【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成25年6月20日(2013.6.20)

【公表番号】特表2012-526454(P2012-526454A)
【公表日】平成24年10月25日(2012.10.25)
【年通号数】公開・登録公報2012-044
【出願番号】特願2012-509876(P2012-509876)
【国際特許分類】
Ｈ０４Ｗ　12/08　(2009.01)
Ｈ０４Ｗ　36/14　(2009.01)
Ｈ０４Ｗ　12/06　(2009.01)
【ＦＩ】
Ｈ０４Ｑ　7/00　１８４
Ｈ０４Ｑ　7/00　３０９
Ｈ０４Ｑ　7/00　１８３

【手続補正書】
【提出日】平成25年4月30日(2013.4.30)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
複数のメディア独立ハンドオーバサービスにセキュリティを提供するプロトコルを実装したコンピュータを有する装置であって、
複数のサービングアクセスネットワークから複数の候補ネットワークへの複数のモバイル装置のハンドオーバに先立って前記複数の候補アクセスネットワークを認証する独立したオーセンティケータを含むサービスポイントであって、前記複数のメディア独立ハンドオーバサービスを提供するサービスポイントと、
認証サーバを介して前記複数のメディア独立ハンドオーバサービスを提供する前記サービスポイントを有するアクセス認証を介してアクセス制御を適用するアクセスコントローラと、を具備し、
前記複数のサービングアクセスネットワークおよび前記複数の候補アクセスネットワークは特定のサービングメディアを有する複数の異種アクセスネットワークに属していて、前記アクセス認証が前記サービスポイントと前記認証サーバとの間で確立される場合、前記モバイル装置が前記複数のメディア独立ハンドオーバサービスに、異種メディア間でアタッチされる前記複数のモバイル装置に関する前記サービスポイントを介してアクセスする権限を与えられる装置。
【請求項２】
前記アクセス認証は、
複数のモバイル装置と前記認証サーバとの間で複数のキーを確立するキー確立プロトコルを含み、
少なくとも１つのキーは、前記サービスポイントと前記複数のモバイル装置との間で送信される複数のメディア独立ハンドオーバメッセージを保護するためにセッションキーを導き出す前記サービスポイントへ配送される請求項１の装置。
【請求項３】
メディア独立ハンドオーバプロトコル上で、前記サービスポイントと前記複数のモバイ

ル装置との間でトランスポートレイヤセキュリティ（ＴＬＳ、transport layer security）ハンドシェイクを行うために使用される、前記アクセス認証および前記キー確立プロトコルのためのトランスポートレイヤセキュリティを具備し、
前記ＴＬＳハンドシェイクは、前記メディア独立ハンドオーバプロトコルの複数のメッセージを保護するために、複数のピア（複数のモバイル装置および前記サービスポイント）間でのセキュリティアソシエーションまたはセキュアセッションを確立する請求項２の装置。
【請求項４】
前記セキュリティアソシエーションまたはセキュアセッションは、前記メディア独立ハンドオーバプロトコル内での複数のピア（モバイル装置およびサービスポイント）に結びつけられ、トランスポートレベルセキュリティが付加される場合には前記複数のメディア独立ハンドオーバメッセージはカプセル化されない請求項３の装置。
【請求項５】
前記複数のメディア独立ハンドオーバサービスは、前記複数のモバイル装置および、同じ前記認証サーバを有する複数の候補アクセスネットワークおよび前記複数のサービングアクセスネットワークを認証する請求項１の装置。
【請求項６】
メディア独立ハンドオーバキーイング材料は、ネットワークアクセスに関するプロアクティブ認証の間に確立されるキーイング材料からブートストラップされ、前記プロアクティブ認証は、前記複数のサービングアクセスネットワークから前記複数の候補アクセスネットワークへの前記複数のモバイル装置のハンドオーバに関する前記ネットワークアクセスに先立って、前記複数の候補アクセスネットワークを認証することを具備する請求項５の装置。
【請求項７】
前記複数のメディア独立ハンドオーバサービスは、前記複数のモバイル装置および、異なる複数の認証サーバを有する複数の候補アクセスネットワークおよび前記複数のサービングアクセスネットワークを認証する請求項１の装置。
【請求項８】
メディア独立ハンドオーバキーイング材料は、前記複数のメディア独立ハンドオーバサービスに関するプロアクティブ認証の間に確立されるキーイング材料からブートストラップされ、前記プロアクティブ認証は、前記複数のサービングアクセスネットワークから前記複数の候補アクセスネットワークへの前記複数のモバイル装置のハンドオーバに先立って、前記複数の候補アクセスネットワークを認証することを具備する請求項７の装置。
【請求項９】
前記認証サーバは拡張認証プロトコル（ＥＡＰ）サーバである請求項１の装置。
【請求項１０】
前記認証サーバは認証、承認およびアカウンティング（ＡＡＡ）サーバである請求項１の装置。
【請求項１１】
前記独立オーセンティケータは、前記複数の異種のアクセスネットワークのぞれぞれの間で双方向通信を管理するための単一のサービスポイントである請求項１の装置。
【請求項１２】
複数のメディア独立ハンドオーバサービスにセキュリティを提供するプロトコルを実装したコンピュータを有する装置であって、
複数のサービングアクセスネットワークから複数の候補ネットワークへの複数のモバイル装置のハンドオーバに先立って前記複数の候補アクセスネットワークを認証する独立したオーセンティケータを含むサービスポイントであって、前記複数のメディア独立ハンドオーバサービスを提供するサービスポイントを具備し、
前記サービスポイントおよび前記複数のモバイル装置は、相互認証およびキー確立を行う装置。

【請求項１３】
前記複数のモバイル装置および前記サービスポイントは、前記複数のモバイル装置の同一性を、ネットワークに属している前記サービスポイントに確実に提供する（または逆の場合も同様）ために、複数の特定のキーの前記キー確立および前記相互認証を行い、
前記複数の特定のキーは、複数のメディア独立ハンドオーバメッセージを保護するために、１対の同一性を結びつける請求項１２の装置。
【請求項１４】
メディア独立ハンドオーバプロトコル上で、前記サービスポイントと前記複数のモバイル装置との間でトランスポートレイヤセキュリティ（ＴＬＳ、transport layer security）ハンドシェイクを行うために使用される、前記相互認証および前記キー確立のためのトランスポートレイヤセキュリティを具備し、
前記ＴＬＳハンドシェイクは、前記メディア独立ハンドオーバプロトコルの複数のメッセージを保護するために、複数のピアモバイル装置間でのセキュリティアソシエーションまたはセキュアセッションを確立する請求項１３の装置。
【請求項１５】
前記セキュリティアソシエーションまたはセキュアセッションは、前記メディア独立ハンドオーバプロトコル内での複数のピア（モバイル装置およびサービスポイント）に結びつけられ、トランスポートレベルセキュリティが付加される場合には前記複数のメディア独立ハンドオーバメッセージはカプセル化されない請求項１４の装置。
【請求項１６】
前記相互認証は、予め共有されるキーまたは信頼される第三者機関に基づいてもよい請求項１３の装置。
【請求項１７】
前記信頼される第三者機関は証明機関である請求項１６の装置。
【請求項１８】
複数のメディア独立ハンドオーバサービスにセキュリティを提供するシステムであって、
複数のメディア独立アクセス機能を有するサービスポイントと、
それぞれ複数のメディア特定アクセス機能を有する複数の異種ネットワークと、
前記複数の異種ネットワークに接続される複数のモバイル装置と、
認証サーバと、
前記複数のメディア独立ハンドオーバサービスを前記認証サーバを介して提供する前記サービスポイントを有するアクセス認証を介してアクセス制御を適用するアクセスコントローラと、を具備し、
前記複数の異種ネットワークは複数のサービングアクセスネットワークと複数の候補アクセスネットワークとを含み、
前記サービスポイントは、前記サービングアクセスネットワークから前記候補アクセスネットワークへの前記複数のモバイル装置のハンドオーバに先立って、前記候補アクセスネットワークを認証し、
前記サービスポイントと前記認証サーバとの間で前記アクセス認証が確立される場合に、前記複数のモバイル装置は、異種メディア間でアタッチされた前記複数のモバイル装置に関する前記サービスポイントを介して、前記複数のメディア独立ハンドオーバサービスにアクセスするシステム。
【請求項１９】
前記アクセス認証は、
複数のモバイル装置と前記認証サーバとの間で複数のキーを確立するキー確立プロトコルを含み、
少なくとも１つのキーは、前記サービスポイントと前記複数のモバイル装置との間で送信される複数のメディア独立ハンドオーバメッセージを保護するためにセッションキーを導き出す前記サービスポイントへ配送される請求項１８のシステム。

【請求項２０】
メディア独立ハンドオーバプロトコル上で、前記サービスポイントと前記複数のモバイル装置との間でトランスポートレイヤセキュリティ（ＴＬＳ、transport layer security）ハンドシェイクを行うために使用される、前記アクセス認証および前記キー確立プロトコルのためのトランスポートレイヤセキュリティを具備し、
前記ＴＬＳハンドシェイクは、前記メディア独立ハンドオーバプロトコルの複数のメッセージを保護するために、複数のピア（モバイル装置およびサービスポイント）間でのセキュリティアソシエーションまたはセキュアセッションを確立する請求項１９のシステム。
【請求項２１】
前記セキュリティアソシエーションまたはセキュアセッションは、前記メディア独立ハンドオーバプロトコル内での複数のピアに結びつけられ、トランスポートレベルセキュリティが付加される場合には前記複数のメディア独立ハンドオーバメッセージはカプセル化されない請求項２０のシステム。
【請求項２２】
前記複数のメディア独立ハンドオーバサービスは、前記複数のモバイル装置および、同じ前記認証サーバを有する複数の候補アクセスネットワークおよび前記複数のサービングアクセスネットワークを認証する請求項１８のシステム。
【請求項２３】
メディア独立ハンドオーバキーイング材料は、ネットワークアクセスに関するプロアクティブ認証の間に確立されるキーイング材料からブートストラップされ、前記プロアクティブ認証は、前記複数のサービングアクセスネットワークから前記複数の候補アクセスネットワークへの前記複数のモバイル装置のハンドオーバに関する前記ネットワークアクセスに先立って、前記複数の候補アクセスネットワークを認証することを具備する請求項２２のシステム。
【請求項２４】
前記複数のメディア独立ハンドオーバサービスは、前記複数のモバイル装置および、異なる複数の認証サーバを有する複数の候補アクセスネットワークおよび前記複数のサービングアクセスネットワークを認証する請求項１８のシステム。
【請求項２５】
メディア独立ハンドオーバキーイング材料は、前記複数のメディア独立ハンドオーバサービスに関するプロアクティブ認証の間に確立されるキーイング材料からブートストラップされ、前記プロアクティブ認証は、前記複数のサービングアクセスネットワークから前記複数の候補アクセスネットワークへの前記複数のモバイル装置のハンドオーバに先立って、前記複数の候補アクセスネットワークを認証することを具備する請求項２４のシステム。
【請求項２６】
複数のメディア独立ハンドオーバサービスにセキュリティを提供するシステムであって、
複数のメディア独立アクセス機能を有するサービスポイントと、
それぞれ複数のメディア特定アクセス機能を有する複数の異種ネットワークと、
前記複数の異種ネットワークに接続される複数のモバイル装置と、を具備し、
前記サービスポイントおよび前記複数のモバイル装置は相互認証およびキー確立を行うシステム。
【請求項２７】
前記複数のモバイル装置および前記サービスポイントは、前記複数のモバイル装置の同一性を、ネットワークに属している前記サービスポイントに確実に提供する（または逆の場合も同様）ために、複数の特定のキーの前記キー確立および前記相互認証を行い、
前記複数の特定のキーは、複数のメディア独立ハンドオーバメッセージを保護するために、１対の同一性を結びつける請求項２６のシステム。

【請求項２８】
メディア独立ハンドオーバプロトコル上で、前記サービスポイントと前記複数のモバイル装置との間でトランスポートレイヤセキュリティ（ＴＬＳ、transport layer security）ハンドシェイクを行うために使用される、前記相互認証および前記キー確立のためのトランスポートレイヤセキュリティを具備し、
前記ＴＬＳハンドシェイクは、前記メディア独立ハンドオーバプロトコルの複数のメッセージを保護するために、複数のピア（モバイル装置およびサービスポイント）間でのセキュリティアソシエーションまたはセキュアセッションを確立する請求項２７のシステム。
【請求項２９】
前記相互認証は、予め共有されるキーまたは信頼される第三者機関に基づいてもよく、前記信頼される第三者機関は証明機関である請求項２７のシステム。
【請求項３０】
複数のメディア独立ハンドオーバサービスにセキュリティを提供するための操作を、プロセッサが実行することが可能なエンコードされた複数の命令を有する、機械がアクセス可能な媒体を具備する製品であって、
前記命令は、
独立したオーセンティケータを含む前記複数のメディア独立ハンドオーバサービスを提供すること、
前記複数のメディア独立ハンドオーバサービスを認証サーバを介して提供するサービスポイントを有するアクセス認証を介してアクセス制御を適用すること、
前記複数のモバイル装置が、異種メディア間にアタッチされる前記複数のモバイル装置に関するサービスポイントを介して前記複数のメディア独立ハンドオーバサービスにアクセスする権限が与えられるように、前記サービスポイントと前記認証サーバとの間で前記アクセス認証を確立することを具備し、
前記独立したオーセンティケータは、複数のサービングアクセスネットワークから前記複数の候補アクセスネットワークへの前記複数のモバイル装置のハンドオーバに先立って、複数の候補アクセスネットワークを認証し、
前記複数のサービングアクセスネットワークおよび前記複数の候補アクセスネットワークのそれぞれは特定のサービングメディアを有する複数の異種アクセスネットワークに属する製品。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００３８
【補正方法】変更
【補正の内容】
【００３８】
ＭＩＨ ＰｏＳのロケーションまたはノードは規格によって固定されない。ＰｏＳのロケーションは、オペレータ配備シナリオおよび技術が特殊なＭＩＨアーキテクチャに基づいて、によって変化してもよい。ＭＩＨ ＰｏＳは、アクセスネットワーク（アクセスネットワーク１，２，４が典型）でのアタッチメントポイント（ＰｏＡ）の隣に存在するか、または同じ場所に配置される。その代わりに、ＰｏＳは、アクセスあるいはコアネットワーク（アクセスネットワーク３が典型）の内部により深く存在してもよい。図４に示されるように、ＭＮでのＭＩＨエンティティは、任意のアクセスネットワーク上のＲ１、Ｒ２あるいはＲ３のいずれかによってＭＩＨネットワークエンティティと通信する。サービングアクセスネットワークでのＰｏＡが同じ場所を共用したＭＩＨ機能がある場合、Ｒ１参照接続は、さらにＰｏＳであるＰｏＡで終了する（モデルのアクセスネットワーク１、２、４へのＭＮはすべて、Ｒ１でありえる）。その場合、Ｒ３参照接続は、（さらにアクセスネットワーク１、２、４へのＭＮによって例証された）どんな非ＰｏＡでも終了するだろう。ＭＩＨイベントは活発なＲ１リンクの両側で起こるかもしれない。ＭＮは典型的

にこれらのイベントに反応する最初のノードである。