(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4673364号
(P4673364)
(45)発行日　平成23年4月20日(2011.4.20)　(24)登録日　平成23年1月28日(2011.1.28)

(51)Int.Cl.　　F I
H04L 9/08 (2006.01)　　H04L 9/00 601B
G09C 1/00 (2006.01)　　G09C 1/00 640E

請求項の数 15　(全 9 頁)

(21)出願番号　特願2007-502442(P2007-502442)
(86)(22)出願日　平成17年4月28日(2005.4.28)
(65)公表番号　特表2007-528650(P2007-528650A)
(43)公表日　平成19年10月11日(2007.10.11)
(86)国際出願番号　PCT/IB2005/001704
(87)国際公開番号　WO2005/107214
(87)国際公開日　平成17年11月10日(2005.11.10)
審査請求日　平成18年9月11日(2006.9.11)
(31)優先権主張番号　0409704.4
(32)優先日　平成16年4月30日(2004.4.30)
(33)優先権主張国　英国(GB)

前置審査

(73)特許権者　398012616
ノキア　コーポレイション
フィンランド　エフイーエンー０２１５０
エスプー　ケイララーデンティエ　４
(74)代理人　100127188
弁理士　川守田　光紀
(72)発明者　ライティネン　ペッカ
フィンランド，ヘルシンキ　ＦＩＮ－００８００，ヒイトマエンティエ　４４　Ａ２

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】エンティティの第１のＩＤおよび第２のＩＤの検証方法

(57)【特許請求の範囲】
【請求項１】
ブートストラップサーバー機能部（BSF）の動作方法であって、
ネットワークアプリケーション機能部（NAF）から公開識別子を受信すること、ただし前記公開識別子は、前記ネットワークアプリケーション機能部が、ユーザ装置（UE）とのUaインターフェースを介する通信のために使用する識別子である、前記受信することと；
前記受信した公開識別子と、前記ネットワークアプリケーション機能部の内部識別子との間のマッピングを検証すること、ただし前記内部識別子は、前記ネットワークアプリケーション機能部が、前記ブートストラップサーバー機能部とのZnインターフェースを介する通信に使用する識別子である、前記検証することと；
を含む、方法。
【請求項２】
前記公開識別子と前記内部識別子との間のマッピングの検証が成功した場合、前記公開識別子を使用して、ネットワークアプリケーション機能部固有キー（NAF固有キー）を生成することを更に含む、請求項１に記載の方法。
【請求項３】
前記ネットワークアプリケーション機能部から、前記ユーザ装置と前記ネットワークアプリケーション機能部との間のサービスに関するユーザ識別子を受信すること；
前記ネットワークアプリケーション機能部から、前記ユーザ装置と前記ネットワークアプリケーション機能部との間のサービスに関するトランザクション識別子を受信すること

；
前記受信したユーザ識別子とトランザクション識別子との間のマッピングを検証すること；
をさらに含み、
前記ユーザ識別子及び前記トランザクション識別子は、前記ネットワークアプリケーション機能部が前記ユーザ装置から受信したものであり、
前記ユーザ識別子と前記トランザクション識別子との間のマッピングの検証が成功した場合に前記ネットワークアプリケーション機能部固有キーを生成する、請求項２に記載の方法。
【請求項４】
前記公開識別子と前記トランザクション識別子とを同じメッセージで受信することを含む、請求項３に記載の方法。
【請求項５】
前記ユーザ識別子と前記トランザクション識別子とを同じメッセージで受信することを含む、請求項４に記載の方法。
【請求項６】
前記NAF固有キーを前記ネットワークアプリケーション機能部に送信することを含む、請求項２から５のいずれかに記載の方法。
【請求項７】
ネットワークアプリケーション機能部（NAF）の動作方法であって、
公開識別子をブートストラップサーバー機能部（BSF）へ送信すること、ただし前記公開識別子は、前記ネットワークアプリケーション機能部が、ユーザ装置（UE）とのUaインターフェースを介する通信のために使用する識別子である、前記送信することと；
前記公開識別子を前記ブートストラップサーバー機能部へ送信することに応じて、前記ブートストラップサーバー機能部が前記公開識別子を使用して生成した、ネットワークアプリケーション機能部固有キー（NAF固有キー）を受信することと；
を含む、方法。
【請求項８】
ブートストラップサーバー機能部（BSF）を含む装置であって、
ネットワークアプリケーション機能部（NAF）から公開識別子を受信する手段、ただし前記公開識別子は、前記ネットワークアプリケーション機能部が、ユーザ装置（UE）とのUaインターフェースを介する通信のために使用する識別子である、前記受信する手段と；
前記受信した公開識別子と、前記ネットワークアプリケーション機能部の内部識別子との間のマッピングを検証する手段、ただし前記内部識別子は、前記ネットワークアプリケーション機能部が、前記ブートストラップサーバー機能部とのZnインターフェースを介する通信に使用する識別子である、前記検証する手段と；
を備える、装置。
【請求項９】
前記公開識別子と前記内部識別子との間のマッピングの検証が成功した場合、前記公開識別子を使用して、ネットワークアプリケーション機能部固有キー（NAF固有キー）を生成するように構成される、請求項８に記載の装置。
【請求項１０】
前記ネットワークアプリケーション機能部から、前記ユーザ装置と前記ネットワークアプリケーション機能部との間のサービスに関するユーザ識別子を受信し；
前記ネットワークアプリケーション機能部から、前記ユーザ装置と前記ネットワークアプリケーション機能部との間のサービスに関するトランザクション識別子を受信し；
前記受信したユーザ識別子とトランザクション識別子との間のマッピングを検証する；
ようにさらに構成され、ただし、
前記ユーザ識別子及び前記トランザクション識別子は、前記ネットワークアプリケーション機能部が前記ユーザ装置から受信したものであり、

前記ユーザ識別子と前記トランザクション識別子との間のマッピングの検証が成功した場合に前記ネットワークアプリケーション機能部固有キーを生成するように構成される、請求項９に記載の装置。

【請求項１１】

前記公開識別子と前記トランザクション識別子とを同じメッセージで受信するように構成される、請求項１０に記載の装置。

【請求項１２】

前記ユーザ識別子と前記トランザクション識別子とを同じメッセージで受信するように構成される、請求項１１に記載の装置。

【請求項１３】

前記NAF固有キーを前記ネットワークアプリケーション機能部に送信するように構成される、請求項８から１２のいずれかに記載の装置。

【請求項１４】

ネットワークアプリケーション機能部（NAF）を含む装置であって、

公開識別子をブートストラップサーバー機能部（BSF）へ送信する手段、ただし前記公開識別子は、前記ネットワークアプリケーション機能部が、ユーザ装置（UE）とのUaインターフェースを介する通信のために使用する識別子である、前記送信する手段を備え、

前記公開識別子を前記ブートストラップサーバー機能部へ送信することに応じて、前記ブートストラップサーバー機能部が前記公開識別子を使用して生成した、ネットワークアプリケーション機能部固有キー（NAF固有キー）を受信するように構成される、

装置。

【請求項１５】

請求項８から１３のいずれかに記載の装置と、請求項１４に記載の装置とを含む、システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ネットワークエンティティのIDの検証に関する。

【発明の背景】

【０００２】

完全にモバイルコンピューティングおよびネットワーキングに向かっている最近の動向は、種々のアクセス技術に進化をもたらしており、またこれによってユーザーは自身のホームネットワーク外にいる場合でもインターネットにアクセスすることができる。完全にユビキタスなワールドワイドウェブ（WWW）アクセスを提供する第1の公衆通信ネットワークはGSMベースの携帯電話ネットワークである。

【０００３】

これまで、インターネットの使用は個人対機械の通信、すなわち情報サービスが多くを占めてきた。いわゆる第3世代（Third Generation；3G）無線ネットワークへの進化はモバイルマルチメディア通信を伴うため、これによってIPベースサービスが公衆モバイルネットワークにおいて利用される方法も変化するであろう。第3世代移動体通信規格化プロジェクト（3rd Generation Partnership Project；3GPP）で規定されるように、IPマルチメディアサブシステム（IP Multimedia Subsystem；IMS）は、携帯音声通信をインターネット技術に統合し、IPベースのマルチメディアサービスをモバイルネットワークで利用可能にする。

【０００４】

発明者は、第3世代無線ネットワークにおける重要な問題、すなわち、いわゆる第3世代汎用認証アーキテクチャ（Generic Authentication Architecture；GAA）におけるIDコヒーレンス確認の問題を認識している。このことは、例えば技術仕様書TS33.220v6に記載されている。

【０００５】

マルチメディア対応の新しい携帯端末（マルチメディア電話）は、独立したアプリケーション開発者がマルチメディア環境用の新しいサービスおよびアプリケーションを設計できるようにするオープン開発プラットフォームを提供する。ユーザーは、新しいアプリケーションやサービスを自身の携帯端末へ次々にダウンロードし、そこでそれらを使用することができる。

【０００６】

GAAは、今後のアプリケーションおよびサービスのためのセキュリティ手続きとして使用されるものである。しかしながら、発明者はGAAにおける欠陥を認識している。

【０００７】

特に、GAAにおいては、ネットワークアプリケーション機能（Network Application Function；NAF）の公開識別子と、NAFのGAA内部識別子との間の結合を検証できるようにする、ブートストラッピングサーバー機能（BSF）の必要性がある。NAFの公開識別子は、Uaインターフェースにおいてユーザー装置（UE）が使用するNAFの公開ホスト名である。内部NAF識別子は、Znインターフェース内の対応するDIAMETERメッセージにおいて使用されるネットワークアドレスである。公開NAF識別子は、ブートストラッピングサーバー機能がNAF固有キー（Ks_NAF）の導出中に使用するため、ブートストラッピング機能において必要である。

【０００８】

この問題は、NAFが仮想名ベースのホスティングをしている場合、すなわち単一のIP（インターネットプロトコル）アドレスにマップされた複数のホスト名を有する場合にはさらに顕著である。したがって、内部NAFアドレスと公開NAFアドレスとの間に一対多のマッピングが存在する場合がある。ドメインネームサーバーは、ブートストラッピングサーバーにおいて或る内部NAFアドレスによって識別される或るNAFアドレスが、或る公開NAFアドレスを使用する権限を与えられていることを検証することができない。

【０００９】

本発明の実施形態は、上述の問題に取り組もうとするものである。

【発明の概要】

【００１０】

本発明の実施形態によれば、エンティティの第1のIDおよび第2のIDの検証方法であって、確認エンティティにおいて第1のID情報を受信するステップと、第2のID情報を前記エンティティから前記確認エンティティへ送信するステップと、前記第1および第2のIDがいずれも前記エンティティに属することを検証するステップと、前記第1および第2のID情報のいずれか1つを使用してキーを生成するステップとを含む方法を提供する。

【００１１】

本発明の別の実施形態によれば、ネットワークアプリケーション機能の外部インターフェースアドレスおよび内部インターフェースアドレスの検証方法であって、ブートストラッピング機能において前記内部インターフェースアドレスをユーザー装置から受信するステップと、前記ブートストラッピング機能において前記外部インターフェースアドレスを前記ネットワークアプリケーション機能から受信するステップと、前記外部インターフェースアドレスおよび前記内部インターフェースアドレスが、同一のネットワークアプリケーション機能に属することを検証するステップとを含む方法を提供する。

【００１２】

本発明の別の実施形態によれば、確認エンティティにおいてエンティティの第1のIDを受信するように構成された確認エンティティを含むシステムであって、前記エンティティは前記エンティティの第2のIDを前記エンティティから前記確認エンティティに送信するように構成され、前記確認エンティティは前記第1および第2のIDがいずれも前記エンティティに属することを検証し、前記第1および第2のIDのいずれか1つからキーを生成するように構成されたシステムを提供する。

【００１３】

本発明の別の実施形態によれば、エンティティの第1のIDおよび前記エンティティの第2

のIDを受信するように構成された確認エンティティであって、前記エンティティの第2のIDは前記エンティティから受信され、前記確認エンティティは前記第1および第2のIDがいずれも前記エンティティに属することを検証し、前記第1および第2のIDのいずれか1つからキーを生成するように構成された確認エンティティを提供する。

【００１４】

本発明の実施形態によれば、第1および第2のIDを含むエンティティであって、前記第2のIDを確認エンティティに送信するように、また前記第2のIDから生成されたキーを前記確認エンティティから受信するように構成されたエンティティを提供する。

【発明の好適な実施形態の詳細な説明】

【００１５】

本発明およびそれがどのように実行に移されるかについてより理解を深めるため、例として添付図面を参照する。

【００１６】

本発明の実施形態を組み込むことが可能なGAAアーキテクチャを示す、図1を参照する。

【００１７】

ユーザー装置UE20が用意される。ユーザー装置は、適合するいかなる形態をとってもよく、例えば、携帯電話、電子手帳、コンピュータ、またはその他適合するいかなる装置であってもよい。ユーザー装置20は、Ubインターフェースを経てブートストラッピングサーバー機能BSF28と通信するように構成される。ユーザー装置20は、Uaインターフェースを経てネットワークアプリケーション機能（NAF）29と通信するためにも構成される。

【００１８】

ネットワークアプリケーション機能29は、許可プロキシ機能25とアプリケーション固有のサーバー26とに分けられる。ネットワークアプリケーション機能29は、Znインターフェースを経てブートストラッピングサーバー機能28に接続される。

【００１９】

ブートストラッピングサーバー機能28は、Zhインターフェースを経て加入者データ管理システム（Home Subscriber System）HSS27に接続される。ブートストラッピングサーバー機能およびユーザー装置はAKA（Authentication and Key Agreement；認証とキー合致）プロトコルを使用して手動で認証し、後にユーザー装置とネットワークアプリケーション機能との間に適用されるセッションキーに合致するように構成されている。ブートストラッピング処理が完了すると、ユーザー装置およびNAFは、いくつかのアプリケーション固有のプロトコルを起動することができる。これらのプロトコルの中では、Ubインターフェースを使用してユーザー装置とブートストラッピングサーバー機能との間の相互認証中に生成されたセッションキーに基づいて、メッセージの認証が行われる。概して、ユーザー装置とNAFとの間に先行するセキュリティアソシエーションはない。NAFは、加入者のブートストラッピングサーバー機能の位置を同定し、これとセキュアに通信できなくてはならない。NAFは、共有キー材料、またはブートストラッピング処理中にUbインターフェースを介してユーザー装置とBSFとの間に確立された、この共有キー材料から導かれたNAF固有のキー材料を取得しなくてはならない。NAFは、共有キーの材料の寿命を確認するように構成される。

【００２０】

HSSは、その通常機能に加えて、ブートストラッピングサーバー機能に関連する加入者プロファイルにパラメータを保存する。場合によっては、いくつかのNAFの使用に関連するパラメータがHSSに保存される。

【００２１】

インターフェースについてさらに詳細に説明する。Uaインターフェースは、Ubインターフェースを経たHTTPダイジェストAKAの起動の結果として、キー材料またはユーザー装置と基地局機能との間の合致を使用して保護されているアプリケーションプロトコルを搬送する。

【００２２】

Ubインターフェースは、ユーザー装置とブートストラッピングサーバー機能との間の相互認証を提供する。これにより、ユーザー装置は3GPP AKAインフラストラクチャに準拠したセッションキーをブートストラッピングすることができる。

【００２３】

BSFとHSSとの間で使用されるZhインターフェースプロトコルは、BSFが要求された認証情報および加入者プロファイル情報をHSSからフェッチできるようにする。3G認証センターへのインターフェースは、HSS内部にある。

【００２４】

Znインターフェースは、キー材料、または、Ubインターフェース上で走る以前のHTTPダイジェストAKAプロトコルの中で導かれたキー材料をBSFからフェッチするために、NAFによって使用される。NAF固有の加入者プロファイル情報をBSFからフェッチするためにも使用される。

【００２５】

要約すると、本発明の実施形態において、NAF29は、NAFの公開識別子をブートストラッピングサーバー機能28に送信する。ブートストラッピングサーバー機能は、公開識別子と内部NAF識別子と間の結合を検証しなければならない。公開NAF識別子は、Ubインターフェースにおけるブートストラッピング処理中に確立される、マスターキー材料（Ks）からNAF固有キー（Ks_NAF）を得るために、BSFによって使用される。

【００２６】

特に、本発明の実施形態は、NAFをホスティングしているネットワーク要素が、ユーザー装置からの次の接続のために供される1つ以上のネットワークインターフェースを有する場合にも適用可能である。これは、公開（または外部）ネットワークインターフェースであり、Uaインターフェースを経る。1つのネットワークインターフェースは、BSFなどのオペレータサービスと接続するためのものであり、これはNAF29とBSF28との間のZnインターフェースを経由する内部ネットワークインターフェースである。

【００２７】

Znインターフェースにおける内部ネットワークインターフェースのアドレスは、例えば、NAFによって、DIAMETERメッセージ内の「起点ホスト」（origin host）フィールドに追加される。本発明の実施形態は、NAFの外部ネットワークインターフェースアドレス、すなわち公開アドレスを、NAFからBSFへ伝達する。これは、情報をNAF29からBSFへトランスポートするために、AVP （Attribute Value Pair；属性値ペア）を使用して行うことができる。前述したように、外部または公開アドレスはBSFによって使用されるが、これは、BSFが、ユーザー装置が使用するNAFの完全修飾ドメイン名（Fully Qualified Domain Name；FQDN）すなわちNAFの公開アドレスから、NAF固有キー（Ks_NAF）を得るためである。BSFは、Znインターフェースにおいて使用される内部アドレス（NAF_id_Zn）によって識別されたNAFが、Uaインターフェースにおいて使用されている外部アドレス（NAF_id_Ua）を使用する権限を与えられていることを確認する。

【００２８】

本発明の実施形態において、NAFは第1のメッセージにおいてNAF_Id_Uaを送信し、応答として確認（またはエラー）メッセージを受信する。UIDは同時に転送されてもされなくてもよい。対応する応答はしたがって公開および内部NAF識別子のマッピングに関するもののみである。本発明の実施形態では、公開および内部NAF識別子はいずれもBSFへ送信され、BSFはそれらの間のマッピングを確認し、公開NAF識別子を使用してNAF固有キーを得る。

【００２９】

次に、本発明の第1の信号フローを示す図2を参照する。図2は、Znインターフェースを経るNAF29とBSF28との間のメッセージングの詳細を示す。Znインターフェースメッセージングが行われる前に、ユーザー装置はUaインターフェースを介してNAFへサービスを要求する。この要求によって、ユーザー装置は、TID（Transaction Identifier；トランザクション識別子）および場合によってはユーザー識別子（User Identifier；UID）を与えら

れる。ユーザー識別子は、後のメッセージ内においてユーザー装置からNAFへトランスポートされ得る。図2は、TIDおよびUIDが同一のメッセージでユーザー装置からNAFへ送信された場合を説明するものである。

【００３０】

ステップ1aにおいて、NAF29は、TIDやNAF_id_UA、UIDをBSF28へ送信する。BSFはUIDに対するTIDのマッピング、およびNAF_id_Uaに対するNAF_id_Znのマッピングを検証する。NAF_id_Uaは、例えば起点ホストAVPから得ることができる。換言すれば、BFSは、内部アドレスによって識別されたNAFが外部アドレスを使用する権限を与えられていることを確認する。これらの検証が成功すると、BSFはNAF_id_UAを使用してKs_NAFを得る。

【００３１】

ステップ2aにおいて、BSFは、Ks_NAFおよびNAF固有ユーザーセキュリティ設定「USS」をNAF29に送信する。本発明の一部の実施形態において、NAFはいかなるUSSも有することができず、したがってUSS AVPは任意的である。Ks_NAFを受信した後、NAFは認証手順を完了し、UIDが正しいと推測することができる。TIDが見つからず、TID対UIDまたはNAF_iD_UAの検証が失敗した場合、BSFはNAFにエラーメッセージを返さなくてはならない。

【００３２】

NAFが複数のTID対UIDマッピングを検証する権限を与えられている場合、NAFはステップ3aにおいてTIDおよび別のUIDを含む追加的な要求をBSFへ送信することができる。TIDおよびUIDを受信すると、BSF28はTID対UIDマッピングを検証し、結果をNAF29へ返さなくてはならない。これはステップ4aにおいて行われる。BSFがこれを行わなくてはならないのは、NAFが複数のTID対UIDマッピングを検証する権限を与えられている場合のみである。この場合、NAFはステップ3aおよび4aを複数回繰り返してもよい。

【００３３】

TIDおよびUIDが異なるメッセージ内において受信された場合を示す図3を参照する。例えば、TIDはUIDのためにNAFへ送信される。

【００３４】

ステップ1bにおいて、NAF29はTIDおよびNAF_ID_UaをBSFへ送信する。BSFは、NAF_id_ZnのNAF_id_Uaに対するマッピングを検証しなくてはならない。検証が成功すると、BSFはNAF_id_Uaを使用してKs_NAFを得る。

【００３５】

ステップ2bにおいて、BSFはKs_NAFおよびNAF固有のUSSをNAFへ送信する。ここでも、NAFはUSSを有していないかもしれず、したがってUSS AVPは任意的である。Ks_NAFを受信した後、NAF29は認証手順を完了することができる。TIDが見つからず、NAF_iD_Uaの検証が失敗した場合、BSF28はNAFにエラーメッセージを返さなくてはならない。

【００３６】

ステップ3bの前に、NAFはユーザー装置からUIDを受信している。ステップ3bにおいて、NAFは検証のためにTIDおよびUIDを送信する。BSFは、ステップ4bにおいてこの検証結果を提供する。この手順は図2のメッセージ3aおよび4aにおけるものと同一である。この場合、NAFは別のメッセージにおいてTID対UIDマッピングを検証することが可能である。ステップ1bおよび2bの間はUIDの検証は行われない。NAFがTID対UIDマッピングを検証する権限を与えられている場合、NAFはステップ5bにおいて別の要求を送信し、ステップ6bにおいて検証結果を得ることができる。これらのステップは、図2のステップ4aおよび4bに相当する。ステップ5bおよび6bは、複数回繰り返してもよい。BSFデータベース内にTIDが見つからない場合やNAF_id_UaおよびNAF_id_Znのマッピングが検証できなかった場合、またはTIDおよびUIDのマッピングが検証できなかった場合、BSFからNAFへエラーメッセージが送信される。

【００３７】

このように、本発明の実施形態によれば、ユーザー装置がＵａインターフェースにおいて使用するＮＡＦ識別子を、ＮＡＦがＢＳＦへ送信することが可能となる。それによってＢＳＦは、Ks_NAFを得ることができる。

【図面の簡単な説明】

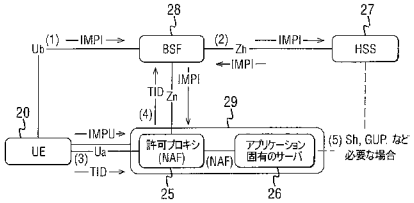
【００３８】

【図１】図１はＧＡＡアプリケーションの概観を示す。

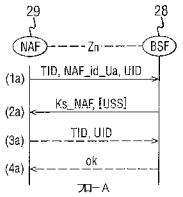
【図２】図２は本発明の一実施形態における第１の信号フローを示す。

【図３】本発明の別の実施形態における第２の信号フローを示す。

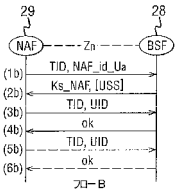
【図１】



【図２】



【図３】



フロントページの続き

(56)参考文献 特開平０３－０７３６３３（ＪＰ，Ａ）
国際公開第２００５／０７４１８８（WO，Ａ１）
欧州特許出願公開第０１３６５６２０（ＥＰ，Ａ１）
Nokia, “NAF-BSF (D interface) Protocol”, 3GPP TSG SA WG3 Security-S3#27, [online], ２００３年 2月２５日, S03-030072, [検索日：平成２２年１０月８日]、インターネット，ＵＲＬ, http://www.3gpp.org/ftp/tsg_sa/wg3_security/TSGS3_27_Sophia_Antipolis/Docs/PDF/S3-030072.pdf
3GPP TSG SA WG3 Security - S3#31, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Feneric Bootstrapping Architecture (Release 6)”, 3GPP TS 33.220, [online], ２００３年１１月, V0.1.1(2003-10), [retrieved on 2011-01-07].Retrieved from the Internet, ＵＲＬ, http://www.3gpp.com/ftp/tsg_sa/WG3_Security/TSGS3_31_Munich/Docs/PDF/S3-030662.pdf

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/08
G09C 1/00