(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5746774号
(P5746774)
(45)発行日　平成27年7月8日(2015.7.8)　(24)登録日　平成27年5月15日(2015.5.15)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601B
H04L 9/14 (2006.01)　H04L 9/00 601E
H04L 9/00 641

請求項の数 12　外国語出願　(全 20 頁)

(21)出願番号　特願2014-633(P2014-633)
(22)出願日　平成26年1月6日(2014.1.6)
(62)分割の表示　特願2010-535908(P2010-535908)の分割
原出願日　平成19年11月30日(2007.11.30)
(65)公開番号　特開2014-99891(P2014-99891A)
(43)公開日　平成26年5月29日(2014.5.29)
審査請求日　平成26年1月14日(2014.1.14)

(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】セキュアな通信のための鍵管理

(57)【特許請求の範囲】
【請求項１】
通信ネットワークにおける当事者端末間のセキュアな通信を確立するための方法であって、
開始者当事者端末が、第１の鍵管理装置への要求に対する応答の中で、マスター鍵を含む第１の鍵情報とバウチャーとを受信するステップと、
前記第１の鍵情報から第１のセッション鍵を生成するステップと、
中間者装置へ前記バウチャーを送信するステップと、
前記中間者装置が前記バウチャーの少なくとも一部を前記第１の鍵管理装置へ転送するステップと、
前記第１の鍵管理装置において前記バウチャーを使用して前記マスター鍵を取り出すステップと、
前記中間者装置において、前記第１の鍵管理装置から前記マスター鍵を受信し、前記第１のセッション鍵及び第２のセッション鍵を取得し、少なくとも１つの応答者当事者端末への前記バウチャーの送信を開始するステップと、
前記少なくとも１つの応答者当事者端末から第２の鍵管理装置へ前記バウチャー又は前記バウチャーの一部を転送するステップと、
前記第２の鍵管理装置が、前記バウチャーを第２の鍵情報に変換するために前記第１の鍵管理装置と通信するステップと、
前記少なくとも１つの応答者当事者端末が、前記第２の鍵管理装置から前記第２の鍵情

報を受信するステップと、
前記少なくとも１つの応答者当事者端末が、前記第２の鍵情報から前記第２のセッション鍵を生成するステップと、
前記開始者当事者端末と前記少なくとも１つの応答者当事者端末とが、前記セキュアな通信のために前記第１のセッション鍵及び前記第２のセッション鍵を使用するステップと、
を備え、
前記セキュアな通信は、前記開始者当事者端末から前記中間者装置へ、そして前記中間者装置から前記少なくとも１つの応答者当事者端末へというパスに沿って進行する
ことを特徴とする方法。
【請求項２】
前記当事者端末の各々が、各自の信用保証情報に基づいて、各自とそれに関連付けられたブートストラッピング機能との間の共有鍵を生成するためのブートストラッピング手順を実行するステップを更に備え、
前記受信する各ステップは、前記当事者端末の各々が各自に関連付けられた前記ブートストラッピング機能との前記ブートストラッピング手順を行った際に生成された前記共有鍵によって受信される情報を保護することを伴う
ことを特徴とする請求項１に記載の方法。
【請求項３】
前記ブートストラッピング手順はＧＢＡ方法に従う
ことを特徴とする請求項２に記載の方法。
【請求項４】
少なくとも１つの前記鍵情報は、対応する生成するステップを不要にするセッション鍵を含む
ことを特徴とする請求項１に記載の方法。
【請求項５】
前記第１の鍵情報は、前記第１の鍵管理装置において格納され、前記バウチャーに含まれる識別情報によって参照され、
前記通信するステップは、前記第１の鍵管理装置において前記第１の鍵情報を取り出すステップと、前記第２の鍵管理装置に前記第１の鍵情報に基づく情報を提供するステップと、を含む
ことを特徴とする請求項２に記載の方法。
【請求項６】
前記識別情報はナンスを含む
ことを特徴とする請求項５に記載の方法。
【請求項７】
前記識別情報は参照アドレスを含む
ことを特徴とする請求項５に記載の方法。
【請求項８】
前記中間者装置から送信する前記ステップは、前記バウチャーの中で与えられるグループＩＤから決定される前記少なくとも１つの応答者当事者端末のグループへ向けて行われる
ことを特徴とする請求項１に記載の方法。
【請求項９】
前記中間者装置は、前記開始者当事者端末の前記第１のセッション鍵を使用して、前記通信を処理するために復号を行い、続いて、前記応答者当事者端末の各々のための前記第２のセッション鍵を使用して前記通信を再暗号化する
ことを特徴とする請求項１に記載の方法。
【請求項１０】
前記第１の鍵管理装置は、前記第１の鍵管理装置がユーザのためにバウチャーを変換す

る場合に当該ユーザが前記グループのメンバーであることを検証することを実行する
ことを特徴とする請求項８に記載の方法。
【請求項１１】
前記少なくとも１つの応答者当事者端末は、前記ネットワークに登録していないとネットワークエンティティによって判定され、
これにより処理が中断され、前記ネットワークエンティティは、前記開始者当事者端末から通信された情報と関連するバウチャーとを登録が検出されるまで格納し、
登録が検出されると、前記ネットワークエンティティは、前記処理を継続し、前記バウチャーを前記少なくとも１つの応答者当事者端末へプッシュする
ことを特徴とする請求項１乃至１０のいずれか１項に記載の方法。
【請求項１２】
通信ネットワークにおける当事者端末間の中間者装置を介したセキュアな通信のための第１及び第２のセッション鍵を生成することを支援する第１の鍵管理装置であって、
開始者当事者端末からの要求に応えて、マスター鍵を含む第１の鍵情報及びバウチャーを生成する手段と、
前記第１の鍵情報を格納する手段と、
前記第１の鍵情報と前記バウチャーとを前記開始者当事者端末へ送信する手段と、
前記中間者装置から前記バウチャーの少なくとも一部を受信する手段と、
前記バウチャーを使用して前記マスター鍵を取り出す手段と、
前記マスター鍵を前記中間者装置へ送信する手段と、
応答者当事者端末から前記バウチャーを受信した第２の鍵管理装置からの要求に応えて、第２の鍵情報を送信する手段と、
を備え、
前記第１及び第２の鍵情報は、それに基づいて前記第１及び第２のセッション鍵がそれぞれ生成される情報であり、
前記セキュアな通信は、前記開始者当事者端末から前記中間者装置へ、そして前記中間者装置から前記応答者当事者端末へというパスに沿って進行することを特徴とする第１の鍵管理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、エンドポイント間でセキュアな通信を確立するという分野におけるものである。特に、本発明は、両エンドポイントが同一種類の基本信用保証情報(basic credential)を使用するという要件を除去する。
【背景技術】
【０００２】
例えばＧＳＭ、ＷＣＤＭＡ、ＷＬＡＮ、ＷｉＭＡＸのような多くのネットワークアクセス技術は、第１のホップ（即ち、ユーザデバイスとネットワークのアクセスポイントとの間の通信）のための基本的なセキュリティを提供する。通信は、プロトコルスタックにおけるレイヤ２又はレイヤ３を使用可能である。ＳＲＴＰ（ＲＦＣ３７１１）及びＭＩＫＥＹ（ＲＦＣ３８３０）は、メディアセキュリティ及び鍵管理のためのプロトコルの例である。ＭＩＫＥＹは、事前共有鍵及びＰＫＩの両方に基づくことができる。また、ＭＩＫＥＹは、ＲＦＣ４５６７を使用してセッションセットアップシグナリング（ＳＩＰ又はＲＴＳＰ）に組み込むことができる。
【０００３】
しかしながら、これらのアクセス技術によって提供される基本的なセキュリティは、十分に安全であると常に見なすことができる訳ではない。実際、例えば８０２．３／Ｅｔｈｅｒｎｅｔ（登録商標）又はＤＳＬのように、アクセス技術によってはいかなる基本的なセキュリティも提供しない。
【０００４】

それゆえ、追加された又は改良されたセキュリティメカニズムを多くのアクセス技術に提供するというニーズが存在する。

【０００５】

鍵管理に対する既存のアプローチの課題は、両エンドポイントが同一種類の基本信用保証情報を使用するという前提に関するものである。しかしながら、この前提は常に成立する訳ではなく、例えば、固定移動体融合（ＦＭＣ）の場合が存在する。ＦＭＣでは、ユーザの一方はＳＩＭベースの信用保証情報（例えば、ＳＩＭ、ＵＳＩＭ、ＩＳＩＭ）を使用する３ＧＰＰ加入者であるかもしれず、他方はＰＫＩベースの信用保証情報を実装した例えばケーブルアクセスのユーザであるかもしれない。

【０００６】

鍵管理を既知のシグナリングプロトコルに組み込むことに関しても一定の課題が存在する。

【０００７】

課題を提示する別の例は「アーリーメディア(early media)」に関するものである。「アーリーメディア」とは、例えばＭＩＫＥＹオーバーＳＩＰに従う鍵管理動作が完了する前にメディアが応答者からのフローバックを開始してもよいということを意味する。それゆえ、ＭＩＫＥＹはＳＩＰを用いてインバンドで搬送されてもよいが、最初の数パケットを保護するために使用可能な鍵は何ら存在しないかもしれない。代替としてメディア・インバンドの鍵管理を使用することは、この課題を解決するかもしれないが、例えばファイアウォールを越える観点からは欠点が存在する。更に、メディアパスでシグナリングを搬送することは、技術上実務的であるとは考えられない。

【０００８】

鍵管理の既知の方法に関する別の課題は、「フォーキング(forking)」に関する。ここで、例えばマルチメディア電話呼（ＭＭＴＥＬ）の開始者は、他方のエンドポイントのユーザが応答のためにどの端末を使用するであろうかということに関して確信が持てないであろう。仮に呼に応答するための端末の全てがＰＫＩ対応であったとしても、異なる端末は異なる公開鍵を使用するであろうから、開始者は招待要求のためにどの鍵を使用すべきかを知ることができない。より正確には、既知の方法によれば、応答者が応答した後になるまでは、鍵管理が開始可能になったり、適切な公開鍵を決定可能になったりすることはない。上述のように、メディア・インバンドの鍵管理は、この課題を緩和するかもしれないが、上述のように欠点が存在する。

【０００９】

鍵管理の既知の方法に関する更に別の課題は、ＩＭＳサービスの中にはピア・ツー・ピア（Ｐ２Ｐ）のものもあり、他方、例えばプッシュ・ツー・トーク・オーバー・セルラ（ＰｏＣ）にようにグループサービスを提供するものもあるということである。グループ鍵を管理することをユーザに対して要求することは課題を生じさせ、事実、全てのグループメンバーが招待に応答してセッションに参加するであろうかということさえ、ユーザは確信を持つことができない。それゆえ、この場合、実際に参加しているメンバーに対してのみセッション鍵を配布することには利点があるであろうから、潜在的にグループセッションに入ることのできるメンバーとグループセッションに参加中のメンバーとを区別するというニーズが存在する。

【００１０】

先行技術に関する更なる課題は、一部のサービス（例えばメッセージング）が、応答者がオンラインであるか否かに依存して異なるやり方で扱われるかもしれないということである。例えば、インスタントメッセージ（ＩＭ）は、受信者がオンラインでない場合、後での配信のための延期メッセージ(deferred message)（ＤＭ）に自動的に変換されるであろう。送信者は、他の当事者がオンラインであるか否かを知ることができないかもしれず、それゆえ、メッセージを送信する時点でどの鍵管理が適切であるかを知ることができないかもしれない。Ｓ／ＭＩＭＥベースのソリューションは、この状況を緩和することができるかもしれないが、Ｓ／ＭＩＭＥは、ＭＭＴＥＬのようなリアルタイムのメディアには

適していない。それゆえ、鍵管理のアプローチは、使用されているＩＭＳサービスがどれであるかに依存するようになるであろうが、これは望ましくない。加えて、Ｓ／ＭＩＭＥには事前共有鍵（例えばＳＩＭ）のサポートが欠如しており、また、Ｓ／ＭＩＭＥで保護された２つのメッセージを関連付け可能であるというセッションの概念が存在しないという事実に起因して、Ｓ／ＭＩＭＥは反射攻撃に対する保護(replay protection)を提供しない。

【発明の概要】

【発明が解決しようとする課題】

【００１１】

本発明の一般的な目的は、開始者当事者と応答者当事者との間のセキュアな通信を確立する既知の方法の欠陥を、メディア保護のために直接使用可能な又はエンド・ツー・エンド合意の基礎を形成する共有鍵をエンドポイント間で確立することにより、克服することである。

【００１２】

セキュリティ管理のために各当事者が使用する信用保証情報の種類からの独立を提供する、開始者当事者と応答者当事者との間のセキュアな通信のための鍵を確立することが目的である。

【課題を解決するための手段】

【００１３】

本発明によれば、ユーザデバイスとの共有鍵を確立する能力を持つ鍵管理サーバ（ＫＭＳ）は、鍵要求に応えて、ユーザにバウチャー及び鍵生成情報を提供する。前記情報を受信した第１のユーザは、セッション鍵を算出し、通信要求の中でバウチャーを第２の当事者へ送信する。第２の当事者は、バウチャーの受信に応えて、同一の又は別のＫＭＳエンティティとセキュアな通信を確立し、バウチャーを提供する。これに応えて、同一の又は別のＫＭＳは、鍵生成情報を返す。前記鍵生成情報に基づいて、第１及び第２の当事者は両者とも、共通のセッション鍵を生成する。

【００１４】

バウチャーは、発行するＫＭＳエンティティによって有利に完全性が保護され、更に、メタデータ、関与する当事者の典型的なＩＤ、生成時刻、シーケンス番号、有効期限、使用形態（プッシュ・ツー・トーク・オーバー・セルラ又は電話など）、通信の種類（例えば、ピア・ツー・ピア又はグループの通信）を含み得る。更に、バウチャーは、セッション鍵のコピー、及び、保護されるプライバシーが典型である暗号化を必要とするその他の情報を含み得る。

【００１５】

本発明の一実施形態では、共有鍵を確立する能力はＧＢＡ手順に基づき、ここで、ユーザ及びネットワークＢＳＦ機能には基本的な共有秘密（例えば、ＳＩＭ／ＵＳＩＭ／ＩＳＩＭベースの秘密）が与えられる。本実施形態に従うＫＭＳエンティティは、ＢＳＦエンティティに対するＮＡＦエンティティとして機能する。

【００１６】

別の実施形態によれば、第１の当事者及び第２の当事者の各々によって生成されるセッション鍵は異なり、これにより、中間当事者は、第１の当事者及び第２の当事者それぞれとのセキュアな通信のためにこれらの鍵を両方とも生成するように構成され、中間当事者は、第１の当事者から第２の当事者へのメッセージを最初に復号し、続いて処理し、再暗号化することにより、メッセージを処理可能である。特に、中間当事者での鍵生成は、第１の当事者から受信するバウチャーに基づいており、バウチャーは、鍵生成に続いて、対応するセッション鍵の生成のために第２の当事者へ転送される。

【００１７】

更に別の実施形態では、第２の当事者は、複数の第２の当事者の集合によって表され、バウチャーを使用する中間当事者は、最初にマスター鍵を生成し、そして、第２の当事者のグループの各メンバーのための個々のセッション鍵及びバウチャーをマスター鍵に基づ

いて生成する。中間当事者は、鍵生成に続いて、第２の当事者の各々へバウチャーを転送し、第２の当事者の各々はその後、対応する個々のセッション鍵を生成する。第２の当事者のグループは、グループＩＤを解決（変換）(resolving)することによって、又は、第１の当事者によって指定される事前定義されたグループを特定することによって、中間当事者において取得可能である。

【００１８】

更に別の実施形態では、中間当事者は第１の当事者から受信した情報を処理せず、それゆえ、第１の当事者及び第２の当事者それぞれとの通信のために別個の鍵を生成する必要が無い。本実施形態では、中間当事者は、第１の当事者から受信したバウチャーをグループ内の第２の当事者の各々へ転送し、これにより、第１の当事者及び各第２の当事者は、セキュアなエンド・ツー・エンド通信のための共有セッション鍵を生成することができる。中間当事者においてバウチャーを傍受し、傍受したバウチャーを使用してＫＭＳ機能に対してバウチャーをセッション鍵に変換するように要求するという可能性を取り除くために、ＫＭＳエンティティには、バウチャーを変換してあげるユーザがグループのメンバーであるということをチェックする機能が備えられる。

【００１９】

第１の当事者から少なくとも１つの第２の当事者へ向けられたメッセージは、延期配信のためにネットワークエンティティに格納することができる。典型的には、中間当事者は、少なくとも１つの第２の当事者がネットワークに登録していないということを発見可能であり、それゆえ、後の配信のためにメッセージをバウチャーと共に格納可能である。その少なくとも１つの第２の当事者がネットワークに登録すると、メッセージを一時的に格納しているエンティティは、上述したプロトコルを継続可能であり、最終的に、メッセージ及び関連するバウチャーを宛先の当事者へプッシュすることができる。

【００２０】

一実施形態によれば、本発明は３ＧＰＰ　ＩＭＳ環境において実装可能である。

【図面の簡単な説明】

【００２１】

【図１】ＧＢＡ／ＧＡＡインタフェースに対するネットワークアプリケーション機能（ＮＡＦ）として機能する認証プロキシ１６０を通してＧＢＡ／ＧＡＡの先行技術の配置を説明する図である。

【図２】ＩＭＳコアネットワーク（ＣＮ）サブシステムの基本的なエレメント及びアプリケーションサーバ２１０に対する接続を説明する図である。

【図３】第１の実施形態を説明するための図である。

【図４】本発明の実施形態に従う信号図を示す図である。

【図５】第２の実施形態を説明するための図である。

【図６】インタフェースの構成例を示す図である。

【図７】本発明に従う装置を示す図である。

【発明を実施するための形態】

【００２２】

以下の説明は、説明を目的とするが限定は目的とせずに、特定の実施形態、手順、技術等のような具体的な詳細を説明する。いくつかの例において、よく知られている方法、インタフェース、回路、及びデバイスに関する詳細な説明は、不要な詳細によって説明を分かりにくくしてしまわないように、省略される。また、個々のブロックがいくつかの図面に示される。理解されるであろうが、これらのブロックの機能は、個々のハードウェア回路を使用して実装されてもよいし、適切にプログラムされたデジタルマイクロプロセッサ又は汎用コンピュータと併せてソフトウェアプログラム及びデータを使用して実装されてもよいし、アプリケーション固有集積回路を使用して実装されてもよいし、及び／又は１以上のデジタル信号プロセッサを使用して実装されてもよい。

【００２３】

セキュリティ鍵の管理の説明を目的として、３ＧＰＰ　ＧＢＡ／ＧＡＡアーキテクチャ

が使用される。しかしながら、本明細書から容易に理解されることとして、ユーザＵＥとアプリケーションサーバ（例えば、ＮＡＦ１６０）との間での共有鍵の生成を提供する、セキュリティ鍵の管理のための他の何らかの方法が使用されてもよい。例えば、ＰＫＩベースの信用保証情報をサポートするＵＥは、アプリケーションサーバとの共有鍵を生成するためにＴＬＳを使用することができるであろう。ユーザ名／パスワードベースのアーキテクチャでは、共有鍵を確立するためにＰＫＣＳ＃５標準を使用可能であろう。等々である。

【００２４】

図１は、ＧＢＡ／ＧＡＡインタフェースに対するネットワークアプリケーション機能（ＮＡＦ）として機能する認証プロキシ１６０を通してＧＢＡ／ＧＡＡの先行技術の配置を説明する図である。汎用ブートストラッピングサーバ機能１１０（ＢＳＦ）及びユーザ装置１０１（ＵＥ）は、ＵＭＴＳ　ＡＫＡプロトコルを使用して相互に認証する。ＵＥは、インタフェース１２０（Ｕｂ）経由でＢＳＦと通信する。ＵＥ及びホーム加入者サーバ１３０（ＨＳＳ）は、ＢＳＦにインタフェース１７０（Ｚｈ）経由で提供される認証ベクトルをＨＳＳが生成する基礎となる鍵を、共有する。ＡＫＡプロトコルによれば、ＢＳＦはＵＥへチャレンジを送信し、ＵＥはＢＳＦへ応答を返す。ＢＳＦがＵＥの応答をＨＳＳにより提供される期待される応答と比較することにより、認証が検証される。認証が成功すると、ＢＳＦ及びＵＥにおいて共有鍵Ｋｓの生成が開始する。ＢＳＦは鍵Ｋｓ及び関連する参照Ｂ－ＴＩＤを格納する。参照Ｂ－ＴＩＤ及び他のデータ（鍵の有効期限など）はその後、完了メッセージの中でＵＥに提供される。加入者ロケータ機能１４０（ＳＬＦ）は、Ｚｈインタフェースの動作と連動して、必要とされる加入者固有データを保持するＨＳＳの名前を取得するためにＢＳＦによる問い合せをインタフェース１９１（Ｄｎ）経由で受ける。ＵＥはネットワークアプリケーション機能プロキシ（ＮＡＦ）１６０を介して、少なくとも１つのアプリケーションサーバ（ＡＳ）１５０＿ｎに対して同時に接続することができる。接続は、ＵＥとＮＡＦとの間の認証に関する第１のステップを含む。これにより、ＵＥは参照Ｂ－ＴＩＤをＮＡＦへ提供し、ＮＡＦは、Ｂ－ＴＩＤを使用して、ＢＳＦに対してインタフェース１９０（Ｚｎ）経由で鍵（Ｋｓ＿ＮＡＦ）を要求する。鍵Ｋｓ＿ＮＡＦは、鍵Ｋｓから導出される。ＵＥでも同じ鍵を導出可能である。認証はその後、導出された鍵Ｋｓ＿ＮＡＦに基づいて行われる。ＵＥとＮＡＦとの間の通信は、インタフェース（Ｕａ）１８０経由である。

【００２５】

説明を目的として、以下の説明では、３ＧＰＰ　ＩＭＳに従うＳＩＰベースのシグナリングが使用される。しかしながら、当業者であれば容易に理解できるように、本発明は、セッションのセットアップのために要求されるメタデータを搬送可能な他のプロトコルを使用することができる。

【００２６】

図２は、ＩＭＳコアネットワーク（ＣＮ）サブシステムの基本的なエレメント及びアプリケーションサーバ２１０に対する接続を説明する図である。図２はホームネットワーク内に位置するアプリケーションサーバを示すが、サービスプラットフォームはホームネットワークの外に位置してもよいということが理解されるはずである。

【００２７】

ＩＰマルチメディア・コアネットワーク（ＩＭ　ＣＮ）サブシステムにより、ＰＬＭＮ及び固定ラインのオペレータは、自分達の加入者に対して、インターネットのアプリケーション、サービス、及びプロトコルに基づきそこに構築されるマルチメディアサービスを提供可能である。その意図は、ＰＬＭＮオペレータ、及び、インターネット及びＩＭＳシステムによって提供されるメカニズムを使用するインターネット空間におけるサプライヤを含む他のサードパーティーサプライヤによって、そのようなサービスが配置されるであろうということである。ＩＭＳシステムは、固定ライン及び無線のユーザのために、音声、ビデオ、メッセージング、データ、及びウェブベースの技術について、これらの収斂を可能にし、また、これらに対するアクセスを可能にする。

【００２８】
プロキシＣＳＣＦ（Ｐ－ＣＳＣＦ）２２０は、ＩＭＳシステム内の最初のコンタクトポイントでありＵＥからのＳＩＰ　ＩＮＶＩＴＥメッセージに応答する。そのアドレスは、発見メカニズムを使用してＵＥ１０１によって発見可能である。Ｐ－ＣＳＣＦはプロキシのように振舞う。即ち、要求を受信し、それに対して内部的にサービス提供するか、又は、それをサービングＣＳＣＦ（Ｓ－ＣＳＣＦ）２３０へ転送する。Ｓ－ＣＳＣＦはＳＩＰ要求をホームネットワークのアプリケーションサーバ２１０へルーティングする。
【００２９】
ここで、図３を参照して、本発明の第１の実施形態を説明する。図３において、同様の符号は図１及び図２における同様のエンティティに対応する。図３には、ＧＢＡ／ＧＡＡ方法に従って各々のブートストラッピング機能ＢＳＦ＿Ａ　１１０＿Ａ及びＢＳＦ＿Ｂ１１０＿Ｂとブートストラッピングを実行可能な２つのユーザエンティティＵＥ＿Ａ及びＵＥ＿Ｂが示されている。しかしながら、当業者によって容易に理解されるように、そのようなサーバとの共有鍵を生成するために利用可能ないかなる他の手段も使用可能である。それゆえ、ブートストラッピングは、ＩＤカードの信用保証情報（例えば、ＳＩＭ、ＵＳＩＭ、又はＩＳＩＭ）に基づいてもよいし、ＰＫＩに基づいてもよいし、ユーザ名／パスワードに基づいてもよい。ブートストラッピングの結果、各ＵＥ及び関連するＢＳＦは、それぞれ共有鍵Ｋｓ＿Ａ及びＫｓ＿Ｂを決定することができる。ユーザＡ及びＢは、３２０で示される通信をセットアップしたいと願う。本発明によれば、各ＵＥは、それぞれ３１０＿Ａ及び３１０＿Ｂで示される鍵管理サーバＫＭＳ＿Ａ及びＫＭＳ＿Ｂによってサポートされる。
【００３０】
本発明によれば、ユーザＡ及びＢは、自分達それぞれのセキュリティ管理を異なる信用保証情報（例えば、＊ＳＩＭカード（ＳＩＭ、ＵＳＩＭ、ＩＳＩＭ）のようなＩＤカード、ユーザ名／パスワード、公開鍵ＰＫＩ、又はパスワードに基づくもの）に基づかせることができる。
【００３１】
鍵管理エンティティＫＭＳ間の３３０で示されるドメイン間ネットワークシグナリングは、例えばＴＬＳ又はＩＰｓｅｃを使用してセキュアにすることができる。シグナリングは、暗号化され、及び／又は、完全性が保護され得る。
【００３２】
通常のＧＢＡ／ＧＡＡインタフェースＵａ、Ｕｂ、Ｚｎが、図１と対応して図３に示される。
【００３３】
ここで、本発明の実施形態に従う信号図を示す図４を参照する。図４において、ＩＭＳ構造及びＧＢＡ／ＧＡＡ構造からのエンティティが、図１乃至図３に関連して説明したように示される。単純化のために、ユーザＡはＵＥ＿Ａと示される場合もある。
【００３４】
以下では、$(x)_K$は、鍵Ｋによるｘの保護を示す。保護は、秘匿性及び／又は完全性の保護として理解され、秘匿性の保護はメッセージｘの部分に対してのみ適用されてもよいということが理解されるはずである。
【００３５】
ここで、先行技術に従うステップ１及びステップ２が実行される。
【００３６】
ステップ１で、ユーザＡはＩＭＳに登録する。
【００３７】
ステップ２で、ユーザＡはＧＢＡブートストラップを実行し、これにより、鍵Ｋｓ＿Ａが生成されてＡとＢＳＦ＿Ａとの間で共有される。このステップにおいて、Ａに対して、ＢＳＦ＿Ａにより参照Ｂ－ＴＩＤ＿Ａが提供される。ステップ２は、サブステップ２：１を含み、ここで、ＫＭＳ＿ＡはＡから参照Ｂ－ＴＩＤを受信し、Ｂ－ＴＩＤは更に、Ｋｓ

＿Ａから導出される鍵ＫＡ＝Ｋｓ＿ＫＭＳ＿ＡをＢＳＦからフェッチするために使用される。Ｋｓ＿Ａ及び派生した他の情報を知っているユーザＡは、同一の鍵を算出する。それゆえ、Ａ及びＫＭＳ＿Ａは、セキュアな通信のために使用可能な鍵ＫＡを共有する。

【００３８】

対応するステップがＢ側で実行され、図４において同一の参照番号で示される。これにより、対応するエンティティ（即ち、Ｋｓ＿Ｂ、Ｂ－ＴＩＤ＿Ｂ、及びＫＢ＝Ｋｓ＿ＫＭＳ＿Ｂ）が生成される。

【００３９】

なお、ユーザとしてのＢは、いくつかのデバイスを持っていてもよく、その各々が、通信のために使用可能である。しかしながら、鍵ＫＢは、ステップ１及び２に従ってブートストラップを実行した特定のデバイスに対してのみ有効である。Ｂがいくつかのデバイスを使用可能であるという事例は、フォーキング問題をもたらし得るものであり、代替実施形態において更に論じられる。現在の第１の実施形態に関しては、Ｂは１つのデバイスだけを使用して通信の招待に応答するものとする。

【００４０】

３において、ユーザＡはユーザＢと通信することを決定する。

【００４１】

ステップ４で、Ａは、本発明に従って鍵管理サーバＫＭＳ＿Ａに対して鍵要求を送信する。このステップにおいて生成される鍵は、引き続いて、Ｂとのセキュアなエンド・ツー・エンド通信のために使用されることになる。鍵要求は次のフォーマットを持つ。

$$\text{GET key info} = (\text{Id\_A, Id B, key\_type, param, ... })_{KA}, \text{B-TID\_A}$$

ここで、Ｉｄ＿Ａ及びＩｄ＿ＢはそれぞれユーザＡ及びＢを特定するＩＤであり、ｋｅｙ＿ｔｙｐｅは要求される鍵の種類（例えば、ポイント・ツー・ポイント通信のための鍵、又はグループ通信のための鍵）である。Ｉｄ＿Ａはグローバルの形式を持ってもよく、典型的にはＩｄ＿Ａ＝Ａ＠ｏｐ．ｃｏｍである。最後に、ｐａｒａｍは、メッセージ内に含めることのできるあらゆる他のパラメータを示す。メッセージは、以前に生成された鍵ＫＡによって暗号化される。加えて、参照Ｂ－ＴＩＤがメッセージに含まれ、これにより、ＫＭＳ＿ＡはＧＢＡ／ＧＡＡ手順に従ってＢＳＦ＿Ａから鍵ＫＡを取得可能である。或いは、ブートストラッピングに対する非ＧＢＡベースのアプローチでは、Ｉｄ＿Ａが鍵ＫＡを一意に決定しない場合は何らかの他の鍵識別情報が使用されるであろう。注意すべきことは、受信者Ｂが使用する信用保証情報の種類に関してはここでは何も言及されておらず、それゆえ、本発明に従う方法は、送信者Ａ又は受信者Ｂでの信用保証情報の種類から独立しているということである。

【００４２】

５において、ＫＭＳ＿Ａは、メッセージ"RETURN key info"を用いてＡに対して応答する。その形式は、

$$\text{RETURN key info} = (\text{Key\_info\_A, VOUCHER})_{KA}$$

である。ここで、Ｋｅｙ＿ｉｎｆｏ＿Ａは鍵K_{AB}、又はステップ６においてＡが鍵K_{AB}を算出することを可能にする鍵材料を含む。ＶＯＵＣＨＥＲというエンティティは、本発明によれば、ＫＭＳ＿Ｂが引き続いて同一の鍵K_{AB}を再生成することを可能にしてＡ及びＢがセキュアに通信できるようにすることになる情報を含む。ＫＭＳ＿ＢがＫＭＳ＿Ａに関して知ることになるようにするため、バウチャーはＩｄ＿Ａを含む。

【００４３】

バウチャーは更に、完全性が保護されており、バウチャーの少なくとも一部は暗号化されていてもよい。典型的な完全性及び秘匿性の鍵は、鍵ＫＡから導出され得る。

【００４４】

鍵K_{AB}は例えば、ＫＡ、及び、ＡとＢとのＩＤ、及び／又は、ナンス(nonce)の暗号化関数として生成可能である。この場合、Ｋｅｙ＿ｉｎｆｏ＿Ａはナンスを含むことになろう。或いは、K_{AB}は完全に乱数鍵であってもよく、この場合、Ｋｅｙ＿ｉｎｆｏ＿Ａは鍵K_{AB}自体を含む。

【００４５】

本実施形態によれば、バウチャー情報は、ＫＭＳ＿Ａに格納されている鍵K_{AB}又は鍵材料を取り出すためのポインタ、典型的にはＢ－ＴＩＤを含む。他の情報がバウチャーに含まれてもよく、例えば、鍵の種類の情報（ピア・ツー・ピア通信又はグループ通信など）、関与する当事者のＩＤ、バウチャーの発行者（即ち、ＫＭＳ＿ＡのＩＤ）、発行時刻又はシーケンス番号、有効期限、使用形態（プッシュ・ツー・トーク・オーバー・セルラ（ＰｏＣ）又はマルチメディア電話（ＭＭＴＥＬ）など）などである。

【００４６】

ステップ７で、ＡはＩＭＳ基盤に従ってＳＩＰ　ＩＮＶＩＴＥをユーザＢへ向け、Ａにサービス提供しているＰ－ＣＳＣＦ、Ｓ－ＣＳＣＦを通過して、Ｂにサービス提供しているＳ－ＣＳＣＦに到達する。ステップ８で、招待メッセージはユーザＢへ転送される。招待メッセージは少なくともバウチャーを含む。このメッセージ内の他の情報として、鍵情報の種類が含まれてもよい。

【００４７】

ステップ９で、ユーザＢは、ＫＭＳ＿Ｂからの鍵K_{AB}の再生成のために、"GET key info"メッセージの中でバウチャーをＫＭＳ＿Ｂへ転送する。このメッセージは、典型的には次の形式を有する。

```
GET key info = VOUCHER, B-TID_B
```

ここで、Ｂ－ＴＩＤ＿Ｂは、ユーザＢの認証のため、及び、ステップ４に関連して上述したのと同様のやり方でユーザＢとＫＭＳ＿Ｂとの間のセキュアな通信のための鍵ＫＢを確立するための、ＧＢＡ／ＧＡＡ参照である。

【００４８】

ステップ９：１で、ＫＭＳ＿ＡとＫＭＳ＿Ｂとの間で通信が発生し、ここで、ＫＭＳ＿Ａは、ＫＭＳ＿Ｂが鍵K_{AB}を再生成する手助けをする。第１の実施形態によれば、バウチャーはステップ５でＫＭＳ＿Ａによって生成されたポインタを含み、ステップ５でユーザＡに返されたものと同じ鍵材料をＫＭＳ＿Ａが取り出すことを可能にする。前記ポインタは、ステップ９：１において鍵要求の中で次の形式で通信される。

```
pointer, Id_B
```

ここで、ポインタはＫＭＳ＿Ｂにおいてバウチャーから抽出され、ＫＭＳ＿Ａにおいて鍵材料を取り出すために使用される。Ｉｄ＿ＢはユーザＢのＩＤである。ＫＭＳ＿Ｂによって鍵要求の中にＩｄ＿Ｂを含めることにより、鍵を要求する者が意図されたユーザＢであるということ（即ち、ユーザＢのふりをしてバウチャーを傍受してユーザＡとのセキュアな通信のための鍵を取得しようとしている者はいないということ）をＫＭＳ＿Ａが判断することが可能になる。

【００４９】

鍵要求に応えて、ＫＭＳ＿Ａは、鍵K_{AB}又は鍵材料（これはその後、ステップ１１における鍵K_{AB}の生成のために、ステップ１０でＫＭＳ＿Ｂによってユーザ Ｂへ転送される）を含む鍵情報Ｋｅｙ＿ｉｎｆｏ＿Ｂを返す。ステップ１０における鍵情報は、ステップ９で典型的には生成された鍵ＫＢを使用して暗号化される。ステップ１０で鍵材料だけが配信された場合、ステップ１１において鍵K_{AB}を生成する鍵生成が実行される。

【００５０】

ステップ１１は、ユーザＢが招待信号７に対するＳＩＰ　２００　ＯＫ応答を返すこと

を含み、すると、ＡとＢとの間のセッションが開始する。

【００５１】

有利なことに、第１の実施形態によれば、上で言及したポインタはエンティティＢ－ＴＩＤ＿Ａを含む。

【００５２】

鍵の種類の情報がポイント・ツー・ポイント通信を指定する場合、ステップ９：１でＫＭＳ＿Ｂへ返される鍵は十分であり、鍵に関する更なる処理は必要とされない。

【００５３】

ＧＢＡ／ＧＡＡ標準から知られていることであるが、参照Ｂ－ＴＩＤは有効期限を持っていてもよい。それゆえ、代替実施形態においては、ＫＭＳ＿Ａは、ユーザＡが新たにブートストラップを実行して新しいＢ－ＴＩＤを生成した場合を管理するために、少なくとも以前に使用されたＢ－ＴＩＤ及び対応する鍵材料を格納することにより状態を維持管理する。

【００５４】

図５を参照して、鍵情報（Ｋｅｙ　ｉｎｆｏ）がグループ鍵が要求されているということを示す場合に関係する第２の実施形態を説明する。図５において、Ａ側とＢ側との間に中間者が挿入される。好ましくは、中間者はＡパート中間者ＩＭ＿Ａ及びＢパート中間者ＩＭ＿Ｂに分割される。典型的には、各パートは、プッシュ・ツー・トーク・オーバー・セルラ・サーバ（ＰｏＣサーバ）を含み得る。図５において、受信者当事者の表記Ｂは、各々が個々のＩＤであるＩＤ＿$Ｂ_k$を持つユーザのグループをここでは表す。更に、単純化のために、Ｂ側の各ユーザは同一のＢＳＦ＿Ｂ及び同一のＫＭＳ＿Ｂに接続するものとするが、各ユーザは別々のＢＳＦ機能及びＫＭＳ機能を使用してもよい。

【００５５】

図５において、同様の信号参照は図４の同様の信号を示すが、信号メッセージ部分は以下に説明するように若干異なっていている場合もある。

【００５６】

ステップ１、２、２：１、３は、第１の実施形態に従う対応するステップと同一であるが、例外として、ステップ３で、被呼当事者Ｂは、ここではグループＩＤである$Ｇ_{ＩＤ}$で特定されるグループを表す。

【００５７】

ステップ４で、今回はＧＥＴメッセージは$Ｇ_{ＩＤ}$を含む。ステップ５で、バウチャー及び鍵材料（例えば、マスター鍵Ｋ）が、ステップ６でのセッション鍵$Ｋ_{ＩＭＡ}$の生成のために返される。或いは、セッション鍵は返答メッセージ中に含まれている。ここで注目されることは、前記セッション鍵は引き続き、グループの参加者と直接ではなく中間者（例えば、ＩＭ＿Ａ）と通信するためにＡによって使用されるであろうということである。マスター鍵及び他の情報は、ブートストラッピングのステップ２、２：１で生成された鍵ＫＡで保護され得る。

【００５８】

ステップ７：１で、図４のステップ７と同様に、ＩＮＶＩＴＥメッセージが、中間者を介してグループへ、或いは中間者のＩＭ＿Ａパートへ、送信される。招待メッセージは、バウチャーと、少なくとも$Ｇ_{ＩＤ}$を含む他の情報とを含む。

【００５９】

ステップ８：１で、中間者ＩＭ＿Ａは、バウチャーからのＩＤ＿Ａがグループ鍵であると認識し、バウチャーをＫＭＳ＿Ａに転送して鍵材料を要求し、すると、ＫＭＳ＿Ａは前記マスター鍵ＫをＩＭ＿Ａに返す。加えて、セッション鍵$Ｋ_{ＩＭＡ}$が、返されるか、又は、ＩＭ＿Ａにおいてマスター鍵から生成される。

【００６０】

ステップ８：２で、ＩＭ＿Ａは、招待メッセージの中で提供されたグループＩＤをユーザＩＤであるＩＤ＿$Ｂ_k$のグループに変換し、各グループメンバーのための個々のセッション鍵$Ｋ_{ＩＭＢ}$をマスター鍵Ｋから生成する。個々の鍵$Ｋ_{ＩＭＢ}$は各$Ｂ_k$のために生成さ

れるということが理解される。加えて、ＫＭＳ＿Ａから受信されない場合、セッション鍵K_{IMA}がマスター鍵Ｋから生成される。注目すべきこととして、中間者は、グループＩＤから個々のグループメンバーを取り出すために関連するグループ管理サーバ（不図示）からの支援を必要とする。

【００６１】

個々の鍵K_{IMB}は、鍵K_{IMB}＝Ｆ（Ｋ，”Ｘ”）として算出可能である。ここで、”Ｘ”は、グループB_kの代表である当事者Ｘに関する何らかの特徴的なＩＤを示す。

【００６２】

セッション鍵K_{IMA}及びK_{IMB}は、引き続き、通信リンクＡ－各々の中間者－Ｂを保護するために使用される。

【００６３】

ステップ７で、中間者ＩＭ＿Ａは、バウチャーを含むＳＩＰ　ＩＮＶＩＴＥメッセージを全てのグループメンバーへ送信する。ＩＭＳ基盤によれば、メッセージはＳ－ＣＳＣＦを通過し、更に、ステップ８でＰ－ＣＳＣＦを経由して受信者B_kにサービス提供しているネットワークに到達する。メッセージ７は図４におけるそのメッセージに対応するが、本実施形態では、送信者はユーザＡではなく中間者である。

【００６４】

図４のステップ９に対応するステップ９で、各受信者B_kは、バウチャーを適切な鍵に変換するためにサービングＫＭＳ＿Ｂにコンタクトする。

【００６５】

ステップ９：１で、第１の実施形態と同様に、ＫＭＳ＿ＡとＫＭＳ＿Ｂとの間で通信が発生し、ここで、ＫＭＳ＿Ａは鍵K_{IMB}、或いはマスター鍵Ｋを、ＫＭＳ＿Ｂへ返し、ステップ１０で、ＫＭＳ＿Ｂから、個々のグループメンバー鍵KB_k（単純化のために図５では鍵ＫＢと示す）で保護されて各グループメンバーへ転送される。メッセージ１０は、図４における同じメッセージに対応する。ステップ１０は全てのグループメンバーB_kに対して繰り返されるということを理解すべきである。鍵ＫＢは、ＫＡに対応して算出され、各B_kが関連するＢＳＦ機能とのブートストラッピングを実行しているものとする。ＫＭＳ＿Ａがマスター鍵Ｋを返す場合、各B_kはそこから、対応する鍵K_{IMB}を算出する。

【００６６】

ステップ１１で、２００　ＯＫ信号が、各々の招待信号７：１、７、及び８に応えて返され、すると、Ａ－ＩＭ－B_k（ｋ＝１，２，．．．）間のセッションが開始可能である。

【００６７】

ここで、ＡはグループメンバーB_kと通信可能であり、その際に、Ａは中間者に対する通信を鍵K_{IMA}を使用して暗号化し、中間者においてメッセージは復号され場合によっては転送される前に処理（例えば、トランスコード）され、鍵K_{IMB}を使用して再暗号化され、全てのB_kに対して個別に転送される。

【００６８】

或いは、K_{IMA}＝K_{IMB}である。

【００６９】

第２の実施形態の代替によれば、ステップ８：１は、鍵K_{IMA}又はマスター鍵Ｋを含まない。それゆえ、本実施形態では、中間者は開始者当事者Ａからの通信を処理するために通信を復号することができない。その結果、鍵K_{IMB}を使用して通信を再暗号化するステップは、無関係である。従って、中間者はこの場合、基本的にＩＮＶＩＴＥメッセージを各メンバーへ提供するためにグループＩＤを個々の応答者グループメンバーに変換するように機能し、引き続いて、情報を更に処理することなく、通信をＡから各B_kへ転送するように機能する。

【００７０】

第２の実施形態の代替は、アップリンク（中間者へ）及び各ダウンリンク（中間者から

ユーザＡ及びＢへの方向）のために別々の鍵を算出することを含む。前記マスター鍵Ｋは、鍵生成のための基礎となり得る。

【００７１】

第２の実施形態の代替実施形態によれば、鍵の種類はアドホックのグループ鍵を示し、これにより、ステップ８：１で、ＩＭ＿Ａは鍵材料Ｋを要求し、ステップ８：２で、Ａからの招待メッセージ７：１において提供された当事者のリストからユーザＩＤであるＩＤ＿$Ｂ_k$のグループを生成する。最後に、ＩＭ＿Ａは、ユーザＡによって指定されたアドホックグループの各メンバーのために、マスター鍵Ｋから個々の鍵$ＫＢ_k$を生成する。

【００７２】

第２の実施形態の更に別の代替によれば、各グループメンバーは個々の鍵を取得するが、この鍵は更に、アップリンク（ユーザＢから中間者ＩＭ＿Ａへの方向）及びダウンリンク（中間者ＩＭ＿ＡからユーザＢへの方向）で異なっていてもよい。典型的には、ＩＭ＿Ａは、次のスキームに従って鍵の個人化（パーソナライゼーション）を実行してもよい。

$$Key\_User\_B_k\_uplink = F(K, "B_k", "UPLINK")$$

ここで、”$Ｂ_k$”は、個々の$Ｂ_k$に特徴的な何らかのデータを示し、Ｋは、以前に定義されたマスター鍵である。各$Ｂ_k$が同一の対応する鍵を生成するために、ステップ７及び８のＩＮＶＩＴＥ信号は好ましくは、特徴情報”$Ｂ_k$”を含み、ＫＭＳ＿Ｂへの要求メッセージ１０にも更に含まれ、ＫＭＳ＿Ｂにおいてその後、パーソナライゼーションが実行される。パーソナライズされた鍵は、最終的に、信号１０の中でユーザ$Ｂ_k$に提供される。

【００７３】

以前の更に別の代替の代替によれば、中間者は、マルチキャストを介してグループ$Ｂ_k$と通信する。この場合、全てのユーザ$Ｂ_k$は、ダウンリンク情報を受信するために同一のグループ鍵を使用する。それゆえ、この場合ダウンリンクのパーソナライゼーションは行われず、全てのユーザ$Ｂ_k$はＫＭＳ＿Ａから同一のダウンリンク鍵を受信する。

【００７４】

第２の実施形態の別の代替によれば、中間者はユーザＡからの通信の処理（例えば、トランスコード）に関与せず、そしてそれゆえ、中間者には、ユーザＡによって通信されるペイロードを復号する能力が備えられない。この場合、それゆえ、ステップ８：１及び８：２は省略され、ステップ７及び８において、バウチャーは、グループＩＤの変換を通して中間者ＩＭ＿Ａによって特定されたグループへと単純に転送される。そして、第１の実施形態と同一の鍵変換メカニズムが、受信側で使用される。効果的には、これは、Ａ側及びＢ側が中間者の干渉無しにエンド・ツー・エンドで通信することを意味する。

【００７５】

例えばマルチキャストの場合に最も考えられることであるが、一般的な課題が現れるかもしれず、それは、中間者又はシグナリングリンクを盗聴してバウチャーを取得した無権限のユーザがそれをＫＭＳ機能へ転送してそれを解決（変換）するように要求できてしまうかもしれないことである。それゆえ、好ましくは、ＫＭＳ機能は、バウチャーを解決してあげるユーザがグループの権限あるメンバーであることをチェック可能であるべきである。それゆえ、この代替実施形態によれば、ユーザ固有ランダムＩＤ、又は他のワンタイムＩＤが、中間者からのＳＩＰシグナリングにバウチャーと共に含まれる。ＳＩＰシグナリングは保護されているので、バウチャー及びＩＤにアクセスしようとする外部当事者に対してＩＤは保護されている。ＫＭＳ機能は、ランダムＩＤがまだいずれの他のユーザによっても提示されていないということをチェックすることができる。

【００７６】

代替として、ＩＤは個々のユーザのための鍵導出に対しても入力されてもよい。

【００７７】

第１及び第２の実施形態によれば、要求信号４において取得される鍵材料は、１以上のセッション鍵$Ｋ_{ＡＢ}$又は$Ｋ_{ＩＭＡ}$を含むことができる。受信された１以上のセッション鍵

は、例えばＭＩＫＥＹプロトコルを使用して、ペイロードデータをセキュアにするために直接的又は間接的に使用可能である。

【００７８】

しかしながら、第１及び第２の実施形態の代替において、信号５は、そこ（ナンス）から対応するセッション鍵を（例えば、ＫＡ＝Ｋｓ＿ＫＭＳ＿Ａから）導出可能な１以上のナンスを含んでもよい。このナンス（例えば、バウチャーに含まれる）の伝送は、暗号化される必要が無い。

【００７９】

ユーザＡが切断した場合、又は、新たなブートストラッピングを実行してそれにより新しい鍵ＫＡ’が新たなブートストラッピングの結果として得られたであろうから以前の鍵ＫＡ＝Ｋｓ＿ＫＭＳ＿Ａがもはや有効ではない場合に、問題が発生するかもしれない。ＫＭＳ＿Ａがバウチャーを受信したときに、その中の情報はセッション鍵K_{AB}又はK_{IM_A}を再生成するのに役に立たないかもしれない。

【００８０】

それゆえ、第１及び第２の実施形態の代替において、ＫＭＳ＿Ａは、状態を維持管理して以前に使用した鍵ＫＡを保存する。

【００８１】

更に別の代替において、バウチャーは、ＫＭＳ＿Ａのみが知っている鍵によって保護されるバウチャーフィールドの中に、鍵ＫＡのコピーを含んでもよい。後者の場合、秘密鍵のみが維持管理される必要があり、個々のユーザの状態をＫＭＳ＿Ａによって維持管理する必要は無い。

【００８２】

第１及び第２の実施形態の別の代替によれば、図４及び図５のステップ７において、Ｓ－ＣＳＣＦは、ユーザＢ（或いは、グループの場合は各ユーザB_k）の代わりに図４及び図５のステップ９及び１０を実行し、バウチャーを鍵生成情報に置き換え、それをステップ８で転送されるＳＩＰメッセージの中に直接含めてもよい。或いは、ステップ８は何らかの他の方法（例えば、ＧＢＡプッシュ）によって実行され、それにより、Ｓ－ＣＳＣＦは信号１２を送信することによってＳＩＰシグナリングを終端する。

【００８３】

いずれかのＢ又はB_kが幾つかの利用可能なデバイスのうちのいずれかでＳＩＰ　ＩＮＶＩＴＥ信号８に対して応答するかもしれないという特別な場合には、幾つかの事前注意が必要である。この場合、応答デバイスはブートストラッピングのステップ１及び２から特定の鍵ＫＢ’又はKB_k’を生成している。それゆえ、招待メッセージに応答するためにどのデバイスが使用されるであろうかを知らないＳ－ＣＳＣＦは、ステップ９を実行する際に全ての可能性を含めなければならず、全ての可能性ある個々の鍵K'_{IMB}を生成するようにステップ９を繰り返す。それゆえ、Ｓ－ＣＳＣＦがＳＩＰ　ＩＮＶＩＴＥ要求８に対する応答を最終的に受信したときに、適切な鍵K'_{IMB}が用意され、ステップ１０における使用の準備ができる。

【００８４】

注目すべきこととして、説明した代替実施形態は、ＳＩＰコアのオペレータが信用されなければならない通信の保護のための鍵をＳ－ＣＳＣＦが知っているという点で、異なる信用モデルを必要とする。しかしながら、これは、通常は妥当な想定である。

【００８５】

第１及び第２の実施形態の別の代替は、メッセージングサービス（即ち、ユーザＡがメッセージをユーザＢ、又はグループの場合は各B_kへ送信する）に関する。メッセージは、招待メッセージ７又は７：１に含まれてもよい。少なくとも１つの受信者がネットワークに登録していないとＳ－ＣＳＣＦによって判定された場合、Ａからメッセージは、受信者Ｂ又はB_kがアクティブであると登録するまで、ネットワークノード（典型的にはネットワークノードＳ－ＣＳＣＦ）にバウチャーと共に格納され得る。

【００８６】

後になって、Ｂがネットワークに登録されると、Ｓ－ＣＳＣＦはプロトコルを継続し、典型的にはＧＢＡプッシュを使用してバウチャーをＢ又はＢ$_k$へプッシュし、Ｂ又はＢ$_k$に対してどこでメッセージを発見可能かを知らせることができる。このアプローチは、延期サービスとして扱うことのできるいかなるサービスに対しても、汎用的に有効である。Ａは、切断した、及び／又は新たなブートストラッピングを実行したかもしれないので、ＫＭＳ＿Ａが正しい鍵生成情報を取り出すことができることを前提とするために、上述したものと同様のメカニズムを使用可能である。

【００８７】

図３は本発明に従う方法に関与する機能間の具体的なインタフェースを示すが、容易に理解されることとして、インタフェースは例えば図６に示すように多数のやり方で異なるように構成可能である。図６において、Ｔ＿Ａインタフェース及びＴ＿Ｂ１インタフェースは、ＧＢＡ方法に従う既知のＵａインタフェースに対応する。

【００８８】

インタフェースＴ＿Ｂ２はＴ＿Ｂ１の代替であり、ここで、ユーザＢはＫＭＳ＿ＢではなくＫＭＳ＿Ａと通信する。

【００８９】

Ｋ＿ＡＢ１は、バウチャーを解決（変換）する際に必要とされる、ＫＭＳ機能間のインタフェースである。

【００９０】

Ｋ＿ＡＢ２は、ＢのドメインのＫＭＳとＡのドメインのＢＳＦとの間の、ドメイン間鍵管理インタフェースである。ドメインＢのＫＭＳは、バウチャーを鍵に変換する支援を得るためにこのインタフェースを使用することができる。

【００９１】

Ｋ＿ＡＢ３は、ＡのドメインのＫＭＳとＢのドメインのＢＳＦとの間の、ドメイン間鍵管理インタフェースである。

【００９２】

容易に理解されるであろうが、第１及び第２の実施形態は共に、ＫＭＳ機能において合法的傍受を提供する。鍵ＫＡを知っている当局は、ＡからＢ又は中間者への通信を傍受することを可能にするセッション鍵Ｋ$_{AB}$（或いは、第２の実施形態では鍵Ｋ$_{IMA}$）を生成することができる。

【００９３】

本発明に従う、通信ネットワークにおける当事者間のセキュアな通信のためのセッション鍵の生成を支援する装置を、図７に示す。

【００９４】

図７において、７１０に、入力／出力ユニットが示される。手段７１０は、他の支援ユニット又はエンドユーザと鍵情報を通信可能であり、典型的には、鍵情報の要求、又は鍵情報に変換するためのバウチャーをエンドユーザから受信する。手段７１０は更に、ブートストラッピング手順において生成された鍵材料を受信するために、支援ブートストラッピング機能との通信を提供する。

【００９５】

手段７２０は、ブートストラッピング機能から典型的には受信したブートストラップ情報からの鍵材料の導出のような、鍵情報の生成を提供する。

【００９６】

手段７３０は、格納された鍵情報を記憶装置７４０から取り出すために、受信したバウチャーを処理する。手段７３０は更に、場合によっては支援ネットワークユニットと通信して、ユーザグループＩＤを個々のグループメンバーに変換する。

【００９７】

７５０において、汎用処理手段は、多様な処理に関する必要な制御を提供する。

【００９８】

このように非限定的な例を介して説明された本発明は、（機能エンティティ、通信イン

タフェース、及びシグナリングを実装するための）多数の変形例を提供するものであると容易に理解される。

【図１】

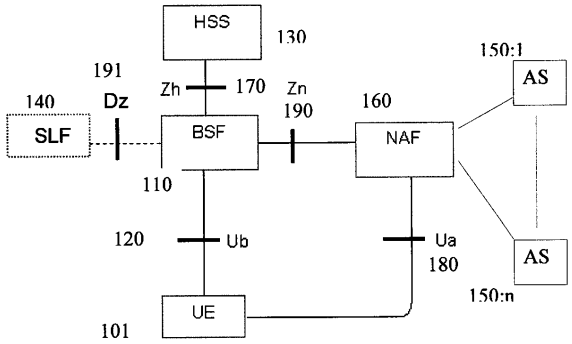

Figure 1

【図２】

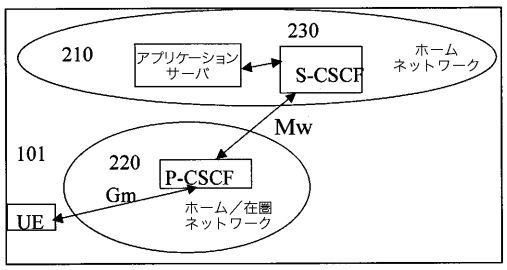

Figure 2

【図３】

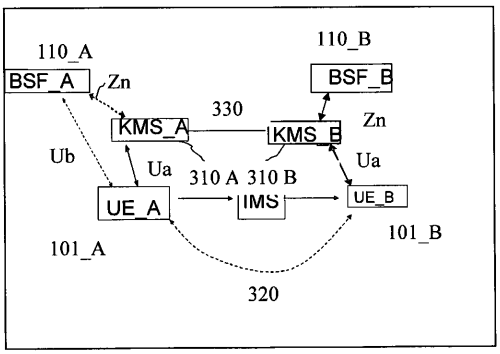

Figure 3

【図６】

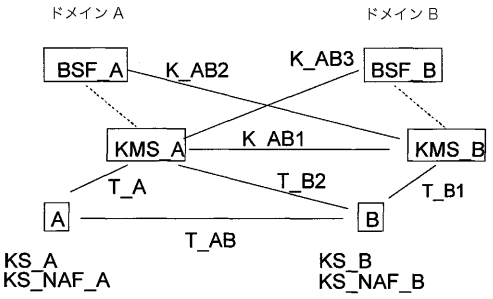

Figure 6

【図７】

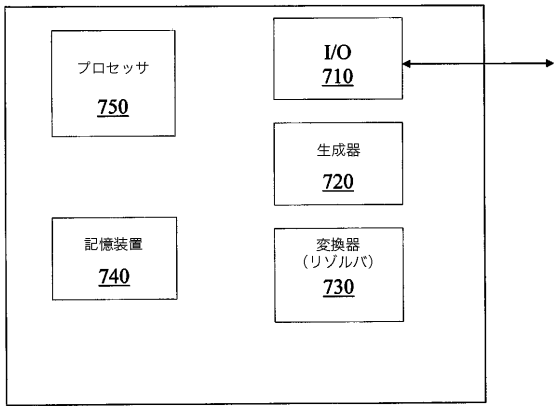

Figure 7

【図４】

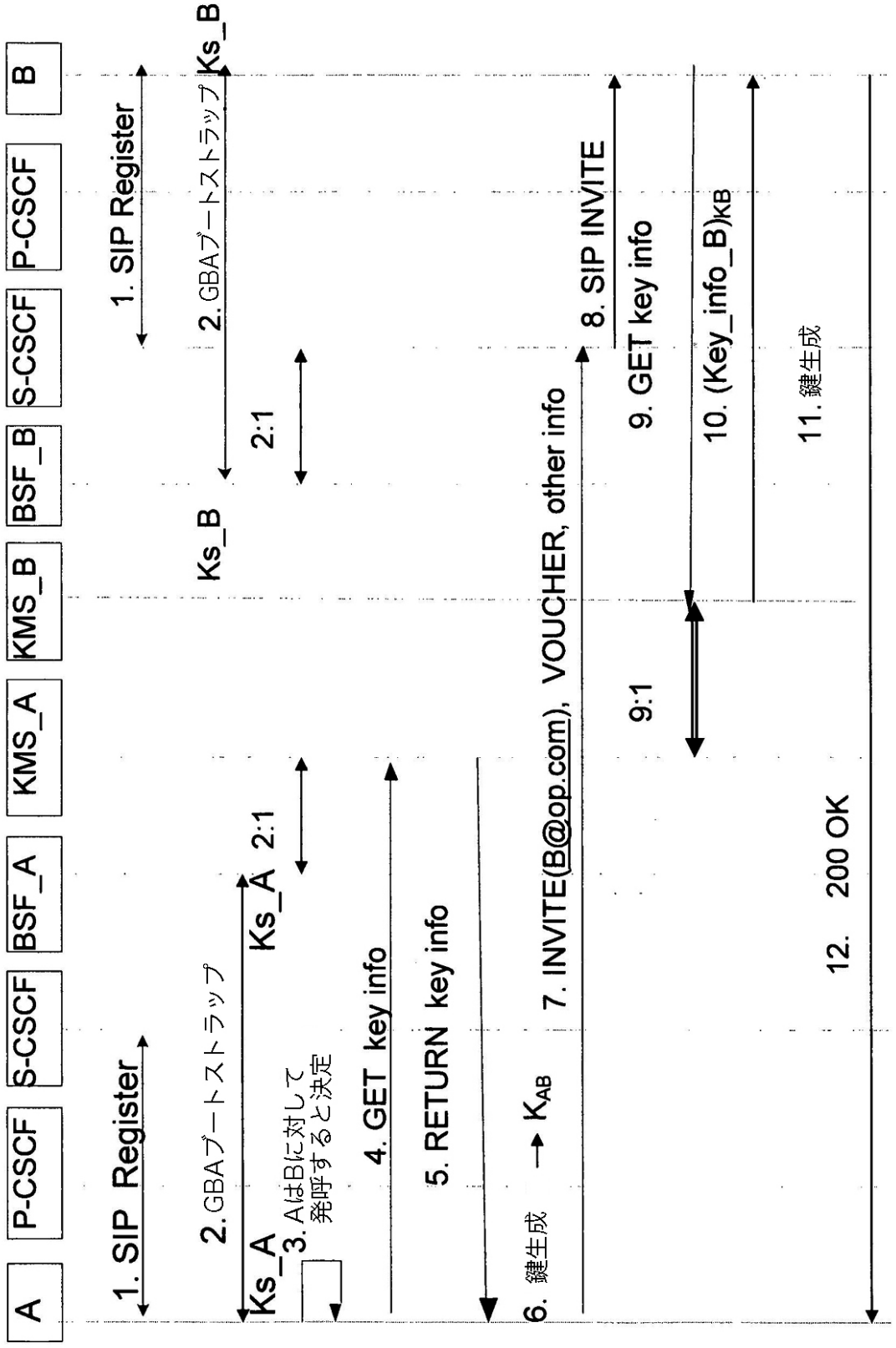
A
P-CSCF
S-CSCF
BSF_A
KMS_A
KMS_B
BSF_B
S-CSCF
P-CSCF
B
1. SIP Register
1. SIP Register
2. GBAブートストラップ
Ks_B
2. GBAブートストラップ
Ks_A
Ks_A
2:1
Ks_B
2:1
3. AはBに対して
発呼すると決定
4. GET key info
5. RETURN key info
6. 鍵生成 → K_{AB}
7. INVITE(B@op.com), VOUCHER, other info
8. SIP INVITE
9. GET key info
9:1
10. $(Key\_info\_B)_{KB}$
11. 鍵生成
12. 200 OK

Figure 4

【図５】

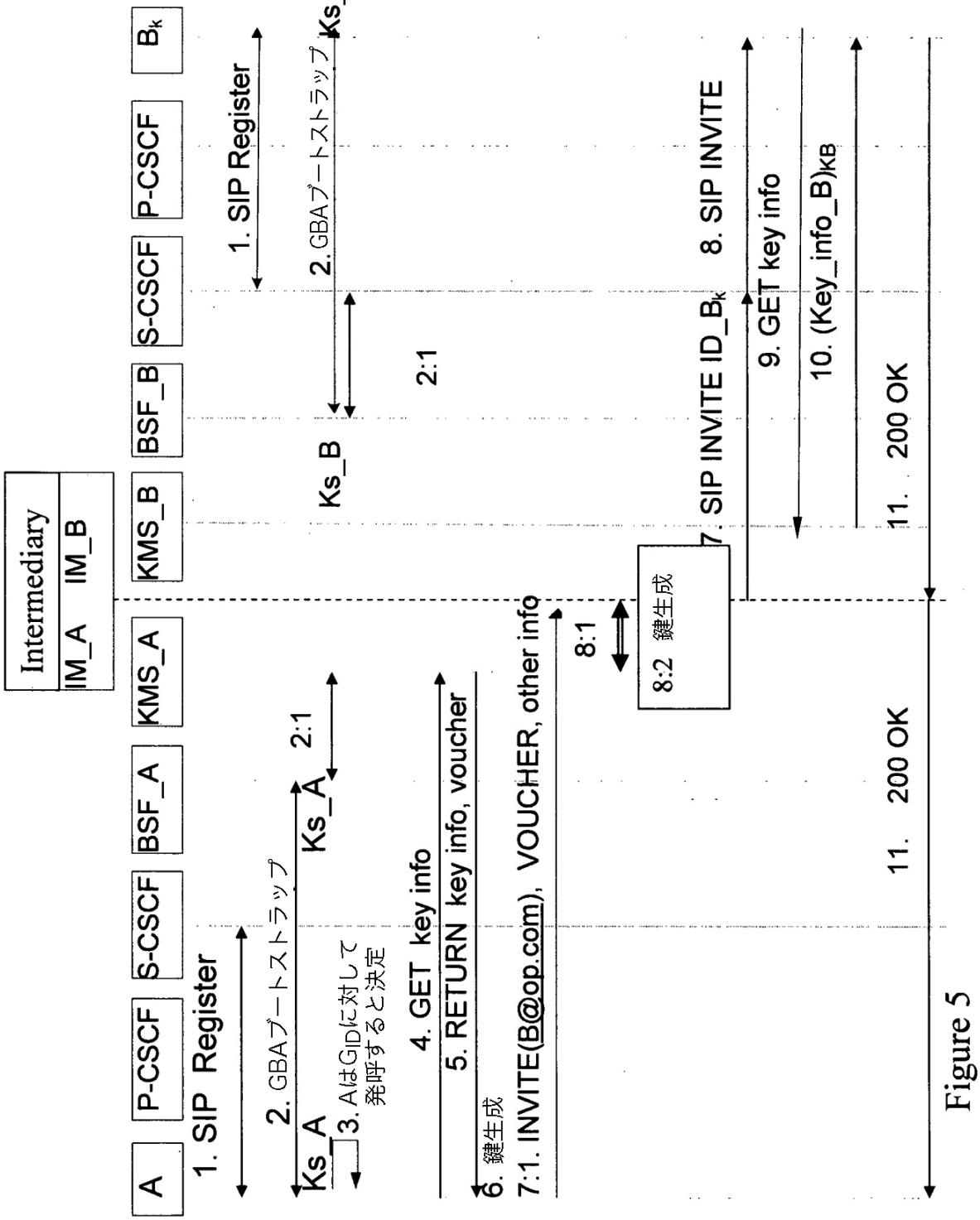
A
P-CSCF
S-CSCF
BSF_A
KMS_A
Intermediary
IM_A IM_B
KMS_B
BSF_B
S-CSCF
P-CSCF
Bk
1. SIP Register
2. GBAブートストラップ
Ks_A
3. AはGIDに対して発呼すると決定
2:1
4. GET key info
5. RETURN key info, voucher
6. 鍵生成
7:1. INVITE(B@op.com), VOUCHER, other info
8:1
8:2 鍵生成
1. SIP Register
2. GBAブートストラップ
Ks_B
Ks_B
2:1
7. SIP INVITE ID_Bk
8. SIP INVITE
9. GET key info
10. (Key_info_B)KB
11. 200 OK
11. 200 OK

Figure 5

フロントページの続き

(74)代理人 100134474
弁理士 坂田 恭弘
(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 チェン, イー
スウェーデン国 スンドビュベリ エス－１７２ ３７, ヘーガリドスヴェーゲン ９
(72)発明者 リンドホルム, フレドリク
スウェーデン国 エルブシェー エス－１２５ ７４, スタムガタン ８７
(72)発明者 マットソン, ジョン
スウェーデン国 テビィ エス－１８７ ７７, ガルムグレンド ５Ｂ
(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, ストップヴェーゲン ９５
(72)発明者 ノールマン, 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 青木 重徳

(56)参考文献 特開２００２－０５１０３６（ＪＰ，Ａ）
特表２００４－５１２７３４（ＪＰ，Ａ）
国際公開第２００７／０８５１７５（WO，Ａ１）
国際公開第２００７／０６２８８２（WO，Ａ１）
国際公開第２００６／１３４５０５（WO，Ａ１）
国際公開第２００３／０６３４１０（WO，Ａ１）
国際公開第２０１０／０９９８２３（WO，Ａ１）
米国特許出願公開第２００７／０１２１５８２（ＵＳ，Ａ１）
欧州特許出願公開第０１３６５６２０（ＥＰ，Ａ１）
岡本 栄司，“明るい情報化社会の実現をめざす暗号技術▲５▼ 暗号鍵配送管理”，ｂｉｔ，日本，共立出版株式会社，１９９１年１１月 １日，Ｖｏｌ．２３，Ｎｏ．１２，ｐ．５１－５９
満保 雅浩，岡本 栄司，“暗号最新事情７ セキュリティインフラストラクチャ Ｙａｋｓｈａ”，ｂｉｔ，日本，共立出版株式会社，１９９６年 ７月 １日，Ｖｏｌ．２８，Ｎｏ．７，ｐ．１０４－１１４

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／０８
Ｈ０４Ｌ ９／１４