(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5216014号
(P5216014)

(45)発行日　平成25年6月19日(2013.6.19)　(24)登録日　平成25年3月8日(2013.3.8)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675A
H04L 9/14 (2006.01)　　H04L 9/00 675D
　　H04L 9/00 641

請求項の数 22　(全 21 頁)

(21)出願番号　特願2009-533280 (P2009-533280)
(86)(22)出願日　平成19年10月11日 (2007.10.11)
(65)公表番号　特表2010-507325 (P2010-507325A)
(43)公表日　平成22年3月4日 (2010.3.4)
(86)国際出願番号　PCT/SE2007/050734
(87)国際公開番号　WO2008/048179
(87)国際公開日　平成20年4月24日 (2008.4.24)
審査請求日　平成22年9月10日 (2010.9.10)
(31)優先権主張番号　60/829,954
(32)優先日　平成18年10月18日 (2006.10.18)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　11/857,621
(32)優先日　平成19年9月19日 (2007.9.19)
(33)優先権主張国　米国 (US)

(73)特許権者　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　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治

最終頁に続く

(54)【発明の名称】通信ネットワークにおける暗号キー管理

(57)【特許請求の範囲】
【請求項１】
認証ノード（４２、４３、４４）に認証データを配信するための認証サーバ（２５）における方法であって、
前記認証ノードは、異なるタイプの複数の認証ノードの１つであり、
前記認証ノードは、複数の異なるバージョンの移動端末（４１、５１、５２、５３）において利用される、異なるバージョンのアイデンティティモジュールを認証するものであり、
当該方法は、
前記認証サーバ（２５）において、マスターキー（Ｓ）を生成する工程と、
前記認証ノードのタイプと前記アイデンティティモジュールのバージョンの異なる組み合わせそれぞれに対して、異なる変換されたキー（Ｓ１、Ｓ２）が導出されるキー分離プロセスを利用して、異なる認証データを、前記マスターキーから暗号として導出する工程と、
前記認証ノードによって認証される、前記認証ノードのタイプと前記アイデンティティモジュールのバージョンの組み合わせに対して導出される認証データを、前記認証ノードに選択的に提供する工程と
を備えることを特徴とする方法。
【請求項２】
前記複数の認証ノードは、リリース８サービングＧＰＲＳサービスノード（Ｒｅｌ８

ＳＧＳＮ）、プレリリース８ＳＧＳＮ（Ｐｒｅ－Ｒｅｌ８　ＳＧＳＮ）、及びＥＰＳ移動管理エンティティ（ＭＭＥ）を含む
ことを特徴とする請求項１に記載の方法。
【請求項３】
前記移動端末のバージョンは、３ＧＰＰリリース８ユーザ機器（Ｒｅｌ８　ＵＥ）とＰｒｅ－Ｒｅｌ８　ＵＥとを含む
ことを特徴とする請求項２に記載の方法。
【請求項４】
前記アイデンティティモジュールは、ＵＭＴＳ加入者アイデンティティモジュール（ＵＳＩＭ）と拡張ＳＩＭ／ＵＳＩＭ（ｘＳＩＭ）を有する
ことを特徴とする請求項３に記載の方法。
【請求項５】
前記提供する工程は、認証される各移動端末で利用される前記アイデンティティモジュールのバージョンを示す情報を、前記認証ノードへ送信することを含む
ことを特徴とする請求項４に記載の方法。
【請求項６】
認証ノード（４２、４３、４４）に認証データを配信するための認証サーバ（２５）であって、
前記認証ノードは、異なるタイプの複数の認証ノードの１つであり、
前記認証ノードは、複数の異なるバージョンの移動端末（４１、５１、５２、５３）において利用される、異なるバージョンのアイデンティティモジュールを認証するものであり、
当該認証サーバは、
マスターキー（Ｓ）を生成する手段と、
前記認証ノードのタイプと前記アイデンティティモジュールのバージョンの異なる組み合わせそれぞれに対する、異なる認証データ（Ｓ１、Ｓ２）を、前記マスターキーから暗号として導出するキー分離手段と、
前記認証ノードによって認証される、前記認証ノードのタイプと前記アイデンティティモジュールのバージョンの組み合わせに対して導出される認証データを、前記認証ノードに提供する手段と
を備えることを特徴とする認証サーバ。
【請求項７】
前記キー分離手段は、前記認証ノードのタイプと前記アイデンティティモジュールのバージョンの異なる組み合わせそれぞれに対して、異なる変換されたキーを、前記マスターキーから暗号として導出する手段を含む
ことを特徴とする請求項６に記載の認証サーバ。
【請求項８】
前記複数の認証ノードは、リリース８サービングＧＰＲＳサービスノード（Ｒｅｌ８　ＳＧＳＮ）、プレリリース８ＳＧＳＮ（Ｐｒｅ－Ｒｅｌ８　ＳＧＳＮ）、及びＥＰＳ移動管理エンティティ（ＭＭＥ）を含む
ことを特徴とする請求項７に記載の認証サーバ。
【請求項９】
前記アイデンティティモジュールは、ＵＭＴＳ加入者アイデンティティモジュール（ＵＳＩＭ）と拡張ＳＩＭ／ＵＳＩＭ（ｘＳＩＭ）を有する
ことを特徴とする請求項８に記載の認証サーバ。
【請求項１０】
認証サーバ（２５）から認証データを受信し、移動端末（５３）を認証するための認証ノード（４３、４４）であって、
前記認証データを受信し、該認証データの一部である第１キー（Ｓ，Ｓ１）を記憶する手段と、

前記第１キー（Ｓ，Ｓ１）から、第２キー（Ｓ２）を暗号として導出する第１キー分離手段と、
前記移動端末（５３）を認証する認証手段（４４）と、
異なるタイプの複数の他の認証ノードに前記第２キー（Ｓ２）を通信する手段と、
前記第１キーから第３キーを暗号として導出する第２キー分離手段（Ｇ）と、
前記第３キーを利用して前記移動端末と通信するセキュリティ処理ノードへ、該第３キーを通信する手段と
を備えることを特徴とする認証ノード。
【請求項１１】
前記第１キー分離手段は、３ＧＰＰ　リリース８サービングＧＰＲＳサービスノード（Ｒｅｌ８　ＳＧＳＮ）、プレリリース８ＳＧＳＮ（Ｐｒｅ－Ｒｅｌ８　ＳＧＳＮ）、及びＥＰＳ移動管理エンティティ（ＭＭＥ）用に、異なる第２キーを暗号として導出するように構成されている
ことを特徴とする請求項１０に記載の認証ノード。
【請求項１２】
前記複数の他の認証ノードに前記第２キー（Ｓ２）を通信する手段は、更に、前記他の認証ノードがＲｅｌ８　ＳＧＳＮあるいはＭＭＥである場合は、前記第２キーが再度変換されるか否かを示す情報を送信する
ことを特徴とする請求項１１に記載の認証ノード。
【請求項１３】
前記複数の他の認証ノードに前記第２キー（Ｓ２）を通信する手段は、更に、前記移動端末で利用されるアイデンティティモジュールのバージョンを示す情報を送信し、それによって、前記他の認証ノードと前記移動端末間のキー分離機能の同期を可能にする
ことを特徴とする請求項１０に記載の認証ノード。
【請求項１４】
認証サーバ（２５）と、異なるアクセスネットワーク（２２、２３）にある第１、第２及び第３のタイプ（４２、４３、４４）の複数の認証ノード間で認証データを共有するシステムであって、
前記認証ノードは、異なるバージョンの複数の移動端末（４１、５１、５２、５３）で利用される異なるバージョンのアイデンティティモジュールを認証し、
前記システムは、
前記認証サーバにおいて、
マスターキー（Ｓ）を生成する手段と、
前記認証ノードのタイプと前記アイデンティティモジュールのバージョンの異なる組み合わせそれぞれに対する、異なる変換されたキー（Ｓ，Ｓ１、Ｓ２）を、前記マスターキーから暗号として導出する第１キー分離手段と、
前記認証ノードによって認証される、前記認証ノードのタイプと前記アイデンティティモジュールのバージョンの組み合わせに対して導出される前記変換されたキー（Ｓ，Ｓ１、Ｓ２）を、前記タイプの前記認証ノードに提供する手段とを備え、
前記複数の認証ノードそれぞれは、
別の認証ノードから認証データ用のリクエストを受信する手段と、
前記変換されたキーを、前記リクエストの送信元の認証ノードへ送信する手段と
を備えることを特徴とするシステム。
【請求項１５】
前記第１、第２及び第３のタイプの認証ノードは、３ＧＰＰ　リリース８サービングＧＰＲＳサービスノード（Ｒｅｌ８　ＳＧＳＮ）、プレリリース８ＳＧＳＮ（Ｐｒｅ－Ｒｅｌ８　ＳＧＳＮ）、及びＥＰＳ移動管理エンティティ（ＭＭＥ）である
ことを特徴とする請求項１４に記載のシステム。
【請求項１６】
Ｒｅｌ８　ＳＧＳＮとＭＭＥそれぞれは、前記変換されたキーを暗号として処理した後

、その暗号として処理された変換されたキーを前記リクエストの送信元の認証ノードへ送信する第２キー分離手段を含む
ことを特徴とする請求項１５に記載のシステム。
【請求項１７】
Ｒｅｌ８　ＳＧＳＮとＭＭＥそれぞれは、前記第１キーを処理した後、その処理された第１キーを、前記移動端末とセキュアな通信を行なうセキュリティ処理ノードへ送信する第３キー分離手段を含む
ことを特徴とする請求項１６に記載のシステム。
【請求項１８】
Ｒｅｌ８　ＳＧＳＮとＭＭＥそれぞれは、受信する認証データに関連付けられているマーカを保持する手段を更に含み、
前記マーカは、前記認証データのソースについての情報を含む
ことを特徴とする請求項１６に記載のシステム。
【請求項１９】
前記認証ノードは、３ＧＰＰ　リリース８サービングＧＰＲＳサービスノード（Ｒｅｌ８　ＳＧＳＮ）、プレリリース８ＳＧＳＮ（Ｐｒｅ－Ｒｅｌ８　ＳＧＳＮ）、及びＥＰＳ移動管理エンティティ（ＭＭＥ）用に、異なる変換されたキーを暗号として導出するように構成されている
ことを特徴とする請求項１８に記載のシステム。
【請求項２０】
前記認証ノードにおける前記送信する手段は、更に、前記リクエストの送信元の認証ノードがＲｅｌ８　ＳＧＳＮあるいはＭＭＥである場合は、前記変換されたキーが再度変換されるか否かを示す情報を送信する
ことを特徴とする請求項１９に記載のシステム。
【請求項２１】
前記認証ノードにおける前記送信する手段は、更に、認証されている移動端末で利用される前記アイデンティティモジュールのバージョンを示す情報を送信する
ことを特徴とする請求項１４に記載のシステム。
【請求項２２】
前記認証サーバにおける前記提供する手段は、更に、前記変換されたキーが導出された前記アイデンティティモジュールのバージョンを示す情報を送信する
ことを特徴とする請求項１４に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願のクロスリファレンス
本願は、２００６年１０月１８日出願の米国仮特許出願第６０／８２９，９５４号の優先権を主張するものであり、その開示は参照することによって本明細書に組み込まれものである。
【０００２】
本発明は、通信ネットワークにおけるセキュア通信に関するものである。より詳細には、限定するものではないが、本発明は、ユーザ端末、アクセスネットワークおよびコアネットワークの様々な組み合わせにわたり、暗号キーを管理するためのシステムおよび方法に向けられたものである。
【背景技術】
【０００３】
図１は、第３世代パートナシッププロジェクト（３ＧＰＰ：Ｔｈｉｒｄ　Ｇｅｎｅｒａｔｉｏｎ　Ｐａｒｔｎｅｒｓｈｉｐ　Ｐｒｏｊｅｃｔ）によって現在定義されるような、進化型パケット・コア・ネットワーク（ＥＰＣ：Ｅｖｏｌｖｅｄ　Ｐａｃｋｅｔ　Ｃｏｒｅ　ｎｅｔｗｏｒｋ）および進化型ＵＴＲＡＮ無線アクセスネットワークの展開（Ｅ－Ｕ

ＴＲＡＮ：Ｅｖｏｌｖｅｄ ＵＴＲＡＮ ｒａｄｉｏ ａｃｃｅｓｓ ｎｅｔｗｏｒｋ）用の、現行の３Ｇネットワークの進化型に関する単純化ブロック図である。この進化型のシステム（ＥＰＣおよびＥ－ＵＴＲＡＮ）の全体は、進化型のパケットシステム（ＥＰＳ：Ｅｖｏｌｖｅｄ Ｐａｃｋｅｔ Ｓｙｓｔｅｍ）１０として参照される。本発明の重要な機能エンティティである、ＥＰＳアーキテクチャのノードは、移動管理エンティティ（ＭＭＥ：Ｍｏｂｉｌｉｔｙ Ｍａｎａｇｅｍｅｎｔ Ｅｎｔｉｔｙ）１１および拡張ノードＢ（ｅＮｏｄｅＢまたはｅＮＢ）１２を含んでいる。完全を期すために（本発明にとっては本質的ではないが）、２つのゲートウェイノードとして、サービング（serving）ゲートウェイ１３およびパケット・データ・ネットワーク（ＰＤＮ：Ｐａｃｋｅｔ Ｄａｔａ Ｎｅｔｗｏｒｋ）ゲートウェイ１４もまた存在することを言及するのは当然である。ＭＭＥ１１は、サービングＧＰＲＳサービスノード（ＳＧＳＮ：Ｓｅｒｖｉｎｇ ＧＰＲＳ Ｓｅｒｖｉｃｅ Ｎｏｄｅ）１５の制御プレーンに類似していて、ユーザ認証を実行し、非アクセス層（ＮＡＳ：Ｎｏｎ－Ａｃｃｅｓｓ Ｓｔｒａｔｕｍ）のシグナリングのセキュリティおよびその類を終結させる。この説明のために、ｅＮＢ１２は、２つの部分に論理的に分けられると見做すことができる。まず、ユーザ・プレーン・エンティティ（ＵＰＥ：Ｕｓｅｒ Ｐｌａｎｅ Ｅｎｔｉｔｙ）１６は、ＲＮＣおよびＳＧＳＮのユーザプレーンに類似していて、また、ＵＰ（Ｕｓｅｒ Ｐｌａｎｅ：ユーザプレーン）のセキュリティを終結させる。本発明に関係するＵＰＥ機能は、ｅＮＢまたはネットワークの何処かに実装することができる。ｅＮＢのその他の論理的な部分は、無線リソース制御（ＲＲＣ：Ｒａｄｉｏ Ｒｅｓｏｕｒｃｅ Ｃｏｎｔｒｏｌ）セキュリティ１７を終結させるエンティティである。ホーム加入者サーバ（ＨＳＳ：Ｈｏｍｅ Ｓｕｂｓｃｒｉｂｅｒ Ｓｅｒｖｅｒ）１８は、加入者プロファイル情報を記憶している。

【０００４】

ＥＰＳアーキテクチャ１０は、「レガシー」（３ＧＰＰ Ｒｅｌ６）コアネットワーク機器および、ＧＳＭ／ＥＤＧＥ無線アクセスネットワーク（ＧＥＲＡＮ：ＧＳＭ／ＥＤＧＥ Ｒａｄｉｏ Ａｃｃｅｓｓ Ｎｅｔｗｏｒｋ）１９およびＵＭＴＳ地上無線アクセスネットワーク（ＵＴＲＡＮ：UMTS Ｔｅｒｒｅｓｔｒｉａｌ Ｒａｄｉｏ Ａｃｃｅｓｓ Ｎｅｔｗｏｒｋ）２０等の関係する無線アクセスネットワークと、効果的およびセキュアに相互動作しなければならない。「効果的」とは、ハンドオーバがシームレスであることを意味し、「セキュアに」とは、１つのアクセスネットワークにおけるセキュリティ暴露（security compromise）が他のアクセスネットワーク（後方交換性であることの必要性によって影響される以上に）に広がらないことを意味する。ＥＰＳアーキテクチャは、セキュリティの基礎として、ユーザ機器（ＵＥ：Ｕｓｅｒ Ｅｑｕｉｐｍｅｎｔ）２１におけるＲｅｌ８タイプの加入者アイデンティティモジュール（ＳＩＭ：Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）メカニズムを使用するであろうと想定している。現在、Ｒ９９＋ＵＳＩＭの使用のみが、ＥＰＳに対して指定されているが、一実施形態では、ＳＩＭは、以下では、ｘＳＩＭと示される「拡張」加入者アイデンティティモジュール／ＵＭＴＳ加入者アイデンティティモジュール（ＳＩＭ／ＵＳＩＭ）であっても良い。

【０００５】

用語「Ｒｅｌ６」は、３ＧＰＰリリース６またはそれ以前の機器を意味する。ＥＰＣノードおよび任意のＵＭＴＳ／ＧＳＭコアネットワーク機器を参照するために、用語「Ｒｅｌ８」が本明細書で利用される。これらの機器は、「ＥＰＳを認知するもの（aware：アウェア）」とされていて、従って、ＥＰＳアーキテクチャと相互動作することができる。例えば、Ｒｅｌ６ ＳＧＳＮは、必要なプロトコルを実装しないので、ＥＰＣノードへハンドオーバすることができないことが想定されている。しかしながら、Ｒｅｌ８ ＳＧＳＮは、いわゆる、Ｓ３およびＳ４インタフェースの実装によりハンドオーバの実行が可能であると想定されている。

【０００６】

３ＧＰＰでは、以下の要件を満足することが、ＥＰＳアーキテクチャにおけるセキュア

通信に望ましいと一般的に合意されている。

【０００７】

・拡張ｘＳＩＭは、使用される場合には、ＵＴＲＡＮ／ＧＥＲＡＮ用にＵＳＩＭと後方互換性がなければならず、キーは、初期認証を行う場所（ＧＥＲＡＮ、ＵＴＲＡＮまたはＥ－ＵＴＲＡＮ）とは独立していなければならない。認証パラメータは、同一フォーマットおよび、その類を有することになろう。

【０００８】

・解決策は、以下の８つの全ての組み合わせに対して動作しなければならない。

【０００９】

・Ｒｅｌ６またはＲｅｌ８　ＵＥ

・ｘＳＩＭまたはＵＳＩＭ

・Ｒｅｌ６またはＲｅｌ８　ＳＧＳＮ

Ｒｅｌ６　ＵＥは、Ｅ－ＵＴＲＡＮ無線インタフェースを単にサポートしないので、解決策は、Ｒｅｌ６　ＵＥとｅＮＢ／Ｅ－ＵＴＲＡＮとの組み合わせと共に動作することは要求されない。

【００１０】

・解決策は、Ｒｅｌ８　ＥＰＳ　ＵＥおよびｘＳＩＭ／ＵＳＩＭ並びにＲｅｌ６　ＳＧＳＮ、Ｒｅｌ８　ＳＧＳＮまたはＥＰＣＭＭＥの６つの構成のいずれかを含む全ての組み合わせに対して動作しなければならない。

【００１１】

・解決策は、Ｒｅｌ６　ＲＡＮまたはＣＮ装置のアップグレードを行うことなく動作しなければならない。但し、Ｒｅｌ８　ＣＮ機器の新機能は許容される。

【００１２】

・Ｒｅｌ８環境（ＳＧＳＮおよびＥＰＣ　ＭＭＥ）において初期接続およびハンドオーバ（Ｈ／Ｏ）が発生する場合、ＵＴＲＡＮ／ＧＥＲＡＮネットワークとＥ－ＵＴＲＡＮネットワークとの間で進行する場合のキー分離がサポートされなければならない。（キー分離とは、１つのキーの公開（exposure）が、別のキーに影響しないことを意味する。）

・ＥＰＳアーキテクチャは、ＵＰ、ＮＡＳおよびＲＲＣキーのキー分離をサポートすることになろう。

【００１３】

・Ｅ－ＵＴＲＡＮ　ｅＮｏｄｅＢキーの公開の影響は、限定的であろう（ＲＲＣのセキュリティは、アイドルからアクティブへの移行時に再確立される）。

【００１４】

追加要件として、拡張ｘＳＩＭは、アクセス認証時に導出される「マスターキー」を提供し、アクセスキーが公開されるとしてもマスターキーがアプリケーション・レイヤにおいてセキュアに使用することができるとすれば有益であろう。同様に、ｘＳＩＭが１２８ビットを上回る実効キーサイズをサポートすることができるとすれば望ましいであろう。

【００１５】

以上の全ての要件を満足する既存の解決策は存在しない。ＧＳＭ／ＵＭＴＳの相互動作のために使用されるものと同様の原理を採用することができないのは、それら原理が要求されるセキュリティレベルを提供しないからである。ＧＳＭおよびＵＭＴＳは効果的な相互動作解決策を指定するしかしながら、ＧＳＭおよびＵＭＴＳは、アクセス間のキー分離を提供しないので、ＧＳＭのセキュリティ暴露は、ＵＭＴＳのセキュリティにある程度の影響を及ぼすことになる。例えば、ＧＳＭ／ＵＭＴＳによって提供されるキーは、セキュリティ暴露のリスクなしでは、アプリケーション・レイヤにおいて再使用することができない。加えて、ＧＳＭもＵＭＴＳも、１２８ビット以上のセキュリティを提供しない。

【００１６】

本技術に必要とされるものは、ユーザ端末、アクセスネットワークおよびコアネットワークの様々な組み合わせに渡る、暗号キーを管理するための効果的でかつセキュアなシステムおよび方法である。このシステムおよび方法は、３ＧＰＰＥＰＳ要件の全てを満すべ

きである。本発明は、そのようなシステムおよび方法を提供し、追加の要件を満足するｘＳＩＭを後に導入するためのプロビジョン（provision）を実現する。
【先行技術文献】
【特許文献】
【００１７】
【特許文献１】米国特許仮出願第６０／８２９，９５４号
【発明の概要】
【発明が解決しようとする課題】
【００１８】
本発明は、ユーザ端末、アクセスネットワークおよびコアネットワークの様々な組み合わせに渡って、暗号キーを管理する認証サーバ及びシステム、および方法に向けられたものである。本発明は、上述で挙げられている３ＧＰＰ　ＥＰＳ要件の全てを満足するので、従来技術の解決策を越える利点を有する。本発明は、これを主として、アクセスネットワーク間のキー分離の提供によって行う。
【課題を解決するための手段】
【００１９】
一態様では、本発明は、第１のアクセスネットワークにおける所与の認証ノードに認証データを配信する認証サーバの方法に向けられたものである。この所与の認証ノードは、様々なアクセスネットワークにおける様々なタイプの複数の認証ノードの１つである。この認証ノードは、複数の様々なバージョンの移動端末において利用される、異なるバージョンのアイデンティティモジュールを認証する。本方法は、認証サーバにおいてマスターキーを生成する工程と、マスターキーから様々な認証データを暗号として導出する工程および導出された認証データを認証ノードに選択的に提供する工程を含んでいる。キー分離処理は、認証ノードのタイプとアイデンティティモジュールのバージョンのそれぞれ異なる組み合わせに対して、変換されたキーを含む異なる認証データを導出する。本方法は、次いで、所与の認証ノードのタイプと、所与の認証ノードによって認証されるアイデンティティモジュールのバージョンとの組み合わせに対して導出される認証データを、所与の認証ノードに選択的に提供する。
【００２０】
別の態様では、本発明は、第１のアクセスネットワークにおける所与の認証ノードに認証データを配信する認証サーバに向けられたものである。ここで、所与の認証ノードは、様々なアクセスネットワークにおける様々なタイプの複数の認証ノードの１つである。認証ノードは、複数の様々なバージョンの移動端末において利用される様々なバージョンのアイデンティティモジュールを認証する。認証サーバは、マスターキーを生成する手段、マスターキーから、認証ノードのタイプとアイデンティティモジュールのバージョンとのそれぞれ異なる組み合わせに対して異なる認証データを暗号として導出するキー分離手段と、および所与の認証ノードのタイプと所与の認証ノードが認証するアイデンティティモジュールのバージョンとの組み合わせに対して導出される認証データを所与の認証ノードに提供する手段を含んでいる。
【００２１】
別の態様では、本発明は、認証サーバから認証データを受信し、移動端末を認証するための認証ノードに向けられたものである。認証ノードは、認証データを受信し、認証データの一部である第１のキーを記憶する手段と、第１のキーから第２のキーを暗号として導出する第１のキー分離手段と、および移動端末を認証する認証手段を含んでいる。認証ノードは、また、様々なタイプの複数の他の認証ノードに第２のキーを通信する手段と、第１のキーから第３のキーを暗号として導出する第２のキー分離手段と、および第３のキーを利用して移動端末と通信するセキュリティ処理ノードに第３のキーを通信する手段とを含んでいる。
【００２２】
別の態様では、本発明は、認証サーバと、様々なアクセスネットワークにおける第１の

、第２のおよび第３のタイプの複数の認証ノードとの間で認証データを共有するシステムに向けられたものである。認証ノードは、複数の異なるバージョンの移動端末のバージョンにおいて利用される、様々なバージョンのアイデンティティモジュールを認証する。本システムは、認証サーバにおいてマスターキーを生成する手段と、マスターキーから、認証ノードのタイプとアイデンティティモジュールのバージョンとのそれぞれ異なる組み合わせに対して異なる変換されたキーを暗号として導出する第１キー分離手段と、および所与のタイプの認証ノードと、所与の認証ノードによって認証されるアイデンティティモジュールのバージョンとの組み合わせに対して導出される、変換されたキーを所与のタイプの認証ノードに提供する手段を含んでいる。本システムは、複数の認証ノードのそれぞれにおいて、別の認証ノードから認証データ用のリクエストを受信する手段と、および変換されたキーをリクエストの送信元の別の認証ノードに転送する手段を含んでいる。

【００２３】

一実施形態では、第１の、第２のおよび第３のタイプの認証ノードは、リリース６サービングＧＰＲＳサービスノード（Ｒｅｌ６　ＳＧＳＮ）、リリース８サービングＧＰＲＳサービスノード（Ｒｅｌ８　ＳＧＳＮ）およびＥＰＣ移動管理エンティティ（ＭＭＥ）である。それぞれＲｅｌ８　ＳＧＳＮおよびＭＭＥは、変換されたキーを暗号として処理した後に、暗号としてその処理した変換されたキーをリクエストの送信元の認証ノードに転送する手段を含んでいる。

【００２４】

以下では、添付する図面を参照する好ましい実施形態の図示により、本発明の本質的特徴を詳細に説明することにする。

【図面の簡単な説明】

【００２５】

【図１】３ＧＰＰによって現在定義される進化型パケット・コア・ネットワーク（ＥＰＣ）および進化型ＵＴＲＡＮ（Ｅ－ＵＴＲＡＮ）無線アクセスネットワークを備える進化型パケットシステム（ＥＰＳ）アーキテクチャ用のシステムアーキテクチャに関する単純化ブロック図である。

【図２】例示的な実施形態における本発明の基本原理を示す単純化ブロック図である。

【図３】マスターキー（Ｍｋ）を変換コーダエンティティ（ＴＣＥ）に記憶する方法およびキー分離を達成する方法を示す単純化ブロック図である。

【図４】ｘＳＩＭを利用するＲｅｌ８　ＵＥの初期認証を示す単純化ブロック図である。

【図５】ｘＳＩＭを利用するＲｅｌ６　ＵＥの初期認証を示す単純化ブロック図である。

【図６】ＵＳＩＭを利用するＲｅｌ６　ＵＥの初期認証を示す単純化ブロック図である。

【図７】ＵＳＩＭを利用するＲｅｌ８　ＵＥの初期認証を示す単純化ブロック図である。

【図８】様々なシステム間の認証ベクトル（ＡＶ）の転送を示す単純化ブロック図である。

【図９】コンテキストがソースからターゲットシステムに転送され、また、転送されたキーが明示的な再認証することなくターゲットシステムによる即時使用に供する場合のアクセス間コンテキスト転送処理を示す単純化ブロック図である。

【発明を実施するための形態】

【００２６】

本発明は、ユーザ端末、アクセスネットワークおよびコアネットワークの様々な組み合わせに渡って、暗号キーを管理するための、認証サーバ及びシステム、および方法に向けられたものである。本発明は、主として、アクセスネットワーク間のキー分離の提供によって、上述で挙げられている３ＧＰＰ　ＥＰＳの要件の全てを満足する。これは、まず、認証手順中にキーを導出するために使用されるマスターキー（Ｍｋ）の導入によって達成される。様々なアクセスタイプ間のハンドオーバ中に、ＵＥがアクセスを変更すると、それぞれのアクセスネットワークにおいてキーを保持する２つのノード間で、Ｍｋまたは変換されたＭｋが受け渡される。Ｍｋの変換は、一方向性関数を介して実行され、また、Ｍｋが何らかの形で暴露（漏洩）される（compromise）と、従前に使用されているマスター

キーへのアクセスを自動的に取得することが可能でないという影響を有している。Ｍｋは決して直接使用されるものでなく、アクセスリンクを保護するために直接使用されるキーを導出するためだけに使用される。

【００２７】

図２は、例示的実施形態における本発明の基本原理を示す単純化ブロック図である。この例で、ＵＥ２１は、Ｒｅｌ８　ＵＴＲＡＮネットワーク２２およびＥ－ＵＴＲＡＮネットワーク２３にアクセスする。変換コーダエンティティ（ＴＣＥ：Ｔｒａｎｓｆｏｒｍａｔｉｏｎ　Ｃｏｄｅｒ　Ｅｎｔｉｔｙ）２５と呼ばれるホーム加入者サブシステム（ＨＳＳ）に近い機能からＵＴＲＡＮネットワークおよびＥ－ＵＴＲＡＮネットワークにＭｋ２４が配信される。ＴＣＥは論理機能であり、一実施形態では、ＨＳＳと共存していても良い。Ｍｋは、各アクセスタイプに対して異なっていても良い。Ｒｅｌ８　ＵＴＲＡＮでは、Ｍｋは関数ｆ１で変換され、ｆ１（Ｍｋ）２６はＵＥと共有される。一方、Ｅ－ＵＴＲＡＮに対しては、Ｍｋは、関数ｆ２で変換され、ｆ２（Ｍｋ）２７をＵＥと共有する。一実施形態では、ｆ１はｆ２と等しいが、別の実施形態では、ｆ１とｆ２は異なる関数である。ＴＣＥ２５は、認証およびキー合意（協定）（ＡＫＡ：Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　Ｋｅｙ　Ａｇｒｅｅｍｅｎｔ）２８を使用してＵＥの認証データを生成する。

【００２８】

キー分離に加えて、本システムは、また、アプリケーションサーバおよびアプリケーションがＵＥにおいて動作して、特定アプリケーションキーの取得および利用を可能にする。アプリケーションキーは、ＴＣＥまたはＨＳＳによって導出／記憶することができる。

【００２９】

図３は、マスターキー（Ｍｋ）２４をＴＣＥ２５に記憶する方法およびキー分離を達成する方法を示す単純化ブロック図である。図におけるイベントフローは以下の通りである：

１．ネットワーク１３２のノードＡ１３１は、ＴＣＥ２５から認証ベクトル（ＡＶ：ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｖｅｃｔｏｒ）を要求する。

【００３０】

２．一方向性関数（ＵＥ２１には既知）またはアイデンティティマッピングのいずれかを使用してＳ１＝ｆ（Ｍｋ）３３を取得するために、ＴＣＥは、ＡＶのＭｋを変換する。ＴＣＥは、ＵＥ用のアプリケーション・レイヤに対するキーをさらに導出するために使用することができるキーとして使用されるＭｋを記憶する。

【００３１】

３．ＴＣＥは、Ｓ１をノードＡ１に送信する。

【００３２】

４．ノードＡ１は、ＵＥに対しＡＫＡを実行し、ＵＥは、局所的に、ＭｋおよびＳ１の双方を導出する。ノードＡ１は、Ｓ１から必要なトラフィック保護キーを導出し、この保護キーを必要とするノードにこの保護キーを転送する。このことは、図３のｆ１関数によって示される。ＵＥは、対応するキーを同様に導出する。

【００３３】

５．次に、ＵＥ２１は、アクセスタイプ２（ネットワーク２）３４へのハンドオーバを実行する。次いで、ノードＡ１は、一方向性関数Ｇをキー Ｓ１に適用し、その結果であるＳ１*＝Ｇ（Ｓ１）３５をノードＡ２３６に送信する。ＵＥは、同様にＧ関数を使用してＳ１を変換する。

【００３４】

６．ノードＡ２およびＵＥは、新規アクセスネットワークにおけるトラフィックを保護するために要求される必要なキーを導出する。ネットワーク２がネットワーク１と比較して異なるタイプのアクセスネットワークである場合、ノードＡ２およびＵＥは、ノードＡ１によって実行されるものとは異なるキーの導出を実行することができる。このことは、図における関数ｆ２によって示される。２つのネットワークが同一のタイプである場合

、ｆ１はｆ２に等しく、Ｇは異なるネットワークにおいて使用されるキーが異なることを保証することになる。２つのネットワークが異なる場合、ｆ１およびｆ２は、現在とは分離するキーを暗号として導出することができ、Ｇは、アイデンティティマッピングによって実現することができる。しかしながら、Ｓ１が暴露される場合、Ｇは過去の暗号化トラフィックを回復することが可能でないという特徴を追加することに注意されたい。将来のトラフィックのみが、暴露される。

【００３５】

ＵＥ２１が、さらに別のネットワークにハンドオーバする場合、ステップ５およびステップ６が繰り返される。

【００３６】

以下で後述するように、キーの導出および変換は大いなる注意を持って設計し、かつレガシーシステムとの後方互換性を許容しなければならない。本発明は、本明細書では、ＵＴＲＡＮ　Ｒｅｌ６、ＵＴＲＡＮ　Ｒｅｌ８およびＥ－ＵＴＲＡＮのコンテキストで説明することにするが、この説明は、本発明の単なる例示であることが理解されるべきである。

【００３７】

考慮すべき「セキュリティデータ」の２つのセットがある。認証ベクトル（ＡＶ）は、セキュリティデータおよびまだ使用されていないキーを含んでいる。ＡＶは、初期認証時にＨＳＳからＳＧＳＮまたはＭＭＥ（ＳＧＳＮまたはＭＭＥは、訪問先ネットワークに存在していないことに注意されたい）へ送信され、１つのＡＶは、後続の各認証において「消費」される。認証においては、ＵＥを最後に認証したＳＧＳＮまたはＭＭＥに記憶される未使用ＡＶが、認証エンティティによって要求されることがありえ、その場合、未使用ＡＶが送信される。本発明のＡＶは、ＵＭＴＳのフォーマットに類似のフォーマット：（ＲＡＮＤ、ＸＲＥＳ、ＡＵＴＮ、「キー」）を有する。ＵＭＴＳでは、「キー」は単にＣｋ、Ｉｋであるが、以下では、このキー要素を「Ｓ」と呼ぶことにする。

【００３８】

本発明の目的のために、セキュリティコンテキストは、現在「アクティブ」キーを含んでいる。セキュリティコンテキストは、また、本発明には本質的ではない、他のデータも含む場合もある。明示的な（再）認証なしにハンドオーバを可能にするために、セキュリティコンテキストは、ソースからターゲットシステムに送信される。

【００３９】

様々なアクセスに介するキーの使用に伴う問題を把握するために、以下の定義を利用する：

・セキュリティコンテキスト／ＡＶのキーを生成するための要素（Ｓ）が［Ｃｋ，Ｉｋ］（ＵＴＲＡＮ）またはＫｃ（ＧＥＲＡＮ）として使用している、または後に直接（さらなる暗号保護なしに）使用することができる場合、セキュリティコンテキスト／ＡＶは「ダーティ（Dirty）」と呼ばれる。Ｅ－ＵＴＲＡＮにおいて、ダーティコンテキストを使用することが可能である（但し、推奨しない）ことに注意されたい。

【００４０】

・［Ｃｋ、Ｉｋ］若しくはＫｃまたはＥ－ＵＴＲＡＮにおける対応するキー群が、そのキーを生成するための要素（Ｓ）から、セキュアな暗号「トゥイーキング（tweaking）」機能のアプリケーションによって導出されている、または導出されるることになる場合、セキュリティコンテキスト／ＡＶは「クリーン（Clean）」と呼ばれる。

【００４１】

完全な解決策を説明するために、３つの問題に取り組まなければならない：

１．ＡＶが、どのようにして初期認証において生成され、ＨＳＳからＳＧＳＮ／ＭＭＥに転送されるか（図４－図７および表１）。

【００４２】

２．（未使用）ＡＶが、ハンドオーバにおいて、どのように送信され、変換されるか（図８および表２）。

【００４３】
３．現在使用されるセキュリティコンテキストが、ハンドオーバにおいて、どのように送信され、変換されるか（図９）。
【００４４】
認証およびキー合意（ＡＫＡ）手順に関して、以下の仮定を設ける：
・Ｒｅｌ８　ＵＥは、Ｒｅｌ６　ＳＧＳＮ、Ｒｅｌ８　ＳＧＳＮまたはＭＭＥに対してＡＫＡを実行するかを知ることになるであろう。ＡＫＡがＲｅｌ６　ＳＧＳＮに対して実行される場合、セキュリティコンテキストは、ダーティとなる：その他の場合、セキュリティコンテキストは、クリーンとなる。ＵＥがＵＭＴＳ　ＡＫＡ（Ｒｅｌ９９＋ＳＧＳＮ）またはＧＳＭ　ＡＫＡ（Ｒｅｌ９８－ＳＧＳＮ）を実行すべきかを知らなければならない場合、この処理は、現行ＧＳＭ／ＵＭＴＳ相互動作に類似する。
【００４５】
・Ｒｅｌ６　ＵＥは、Ｒｅｌ８　ＳＧＳＮをＲｅｌ６　ＳＧＳＮと区別することができないであろう。
【００４６】
・ＨＳＳは、ＳＩＭ（ｘＳＩＭまたはＵＳＩＭ）のバージョンを知ることになろう。この知識は、ＨＳＳ近傍のネットワークノードに送信することができる（例えば、ＩＭＳＩからまたは明示的なシグナリングにより）と想定する。情報がＲｅｌ８　ＳＧＳＮ／ＭＭＥに（およびその間で）渡されることもまた必要である。
【００４７】
・ＳＧＳＮ／ＭＭＥは、ＵＥのＡＫＡ機能を知ることになるであろう。ネットワーク接続時にＵＥから送信されるクラスマーク情報からおよび／またはＨＳＳからの情報から、この情報が取得されると（今日のように）想定する。Ｒｅｌ６　ＳＧＳＮは、Ｒｅｌ８　ＵＥが、Ｒｅｌ６　ＵＭＴＳ　ＡＫＡが可能であることをただ認識するのみであろうことに注意されたい。
【００４８】
・ｘＳＩＭは、ｘＳＩＭが「実際の」Ｒｅｌ８　ｘＳＩＭとして使用されるか、またはレガシーのＲｅｌ６　ＵＥにおいて使用されるかを、ｘＳＩＭに告げることで、ＵＳＩＭをシミュレートすることを必要とする２つの論理Ｉ／Ｏインタフェースを有することになろう。逆に、Ｒｅｌ８　ＵＥは、ｘＳＩＭをＵＳＩＭと区別することができると想定することができる。
【００４９】
以上のクリーン／ダーティの定義により、本発明は以下の点を満足する：
・ＡＫＡが（ＥＰＳ）ＭＭＥに対して実行される場合、Ｒｅｌ８　ＵＥは使用中でなければならず、クリーンコンテキストは、ｘＳＩＭおよびＵＳＩＭ双方に対して確立することができる。
【００５０】
・ＡＫＡがＲｅｌ８　ＳＧＳＮに対して実行される場合、コンテキストは、ＵＥの能力（Ｒｅｌ８またはＲｅｌ６）に依存してクリーンまたはダーティとなる。
【００５１】
・ＡＫＡがＲｅｌ６　ＳＧＳＮに対して実行される場合、コンテキストは、常にダーティとなる。ｘＳＩＭの場合、ｘＳＩＭは、このことが生じるかを知っているであろうし、以下に説明するように対処することができる。
【００５２】
以下では、ソース／ターゲットアクセスシステム間のコンテキスト送信に対する仮定（または以上の結果）である。
【００５３】
・Ｒｅｌ６　ＳＧＳＮにおいて取り扱われるセキュリティコンテキストは、（定義により）「ダーティ」である。
【００５４】

・ハンドオーバでは、ソースＭＭＥまたはＲｅｌ８　ＳＧＳＮは、（新規機能を含むと想定することができるので）セキュリティコンテキストが、Ｒｅｌ６　ＳＧＳＮ、Ｒｅｌ８　ＳＧＳＮまたはターゲットＭＭＥに送信されるかを知ることになる。ソースシステムによるコンテキスト変換は、状況に依存することになる。

【００５５】

・ハンドオーバでは、ターゲットＭＭＥまたはＲｅｌ８　ＳＧＳＮは、セキュリティコンテキストがＲｅｌ６　ＳＧＳＮ、Ｒｅｌ８　ＳＧＳＮまたはソースＭＭＥから到来するかを同様に知ることになるであろう。

【００５６】

・Ｒｅｌ８　ＳＧＳＮのみがターゲットＥ－ＵＴＲＡＮシステムへのハンドオーバを実行することができ、セキュリティコンテキストをＭＭＥに送信することができる、これは、新規のシグナリング信号（Ｒｅｌ６　ＳＧＳＮでは存在しない）が必要されるからである。

【００５７】

・ＭＭＥおよびＲｅｌ８　ＳＧＳＮは、相互間で（明示的なシグナリングによって）送信される場合、セキュリティコンテキストが「クリーン」または「ダーティ」であるかを指示することができる。このことは「最適」な場合である、それは、ソースおよびターゲットシステム双方が新規の機能をサポートすることができるからである。

【００５８】

・Ｒｅｌ８　ＵＥは、ハンドオーバがＲｅｌ８　ＳＧＳＮとＭＭＥとの間であると判定することができる。これは、ＵＥが無線技術の変更に気付くからである。おそらく必要ではないが、明示的な追加のシグナリングも存在しうる。同じことは、Ｒｅｌ６　ＳＧＳＮとＲｅｌ８　ＳＧＳＮとの間のハンドウオーバに対しては想定できない。これは、ＵＥが依然としてＵＴＲＡＮに存在するからである。一実施形態では、本発明は、ＵＥに、ハンドオーバがＲｅｌ６　ＳＧＳＮとＲｅｌ８　ＳＧＳＮとの間であることを判定することを可能にする新規のシグナリングによって、更に、改善される。

【００５９】

以下の説明では、名称Ｆ１、Ｆ２およびＧは、２５６ビットを２５６ビットにマッピングする、適切な暗号化関数を示している。ビット長は、２５６ビットとは異なる長さ（より長いまたはより短い）であってもよいが、２５６ビットは、３ＧＰＰ　ＳＡ３における現行の作業仮定であることに注意すべきである。これらのキービットから、追加キーを導出することができる。Ｆ３は、２５６ビットを６つ（迄）の２５６ビット・ストリング・セットにマッピングする関数である。（６番目のストリングの存在は、アクセス技術がユーザプレーン統合を実装するかに依存し、この統合は、Ｅ－ＵＴＲＡＮに対する事例ではない）。（選択的には、Ｆ３は、６つの異なる関数のセットを使用して実現することができる）。Ｆ－関数は、（未使用）ＡＶに適用される。一方、Ｇ－関数は、アクティブなセキュリティコンテキストに適用される。Ｆ２およびＦ３は、以下で説明されるように、セキュリティコンテキストにおいても使用される。

【００６０】

図４－図７では、セキュリティコンテキストおよびＡＶは、キーＳ１、Ｓ２およびＳによって示される。これは、これらは、キー導出によって影響を受ける唯一のパラメータ群であるからである。（少なくとも）４レベルのキー階層が導入される。ここで、「下位」キーは、「上位」キーから導出される。ｘＳＩＭが使用される場合、以下の全ての事項を適用する：

・Ｋは、内部のｘＳＩＭ／ＨＳＳキーである。

【００６１】

・Ｓは、ＡＫＡにおいてＫから導出され、ＨＰＬＭＮまたはｘＳＩＭの外部に決して晒されない「スーパキー」と見なすことができる。Ｓは、初期の３ＧＰＰ汎用ブートストラップアーキテクチャ（ＧＢＡ：Ｇｅｎｅｒｉｃ　Ｂｏｏｔｓｔｒａｐｐｉｎｇ　Ａｒｃｈｉｔｅｃｔｕｒｅ）手順によって生成されるキーに対する関数に類似している。

【００６２】
・Ｓ１は、Ｆ１を使用してＳから導出される「マスター・セッション・キー」であり、また、セッションキーを導出するために、Ｒｅｌ８　ＳＧＳＮおよびＥＰＳ　ＭＭＥによって使用される。
【００６３】
・Ｓ２は、Ｆ２を使用してＳ１から導出されるセッションキーである。
【００６４】
－　Ｅ－ＵＴＲＡＮに対しては、６つまでのトラフィックキーが必要とされる（ＵＰ、ＮＡＳおよびＲＲＣに対する完全性／秘匿キー群）。これらのさらなるキー群は、関数Ｆ３によってＳ２から導出される。
【００６５】
－　Ｒｅｌ６／Ｒｅｌ８　ＵＭＴＳに対しては、Ｓ２は、Ｒｅｌ８またはＲｅｌ６で使用される２つのトラフィックキー（Ｃｋ，Ｉｋ）に対応する。
【００６６】
端末側では、Ｒｅｌ８　ＵＥにおけるｘＳＩＭではなくＵＳＩＭが使用される場合、ＵＥは、依然として、下位のキーを「エミュレートする」（ＵＭＴＳ　ＵＥが、ＳＩＭに対するＵＳＩＭ機能をエミュレートする方法と同様）ことができる。しかしながら、ＵＥが、Ｒｅｌ６　ＵＥである場合、それはできない。この場合、Ｓは、単に以下に説明するように、ＵＳＩＭによって直接出力されるＣｋ‖Ｉｋとなるであろう。
【００６７】
同様に、ネットワーク側では、いくつかの場合、関数Ｆ１、Ｆ２およびＦ３をサポートしない、あるレガシーシステムにより、上述のキー階層は「崩壊する」であろう。より詳細には、このことは、Ｆ１、Ｆ２およびＦ３がＲｅｌ６システムにおける「平凡な」機能と考えることができることによるものである（例えば、Ｆ２（ｘ）＝ｘ、アイデンティティ）。Ｒｅｌ８　ＵＥ／ｘＳＩＭは、この状況に適合しなければならない。
【００６８】
従って、考慮しなければならない互換性についての多くの事例が存在する。以下の図は、ネットワーク側の３つの場合（Ｒｅｌ６、Ｒｅｌ８またはＭＭＥ）のＳＩＭ／ＵＥの組み合わせに関する、４つの取り得る変形に対する（初期）認証時のキー／ＡＶ処理の場合に応じた説明を示している。まず、いくつかのさらなる記法を説明することにする。
【００６９】
ＴＣＥ２５は、ＧＢＡブートストラップ手順におけるＫに類似する、アプリケーションキー（またはマスターキー）Ｓを保持する小さな楔（shim）レイヤであっても良い。ＴＣＥは、また、ＵＥにおけるＳＩＭのタイプに依存して、必要なキーの導出も実行する。ＴＣＥは、ＨＳＳ１８において、または別のエンティティとして実現されても良い。ＴＣＥは、ＵＥ２１のリリースバージョンを知らないので、ＴＣＥは、純粋にｘＳＩＭ／ＵＳＩＭバージョンに基づき、そのデータを送信しなければならない。
【００７０】
上述の議論では、Ｒｅｌ６ネットワークとＲｅｌ８ネットワークとの間を区別している。ＥＰＳと相互動作する必要があるＲｅｌ７ネットワークも存在している。この時、セキュリティの観点からは、Ｒｅｌ６からＲｅｌ７への大きな変更はないが、Ｒｅｌ７を未だ完全に定義されていない。従って、３ＧＰＰ　Ｒｅｌ７が、上述で議論されるような新規のキー管理機能を導入していない場合、上述の議論において、Ｒｅｌ６ネットワークが行うように、Ｒｅｌ７　３ＧＰＰネットワークは、ＥＰＳと正確に相互動作するであろう。一方、Ｒｅｌ７が、Ｒｅｌ８に対して想定する新規のキー管理機能を導入する場合、上述のＲｅｌ８が行うように、Ｒｅｌ７ネットワークはＥＰＳと正確に相互動作するであろう。要するに、導入する新規のキー管理機能が何であるかに依存して、ＥＰＳと相互動作するＲｅｌ７ネットワークは、Ｒｅｌ６ネットワークまたはＲｅｌ８ネットワークとして扱うことになろう。同じことが、後続の議論に対しても当てはまる。用語「プレＲｅｌ８（Pre-Rel8）」は、Ｒｅｌ８ノードに対して想定される新規のキー管理機能を導入しないＲ

ｅｌ６ノードまたはＲｅｌ７ノードを参照するために、本明細書で利用される。

【００７１】

図において、「ダーティ」および「クリーン」とマークされているボックスは、コンテキスト／ＡＶが、上述で定義されるクリーンまたはダーティであるかを示している。Ｒｅｌ６　ＳＧＳＮの場合、コンテキスト／ＡＶがクリーンであるかか否かを告げる明示的な「フラグ」は存在しない（常にダーティであるので）。但し、この情報は、非明示的にＲｅｌ８　ＳＧＳＮによって推論することができる。これは、Ｒｅｌ８　ＳＧＳＮが、コンテキスト／ＡＶをＲｅｌ６　ＳＧＳＮから受信しているからである。

【００７２】

簡単のため、図では、キーＳ２は、ＲＮＣ／ｅノードＢから送信されることだけを示している。Ｆ－関数を使用して、Ｓ２は、さらにトラフィックキー（ＧＥＲＡＮに対するＫｃ、ＵＴＲＡＮに対するＣＫ／ＩＫ、およびＥ－ＵＴＲＡＮに対するＵＰ／ＮＡＳ／ＲＲＣキー）に処理されることを注意されたい。保護用のエンドポイントは、ＥＰＳでは、様々なトラフィックのタイプに対して異なるので、この処理は、好ましくは、ＭＭＥにおいて実行され、処理結果が、保護エンドポイント（ｅノードＢ）に送信されても良いし、またはＳ２が与えられている場合には、ｅノードＢ自身によってＵＰ／ＲＲＣキー群を導出することができる。ＵＭＴＳに大使邸は、ＣＫおよびＩＫは、それぞれＳ２の第１のおよび第２の半分とすることができる。

【００７３】

処理は、まず、ＨＳＳ／ＳＧＳＮ／ＭＭＥのＡＶの部分であるキー、および（初期）認証時のキーＳＩＭ／ＵＥに対して説明する。図４－図７は、明示的な認証を示すことに注意すべきである。コンテキスト送信によって達成される非明示的な認証は、後述する。

【００７４】

図４は、ｘＳＩＭを利用するＲｅｌ８　ＵＥ４１の初期認証を示す単純化ブロック図である。ＵＥは、Ｒｅｌ６　ＳＧＳＮ４２、Ｒｅｌ８　ＳＧＳＮ４３およびＭＭＥ４４間を区別することができるので、ＵＥは、セキュリティコンテキストがダーティであるかクリーンであるか（即ち、ネットワークが、ＳＧＳＮ／ＭＭＥに記憶されるＳ１－キーを有するか）を保持する。ＵＥが、Ｒｅｌ６　ＳＧＳＮ４２と通信する場合、ＵＥは、コンテキストをダーティとしてマークする。ＵＥがＲｅｌ８　ＳＧＳＮ４３またはＭＭＥ４４と通話する場合、ＵＥは、コンテキストをクリーンとマークする。ＵＥは、トラフィックを保護するために、常に、Ｓ２（または下位の、Ｆ３により導出されるキー）を使用することに注意されたい。これは、ＳＧＳＮ／ＭＭＥ間のＡＶの送信を可能にする。

【００７５】

図５は、ｘＳＩＭを利用するＲｅｌ６　ＵＥ５１の初期認証を示す単純化ブロック図である。ＵＥは、Ｒｅｌ６であるので、ＵＥは、Ｅ－ＵＴＲＡＮネットワークへハンドオーバすることができない。それゆえ、Ｒｅｌ８　ＳＧＳＮ４３にクリーンコンテキストを保持する利得はなく（これが原理的において可能であっても）、また、ＭＭＥ４４を考慮する必要はない。Ｆ２関数が適用されるべきか（この場合に行うように）否かを判定することができるｘＳＩＭまたはＵＳＩＭをＵＥが有するかを、Ｒｅｌ８　ＳＧＳＮは区別することができなければならない（図６参照）。この情報は、ＡＶと共にＴＣＥ２５から渡されることができる。従って、拡張ｘＳＩＭに対するプロビジョンがなされる場合における、ＳＧＳＮ間で受け渡しされる場合には、各ＡＶはこの情報を搬送しなければならない。もちろん、ＵＳＩＭのみが使用される限り、この情報は必要とされない。

【００７６】

図６は、ＵＳＩＭを利用するＲｅｌ６　ＵＥ５２の初期認証を示す単純化ブロック図である。ＴＣＥ２５は、透過的に動作する（即ち、機能は、通常のＲｅｌ６ネットワークにおける機能と同一である）。再度、Ｒｅｌ８　ＳＧＳＮ４３は、クリーンコンテキストを維持する必要はなく、また、ＭＭＥ４４を考慮する必要がない。これは、ＵＥは、Ｅ－ＵＴＲＡＮネットワークへハンドオーバすることができないからである。

【００７７】

図７は、ＵＳＩＭを利用するＲｅｌ８　ＵＥ５３の初期認証を示す単純化ブロック図である。この場合、ＵＥは、ＳＧＳＮおよびＭＭＥの両方に接続することができることに注意することが重要である。Ｒｅｌ８　ＵＥが、必要なキー導出を実行するラッパ（wrapper）機能を周りに実装している場合、これはＵＳＩＭで達成することが可能である。

【００７８】

ＵＥ５３のラッパ機能は、以下の動作を実行する：

・Ｒｅｌ６　ＳＧＳＮ４２と通信する場合、ラッパ機能は、特別な機能を実行しないが、コンテキストをダーティとマークする。

【００７９】

・Ｒｅｌ８　ＳＧＳＮ４３またはＭＭＥ４４と通信する場合、ラッパ機能は、Ｓ１＝Ｆ１（Ｓ）およびＳ２＝Ｆ２（Ｓ１）を計算し、Ｓ１を記憶し、コンテキストをクリーンとマークする。Ｓ２が、Ｆ３の使用によりトラフィック保護キーを導出するために使用される。

【００８０】

図４－図７は、本発明の教示に従う（初期）認証の取扱いを示している。以下では、ハンドオーバの場合、および様々なシステム間のコンテキスト／ＡＶフェッチ／転送を説明する。

【００８１】

まず、ＡＶのフェッチを見ると、ＳＧＳＮおよびＭＭＥの様々なリリース間でＡＶが転送されても良い。この転送は、ＳＩＭのバージョンおよびターゲット／ソースシステムのリリースに依存する。特に、Ｒｅｌ８　ＳＧＳＮ及びＭＭＥに、ＴＣＥから転送する場合には、ＡＶを、ＵＳＩＭまたはｘＳＩＭＡＶとマークしなければならない。以下の表１は、ＡＶで、ＴＣＥからＳＧＳＮ／ＭＭＥに提供されるキーを示している。

【００８２】

【表１】

SGSN/MMEのAVに記憶されるAVキー（TCEから受信される場合）：

	Rel6 SGSN	Rel8 SGSN	MME
xSIM	S2	S1	S1
USIM	S	S	S1

【００８３】

ＳＧＳＮ／ＭＭＥにおけるＡＶに記憶されるＡＶキー（ＴＣＥから受信する場合）

次にＡＶの転送を見ると、以下の表２は、ＡＶを転送する場合のソースおよびターゲットＳＧＳＮ／ＭＭＥによって実行される動作を示している。

【００８４】

表２の記法の説明：

・ＡＶｋは、ＡＶで搬送されるキーである（ＡＶｋは、Ｓ、Ｓ１またはＳ２に等しい場合がある）。

【００８５】

・Ｓ－ビットは、ＡＶが原則として生成される、ＳＩＭのタイプを示すビット（即ち、値）である。Ｒｅｌ６　ＳＧＳＮから転送される場合、この情報は利用できず、従って、Ｓ－ビットは、次いで、Ｒｅｌ８　ＳＧＳＮによって「未知」に設定される。Ｓ－ビットは、拡張ｘＳＩＭをサポートしている場合にのみ必要となる。

【００８６】

・Ｄ－ビットは、ダーティビットである。Ｄ－ビットが設定される場合、それは、ＡＶｋは、再度決して変換されてはならないことを意味する。

【００８７】

・Ｔｘは、転送を意味する。

【００８８】
【表２】

AV転送

	ソースノード動作	宛先ノード動作
SGSN Rel6から SGSN Rel6へ	Tx(AVk_src)	AV= (AVk_src) (レガシーRel6 オペレーション)
SGSN Rel6から SGSN Rel8または MMEへ	Tx(AVk_src)	AV=(AVk_src, S-bit=unknown（未知）、 D-bit=true（真）、 注：D-bitが設定される、 これは、AVkがSGSN Rel8 とMMEによって直接使用 されることを意味する。

SGSN Rel8から
SGSN Rel6へ
	If (D-bit == true OR S-bit ==
	USIM)
	Tx(AVk_src)
	If (S-bit ==xSIM)
	Tx (F2(AVk_src))
		AV=(AVk_src)
		注：レガシーRel6
		オペレーション

SGSN Rel8から SGSN Rel8へ	Tx(AVk_src, S-bit, D-bit)	AV=(AVk_src, S-bit, D-bit)
SGSN Rel8からMMEへ	Tx(AVk_src, S-bit, D-bit) 注：USIMの場合、AVk_srcへの 変換はなされない、これは、 SGSN Rel8は、AVが戻される 場合に、変換が実行されているか どうかを区別することができない からである。（CTXk initは、 代わりに、変換を取り扱う）。 単なるD-bitよりもより細かい キーレベルが使用される場合には、 この制約は必要でない。	AV=(AVk_src, S-bit, D-bit)
MMEからMMEへ	Tx(AVk_src, S-bit, D-bit)	AV=(AVk_src, S-bit, D-bit)
MMEからSGSN Rel6へ	本実施形態では許容されない （MMEが、Sの知識を有して おらず、かつUEがUSIMを 有している場合は実現できない）	
MMEからSGSN Rel8へ	Tx(AVk_src, S-bit, D-bit)	AV=(AVk_src, S-bit, D-bit)

【００８９】
図８は、様々なシステム間の認証ベクトル（ＡＶ）の転送を示す単純化ブロック図である。Ｒｅｌ８　ＳＧＳＮ４３にクリーンＡＶがある場合、クリーンＡＶは、ダーティＡＶに変換して（上記の表２参照）、Ｒｅｌ６　ＳＧＳＮ４２に送信することができる。Ｒｅｌ６　ＳＧＳＮにＭＭＥ４４からＡＶをフェッチすることを許容することは可能であろう

が、そうするためには、ＭＭＥは、キーＳに関する知識を持たなければならない（ＵＥがＵＳＩＭを有する場合）ことに注意されたい。別の実施形態では、Ｒｅｌ６　ＳＧＳＮは、Ｒｅｌ８エンティティからＡＶをフェッチすることは許容されない。この場合、ＵＥは、ＵＳＩＭを有する場合、Ｒｅｌ８　ＳＧＳＮは、Ｓ１を受信することができる（正にＭＭＥのように）。

【００９０】

キー確立の失敗が発生しうる仮定例は、ユーザが次のことを行う場合である：

１．Ｒｅｌ８　ＵＥおよびＵＳＩＭを使用してＭＭＥで認証する。ＭＭＥは、Ｓ１を含むＡＶのバッチをＴＣＥからダウンロードする。

【００９１】

２．次に、ユーザは、Ｒｅｌ８　ＵＥをオフにし、ＵＳＩＭをＲｅｌ６　ＵＥに移し、ＲＥｌ６　ＳＧＳＮに対する認証を試行する。

【００９２】

３．ＲＥｌ６　ＳＧＳＮまたはＲｅｌ８　ＳＧＳＮは、ＴＣＥからＡＶをフェッチする代わりにＭＭＥからＡＶをフェッチし、次いでＵＥを調べることができる。

【００９３】

４．認証は成功するであろうが、ＳＧＳＮおよびＵＥは、異なるセキュリティコンテキストを保持するであろう（リンク保護キー）。ＳＧＳＮは、Ｓ２を保持するであろうし、ＵＥはＳを保持するであろう。ここで、キーの相違の検出には困難がありうることに注意されたい。

【００９４】

この状況が発生するのを防ぐために、ＭＭＥからＳＧＳＮにＡＶを転送する機能を取り除くことができる。これは妥当な解決策であることは、アクティブな「セキュリティコンテキスト」（キー群）を転送し、必要である場合には、ＨＳＳ／ＴＣＥからＳＧＳＮに後で新規のＡＶをダウンロードすることによって、シームレスなハンドオーバを依然としてサポートしうるからである。ＭＭＥにおける未使用ＡＶは、この場合、単に排除（フラッシュ：flush）されるであろう。

【００９５】

上述の問題は、「レガシー」リリースを更新することを可能とすることなく、ＳＩＭ、ＵＥリリースおよびネットワークリリースの全ての取り得る組み合わせを可能とすることの要望による副次的な影響である。Ｒｅｌ８　ＳＧＳＮに対する状況を解消する別の取り得る方法は、例えば、ＵＥで使用されるＳＩＭ（ＵＳＩＭ／ｘＳＩＭ）のタイプを告げるＳＧＳＮへ、Ｒｅｌ８　ＵＥからの新規のシグナリングを導入することである。これは、クラスマーク（階級値：classmark）情報またはその他のシグナリングで行うことができる。Ｒｅｌ８　ＳＧＳＮが、このシグナリングを受信しない場合、ＳＧＳＮは、ＵＥがＲｅｌ６　ＵＥであり、失敗が生じるであろうと結論付けることができる。

【００９６】

図９は、コンテキストがソースからターゲットシステムに転送され、転送されたキーが明示的な再認証することなく、ターゲットシステムによる即時使用に供する場合の、アクセス間コンテキスト転送処理を示す単純化ブロック図である。関数「Ｇ」は、このために利用される。尚、依然としてクリーンであるコンテキスト（即ち、Ｒｅｌ８　ＳＧＳＮ内およびＲｅｌ８　ＳＧＳＮとＭＭＥ間の転送）の場合、Ｇは、常にＳ１キーに適用されて、「クリーン性」を維持する。既にダーティであるコンテキストは処理されない。換言すれば、ダーティコンテキストに対しては、Ｓ２キーはそのまま手渡される。いくつかの場合、ダーティコンテキストを処理することは可能でありうるが、そうすることは何ら有意な特別の保護をもたらさないことに注意されたい。Ｒｅｌ６　ＳＧＳＮへの転送をＧにより決して処理されないが、原理的には、新規のシグナリングの導入によってそのようにすることは可能であろう。ＵＥに類似の処理を実行することを告げるために、このシグナリングは、Ｒｅｌ８／Ｒｅｌ６のハンドオーバにおいて必要とされるであろう。そうでなければ、ＵＥは転送に気付かず（アウェアでなく）、間違っているキーを使用することにな

るであろう。

【００９７】

Ｆ１、Ｆ２、Ｆ３およびＧは、暗号化関数（機能）である。これらはすべて、例えば、高度暗号化標準（ＡＥＳ：Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）、ＳＨＡ２５６アルゴリズムおよびその類のような、標準のブロックを構築することによって実現することができる。Ｆ１、Ｆ２、Ｆ３およびＧは、少なくとも（強力な）一方向性関数であるべきであり、好ましくは、擬似ランダム関数であるべきである。Ｆ３は、その上、ＥＰＳネットワークに対して、６つまでのキーを生成することを必要とする。これは、キー＝Ｆ３（Ｓ１，＜ｌａｂｅｌ＞）等の「ｌａｂｅｌ（ラベル）」を使用して行うことができ、ここで、ｌａｂｅｌ（ラベル）は、個別キーに対し個別の値を取る。この場合、Ｆ３は、擬似ランダム関数であるべきである。関数Ｆ３は、好ましくは、また、使用対象のキーで用いられるアルゴリズムの「ＩＤ」に依存するようにする。

【００９８】

ＵＥがＲｅｌ８　ＳＧＳＮとＭＭＥとの間を「往来（ｐｉｎｇ－ｐｏｎｇ）」する場合、Ｇが、数回適用されても良いことに注意されたい。Ｇは、その場合、好ましくは、反復しても劣化しない特性を持つべきである。これを達成する１つの方法は、Ｇが擬似ランダム順列であるとさらに想定することである。その場合、例えば、次のことがありえよう：

target_system_S1=G(source_system_S1, c,...)

ここで、ｃは、各「往」または「来」において増加するカウンタである。システムＩＤ等のその他の入力もまた含みうる。

【００９９】

いくつかの拡張を、また、Ｒｅｌ６／Ｒｅｌ８ハンドオーバに対して行うことができる。まず、新規のシグナリングを、Ｒｅｌ８　ＳＧＳＮからＲｅｌ８　ＵＥに導入し、ＵＥに、ＵＥがＲｅｌ６　ＳＧＳＮへ／からハンドオーバされることを告げる。そして、上述のように、Ｒｅｌ６／Ｒｅｌ８　ＳＧＳＮのハンドオーバ時にＧをまた適用することによって、この解決策がさらに改善することができる。ＵＥは、次に、明示的なシグナリングによって、この状況に気付く（アウェアである）ので、ＵＥおよびＲｅｌ８　ＳＧＳＮは、完全同期して、要求される関数Ｇを適用することができる。

【０１００】

本発明の好ましい実施形態は、添付図面において示され、上述の発明を実施するための形態において説明されているが、本発明は、開示されている実施形態に制限されず、本発明の範囲を逸脱することなく数多くの再構成、変形および置換が可能であることが理解される。また、この説明は、Ｅ－ＵＴＲＡＮとＵＴＲＡＮネットワークとの間の相互動作に焦点を当てているが、キー分離の原理は、Ｅ－ＵＴＲＡＮと非３ＧＰＰアクセス技術（例えば、ＣＤＭＡ２０００、ＩＥＥＥ８０２．１１、ＩＥＥＥ８０２．１６等）との間、または、任意の２つの非３ＧＰＰネットワーク間の相互動作に等しく適用可能（および有用）であろう。明細書では、特許請求の範囲によって定義される本発明の範囲内に入るあらゆる変形を意図するものである。

【図１】

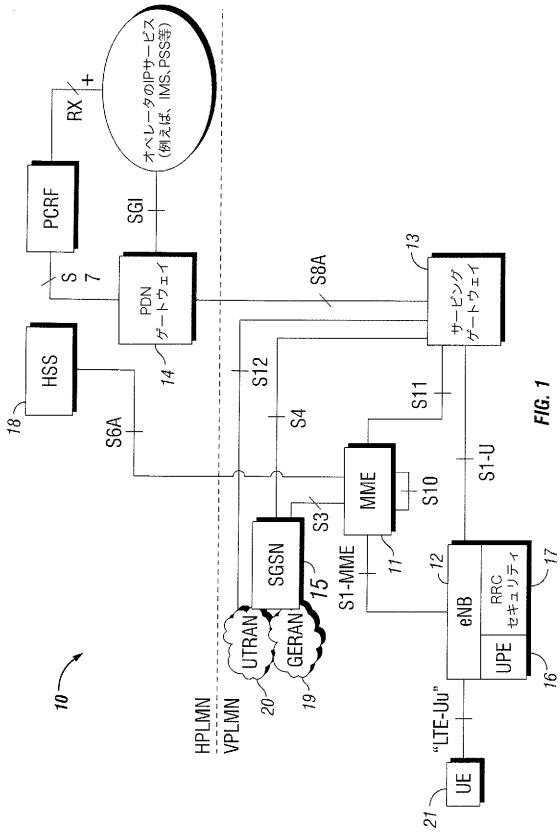

FIG. 1

【図２】

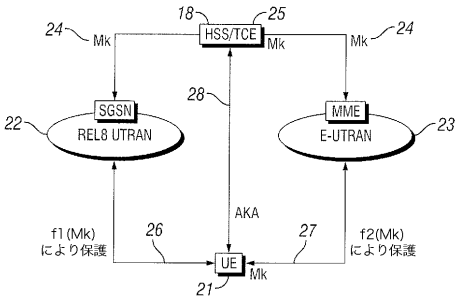

FIG. 2

【図３】

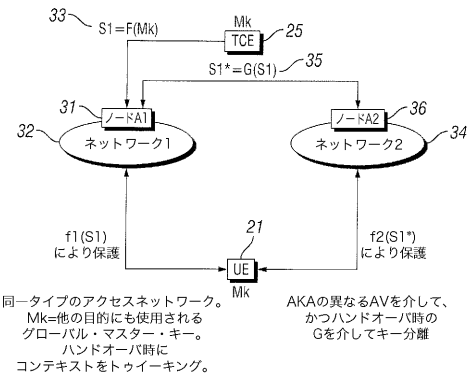

FIG. 3

【図４】

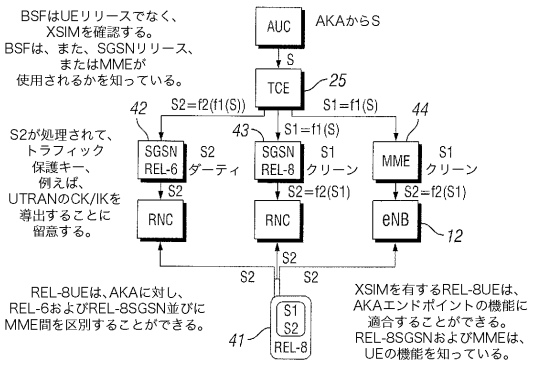

FIG. 4

【図６】

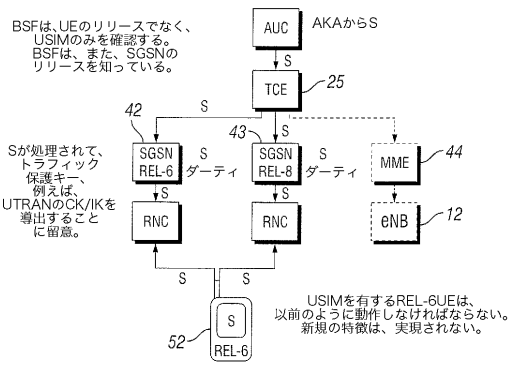

FIG. 6

【図５】

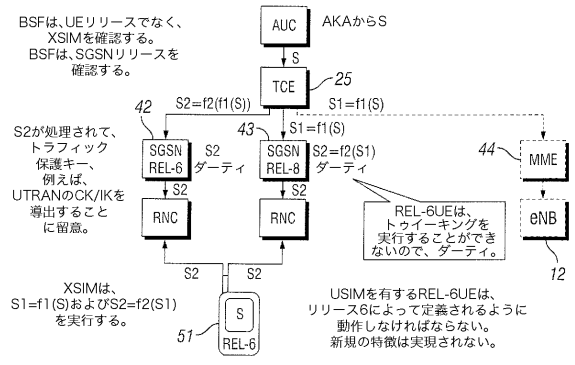

FIG. 5

【図７】

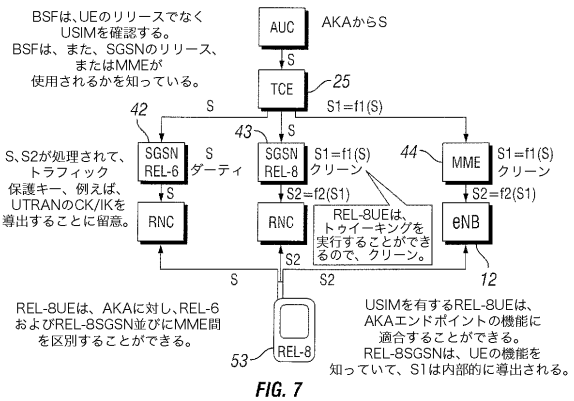

FIG. 7

【図８】

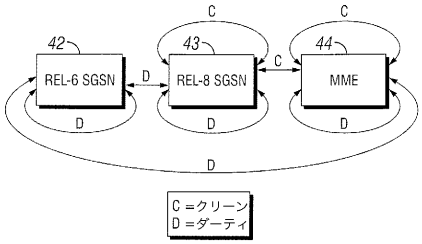

FIG. 8

【図９】

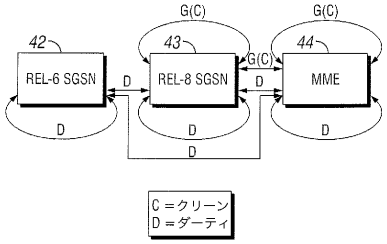

FIG. 9

フロントページの続き

(72)発明者 ブロム, ロルフ
スウェーデン国 イェルフェッラ エス－１７５ ６８, スベルドヴェーゲン ２
(72)発明者 ネスルンド, マッツ
スウェーデン国 ブロンマ エス－１６８ ３６, ストプヴェーゲン ９５
(72)発明者 ノーマン, カール
スウェーデン国 ストックホルム エス－１１６ ２８, スティグベリスガタン ３２エー

審査官 松平 英

(56)参考文献 特開２００４－３０４８０４（ＪＰ，Ａ）
特開２００５－０４５４１８（ＪＰ，Ａ）
特開２００５－３４１２９０（ＪＰ，Ａ）
特開２００６－１２１６９８（ＪＰ，Ａ）
特開２００６－１９７５３６（ＪＰ，Ａ）
特開２００７－０５３６７４（ＪＰ，Ａ）
特表２００４－５１８３０９（ＪＰ，Ａ）
特表２００７－５０７１５７（ＪＰ，Ａ）
特表２００７－５１３５８５（ＪＰ，Ａ）
特表２００７－５１３５８７（ＪＰ，Ａ）
特表２００８－５１９５０８（ＪＰ，Ａ）
国際公開第２００６／０６４７０５（WO，Ａ１）
松中 隆志 他，異ネットワーク間ハンドオーバにおけるユーザの有効期限を考慮した効率的な認証方式の提案，電子情報通信学会２００５年通信ソサイエティ大会講演論文集２，社団法人電子情報通信学会，２００５年 ９月 ７日，ｐ．Ｓ－９～Ｓ－１０
藤野 庄三 他，ＰＡＮシステムにおける認証手順と端末切り替え方式，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００６年 ２月２３日，Ｖｏｌ．１０５ Ｎｏ．６２７，ｐ．１６９～１７２
Yan Zhang et al, An improvement for authentication protocol in third-generation wireless networks, IEEE Transactions on Wireless Communications, IEEE, ２００６年 ９月, Volume 5 , Issue 9, p.2348－2352
3GPP TSG SA WG3 Security －SA3#44 S3-060476, [online], ２００６年 ７月 ４日, [平成２４年１１月９日検索], インターネット<URL: http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_44_Tallinn/Docs/>

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／００
Ｇ０９Ｃ １／００
Ｈ０４Ｌ １２／００
Ｈ０４Ｌ ２９／００
Ｈ０４Ｗ ４／００