(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2010-539786
(P2010-539786A)
(43)公表日　平成22年12月16日(2010.12.16)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601A	5J104
H04W 12/08	(2009.01)	H04Q	7/00	184	5K067
H04M 11/00	(2006.01)	H04L	9/00	601E	5K201
		H04M	11/00	303	

審査請求 未請求　予備審査請求 未請求　（全 18 頁）

(21)出願番号　特願2010-524820 (P2010-524820)
(86)(22)出願日　平成20年5月20日 (2008.5.20)
(85)翻訳文提出日　平成22年3月19日 (2010.3.19)
(86)国際出願番号　PCT/SE2008/050591
(87)国際公開番号　WO2009/038522
(87)国際公開日　平成21年3月26日 (2009.3.26)
(31)優先権主張番号　60/972,955
(32)優先日　平成19年9月17日 (2007.9.17)
(33)優先権主張国　米国 (US)

(71)出願人　598036300
テレフオンアクチーボラゲット　エル　エム　エリクソン（パブル）
スウェーデン国　ストックホルム　エス－１６４　８３
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100109346
弁理士　大貫　敏史
(72)発明者　ブロム，ロルフ
スウェーデン国，エス－１７５　６８　イェルファラ，スヴェルドヴェーゲン　２
(72)発明者　ミルディ，グナー
スウェーデン国，ソレンツナ　エス－１９１　６２，ツレベルグズ　アレ　７

最終頁に続く

(54)【発明の名称】電気通信システムにおける方法および構成

(57)【要約】
ユーザ装置ＵＥ（１１）とサービスｅＮｏｄｅＢ（１２）との間のＲＲＣ／ＵＰトラフィックを保護するためのセキュリティキーＫ＿ｅＮＢが、次世代パケットシステムＥＰＳのモビリティ管理エンティティ（１３）ＭＭＥおよび前記ＵＥ（１１）における方法および構成によって確立される。ＭＭＥおよびＵＥは、ＵＥからＭＭＥに送信される少なくともＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱから、およびＭＭＥとＵＥとの間で共有されるアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから、セキュリティキーＫ＿ｅＮＢを導出する。

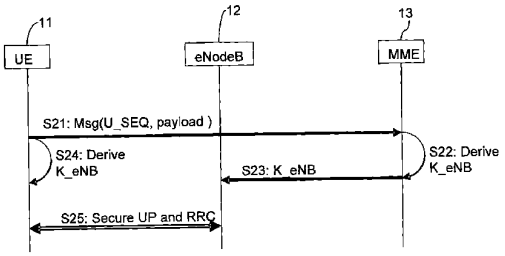


Fig. 2

【特許請求の範囲】
【請求項１】
次世代パケットシステムＥＰＳのモビリティ管理エンティティ（１３）ＭＭＥにおいて、ユーザ装置（１１）ＵＥと前記ＵＥにサービスするｅＮｏｄｅＢ（１２）との間のＲＲＣ／ＵＰトラフィックを保護するためにセキュリティキーＫ＿ｅＮＢを確立する方法であって、以下の
－　ＮＡＳサービス要求を前記ＵＥから受信するステップ（３２、５２）であって、前記要求が、ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示すステップと、
－　少なくとも前記受信されたＮＡＳ＿Ｕ＿ＳＥＱから、および前記ＵＥと共有される、記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから、前記セキュリティキーＫ＿ｅＮＢを導出するステップ（３３、５３）と、
－　前記導出されたＫ＿ｅＮＢを、前記ＵＥにサービスする前記ｅＮｏｄｅＢ（１２）に転送するステップ（３４）と、
を含む、ＭＭＥにおける方法。
【請求項２】
前記Ｋ＿ｅＮＢが、擬似乱数関数ＰＲＦを用いて、前記ＮＡＳ＿Ｕ＿ＳＥＱおよび前記Ｋ＿ＡＳＭＥから導出される、請求項１に記載のＭＭＥにおける方法。
【請求項３】
受信された下位ビットから前記完全なＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを再構成するさらなるステップを含む、請求項１または２に記載のＭＭＥにおける方法。
【請求項４】
前記ＵＥ（１１）から受信された前記ＮＡＳサービス要求の完全性を検査するさらなるステップを含む、上述の請求項のいずれか一項に記載のＭＭＥにおける方法。
【請求項５】
前記受信されたＮＡＳ＿Ｕ＿ＳＥＱの通知を前記ＵＥ（１１）に返すさらなるステップ（５４、５５）を含む、上述の請求項のいずれか一項に記載のＭＭＥにおける方法。
【請求項６】
前記ＮＡＳ＿Ｕ＿ＳＥＱが、前記Ｋ＿ｅＮＢを前記ｅＮｏｄｅＢ（１２）に転送するセットアップメッセージに含まれる、請求項５に記載のＭＭＥにおける方法。
【請求項７】
次世代パケットシステムＥＰＳのユーザ装置（１１）ＵＥにおいて、サービスｅＮｏｄｅＢ（１２）と交換されるＲＲＣ／ＵＰトラフィックを保護するためにセキュリティキーＫ＿ｅＮＢを確立する方法であって、以下の
－　ＮＡＳサービス要求をモビリティ管理エンティティＭＭＥに送信するステップ（３１、５１）であって、前記要求が、ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱ）を示すステップと、
－　少なくとも前記ＮＡＳ＿Ｕ＿ＳＥＱから、および前記ＭＭＥと共有される、記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから、前記Ｋ＿ｅＮＢを導出するステップ（３５、５６）と、
を含む、ＵＥにおける方法。
【請求項８】
前記Ｋ＿ｅＮＢが、擬似乱数関数ＰＲＦを用いて、前記ＮＡＳ＿Ｕ＿ＳＥＱおよび前記Ｋ＿ＡＳＭＥから導出される、請求項７に記載のＵＥにおける方法。
【請求項９】
前記ＭＭＥに送信された前記ＮＡＳサービス要求の完全性を保護するさらなるステップを含む、請求項７または８に記載のＵＥにおける方法。
【請求項１０】
前記ＭＭＥに送信された前記ＮＡＳサービス要求の前記ＮＡＳ＿Ｕ＿ＳＥＱを記憶するステップを含む、請求項７～９のいずれか一項に記載のＵＥにおける方法。

【請求項１１】
前記ＭＭＥに送信された前記ＮＡＳサービス要求の前記ＮＡＳ＿Ｕ＿ＳＥＱの通知を、前記ｅＮｏｄｅＢ（１２）を介して前記ＭＭＥ（１３）から逆に受信するステップ（５５）を含む、請求項７～９のいずれか一項に記載のＵＥにおける方法。
【請求項１２】
前記Ｋ＿ｅＮＢが、前記ｅＮｏｄｅＢからのセキュリティ構成メッセージの受信後に、前記ＮＡＳ＿Ｕ＿ＳＥＱおよび前記Ｋ＿ＡＳＭＥから導出される、請求項１０または１１に記載のＵＥにおける方法。
【請求項１３】
次世代パケットシステムＥＰＳ用に構成されたモビリティ管理エンティティ（１３）ＭＭＥであって、ＵＥ（１１）と前記ＵＥにサービスするｅＮｏｄｅＢ（１２）との間のＲＲＣ／ＵＰトラフィックを保護するためにセキュリティキーＫ＿ｅＮＢを確立するように構成され、
－　前記ＵＥからＮＡＳサービス要求を受信するための手段（６２）であって、前記要求が、ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示す手段と、
－　少なくとも前記受信されたＮＡＳ＿Ｕ＿ＳＥＱから、および前記ＵＥと共有される、記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから、Ｋ＿ｅＮＢを導出するための手段（６３）と、
－　前記導出されたＫ＿ｅＮＢを、前記ＵＥにサービスする前記ｅＮｏｄｅＢに送信するための手段（６４）と、
を特徴とするＭＭＥ。
【請求項１４】
擬似乱数関数ＰＲＦを用いて、前記ＮＡＳ＿Ｕ＿ＳＥＱおよび前記Ｋ＿ＡＳＭＥから前記Ｋ＿ｅＮＢを導出するように構成された、請求項１３に記載のＭＭＥ。
【請求項１５】
受信された下位ビットから前記完全なＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを再構成するように構成された、請求項１３または１４に記載のＭＭＥ。
【請求項１６】
前記ＵＥ（１１）から受信された前記ＮＡＳサービス要求の完全性を検査するように構成された、請求項１３～１５のいずれか一項に記載のＭＭＥ。
【請求項１７】
前記ＮＡＳ＿Ｕ＿ＳＥＱの通知が前記ｅＮｏｄｅＢ（１２）に転送（５４）され、前記ｅＮｏｄｅＢから前記ＵＥ（１１）に返される（５５）ように構成された、請求項１３～１６のいずれか一項に記載のＭＭＥ。
【請求項１８】
次世代パケットシステム（ＥＰＳ）用に構成されたユーザ装置（１１）ＵＥであって、サービスｅＮｏｄｅＢ（１２）と交換されるＲＲＣ／ＵＰトラフィックを保護するためにセキュリティキーＫ＿ｅＮＢを確立するように構成され、
－　ＮＡＳサービス要求をＭＭＥ（１３）に送信するための手段（６６）であって、前記要求が、ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示す手段と、
－　少なくとも前記ＮＡＳ＿Ｕ＿ＳＥＱから、および前記ＭＭＥ（１３）と共有される、記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから、Ｋ＿ｅＮＢを導出するための手段（６７）と、
を特徴とするＵＥ。
【請求項１９】
擬似乱数関数ＰＲＦを用いて、前記ＮＡＳ＿Ｕ＿ＳＥＱおよび前記Ｋ＿ＡＳＭＥから前記Ｋ＿ｅＮＢを導出するように構成された、請求項１８に記載のＵＥ（１１）。
【請求項２０】
前記ＭＭＥ（１３）に送信される前記ＮＡＳサービス要求の完全性を保護するように構成された、請求項１８または１９に記載のＵＥ。

【請求項２１】
前記ＭＭＥ（１３）に送信される前記ＮＡＳサービス要求の前記ＮＡＳ＿Ｕ＿ＳＥＱを記憶するように構成された、請求項１８～２０のいずれか一項に記載のＵＥ。
【請求項２２】
前記ＭＭＥ（１３）に送信された前記ＮＡＳサービス要求の前記ＮＡＳ＿Ｕ＿ＳＥＱの通知を、前記ｅＮｏｄｅＢ（１２）を介して前記ＭＭＥから逆に受信するように構成された、請求項１８～２０のいずれか一項に記載のＵＥ。
【請求項２３】
前記ｅＮｏｄｅＢ（１２）からのセキュリティ構成メッセージの受信後に、前記Ｋ＿ｅＮＢを導出するように構成された、請求項２１または２２に記載のＵＥ。
【発明の詳細な説明】
【技術分野】
【０００１】
技術分野
本発明は、電気通信システムにおける方法および構成に関し、特に、ＵＥによってトリガされたサービス要求のための、ＥＰＳ（次世代パケットシステム）、すなわちＥ－ＵＴＲＡＮ（次世代ＵＭＴＳ地上無線アクセスネットワーク）およびＥＰＣ（次世代パケットコアネットワーク）におけるセキュリティソリューションに関する。より具体的には、本発明は、ＥＰＳ（次世代パケットシステム）用のＭＭＥ（モビリティ管理エンティティ）およびＵＥ（ユーザ装置）において、ＲＲＣ／ＵＰトラフィックを保護するためにセキュリティキーを確立する方法および構成に関する。
【背景技術】
【０００２】
背景
ＥＰＳアーキテクチャでは、加入者認証は、ＵＥとＭＭＥ（モビリティ管理エンティティ）との間で実行され、かつＭＭＥは、例えば、モビリティ、ＵＥ識別情報、およびセキュリティパラメータを管理する。ＥＰＳにおけるセキュリティ手順を定義するための基礎は、セキュリティキーＫ＿ＡＳＭＥであり、このキーは、ＭＭＥとＵＥとの間で共有され、かつＵＥの認証において確立される。ＡＳＭＥ（アクセスセキュリティ管理エンティティ）と呼ばれる、ＥＰＳアーキテクチャの機能エンティティは、例えばＭＭＥと同じ場所に配置してもよく、ＡＳＭＥは、ホームネットワークに制限されたＣＫ／ＩＫキーから導出されたセキュリティキーＫ＿ＡＳＭＥを受信および記憶する。ＡＳＭＥは、セキュリティキーＫ＿ＡＳＭＥから、ＮＡＳシグナリング、すなわち次世代パケットコア（ＥＰＣ）ネットワークのＭＭＥとＵＥとの間の非アクセス層シグナリングを保護するために用いられるＮＡＳセキュリティコンテキストを導出する。ＮＡＳセキュリティコンテキストには、Ｋ＿ＮＡＳ＿ｅｎｃ、Ｋ＿ＮＡＳ＿ｉｎｔなど、ＮＡＳシグナリングの暗号化および完全性保護用のパラメータ、ならびにＮＡＳ＿Ｕ＿ＳＥＱおよびＮＡＳ＿Ｄ＿ＳＥＱなど、アップリンクおよびダウンリンクシーケンス番号が含まれ、シーケンス番号は、暗号化および完全性保護手順への入力だけでなく、古いメッセージの再生を防ぐために用いられる。ＡＳＭＥは、ＭＭＥにＮＡＳセキュリティコンテキストを提供し、１つのＮＡＳセキュリティコンテキストが、ＭＭＥに保持され、対応するＮＡＳセキュリティコンテキストが、ＵＥに保持され、再生保護、完全性保護および暗号化は、ＭＭＥおよびＵＥのＮＡＳセキュリティコンテキストのシーケンス番号が、再使用されないことに基づいている。
【０００３】
ＵＥとサービスｅＮｏｄｅＢ（すなわち、ＥＰＳアーキテクチャにおける無線基地局）との間のＵＰ／ＲＲＣトラフィックを保護するためのセキュリティコンテキストもまた、前記セキュリティキーＫ＿ＡＳＭＥに基づくのが好ましい。ＵＰ／ＲＲＣセキュリティコンテキストを確立する手順には、Ｋ＿ｅＮＢと呼ばれるキーであって、これから、暗号化キーＫ＿ｅＮＢ＿ＵＰ＿ｅｎｃが、ＵＰ（ユーザ平面）すなわちＥＰＣおよびＥ－ＵＴＲＡＮ上で転送されるエンドユーザデータを保護するために導出されるキー、ならびにＲＲ

Ｃ（無線資源制御）を保護するための暗号化キーＫ＿ｅＮＢ＿ＲＲＣ＿ｅｎｃおよび完全性保護キーＫ＿ｅＮＢ＿ＲＲＣ＿ｉｎｔを導出することが含まれる。

【０００４】

図１は、ＥＰＳアーキテクチャにおける、ＵＥが開始したアイドルからアクティブへの状態遷移のための従来の例示的なシグナリングフローを示す。アイドルＵＥは、ＥＰＳのＥＰＣ（次世代パケットコア）だけに認識されており、ＵＰ／ＲＲＣセキュリティコンテキストは、ｅＮｏｄｅＢとＵＥとの間には存在しない。アクティブ状態におけるＵＥは、ＥＰＣおよびＥＵＴＲＡＮの両方において認識されており、ＵＰ／ＲＲＣセキュリティコンテキストが、ＵＥとそのサービスｅＮｏｂｅＢとの間でＵＰ／ＲＲＣトラフィックを保護するために確立された。

【０００５】

図１は、ＵＥ１１、ｅＮｏｄｅＢ１２、ＭＭＥ１３、サービスＧＷ（ゲートウェイ）１４、ＰＤＮゲートウェイ１５、およびＨＳＳ（ホーム加入者サーバ）１６を示す。サービスゲートウェイ１４は、ＥＵＴＲＡＮに向かってインタフェースを終端するＥＰＣのノードであり、ＰＤＮゲートウェイは、ＰＤＮ（パケットデータネットワーク）に向かってインタフェースを終端するＥＰＣのノードである。ＵＥが複数のＰＤＮにアクセスする場合には、そのＵＥのために複数のＰＤＮゲートウェイがあってもよい。信号Ｓ１および信号Ｓ２では、ＮＡＳサービス要求は、ＵＥからＭＭＥへ透過的に転送され、かつＮＡＳサービス要求は、ＮＡＳ＿Ｕ＿ＳＥＱに基づいて、完全性が保護される。オプションの信号Ｓ３では、ＵＥは、ＭＭＥによって認証され、Ｋ＿ＡＳＭＥは、ＨＳＳ（ホーム加入者サーバ）に記憶された加入者データを用いて確立され、ＭＭＥは、Ｓ４で、初期コンテキストセットアップ要求をｅＮｏｄｅＢに送信する。信号Ｓ５およびＳ６では、ｅＮｏｄｅＢは、ＵＥとの無線ベアラを確立してアップリンクデータを転送し、信号Ｓ７で、初期コンテキストセットアップ完了メッセージをＭＭＥへ返す。信号Ｓ８では、ＭＭＥは、更新ベアラ要求をサービスＧＷに送信し、サービスＧＷは、信号Ｓ９で応答する。

【０００６】

従来のソリューションでは、ＲＲＣ／ＵＰセキュリティコンテキスト用の、ＵＥおよびＭＭＥによるＫ＿ｅＮＢの導出は、例えば、ＭＭＥからＵＥに送信されたＮＡＳサービス受理メッセージまたは他の明示的な情報に基づいている。しかしながら、図１における例示的な従来のＥＰＳシグナリングフローに示されているように、ＭＭＥは、通常、ＥＰＳにおいて、ＵＥからＮＡＳサービス要求を受信しても、いかなるＮＡＳサービス受理も送信しない。したがって、ＮＡＳサービス受理メッセージにおける情報からＫ＿ｅＮＢを導出することは不可能である。

【０００７】

例示的な公知のソリューションによれば、Ｋ＿ｅＮＢは、ＮＡＳサービス受理メッセージにおいてＭＭＥによって用いられるＫ＿ＡＳＭＥおよびＮＡＳ＿Ｄ＿ＳＥＱからＭＭＥによって導出され、ＵＥは、ＮＡＳサービス受理メッセージからシーケンス番号ＮＡＳ＿Ｄ＿ＳＥＱを検索し、かつＭＭＥと同じＫ＿ｅＮＢ導出を実行することによって、同じＫ＿ｅＮＢを導出する。ＭＭＥは、それがｅＮｏｄｅＢへのＳ１接続を設定する場合に、Ｋ＿ｅＮＢをｅＮｏｄｅＢに転送する。しかしながら、この公知のソリューションの欠点は、明示的なＮＡＳサービス受理メッセージがＭＭＥからＵＥに対して定義されない場合には、図１における例示的な従来のＥＰＳシグナリングフローにおけるように、ＵＥが、ＭＭＥと同じＫ＿ｅＮＢを導出することは不可能であることである。たとえＵＥが、現在のＮＡＳダウンリンクシーケンス番号ＮＡＳ＿Ｄ＿ＳＥＱを推定することが技術的に可能であっても、この推定は誤っている可能性がある。なぜなら、ＭＭＥは、損失してＵＥによって決して受信されなかったＮＡＳメッセージを送信したかもしれないからである。かかる場合には、ＭＭＥは、そのＮＡＳ＿Ｄ＿ＳＥＱを更新し、ＵＥが、この更新に気づくこともなく、ＵＥにおける誤ったＮＡＳ＿Ｄ＿ＳＥＱにつながることになろう。

【０００８】

別の例示的な公知のソリューションによれば、Ｋ＿ｅＮＢの導出は、特にＫ＿ｅＮＢの

導出のために保持される別個のシーケンス番号に基づき、このシーケンス番号は、ＵＥがそれをＭＭＥに送信するかまたはＭＭＥがそれをＵＥに送信することによって、ＮＡＳサービス要求手順の間に明示的に同期される。しかしながら、このソリューションの欠点は、別個のシーケンス番号の特別な複雑さである。なぜなら、再生攻撃を防ぐために、別個のシーケンス番号をＵＥおよびＭＭＥの両方において保持しなければならないからである。

【発明の概要】

【発明が解決しようとする課題】

【０００９】

概要

本発明の目的は、上記で概説した課題に取り組むことであり、この目的および他の目的は、独立請求項による方法および構成ならびに従属請求項による実施形態によって達成される。

【課題を解決するための手段】

【００１０】

本発明の基本的な考えは、Ｋ＿ｅＮＢが、Ｋ＿ＡＳＭＥから、およびＵＥからＭＭＥへのＮＡＳサービス要求メッセージのＮＡＳ＿Ｕ＿ＳＥＱから導出され、それによって、ｅＮｏｄｅＢにおけるＵＰ／ＲＲＣセキュリティコンテキストの確立をトリガするということである。

【００１１】

ＭＭＥからＵＥへの明示的なダウンリンクＮＡＳサービス受理メッセージまたはシーケンス番号が必要ではないこと、およびＮＡＳセキュリティコンテキストの再生保護機能が、ＲＲＣおよびＵＰセキュリティコンテキストにおいて再利用されることが、本発明の利点である。

【００１２】

一態様によれば、本発明は、次世代パケットシステムＥＰＳのモビリティ管理エンティティＭＭＥにおいて、ユーザ装置ＵＥとＵＥにサービスするｅＮｏｄｅＢとの間のＲＲＣ／ＵＰトラフィックを保護するためにセキュリティキーＫ＿ｅＮＢを確立する方法を提供する。この方法には、ＵＥからＮＡＳサービス要求を受信するステップであって、この要求が、ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示すステップと、少なくとも前記受信されたＮＡＳ＿Ｕ＿ＳＥＱから、および前記ＵＥと共有される、記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥからセキュリティキーＫ＿ｅＮＢを導出するステップと、前記導出されたＫ＿ｅＮＢを、前記ＵＥにサービスするｅＮｏｄｅＢに転送するステップと、が含まれる。

【００１３】

第２の態様によれば、本発明は、次世代パケットシステムＥＰＳ用のモビリティ管理エンティティＭＭＥを提供する。ＭＭＥは、ＵＥとＵＥにサービスするｅＮｏｄｅＢとの間のＲＲＣ／ＵＰトラフィックを保護するために、セキュリティキーＫ＿ｅＮＢを確立するように構成される。ＭＭＥには、ＵＥからＮＡＳサービス要求を受信するための手段であって、この要求が、ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示す手段と、少なくとも前記受信されたＮＡＳ＿Ｕ＿ＳＥＱから、および前記ＵＥと共有される、記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥからＫ＿ｅＮＢを導出するための手段と、ならびに、前記導出されたＫ＿ｅＮＢを、前記ＵＥにサービスするｅＮｏｄｅＢに送信するための手段と、が含まれる。

【００１４】

第１および第２の態様は、さらに、方法および対応する手段を提供し、これらに従って、ＭＭＥが、擬似乱数関数ＰＲＦを用いてＮＡＳ＿Ｕ＿ＳＥＱおよびＫ＿ＡＳＭＥからＫ＿ｅＮＢを導出可能になる。ＭＭＥは、さらに、受信された下位ビットから完全なＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを再構成し、ＵＥから受信されたＮＡＳサービス要求の完全性を検査してもよい。さらに、ＭＭＥは、受信されたＮＡＳ＿Ｕ＿Ｓ

ＥＱの通知をＵＥに返してもよく、ＮＡＳ＿Ｕ＿ＳＥＱは、Ｋ＿ｅＮＢをｅＮｏｄｅＢに転送するセットアップメッセージに含まれていてもよい。それによって、ＵＥは、ＭＭＥに送信されるＮＡＳ＿Ｕ＿ＳＥＱを覚えている必要がない。

【００１５】

第３の態様によれば、本発明は、次世代パケットシステムＥＰＳのユーザ装置ＵＥにおいて、サービスｅＮｏｄｅＢと交換されるＲＲＣ／ＵＰトラフィックを保護するためにセキュリティキーＫ＿ｅＮＢを確立する方法を提供する。この方法には、ＮＡＳサービス要求をモビリティ管理エンティティＭＭＥに送信するステップであって、この要求が、ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示すステップと、少なくとも前記ＮＡＳ＿Ｕ＿ＳＥＱから、および前記ＭＭＥと共有される、記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから、Ｋ＿ｅＮＢを導出するステップと、が含まれる。

【００１６】

第４の態様によれば、本発明は、次世代パケットシステムＥＰＳ用に構成されたユーザ装置ＵＥを提供する。ＵＥは、サービスｅＮｏｄｅＢと交換されるＲＲＣ／ＵＰトラフィックを保護するために、セキュリティキーＫ＿ｅＮＢを確立するように構成される。ＵＥには、ＮＡＳサービス要求をＭＭＥに送信するための手段であって、この要求が、ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示す手段と、ならびに、少なくとも前記ＮＡＳ＿Ｕ＿ＳＥＱから、および前記ＭＭＥと共有される、記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから、Ｋ＿ｅＮＢを導出するための手段と、が含まれる。

【００１７】

第３および第４の態様は、さらに、方法および対応する手段を提供し、これらに従って、ＵＥが、擬似乱数関数ＰＲＦを用いてＮＡＳ＿Ｕ＿ＳＥＱおよびＫ＿ＡＳＭＥからＫ＿ｅＮＢを導出し、ＭＭＥに送信されるＮＡＳサービス要求の完全性を保護する。さらに、ＵＥは、ＭＭＥに送信されるＮＡＳサービス要求のＮＡＳ＿Ｕ＿ＳＥＱを記憶するか、または代替として、ＭＭＥに送信されたＮＡＳサービス要求のＮＡＳ＿Ｕ＿ＳＥＱの通知を、ｅＮｏｄｅＢを介してＭＭＥから逆に受信してもよい。この代替実施形態は、ＵＥが、ＭＭＥに送信されたＮＡＳ＿Ｕ＿ＳＥＱを覚えている必要がないという利点を有する。ＵＥは、さらに、ｅＮｏｄｅＢからのセキュリティ構成メッセージの受信後に、ＮＡＳ＿Ｕ＿ＳＥＱおよびＫ＿ＡＳＭＥからＫ＿ｅＮＢを導出してもよい。

【００１８】

ここで、添付の図面に関連して、より詳細に本発明を説明する。

【図面の簡単な説明】

【００１９】

図面の簡単な説明

【図１】ＥＰＳにおいて従来のＵＥによってトリガされたサービス要求を示すシグナリング図である。

【図２】本発明の第１の実施形態を示すシグナリング図であり、これによれば、ＵＥは、ＮＡＳサービス要求メッセージでＭＭＥに送信されたＮＡＳ＿Ｕ＿ＳＥＱを覚えている。

【図３】ＵＥおよびＭＭＥによるＫ＿ｅＮＢの導出を示す流れ図である。

【図４】本発明の第２の実施形態を示すシグナリング図であり、この場合には、ＭＭＥは、受信されたＮＡＳ＿Ｕ＿ＳＥＱをＵＥに返す。

【図５】図４に表された第２の実施形態を示す流れ図である。

【図６ａ】セキュリティキーＫ＿ｅＮＢを導出するための手段を提供されたＭＭＥ（モビリティ管理エンティティ）を概略的に示す。

【図６ｂ】セキュリティキーＫ＿ｅＮＢを導出するための手段を提供されたＵＥを概略的に示す。

【発明を実施するための形態】

【００２０】

詳細な説明

以下の説明では、本発明の完全な理解を提供するために、特定のアーキテクチャおよびステップシーケンスなどの特定の詳細が記載される。しかしながら、本発明が、これらの特定の詳細から逸脱する可能性がある他の実施形態において実行し得ることは、当業者には明らかである。

【００２１】

さらに、説明される機能が、プログラムされたマイクロプロセッサもしくは汎用コンピュータと共に機能するソフトウェアを用いて、かつ／または特定用途向け集積回路を用いて実現可能であることが明らかである。本発明が一方法の形態で説明される場合には、本発明はまた、コンピュータプログラム製品において、ならびにコンピュータプロセッサおよびメモリを含むシステムにおいて具体化してもよく、この場合に、メモリは、説明される機能を実行可能な１つまたは複数のプログラムで符号化される。

【００２２】

本発明の概念は、セキュリティキーＫ＿ｅＮＢが、アクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから、およびＵＥからＭＭＥに送信されるＮＡＳサービス要求メッセージのアップリンクシーケンスカウンタＮＡＳ＿Ｕ＿ＳＥＱから導出され、それによって、ｅＮｏｄｅＢにおいてＵＰ／ＲＲＣセキュリティコンテキストの確立をトリガするということである。

【００２３】

ＵＥがアイドルモードにある場合には、ＮＡＳセキュリティコンテキストが、存在しかつ例えば、上記のＫ＿ＮＡＳ＿ｅｎｃ、Ｋ＿ＮＡＳ＿ｉｎｔ、ＮＡＳ＿Ｕ＿ＳＥＱ、およびＮＡＳ＿Ｄ＿ＳＥＱを含み、ＮＡＳメッセージは、完全性および場合により機密性を保護される。したがって、ＮＡＳセキュリティコンテキストにはまた、ＵＥのセキュリティ能力、特に暗号化および完全性アルゴリズムが含まれる。

【００２４】

ＮＡＳメッセージの保護は、ＮＡＳセキュリティキーＫ＿ＮＡＳ＿ｅｎｃ、Ｋ＿ＮＡＳ＿ｉｎｔ、ならびにメッセージの方向についてアップリンクおよびダウンリンクシーケンスカウンタＮＡＳ＿Ｕ＿ＳＥＱまたはＮＡＳ＿Ｄ＿ＳＥＱに基づいている。完全なシーケンスカウンタは、通常、ＮＡＳメッセージと共に送信されず、下位ビットいくつかだけであり、完全なシーケンス番号は、上位ビットの局所推定および受信された下位ビットから、受信端で再構成される。

【００２５】

上記の図１に示すように、本発明の概念は、ＵＥによってトリガされたサービス要求用のシグナリング図のコンテキストにおいて説明してもよい。

【００２６】

図１における従来のシグナリング図のＳ１およびＳ２では、ＮＡＳサービス要求は、アップリンクシーケンスカウンタＮＡＳ＿Ｕ＿ＳＥＱを含むが、ＵＥからＭＭＥに転送され、ＮＡＳサービス要求メッセージは、前記ＮＡＳ＿Ｕ＿ＳＥＱに基づいて完全性が保護される。ＭＭＥは、メッセージの完全性を検査し、それが再生でない場合には、それを受理し、これによって、ＮＡＳ＿Ｕ＿ＳＥＱが、新しく以前に用いられなかったことが保証される。

【００２７】

その後、本発明によれば、ＭＭＥは、少なくとも、受信されたアップリンクシーケンスカウンタＮＡＳ＿Ｕ＿ＳＥＱおよびＫ＿ＡＳＭＥに基づき、従来のキー導出関数を用いて、Ｋ＿ｅＮＢを導出するが、これは、図１に示す従来のシグナリング図には含まれない。したがって、シーケンスカウンタは、認証においてのみリセットしてもよい。ＭＭＥは、信号Ｓ４のメッセージ、初期コンテキストセットアップ要求（Ｓ１－ＡＰ）で、またはそこに相乗りして、導出されたＫ＿ｅＮＢをｅＮｏｄｅＢに送信する。

【００２８】

信号Ｓ５では、ｅＮｏｄｅＢは、無線ベアラ確立およびセキュリティ構成メッセージ（

セキュリティモードコマンド）をＵＥに送信する。図１におけるように、これらのメッセージは、２つの別個のメッセージとして、または１つのメッセージに組み合わせて送信してもよく、ＵＥによるこれらのメッセージの受信は、暗黙のうちに、信号Ｓ１におけるＵＥのＮＡＳサービス要求の確認になる。セキュリティモードコマンドは、例えば、保護がいつ開始すべきかおよびどのアルゴリズムを用いるべきかを決定する。

【００２９】

本発明によれば、ＵＥは、信号Ｓ５でメッセージを受信すると、以前に実行されていない場合には、少なくともＮＡＳ＿Ｕ＿ＳＥＱおよびＫ＿ＡＳＭＥに基づき、従来のキー導出関数を用いて、Ｋ＿ｅＮＢを導出する。その後、ｅＮｏｄｅＢおよびＵＥは、ＵＰ／ＲＲＣセキュリティコンテキストを確立するが、これは、図１における従来のシグナリング図には示されていない。

【００３０】

本発明の第１の実施形態によれば、ＵＥは、信号Ｓ１における初期ＮＡＳサービス要求に含まれるアップリンクシーケンスカウンタＮＡＳ＿Ｕ＿ＳＥＱを記憶し、記憶されたＮＡＳ＿Ｕ＿ＳＥＱをＫ＿ｅＮＢの導出のために用いる。

【００３１】

しかしながら、第２の実施形態によれば、ＭＭＥには、アップリンクシーケンスカウンタＮＡＳ＿Ｕ＿ＳＥＱ、または信号Ｓ４でｅＮｏｄｅＢに送信されるＳ１－ＡＰセットアップメッセージにおける、ＮＡＳ＿Ｕ＿ＳＥＱを示す下位ビットだけが含まれ、この場合には、この情報はまた、ＲＲＣ／ＵＰコンテキスト確立中にｅＮｏｄｅＢからＵＥに転送される。この場合に、ＵＥは、Ｋ＿ｅＮＢの導出のためにｅＮｏｄｅＢからＮＡＳ＿Ｕ＿ＳＥＱの通知を検索することができ、信号Ｓ１およびＳ２でＭＭＥに送信されたＮＡＳサービス要求メッセージのＮＡＳ＿Ｕ＿ＳＥＱを保持する必要がない。

【００３２】

図２は、本発明の第１の実施形態を示すが、この場合には、ＵＥは、信号Ｓ２４におけるＫ＿ｅＮＢの導出のために、信号Ｓ２１における初期ＮＡＳサービス要求メッセージのＮＡＳ＿Ｕ＿ＳＥＱを保持する。ＭＭＥは、信号Ｓ２１でＵＥからＮＡＳ＿Ｕ＿ＳＥＱを受信するか、またはＮＡＳ＿Ｕ＿ＳＥＱを示す下位ビットだけを受信し、ＮＡＳ＿Ｕ＿ＳＥＱおよびＫ＿ＡＳＭＥに基づいてＳ２２においてＫ＿ｅＮＢを導出する。ＭＭＥは、導出されたＫ＿ｅＮＢを信号Ｓ２３でｅＮｏｄｅＢに転送する。

【００３３】

その後、図２には示していないが、ｅＮｏｄｅＢおよびＵＥは、Ｋ＿ｅＮＢを用いてＵＰ／ＲＲＣセキュリティコンテキストを確立するが、ＵＰ／ＲＲＣセキュリティコンテキストには、ＵＰトラフィックを保護するための暗号化キーＫ＿ｅＮＢ＿ＵＰ＿ｅｎｃ、ならびにＲＲＣトラフィックの保護のための暗号化キーおよび完全性保護キー、Ｋ＿ｅＮＢ＿ＲＲＣ＿ｅｎｃおよびＫ＿ｅＮＢ＿ＲＲＣ＿ｉｎｔがそれぞれ含まれ、それによって、信号Ｓ２５において安全なＵＰ／ＲＲＣトラフィックを可能にする。

【００３４】

Ｋ＿ｅＮＢの導出は、従来のキー導出関数によって、例えば擬似乱数関数Ｋ＿ｅＮＢ＝ＰＲＦ（Ｋ＿ＡＳＭＥ、ＮＡＳ＿Ｕ＿ＳＥＱ、．．．）によって、実行される。

【００３５】

上記のＰＲＦ関数においてドットで示すように、Ｋ＿ｅＮＢ導出関数は、例えばｅＮｏｄｅＢ識別情報などの追加的な従来の入力値を有してもよい。

【００３６】

図３は、本発明による方法を示す流れ図であり、ステップ３１において、ＵＥ１１は、初期ＮＡＳサービス要求メッセージをＭＭＥ１３に送信するが、このメッセージは、通常、カウンタの下位ビットだけを送信することによって、ＮＡＳアップリンクシーケンスカウンタＮＡＳ＿Ｕ＿ＳＥＱを示す。ステップ３２において、ＭＭＥは、ＵＥからＮＡＳサービス要求メッセージを受信し、ＮＡＳ＿Ｕ＿ＳＥＱを取得し、受信された下位ビットから完全なシーケンスを再構成する。ステップ３３において、ＭＭＥは、適切なキー導出関

数、例えば擬似乱数関数を用いて、少なくとも受信したＮＡＳ＿Ｕ＿ＳＥＱ、およびＡＳＭＥ（アクセスセキュリティモビリティエンティティ）からのＫ＿ＡＳＭＥから、セキュリティキーＫ＿ｅＮＢを導出する。

【００３７】

その後、ＭＭＥは、ステップ３４において、ＵＥと共有される完全なＵＰ／ＲＲＣセキュリティコンテキストを確立するためにｅＮｏｄｅＢによって用いられるように、導出されたＫ＿ｅＮＢをｅＮｏｄｅＢ１２に転送する。ステップ３５において、前記ＵＥは、少なくとも記憶されたＫ＿ＡＳＭＥから、およびステップ３１においてＵＥからＭＭＥに送信された初期ＮＡＳサービス要求メッセージのＮＡＳ＿Ｕ＿ＳＥＱから、同じＫ＿ｅＮＢを導出し、導出されたＫ＿ｅＮＢからＵＰ／ＲＲＣセキュリティコンテキストを確立する。

【００３８】

本発明の第１の実施形態では、ＵＥは、初期ＮＡＳサービス要求メッセージでＭＭＥに送信されたＮＡＳ＿Ｕ＿ＳＥＱを記憶し、記憶されたシーケンス番号を用いてＫ＿ｅＮＢを導出する。

【００３９】

図４は、本発明の第２の実施形態を示すシグナリング図であり、この場合には、ＵＥは、ＮＡＳ＿Ｕ＿ＳＥＱを記憶する必要がない。代わりに、ＭＭＥは、ｅＮｏｄｅＢを介して、受信したＮＡＳ＿Ｕ＿ＳＥＱの通知をＵＥに返す。図２の信号Ｓ２１に対応する信号Ｓ４１において、ＵＥ１１は、アップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示す初期ＮＡＳサービス要求をＭＭＥ１３に送信し、Ｓ４２において、ＭＭＥは、ＮＡＳ＿Ｕ＿ＳＥＱを受信し、少なくともＮＡＳ＿Ｕ＿ＳＥＱおよびＫ＿ＡＳＭＥに基づいて、Ｋ＿ｅＮＢを導出する。しかしながら、この第２の実施形態によれば、ＭＭＥは、導出されたＫ＿ｅＮＢと一緒にｅＮｏｄｅＢ１２に送信される、信号Ｓ４３において前記受信ＮＡＳ＿Ｕ＿ＳＥＱの通知を含み、ｅＮｏｄｅＢは、信号Ｓ４４においてＮＡＳ＿Ｕ＿ＳＥＱをＵＥに転送する。その後、信号Ｓ４５において、ＵＥは、少なくともＫ＿ＡＳＭＥから、およびＭＭＥによって返されたＮＡＳ＿Ｕ＿ＳＥＱから、Ｋ＿ｅＮＢを導出する。信号Ｓ４６において、導出されたセキュリティキーＫ＿ｅＮＢから、ｅＮｏｄｅＢおよびＵＥは、ＵＰ／ＲＲＣセキュリティコンテキストを確立し、それによって、安全なＵＰ／ＲＲＣトラフィックを可能にする。

【００４０】

図５は、本発明の第２の実施形態による上記の方法を示す流れ図であり、この場合には、ＮＡＳ＿Ｕ＿ＳＥＱの通知は、ＭＭＥによってＵＥに返される。ステップ４１において、ＵＥ１１は、初期ＮＡＳサービス要求メッセージをＭＭＥ１３に送信するが、このメッセージは、通常、ＮＡＳアップリンクシーケンスカウンタＮＡＳ＿Ｕ＿ＳＥＱの下位ビットを示す。ステップ５２において、ＭＭＥは、ＵＥからＮＡＳサービス要求メッセージを受信し、それによって、ＮＡＳ＿Ｕ＿ＳＥＱを取得し、必要に応じて、受信された下位ビットから完全なＮＡＳ＿Ｕ＿ＳＥＱを再構成する。ステップ５３において、ＭＭＥは、適切なキー導出関数を用い、少なくとも受信されたＮＡＳ＿Ｕ＿ＳＥＱおよびＫ＿ＡＳＭＥからセキュリティキーＫ＿ｅＮＢを導出する。

【００４１】

その後、ＭＭＥは、ステップ５４において、導出されたＫ＿ｅＮＢをｅＮｏｄｅＢ１２に転送するメッセージに、ＮＡＳアップリンクシーケンスカウンタＮＡＳ＿Ｕ＿ＳＥＱの通知を含め、ｅＮｏｄｅＢは、ＵＰ／ＲＲＣセキュリティコンテキストを確立するために、受信されたセキュリティキーＫ＿ｅＮＢを用いる。受信されたＮＡＳ＿Ｕ＿ＳＥＱは、ステップ５５において、ｅＮｏｄｅＢによってＵＥ１１に転送され、ステップ５６において、ＵＥは、ｅＮｏｄｅＢと共有されるＵＰ／ＲＲＣセキュリティコンテキストを確立するために、少なくともＫ＿ＡＳＭＥから、および前記受信されたＮＡＳ＿Ｕ＿ＳＥＱから、セキュリティキーＫ＿ｅＮＢを導出する。

【００４２】

ステップ５３におけるＭＭＥによる、およびステップ５６におけるＵＥによるＫ＿ｅＮＢの導出は、適切な従来のキー導出関数、例えば擬似乱数関数Ｋ＿ｅＮＢ＝ＰＲＦ（Ｋ＿ＡＳＭＥ、ＮＡＳ＿Ｕ＿ＳＥＱ、．．．）によって実行される。通常、キー導出関数は、追加的な従来の入力値、例えばｅＮｏｄｅＢ識別情報を有する。

【００４３】

図６ａは、本発明に従って、ＥＰＳ用のＭＭＥ１３（モビリティ管理エンティティ）を示すが、このＭＭＥ１３は、ＵＥとサービスｅＮｏｄｅＢとの間のＵＰ／ＲＲＣトラフィックを保護するためのセキュリティコンテキスト用のセキュリティキーＫ＿ｅＮＢを確立するようにさらに構成される。ＭＭＥには、図示していないが、ＥＰＳにおけるノードと、例えばＳ１－ＭＭＥインタフェースを介してｅＮｏｄｅＢｓと通信するための従来の通信手段が設けられる。さらに、図１のＭＭＥでは、ＡＳＭＥ（アクセスセキュリティ管理エンティティ）６１が、破線によって示されている。なぜなら、ＥＰＳのこの機能エンティティは、ＭＭＥと同じ場所に配置してもよいからである。

【００４４】

セキュリティキーＫ＿ｅＮＢを確立するための、図６ａに示すＭＭＥ１３の手段には、（ＵＥのサービスｅＮｏｄｅＢを介した）ＵＥからのＮＡＳ＿Ｕ＿ＳＥＱを含むＮＡＳサービス要求メッセージを受信するために受信手段６２と、従来のキー導出関数を用い、少なくとも受信されたＮＡＳ＿Ｕ＿ＳＥＱおよび記憶されたＫ＿ＡＳＭＥに基づいて、セキュリティキーＫ＿ｅＮＢを導出するためのキー導出手段６３と、導出されたＫ＿ｅＮＢを、ＵＥにサービスするｅＮｏｄｅＢに送信するための送信手段６４と、が含まれる。

【００４５】

図６ｂは、本発明によるＵＥ１１（ユーザエンティティ）を示すが、ＵＥは、ＥＰＳ用に構成され、さらに、ＵＥのサービスｅＮｏｄｅＢと交換されるＵＰ／ＲＲＣトラフィックを保護するためのセキュリティコンテキスト用のセキュリティキーＫ＿ｅＮＢを確立するように構成される。ＵＥには、そのサービスｅＮｏｄｅＢへのＬＴＥ－Ｕｕインタフェースを介してＥＰＳにおけるノードと通信するための従来の通信手段（図示せず）が設けられる。

【００４６】

セキュリティキーＫ＿ｅＮＢを確立するための、図６ｂに示すＵＥ１１の手段には、サービスｅＮｏｄｅＢを介して、ＮＡＳサービス要求メッセージをＭＭＥに送信するための送信手段６６であって、この要求が、アップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示す手段が含まれ、セキュリティキーＫ＿ｅＮＢを確立するための手段には、従来のキー導出関数を用い、少なくともＮＡＳ＿Ｕ＿ＳＥＱおよび記憶されたＫ＿ＡＳＭＥに基づいて、セキュリティキーＫ＿ｅＮＢを導出するためのキー導出手段６７が含まれる。

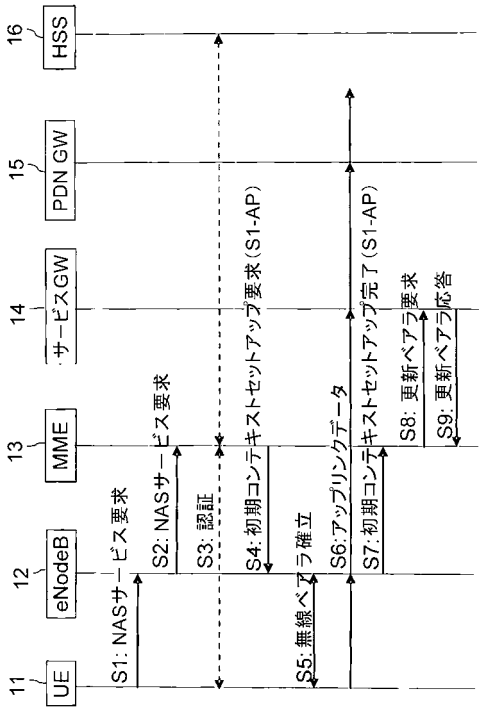
【００４７】

図６ａおよび６ｂに示すように、ＭＭＥおよびＵＥの上記の手段は、ソフトウェアおよびハードウェアの適切な組み合わせ、例えばプログラムされたマイクロプロセッサまたは特定用途向け集積回路、ならびに従来の無線送信機および受信機を用いて、説明した機能を実現する。

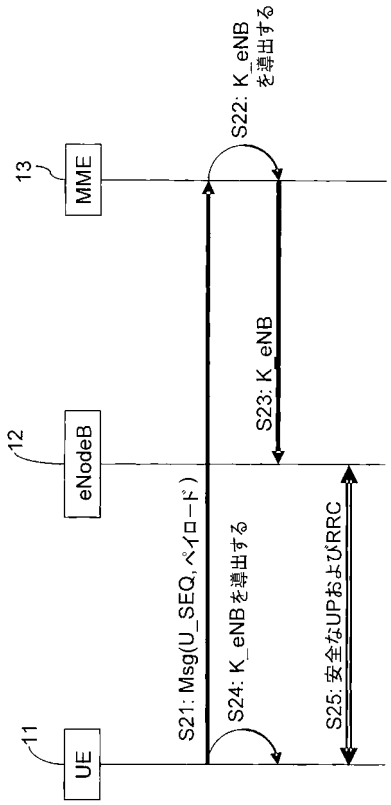
【００４８】

特定の例示的な実施形態に関連して本発明を説明したが、この説明は、一般に単に本発明の概念を示すように意図されており、本発明の範囲を限定するように理解すべきではない。

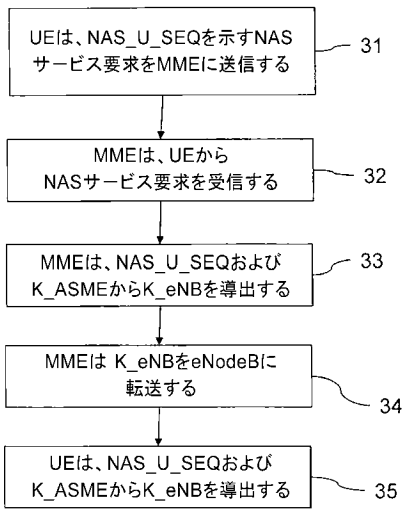
【図１】


16
HSS
15
PDN GW
14
サービスGW
13
MME
12
eNodeB
11
UE
S1: NASサービス要求
S2: NASサービス要求
S3: 認証
S4: 初期コンテキストセットアップ要求(S1-AP)
S5: 無線ベアラ確立
S6: アップリンクデータ
S7: 初期コンテキストセットアップ完了(S1-AP)
S8: 更新ベアラ要求
S9: 更新ベアラ応答

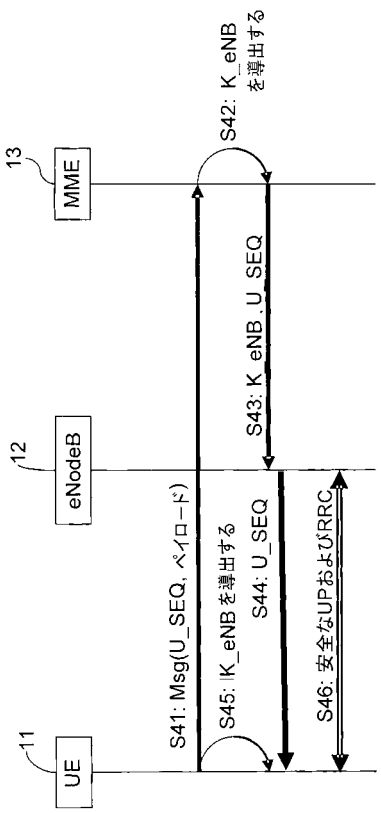
【図２】


13
MME
12
eNodeB
11
UE
S22: K_eNB を導出する
S23: K_eNB
S21: Msg(U_SEQ, ペイロード)
S24: K_eNBを導出する
S25: 安全なUPおよびRRC

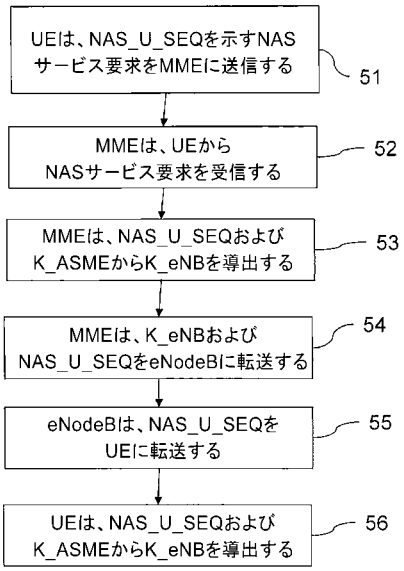
【図３】


UEは、NAS_U_SEQを示すNAS サービス要求をMMEに送信する
31
MMEは、UEから NASサービス要求を受信する
32
MMEは、NAS_U_SEQおよび K_ASMEからK_eNBを導出する
33
MMEは K_eNBをeNodeBに 転送する
34
UEは、NAS_U_SEQおよび K_ASMEからK_eNBを導出する
35

【図４】


13
MME
12
eNodeB
11
UE
S42: K_eNB を導出する
S43: K_eNB_U_SEQ
S41: Msg(U_SEQ, ペイロード)
S45: K_eNBを導出する
S44: U_SEQ
S46: 安全なUPおよびRRC

【図５】



【図６ａ】

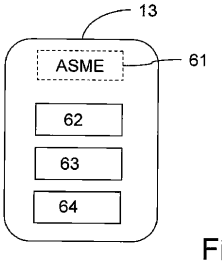


Fig. 6a

【図６ｂ】

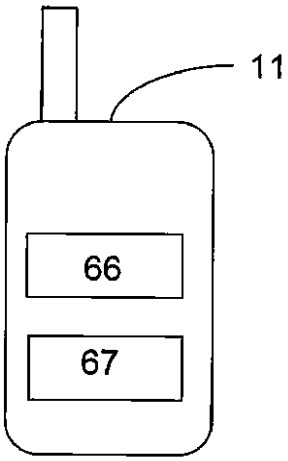


Fig. 6b

【国際調査報告】

1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/050591

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
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)

IPC: H04L, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	NOKIA: 'Generation of separate keys for NAS/UP/RRC during initial access and handover', S3-060648, 3GPP TSG SA WG3 Security S3#45, 31 October - 3 November, 2006, Dulles, USA. [retrieved on 2008-04-21] Retrieved from the Internet: <http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_45_Ashburn/Docs/> See whole document ---	1-23
A	NOKIA, ERICSSON: 'MAC, RLC and RRC Layer Security', S3-060456, 3GPP TSG SA WG3 Security #44, July 11-14, 2006, Tallinn, Estonia. [retrieved on 2008-04-21] Retrieved from the Internet: <http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_44_Tallinn/Docs/> See whole document ---	1-23

[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
4 December 2008	10 -12- 2008
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Christian Wall/PR Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/050591

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 0124560 A1 (SIMOCO INTERNATIONAL LIMITED), 5 April 2001 (05.04.2001), abstract ---	1-23
A	WO 2007022731 A1 (HUAWEI TECHNOLOGIES CO., LTD.), 1 March 2007 (01.03.2007), abstract --- --------	1-23

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/050591

International patent classification (IPC)
H04L 9/08 (2006.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

Use the application number as username.
The password is **LXZWIYDIID**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

INTERNATIONAL SEARCH REPORT
Information on patent family members

01/11/2008

International application No.
PCT/SE2008/050591

WO	0124560	A1	05/04/2001	AU	7534900	A	30/04/2001
				GB	0023682	D	00/00/0000
				GB	2359464	A	22/08/2001
				GB	9922847	D	00/00/0000
WO	2007022731	A1	01/03/2007	CN	1921682	A	28/02/2007

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MT,NL,NO,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 ノーマン，カール
スウェーデン国，エス－１１６ ２８ ストックホルム，スティグベルグスガタン ３２エー

Ｆターム(参考) 5J104 AA16 EA04 EA15 EA16 JA03 NA02 NA37
5K067 AA35 DD17 HH36
5K201 AA02 AA08 BB05 BB06 EA04 FA01