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

特許第5519736号
(P5519736)

(45)発行日　平成26年6月11日(2014.6.11)　(24)登録日　平成26年4月11日(2014.4.11)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601C
G06F 21/44	(2013.01)	H04L	9/00	601B
H04W 12/06	(2009.01)	G06F	21/20	144C
		H04W	12/06	

請求項の数 32　(全 27 頁)

(21)出願番号	特願2012-157137 (P2012-157137)
(22)出願日	平成24年7月13日 (2012.7.13)
(62)分割の表示	特願2008-531816 (P2008-531816)の分割
原出願日	平成18年9月26日 (2006.9.26)
(65)公開番号	特開2012-253782 (P2012-253782A)
(43)公開日	平成24年12月20日 (2012.12.20)
審査請求日	平成24年7月30日 (2012.7.30)
(31)優先権主張番号	60/720,445
(32)優先日	平成17年9月26日 (2005.9.26)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	11/397,837
(32)優先日	平成18年4月4日 (2006.4.4)
(33)優先権主張国	米国 (US)

(73)特許権者　398012616
ノキア　コーポレイション
フィンランド　エフイーエン－０２１５０
エスプー　ケイララーデンティエ　４
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100092624
弁理士　鶴田　準一
(74)代理人　100141162
弁理士　森　啓
(74)代理人　100141254
弁理士　榎原　正巳

最終頁に続く

(54)【発明の名称】ブートストラッピングアーキテクチャ内でキーをリフレッシュするための方法および装置

(57)【特許請求の範囲】

【請求項１】

プロセッサにより実行される方法において、認証および安全なサービスを提供するように構成されたネットワークエレメントへの伝送のために、アプリケーション要求を前記プロセッサにより生成するステップと、

前記アプリケーション要求に応えて、前記ネットワークエレメントとの安全な通信を提供するのに使用されるキーのリフレッシュを標示するメッセージを前記プロセッサにより受信するステップと、

前記受信したメッセージに基づきリフレッシュ済みキーを前記プロセッサにより導出するステップと、を備える方法であって、

ブートストラッピング機能を提供するように構成されたブートストラッピングネットワークエレメントに対し前記ネットワークエレメントが認証要求を送信する前に、前記リフレッシュ済みキーが、ブートストラップ手続きが以前に行われた場合には、該ブートストラップ手続きの１つ以上のパラメータから導出される、方法。

【請求項２】

前記受信するステップにおける前記メッセージが、前記ネットワークエレメントにより選択される乱数を含む、請求項１に記載の方法。

【請求項３】

第２の乱数を生成するステップと、

ネットワークエレメントに対し第２のアプリケーション要求を伝送するステップであっ

て、前記第２のアプリケーション要求が前記第２の乱数を含むクレデンシャルを特定する、ステップをさらに備え、
前記乱数が前記ブートストラッピング機能を提供するように構成された前記ブートストラッピングネットワークエレメントに転送される、請求項２に記載の方法。
【請求項４】
前記ブートストラッピングネットワークエレメントがさらに、前記リフレッシュ済みキーおよびユーザプロファイルのアプリケーション特定部分を含む認証回答を生成するように構成されている、請求項３に記載の方法。
【請求項５】
前記第２のアプリケーション要求内で特定されている前記クレデンシャルを確認するステップをさらに備える請求項３に記載の方法。
【請求項６】
ネットワークエレメントに対し第２のアプリケーション要求を伝送するステップをさらに備え、
前記第２のアプリケーション要求がトランザクション識別子およびアプリケーションプロトコルメッセージを含むクレデンシャルを特定し、
前記ネットワークエレメントが、前記ブートストラッピング機能を提供するように構成された前記ブートストラッピングネットワークエレメントに対する伝送についての前記認証要求を生成し、
前記認証要求が前記トランザクション識別子、前記乱数および前記ネットワークエレメントのドメイン名を特定する、請求項２に記載の方法。
【請求項７】
前記ブートストラッピングネットワークエレメントがさらに、前記トランザクション識別子に基づいてブートストラッピングキーを検索し、
前記ブートストラッピングキーおよび前記乱数に基づいてフレッシュセッションキーを生成し、かつ
生成された前記フレッシュセッションキー、検索されたリフレッシュ済みキーに結びつけられた寿命パラメータおよびユーザプロファイルを内含する認証回答を生成するように構成されており、
前記方法は、成功した認証を標示する前記ネットワークエレメントからアプリケーション回答を受信するステップをさらに備える、請求項６に記載の方法。
【請求項８】
前記ネットワークエレメントが、スペクトラム拡散を用いて通信するように、および、一般的認証アーキテクチャに従って動作するように＜ように＞構成されている、請求項１に記載の方法。
【請求項９】
プロセッサにより実行される方法において、
リフレッシュ済みキーに対応する乱数を前記プロセッサにより生成するステップと、
認証および安全なサービスを提供するように構成されたネットワークエレメントに対しアプリケーション要求を前記プロセッサにより伝送するステップであって、
前記アプリケーション要求は、トランザクション識別子、前記乱数およびアプリケーションプロトコルメッセージを特定し、
前記ネットワークエレメントがさらに、前記アプリケーション要求が送信された後に、ブートストラッピング機能を提供するように構成されたブートストラッピングネットワークエレメントに対して認証要求を転送するように構成され、
前記認証要求が前記トランザクション識別子、前記乱数および前記ネットワークエレメントと結びつけられたドメイン名を特定し、
前記ブートストラッピングネットワークエレメントがさらに、前記トランザクション識別子に基づいてブートストラッピングキーを検索し、
前記ブートストラッピングキーおよび乱数に基づいてフレッシュセッションキーを生

成し、かつ、
生成された前記フレッシュセッションキー、検索されたリフレッシュ済みキーに結びつけられた寿命パラメータおよびユーザプロファイルを内含する認証回答を生成するように構成されている、ステップと、
成功した認証を標示する前記ネットワークエレメントからアプリケーション回答を前記プロセッサにより受信するステップと、を備える方法であって、
前記アプリケーション要求が前記ネットワークエレメントに送信される前に、前記リフレッシュ済みキーが利用可能である、方法。
【請求項１０】
前記ネットワークエレメントおよび前記ブートストラッピングネットワークエレメントが、スペクトラム拡散を用いて通信し、かつ、汎用認証アーキテクチャに従って動作するように構成されている、請求項９に記載の方法。
【請求項１１】
プロセッサにより実行される方法において、
第１の乱数を前記プロセッサにより生成するステップと、
安全なサービスを提供するように構成されたネットワークエレメントに対してアプリケーション要求を前記プロセッサにより伝送するステップであって、
前記アプリケーション要求がトランザクション識別子、前記第１の乱数およびアプリケーションプロトコルメッセージを特定し、
前記ネットワークエレメントがさらに第２の乱数を選択するように構成されている、ステップと、
前記ネットワークエレメントから第２の乱数を特定するアプリケーション回答を前記プロセッサにより受信するステップと、
前記アプリケーション回答に応答して、ブートストラッピングキー、前記第１の乱数および前記第２の乱数に基づいてフレッシュセッションキーを前記プロセッサにより導出するステップであって、前記フレッシュセッションキーが前記ネットワークエレメントとの安全な通信を提供するために使用されるステップと、を備える方法であって、
ブートストラッピング機能を提供するように構成されたブートストラッピングネットワークエレメントに対し前記ネットワークエレメントが認証要求を送信する前に、前記フレッシュセッションキーが、ブートストラップ手続きが以前に行われた場合には、該ブートストラップ手続きの１つ以上のパラメータから導出される、方法。
【請求項１２】
前記ネットワークエレメントが、スペクトラム拡散を用いて通信しかつ汎用認証アーキテクチャに従って動作するように構成されている、請求項１１に記載の方法。
【請求項１３】
前記ブートストラッピングネットワークエレメントがさらに、
前記トランザクション識別子に基づいてブートストラッピングキーを検索し、
前記ブートストラッピングキーおよび前記第２の乱数に基づいてフレッシュセッションキーを生成し、かつ、
生成された前記フレッシュセッションキー、検索されたリフレッシュ済みキーに結びつけられた寿命パラメータおよびユーザプロファイルを内含する認証回答を生成する、
ように構成されており、
前記方法は、成功した認証を標示する、前記ネットワークエレメントからの別のアプリケーション回答を受信するステップをさらに備える、請求項１１に記載の方法。
【請求項１４】
安全なサービスを提供するように構成されたネットワークエレメントに対する伝送のためのアプリケーション要求を生成するように構成され、さらに前記アプリケーション要求に応答して、前記ネットワークエレメントとの安全な通信を提供するのに使用されるキーのリフレッシュを標示するメッセージを受信するように構成され、さらには、受信した前記メッセージに基づきリフレッシュ済みキーを導出するように構成されているプロセッサ

、
を備える装置であって、
ブートストラッピング機能を提供するように構成されたブートストラッピングネットワークエレメントに対し前記ネットワークエレメントが認証要求を送信する前に、前記リフレッシュ済みキーが、ブートストラップ手続きが以前に行われた場合には、該ブートストラップ手続きの１つ以上のパラメータから導出される、装置。
【請求項１５】
前記メッセージが、前記ネットワークエレメントにより選択される乱数を含む、請求項１４に記載の装置。
【請求項１６】
請求項１４に記載の装置およびネットワークエレメントを備えるシステム。
【請求項１７】
前記プロセッサがさらに、第２の乱数を生成し、かつ、前記ネットワークエレメントに対する伝達のための第２のアプリケーション要求を生成するように構成されており、
前記第２のアプリケーション要求が前記第２の乱数を含むクレデンシャルを特定し、
前記乱数が前記ブートストラッピング機能を提供するように構成された前記ブートストラッピングネットワークエレメントに転送される、請求項１５に記載の装置。
【請求項１８】
前記ブートストラッピングネットワークエレメントがさらに、前記リフレッシュ済みキーおよびユーザプロファイルのアプリケーション特定部分を含む認証回答を生成するように構成されている、請求項１７に記載の装置。
【請求項１９】
前記プロセッサがさらに、前記第２のアプリケーション要求内で特定されている前記クレデンシャルを確認するように構成されている、請求項１７に記載の装置。
【請求項２０】
前記プロセッサがさらに、前記ネットワークエレメントに対する伝達のための第２のアプリケーション要求を生成するように構成されており、
前記第２のアプリケーション要求がトランザクション識別子およびアプリケーションプロトコルメッセージを含むクレデンシャルを特定し、
前記ネットワークエレメントが、前記ブートストラッピング機能を提供するように構成された前記ブートストラッピングネットワークエレメントに対する伝送についての前記認証要求を生成し、
前記認証要求が前記トランザクション識別子、前記乱数および前記ネットワークエレメントのドメイン名を特定する、請求項１５に記載の装置。
【請求項２１】
前記ブートストラッピングネットワークエレメントがさらに、前記トランザクション識別子に基づいてブートストラッピングキーを検索し、
前記ブートストラッピングキーおよび乱数に基づいてフレッシュセッションキーを生成し、かつ、
前記検索されたリフレッシュ済みキー、生成された前記フレッシュセッションキーに結びつけられた寿命パラメータおよびユーザプロファイルを内含する認証回答を生成するように構成されており、
前記装置は、前記プロセッサに結合され、かつ成功した認証を標示するアプリケーション回答を前記ネットワークエレメントから受信するように構成されたトランシーバをさらに備える、請求項２０に記載の装置。
【請求項２２】
前記ネットワークエレメントが、スペクトラム拡散を用いて通信し、かつ、汎用認証アーキテクチャに従って動作するように構成されている、請求項１４に記載の装置。
【請求項２３】
請求項１４に記載の装置およびネットワークエレメントを備えるシステム。

【請求項２４】
リフレッシュ済みキーに対応する乱数を生成するように構成されたプロセッサと、
安全なサービスを提供するように構成されたネットワークエレメントに対しアプリケーション要求を伝送するように構成されたトランシーバと、を備える装置であって、
前記アプリケーション要求は、トランザクション識別子、前記乱数およびアプリケーションプロトコルメッセージを特定し、
前記ネットワークエレメントはさらに、前記アプリケーション要求が送信された後に、ブートストラッピング機能を提供するように構成されたブートストラッピングネットワークエレメントに対し認証要求を転送するように構成されており、
前記認証要求が前記トランザクション識別子、前記乱数および、前記ネットワークエレメントに結びつけられたドメイン名を特定しており、
前記ブートストラッピングネットワークエレメントがさらに、
前記トランザクション識別子に基づいてブートストラッピングキーを検索し、
前記ブートストラッピングキーおよび乱数に基づいてフレッシュセッションキーを生成し、かつ、
生成された前記フレッシュセッションキー、検索されたリフレッシュ済みキーに結びつけられた寿命パラメータおよびユーザプロファイルを内含する認証回答を生成するように構成されており、
前記トランシーバはさらに、成功した認証を標示するアプリケーション回答を前記ネットワークエレメントから受信するように構成されており、
前記アプリケーション要求が前記ネットワークエレメントに送信される前に、前記リフレッシュ済みキーが利用可能である、装置。
【請求項２５】
前記ネットワークエレメントおよび前記ブートストラッピングネットワークエレメントが、スペクトラム拡散を用いて通信し、かつ、汎用認証アーキテクチャに従って動作するように構成されている、請求項２４に記載の装置。
【請求項２６】
請求項２４に記載の装置およびネットワークエレメントを備えるシステム。
【請求項２７】
第１の乱数を生成するように構成されているプロセッサと、
前記プロセッサに結合され、かつネットワークエレメントに対するアプリケーション要求を伝送するように構成されているトランシーバと、を備える装置であって、
前記アプリケーション要求は、トランザクション識別子、前記第１の乱数およびアプリケーションプロトコルメッセージを特定し、
前記ネットワークエレメントがさらに第２の乱数を選択するように構成されており、
前記トランシーバがさらに、前記ネットワークエレメントからの前記第２の乱数を特定するアプリケーション回答を受信するように構成されており、
前記プロセッサがさらに、前記アプリケーション回答に応答して、ブートストラッピングキー、前記第１の乱数、および前記第２の乱数に基づいてフレッシュセッションキーを導出するように構成されており、
前記フレッシュセッションキーが、前記ネットワークエレメントとの安全な通信を提供するために使用されており、
ブートストラッピング機能を提供するように構成されたブートストラッピングネットワークエレメントに対し前記ネットワークエレメントが認証要求を送信する前に、前記フレッシュセッションキーが、ブートストラップ手続きが以前に行われた場合には、該ブートストラップ手続きの１つ以上のパラメータから導出される、装置。
【請求項２８】
前記ネットワークエレメントおよび前記ブートストラッピングネットワークエレメントが、スペクトラム拡散を用いて通信し、かつ汎用認証アーキテクチャに従って動作するように構成されている、請求項２７に記載の装置。

【請求項２９】
プロセッサにより実行される方法であって、
ユーザ機器から、トランザクション識別子を特定するアプリケーション要求を前記プロセッサにより受信するステップと、
前記アプリケーション要求に応答して、新しいブートストラッピングが実施されたことを前記ユーザ機器が標示しているかまたは、前記ユーザ機器がセッションキーをリフレッシュしようとしているかを受信済みの前記トランザクション識別子に基づいて、前記新しいブートストラッピングを実施することなく、前記プロセッサにより決定するステップと、
前記決定に基づいて、前記新しいブートストラッピングを実施することなく、セッションキーを前記プロセッサによりリフレッシュするか、または新規ブートストラッピングと結びつけられた新規ブートストラッピングキーマテリアルを前記プロセッサにより使用するステップと、を備える方法。
【請求項３０】
前記ユーザ機器が、スペクトラム拡散を用いて通信し、かつ汎用認証アーキテクチャに従って動作するように構成されている、請求項２９に記載の方法。
【請求項３１】
ユーザ機器から、トランザクション識別子を特定するアプリケーション要求を受信するための手段と、
前記アプリケーション要求に応答して、新しいブートストラッピングが実施されたことを前記ユーザ機器が標示しているかまたは、受信済みの前記トランザクション識別子に基づいて、前記新しいブートストラッピングを実施することなく、前記ユーザ機器がセッションキーをリフレッシュしようとしているかを決定するための手段と、
前記決定に基づいて、新しいブートストラッピングを実施することなく、前記セッションキーをリフレッシュするか、または新規ブートストラッピングキーマテリアルを使用するための手段と、を備えるシステム。
【請求項３２】
前記ユーザ機器が、スペクトラム拡散を用いて通信し、かつ汎用認証アーキテクチャに従って動作するように構成されている、請求項３１に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は通信、より特定的には通信システム内での認証サービスの提供に関する。
【背景技術】
【０００２】
セルラーシステム（例えばスペクトラム拡散システム（例えば符号分割多元接続（ＣＤＭＡ）ネットワーク）または時分割多元接続（ＴＤＭＡ）ネットワーク）といったような無線通信システムは、豊富なサービスおよびフィーチャセットと共に可動性という利便性をユーザに提供する。この利便性のため、事業用および個人用として認められた通信様式として、増加を続ける消費者がこれを採用するに至っている。さらに多くの採用を促すべく、メーカからサービスプロバイダに至るまでの電気通信業界は、さまざまなサービスおよび特徴の基礎にある通信プロトコルのための標準を開発することに多大な費用と努力を払って合意してきた。この研究努力の１つの主要な分野には、認証のためのキープロビジョニングおよび安全な通信の確立が関与している。残念なことに、この機能は、現行のプロトコルによっては有効にサポートされていない。
【先行技術文献】
【非特許文献】
【０００３】
【非特許文献１】第３世代パートナシッププロジェクト：３ＧＰＰＴＳ３３．２２０
【非特許文献２】第３世代パートナシッププロジェクト：３ＧＰＰＴＳ２４．１０９

【非特許文献３】第３世代パートナシッププロジェクト：３ＧＰＰ２Ｓ．ＰＯ１０９
【発明の概要】
【発明が解決しようとする課題】
【０００４】
従って、通信プロトコルを利用するためにネットワークエレメントを必要とすることなくネットワークエレメント（またはデバイス）間のブートストラッピングを容易にし、かくしてハードウェアのアップグレード／修正を回避するためにキープロビジョニングを提供するためのアプローチに対するニーズが存在している。
【課題を解決するための手段】
【０００５】
これらのおよびその他のニーズは、ブートストラッピングアーキテクチャ内でより有効にキープロビジョニングをサポートするための１つのアプローチを提示する本発明により対処されている。
【０００６】
これらのおよびその他のニーズは、安全な通信を提供するために通信ネットワーク内でセッションキーをリフレッシュするためのアプローチを提示する本発明により対処されている。
【０００７】
本発明の実施形態の一態様によれば、本方法には認証および安全なサービスを提供するように構成されたネットワークエレメントに対しアプリケーション要求を伝送するステップを備える。本方法は同様に、アプリケーション要求に応えて、ネットワークエレメントとの安全な通信を提供するのに使用されるキーのリフレッシュを標示するメッセージを受信するステップをも備える。本方法はさらに、受信したメッセージに基づきリフレッシュ済みキーを導出するステップをも備える。
【０００８】
本発明の実施形態のもう１つの態様によれば、本方法には、リフレッシュされたキーに対応する乱数を生成するステップを備える。本方法は同様に、認証および安全なサービスを提供するように構成されたネットワークエレメントに対しアプリケーション要求を伝送するステップにおいて、アプリケーション要求がトランザクション識別子、乱数、およびアプリケーションプロトコルメッセージを特定しているステップをも備える。本ネットワークエレメントはさらに、ブートストラッピング機能を提供するように構成されたブートストラッピングネットワークエレメントに対して認証要求を転送するように構成されている。認証要求は、トランザクション識別子、乱数およびネットワークエレメントと結びつけられたドメイン名を特定する。ブートストラッピングネットワークエレメントはさらに、トランザクション識別子に基づいてブートストラッピングキーを検索し、ブートストラッピングキーおよび乱数に基づいてフレッシュセッションキーを生成し、かつ検索されたリフレッシュ済みキー、生成されたフレッシュセッションキーに結びつけられた寿命パラメータおよびユーザプロファイルを内含する認証回答を生成するように構成されている。さらに、本方法は、成功した認証を標示するアプリケーション回答をネットワークエレメントから受信するステップを備える。
【０００９】
本発明の実施形態のもう１つの態様によれば、本方法には、第１の乱数を生成するステップおよび安全なサービスを提供するように構成されたネットワークエレメントに対してアプリケーション要求を伝送するステップを備える。本アプリケーション要求はトランザクション識別子、乱数およびアプリケーションプロトコルメッセージを特定する。本ネットワークエレメントはさらに第２の乱数を選択するように構成されている。本方法は同様に、ネットワークエレメントから第２の乱数を特定するアプリケーション回答を受信するステップをも備える。さらに、本方法は、ブートストラッピングキー、第１の乱数および第２の乱数に基づいてフレッシュセッションキーを導出するステップを備え、ここで、このフレッシュセッションキーはネットワークエレメントとの安全な通信を提供するために

使用される。

【００１０】

本発明の実施形態のもう１つの態様によれば、装置には、安全なサービスを提供するように構成されたネットワークエレメントに対する伝送のためのアプリケーション要求を生成するように構成されたプロセッサが含まれている。本プロセッサは、さらに、アプリケーション要求に応えて、ネットワークエレメントとの安全な通信を提供するのに使用されるキーのリフレッシュを標示するメッセージを受信するように構成されている。本プロセッサはさらに、受信したメッセージに基づきリフレッシュ済みキーを導出するように構成されている。

【００１１】

本発明の実施形態のもう１つの態様によれば、装置は、乱数を生成するように構成されたプロセッサを備える。本装置は同様に、安全なサービスを提供するように構成されたネットワークエレメントに対しアプリケーション要求を伝送するように構成されたトランシーバを備える。本アプリケーション要求は、トランザクション識別子、乱数およびアプリケーションプロトコルメッセージを特定する。ネットワークエレメントはさらに、ブートストラッピング機能を提供するように構成されたブートストラッピングネットワークエレメントに対し認証要求を転送するように構成されている。認証要求は、トランザクション識別子、乱数およびネットワークエレメントと結びつけられたドメイン名を特定する。ブートストラッピングネットワークエレメントはさらに、トランザクション識別子に基づいてブートストラッピングキーを検索し、ブートストラッピングキーおよび乱数に基づいてフレッシュセッションキーを生成し、生成されたフレッシュセッションキー、フレッシュセッションキーと結びつけられた寿命パラメータおよびユーザプロファイルを内含する認証回答を生成するように構成されている。トランシーバはさらに、成功した認証を標示するアプリケーション回答をネットワークエレメントから受信するように構成されている。

【００１２】

本発明の１実施形態のもう１つの態様によれば、装置は、第１の乱数を生成するように構成されているプロセッサを備える。本装置は同様に、プロセッサに結合され、ネットワークエレメントに対するアプリケーション要求を伝送するように構成されているトランシーバをも備え、アプリケーション要求はトランザクション識別子、乱数およびアプリケーションプロトコルメッセージを特定する。ネットワークエレメントはさらに第２の乱数を選択するように構成されている。本トランシーバはさらに、ネットワークエレメントからの第２の乱数を特定するアプリケーション回答を受信するように構成されている。本プロセッサはさらに、ブートストラッピングキー、第１の乱数、および第２の乱数に基づいてフレッシュセッションキーを導出するように構成されており、本フレッシュセッションキーは、ネットワークエレメントとの安全な通信を提供するために使用されている。

【００１３】

本発明の１実施形態のもう１つの態様によれば、本方法は、ユーザ機器から、アプリケーション要求を受信するステップを備える。本要求はトランザクション識別子を特定する。本方法は同様に、新しいブートストラッピングが実施されたことをユーザ機器が標示しているか、または、ユーザ機器がセッションキーをリフレッシュしようとしているかを受信済みトランザクション識別子に基づいて決定するステップも備える。本方法は、この決定に基づいてセッションキーをリフレッシュするかまたは新規ブートストラッピングと結びつけられた新規ブートストラッピングキーマテリアルを使用するステップをさらに備える。

【００１４】

本発明の１実施形態のもう１つの態様によれば、システムは、ユーザ機器から、アプリケーション要求を受信するための手段を備える。本要求はトランザクション識別子を特定する。本システムは、同様に、新しいブートストラッピングが実施されたことをユーザ機器が標示しているか、または、ユーザ機器がセッションキーをリフレッシュしようとしているかを受信済みトランザクション識別子に基づいて決定するための手段をも備える。さ

らには、システムは、この決定に基づいてセッションキーをリフレッシュするかまたは新規ブートストラッピングと結びつけられた新規ブートストラッピングキーマテリアルを使用するための手段を備える。

【００１５】

本発明のさらにその他の態様、特徴および利点は、本発明を実施するために考慮されている最良の態様を含め、一定の特定の実施形態および実装を単に例示することによって、以下の詳細な記述から容易に明らかになる。本発明は同様に、その他の異なる実施形態でも可能であり、そのいくつかの細部を、全て本発明の精神および範囲から逸脱することなく、さまざまな明らかな観点から修正することができる。従って、図面および記述は本来、制限的な意味のない例示的なものとしてみなされるべきである。

【００１６】

本発明は、同じ番号が類似の要素を意味する添付図面の図において、制限的な意味なく一例として示されている。

【図面の簡単な説明】

【００１７】

【図１】本発明の種々の実施形態による、キーのリフレッシュを提供する能力をもつブートストラッピングアーキテクチャ例を示す図である。

【図２Ａ】本発明の種々の実施形態による、キーリフレッシュプロセスのフローチャートである。

【図２Ｂ】本発明の種々の実施形態による、キーリフレッシュプロセスのフローチャートである。

【図３】セッションキーをリフレッシュするための従来のブートストラッピング手順のフローチャートである。

【図４】本発明の一実施形態による、２つのノンスを利用することによりセッションキーをリフレッシュするための手順を示す図である。

【図５】本発明の一実施形態による、ネットワークアプリケーションの乱数を利用することによりセッションキーをリフレッシュするための手順を示す図である。

【図６】本発明の一実施形態による、ユーザ機器の乱数を利用することによりセッションキーをリフレッシュするための手順を示す図である。

【図７】本発明の一実施形態による、ブートストラッピングサーバ機能（ＢＳＦ）を関与させることなくセッションキーをリフレッシュするための手順を示す図である。

【図８】本発明の種々の実施形態を実施するために使用することのできるハードウェアを示す図である。

【図９Ａ】本発明の種々の実施形態をサポートする能力をもつ異なるセルラー方式移動電話システムを示す図である。

【図９Ｂ】本発明の種々の実施形態をサポートする能力をもつ異なるセルラー方式移動電話システムを示す図である。

【図１０】本発明の一実施形態による、図９Ａおよび９Ｂのシステム内で動作する能力をもつ移動局の構成要素例を示す図である。

【図１１】本発明の一実施形態による、本書に記述されているプロセスをサポートする能力をもつ企業ネットワークを示す図である。

【発明を実施するための形態】

【００１８】

本出願は、その全体が本書に参考として内含される「ブートストラッピングアーキテクチャ内でキーをリフレッシュするための方法および装置」という題の２００５年９月２６日付け米国仮出願第６０／７２０，４４５号の３５Ｕ．Ｓ．Ｃ．§１１９（ｅ）に基づく先行出願日の利益を請求するものである。

【００１９】

汎用ブートストラッピングアーキテクチャを利用してキーをリフレッシュするための装置、方法およびソフトウェアが開示されている。以下の記述では、説明を目的として、本

発明の実施形態を徹底的に理解できるようにするために数多くの特定的詳細が示されている。しかしながら、当業者にとっては、本発明の実施形態をこれらの特定的詳細無しでまたは同等の配置を用いて実践することもできるということは明らかである。その他の例においては、本発明の実施形態を不必要にあいまいにしないようにブロックダイアグラム形態で周知の構造および装置が示されている。

【００２０】

さらに、本発明の実施形態はスペクトラム拡散システムに関して論述されているものの、当業者は、本発明の実施形態があらゆるタイプの無線通信システムならびに有線ネットワークに対し応用可能であるということを認識している。さらに、本書で記述されているプロトコルおよびプロセスは、移動体および／または無線デバイスによってのみならず、あらゆる固定式（または非移動体式）通信デバイス（例えばデスクトップコンピュータ、ネットワークアプライアンスなど）またはネットワークエレメントまたはノードによっても実施可能であると考えられている。

【００２１】

本発明のさまざまな実施形態が、３ＧＰＰ（ユニバーサル・モバイル・テレコミュニケーション・システム（ＵＭＴＳ））および３ＧＰＰ２（ｃｄｍａ２０００）といったようなスペクトラム拡散ネットワーク内でのキーリフレッシュメカニズムに関係している。一実施形態による発明は、符号分割多元接続（ＣＤＭＡ）ＥＶ－ＤＯ（エボリューション・データ専用）ネットワーク内での第３世代パートナシッププロジェクト（３ＧＰＰ２）汎用ブートストラッピングアーキテクチャ（ＧＢＡ）機能性を用いた無線ネットワークにおけるｃｄｍａ２０００ＩＰデータ接続性および可動性サポートのための手順を提供している。一例として、典型的なブートストラッピング手順は、本書にその全体が参考として内含されている３ＧＰＰＴＳ３３．２２０、３ＧＰＰＴＳ２４．１０９および３ＧＰＰ２Ｓ．ＰＯ１０９の中で定義されている。

【００２２】

種々の典型的実施形態に従って、キープロビジョニングアプローチは無線ネットワーク環境という状況下で論述されているものの、これをＣＤＭＡ２０００とＷｉＭａｘ（マイクロ波アクセス用世界的相互運用性）アクセス間の相互作用または３ＧＰＰネットワークとＷＬＡＮＩＷまたはＷｉＭａｘアクセス間の対話といったようなその他の環境にも応用することも可能である。

【００２３】

図１は、本発明の種々の実施形態による、キーリフレッシュを提供する能力をもつ典型的ブートストラッピングアーキテクチャを示す図である。例示を目的として、ブートストラッピングアーキテクチャ１００は、３ＧＰＰ２（第３世代パートナシッププロジェクト２）における汎用ブートストラッピングアーキテクチャ（ＧＢＡ）に関連して説明されている。ＧＢＡは、３ＧＰＰ／３ＧＰＰ２（第３世代パートナシッププロジェクト／第３世代パートナシッププロジェクト２）において定義された汎用認証アーキテクチャ（ＧＡＡ）の１構成要素である。基本的エレメントとしては、ＵＥ（ユーザ機器：Ｕｓｅｒ Ｅｑｕｉｐｍｅｎｔ）１０１、ブートストラッピングを担当するブートストラッピングサーバ機能（ＢＳＦ）１０３およびネットワークアプリケーション機能（ＮＡＦ）１０５が含まれる。典型的実施形態においては、ＮＡＦ１０５は、サーバといったようなあらゆるタイプのネットワークエレメントの中でホストされ得る。従って、ＮＡＦ１０５は、導出された安全キーを用いる上でＵＥ１０１が通信するアプリケーションサーバとして役立つことができる。本書で使用されている（さまざまな実施形態に従った）「アプリケーション」という用語は通信サービスを意味し、アプリケーションサーバ内部の１アプリケーションの実際のインスタンスに制限されていない。

【００２４】

ＢＳＦ１０３は、システム１００内でのブートストラッピング手順の後に加入者のブートストラッピング情報を処理する。ブートストラッピング手順はＵＥ１０１とＢＳＦ１０３の間のセキュリティアソシエーションを作り上げる。記憶されたユーザのブートストラ

ッピング情報およびセキュリティアソシエーションを用いて、ＢＳＦ１０３は、ＵＥ１０１が接触したネットワークアプリケーション機能（例えばＮＡＦ１０５）に対する安全なサービスを提供することができる。本明細書で使用される「安全なサービス」には、安全な形でサービスを提供することが関与する。ブートストラッピングは、例えばＵＥ１０１とネットワークの間に維持された長期共有秘密などに基づいてＵＥ１０１とＢＳＦ１０３の間で実施可能である。ブートストラッピングが完了した後、ＵＥ１０１およびＮＡＦ１０５は、メッセージの認証または一般にそのセキュリティがブートストラッピング中に合意されたキーから導出されたセッションキーに基づくことになる一部のアプリケーション特定プロトコルを実行することができる。メッセージのセキュリティには、認証、許可、機密性および完全性保護が含まれるがこれらに制限されるわけではない。

【００２５】

ＢＳＦ１０３およびＵＥ１０１は、後でＵＥ１０１とＮＡＦ１０５との間で使用するためのセッションキーを導出するのに使用されるキーを互いにを認証しこれに合意する。ＢＳＦ１０３は、キー導出手順を用いることにより、特定のＮＡＦ（例えばＮＡＦ１０５）にキーマテリアルの応用可能性を制限することができる。典型的実施形態においては、ブートストラッピング手順の後、ＵＥ１０１およびＢＳＦ１０３の両方共がキーマテリアル（Ｋｓ）、ブートストラッピングトランザクション識別子（Ｂ－ＩＴＤ）、キーマテリアル寿命およびその他のパラメータについて合意しており、ＮＡＦ１０５に対応するキーマテリアル（「Ｋｓ_ＮＡＦ」と記されている）およびＢ－ＴＩＤは、ＵＥ１０１とＮＡＦ１０５との間のトラヒックを相互に認証し任意にはこれを保護するためにＵａインタフェース内で使用され得る。「移動局（ＭＳ）」、「ユーザ機器（ＵＥ）」、「ユーザ端末」および「移動ノード（ＭＮ）」という用語は、あらゆるタイプのクライアントデバイスまたは端末を表わすために状況に応じて互換的に使用されている。例えば、３ＧＰＰ標準はＵＥという用語を用い、３ＧＰＰ標準はＭＳを採用し、一方ＭＮはインタネットプロトコル（ＩＰ）関連の状況下で用いられている。例えばＵＥ１０１は、移動体通信デバイスまたは携帯電話またはその他の無線デバイスであり得る。ＵＥ１０１は、トランシーバ能力をもつ携帯情報端末（ＰＤＡ）またはトランシーバ能力をもつパーソナルコンピュータといったようなデバイスでもあり得る。ＵＥ１０１は、ＢＳＦ１０３と通信するため無線通信トランシーバを用いて送受信する。ＢＳＦ１０３は、ホームロケーションレジスタ１０９との間でデータを送受信する。

【００２６】

図示した通り、ブートストラッピングシステム１００をサポートするために一定数の基準点Ｕｂ、Ｕａ、Ｚｈ１、Ｚｈ２、Ｚｈ３およびＺｎが定義されている。基準点Ｕｂは、ＵＥ１０１とＢＳＦ１０３との間の相互認証を提供し、ＵＥ１０１がキーマテリアルＫｓをブートストラップできるようにする。Ｕａインタフェースは、ＵＥ１０１とＢＳＦ１０３の間の合意されたキーマテリアルＫｓから導出されたキーマテリアルにより安全保護されるアプリケーションプロトコルを搬送している。Ｚｈ１、Ｚｈ２およびＺｈ３基準点は、要求された認証情報およびユーザセキュリティ設定値を、ＢＳＦ１０３とホーム加入者システム（ＨＳＳ）１０７（ここでは、ブートストラッピングにおいて認証およびキー合意（ＡＫＡ）が使用される）、ホームロケーションレジスタ（ＨＬＲ）１０９（ここではＣＡＶＥ（セルラ認証および音声暗号化）アルゴリズムを用いてブートストラップすることができる）、および認証、許可およびアカウンティング（ＡＡＡ）サーバ１１１（ここではブートストラッピングにおいてＭＮ－ＡＡＡキーが用いられる）との間で交換する目的で利用される。Ｚｎインタフェースは、ＮＡＦ１０５が導出されたキーマテリアルおよびアプリケーション特定ユーザセキュリティ設定値をＢＳＦ１０３からフェッチすることができるようにする。

【００２７】

ＧＢＡオペレーションは、典型的実施形態に従うと、以下の通りである。ＵＥ１０１とＢＳＦ１０３（ホームネットワーク内にあるもの）との間でブートストラッピング手順が実施される。ブートストラッピングの間に、ＭＳ１０１とホームネットワークとの間の長

期共有秘密に基づいてＭＳ１０１とネットワークとの間で相互認証が実施される。例えば３ＧＰＰ２においては、この長期共有秘密は、ＨＳＳ１０７、ＨＬＲ１０９、およびＡＡＡサーバ１１１内に記憶され得る。３ＧＰＰにおいては、ブートストラッピングはＡＫＡまたは加入者識別モジュール（ＳＩＭ）認証のいずれかに基づいている。ブートストラッピング手順の結果として、ブートストラッピングキーKsがＭＳ１０１およびＢＳＦ１０３の両方によって生成される。Ｋｓは、同様にブートストラッピングトランザクション識別子（Ｂ－ＴＩＤ）および、キーＫｓの失効または継続時間に関する値を提供する寿命とも結びつけられる。

【００２８】

次のステップとして、ＭＳ１０１は、ＮＡＦ１０５と呼ばれるネットワーク内のアプリケーション機能に対して、アプリケーションについての共有秘密を提供するのにＧＢＡを使用できるということを標示する。代替的には、ＮＡＦ１０５は、ＧＢＡが使用されるはずであることをＭＳ１０１に標示することができる。その後、ＮＡＦ１０５はＢＳＦ１０３からKs_ＮＡＦを検索する。同時にＭＳは同じKs_ＮＡＦを導出する。Ks_ＮＡＦは次に、任意のさらなるセキュリティオペレーションのためにＭＳ１０１とＮＡＦ１０５の間の共有秘密として使用される。セキュリティを追加するために、キーは定期的にかまたは要望に応じてリフレッシュされる。

【００２９】

システム１００内でキーをリフレッシュするプロセスについてここで記述する。

【００３０】

図２Ａおよび２Ｂは、該発明のさまざまな実施形態に従ったキーリフレッシュプロセスのフローチャートである。図２Ａに示されているように、キーをリフレッシュする一般的プロセスには、ステップ２０１にあるように、そのキーがリフレッシュを必要としているか否かを決定する段階が関与している。次に、ステップ２０３を通して、新しいブートストラッピング手順を実施することなくキーをリフレッシュするために、システム１００のブートストラッピングアーキテクチャが利用される。例えば、３ＧＰＰ２ＧＢＡにおいては、このＮＡＦキーリフレッシュメカニズムにより、ＮＡＦキーは、新しいブートストラッピングを実施する必要なくリフレッシュされ得ることになる。新しいブートストラッピング手順を開始するのは、計算、エアインタフェースおよびＵＥ１０１およびネットワークの両方におけるその他の資源に関してコストが高くつくことである。従って、プロセスがいつブートストラップするべきかそしていつリフレッシュするべきかを決定することが重要である（これは図２Ｂに関して説明されている）。

【００３１】

実施すべきプロセスについてＭＮ１０１に命令する（すなわちキーリフレッシュメカニズムを実行するかまたは新しいブートストラップを実施する）標示または識別子を提供するようにＵａプロトコルを修正できるということが認識されている。しかしながら、ある種の状況下では、Ｕａプロトコルは、かかる標示をサポートしない可能性があり、さらに、プロトコルを修正することは望ましくないかもしれない。

【００３２】

以下の手順は有利にも、プロトコルの修正は回避するが、従来のアプローチ内のあいまいさ（例えば現行のＧＢＡ仕様）には対処している。ＭＮ１０１はＮＡＦ（例えばＮＡＦ１０５）と接触する前に有効なKsを必要とする。有効なKsが存在しない場合、ＭＮ１０１は、ＮＡＦ１０５と接触する前に新しいブートストラッピング手順を実施する。この例では、ＮＡＦ１０５がキーリフレッシュメカニズムをサポートすることが仮定されるが、かかるメカニズムはＭＮ１０１に対するオプションとなっている。

【００３３】

ステップ２１１では、ＮＡＦ１０５はＭＮ１０１からアプリケーション要求を受理する。ＮＡＦ１０５が（クレデンシャルを含む）ＭＮ１０１からの要求を拒絶した場合には、ＭＮ１０１は、リフレッシュメカニズムがＭＮ１０１によりサポートされていると仮定して、そのキーをリフレッシュする。そうでなければ、ＭＮ１０１はブートストラッピング

を実施する。ＮＡＦ１０５は、典型的な実施形態においては、Ｂ－ＴＩＤといったようなトランザクション識別子に基づいて、新しいブートストラッピングが実施されたことをＭＮ１０１が標示しているかまたはＭＮ１０１が、Ｂ－ＴＩＤといったようなトランザクション識別子に基づいてそのキーをリフレッシュしようとしているかを決定することができる（ステップ２１３）。Ｂ－ＴＩＤが、ステップ２１５で決定されている通り先行するトランザクションで使用されたものと同じである（すなわち整合する）場合には、ＭＮ１０１はリフレッシュを実施する（ステップ２１７）。そうでなければ、新しいブートストラッピング手順が実施された（ステップ２１９）。

【００３４】

図３は、セッションキーをリフレッシュするための従来のブートストラッピング手順のダイアグラムである。このアプローチは、３ＧＰＰ２仕様Ｓ．ＰＯ１０９で記述されたＮＡＦキーリフレッシュメカニズムに追従し、図４～７に詳しく示されているリフレッシュメカニズムと対比される目的で説明される。図３のシナリオでは、ＵＥ１０１が最初から、ＧＢＡにより導出されたセキュリティマテリアルがUaインタフェースを安全保護するために使用されることになる、ＮＡＦキー（Ｋｓ_ＮＡＦ）をリフレッシュする必要があることに気づいている、ということが仮定されている。ステップ３０１では、ＵＥ１０１はアプリケーション要求をＮＡＦ１０５に送る。要求は、必ずしも明示的に提供される必要のないトランザクション識別子（例えばブートストラッピングトランザクション識別子、Ｂ－ＴＩＤ）、アプリケーションプロトコルメッセージ（「ｍｓｇ」と示されている）、メッセージ認証コード（ＭＡＣ）、およびＵＥ１０１により提供される乱数であるＵＥノンス（$RAND_{UE}$）を含む。「ｍｓｇ」は、アプリケーション特異的データセットを表わす。ＭＡＣは、特定のメッセージを認証するために用いられる予め定められた値である。

【００３５】

次に、ＮＡＦ１０５は、$RAND_{NAF}$と呼ばれる乱数を選択する。ＮＡＦ１０５はこのときステップ３０３にあるようにＢＳＦ１０３に対して認証要求を送る。要求には、Ｂ－ＴＩＤ、$RAND_{UE}$、$RAND_{NAF}$、およびＮＡＦ１０５の完全に修飾ドメイン名（ＦＱＤＮ）であるＮＡＦ＿Ｉｄが含まれる。ＢＳＦ１０３は、受信したＢ－ＴＩＤに基づいてＫｓを検索する。ＢＳＦ１０３はこのとき、Ｋｓ、$RAND_{UE}$、$RAND_{NAF}$、ＮＡＦ＿Ｉｄそして場合によってはその他の情報から新しいＫｓ＿ＮＡＦを導出する。ＢＳＦ１０３は、その寿命と共にＫｓ＿ＮＡＦを、そして場合によってはユーザプロファイルを、ステップ３０５を通して認証回答メッセージ内でＮＡＦ１０５に戻す。「Ｐｒｏｆ」は、ユーザプロファイルのアプリケーション特定パート（または部分）を示す。ＮＡＦ１０５は、ステップ３０７にあるように、Ｋｓ＿ＮＡＦ、その付随する寿命、およびユーザプロファイルを記憶し、アプリケーション回答メッセージの中でＵＥ１０１に対し$RAND_{NAF}$を送る（ステップ３０９）。ＵＥ１０１が最終的に$RAND_{NAF}$を受信するこの時点で初めて、ＵＥ１０１はリフレッシュされたＫｓ＿ＮＡＦを計算することができる、という点が指摘される。

【００３６】

以上の従来のＮＡＦキーリフレッシュメカニズムには、残念なことに、ＵＥ１０１からのノンスとＮＡＦ１０５からのノンスの両方が関与し、ＵＥ１０１はこのノンスを最初に送らなくてはならない。この融通性のなさのため、ＵＥ１０１およびＮＡＦ１０５は、ＮＡＦキーがリフレッシュされ得る前に多数のメッセージを交換しなければならない可能性があり、これは貴重な無線資源を無駄にするばかりでなく、さらに大きな遅延を導入する。さらに、ノンスは、既存のＵａプロトコル内で送付されなくてはならない。しかしながら、全てのＵａプロトコルが両方向でのノンスの搬送をサポートするわけではない。

【００３７】

現行のＧＢＡ標準が、ブートストラッピングプロセスのリフレッシュまたは再開始の検出に関して不明瞭であるということが指摘される。特に、ＮＡＦ１０５は新しいブートストラッピングを実施するようＵＥ１０１に要求する能力をもつ。明示的な標示をサポートしないＵａプロトコルについては、ＵＥ１０１は、いつリフレッシュすべきかまたはいつ

再度ブートストラップすべきかがわからなくなる。本発明の一実施形態によるアプローチはこの不明瞭さを無くするものである。

【００３８】

本発明の種々の実施形態が、図３の従来のメカニズムに比べて単純化された複数のＮＡＦキーリフレッシュメカニズムを提供する。さらに、本アプローチは有利にも、Ｕａインタフェース上の既存のプロトコルに対する修正を最小限におさえながら、キーをリフレッシュするためのメカニズムを提供している。

【００３９】

図４～７は、ＮＡＦキーリフレッシュメカニズムを実施するための種々の実施形態を例示している。

【００４０】

図４は、本発明の一実施形態による２つのノンスを利用することによりセッションキーをリフレッシュするための手順を示す図である。この実施形態においては、２つのノンスが利用され、ここでＮＡＦ１０５は１つのノンスをまず最初に送ることができる。すなわち$RAND_{UE}$および$RAND_{NAF}$の両方が使用されるが、ＮＡＦ１０５は、そのノンスを最初に送ることが許されており、かくして、ＵＥ１０１はリフレッシュされたＫｓ＿ＮＡＦ１０５をより早く導出することができることになる。このオペレーションは以下のように説明される。

【００４１】

ステップ４０１で、ＵＥ１０１は、Ｂ－ＴＩＤおよびアプリケーションプロトコルメッセージ（図中「ｍｓｇ」と記されている）を伴うアプリケーション要求を送る。ＮＡＦ１０５は、ステップ４０３を通して、Ｋｓ＿ＮＡＦがリフレッシュされるべきであるという標示（これは暗示的であり得る）と共に、アプリケーション回答を送る。ＮＡＦ１０５は同様に「積極的に」その独自のノンス$RAND_{NAF}$をも内含する。ＮＡＦ１０５は同様に、認証チャレンジをも内含し得る。

【００４２】

次に、ＵＥ１０１は、その独自の乱数$RAND_{UE}$を選択する。この時点で、ＵＥ１０１は、リフレッシュされたＫｓ＿ＮＡＦ１０５を導出することができる。ＵＥ１０１は、場合によってはリフレッシュされたＫｓ＿ＮＡＦ１０５に基づいてクレデンシャルと共に、アプリケーション要求を送る（ステップ４０５）。要求は同様に、Ｂ－ＴＩＤ、アプリケーションプロトコルメッセージおよび$RAND_{UE}$をも含む。ステップ４０７では、ＮＡＦ１０５は次に認証要求をＢＳＦ１０３に送る。要求はＢ－ＴＩＤ、$RAND_{UE}$、$RAND_{NAF}$およびＮＡＦ＿Ｉｄを含む。ＮＡＦ＿Ｉｄは、ＮＡＦ１０５の完全修飾ドメイン名である。

【００４３】

その後、ＢＳＦ１０３は、受信されたＢ－ＴＩＤに基づいてＫｓを検索する。ＢＳＦ１０３はその後、Ｋｓ、$RAND_{UE}$、$RAND_{NAF}$、ＮＡＦ＿Ｉｄそして場合によってはその他の情報から新しいＫｓ＿ＮＡＦを導出する。ＢＳＦ１０３は、その寿命そして任意にはユーザプロファイルと合せてＫｓ＿ＮＡＦを、ステップ４０９を通して認証回答メッセージ内でＮＡＦ１０５に転送する。前述のとおり、「Ｐｒｏｆ」は、ユーザプロファイルのアプリケーション特定パートまたは部分を表わす。

【００４４】

ステップ４１１では、ＮＡＦ１０５は、Ｋｓ＿ＮＡＦ、その付随する寿命およびユーザプロファイルを記憶する。この時点で、ＮＡＦ１０５は、Ｋｓ＿ＮＡＦを用いて（ステップ４０５内で）ＵＥ１０１により送られたクレデンシャルを確認することができる。成功した場合、ＵＥ１０１は認証され、アプリケーション回答はＵＥ１０１に送り戻される。ＮＡＦ１０５かその$RAND_{NAF}$を最初に送ることができるようにすることによって、Ｋｓ＿ＮＡＦは従来のアプローチよりも早くＵＥ１０１において利用可能となる。

【００４５】

図４の上述のアプローチでは、キーリフレッシュを効率良く提供するために２つのノン

スが利用される。代替的には、セッションキーをリフレッシュするために単一のノンスのみ（$RAND_{UE}$または$RAND_{NAF}$のいずれか、ただし両方ではない）を使用することができる。従って、２つのケースすなわち（１）（図５に示されている）$RAND_{UE}$および（２）（図６に示されている）$RAND_{NAF}$が存在する。

【００４６】

図５は、本発明の実施形態に従った、ネットワークアプリケーションの乱数を利用することによりセッションキーをリフレッシュするための手順を示す図である。このケースは、ＵＥ１０１がＮＡＦ１０５と接触する前に、Ｋｓ＿ＮＡＦがリフレッシュされる必要があることを知らない場合にあてはまり得る。図示されている通り、ＵＥ１０１は、ステップ５０１の場合と同様に、Ｂ－ＴＩＤそしてアプリケーションプロトコルメッセージ（「ｍｄｇ」と示されている）を伴うアプリケーション要求を送る。ステップ５０３では、ＮＡＦ１０５は、Ｋｓ＿ＮＡＦがリフレッシュされるべきであるという（明示されないことがある）標示と共に、アプリケーション回答を送る。ＮＡＦ１０５は同様に、その独自のノンス$RAND_{NAF}$を「積極的に」内含する。ＮＡＦ１０５は同様に、認証チャレンジ（図示せず）をも含み得る。

【００４７】

この時点で、ＵＥ１０１は、Ｋｓ、$RAND_{NAF}$、ＮＡＦ＿Ｉｄそして場合によってはその他の情報からのリフレッシュされたＫｓ＿ＮＡＦ１０５を導出することができるが、$RAND_{UE}$から導出することはできない。従ってＵＥ１０１は、新たにリフレッシュされたＫｓ＿ＮＡＦ（図示せず）に基づくものであるクレデンシャルを含み得る。ＵＥ１０１は、ステップ５０５を通して新しいアプリケーション要求を送る。要求は同様にＢ－ＴＩＤおよびアプリケーションプロトコルメッセージをも含む。

【００４８】

ステップ５０７においては、ＮＡＦ１０５は、ＢＳＦ１０３に対し認証要求を送る。１例を挙げると、該要求は、Ｂ－ＴＩＤ、$RAND_{NAF}$およびＮＡＦ＿Ｉｄ（ＮＡＦ１０５の完全修飾ドメイン名）を含む。ＢＳＦ１０３は、受信したＢ－ＴＩＤに基づいてＫｓを検索する。ＢＳＦ１０３は次に、Ｋｓ、$RAND_{NAF}$そしてＮＡＦ＿Ｉｄから新しいＫｓ＿ＮＡＦを導出する。これらのパラメータに加えて、導出はその他の情報に基づくものでもあり得る。ＢＳＦ１０３は、ＮＡＦ１０５への伝送のため、認証回答メッセージ内でＫｓ＿ＮＡＦ、付随する寿命およびユーザプロファイル（任意）を特定する（ステップ５０９）。

【００４９】

ＮＡＦ１０５は、ステップ５１１の場合と同様に、Ｋｓ＿ＮＡＦ、その付随する寿命およびユーザプロファイルを記憶する。この時点で、ＮＡＦ１０５は、Ｋｓ＿ＮＡＦを用いてステップ５０５内でＵＥ１０１により送られたクレデンシャルを確認することができる。成功した場合、ＵＥ１０１は認証され、アプリケーション回答がＵＥ１０１に対して発行される。

【００５０】

図６は、本発明の一実施形態に従って、ユーザ機器の乱数（例えば$RAND_{UE}$）を利用することによりセッションキーをリフレッシュするための手順を示す図である。このケースは、ＵＥ１０１が、ＮＡＦ１０５と接触した時点でＫｓ＿ＮＡＦをリフレッシュする必要があるということを知っている場合にあてはまり得る。ステップ６０１では、ＵＥ１０１は、Ｂ－ＴＩＤ、$RAND_{UE}$およびアプリケーションプロトコルメッセージを伴うアプリケーション要求を送る。基本的に、ＵＥ１０１は極く最初にＫｓ＿ＮＡＦキーをリフレッシュすることを望んでいる。その結果ＵＥ１０１はすでにリフレッシュされたＫｓ＿ＮＡＦを利用できる状態にあり、従って、リフレッシュされたＫｓ＿ＮＡＦ（図示せず）に基づいてクレデンシャルを含み得る。

【００５１】

ステップ６０３では、ＮＡＦ１０５は認証要求をＢＳＦ１０３に送る。要求はＢ－ＴＩＤ、$RAND_{UE}$およびＮＡＦ＿Ｉｄを含む。ＢＳＦ１０３は、受信したＢ－ＴＩＤに基づ

いてＫｓを検索し、次にＫｓ、$ＲＡＮＤ_{UE}$、ＮＡＦ＿Ｉｄおよび場合によってはその他の情報から新しいＫｓ＿ＮＡＦを導出する。ＢＳＦ１０３は、ＮＡＦ１０５に対して、１つの認証回答メッセージ内でユーザプロファイルおよびＫｓ＿ＮＡＦとその寿命を伝送する（ステップ６０５）。

【００５２】

ステップ６０７では、ＮＡＦ１０５はＫｓ＿ＮＡＦ、付随する寿命およびユーザプロファイルを記録する。ＮＡＦ１０５は、Ｋｓ＿ＮＡＦを用いてステップ６０１内でＵＥ１０１により送付されたクレデンシャルを確認することができる。成功した場合、ＵＥ１０１は認証され、ステップ６０９を通してＵＥ１０１にアプリケーション回答が送り戻される。

【００５３】

一定の与えられたＫｓおよびＮＡＦ１０５については、同じ$ＲＡＮＤ_{UE}$は同じＫｓ＿ＮＡＦを結果としてもたらすことになるということが指摘される。従って、ＵＥ１０１が、特定の１Ｋｓの寿命全体にわたり２回以上同じ$ＲＡＮＤ_{UE}$を使用しないことが望ましいかもしれない。ある実施形態においては、ＮＡＦ１０５は、２重使用を回避するべく特定のＢ－ＴＩＤが利用を監視するようにＵＥ１０１により以前に使用された$ＲＡＮＤ_{UE}$のリストを維持することができる。

【００５４】

図７は、本発明の一実施形態による、ブートストラッピングサーバ機能（ＢＳＦ）が関与することなく、セッションキーをリフレッシュするための手順を示す図である。図７に示されているように、アプリケーションキーはＢＳＦが関与することさえなく、リフレッシュされ得る。これは、キー導出の追加レベルを導入し、かくして、初期Ｋｓ＿ＮＡＦをシードとして用いて、アプリケーションにより実際に用いられているキーであるセッションキーＳＫを導出することによって達成される。このプロセスについて以下で説明する。

【００５５】

ステップ７０１～７０９は、図３のステップ３０１～３０９と類似している。すなわちこれらのステップ７０１～７０９は、現在３ＧＰＰ／３ＧＰＰ２ＧＢＡ仕様書中で規定されているようなキーリフレッシュの無い基本的なブートストラッピング利用手順を捕捉する。ステップ４０７の終りで、ＵＥ１０１およびＮＡＦ１０５の両方共が同じＫｓ＿ＮＡＦを有する。すなわち、ＵＥ１０１はステップ７１１にある通り、Ｋｓ＿ＮＡＦを導出することができる。図７のアプローチの下では、このＫｓ＿ＮＡＦは、ＵＥ１０１とＮＡＦ１０５の間で使用されるべきさらなるセッションキーを導出するためのシードとして使用される。

【００５６】

アプリケーションセッションをセットアップしなければならない場合、ＵＥ１０１はＮＡＦ１０５に対しアプリケーション要求を送り（ステップ７１３）、これにはＢ－ＴＩＤ、プロトコルメッセージ、ＭＡＣおよび$ＲＡＮＤ_{UE}$が含まれ得る。アプリケーション要求を受理した時点で、ＮＡＦ１０５は、Ｋｓ＿ＮＡＦが存在することを決定する。ＮＡＦ１０５は、$ＲＡＮＤ_{NAF}$を選択し、Ｋｓ＿ＮＡＦ、$ＲＡＮＤ_{UE}$、$ＲＡＮＤ_{NAF}$および場合によってはその他の情報に基づいてフレッシュセッションキーＳＫを導出する（ステップ７１５）。ＮＡＦ１０５は、ＵＥ１０１に対するアプリケーション回答の中で$ＲＡＮＤ_{NAF}$を転送する（ステップ７１７）。

【００５７】

この段階で、ＵＥ１０１はまた、ステップ７１９にあるように、ＮＡＦ１０５のものと類似する要領でセッションキーＳＫをも導出する。この時点以降、ＳＫは、ＵＥ１０１とＮＡＦ１０５の間に安全なセッションを確立するために使用可能である。ＢＳＦ１０３はこのＳＫ生成プロセスに関与しないという点が指摘される。このアプローチは、ＢＳＦ１０３の作業負荷を削減するという付加的な利点を有する。

【００５８】

各々の新しいセッションについては、ステップ７１３および７１７を反復することによ

って新しいＳＫが生成可能である。$ＲＡＮＤ_{UE}$および$ＲＡＮＤ_{NAF}$は両方共以上の記述において使用されているものの、（前述した通り）単一のノンスを使用することも可能であるという点が指摘される。

【００５９】

３ＧＰＰおよび３ＧＰＰ２ネットワークの認証インフラストラクチャを活用することによって、汎用ブートストラッピングアーキテクチャ（ＧＢＡ）は、ＵＥ１０１とホームネットワーク（ＢＳＦ１０３）の間の共有秘密のブートストラッピングを可能にし、次にこれを用いてＵＥ１０１とＮＡＦ１０５の間で使用すべきさらなる共有秘密を導出することができる、ということが認識されている。

【００６０】

当業者であれば、キーをリフレッシュするためのプロセスを、ソフトウェア、ハードウェア（例えば汎用プロセッサ、デジタル信号処理（ＤＳＰ）チップ、アプリケーション特異的集積回路（ＡＳＴＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）など）、ファームウェアまたはそれらの組合せを介して実装することができるということを認識するものと思われる。記述された機能を実施するためのこのような典型的ハードウェアが、以下で図８に関して詳述される。

【００６１】

図８は、本発明の種々の実施形態をその上に実装できる典型的ハードウェアを例示している。計算システム８００には、母線８０１または情報を通信するためのその他の通信メカニズム、および情報処理のために母線８０１に結合されるプロセッサ８０３が含まれている。計算システム８００は同様に、プロセッサ８０３が実行すべき命令および情報を記憶するために母線８０１に結合されるランダムアクセスメモリ（ＲＡＭ）またはその他のダイナミック記憶デバイスといったような主メモリ８０５をも内含している。主メモリ８０５は、プロセッサ８０３による命令の実行中に一時的数値変数またはその他の中間情報を記憶するためにも使用可能である。計算システム８００は、さらに、プロセッサ８０３のための命令および静的情報を記憶するために、母線８０１に結合された読取り専用メモリ（ＲＯＭ）８０７またはその他の静的記憶デバイスをも含み得る。情報および命令を永続的に記憶するために、磁気ディスクまたは光ディスクといったような記憶デバイス８０９が母線８０１に結合される。

【００６２】

計算システム８００は、ユーザに対し情報を表示するため、液晶ディスプレイまたはアクティブマトリクスディスプレイといったようなディスプレイ８１１に対し、母線８０１を介して結合可能である。英数字およびその他のキーを内含するキーボードといったような入力デバイス８１３を、プロセッサ８０３に情報およびコマンドセレクションを通信する目的で母線８０１に結合することができる。入力デバイス８１３は、プロセッサ８０３に方向情報およびコマンドセレクションを通信するためおよびディスプレイ８１１上のカーソル動作を制御するために、マウス、トラックボールまたはカーソル方向キーといったようなカーソル制御機構を含み得る。

【００６３】

該発明のさまざまな実施形態に従うと、本書に記述されているプロセスは、主メモリ８０５内に収納された命令の配置をプロセッサ８０３が実行したのに応答して、計算システム８００によって提供され得る。かかる命令は、記憶デバイス８０９といったようなもう１つのコンピュータ可読な媒体から、主メモリ８０５内に読取られ得る。主メモリ８０５内に収納された命令の配置が実行されたことにより、プロセッサ８０３は本書に記述されたプロセスステップを実施させられることになる。多重処理配置内の単数または複数のプロセッサを利用して、主メモリ８０５内に収納された命令を実行することも可能である。変形形態においては、本発明の実施形態を実装するためにソフトウェア命令の代りにかまたはそれと組合せた形で配線回路を使用することができる。もう１つの例においては、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）といったような再構成可能なハードウェアを使用することができ、ここではその論理ゲートの機能性および接続形態を、標準的

にはメモリルックアップテーブルをプログラミングすることによって、ランタイムでカスタマイズすることができる。かくして、本発明の実施形態は、ハードウェア回路およびソフトウェアの何らかの特定的組合せに制限されない。

【００６４】

計算システム８００は同様に、母線８０１に結合された少なくとも１つの通信インタフェース８１５をも含んでいる。通信インタフェース８１５は、ネットワークリンク（図示せず）に対する２方向データ通信結合を提供する。通信インタフェース８１５は、種々のタイプの情報を表わすデジタルデータストリームを搬送する電気、電磁または光通信を送受信する。さらに通信インタフェース８１５は、ユニバーサル・シリアル・バス（ＵＳＢ）インタフェース、ＰＣＭＣＩＡ（パソコンメモリカード国際協会）インタフェースなどといった周辺インタフェースデバイスを内含し得る。

【００６５】

プロセッサ８０３は、伝送されたコードを受信中に実行し、および／または、本コードを後で実行するために記憶デバイス８０９またはその他の不揮発性記憶装置内に記憶することができる。このようにして、計算システム８００は、搬送波の形でアプリケーションコードを得ることができる。

【００６６】

本書で使用されている「コンピュータ可読媒体」という用語は、実行のためにプロセッサ８０３に対する命令を提供することに参与するあらゆる媒体を意味する。かかる媒体は、不揮発性媒体、揮発性媒体および伝送媒体を含めた（ただしこれらに制限されるわけではない）数多くの形態をとり得る。不揮発性媒体には、例えば、光ディスクまたは磁気ディスク例えば記憶デバイス８０９が含まれる。揮発性媒体には、主メモリといったダイナミックメモリが含まれる。伝送媒体には、母線８０１を含む電線を内含する同軸ケーブル、銅線および光ファイバが含まれる。伝送媒体は同様に、無線周波数（ＲＦ）および赤外線（ＩＲ）データ通信の間に生成されるものといったような音波、光波または電磁波の形も取り得る。コンピュータ可読媒体の一般的な形態としては、例えばフロッピー（登録商標）ディスク、フレキシブルディスク、ハードディスク、磁気テープ、その他の任意の磁気媒体、ＣＤ－ＲＯＭ、ＣＤＲＷ、ＤＶＤ、その他の任意の光媒体、パンチカード、紙テープ、光マークシート、孔またはその他の光学的に認識可能なインデックスのパターンを伴うその他の物理的媒体、ＲＡＭ、ＰＲＯＭおよびＥＰＲＯＭ、フラッシュＥＰＲＯＭ、任意のその他のメモリチップまたはカートリッジ、搬送波またはコンピュータが読み取ることのできる任意のその他の媒体が含まれる。

【００６７】

実行のためにプロセッサに命令を提供することには、さまざまな形態のコンピュータ可読媒体が関与し得る。例えば、本発明の少なくとも一部分を実施するための命令は、遠隔コンピュータの磁気ディスク上に当初担持され得る。かかるシナリオでは、遠隔コンピュータは命令を主メモリ内にロードし、モデムを用いて電話回線上で命令を送る。局所システムのモデムが電話回線上でデータを受信し、赤外線送信機を用いてそのデータを赤外線信号に変換し、赤外線信号を携帯情報端末（ＰＤＡ）またはラップトップといったような携帯式計算デバイスに伝送する。携帯式計算デバイス上の赤外線検出器は、赤外線信号が担持する情報および命令を受信し、データを母線上に置く。母線はデータを主メモリに搬送し、そこからプロセッサが命令を検索し実行する。主メモリが受信した命令は任意には、プロセッサによる実行の前または後のいずれかで記憶デバイス上に記憶され得る。

【００６８】

図９Ａおよび９Ｂは、発明のさまざまな実施形態をサポートする能力をもつ異なるセルラー方式移動電話を示す図である。図９Ａおよび９Ｂは、トランシーバが（デジタル信号プロセッサ（ＤＳＤ）の一部分として）、設置されている基地局および移動局（例えば送受話器）の両方、基地局および移動局内の半導体デバイスおよび／またはハードウェア、ソフトウェア、集積回路を各々が伴う典型的なセルラー方式移動電話システムを示している。一例を挙げると、無線ネットワークは、世界共通の次世代携帯電話システム２０００

（ＩＭＴ－２０００）のために国際電話通信連合（ＩＴＵ）が定義したような第２および第３世代（２Ｇおよび３Ｇ）サービスをサポートする。説明を目的として、無線ネットワークの搬送波およびチャンネル選択について、ｃｄｍａ２０００アーキテクチャに関連して説明する。ＩＳ－９５の第３世代バージョンとして、ｃｄｍａ２０００が第３世代パートナシッププロジェクト２（３ＧＰＰ２）の中で標準化されつつある。

【００６９】

無線ネットワーク９００には、基地局サブシステム（ＢＳＳ）９０３と通信状態で、移動局９０１（例えば送受話器、端末、局、ユニット、デバイスまたはユーザに対する任意のタイプのインタフェース（例えば「ウェアラブル」回路など））が含まれている。本発明の１実施形態に従うと、無線ネットワークは、世界共通の次世代携帯電話システム２０００（ＩＭＴ－２０００）のために国際電気通信連合（ＩＴＵ）が定義したような第３世代（３Ｇ）サービスをサポートする。

【００７０】

この例では、ＢＳＳ９０３は、トランシーバ基地局（ＢＴＳ）９０５と基地局コントローラ（ＢＳＣ）９０７を内含する。単一のＢＴＳが示されているが、例えば２地点間リンクを通して多重ＢＴＳが標準的にＢＳＣに接続されるということが認識されている。各ＢＳＳ９０３は、伝送制御エンティティまたはパケット制御機能（ＰＣＦ）９１１を通してパケットデータ提供ノード（ＰＤＳＮ）９０９にリンクされる。ＰＤＳＮ９０９は、外部ネットワーク、例えばインタネット９１３またはその他の個人消費者ネットワーク９１５に対するゲートウェイとして役立つことから、ＰＤＳＮ９０９は、ユーザの識別および特権を安全に決定し各ユーザの活動を追跡するためにアクセス、許可およびアカウンティングシステム（ＡＡＡ）９１７を内含することができる。ネットワーク９１５は、ホームＡＡＡ９３７により安全保護されたホームエージェント（ＨＡ）９３５を通してアクセスされる単数または複数のデータベース９３３にリンクされたネットワーク管理システム（ＮＭＳ）９３１を含む。

【００７１】

単一のＢＳＳ９０３が示されているが、移動体交換局（ＭＳＣ）９１９には標準的に多数のＢＳＳ９０３が接続されているということが認識されている。ＭＳＣ９１９は、公衆交換電話ネットワーク（ＰＳＴＮ）９２１といったような回路交換電話ネットワークに対する接続性を提供している。同様に、ＭＳＣ９１９を同じネットワーク９００上のその他のＭＳＣ９１９および／またはその他の無線ネットワークに対し接続することができるということも認識されている。ＭＳＣ９１９は一般に、このＭＳＣ９１９に対する動作中の加入者についての一時的情報を保持するビジターロケーションレジスタ（ＶＬＲ）９２３とコロケートされている。ＶＬＲ９２３データベース内部のデータは、大方の場合、詳細な加入者サービス加入情報を記憶するホームロケーションレジスタ（ＨＬＲ）９２５データベースのコピーである。一部の実装においては、ＨＬＲ９２５およびＶＬＲ９２３は同じ物理的データベースである。しかしながらＨＬＲ９２５は、例えばシグナリングシステムナンバー７（ＳＳ７）ネットワークなどを通してアクセスされる遠隔な場所に位置づけされ得る。秘密認証キーといったような加入者特異的認証データを含む認証センタ（ＡｕＣ）９２７が、ユーザを認証する目的でＨＬＲ９２５と結びつけられる。さらにＭＳＣ９１９は無線ネットワーク９００に対しおよびここから簡易メッセージを保管し転送するショートメッセージサービスセンタ（ＳＭＳＣ）９２９に接続される。

【００７２】

セルラー方式電話システムの標準的なオペレーションの間、ＢＴＳ９０５は、電話呼出しまたはその他の通信を行う移動体ユニットセット９０１から逆方向リンク信号セットを受信し復調する。一定の与えられたＢＴＳ９０５により受信された各々の逆方向リンク信号は、その局内で処理される。結果として得られたデータはＢＳＣ９０７に転送される。ＢＳＣ９０７は、ＢＴＳ９０５間のソフトハンドオフの編成を含めた呼出し資源割当ておよび移動性管理という機能性を提供する。ＢＳＣ９０７は同様に、それ自体ＰＳＴＮ９２１とのインタフェースのための付加的な経路指定および／または切換えを提供するＭＳＣ

９１９に対し、受信データを経路指定する。ＭＳＣ９１９は同様に、呼出しセットアップ、呼出し経路、ＭＳＣ間ハンドオーバおよび補足的サービスおよび収集、課金およびアカウンティング情報の管理をも担当する。同様にして、無線ネットワーク９００は、順方向リンクメッセージを送る。ＰＳＴＮ９２１は、ＭＳＣ９１９とインタフェースする。ＭＳＣ９１９はさらに、ＢＳＣ９０７とインタフェースし、このＢＳＣ９０７はそれ自体ＢＴＳ９０５と通信し、これらのＢＴＳ９０５は順方向リンク信号セットを変調し移動体ユニットセット９０１に伝送する。

【００７３】

図９Ｂに示されているように、ジェネラル・パケット・ラジオ・サービス（ＧＰＲＳ）インフラストラクチャ９５０の２つのキー素子は、サービングＧＰＲＳサポーティングノード（ＳＧＳＮ）９３２とゲートウェイＧＰＲＳサポートノード（ＧＧＳＮ）９３４である。さらに、ＧＰＲＳインフラストラクチャはパケット制御ユニットＰＣＵ（１３３６）および、請求システム９３９にリンクされた課金ゲートウェイ機能（ＣＧＦ）９３８を内含する。ＧＰＲＳである移動局（ＭＳ）９４１は、加入者識別モジュール（ＳＩＭ）９４３を利用する。

【００７４】

ＰＣＵ９３６は、エアインタフェースアクセス制御、エアインタフェース上のパケットスケジューリングおよびパケットアセンブリおよび再アセンブリといったＧＰＲＳ－関連の機能を担当する論理ネットワークエレメントである。一般に、ＰＣＵ９３６はＢＳＣ９４５と物理的に統合されている。しかしながらこれをＢＴＳ９４７またはＳＧＳＮ９３２とコロケートすることが可能である。ＳＧＳＮ９３２は、移動性管理、セキュリティ、およびアクセス制御機能を含めたＭＳＣ９４９と同等の機能を提供するが、パケット交換方式のドメインにおいてである。さらに、ＳＧＳＮ９３２は、ＢＳＳＧＰＲＳプロトコル（ＢＳＳＧＰ）を用いるフェーム・リレーベースのインタフェースなどを通したＰＣＵ９３６との接続性を有する。１つのＳＧＳＮしか示されていないが、多数のＳＧＳＮ９３１が利用可能であり、サービスエリアを対応する経路指定エリア（ＲＡ）に分割できるということが認識されている。ＳＧＳＮ／ＳＧＳＮインタフェースは、進行中の自己啓発計画（ＰＤＰ）の状況の間にＲＡ更新が行なわれた場合に旧ＳＧＳＮから新ＳＧＳＮへのパケットトンネリングを可能にする。与えられたＳＧＳＮが多数のＢＳＣ９４５にサービス提供し得るものの、任意の与えられたＢＳＣ９４５は一般に１つのＳＧＳＮ９３２とインタフェースする。同様にＳＧＳＮ９３２は任意には、ＧＰＲＳ増強型移動体アプリケーションパート（ＭＡＰ）を用いてＳＳ７ベースのインタフェースを通してＨＬＲ９５１と、またはシグナル伝達接続制御パート（ＳＣＣＰ）を用いてＳＳ７ベースのインタフェースを通してＭＳＣ９４９と接続される。ＳＧＳＮ／ＨＬＲインタフェースは、ＳＧＳＮ９３２がＨＬＲ９５１に対しロケーション更新を提供し、かつＳＧＳＮサービスエリア内部でＧＰＲＳ関連の加入情報を検索することができるようにする。ＳＧＳＮ／ＭＳＣインタフェースは、音声電話について加入者をページングすることといったようなパケットデータサービスと回路交換サービスの間の協調を有効化する。最後に、ＳＧＳＮ９３２は、ネットワーク９５０上でのショートメッセージ機能を有効化するためのＳＭＳＣ９５３とインタフェースする。

【００７５】

ＧＧＳＮ９３４は、インタネット９１３またはその他の個人顧客ネットワーク９５５といったような外部パケットデータネットワークに対するゲートウェイである。ネットワーク９５５は、ＰＤＳＮ９６１を通してアクセスされる単数または複数のデータベース９５５に対してリンクされるネットワーク管理システム（ＮＭＳ）９５７を含む。ＧＧＳＮ９３４は、インタネットプロトコル（ＩＰ）アドレスを割当て、遠隔認証ダイヤルインユーザサービスのホストとして行動するユーザを認証することもできる。ＧＧＳＮ９３４にあるファイアウォールが同じく、無許可のトラフィックを禁止するためファイアウォール機能を実施する。１つのＧＧＳＮ９３４のみが示されているが、与えられたＳＧＳＮ９３２が単数または複数のＧＧＳＮ９３３とインタフェースして、ユーザデータが２つのエンテ

ィティの間ならびにネットワーク９５０の間でトンネリングされ得るようにすることができるということが認識されている。外部データネットワークがＧＰＲＳネットワーク９５０上でセッションを初期化する場合、ＧＧＳＮ９３４は、ＭＳ９４１に現在サービス提供しているＳＧＳＮ９３２についてＨＬＲ９５１に問合せを行う。

【００７６】

ＢＴＳ９４７とＢＳＣ９４５は、どの移動局（ＭＳ）９４１が何時無線チャンネルにアクセスできるかの制御を含め、無線インタフェースを管理する。これらの素子は基本的に、ＭＳ９４１とＳＧＳＮ９３２との間でメッセージを中継する。ＳＧＳＮ９３２は、ＭＳ９４１と通信し、データを送受し、そのロケーションを追跡する。ＳＧＳＮ９３２は、同様に、ＭＳ９４１を登録し、ＭＳ９４１を認証し、ＭＳ９４１に送られたデータを暗号化する。

【００７７】

図１０は、本発明の一実施形態による、図９Ａおよび９Ｂのシステム内で動作する能力をもつ移動局（例えば送受話器）の典型的な構成要素を示す図である。一般に、無線受信機をフロントエンドおよびバックエンド特性に関して定義づけすることが多い。受信機のフロントエンドは、無線周波数（ＲＦ）回路の全てを包含し、一方バックエンドはベースバンド処理回路の全てを包含する。電話の関係ある内部構成要素としては、主制御ユニット（ＭＣＵ）１００３、デジタル信号プロセッサ（ＤＳＰ）１００５およびマイクロホン利得制御ユニットおよびスピーカ利得制御ユニットを内含する受信機／送信機ユニットが含まれる。主表示ユニット１００７が、さまざまなアプリケーションおよび移動局機能を支援してユーザにディスプレイを提供する。オーディオ機能回路１００９には、マイクロホン１０１１およびこのマイクロホンからの音声信号を増幅するマイクロホン増幅器が含まれる。マイクロホン１０１１からの増幅された音声信号出力は、符号器／復号器（ＣＯＤＥＣ）１０１３に供給される。

【００７８】

無線セクション１０１５は出力を増幅し、アンテナ１０１７を介して移動体通信システム（例えば図１４Ａまたは１４Ｂのシステム）内に内含される基地局と通信するために周波数を変換する。パワーアンプ（ＰＡ）１０１９および送信機／変調回路は、当該技術分野において既知であるように、デュプレクサ１０２１またはサーキュレータまたはアンテナスイッチに結合されたＰＡ１０１９からの出力と共に、ＭＣＵ１００３に対する作動的応答性をもつ。ＰＡ１０１９は同様に、バッテリーインタフェースおよび電力制御ユニット１０２０にも結合する。

【００７９】

使用中、移動局１００１のユーザは、マイクロホン１０１１に話しかけ、その声はあらゆる検出済みバックグランドノイズと共に、アナログ電圧に変換される。次にアナログ電圧は、アナログ－デジタル変換器（ＡＤＣ）１０２３を通してデジタル信号に変換される。制御ユニット１００３は、音声符号化、チャンネル符号化、暗号化およびインタリーブといったような内部での処理のため、ＤＳＰ１００５内にデジタル信号を経路指定する。典型的実施形態においては、処理された音声信号は、本書に全体が参考として内含されている電気通信工業会のＴＩＡ／ＥＩＡ／ＩＳ－９５－Ａデュアルモード広帯域スペクトラム拡散セルラー方式システムのための移動局－基地局互換性標準の中に詳述されているような符号分割多元接続（ＣＤＭＡ）のセルラー方式伝送プロトコルを用いて、個別には示されていない複数のユニットにより符号化される。

【００８０】

符号化された信号は次に、位相および振幅ひずみといったような空気を通した伝送中に発生するあらゆる周波数依存性機能障害を補償するため、等化器１０２５に経路指定される。ビットストリームを等化した後、変調器１０２７は信号を、ＲＦインタフェース１０２９内で生成されたＲＦ信号と組み合わせる。変調器１０２７は、周波数または位相変調を介して正弦波を生成する。伝送のための信号を準備するために、アップコンバータ１０３１は、変調器１０２７から出力された正弦波を合成装置１０３３により生成されたもう

１つの正弦波と組合せて所望の伝送周波数を達成する。次に信号は、この信号を適切なパワーレベルまで増大させるべくＰＡ１０１９を通して送られる。実用システムにおいては、ＰＡ１０１９は、ネットワーク基地局から受信された情報からＤＳＰ１００５によりその利得が制御される可変的利得増幅器として作用する。次に信号はデュプレクサ１０２１内でろ過され、任意にはインピーダンスを整合させて最大の電力伝達を提供するべくアンテナ結合器１０３５に送られる。最終的に、信号はアンテナ１０１７を介してローカル基地局に伝送される。自動利得制御（ＡＧＣ）を供給して、受信機の最終段の利得を制御することができる。信号は、ここから、もう１つのセルラー方式電話、その他の携帯電話または公衆交換式電話ネットワーク（ＰＳＴＮ）に接続された固定電話またはその他の電話通信ネットワークであり得る遠隔の電話に転送可能である。

【００８１】

移動局１００１に伝送された音声信号は、アンテナ１０１７を介して受信され、低雑音増幅器（ＬＮＡ）１０３７により直ちに増幅される。復調器１０４１がＲＦをはぎ取り（strip away）１つのデジタルビットストリームのみを残す間に、ダウンコンバータ１０３９が搬送波周波数を低下させる。その後、信号は等化器１０２５を通過し、ＤＳＰ１００５により処理される。デジタル－アナログ変換器（ＤＡＣ）１０４３が信号を変換し、結果としての出力はスピーカ１０４５を通してユーザに伝送され、これらは全て、中央処理ユニット（ＣＰＵ）（図示せず）として実装され得る主制御ユニット（ＭＣＵ）１００３の制御下で行なわれる。

【００８２】

ＭＣＵ１００３はキーボード１０４７からの入力信号を含むさまざまな信号を受信する。ＭＣＵ１００３はディスプレイコマンドおよびスイッチコマンドをディスプレイ１００７および音声出力切換えコントローラにそれぞれ送達する。さらに、ＭＣＵ１００３はＤＳＰ１００５と情報を交換し、任意に内蔵されたＳＩＭカード１０４９およびメモリ１０５１にアクセスすることができる。さらに、ＭＣＵ１００３は、局から要求されたさまざまな制御機能を実行する。ＤＳＰ１００５は、実装に応じて、音声信号上のさまざまな従来のデジタル処理機能のいずれかを実施し得る。さらに、ＤＳＰ１００５はマイクロホン１０１１により検出された信号から局所環境のバックグランドノイズレベルを決定し、マイクロホン１０１１の利得を、移動局１００１のユーザの自然な傾向を補償するように選択されたレベルに設定する。

【００８３】

ＣＯＤＥＣ１０１３はＡＤＣ１０２３およびＤＡＣ１０４３を内含する。メモリ１０５１は、呼出し入電発信音データを含めたさまざまなデータを記憶し、例えば、世界的なインタネットを介して受信された音楽データを含めたその他のデータを記憶する能力をもつ。ソフトウェアモジュールは、ＲＡＭメモリ、フラッシュメモリ、レジスタまたは当該技術分野において既知の書込み可能な記憶媒体の任意のその他の形態の中に常駐し得ると思われる。メモリデバイス１０５１は、単一のメモリ、ＣＤ、ＤＶＤ、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ、光学記憶装置、またはデジタルデータを記憶する能力をもつその他のあらゆる不揮発性記憶媒体であり得るが、これらに制限されるわけではない。

【００８４】

任意に内蔵されたＳＩＭカード１０４９は、例えば、セル方式の携帯電話番号、搬送波供給サービス、加入詳細およびセキュリティ情報といったような重要な情報を搬送する。ＳＩＭカード１０４９はまず第一に無線ネットワーク上で移動局１００１を識別するために役立つ。カード１０４９は同様に、個人電話番号簿、テキストメッセージおよびユーザ特定的移動局設定値を記憶するためのメモリをも収納している。

【００８５】

図１１は、パケットベースのおよび／またはセルベースの技術（例えば非周期転送モード（ＡＴＭ）、イーサネット（登録商標）、ＩＰベースの技術など）を用いるあらゆるタイプのデータ通信ネットワークであり得る典型的な企業ネットワークを示している。企業ネットワーク１１０１は、各々上述のプロセスを実施するように構成されている有線ノー

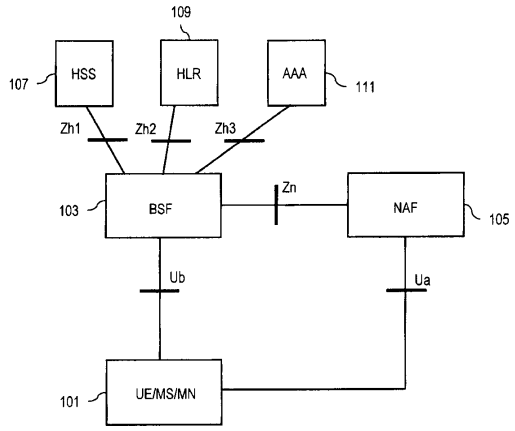
ド１１０３ならびに無線ノード１１０５～１１０９（固定または移動）のための接続性を提供する。企業ネットワーク１１０１は、ＷＬＡＮネットワーク１１１１（例えばＩＥＥＥ８０２．１１）、ｃｄｍａ２０００セルラネットワーク１１１３、電話通信ネットワーク１１１５（例えばＰＳＴＮ）または公衆データネットワーク１１１７（例えばインタネット）といったようなさまざまなその他のネットワークと通信することができる。

【００８６】

本発明は数多くの実施形態および実装に関連して記述されてきたが、本発明はこれに制限されるわけではなく、添付の特許請求の範囲内に入るさまざまな明白な修正および等価の配置を網羅するものである。本発明の特長は請求項間のいくつかの組合せの中で表現されているが、これらの特長を任意の組合せおよび順序で配置することもできるということが考慮されている。

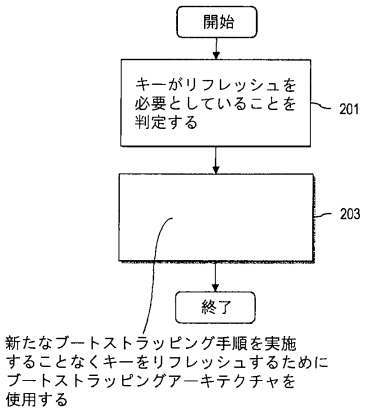
【図１】

図1



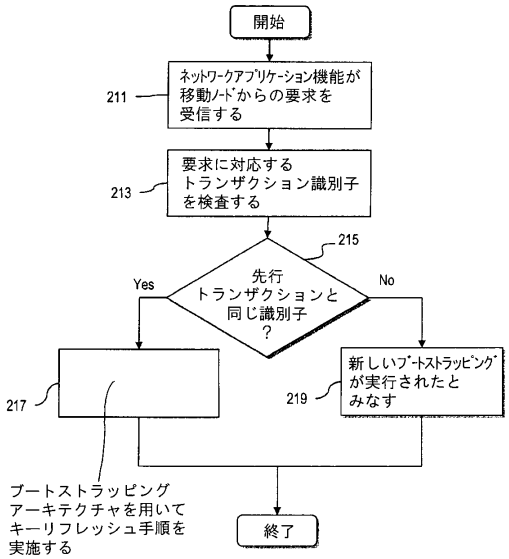
【図２Ａ】

図2A



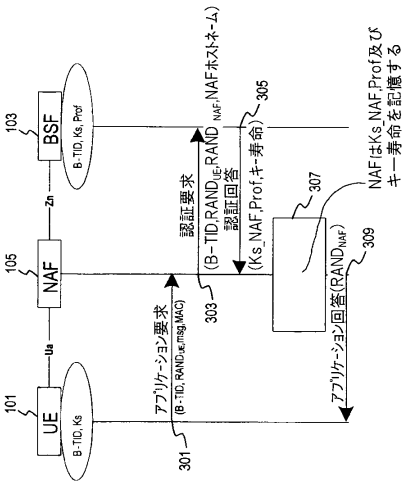
【図２Ｂ】

図2B



【図３】

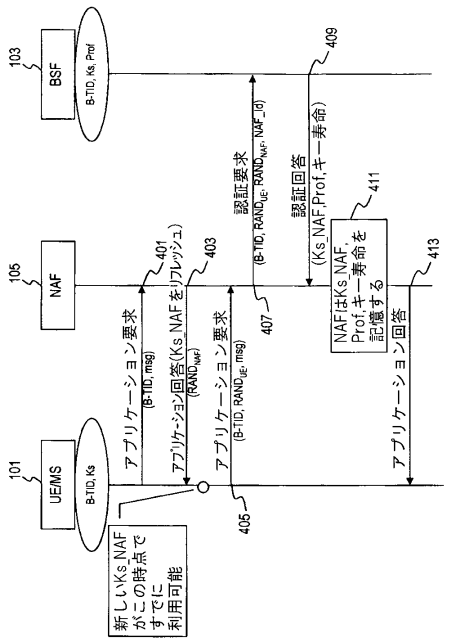
図3



背景技術

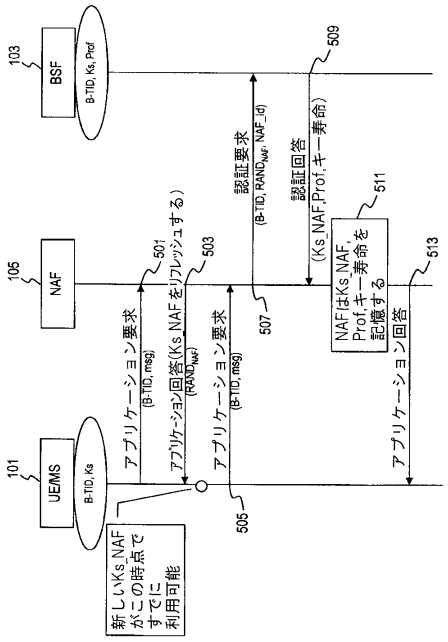
【図４】

図4



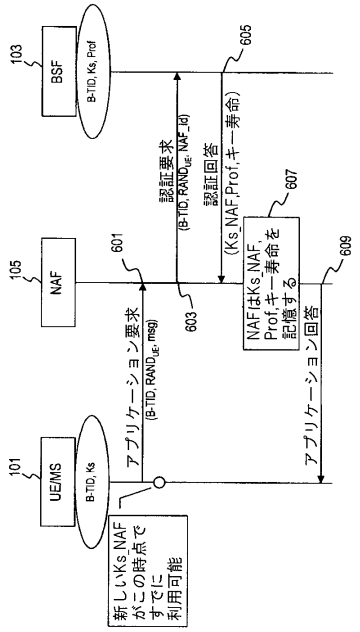
【図５】

図5



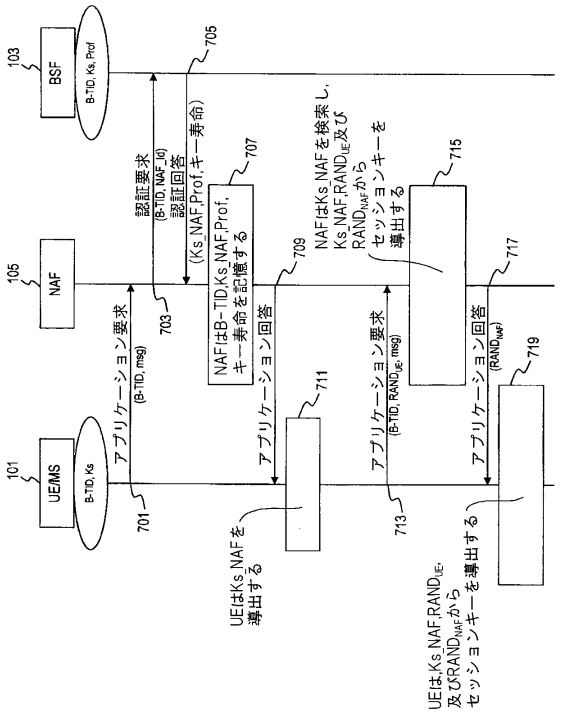
【図６】

図6



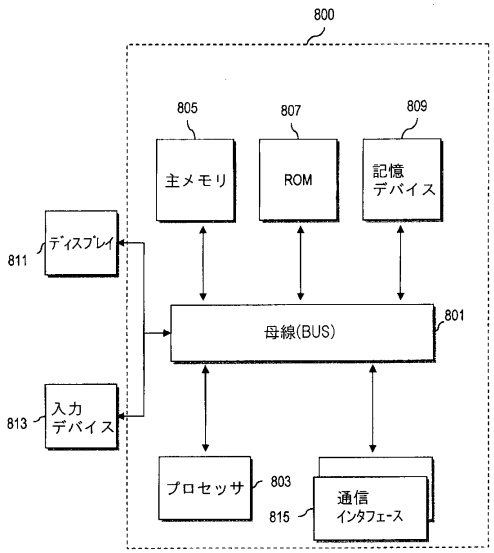
【図７】

図7



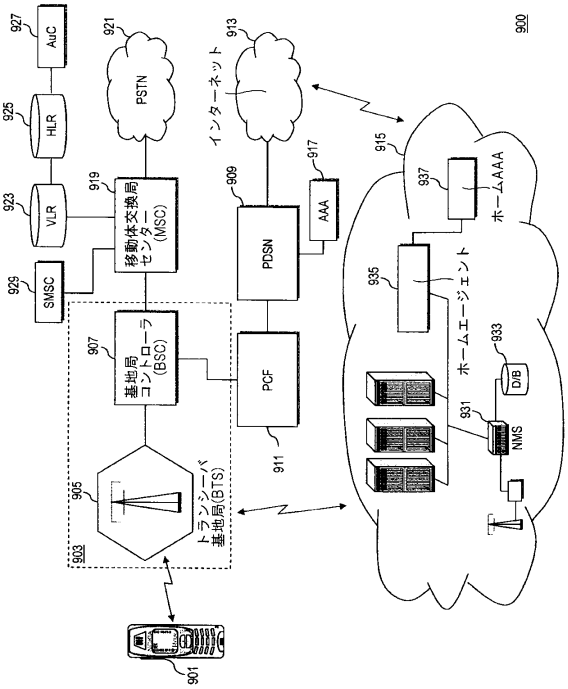
【図８】

図8



【図９Ａ】

図9A



【図９Ｂ】

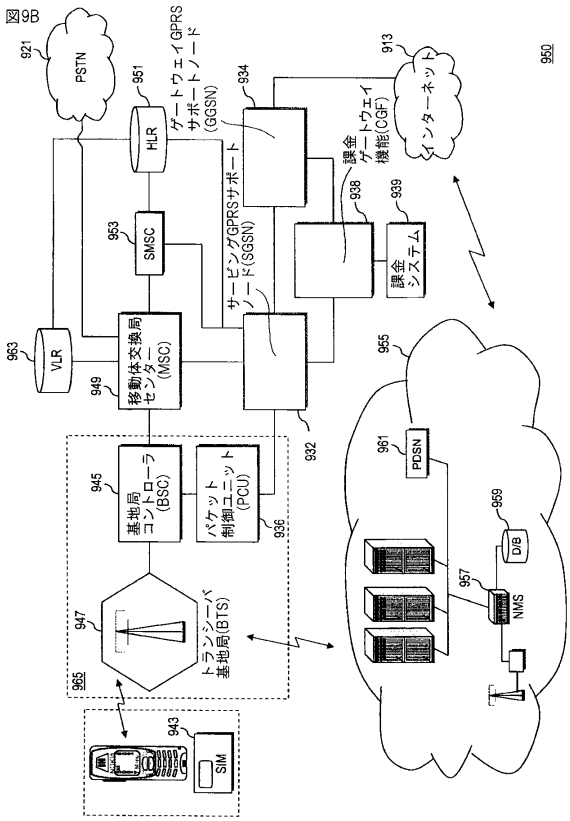


図9B
PSTN
921
ゲートウェイGPRS
サポートノード
(GGSN)
951
HLR
934
913
インターネット
課金
ゲートウェイ
機能(CGF)
938
939
課金
システム
950
SMSC
953
サービングGPRSサポート
ノード(SGSN)
963
VLR
移動体交換局
(MSC)
949
955
961
PDSN
932
945
基地局
コントローラ
(BSC)
パケット
制御ユニット
(PCU)
936
959
DVB
957
NMS
947
トランシーバ
基地局(BTS)
965
943
SIM

【図１０】

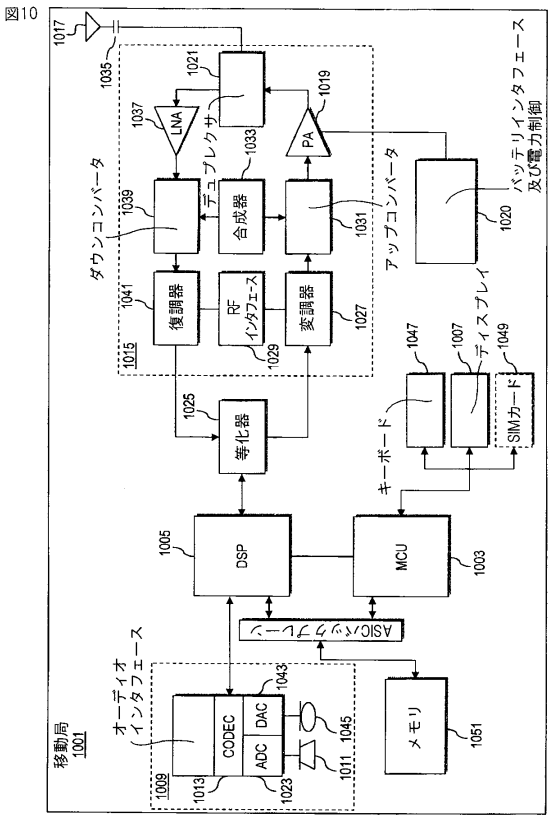


図10
1017
1035
1021
1019
1037
LNA
PA
デュプレクサ
1033
ダウンコンバータ
1039
合成器
1031
アップコンバータ
1020
バッテリインタフェース
及び電力制御
1041
復調器
RF
インタフェース
1029
変調器
1027
1015
1047
1007
ディスプレイ
1049
SIMカード
キーボード
1025
等化器
1005
DSP
MCU
1003
ASICハードウェア
オーディオ
インタフェース
1009
CODEC
DAC
ADC
1043
1045
1011
1013
1023
メモリ
1051
移動局
1001

【図１１】

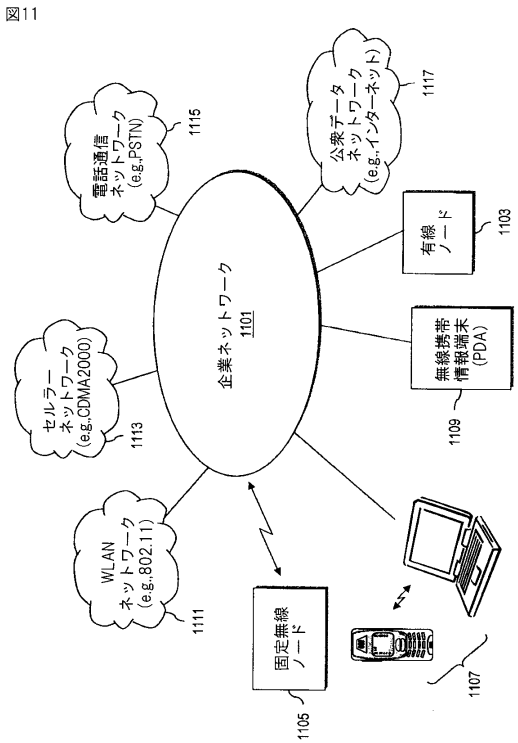


図11
電話通信
ネットワーク
(e.g.,PSTN)
1115
公衆データ
ネットワーク
(e.g.,インターネット)
1117
有線
ノード
1103
企業ネットワーク
1101
無線携帯
情報端末
(PDA)
1109
セルラー
ネットワーク
(e.g.CDMA2000)
1113
WLAN
ネットワーク
(e.g.,802.11)
1111
固定無線
ノード
1105
1107

フロントページの続き

(72)発明者 バイコ，ガボル
アメリカ合衆国，カリフォルニア ９４０４３，マウンテン ビュー，フェアチャイルド ドライブ ３１３
(72)発明者 チャン，タット クン
アメリカ合衆国，カリフォルニア ９２１３１，サンディエゴ，スクリップス ポーウェイ パークウェイ １０３８６，＃７３

審査官 青木 重徳

(56)参考文献 特開２０００－０８３０１７（ＪＰ，Ａ）
特開２００２－２３２９６２（ＪＰ，Ａ）
特表２００８－５３７４４５（ＪＰ，Ａ）
特表２００８－５３８４８２（ＪＰ，Ａ）
国際公開第２００５／０４６１１８（WO，Ａ１）
Gabor Bajko, Tat Chan, “Key refreshing machanism”, 3RD GENERATION PARTNERSHIP PROJECT 2 "3GPP2", [online], ２００５年 9月２７日, [retrieved on 2013-09-20]. Retrieved from the Internet, ＵＲＬ, <ftp://ftp.3gpp2.org/TSGS/Working/_2005/2005-09-Vancouver/WG%204%20Security/S40-20050926-011_key_refresh_discussion.doc>
“3GPP TS 33.220 V6.3.0”, ARIB STD-T63-33.220 V6.3.0 Generic Authentication Architecture (GAA); Generic bootstrapping architec, [online], ２００４年１２月, [retrieved on 2011-04-20]. Retrieved from the Internet, ＵＲＬ, <http://www.arib.or.jp/IMT-2000/ARIB-STD/ITU-T/Rel6T/A33220-630.pdf>
“key lifetime of GBA”, 3GPP TSG SA WG3 Security - S3#36, [online], ２００４年１１月２３日, S3-040924, [retrieved on 2011-04-21]. Retrieved from the Internet, ＵＲＬ, <http://www.3gpp.org/FTP/tsg_sa/WG3_Security/TSGS3_36_Shenzhen/Docs/PDF/S3-040924.pdf>
“Key handling in the UE in a Generic Bootstrapping Architecture - Pseudo-CR”, 3G TSC SA WG3 Security - S3#32, [online], ２００４年 2月 3日, 6.9.2(GBA), p.1-4, [retrieved on 2014-02-27]. Retrieved from the Internet, ＵＲＬ, <http://www.3gpp.org/ftp/tsg_sa/wg3_security/TSGS3_32_Edinburgh/Docs/PDF/S3-040041.pdf>

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／０８
Ｇ０６Ｆ ２１／４４
Ｈ０４Ｗ １２／０６