(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2008-538482
(P2008-538482A)
(43)公表日　平成20年10月23日(2008.10.23)

(51)Int.Cl.			F I			テーマコード（参考）
H04Q	7/38	(2006.01)	H04Q	7/00	182	5J104
H04Q	7/32	(2006.01)	H04Q	7/00	183	5K067
H04Q	7/24	(2006.01)	H04Q	7/00	641	
H04L	9/08	(2006.01)	H04Q	7/00	670	
			H04L	9/00	601A	

審査請求 未請求　予備審査請求 未請求　（全 14 頁）　最終頁に続く

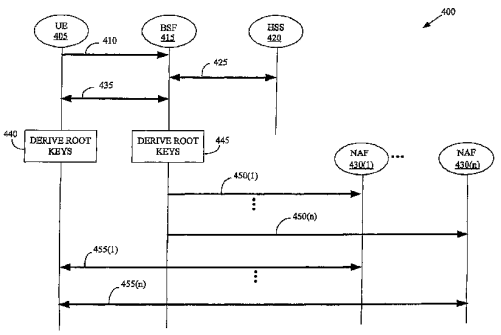
(21)出願番号　特願2008-507705 (P2008-507705)
(86)(22)出願日　平成18年4月10日 (2006.4.10)
(85)翻訳文提出日　平成19年10月18日 (2007.10.18)
(86)国際出願番号　PCT/US2006/013195
(87)国際公開番号　WO2006/113189
(87)国際公開日　平成18年10月26日 (2006.10.26)
(31)優先権主張番号　11/108,609
(32)優先日　平成17年4月18日 (2005.4.18)
(33)優先権主張国　米国 (US)

(71)出願人　596092698
ルーセント　テクノロジーズ　インコーポレーテッド
アメリカ合衆国．０７９７４－０６３６　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　６００
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100085176
弁理士　加藤　伸晃
(74)代理人　100094112
弁理士　岡部　譲
(74)代理人　100096943
弁理士　臼井　伸一

最終頁に続く

(54)【発明の名称】ルート鍵の提供

(57)【要約】
本発明は、少なくとも１つのネットワーク・アプリケーション機能との通信を認証するための鍵素材の生成の方法を提供する。この方法は、ブートストラッピング鍵要求に応答して第１の鍵素材を決定することと、第１の鍵素材の決定に応答して第２の鍵素材を決定することとを含む。第２の鍵素材は、第１の鍵素材の決定に応答して、決定され、少なくとも１つのネットワーク・アプリケーション機能に提供される第３の鍵素材に一致する。



【特許請求の範囲】
【請求項１】
少なくとも１つのネットワーク・アプリケーション機能との通信を認証するための鍵素材の生成の方法であって、
ブートストラッピング鍵要求に応答して第１の鍵素材を決定することと、
前記第１の鍵素材の決定に応答して第２の鍵素材を決定することであって、前記第２の鍵素材が、前記第１の鍵素材の決定に応答して、決定され、前記少なくとも１つのネットワーク・アプリケーション機能に提供される第３の鍵素材に一致することと
を含む方法。
【請求項２】
ブートストラッピング鍵プロビジョニングの要求を提供することと、
ホーム加入者サーバ、ホーム・ロケーション・レジスタ、および認証、認可およびアカウンティング・サーバのうちの少なくとも１つに格納されているブートストラッピング情報にアクセスすることであって、前記ブートストラッピング情報にアクセスすることが、ユーザ・プロファイル、認証ベクトル、鍵値、ユーザ・セキュリティ設定、前記少なくとも１つのネットワーク・アプリケーション機能の指示、および前記少なくとも１つのネットワーク・アプリケーション機能のアドレスのうちの少なくとも１つにアクセスすることを含むことと、
前記ブートストラッピング情報に基づいて第１の鍵素材を決定することと
を含む請求項１に記載の方法。
【請求項３】
ブートストラッピング鍵生成プロセスを使用して、ブートストラッピング・サーバ機能を認証することを含む請求項２に記載の方法。
【請求項４】
前記第２の鍵素材を決定することが、鍵導出関数に基づいて、前記少なくとも１つのネットワーク・アプリケーション機能に関連する少なくとも１つのルート鍵を決定することを含む請求項１に記載の方法。
【請求項５】
前記第２の鍵素材を使用して、前記少なくとも１つのネットワーク・アプリケーション機能との少なくとも１つの安全な接続を形成することを含む請求項１に記載の方法。
【請求項６】
少なくとも１つのネットワーク・アプリケーション機能との通信を認証するための鍵素材の生成の方法であって、
ブートストラッピング鍵要求に応答して第１の鍵素材を決定することと、
前記第１の鍵素材の決定に応答して第２の鍵素材を決定することであって、前記第２の鍵素材が、前記第１の鍵素材の決定に応答して、前記ユーザ機器によって決定される第３の鍵素材に一致することと
前記第２の鍵素材を前記少なくとも１つのネットワーク・アプリケーション機能に提供することと
を含む方法。
【請求項７】
ブートストラッピング鍵プロビジョニングの要求を受信することと、
ホーム加入者サーバ、ホーム・ロケーション・レジスタ、および認証、認可およびアカウンティング・サーバのうちの少なくとも１つに格納されているブートストラッピング情報にアクセスすることであって、前記ブートストラッピング情報にアクセスすることが、ユーザ・プロファイル、認証ベクトル、鍵値、ユーザ・セキュリティ設定、前記少なくとも１つのネットワーク・アプリケーション機能の指示、および前記少なくとも１つのネットワーク・アプリケーション機能のアドレスのうちの少なくとも１つにアクセスすることを含むことと、
前記ブートストラッピング情報に基づいて第１の鍵素材を決定することと

を含む請求項６に記載の方法。
【請求項８】
ブートストラッピング鍵生成プロセスを使用して前記ユーザ機器を認証することを含む請求項７に記載の方法。
【請求項９】
前記第２の鍵素材を決定することが、鍵導出関数に基づいて、前記少なくとも１つのネットワーク・アプリケーション機能に関連する少なくとも１つのルート鍵を決定することを含む請求項６に記載の方法。
【請求項１０】
前記第２の鍵素材を前記少なくとも１つのネットワーク・アプリケーション機能に提供することが、実質的に、前記第２の鍵素材を使用して前記ユーザ機器と前記少なくとも１つのネットワーク・アプリケーション機能との間に少なくとも１つの安全な接続が形成される前に、少なくとも１つのネットワーク・アプリケーション機能への前記第２の鍵素材を提供することを含む請求項６に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に通信システムに関し、より詳細には無線通信システムに関する。
【背景技術】
【０００２】
従来の無線通信システムは、様々な認証技術を使用して、システムを介して送信される情報のセキュリティおよび／または保全性を保護する。例えば、Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ａｇｒｅｅｍｅｎｔ（ＡＫＡ）プロトコルは、Ｔｈｉｒｄ Ｇｅｎｅｒａｔｉｏｎ Ｐａｒｔｎｅｒｓｈｉｐ Ｐｒｏｊｅｃｔ（３ＧＰＰ）認証インフラストラクチャに実装されている。ネットワークにおける、および／またはユーザ側のアプリケーション機能がブートストラッピング技術を使用して共有鍵を確立できるようにするために、３ＧＰＰ ＡＫＡプロトコルを活用することができる。
【０００３】
図１は、３ＧＰＰ ＡＫＡプロトコルに基づくブートストラッピング・アーキテクチャ１００の従来のモデルを概念的に示す。ブートストラッピング・アーキテクチャ１００は、インターフェイスＺｈによってブートストラッピング・サーバ機能（Bootstrapping Server Function：ＢＳＦ）に結合されるホーム加入者サーバ（Home Subscriber Server：ＨＳＳ）を含む。ＢＳＦは、インターフェイスＵｂによって１つまたは複数のユーザ機器（ＵＥ、一般にモバイル・ユニットとも呼ばれる）に結合される。また、ＢＳＦは、インターフェイスＺｎによってネットワーク・アプリケーション機能（ＮＡＦ）にも接続される。ＮＡＦは、インターフェイスＵａによってＵＥに結合される。ブートストラッピング・アーキテクチャ１００に含まれるエンティティについては、参照によりその全部が本明細書に組み込まれる、３ＧＰＰ技術仕様書 ３ＧＰＰ ＴＳ ３３．２２０ Ｖ６．３．０（２００４－１２）に詳細に記載されている。
【０００４】
図２は、従来のブートストラッピング手順２００を概念的に示している。ＵＥは、矢印２０５によって示されるように、ＢＳＦに要求を送信することによって、ブートストラッピング手順２００を開始することができる。ＢＳＦは、双方向矢印２１０によって示されるように、ユーザ・セキュリティ設定および／または認証データ、例えば認証ベクトルなどをＨＳＳから取り出すことができる。ＢＳＦは、（矢印２１５によって示される）認証要求をＵＥに送信する。認証要求２１５は、ＨＳＳから取り出されたユーザ・セキュリティ設定および／または認証データに基づいて形成することができる。認証要求２１５は、認証プロセスで使用され得る乱数および／または認証トークンを含み得る。ＵＥは、Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ａｇｒｅｅｍｅｎｔ手順を実行して（２２０）、認証要求が許可されたネットワークからのものであることを確認する。ＵＥは、様

々なセッション鍵および／またはダイジェストＡＫＡ応答（digest AKA response）を計算することもできる。

【０００５】

ダイジェストＡＫＡ応答は、（矢印２２５によって示されるように）ＢＳＦに送信され、ＢＳＦは、ダイジェストＡＫＡ応答に基づいてＵＥを認証することができる（２３０）。次いでＢＳＦは、１つまたは複数の鍵（Ｋｓ）、および鍵の１つまたは複数のライフタイムを生成することができる（２３０）。矢印２３５によって示されるように、鍵を含む確認メッセージ、および入手可能な場合は鍵のライフタイムがＵＥに送信される。確認メッセージの受信に応答して、ＵＥは、ＢＳＦによって生成された１つまたは複数の鍵（Ｋｓ）に対応すべき１つまたは複数の鍵（Ｋｓ）を生成することができる（２４０）。ＵＥおよびＢＳＦは、鍵（Ｋｓ）を使用して、ＵＥとＮＡＦとの間の通信に使用できる鍵素材（key material）Ｋｓ＿ＮＡＦを生成することができる。

【０００６】

図３は、ＵＥとＮＡＦとの間の安全な通信リンクを形成する従来の方法３００を概念的に示す。ＵＥは、鍵（Ｋｓ）を使用して鍵素材Ｋｓ＿ＮＡＦを導出し（３０５）、次いで矢印３１０によって示されるように、ＮＡＦにアプリケーション要求を送信する。アプリケーション要求３１０は、一般に、ブートストラッピング・トランザクション識別子（Ｂ－ＴＩＤ）、および他の情報を含む。ＮＡＦは、矢印３１５によって示されるように、ＢＳＦに認証要求を送信する。認証要求３１５は、Ｂ－ＴＩＤおよびＮＡＦホスト名を含む。ＢＳＦは、矢印３２０によって示されるように、認証応答を提供する。認証応答３２０は、一般に、鍵（Ｋｓ）から導出された鍵素材Ｋｓ＿ＮＡＦ、および適切な任意の鍵のライフタイムを含む。鍵素材Ｋｓ＿ＮＡＦは、ＮＡＦによって格納され（３２５）、アプリケーション応答がＵＥに提供される。安全な通信リンクを形成する方法３００が完了すると、ＵＥおよびＮＡＦは、図１に示されているインターフェイスＵａを介して安全に通信することができる。

【非特許文献１】３ＧＰＰ技術仕様書　３ＧＰＰ　ＴＳ　３３．２２０　Ｖ６．３．０（２００４－１２）

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかしながら上述した３ＧＰＰ　ＧＢＡアーキテクチャなど、従来のブートストラッピング手順は、様々なサービスおよび技術によって必要とされるルート鍵、特に、既存のサービスによって必要とされるルート鍵のプロビジョニングに配慮してない。例えば、ＢＴＩＤなどの情報やＵＥとＮＡＦとの間に送信される様々な知識の交換を容易にするために、ルート鍵のプロビジョニングの標準を変更する必要がある場合がある。ブートストラッピング手順と互換性があるように設計されていない新しいおよび／または既存のサービスは、それらの既存のハードウェアおよび／またはソフトウェアを使用してルート鍵を確立することができない場合がある。さらに、ブートストラップのプロビジョニングに対応するようにハードウェアおよび／またはソフトウェアを変更することによって、結果として他のアプリケーションによって使用されるソフトウェアおよび／またはライブラリに望ましくない変更がもたらされる可能性がある。

【課題を解決するための手段】

【０００８】

以下は、本発明のいくつかの態様を基本的に理解できるように、本発明の簡単な概略を示す。この概略は、本発明の網羅的な概要ではない。本発明の主要なまたは重要な要素を特定したり、本発明の範囲を表したりするものではない。その唯一の目的は、後述されるより詳細な説明の前置きとして簡単な形でいくつかの概念を示すことである。

【０００９】

本発明の一実施形態では、少なくとも１つのネットワーク・アプリケーション機能との通信を認証するための鍵素材の生成の方法が提供される。この方法は、ブートストラッピ

ング鍵要求に応答して第１の鍵素材を決定することと、第１の鍵素材の決定に応答して第２の鍵素材を決定することとを含み得る。第２の鍵素材は、第１の鍵素材の決定に応答して、決定され、前記少なくとも１つのネットワーク・アプリケーション機能に提供される第３の鍵素材に一致し得る。

【００１０】

本発明の別の実施形態では、少なくとも１つのネットワーク・アプリケーション機能との通信を認証するための鍵素材の生成の方法が提供される。この方法は、ブートストラッピング鍵要求に応答して第１の鍵素材を決定することと、第１の鍵素材の決定に応答して第２の鍵素材を決定することとを含み得る。第２の鍵素材は、第１の鍵素材の決定に応答してユーザ機器によって決定される第３の鍵素材に一致する。この方法は、第２の鍵素材を少なくとも１つのネットワーク・アプリケーション機能に提供することを含み得る。

【００１１】

本発明は、添付の図面と併せて、以下の説明を参照することによって理解できる。図中、同様の参照番号は、同様の要素を示す。

本発明は、様々な変更形態および代替形式の余地があるが、その特定の実施形態は、図面において一例として示されており、本明細書で詳しく説明される。しかし、本明細書における特定の実施形態の説明は、本発明を開示された特定の形式に限定するものではなく、逆に、本発明は、変更形態、均等物、および代替形態を添付の特許請求の範囲によって定義された本発明の意図および範囲内に包含するものであることを理解されたい。

【発明を実施するための最良の形態】

【００１２】

本発明の例示の実施形態について以下で説明する。明瞭にするために、本明細書に実際の実装形態のすべての特徴が記載されているわけではない。任意のこうした実際の実施形態の開発において、実施形態ごとに異なる、システム関連やビジネス関連の制約の遵守など、開発者に特有の目的を達成するために、多数の実施に特有の決定がなされるべきであることは当然理解されよう。さらに、こうした開発努力は、複雑で時間がかかり得るが、それにもかかわらず、本開示の恩恵を有する当業者には日常の仕事であることを理解されよう。

【００１３】

本発明の一部およびそれに対応する詳細な説明は、ソフトウェア、またはコンピュータ・メモリ内のデータ・ビットに関する演算のアルゴリズムおよびシンボリック表現に関して提供される。こうした説明および表現は、当業者がその仕事の内容を他の当業者に有効に伝えるためのものである。アルゴリズムは、本明細書で使用され、一般に使用される用語であるが、所望の結果をもたらす自己矛盾のない一連の工程であると考えられる。こうした工程は、物理量の物理的な操作を必要とするものである。通常、必ずしもそうではないが、こうした量は、格納し、転送し、結合し、比較し、別の方法で処理することができる光、電気、または磁気の信号の形をとる。主に一般的な使用の理由で、こうした信号をビット、値、要素、シンボル、文字、用語、番号などと呼ぶことが時として便利であることがわかっている。

【００１４】

しかし、こうした類似のすべての用語は、適切な物理量と関連付けられており、単にこうした量に適用される便利なラベルにすぎないことに留意されたい。特に明記しない限り、または説明から明らかであるように、「処理する」、「計算する」、「算出する」、「決定する」、または「表示する」などの用語は、コンピュータ・システムのレジスタおよびメモリ内の物理、電子量として表されるデータを処理し、コンピュータ・システムのメモリまたはレジストリまたはこうした他の情報記憶、送信、または表示装置内の物理量として同様に表される他のデータに変換するコンピュータ・システムまたは類似の電子コンピューティング装置のアクションおよびプロセスを指す。

【００１５】

また、本発明のソフトウェアで実施される態様は、一般に、ある形式のプログラム格納

媒体上に符号化され、またはあるタイプの送信媒体を介して実施されることにも留意されたい。プログラム記憶媒体は、磁気（フロッピー（登録商標）・ディスク、ハード・ドライバなど）でも光（コンパクト・ディスク読み取り専用メモリ、すなわち「ＣＤ－ＲＯＭ」など）でもよく、読み取り専用でもランダム・アクセスでもよい。同様に、送信媒体は、より線対、同軸ケーブル、光ファイバ、または当技術分野で知られている他の何らかの適した送信媒体とすることができる。本発明は、任意の所与の実施のこれらの態様によって制限されない。

【００１６】

次に、本発明を、添付の図面を参照して説明する。様々な構造、システム、および装置は、単に説明の目的で、当業者にはよく知られている詳細で本発明を不明瞭にしないように、図に概略的に示されている。それにもかかわらず、添付の図は、本発明の例示的な例を示し、説明するために含まれる。本明細書に使用される単語および句は、当業者によるこれらの単語および句の理解と一致する意味を持つと理解され、解釈されるものとする。用語または句の特別な定義、すなわち、当業者によって理解される通常の慣用的な意味とは異なる定義は、本明細書における用語または句の一貫した使用によっては暗示されないものとする。用語または句が、特別な意味、すなわち、当業者によって理解される以外の意味を持つ範囲で、こうした特別な定義は、この用語または句の特別な定義を直接、かつ明確に提供する定義的な方法で、本明細書に明示的に記載される。

【００１７】

図４は、鍵をプロビジョニングする方法４００の一実施形態例を概念的に示す。例示の実施形態では、ユーザ機器（ＵＥ）４０５は、（矢印４１０によって示されるように）ブートストラッピング要求を提供する。例えば、ユーザ機器４０５は、ブートストラッピング要求４１０をブートストラッピング・サーバ機能４１５に提供することができる。モバイル・ユニットとも呼ばれ得るユーザ機器４０５は、携帯電話、ＰＤＡ、スマート・フォン、テキスト・メッセージ装置（text messaging device）、ラップトップ・コンピュータなどを含み得る。ブートストラッピング・サーバ機能４１５は、矢印４２５によって示されるように、ブートストラッピング情報をホーム加入者サーバ（ＨＳＳ）４２０から取り出す。様々な代替実施形態では、ブートストラッピング情報は、認証ベクトル、１つまたは複数の鍵値、汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定（ＧＵＳＳ）などのユーザ・セキュリティ設定、１つまたは複数のネットワーク・アプリケーション機能（ＮＡＦ）４３０（１－ｎ）を示す情報、ネットワーク・アプリケーション機能４３０（１－ｎ）のアドレスなどを含み得る。代替実施形態では、他のエンティティがブートストラッピング情報のすべてまたは一部を提供することができることを当業者であれば理解されたい。こうしたエンティティは、ホーム・ロケーション・レジスタや、認証、許可、アカウンティング（Authentication Authorization and Accounting：ＡＡ）サーバなどを含み得る。

【００１８】

ユーザ機器４０５およびブートストラッピング・サーバ機能４１５は、矢印４３５によって示されるように、相互に認証し合う。一実施形態では、ユーザ機器４０５およびブートストラッピング・サーバ機能４１５は、３ＧＰＰ技術仕様書　３ＧＰＰ　ＴＳ　３３．２２０　Ｖ６．３．０（２００４－１２）に記載されている汎用ブートストラッピング・アーキテクチャに実装されているブートストラッピング鍵生成プロセスなどのブートストラッピング鍵生成プロセスを使用して、互いに認証し合う。鍵素材は、相互認証手順４３５中に決定される。例えば、汎用ブートストラッピング・アーキテクチャに実装されたブートストラッピング鍵生成プロセスは、相互認証手順４３５中に鍵素材（Ｋｓ）を形成することができる。

【００１９】

ユーザ機器４０５およびブートストラッピング・サーバ機能４１５は、ネットワーク・アプリケーション機能４３０（１－ｎ）に関連する鍵素材（Ｋｓ＿ＮＡＦ１，．．．，Ｋｓ＿ＮＡＦｎ）を別々に導出する（４４０および４４５）。一実施形態では、ユーザ機器

４０５およびブートストラッピング・サーバ機能４１５によって導出された（４４０および４４５）鍵素材（Ｋｓ＿ＮＡＦ１，．．．，Ｋｓ＿ＮＡＦｎ）は、認証プロセス４３５中に決定された鍵素材に基づいて決定される。また、鍵素材（Ｋｓ＿ＮＡＦ１，．．．，Ｋｓ＿ＮＡＦｎ）は、ユーザ機器４０５およびブートストラッピング・サーバ機能４１５の相互認証（４３５）に応答して導出され得る（４４０および４４５）。鍵素材（Ｋｓ＿ＮＡＦ１，．．．，Ｋｓ＿ＮＡＦｎ）は、適切な鍵導出関数を使用して導出され得る。例えば、ネットワーク・アプリケーション機能４３０（１）に関連する鍵素材は、例えば、Ｋｓ＿ＮＡＦ１＝ＫＤＦ（Ｋｓ，ＮＡＦ１，その他のパラメータ）など、鍵導出関数ＫＤＦ（）を使用して導出することができ、式中、ＮＡＦ１は、ネットワーク・アプリケーション機能４３０（１）を示す情報を含む。

【００２０】

一実施形態では、ユーザ機器４０５およびブートストラッピング・サーバ機能４１５によって導出された（４４０および４４５）鍵素材は、１つまたは複数のルート鍵を含む。本明細書で使用される場合、「ルート鍵」という用語は、少なくともユーザ機器４０５およびネットワーク・アプリケーション機能４３０（１－ｎ）に共通の鍵を指す。ルート鍵は、ユーザ機器４０５と１つまたは複数のネットワーク・アプリケーション機能４３０（１－ｎ）との間の安全な通信セッションを確立するために使用され得るセッション鍵など、他の鍵を導出するために使用することができる。ルート鍵は、ロケーション・サービス（location service）などの新しいサービス、既存のサービス、および／またはＩＥＥＥ８０２．１１技術、Ｂｌｕｅｔｏｏｔｈ技術、ＩＰマルチメディア・システム（ＩＭＳ）などのネットワーク・オーバーレイ（network overlay）など異なるアクセス技術のセキュリティを提供するために使用することができる。

【００２１】

ルート鍵は、何日も、何ヶ月も、または何年もなど、相対的に長い期間にわたって維持され得る。例えば、ユーザ機器４０５に関連するルート鍵は、ユーザ機器４０５のユーザに関連するサブスクリプション期間中、変わらない場合がある。しかし、ユーザ機器４０５に関連するルート鍵は、変更したりリフレッシュしたりすることができることを当業者であれば理解されたい。例えば、不揮発性メモリを有していないユーザ機器４０５によって格納されたルート鍵は、ユーザ機器４０５の電源が切断されたときに失われたり消去されたりする可能性があり、この場合、新しいルート鍵を決定することができる。別の例では、相互認証手順４３５中に決定された鍵素材を変更することができ、その変更に応答して１つまたは複数の新しいルート鍵を形成することができる。

【００２２】

次いで鍵素材（Ｋｓ＿ＮＡＦ１，・・・，Ｋｓ＿ＮＡＦｎ）は、矢印４５０（１－ｎ）によって示されるように、関連のネットワーク・アプリケーション機能４３０（１－ｎ）に提供される。例示の実施形態では、ブートストラッピング・サーバ機能４１５は、鍵素材（Ｋｓ＿ＮＡＦ１，・・・，Ｋｓ＿ＮＡＦｎ）の決定（４４５）に応答して、鍵素材（Ｋｓ＿ＮＡＦ１，・・・，Ｋｓ＿ＮＡＦｎ）を関連のネットワーク・アプリケーション機能４３０（１－ｎ）に提供する。したがって、ネットワーク・アプリケーション機能４３０（１－ｎ）は、鍵素材（Ｋｓ＿ＮＡＦ１，・・・，Ｋｓ＿ＮＡＦｎ）を要求する必要がなく、例えば、鍵素材（Ｋｓ＿ＮＡＦ１，・・・，Ｋｓ＿ＮＡＦｎ）がネットワーク・アプリケーション機能４３０（１－ｎ）にプッシュされてもよい。一実施形態では、鍵素材（Ｋｓ＿ＮＡＦ１，・・・，Ｋｓ＿ＮＡＦｎ）は、おおむね同時に関連のネットワーク・アプリケーション機能４３０（１－ｎ）に提供される。しかし、鍵素材（Ｋｓ＿ＮＡＦ１，・・・，Ｋｓ＿ＮＡＦｎ）が任意の順序で、ネットワーク・アプリケーション機能４３０（１－ｎ）へのプロビジョニング間の任意の時間遅延で、関連のネットワーク・アプリケーション機能４３０（１－ｎ）に提供され得ることを当業者であれば理解されたい。

【００２３】

鍵素材（Ｋｓ＿ＮＡＦ１，・・・，Ｋｓ＿ＮＡＦｎ）が関連のネットワーク・アプリケーション機能４３０（１－ｎ）に提供されると、ユーザ機器４０５は、矢印４５５（１－

ｎ）によって示されるように、鍵素材（Ｋｓ＿ＮＡＦ１，・・・，Ｋｓ＿ＮＡＦｎ）を使用して、ネットワーク・アプリケーション機能４３０（１－ｎ）のうちの１つまたは複数との安全な通信リンクを確立することができる。例えば、ユーザ機器４０５およびネットワーク・アプリケーション機能４３０（１－ｎ）に格納されている鍵素材（Ｋｓ＿ＮＡＦ１，・・・，Ｋｓ＿ＮＡＦｎ）は、同じであるはずであり、したがって、ユーザ機器４０５および適切なネットワーク・アプリケーション機能４３０（１－ｎ）を相互認証するために使用され得る。いくつかの実施形態では、ネットワーク・アプリケーション機能４３０（１－ｎ）のルート鍵を、そのドメイン名が変更される可能性がある、またはユーザ機器４０５にはわからない可能性のあるネットワークにおけるいくつかのサーバに格納することができる。したがって、オペレータは、ユーザ・サービス・プロファイルを、ルート鍵を必要とするネットワーク・アプリケーション機能４３０（１－ｎ）の適切なアドレスを含むブートストラッピング・サーバ機能４１５に提供することができる。

【００２４】

方法４００は、ハードウェア、ソフトウェア、またはその組み合わせを使用して実施することができる。一実施形態では、ユーザ機器４０５で使用されるブートストラッピングおよびルート鍵プロビジョニング・ソフトウェアは、任意のアプリケーション固有のコードとは無関係とすることができる。鍵素材（Ｋｓ＿ＮＡＦ１，・・・，Ｋｓ＿ＮＡＦｎ）が導出されると、ブートストラッピングおよび／またはルート鍵プロビジョニング・コードは、適切な記憶域を新しい鍵素材で更新することができる。次いでユーザ機器４０５におけるアプリケーションは、インターフェイスすることなく、またはブートストラッピングおよび／またはルート鍵プロビジョニング・コードを認識していなくても、ルート鍵を使用して、そのそれぞれのアプリケーションを安全にすることができる。また、鍵素材をブートストラッピング・サーバ機能４１５から受信し、記憶域を新しい鍵素材で更新することができるように、ネットワーク・アプリケーション機能４３０（１－ｎ）に新しいソフトウェアを追加することもできる。ネットワーク・アプリケーション機能４３０（１－ｎ）におけるソフトウェアの残りは、更新されたり、変更されたり、または汎用ブートストラッピング・アーキテクチャなど、ブートストラッピング・アーキテクチャの存在を認識させたりする必要はない。したがって、ブートストラッピングおよび／またはルート鍵プロビジョニング・コードを追加することによってもたらされる、ユーザ機器４０５、ネットワーク・アプリケーション機器４３０（１－ｎ）、および／または既存のサービスに対する中断を低減することができる。

【００２５】

これに対して、従来のブートストラッピングおよび／またはルート鍵プロビジョニング技術で、Ｕａインターフェイスを介して交換を運ぶには、送受信機およびＮＡＦにおける既存のソフトウェアへの変更を必要とする。第２に、ルート鍵が一度におよびその使用の前にプロビジョニングされない場合、ユーザ機器が特定のＮＡＦからのサービスを必要とするとき、ユーザ機器は、ルート鍵を更新する必要があることになる。このことは、ルート鍵プロビジョニング・プロセスが今から始まるべきであることを示すために、ユーザ機器またはＮＡＦにおけるサービス論理を変更することを必要とすることになる。

【００２６】

上記に開示した特定の実施形態は、例にすぎず、本発明は、本明細書の教示の恩恵を有する当業者には明らかな、異なるが等価の方法で変更し、実施することができる。さらに、頭記の特許請求の範囲に記載された以外、本明細書に示された構造および設計の詳細に制限は加えられないものとする。したがって、上記に開示された特定の実施形態は、改変または変更することができることは明らかであり、こうしたすべての変形形態は、本発明の範囲および意図内にあると考えられる。したがって、本発明に求められる保護は、頭記の特許請求の範囲に記載されている。

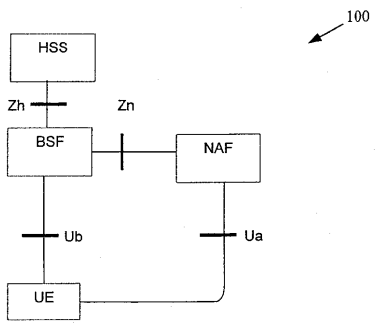
【図面の簡単な説明】

【００２７】

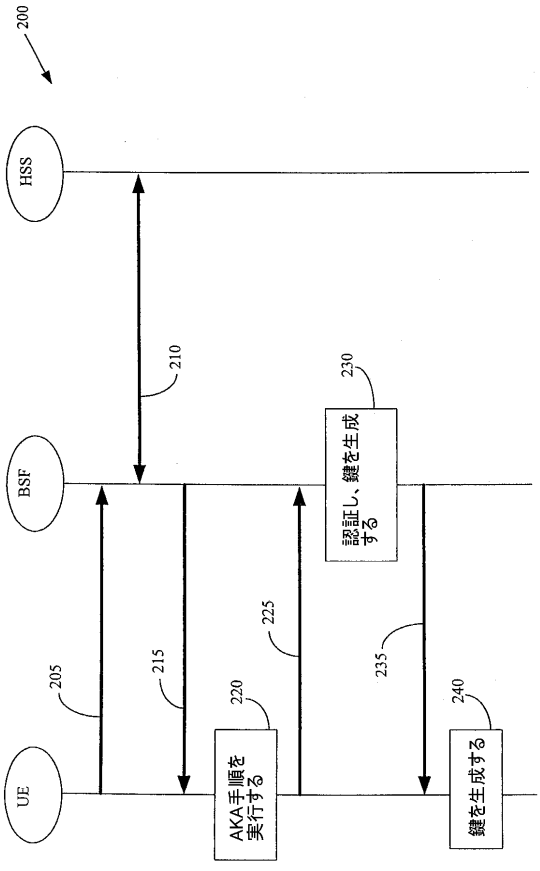
【図１】３ＧＰＰ　ＡＫＡプロトコルに基づくブートストラッピング・アーキテクチャの

従来のモデルを概念的に示す図である。
【図２】従来のブートストラッピング手順を概念的に示す図である。
【図３】ＵＥとＮＡＦとの間の安全な通信リンクを形成する従来の方法を概念的に示す図である。
【図４】本発明による鍵を提供する方法の一実施形態例を概念的に示す図である。

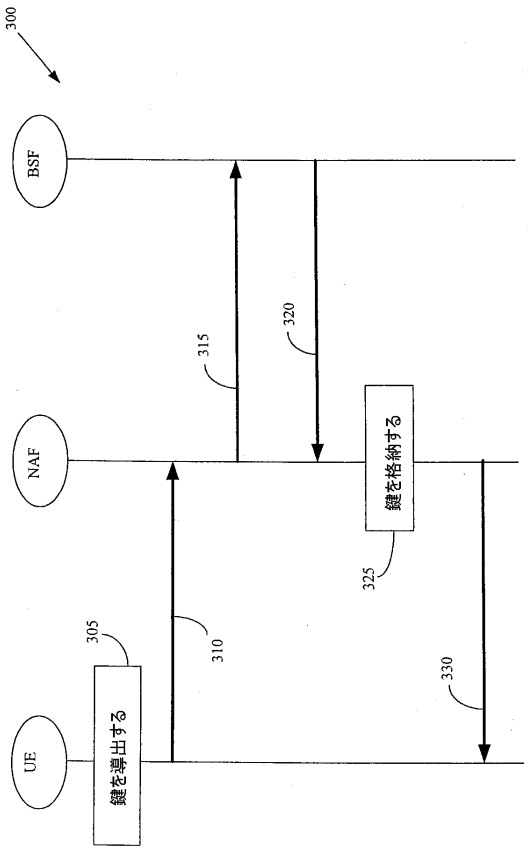
【図１】



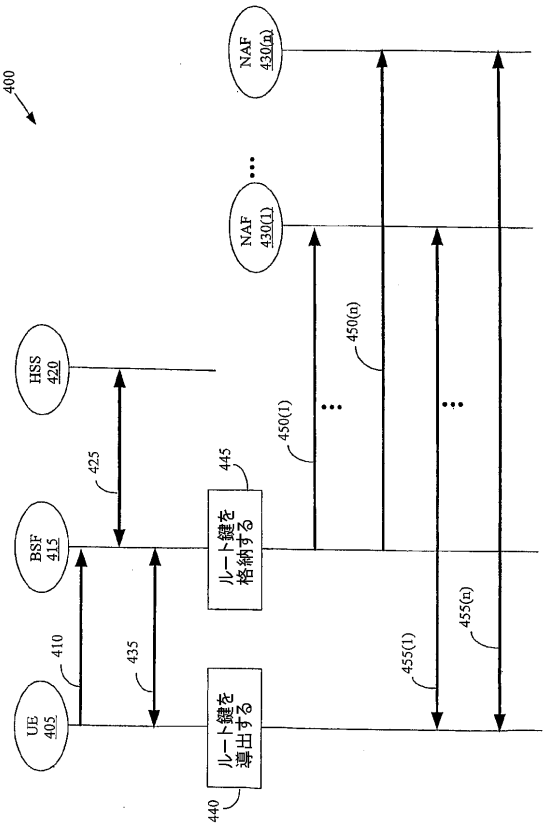
【図２】



【図３】


300
BSF
NAF
UE
315
320
310
305
330
325
鍵を導出する
鍵を格納する

【図４】


400
NAF 430(n)
NAF 430(1)
HSS 420
BSF 415
UE 405
425
410
435
445
440
450(1)
450(n)
455(1)
455(n)
ルート鍵を格納する
ルート鍵を導出する

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/013195

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08

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)
H04L

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

Electronic data base consulted during the international search (name of data base and, where practical, 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.
X	"Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture (3GPP TS 33.220 version 6.3.0 Release 6); ETSI TS 133 220" ETSI STANDARDS, EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE, SOPHIA-ANTIPO, FR, vol. 3-SA3, no. V630, December 2004 (2004-12), XP014028221 ISSN: 0000-0001 cited in the application figure 4.3 paragraph [4.2.1] paragraph [4.5.2] - paragraph [4.5.3] -/--	1-10

[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 document 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
13 September 2006	21/09/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	GARCIA MAHEDERO, P

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/013195

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MENEZES A J ET AL: "Handbook of Applied Cryptography, key establishment protocols" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, pages 489-508, XP002283799 ISBN: 0-8493-8523-7	1,6
A	page 500, paragraph 12.22	2-5,7-10
A	WO 2004/034205 A (KOOLSPAN; FASCENDA, ANTHONY, C) 22 April 2004 (2004-04-22) abstract paragraph [0012] - paragraph [0018]	1-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No
PCT/US2006/013195

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004034205 A	22-04-2004	AU 2003277308 A1	04-05-2004
		AU 2003282495 A1	04-05-2004
		AU 2003282497 A1	04-05-2004
		WO 2004034213 A2	22-04-2004
		WO 2004034214 A2	22-04-2004

フロントページの続き

(51)Int.Cl.	F I	テーマコード（参考）
	H04L 9/00 601E	

(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,HU,IE,IS,IT,LT,LU,LV,MC,NL,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,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．Ｂｌｕｅｔｏｏｔｈ

(74)代理人 100101498
弁理士 越智 隆夫
(74)代理人 100104352
弁理士 朝日 伸光
(74)代理人 100128657
弁理士 三山 勝巳
(72)発明者 パテル，サルヴァル
アメリカ合衆国 ０７０４５ ニュージャーシィ，モントヴィル，ミラーズ レーン ３４

Ｆターム(参考) 5J104 AA01 AA16 AA32 EA04 EA15 EA16 EA17 EA18 JA03 NA02
NA27 NA37 PA01 PA07
5K067 AA30 BB04 DD24 EE02 EE16 HH23 HH24 JJ64