なくとも完全性保障のセッション鍵）は含まれない。追加認証ベクトルの受信によって、サービス検証メッセージがオペレータのホームネットワークから要求されたことがサービングネットワークに暗黙にシグナリングされ得る。この要求はさらに、３ＧＰＰのＴＳ３３．４０１ に従って、ＭＭＥとＨＥとの間のメッセージ内のＮＡＳサービス検証要求で明示的にされ得る。従来技術における、ＴＳ３３．４０１ に準拠した認証手順の一部として実行されるＡＫＡはこの図では示されない。次いで段階７で、サービングネットワークは、第２のＡＫＡ（または潜在的な後継であるＡＫＡ＊）手順を実行し、ここでサービングネットワークは、実行されるこの追加のＡＫＡの完全性保障セッション鍵がサービス検証メッセージに署名するのに使用されること、およびこれらのサービス検証メッセージが要求されることをＮＡＳセキュリティモードコマンドメッセージでＵＥにシグナリングする。段階８で、ＵＥは、ＮＡＳセキュリティモード完全メッセージでサービングネットワークへの要求を確認する。サービス検証メッセージのＭＡＣフィールドを生成するべく、実行される第２のＡＫＡによって生じる完全性保障鍵がＵＥ内に記憶される。

【００３３】

ユーザはここで、局所的にルーティングされるボイスコールを開始する。したがって、第１のサービス検証メッセージがＵＥ内に生成され、段階９で、ＮＡＳサービス検証メッセージがサービングネットワークのサービングモビリティ管理エンティティ（ＭＭＥ）に送信される。第１のサービス検証メッセージは、ユーザのＧＵＴＩと、メッセージシーケンス番号「１」と、現在のタイムスタンプと、１分間の予想される周期性と、サービス識別子としての「ローカルボイスコール」と、空のフィードバック情報フィールドと、メッセージの第１の７つのフィールドの有効なメッセージ認証コードと、を含む。

【００３４】

段階１０で、サービングネットワークのＭＭＥは、サービス検証メッセージを課金データ機能（ＣＤＦ）に転送する。段階１１で、ＣＤＦはさらに、課金トリガ機能（ＣＴＦ）から課金イベントメッセージを受信し、ＣＤＲを生成し、本発明に従ってサービス検証メッセージをＣＤＲに連結する。サービス検証メッセージはＵＥによって自律的に生成されるため、ホームネットワークまたは移動先ネットワークによって構成される、またはそれらのネットワークから影響を受ける。サービス検証メッセージをＣＤＲと同期することで、結果、対応するサービス検証メッセージが各ＣＤＲと連結されることは有益である。しかし、同期的でない解決策も同様に可能であろう。この場合、単一のＣＤＲは、ＣＤＲ内のメッセージの可用性に応じて、０、１または複数のサービス検証メッセージを含んでもよい。１つより多くのサービス検証メッセージが単一のＣＤＲの中に含まれる場合、サービス検証メッセージを含まなかった前のＣＤＲを検証することができる。

【００３５】

段階１２で、ＣＤＦによって作り出された（サービス検証メッセージが連結される）ＣＤＲが、Ｇａ基準点を介して直ちに課金ゲートウェイ機能（ＣＧＦ）に転送される。段階１３で、ＣＧＦは、サービス検証メッセージが含まれているＴＡＰ課金メッセージを生成し、ＴＡＰ課金メッセージは、ＣＡＭＥＬインタフェースを介して、ＳＳ７で、ホームオペレータのＣＧＦに転送される。段階１４で、ホームオペレータのＣＧＦは、課金手続きに進む前に、要求されたサービス検証メッセージを検証する。

【００３６】

上記の代替形態は、トリガに基づいて移動先ネットワークからサービス検証メッセージを生成することである。ＣＤＦ、または移動先ネットワークの課金システムのその他あらゆるエンティティは、新しいＮＡＳメッセージで、または周知のＮＡＳメッセージ内の新しい情報でＵＥをトリガし、ＴＡＰのあらゆる課金メッセージが課金サービスを検証する１つのサービス検証メッセージを含むことが確実になるように、サービス検証メッセージを生成することができる。この代替形態では、ＵＥはサービス検証メッセージの生成時間を制御しないので、このサービス検証メッセージは予想される次のサービス検証メッセー

ジに関するあらゆる情報を含まない場合がある、すなわち、周期性情報がない。

【００３７】

移動先（ローミング）ネットワークによるサービスのセットアップまたはサービスの提供を検証するためにＵＥ内でサービス検証メッセージを生成することができる。サービス検証メッセージは、移動先ネットワークによるサービスのセットアップまたはサービスの提供に関するサービス情報、およびホームネットワークへのサービス情報を検証する署名を含むことができる。

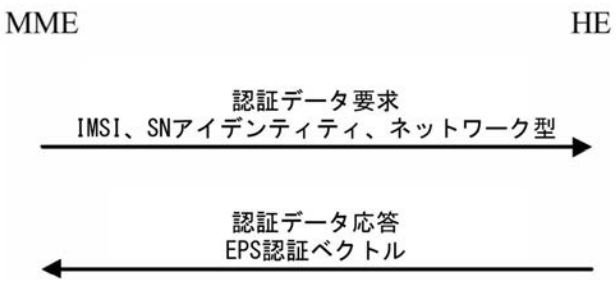
【００３８】

本発明は、一態様において、課金されるサービスのセットアップまたはサービスの提供に関する移動先からホームネットワークまでの課金情報（ＣＤＲ）に関して、サービス検証メッセージをホームネットワークに送信するために移動先ネットワークに送信する。

【００３９】

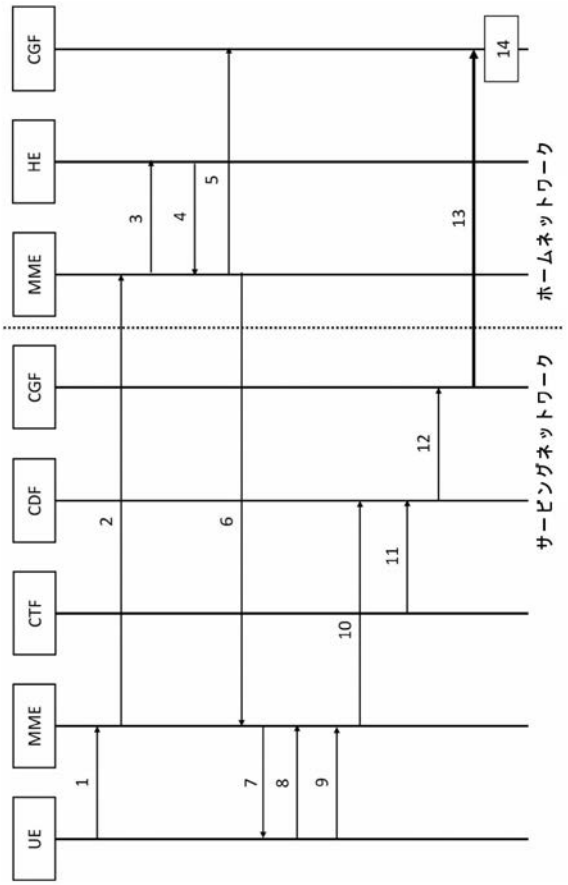
つまり、本発明は、課金されるサービスのセットアップまたはサービスの提供に関する移動先からホームネットワークまでの課金情報（課金データ記録（ＣＤＲ））に関して、移動先ネットワークを介してサービス検証メッセージをホームネットワークに送信する。サービス検証メッセージは、ＵＥとホームオペレータとの間で共有される完全性保障鍵と、タイムスタンプまたはメッセージシーケンス番号、もしくはその両方を用いたリプレー保護と、第１の事前のサービス検証メッセージと、第１のメッセージまたは全てのメッセージの中のその後に続くメッセージの予想される周期性と、最後のサービス時間のフィードバックと、サービス、例えば、データトラフィックおよびボイスコールサービス毎のサービス検証メッセージと、移動先ネットワークによってトリガされる、すなわち、移動先ネットワークからオンデマンドで生成されるサービス検証メッセージと、を含むことができる。ＵＥとホームオペレータとの間で共有される完全性保障鍵は、実行される２回目のＡＫＡを介して生成される、または、サービングネットワークの専用セッション鍵を得ることによって獲得される。

【図１】



【図２】

【図３】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2018/071160

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04M15/00 H04W12/04 H04W12/06 H04W12/10
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)
H04M 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 2002/161723 A1 (ASOKAN NADARAJAH [FI] ET AL) 31 October 2002 (2002-10-31) cited in the application	1,5-9
Y	figures 1,2,6,7,8,9 paragraph [0008] - paragraph [0011] paragraph [0028] - paragraph [0032] paragraph [0036] - paragraph [0037] paragraph [0043] paragraph [0050] - paragraph [0052] paragraph [0055] - paragraph [0059] ----- -/--	2-4

[X] Further documents are listed in the continuation of Box C.

[X] 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
23 August 2018	03/09/2018

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	Veshi, Erzim

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2018/071160

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Release 15)", 3GPP DRAFT; 33401-F00, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , no. ;20170601 12 June 2017 (2017-06-12), XP051310313, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_87_Ljubljana/SA/33401-f00.doc [retrieved on 2017-06-12] cited in the application	2-4
A	figures 6.1.1-1, 6.1.2-1, 6.2-1 paragraph [6.1.1] - paragraph [6.1.5] paragraph [7.2.1] - paragraph [7.2.4] paragraph [0A.2]	1,5-9
A	EP 2 509 352 A2 (APPLE INC [US]) 10 October 2012 (2012-10-10) paragraph [0044] - paragraph [0046]; figure 1	2,3
A	WO 2005/004456 A1 (ERICSSON TELEFON AB L M [SE]; AHLBAECK HANS [FI]; HAKALA HARRI TAPANI) 13 January 2005 (2005-01-13) cited in the application figure 2 page 2, line 9 - page 3, line 25 page 8, line 1 - page 8, line 21	1-9

1

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2018/071160

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002161723 A1	31-10-2002	AU 2003230056 A1	11-11-2003
		CN 1666211 A	07-09-2005
		EP 1509863 A2	02-03-2005
		EP 2369545 A1	28-09-2011
		JP 4518942 B2	04-08-2010
		JP 2005525733 A	25-08-2005
		KR 20040102228 A	03-12-2004
		US 2002161723 A1	31-10-2002
		WO 03096140 A2	20-11-2003
EP 2509352 A2	10-10-2012	AU 2012201945 A1	25-10-2012
		BR 102012007970 A2	07-01-2014
		EP 2509352 A2	10-10-2012
		EP 2827629 A1	21-01-2015
		JP 2012231466 A	22-11-2012
		JP 2014158300 A	28-08-2014
		KR 20120113690 A	15-10-2012
		KR 20140107168 A	04-09-2014
		TW 201251482 A	16-12-2012
		US 2012260090 A1	11-10-2012
		US 2015326568 A1	12-11-2015
		US 2016218874 A1	28-07-2016
		WO 2012138778 A2	11-10-2012
WO 2005004456 A1	13-01-2005	AU 2003271743 A1	21-01-2005
		CN 1792085 A	21-06-2006
		EP 1639800 A1	29-03-2006
		JP 4335874 B2	30-09-2009
		JP 2006527930 A	07-12-2006
		US 2007219870 A1	20-09-2007
		WO 2005004456 A1	13-01-2005

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）
H04W	***4/24***	***(2009.01)***	H04W	4/24		
H04L	***9/32***	***(2006.01)***	H04L	9/00	675A	
G09C	***1/00***	***(2006.01)***	G09C	1/00	640E	
H04W	*36/14*	*(2009.01)*	H04W	36/14		

(81)指定国・地域　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,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JO,JP,KE,KG,KH,KN,KP,KR,KW,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

(72)発明者　ハンス、マーティン
ドイツ国、プラッハ　８２０４９　ツークシュピッツシュトラーセ　１５　アイピーコム　ゲーエムベーハー　ウント　コー.　カーゲー内

Ｆターム(参考) 5K025 BB07 CC04 EE18 EE22 FF17 HH01 HH17
5K067 AA29 DD11 EE04 JJ71
5K201 AA09 BB04 CB19 CC01 EA07 EC01 ED04 FA07