

(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2017-502624

(P2017-502624A)

(43) 公表日 平成29年1月19日(2017.1.19)

(51) Int.Cl.	F I	テーマコード (参考)
H04M 11/00 (2006.01)	H04M 11/00 302	5K201
G06F 21/33 (2013.01)	G06F 21/33	

審査請求 有 予備審査請求 未請求 (全 29 頁)

(21) 出願番号	特願2016-557360 (P2016-557360)	(71) 出願人	000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(86) (22) 出願日	平成26年12月18日(2014.12.18)	(74) 代理人	100103894 弁理士 冢入 健
(85) 翻訳文提出日	平成28年6月7日(2016.6.7)	(72) 発明者	クンツ アンドレアス ドイツ連邦共和国、69115 ハイデル ベルク、クアフェアステンアンラゲ 3 6、エヌイーシー ヨーロッパ リミテッ ド内
(86) 国際出願番号	PCT/JP2014/006334	(72) 発明者	ジャン シャオウエイ 東京都港区芝五丁目7番1号 日本電気株 式会社内
(87) 国際公開番号	W02015/093058		
(87) 国際公開日	平成27年6月25日(2015.6.25)		
(31) 優先権主張番号	特願2013-262170 (P2013-262170)		
(32) 優先日	平成25年12月19日(2013.12.19)		
(33) 優先権主張国	日本国(JP)		
(31) 優先権主張番号	特願2014-2633 (P2014-2633)		
(32) 優先日	平成26年1月9日(2014.1.9)		
(33) 優先権主張国	日本国(JP)		

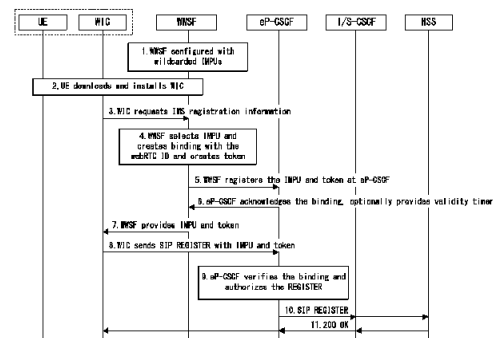
最終頁に続く

(54) 【発明の名称】 webRTCのための装置、システム、及び方法

(57) 【要約】

webRTC IMSクライアントの認証及び認可が、モバイルネットワークオペレータのIMSにおいてどのように達成することができるかについてのソリューションを提供する。WIC(20)は、IMSに登録するために、IMPU、IMPI、GRUU等であり得るIDを使用する。WIC(20)は、WWSF(30)によってeP-CSCF(40)アドレス及び認証情報を用いて事前設定され得るが、そうでない場合、この情報は、直接IMSから又はWWSF(30)を介して、又は例えばOMA DMである他のデバイス管理手順を介して、検索されるべきである。加入者が、既に有効なwebRTCアカウント又はメンバーシップを有すること、及びこれがWWSF(30)によって、有効にされ、認証され、及び認可され得ることがさらに想定される。

【選択図】図13



【特許請求の範囲】

【請求項 1】

通信システムにおける認証方法であって、

IMS (IP (Internet Protocol) Multimedia Subsystem) 登録において WWSF (WebRTC (Web Real Time Communication) Web Server Function) から UE (User Equipment) へトークンを送信することと、

前記トークンを伴う REGISTER メッセージを前記 UE から eP-CSCF (enhanced Proxy-CSCF (Call Session Control Function)) へ送信することと、

前記 eP-CSCF によって前記トークンを検証することと、

前記 REGISTER メッセージを前記 eP-CSCF から S-CSCF (Serving-CSCF) へ転送することと、

加入者プロファイルを HSS (Home Subscriber Server) から前記 S-CSCF へ受信することと、

200 OK メッセージを前記 S-CSCF から前記 eP-CSCF を介して前記 UE へ送信することと、を含む

認証方法。

【請求項 2】

前記認証方法の開始にあたって、前記 UE によって前記 IMS 登録のための情報を前記 WWSF に要求することをさらに含む、請求項 1 に記載の認証方法。

【請求項 3】

前記 WWSF によって前記トークンを認可ノードに要求することをさらに含む、請求項 1 又は 2 に記載の認証方法。

【請求項 4】

前記 WWSF は、前記トークンと共に IMPU (IMS public user identity) を前記 UE へ送信し、

前記 UE は、前記 IMPU 及び前記トークンを伴う前記 REGISTER メッセージを前記 eP-CSCF へ送信し、

前記 eP-CSCF は、前記トークンと共に前記 IMPU を検証する、

請求項 1 ～ 3 のいずれか 1 項に記載の認証方法。

【請求項 5】

前記 UE は、WIC (WebRTC IMS Client) である、請求項 1 ～ 4 のいずれか 1 項に記載の認証方法。

【請求項 6】

UE (User Equipment) を認証する通信システムであって、

WWSF (WebRTC (Web Real Time Communication) Web Server Function) と、eP-CSCF (enhanced Proxy-CSCF (Call Session Control Function)) と、S-CSCF (Serving-CSCF) と、HSS (Home Subscriber Server) と、を備え、

前記 WWSF は、IMS (IP (Internet Protocol) Multimedia Subsystem) 登録においてトークンを前記 UE へ送信し、

前記 UE は、前記トークンを伴う REGISTER メッセージを前記 eP-CSCF へ送信し、

前記 eP-CSCF は、前記トークンを検証し、

前記 eP-CSCF は、前記 REGISTER メッセージを前記 S-CSCF へ転送し、

、

前記 S-CSCF は、加入者プロファイルを前記 HSS から受信し、

前記 S-CSCF は、200 OK メッセージを前記 eP-CSCF を介して前記 UE

10

20

30

40

50

へ送信する、
通信システム。

【請求項 7】

前記 UE は、前記 IMS 登録のための情報を前記 WWSF に要求する、請求項 6 に記載の通信システム。

【請求項 8】

認可ノードをさらに備え、
前記 WWSF は、前記トークンを前記認可ノードに要求する、
請求項 6 又は 7 に記載の通信システム。

【請求項 9】

前記 WWSF は、前記トークンと共に IMPU (IMS public user identity) を前記 UE へ送信し、
前記 UE は、前記 IMPU 及び前記トークンを伴う前記 REGISTER メッセージを前記 ePCSCF へ送信し、
前記 ePCSCF は、前記トークンと共に前記 IMPU を検証する、
請求項 6 ～ 8 のいずれか 1 項に記載の通信システム。

【請求項 10】

前記 UE は、WIC (WebRTC IMS Client) である、請求項 6 ～ 9 のいずれか 1 項に記載の通信システム。

【請求項 11】

UE (User Equipment) の認証方法であって、
IMS (IP (Internet Protocol) Multimedia Subsystem) 登録においてトークンを WWSF (WebRTC (Web Real Time Communication) Web Server Function) から受信することと、
前記トークンを検証して REGISTER メッセージを S-CSCF (Serving-CSCF) へ転送する ePCSCF (enhanced Proxy-CSCF (Call Session Control Function)) へ、前記トークンを伴う前記 REGISTER メッセージを送信することと、
HSS (Home Subscriber Server) から加入者プロフィールを受信する前記 S-CSCF から、前記 ePCSCF を介して 200 OK メッセージを受信することと、を含む
認証方法。

【請求項 12】

前記認証方法の開始にあたって、前記 IMS 登録のための情報を前記 WWSF に要求することをさらに含む、請求項 11 に記載の認証方法。

【請求項 13】

前記 UE は、前記トークンと共に IMPU (IMS public user identity) を前記 WWSF から受信し、
前記 UE は、前記トークンと共に前記 IMPU を検証する前記 ePCSCF へ、前記 IMPU 及び前記トークンを伴う前記 REGISTER メッセージを送信する、
請求項 11 又は 12 に記載の認証方法。

【請求項 14】

前記 UE は、WIC (WebRTC IMS Client) である、請求項 11 ～ 13 のいずれか 1 項に記載の認証方法。

【請求項 15】

WWSF (WebRTC (Web Real Time Communication) Web Server Function) と、ePCSCF (enhanced Proxy-CSCF (Call Session Control Function)) と、S-CSCF (Serving-CSCF) と、HSS (Home Subscrib

10

20

30

40

50

er Server) と、を含む通信システムに接続可能なUEであって、

IMS (IP (Internet Protocol) Multimedia Subsystem) 登録においてトークンを前記WWSFから受信し、前記HSSから加入者プロフィールを受信する前記S-CSCFから、前記eP-CSCFを介して200 OKメッセージを受信する受信部と、

前記トークンを検証してREGISTERメッセージを前記S-CSCFへ転送する前記eP-CSCFへ、前記トークンを伴う前記REGISTERメッセージを送信する送信部と、を備える、

UE。

【請求項16】

10

前記UEは、前記IMS登録のための情報を前記WWSFに要求する、請求項15に記載のUE。

【請求項17】

前記受信部は、前記トークンと共にIMPU (IMS public user identity) を前記WWSFから受信し、

前記送信部は、前記トークンと共に前記IMPUを検証する前記eP-CSCFへ、前記IMPU及び前記トークンを伴う前記REGISTERメッセージを送信する、

請求項15又は16に記載のUE。

【請求項18】

前記UEは、WIC (WebRTC IMS Client) である、請求項15～17のいずれか1項に記載のUE。

20

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、webRTC (Web Real Time Communication) のための装置、システム、及び方法に関し、特に、IMS (IP (Internet Protocol) Multimedia Subsystem) へのwebRTCクライアントのセキュア認証 (secure authentication) 技術に関する。

【背景技術】

【0002】

webRTCと呼ばれる新たなサービス、すなわち、音声及びビデオ通話のようなリアルタイムコミュニケーションサービスは、IETF (Internet Engineering Task Force) に規定されており、盛んに取り組まれている。webRTCは、スタンドアローン・サイロサービス (standalone silo service) として動作しないように、他のネットワークとインターワークする (interwork)。これは、他のwebRTCユーザとだけでなく、通常の電話とも通話したい最終顧客 (end customer) にとって重要である。

【0003】

この機能を提供するために、非特許文献1に開示されているように、3GPP (3rd Generation Partnership Project) にて研究が行われている。

40

【先行技術文献】

【非特許文献】

【0004】

【非特許文献1】3GPP TR23.701, “Study on Web Real Time Communication (WebRTC) access to IMS (Stage 2) (Release 12)”, V0.3.0, 2013年11月

【非特許文献2】3GPP TR33.abc (S3-131125), “Study on Security for WebRTC IMS Client access to IMS; (Release 12)”, V0.1.0, 2013年11月

50

【発明の概要】

【発明が解決しようとする課題】

【0005】

SA3 (security working group) においていくつかのセキュリティソリューションが開始されたが、webRTCクライアントが、モバイルオペレータのIP Multimedia Subsystem (IMS) に登録及び接続したいときに、現在のソリューション及びその合意は、モバイルデバイスにおけるwebRTCクライアントのセキュア認証 (Authentication) 及び認可 (Authorization) メカニズムを欠いている。認証されておらず及び／又は認可されていない任意のwebRTCクライアントを伴うインターネットからオペレータのIMSシステムへの攻撃を防止するために、最終顧客及びモバイルオペレータの両方を保護するためのセキュアソリューションを提供することが重要である。

10

【0006】

IMSへの認証及び認可を保証するアイデンティティの割り当てと正しいマッピング (またはバインディング) の問題は、図12に示される。

【0007】

User Equipment (UE) のブラウザは、WebRTC Web Server Function (WSF) からwebRTC IMS Client (WIC) をダウンロードする。WSFは、認証されたwebアイデンティティに関連したWICに対して、認可されたIMSアイデンティティの正確で一貫した割り当てを管理することについて責任がある。3GPPにおいて、WSFが、オペレータ・ホームIMS、又はホームIMSに認可されたサードパーティー・ネットワーク (third party network) に存在してもよいことが提案されている。

20

【0008】

UEがIMSサービスにアクセスするときに、ネットワークは、UEがそのようなサービスへのアクセスを許可されているかどうかを検証するために認可を実行すべきである。現在のシステムにおいて、WSFから割り当てられる2つの独立したアイデンティティ (webRTCアイデンティティ及びIMSアイデンティティ) がある。ネットワークがアイデンティティの検証に失敗した場合、認可されていないWICがIMSサービスへアクセスすること、及びネットワークへのDoS (Denial of Service) 攻撃を起こし得る。非特許文献1及び2にて提案された認証手順は、これらの脅威に対して十分ではない。

30

【0009】

それらの脅威に対抗するために、ネットワークは、WSFによって行われる認証及び／又は認可を検証することが必要である。webRTCアイデンティティとIMSアイデンティティとの間のバインディングは、ネットワークが検証を実行するために必要である。

【0010】

以下のセクションでは、どのようにIMSアイデンティティとのバインディングが実行されるのか、どのようにIMSネットワークはこのバインディングについて知らされるのか、及び追加の認証メカニズムが必要かどうかについて説明する。

40

【課題を解決するための手段】

【0011】

本発明は、webRTC IMSクライアントの認証及び認可が、モバイルネットワークオペレータのIMSにおいてどのように達成することができるかの様々な態様を提案する。WICは、IMSに登録するためにIDを使用し、そのIDは、IMS public user identity (IMPU)、IMS private identity (IMPI)、globally routable user agent URI (GRUU) 等であり得る。

【0012】

50

W I Cは、W W S Fによってe P - C S C Fアドレス及び認証情報を用いて事前設定され得るが、そうでない場合、この情報は、直接I M Sから又はW W S Fを介して、又は例えばO M A D M (O p e n M o b i l e A l l i c a n c e D e v i c e M a n a g e m e n t)である他のデバイス管理手順を介して、検索されるべきである。

【0013】

加入者が、既に有効なw e b R T Cアカウント又はメンバーシップを有すること、及びこれがW W S Fによって、有効にされ、認証され、及び認可され得ることがさらに想定される。

【0014】

本発明の第1の実施の態様にかかる方法は、通信システムにおける認証方法を提供する。この方法は、I M S登録においてW W S FからU Eへトークンを送信することと、前記トークンを伴うR E G I S T E Rメッセージを前記U Eからe P - C S C Fへ送信することと、前記e P - C S C Fによって前記トークンを検証することと、前記R E G I S T E Rメッセージを前記e P - C S C FからS - C S C Fへ転送することと、加入者プロフィール(s u b s c r i p t i o n p r o f i l e)をH S Sから前記S - C S C Fへ受信することと、200 O Kメッセージを前記S - C S C Fから前記e P - C S C Fを介して前記U Eへ送信することと、を含む。

【0015】

また、本発明の第2の実施の態様にかかるシステムは、U Eを認証する通信システムである。このシステムは、W W S Fと、e P - C S C Fと、S - C S C Fと、H S Sと、を含む。前記W W S Fは、I M S登録においてトークンを前記U Eへ送信する。前記U Eは、前記トークンを伴うR E G I S T E Rメッセージを前記e P - C S C Fへ送信する。前記e P - C S C Fは、前記トークンを検証する。前記e P - C S C Fは、前記R E G I S T E Rメッセージを前記S - C S C Fへ転送する。前記S - C S C Fは、加入者プロフィールを前記H S Sから受信する。前記S - C S C Fは、200 O Kメッセージを前記e P - C S C Fを介して前記U Eへ送信する。

【0016】

また、本発明の第3の実施の態様にかかる方法は、U Eの認証方法を提供する。この方法は、I M S登録においてトークンをW W S Fから受信することと、前記トークンを検証してR E G I S T E RメッセージをS - C S C Fへ転送するe P - C S C Fへ、前記トークンを伴う前記R E G I S T E Rメッセージを送信することと、H S Sから加入者プロフィールを受信する前記S - C S C Fから、前記e P - C S C Fを介して200 O Kメッセージを受信することと、を含む。

【0017】

さらに、本発明の第4の実施の態様にかかる装置は、W W S Fと、e P - C S C Fと、S - C S C Fと、H S Sと、を含む通信システムに接続可能なU Eである。このU Eは、I M S登録においてトークンを前記W W S Fから受信し、前記H S Sから加入者プロフィールを受信する前記S - C S C Fから、前記e P - C S C Fを介して200 O Kメッセージを受信する受信部と、前記トークンを検証してR E G I S T E Rメッセージを前記S - C S C Fへ転送する前記e P - C S C Fへ、前記トークンを伴う前記R E G I S T E Rメッセージを送信する送信部と、を含む。

【発明の効果】

【0018】

本発明により、例えば、I M Sへのw e b R T Cクライアントのセキュア認証をすることができる。

【図面の簡単な説明】

【0019】

【図1】本発明の第1の実施の形態にかかる静的なI M S I D割り当ての一例を示すブロック図である。

【図2】第1の実施の形態にかかる静的なI M S I D割り当てのためのコールフローの

10

20

30

40

50

一例を示すシーケンス図である。

【図 3】本発明の第 2 の実施の形態にかかる動的な IMS ID 割り当ての一例を示すブロック図である。

【図 4】第 2 の実施の形態にかかる動的な IMS ID 割り当てのためのコールフローの一例を示すシーケンス図である。

【図 5】第 2 の実施の形態にかかる動的な IMS ID 割り当てのためのコールフローの他の例を示すシーケンス図である。

【図 6】第 2 の実施の形態にかかる WWSF 及び eP-CSCF における同期されていない登録解除及びバインディング除去の一例を示すシーケンス図である。

【図 7】第 2 の実施の形態にかかる WWSF 及び eP-CSCF における同期された登録解除及びバインディング除去の一例を示すシーケンス図である。

【図 8】本発明の第 3 の実施の形態にかかる信頼されたサード・パーティーの AAA における webRTC ID 検証の一例を示すブロック図である。

【図 9】第 3 の実施の形態にかかる信頼されたサード・パーティーの AAA における webRTC ID 検証のためのコールフローの一例を示すシーケンス図である。

【図 10】第 3 の実施の形態にかかる信頼されたサード・パーティーの AAA における同期されていない登録解除の一例を示すシーケンス図である。

【図 11】第 3 の実施の形態にかかる信頼されたサード・パーティーの AAA における同期された登録解除の一例を示すシーケンス図である。

【図 12】典型的なアイデンティティマッピングを示すブロック図である。

【図 13】3GPP に提案される WWSF トークンによる webRTC クライアント認証を示すシーケンス図である。

【図 14】本発明にかかる UE の構成例を示すブロック図である。

【発明を実施するための形態】

【0020】

以下、本発明の第 1 から第 3 の実施の形態を、図面を参照して説明する。

【0021】

< 第 1 の実施の形態 >

本実施の形態は、webRTC アイデンティティごとの WWSF への静的な IMS ID 割り当てを提案する。図 1 にアイデンティティバインディングの原理を示す。

【0022】

WWSF 30 及び HSS (Home Subscriber Server) 60 は、wh インタフェースを介してアイデンティティ情報を交換することができる。その情報は、IMS ID に対応する特定の webRTC アイデンティティと、必要であれば IMS 認証のためのパスワードを含むが、このパラメータセットに制限されない。

【0023】

図 2 は、ステップ S11 から S15 の事前準備段階により IMS 登録のためのコールフロー (call flow) を提供する。

【0024】

ステップ S11: UE 10 は、IMS 加入者 (IMS subscriber) 及び webRTC 加入者 (webRTC subscriber) であり、IMS オペレータに自身の webRTC ID を登録する。これは、その IMS 登録の間に IMS クライアントに通常使用される通常の IMS 登録メッセージにおいて行われ得る。

【0025】

ステップ S12: HSS 60 は、webRTC ID と IMS ID との間でバインディングを生成する。それは、新たな WIC IMS ID と、必要であれば対応するパスワード又は他の認証に関連する情報を生成する。WIC の IMS ID は、通常の IMS クライアントのものとは異なる。

【0026】

ステップ S13: HSS 60 は、webRTC ID から WWSF アドレスを導出する

。HSS 60は、WSF 30を見つけるために、webRTCプロバイダごとにルックアップテーブルを有することができ、又は固定されたフォーマット、例えば「wssf@webrtcprovider.com」を有する。HSS 60は、whインタフェースを介してWSF 30に、生成されたWIC IMS ID、パスワード、及びwebRTC IDを提供する。HSS 60は、他のsubscription又は認証に関連する情報も提供し得る。WIC 20は、正しいeP-CSCF (enhanced Proxy-Call Session Control Function) アドレスを検索することができないかもしれない。したがって、HSS 60は、eP-CSCFをこのメッセージに含め得る。その情報はまた、WIC 20が例えばWSF 30によって事前設定されるかどうか

10

【0027】

ステップS14: WSF 30は、webRTC IDとWIC IMS IDと、もし提供されるならばパスワード及び他の情報との間でバインディングを生成する。

【0028】

ステップS15: webRTCを使用可能にされたブラウザ (webRTC-enabled browser) 内から、ユーザーは、WSF 30とのHTTPS (Hypertext Transfer Protocol Secure) 接続を開始するために、WSF 30へのURI (Uniform Resource Identifier) にアクセスし得る。TLS (Transport Layer Security) 接続は、サーバ証明書 (server certificate) に基づいてサーバの一方

20

【0029】

ステップS16: WIC 20は、自身のwebRTC IDを用いてWSF 30に登録する。WSF 30は、共通のウェブ認証手順 (common web authentication procedure) を用いてユーザを認証し得る。

【0030】

ステップS17: WSF 30は、対応するIMS ID、及び可能な場合、パスワード、eP-CSCFアドレス、認証情報等を、WIC 20へ提供する。その情報はまた、WIC 20が事前設定されるかどうか

30

【0031】

ステップS18: WIC 20は、受信した情報を格納し、WIC IMS IDを用いて、REGISTERメッセージをeP-CSCF 40に送信する。このメッセージは、望ましくは、SIP (Session Initiation Protocol) メッセージであり得るが、WebSocket、JSON (JavaScript (登録商標) Object Notation) 等のような他のプロトコルに基づくことができる。

【0032】

ステップS19: S-CSCF (Serving-CSCF) 50は、HSS 60から認証データを検索し、401 unauthorized responseを用いてUE 10にチャレンジする。このメッセージは、望ましくは、SIPメッセージであり得るが、WebSocket、JSON等のような他のプロトコルに基づくことができる。

40

【0033】

ステップS20: WIC 20は、WSF 30から受信した情報 (パスワード、情報に関する他の認証) を用いてチャレンジを解決し、別のREGISTERメッセージをeP-CSCF 40に送信する。このメッセージは、望ましくは、SIPメッセージであり得るが、WebSocket、JSON等のような他のプロトコルに基づくことができる。

【0034】

ステップS21: S-CSCF 50は、200 OK又は他の適切なメッセージを用いてWIC 20に対して登録に確認応答し (acknowledge)、HSS 60から

50

加入者プロフィールを検索する。このメッセージは、望ましくは、SIPメッセージであり得るが、Web Socket、JSON等のような他のプロトコルに基づくことができる。

【0035】

本実施の形態は、webRTCユーザが同時にIMS加入者でもあることを必要とする。WIC 20が、UICC (Universal Integrated Circuit Card) にアクセスできず、P-CSCF割り当てを有さないので、HSS 60は、webRTCサービスプロバイダとのインタフェースを必要とし、IMS ID+パスワード及びeP-CSCFアドレスを交換する。

【0036】

<第2の実施の形態>

本実施の形態において、WWSFは、IMSオペレータのHSSから受信したIMS IDのプールを使用している。その背景にあるアイデアは、webRTCサービスプロバイダが、自身のIMS subscriptionをwebRTCユーザが有すると仮定せず、したがって、webRTCサービスプロバイダが、オンデマンド (on demand) でwebRTC IMSクライアントに割り当てられ得るIMS subscriptionのプールを保持する。アーキテクチャを図3に示す。

【0037】

IMS IDのプールは、wildcarded IMPUのフォーム (form) でWWSF 30に提供され得るが、それはIMPUのリストにすることもでき、これに制限されない。

【0038】

図4にその手順のコールフローを示す。

【0039】

ステップS31: WWSF 30は、オンデマンドでwebRTCユーザにより共有される例えば、wildcarded IMPU、又はIMPUのリストであるIMS IDのプールを用いて事前設定される。HSS 60は、WWSF 30にコンフィギュレーションを提供し、また、例えばeP-CSCFアドレス、認証情報、パスワード等の追加の情報も提供し得る。

【0040】

ステップS32: webRTCを使用可能にされたブラウザ内から、ユーザは、WWSF 30とのHTTPS接続を開始するために、WWSF 30のURIにアクセスし得る。TLS接続は、サーバ証明書に基づいてサーバの一方の認証を提供し得る。ブラウザは、WWSF 30からWIC 20をダウンロードし、WIC 20を初期設定して、準備段階は完了する。

【0041】

ステップS33: WIC 20は、自身のwebRTC IDを用いてWWSF 30に登録する。WWSF 30は、必要であれば、認証手続を開始し得る。

【0042】

ステップS34: WWSF 30は、現在使用されていないIMS IDを選択する、又はwildcarded IMPUの場合に、例えばwebRTC IDに基づきIMPUを生成する。WWSF 30は、このIMS IDをwebRTC IDにバインドし、且つ入手可能な場合、IMS IDを、パスワード、eP-CSCFアドレス、認証情報等にバインドする。その情報はまた、WIC 20が、WWSF 30によってeP-CSCFアドレス及び認証情報を用いて事前設定されるか否かに依存している。

【0043】

ステップS35: WWSF 30は、webRTC ID及びIMS IDのバインディングをeP-CSCF 40に登録する。

【0044】

ステップS36: eP-CSCF 40及びWWSF 30は信頼関係 (trust r

10

20

30

40

50

e l a t i o n s h i p) を有し、お互いに認証し得る。e P - C S C F 40は、バイ
ンディングを格納し、バインディングに確認応答する。それはバインディングのための v
a l i d i t y t i m e rを開始することができ、W W S F 30にその t i m e rを提
供する。

【0045】

ステップS37: W W S F 30は、w e b R T C I Dにバインドしている I M S I
DをW I C 20に提供する。

【0046】

ステップS38: W I C 20は、受信した情報を格納し、I M S I Dを伴うR E G I
S T E Rメッセージをe P - C S C F 40に送信する。このメッセージは、望ましくは
、S I Pメッセージであり得るが、W e b S o c k e t、J S O N等のような他のプロト
コルに基づくことができる。

10

【0047】

ステップS39: e P - C S C F 40は、w e b R T C I D及びI M S I Dのバイ
ンディングを検証し、R E G I S T E Rを認可する。e P - C S C F 40は、S - C S
C F 50によるチャレンジの必要をなくすために、そのバインディングが検証された及
び／又は登録が認可されたことを示すインジケータ (i n d i c a t o r)、フラグ、又
は他のパラメータをR E G I S T E R内に含めることができる。このメッセージは、望ま
しくは、S I Pメッセージであり得るが、W e b S o c k e t、J S O N等のような他の
プロトコルに基づくことができる。

20

【0048】

ステップS40: e P - C S C F 40は、I M S I Dを伴うR E G I S T E Rを(潜
在的にI B C F (I n t e r c o n n e c t i o n B o r d e r C o n t r o l) 又は
I - C S C F (I n t e r r o g a t i n g - C S C F) のような他のI M S ノードを介
して) S - C S C F 50に転送し、前のステップにおいて説明されるようにそれにマー
クを付け得る。S - C S C F 50は、加入者プロファイルをH S S 60に要求する。こ
のメッセージは、望ましくは、S I Pメッセージであり得るが、W e b S o c k e t、J
S O N等のような他のプロトコルに基づくことができる。

【0049】

ステップS41: S - C S C F 50は、登録に確認応答し、このw e b R T Cサービ
スプロバイダのための一般加入者プロファイルをH S S 60から検索する。200 O K
又は他の適切なメッセージがW I C 20へ転送される。このメッセージは、望ましくは
、S I Pメッセージであり得るが、W e b S o c k e t、J S O N等のような他のプロト
コルに基づくことができる。

30

【0050】

本実施の形態の他のバリエーションにおいて、図5に示す以下のコールフローを適用す
る。

【0051】

前の図4と同じ原則が適用され、すなわちステップはほぼ同じであり、ステップS51
b及び検証ステップS56により2つだけ追加のステップが含まれている。

40

【0052】

ステップS51a: W W S F 30は、オンデマンドでw e b R T Cユーザにより共有
される例えば、w i l d c a r d e d I M P U、又はI M P UのリストであるI M S I
Dのプールを用いて事前設定される。H S S 60は、W W S F 30にコンフィギュレー
ションを提供し、また、例えばe P - C S C Fアドレス、認証情報、パスワード等の追加
の情報も提供し得る。

【0053】

ステップS51b: H S S 60は、W W S F I D及びその許可されたI M S I D
をe P - C S C F 40に提供する。それはP S I (P r o j e c t S e r v e r I n
t e r f a c e) ルーティングを使用することができ、適切なS I Pメッセージ、例えば

50

OPTIONS、UPDATE、INVITE、REGISTER、200 OK、MESSAGE等を使用することができる。

【0054】

ステップS52: webRTCを使用可能にされたブラウザ内から、ユーザは、WWSF 30とのHTTPS接続を開始するために、WWSF 30のURIにアクセスし得る。TLS接続は、サーバ証明書に基づいてサーバの一方の認証を提供し得る。ブラウザは、WWSF 30からWIC 20をダウンロードし、WIC 20を初期設定して、準備段階は完了する。

【0055】

ステップS53: WIC 20は、自身のwebRTC IDを用いてWWSF 30に登録する。WWSF 30は、必要であれば、認証手続を開始し得る。

10

【0056】

ステップS54: WWSF 30は、現在使用されていないIMS IDを選択する、又はwildcarded IMPUの場合に、例えばwebRTC IDに基づきIMPUを生成する。WWSF 30は、このIMS IDをwebRTC IDにバインドし、且つ入手可能な場合、IMS IDを、パスワード、eP-CSCFアドレス、認証情報等にバインドする。その情報はまた、WIC 20が、WWSF 30によってeP-CSCFアドレス及び認証情報を用いて事前設定されるか否かに依存している。

【0057】

ステップS55: WWSF 30は、webRTC ID及びIMS IDのバインディングをeP-CSCF 40に登録する。

20

【0058】

ステップS56: eP-CSCF 40及びWWSF 30は信頼関係を有し、お互いに認証し得る。eP-CSCF 40は、ステップS51bにおけるHSS provisioningに基づいて、WWSF 30がそのIMS IDの使用を認可されているかどうかを検証する。eP-CSCF 40は、webRTC ID及びIMS IDのバインディングのためのvalidity timerを開始することができる。

【0059】

ステップS57: eP-CSCF 40は、WWSF 30に対してwebRTC ID及びIMS IDのバインディングを確認応答し、バインディングが有効な期間のためのvalidity timerを提供し得る。

30

【0060】

ステップS58: WWSF 30は、webRTC IDにバインドしているIMS IDをWIC 20に提供する。

【0061】

ステップS59: WIC 20は、受信した情報を格納し、IMS IDを伴うREGISTERメッセージをeP-CSCF 40に送信する。このメッセージは、望ましくは、SIPメッセージであり得るが、WebSocket、JSON等のような他のプロトコルに基づくことができる。

【0062】

40

ステップS60: eP-CSCF 40は、webRTC ID及びIMS IDのバインディングを検証し、REGISTERを認可する。eP-CSCF 40は、S-CSCF 50によるチャレンジの必要をなくすために、そのバインディングが検証された及び／又は登録が認可されたことを示すインジケータ、フラグ、又は他のパラメータをREGISTER内に含めることができる。このメッセージは、望ましくは、SIPメッセージであり得るが、WebSocket、JSON等のような他のプロトコルに基づくことができる。

【0063】

ステップS61: eP-CSCF 40は、IMS IDを伴うREGISTERを（潜在的にIBCF又はI-CSCFのような他のIMSノードを介して）S-CSCF 5

50

0に転送し、前のステップにおいて説明されるようにそれにマークを付け得る。S-CSCF 50は、加入者プロファイルをHSS 60に要求する。このメッセージは、望ましくは、SIPメッセージであり得るが、WebSocket、JSON等のような他のプロトコルに基づくことができる。

【0064】

ステップS62：S-CSCF 50は、登録に確認応答し、このwebRTCサービスプロバイダのための一般加入者プロファイルをHSS 60から検索する。200 OK又は他の適切なメッセージがWIC 20へ転送される。このメッセージは、望ましくは、SIPメッセージであり得るが、WebSocket、JSON等のような他のプロトコルに基づくことができる。

10

【0065】

(登録解除及びバインディング除去)

ある時点では、UE 10、すなわちWIC 20は、これ以上IMS登録されていたくないかもしれない。そのとき、WIC 20は、S-CSCF 50が登録を除去するように、期限切れのtimerに基づきタイムアウトし得るIMS登録をリフレッシュ(refresh)しないことができる。

【0066】

WIC 20は、積極的に登録解除を望むことができ、これは終端コールが直接失敗する利点を有し、calling partyが直接知らされ得るように、配信されないタイムアウト(undelivered timeout)に起因しない。また、フリーIMS IDは、他のwebRTC IDに割り当てるために再利用可能である。

20

【0067】

図6に、同期されていない登録解除をどのように行うことができるかを示す。

【0068】

ステップS71：WIC 20は、自身のwebRTC IDを伴う登録解除メッセージをWWSF 30に送信する。

【0069】

ステップS72：WWSF 30は、WIC stateを未登録に設定し、IMS IDとwebRTC IDとのバインディングを除去する。WWSF 30は、図7に示すようにバインディングの除去についてeP-CSCF 40に知らせ得る。

30

【0070】

ステップS73：WWSF 30は、登録解除に確認応答する。

【0071】

ステップS74：WIC 20は、0に等しい期間満了timerと共にIMS ID及びwebRTC IDを伴うREGISTERメッセージをeP-CSCF 40に送信する。このメッセージは、望ましくは、SIPメッセージであり得るが、WebSocket、JSON等のような他のプロトコルに基づくことができる。

【0072】

ステップS75：eP-CSCF 40は、webRTC ID及びIMS IDのバインディングを検証し、REGISTERを認可する。eP-CSCF 40は、S-CSCF 50によるチャレンジの必要をなくすために、そのバインディングが検証された及び／又は登録が認可されたことを示すインジケータ、フラグ、又は他のパラメータをREGISTER内に含めることができる。このメッセージは、望ましくは、SIPメッセージであり得るが、WebSocket、JSON等のような他のプロトコルに基づくことができる。

40

【0073】

ステップS76：eP-CSCF 40は、IMS IDを伴うREGISTERを(潜在的にIBCF又はI-CSCFのような他のIMSノードを介して)S-CSCF 50に転送し、前のステップにおいて説明されるようにそれをマークし得る。S-CSCF 50は、登録解除についてHSS 60に知らせる。このメッセージは、望ましくは、S

50

I Pメッセージであり得るが、Web S o c k e t、J S O N等のような他のプロトコルに基づくことができる。

【0074】

ステップS77：S-C S C F 50は、登録解除に確認応答する。200 OK又は他の適切なメッセージがW I C 20へ転送される。このメッセージは、望ましくは、S I Pメッセージであり得るが、Web S o c k e t、J S O N等のような他のプロトコルに基づくことができる。

【0075】

ステップS78：e P-C S C F 40は、I M S登録解除が成功したという確認応答（a c k n o w l e d g e m e n t）を受信した時点で、w e b R T C I DとI M S I Dとの間のバインディングを除去する。 10

【0076】

登録解除のバリエーションにおいて、W I C 20は、ステップS74にて登録解除メッセージをI M Sに直接送信することができ、e P-C S C F 40は、登録解除及び／又はバインディングの除去についてW W S F 30に知らせるよう気を付ける。

【0077】

図7に、w e b R T CプロバイダとI M Sプロバイダとの間で同期された登録解除をどのように行うことができるかの他のバリエーションを示す。

【0078】

ステップS81：W I C 20は、自身のw e b R T C I Dを伴う登録解除メッセージをW W S F 30に送信する。 20

【0079】

ステップS82：W W S F 30は、I M S I D及びw e b R T C I Dのタプル（t u p l e）を伴う登録解除メッセージをe P-C S C F 40に送信する。W W S F 30は、既にバインディングを除去し得るが、後の段階、例えばステップS88にてそれを行うこともできる。

【0080】

ステップS83：e P-C S C F 40は、w e b R T C I DとI M S I Dとの間のバインディングを検証し、0に等しい期間満了t i m e rと共にI M S I D及びw e b R T C I Dを伴うS-C S C F 50へのR E G I S T E Rメッセージを生成する。このメッセージは、望ましくは、S I Pメッセージであり得るが、Web S o c k e t、J S O N等のような他のプロトコルに基づくことができる。 30

【0081】

ステップS84：e P-C S C F 40は、0に等しい期間満了t i m e rと共にI M S I D及びw e b R T C I Dを伴うR E G I S T E Rメッセージを（潜在的にI B C F又はI-C S C Fのような他のI M Sノードを介して）S-C S C F 50に送信する。e P-C S C F 40は、そのバインディングが検証された及び／又は登録が認可されたことを示すインジケータ、フラグ、又は他のパラメータを含めることができる。S-C S C F 50は、登録解除についてH S S 60に知らせる。このメッセージは、望ましくは、S I Pメッセージであり得るが、Web S o c k e t、J S O N等のような他のプロトコルに基づくことができる。 40

【0082】

ステップS85：S-C S C F 50は、登録解除に確認応答する。200 OK又は他の適切なメッセージがe P-C S C F 40へ転送される。このメッセージは、望ましくは、S I Pメッセージであり得るが、Web S o c k e t、J S O N等のような他のプロトコルに基づくことができる。

【0083】

ステップS86：e P-C S C F 40は、w e b R T C I D及びI M S I Dのバインディングを除去する。

【0084】

ステップS87：eP-CSCF 40は、成功した登録解除に確認応答する。

【0085】

ステップS88：WWSF 30は、WIC stateを未登録に設定し、IMS IDとwebRTC IDとのバインディングを除去する。

【0086】

ステップS89：WWSF 30は、登録解除に成功したことをWIC 20に確認応答する。

【0087】

＜第3の実施の形態＞

本実施の形態において、サード・パーティー認証（third party authentication）と、IMSオペレータだけでなくwebRTCサービスプロバイダにより信頼された認可サーバとが使用される。アーキテクチャを図8に示す。

【0088】

AAA（Authentication Authorization and Accounting）70は、特定のwebRTC IDのために、WWSF 30にトークン又は他のメカニズムを提供する。AAA 70は、信頼されたサード・パーティーによりホストされたモバイルオペレータ又はインターネット内に配置され得る。WIC 20が、特定の時間間隔内で、正しいwebRTC IDと共にトークンを使用する場合、HSS 60は、WIC 20が登録することを許可されるかどうかをAAA 70でチェックする。このために、webRTCユーザは、IMS登録を有する必要はなく、IMSネットワーク又はモバイルネットワークの加入者になるユーザを有していない。

【0089】

図9にその手順のコールフローを示す。

【0090】

ステップS91：webRTCを使用可能にされたブラウザ内から、ユーザは、WWSF 30とのHTTPS接続を開始するために、WWSF 30のURIにアクセスし得る。TLS接続は、サーバ証明書に基づいてサーバの一方方向の認証を提供し得る。ブラウザは、WWSF 30からWIC 20をダウンロードし、WIC 20を初期設定して、準備段階は完了する。

【0091】

ステップS92：WIC 20は、自身のwebRTC IDを用いてWWSF 30に登録する。WWSF 30は、必要であれば、認証手続を開始し得る。

【0092】

ステップS93：WIC 20が事前設定されていない場合、WWSF 30はeP-CSCF 40を選択する。webRTCが少なくとも1つのIMSオペレータとService Level Agreementを有していると仮定される。したがって、WWSF 30は、eP-CSCFアドレスを知り、特定のwebRTC IDごとに1つ選択することができる。

【0093】

ステップS94：WWSF 30は、webRTC IDのためのトークンをAAA 70に要求する。

【0094】

ステップS95：AAA 70は、webRTC IDのためのトークンを生成し、バインディングを格納する。トークンは、制限された有効時間（limited validity time）を有し得る。

【0095】

ステップS96：AAA 70は、webRTC IDのためのトークンを許可（grant）し、それとオプションで関連情報（例えば、validity timer）とをWWSF 30に送信する。

【0096】

10

20

30

40

50

ステップS 9 7 : W W S F 3 0 は、トークン及びオプションで e P - C S C F アドレスを W I C 2 0 に提供する。

【0 0 9 7】

ステップS 9 8 : W I C 2 0 は、自身の w e b R T C I D 及びトークンを伴う R E G I S T E R を、e P - C S C F 4 0 及び S - C S C F 5 0 に送信する。

【0 0 9 8】

ステップS 9 9 : S - C S C F 5 0 は、この w e b R T C I D 及びトークンのために認証要求 (a u t h e n t i c a t i o n r e q u e s t) を実行する。

【0 0 9 9】

ステップS 1 0 0 : H S S 6 0 は、w e b R T C I D 及びトークンを検証することを A A A 7 0 に要求する。 10

【0 1 0 0】

ステップS 1 0 1 : H S S 6 0 は、認証に確認応答し、この w e b R T C サービスプロバイダのために一般加入者プロフィールを S - C S C F 5 0 に提供する。

【0 1 0 1】

ステップS 1 0 2 : S - C S C F 5 0 は、2 0 0 O K 又は他の適切なメッセージを用いて R E G I S T E R に確認応答する。

【0 1 0 2】

(登録解除及びバインディング除去)

ある時点では、U E 1 0、すなわち W I C 2 0 は、これ以上 I M S 登録されていたくないかもしれない、そのとき、W I C 2 0 は、S - C S C F 5 0 が登録を除去するように、期限切れの t i m e r に基づきタイムアウトし得る I M S 登録をリフレッシュしないことができる。 20

【0 1 0 3】

W I C 2 0 は、積極的に登録解除を望むことができ、これは終端コールが直接失敗する利点を有し、c a l l i n g p a r t y が直接知らされ得るように、配信されないタイムアウトに起因しない。また、フリー I M S I D は、他の w e b R T C I D に割り当てられるために再利用可能である。

【0 1 0 4】

図 1 0 に、同期されていない登録解除をどのように行うことができるかを示す。 30

【0 1 0 5】

ステップS 1 1 1 : W I C 2 0 は、自身の w e b R T C I D を伴う登録解除メッセージを W W S F 3 0 に送信する。

【0 1 0 6】

ステップS 1 1 2 : W W S F 3 0 は、トークン及び／又はバインディングを除去するために、w e b R T C I D を伴う要求メッセージを A A A 7 0 に送信する。

【0 1 0 7】

ステップS 1 1 3 : A A A 7 0 は、I M S 登録解除が起こった時点で、そのバインディングにマークを付け、それはすぐに除去される。

【0 1 0 8】

ステップS 1 1 4 : A A A 7 0 は、トークン及び／又はバインディングの除去の情報が準備されたこと、及び今や W I C 2 0 が I M S 登録解除を実行できることを確認応答する。 40

【0 1 0 9】

ステップS 1 1 5 : W W S F 3 0 は、W I C s t a t e を未登録に設定し、w e b R T C I D と他の情報とのバインディングを除去し、登録解除に成功したことを W I C 2 0 に確認応答する。

【0 1 1 0】

ステップS 1 1 6 : W I C 2 0 は、0 に等しい期間満了 t i m e r と共に w e b R T C I D を伴う R E G I S T E R メッセージを (潜在的に I B C F 又は I - C S C F のよ 50

うな他のIMSノードを介して) S-CSCF 50に送信する。eP-CSCF 40は、そのバインディングが検証された及び／又は登録が認可されたことを示すインジケータ、フラグ、又は他のパラメータを含めることができる。

【0111】

ステップS117: S-CSCF 50は、webRTC IDのための登録解除についてHSS 60に知らせる。このメッセージは、望ましくは、SIPメッセージであり得るが、WebSocket、JSON等のような他のプロトコルに基づくことができる。

【0112】

ステップS118: HSS 60は、webRTC IDを認証すること、及びバインディングを除去することをAAA 70に要求する。AAA 70は、webRTC IDを認証し、バインディングを除去したことをHSS 60に示す。

10

【0113】

ステップS119: HSS 60は、登録解除に確認応答する。このメッセージは、望ましくは、SIPメッセージであり得るが、WebSocket、JSON等のような他のプロトコルに基づくことができる。

【0114】

ステップS120: S-CSCF 50は、200 OK又は他の適切なメッセージをWIC 20に送信する。このメッセージは、望ましくは、SIPメッセージであり得るが、WebSocket、JSON等のような他のプロトコルに基づくことができる。

【0115】

20

登録解除のバリエーションにおいて、WIC 20は、ステップS116にて登録解除メッセージをIMSに直接送信することができ、AAA 70は、登録解除、及び／又はバインディング及び／又はトークンの除去についてWSF 30に知らせるよう気を付ける。

【0116】

図11に、同期されたマナーにおいて登録解除をどのように行うことができるかの他のバリエーションを示す。

【0117】

ステップS131: WIC 20は、自身のwebRTC IDを伴う登録解除メッセージをWSF 30に送信する。

30

【0118】

ステップS132: WSF 30は、トークン及び／又はバインディングを除去するために、webRTC IDを伴う要求メッセージをAAA 70に送信する。

【0119】

ステップS133: AAA 70は、バインディングを除去し、IMS登録解除をHSS 60に要求する。また、AAA 70は、成功した登録解除についての確認応答をHSS 60から得た時点で、バインディングを除去することもできる。

【0120】

ステップS134: HSS 60は、0に等しい期間満了timerと共にwebRTC IDを伴うREGISTERメッセージをeP-CSCF 40に送信する。このメッセージは、望ましくは、SIPメッセージであり得るが、WebSocket、JSON等のような他のプロトコルに基づくことができる。

40

【0121】

ステップS135: eP-CSCF 40は、登録解除に確認応答し、間にあるすべてのノード、例えばS-CSCF 50は、加入者プロファイルを除去する。このメッセージは、望ましくは、SIPメッセージであり得るが、WebSocket、JSON等のような他のプロトコルに基づくことができる。

【0122】

上述した説明に基づいて、下記文書を3GPPに提案する。

【0123】

50

議論：

現在のwebRTC TR 33. abcは、ユーザが個人のIMPUと共にsubscriptionを有し、IMSとの認証を行うIMS認証メカニズム（例えば、IMSDigest）を使用するという仮定に基づいて、IMSにおけるwebRTC IMSクライアントの認証のための2つの異なるソリューションを説明している。この仮定は、webRTCインターワーキング機能（webRTC interworking feature）の有用性を極めて制限する。なぜなら、もしユーザがIMSクライアントを有し、webRTCなしでIMSセッションをセットアップできるならば、webRTC通信を使用する意味がないからである。

【0124】

TR 23. 701における現在の研究の結論では、eP-CSCFのための以下の機能を載せている。

- －eP-CSCFは、WSFにより実行されるあらゆるUE認証を検証し、WSFにより既に認証されたUEのために、IMSにおいて、TS 33. 203に定義されているようにTrusted Node Authentication (TNA)を実行する。

- －Web認証シナリオ（Web authentication scenarios）のために、eP-CSCFは、WICに付すIMSアイデンティティを割り当てることをWSFが認可されていることを検証する。

- －eP-CSCFは、IMS又はWeb認証シナリオを使用して、WICのためのIMS登録を実行する。

【0125】

これらの必須の機能を達成可能とするために、eP-CSCFは、WSFの使用されたアイデンティティについての知識を有する必要がある。

【0126】

TR 23. 701のオリジナルのソリューション3においてW2リファレンスポイントで示されるように、WSFが関連情報をeP-CSCFに提供することが、ここで提案される。また、IMS登録のプールから、IMSに対する登録を望むWICに、有効なIMPUを割り当てることをWSFに許可することによって、IMS登録に必須の制限を克服することが提案される。IMS登録のプールは、wildcarded IMPUを用いて簡単に実現できる。

【0127】

WICの要求に際して、WSFは、IMPUをWICに提供し、このIMPUのためのトークンをeP-CSCFに提供する。eP-CSCFは、この情報に基づいて、WICからの登録要求を認証することができる。

【0128】

提案：

webRTC TR 33. abcに以下の文章を追加することを提案する。

【0129】

6. 1. x eP-CSCFでのWSFトークンを用いてのwebRTC IMSクライアントの認証

WSFは、IMSオペレータのHSSから受信したIMS IDのプールを使用している。その背景にあるアイデアは、webRTCサービスプロバイダが、自身のIMS subscriptionをwebRTCユーザが有すると仮定せず、したがって、webRTCサービスプロバイダが、オンデマンドでwebRTC IMSクライアントに割り当てられ得るIMS subscriptionのプールを保持する。IMS IDのプールは、wildcarded IMPUのフォームでWSFに提供され得る。

【0130】

図13に認証手順のコールフローを示す。

【0131】

10

20

30

40

50

1: WWSFは、オンデマンドでwebRTCユーザにより共有されるwildcarded IMPUを用いて事前設定される。

【0132】

2: webRTCを使用可能にされたブラウザ内から、ユーザは、WWSFとのHTTPS接続を開始するために、WWSFのURIにアクセスする。TLS接続は、サーバ証明書に基づいてサーバの一方の認証を提供する。ブラウザは、WWSFからWICをダウンロードし、WICを初期設定する。

【0133】

3: WICは、自身のwebRTC IDを用いて、IMS登録情報(IMS registration information)をWWSFに要求する。WWSFは、必要であれば、認証手続を開始し得る。

10

【0134】

4: WWSFは、例えば、そのwebRTC IDに基づいて、wildcarded IMPUからIMPUを生成する。WWSFは、このIMPUをwebRTC IDにバインドし、トークンを生成する。

【0135】

5: WWSFは、IMPU及びトークンをeP-CSCFに登録する。

【0136】

6: P-CSCF及びWWSFは、信頼関係を有し、お互いに認証し得る。eP-CSCFは、バインディングを格納し、バインディングに確認応答する。それはバインディングのためのvalidity timerを開始することができ、WWSFにそのtimerを提供する。

20

【0137】

7: WWSFは、webRTC IDにバインドしているIMPU及びトークンをWICに提供する。

【0138】

8: WICは、受信した情報を格納し、IMPU及びトークンを用いてREGISTERメッセージをeP-CSCFに送信する。

【0139】

9: eP-CSCFは、IMPU及びトークンのバインディングを検証し、REGISTERを認可する。eP-CSCFは、S-CSCFによるチャレンジの必要をなくするために、そのバインディングが検証された及び／又は登録が認可されたことを示すインジケータ、フラグ、又は他のパラメータをREGISTER内に含めることができる。

30

【0140】

10: eP-CSCFは、REGISTERをS-CSCFに転送する。S-CSCFは、加入者プロファイルをHSSに要求する。

【0141】

11: S-CSCFは、登録に確認応答し、このwebRTCサービスプロバイダのための一般加入者プロファイルをHSSから検索する。200 OKメッセージがWICへ転送される。

40

【0142】

図14に、この認証手順におけるUE 10の構成例を示す。図14に示すように、UE 10は、少なくとも受信部11と、送信部12と、を備える。受信部11は、IMS登録において、トークンをWWSF 30から受信し、200 OKメッセージをS-CSCF 50から受信する。上述したように、S-CSCF 50は、HSS 60からeP-CSCF 40を介して加入者プロファイルを受信する。送信部12は、トークンを伴うREGISTERメッセージをeP-CSCF 40に送信する。上述したように、eP-CSCF 40は、トークンを検証し、REGISTERメッセージをS-CSCF 50へ転送する。UE 10は、そこから認証の開始に際して、IMS登録のための情報をWWSF 30に要求し得る。受信部11は、トークンと共にIMPUをWWSF 30

50

から受信し得る。送信部 12 は、IMPU 及びトークンを伴う REGISTER メッセージを eP-CSCF 40 に送信し得る。上述したように、eP-CSCF 40 は、トークンと共に IMPU を検証する。さらに、上述したように、UE 10 は、WIC 20 を WWSF 30 からダウンロードすることができ、したがって、WIC 20 として機能／動作する。なお、これらのユニット 11 及び 12 は、バス等を介して相互接続される。これらのユニット 11 及び 12 は、例えば、図 1、3 及び 8 のそれぞれに示された EPC (Evolved Packet Core) を介して WWSF 30 及び eP-CSCF 40 との通信を実行するランシーバと、図 2、4～7、9～11 及び 13 のそれぞれに示されたプロセス又はそれに同等な (equivalent) プロセスを実行するために、このランシーバを制御する CPU (Central Processing Unit) 等のコントローラと、で構成できる。

10

【0143】

なお、本発明は、上記の実施の形態によって限定されるものではなく、特許請求の範囲の記載に基づき、当業者によって種々の変更が可能なことは明らかである。

【0144】

上記の実施の形態の一部又は全部は、以下の付記のようにも記載され得るが、以下には限られない。

【0145】

(付記 1)

webRTC ID 及び IMS ID のバインディング

20

a. バインディングは、HSS、WWSF、又は AAA で生成できる。

b. バインディングは、(ネットワーク) エンティティ、例えば HSS から WWSF、WWSF から eP-CSCF、に提供することができる。

c. バインディングの検証は、バインディングを生成したエンティティ、又はバインディングを提供されたエンティティで行うことができる。

d. これ以上必要でなくなった時点で IMS 登録解除を含めたバインディングの除去

【0146】

(付記 2)

UE WIC が web アイデンティティ (webRTC ID) を用いて IMS サービスにアクセスするときに、上述したバインディングの検証によって、オペレータは、認証及び認可を実行することができる。

30

【0147】

(付記 3)

WIC から登録メッセージを送信するための認証及び認可を制限する有効時間

【0148】

(付記 4)

WWSF による UE WIC への eP-CSCF 割り当て

【0149】

(付記 5)

IMS ID の代わりに webRTC ID を用いるだけでなく、静的な webRTC ID を IMS バインディングに用いる、又は動的なバインディングを IMS ID のプールに用いる。

40

【0150】

この出願は、2013 年 12 月 19 日に提出された日本出願特願 2013-262170、及び 2014 年 1 月 9 日に提出された日本出願特願 2014-002633 を基礎とする優先権を主張し、それらの開示の全てをここに取り込む。

【符号の説明】

【0151】

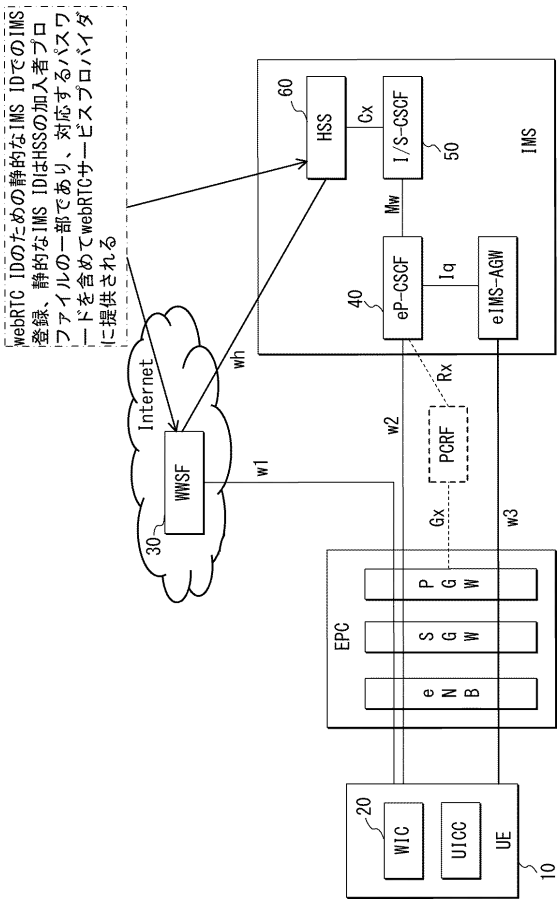
10 UE

11 受信部

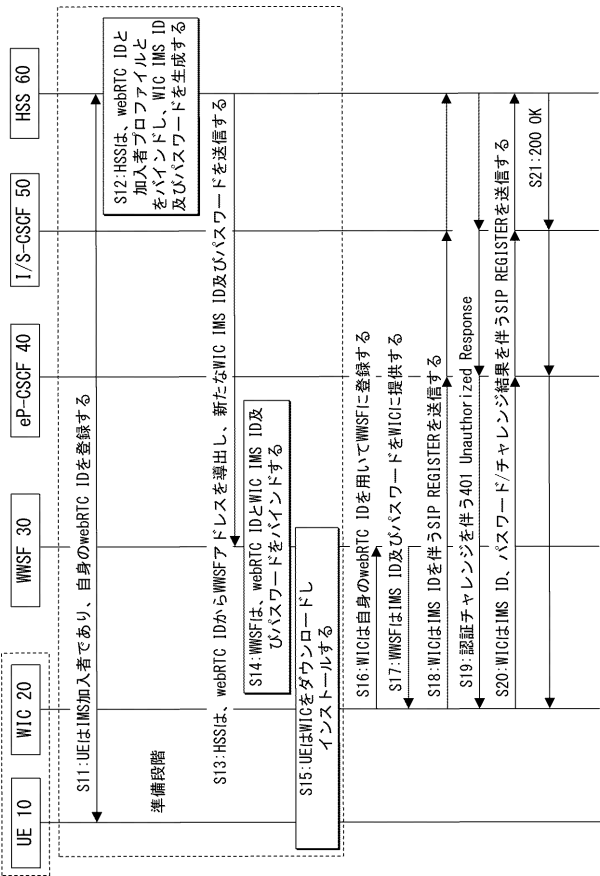
50

1 2 送信部
2 0 W I C
3 0 W W S F
4 0 e P - C S C F
5 0 I / S - C S C F
6 0 H S S
7 0 A A A

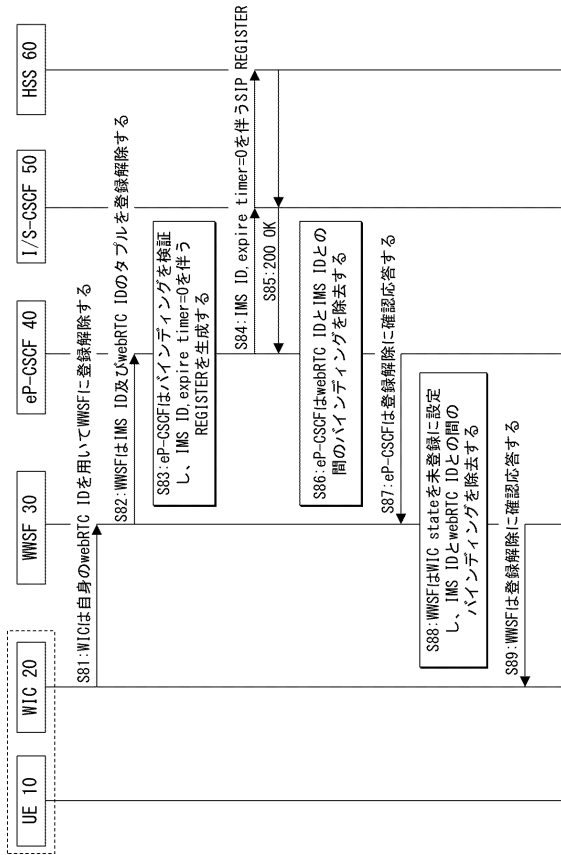
【図 1】



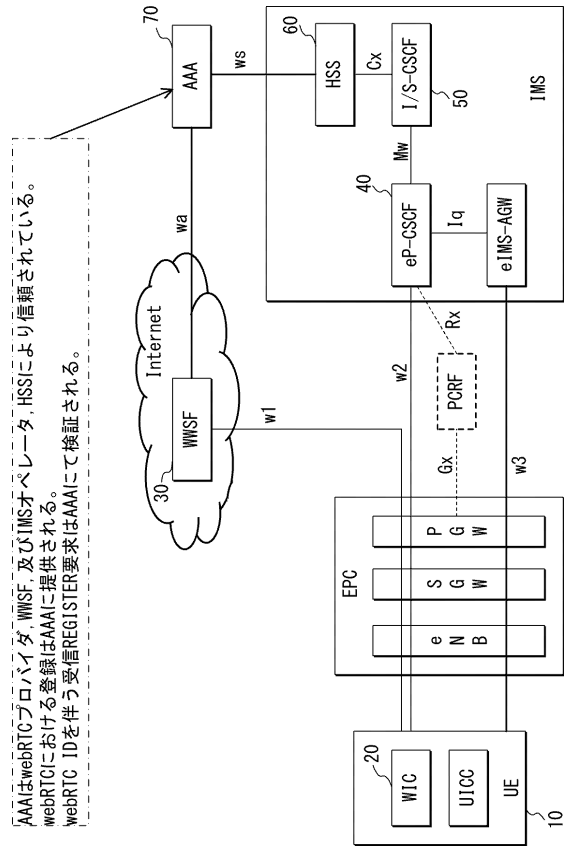
【図 2】



【図 7】

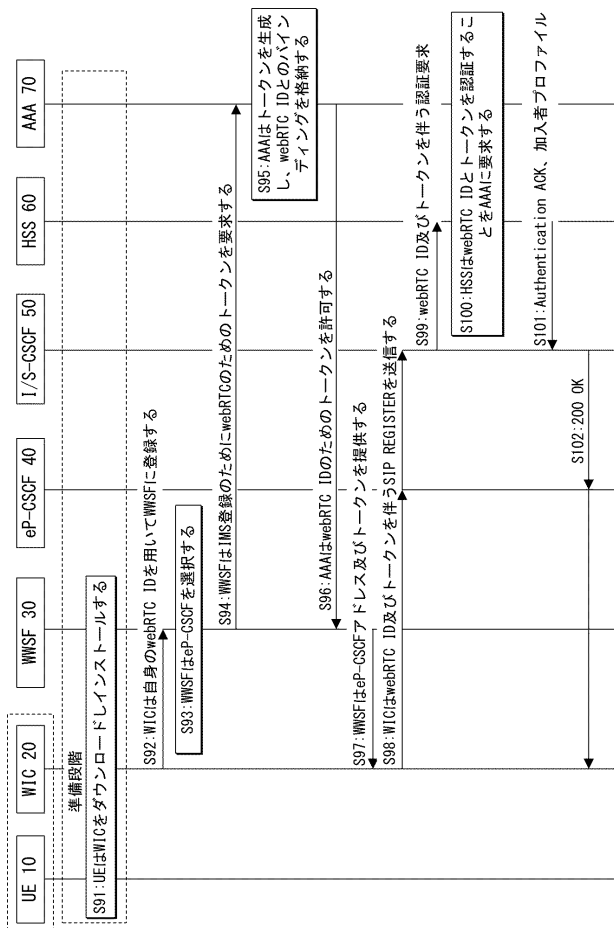


【図 8】

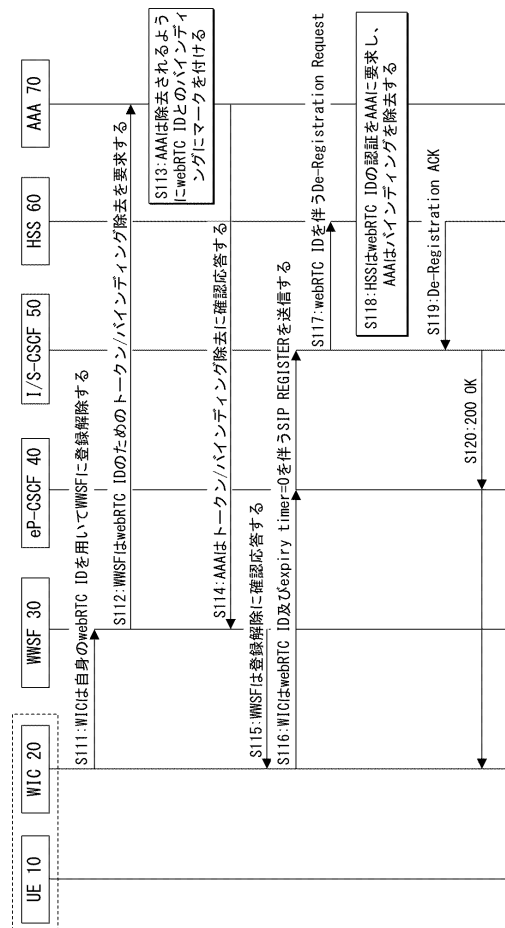


AAAはwebRTCプロバイダ WWSF 及びIMSオペレータ、HSSにより信頼されている。webRTCにおける登録はAAAに提供される。webRTC IDを伴う登録REGISTER要求はAAAにて検証される。

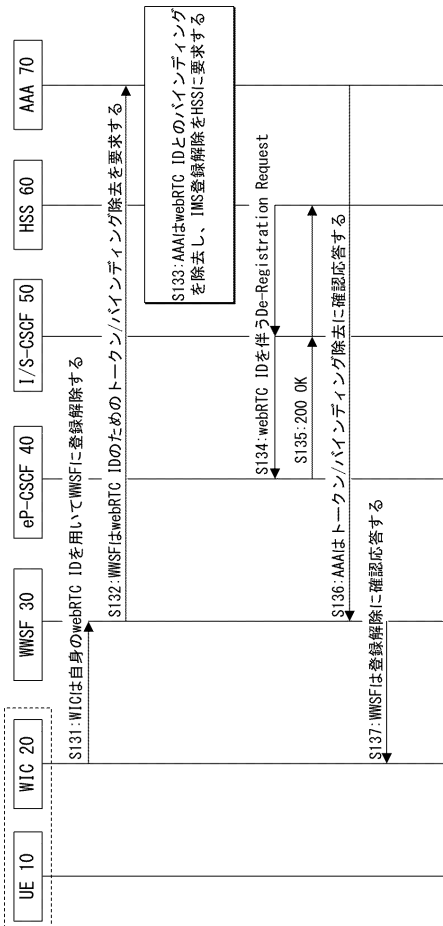
【図 9】



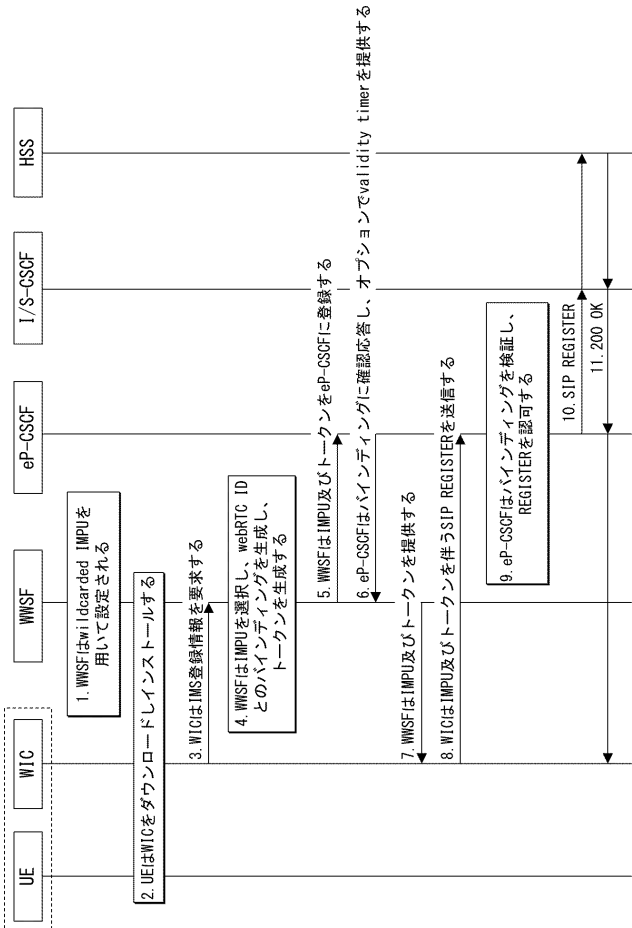
【図 10】



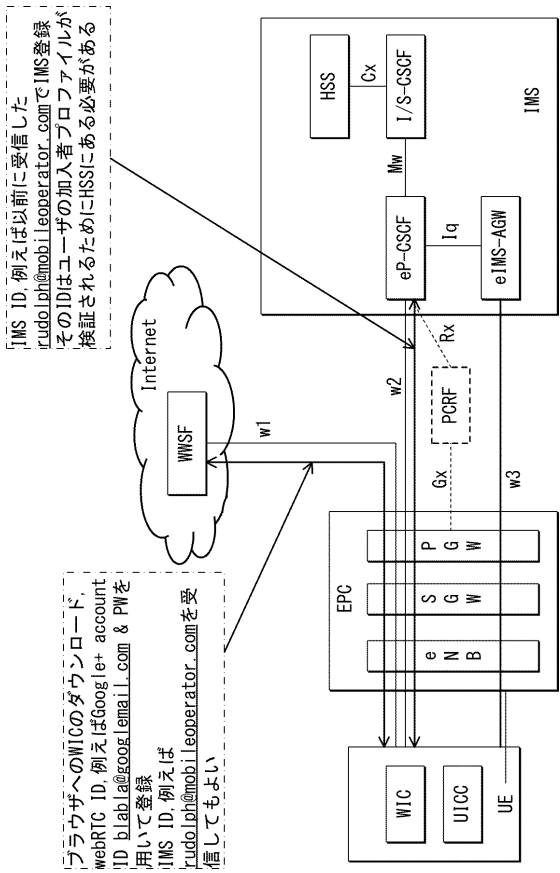
【図 1 1】



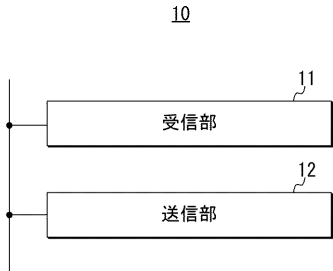
【図 1 3】



【図 1 2】



【図 1 4】



【手続補正書】

【提出日】平成28年6月7日(2016.6.7)

【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】

通信システムにおける認証方法であって、

IMS (IP (Internet Protocol) Multimedia Subsystem) 登録においてWWSF (WebRTC (Web Real Time Communication) Web Server Function) からUE (User Equipment) へトークンを送信することと、

前記トークンを伴うREGISTERメッセージを前記UEからeP-CSCF (enhanced Proxy-CSCF (Call Session Control Function)) へ送信することと、

前記eP-CSCFによって、有効時間を有する前記トークンを検証することと、

前記REGISTERメッセージを前記eP-CSCFからS-CSCF (Serving-CSCF) へ転送することと、

加入者プロフィールをHSS (Home Subscriber Server) から前記S-CSCFへ受信することと、

200 OKメッセージを前記S-CSCFから前記eP-CSCFを介して前記UEへ送信することと、を含む

認証方法。

【請求項2】

前記認証方法の開始にあたって、前記UEによって前記IMS登録のための情報を前記WWSFに要求することをさらに含む、請求項1に記載の認証方法。

【請求項3】

前記WWSFによって前記トークンを認可ノードに要求することをさらに含む、請求項1又は2に記載の認証方法。

【請求項4】

前記WWSFは、前記トークンと共にIMPU (IMS public user identity) を前記UEへ送信し、

前記UEは、前記トークンと共に前記IMPUを伴う前記REGISTERメッセージを前記eP-CSCFへ送信し、

前記eP-CSCFは、前記トークンと共に前記IMPUを検証する、

請求項1～3のいずれか1項に記載の認証方法。

【請求項5】

前記UEは、WIC (WebRTC IMS Client) である、請求項1～4のいずれか1項に記載の認証方法。

【請求項6】

UE (User Equipment) を認証する通信システムであって、

WWSF (WebRTC (Web Real Time Communication) Web Server Function) と、eP-CSCF (enhanced Proxy-CSCF (Call Session Control Function)) と、S-CSCF (Serving-CSCF) と、HSS (Home Subscriber Server) と、を備え、

前記WWSFは、IMS (IP (Internet Protocol) Multimedia Subsystem) 登録においてトークンを前記UEへ送信し、

前記UEは、前記トークンを伴うREGISTERメッセージを前記eP-CSCFへ送信し、

前記eP-CSCFは、有効時間を有する前記トークンを検証し、

前記eP-CSCFは、前記REGISTERメッセージを前記S-CSCFへ転送し、

前記S-CSCFは、加入者プロフィールを前記HSSから受信し、

前記S-CSCFは、200 OKメッセージを前記eP-CSCFを介して前記UEへ送信する、

通信システム。

【請求項7】

前記UEは、前記IMS登録のための情報を前記WSFに要求する、請求項6に記載の通信システム。

【請求項8】

認可ノードをさらに備え、

前記WSFは、前記トークンを前記認可ノードに要求する、

請求項6又は7に記載の通信システム。

【請求項9】

前記WSFは、前記トークンと共にIMPU (IMS public user identity) を前記UEへ送信し、

前記UEは、前記トークンと共に前記IMPUを伴う前記REGISTERメッセージを前記eP-CSCFへ送信し、

前記eP-CSCFは、前記トークンと共に前記IMPUを検証する、

請求項6～8のいずれか1項に記載の通信システム。

【請求項10】

前記UEは、WIC (WebRTC IMS Client) である、請求項6～9のいずれか1項に記載の通信システム。

【請求項11】

UE (User Equipment) の認証方法であって、

IMS (IP (Internet Protocol) Multimedia Subsystem) 登録においてトークンをWSF (WebRTC (Web Real Time Communication) Web Server Function) から受信することと、

有効時間を有する前記トークンを検証してREGISTERメッセージをS-CSCF (Serving-CSCF) へ転送するeP-CSCF (enhanced Proxy-CSCF (Call Session Control Function)) へ、前記トークンを伴う前記REGISTERメッセージを送信することと、

HSS (Home Subscriber Server) から加入者プロフィールを受信する前記S-CSCFから、前記eP-CSCFを介して200 OKメッセージを受信することと、を含む

認証方法。

【請求項12】

前記認証方法の開始にあたって、前記IMS登録のための情報を前記WSFに要求することをさらに含む、請求項11に記載の認証方法。

【請求項13】

前記UEは、前記トークンと共にIMPU (IMS public user identity) を前記WSFから受信し、

前記UEは、前記トークンと共に前記IMPUを検証する前記eP-CSCFへ、前記トークンと共に前記IMPUを伴う前記REGISTERメッセージを送信する、

請求項11又は12に記載の認証方法。

【請求項14】

前記UEは、WIC (WebRTC IMS Client) である、請求項11～13のいずれか1項に記載の認証方法。

【請求項15】

WWSF (WebRTC (Web Real Time Communication) Web Server Function) と、eP-CSCF (enhanced Proxy-CSCF (Call Session Control Function)) と、S-CSCF (Serving-CSCF) と、HSS (Home Subscriber Server) と、を含む通信システムに接続可能なUEであって、

IMS (IP (Internet Protocol) Multimedia Subsystem) 登録においてトークンを前記WWSFから受信し、前記HSSから加入者プロフィールを受信する前記S-CSCFから、前記eP-CSCFを介して200 OKメッセージを受信する受信部と、

有効時間を有する前記トークンを検証してREGISTERメッセージを前記S-CSCFへ転送する前記eP-CSCFへ、前記トークンを伴う前記REGISTERメッセージを送信する送信部と、を備える、

UE。

【請求項16】

前記UEは、前記IMS登録のための情報を前記WWSFに要求する、請求項15に記載のUE。

【請求項17】

前記受信部は、前記トークンと共にIMPU (IMS public user identity) を前記WWSFから受信し、

前記送信部は、前記トークンと共に前記IMPUを検証する前記eP-CSCFへ、前記トークンと共に前記IMPUを伴う前記REGISTERメッセージを送信する、

請求項15又は16に記載のUE。

【請求項18】

前記UEは、WIC (WebRTC IMS Client) である、請求項15～17のいずれか1項に記載のUE。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/JP2014/006334

A. CLASSIFICATION OF SUBJECT MATTER INV. H04L29/08 ADD. H04L29/06		
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 practicable, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Web Real Time Communication (WebRTC) access to IMS (Stage 2) (Release 12)", 3GPP DRAFT; 23701-030 RM, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE 25 November 2013 (2013-11-25), XP050764393, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg_sa/WG2_Arch/Latest_SA2_Specs/Latest_draft_S2_Specs/[retrieved on 2013-11-25] cited in the application paragraph [A.2.1.3]; figures A.2.1.3-1 -/--	1-18
☒ Further documents are listed in the continuation of Box C. ☐ 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 application or patent 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
29 April 2015		08/05/2015
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Gioe', Pietro

INTERNATIONAL SEARCH REPORT

International application No

PCT/JP2014/006334

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	paragraph [6.3.2.1.3]; figures 6.3.2.1.3-1 paragraph [6.5.2.1.2.1]; figures 6.5.2.1.2.1-1 ----- "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Security for WebRTC IMS Client access to IMS; (Release 12)", 3GPP DRAFT; 33ABC-010 V1 RM, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE 21 November 2013 (2013-11-21), XP050766138, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_73_SanFrancisco/Drafts/ [retrieved on 2013-11-21] cited in the application paragraph [6.2.1] -----	1-18
A	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services (Release 12)", 3GPP STANDARD; 3GPP TS 33.203, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG3, no. V12.3.0, 19 September 2013 (2013-09-19), pages 1-122, XP050712660, [retrieved on 2013-09-19] page 109 - page 111 -----	1-18

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US

(72)発明者 プラサド アナンド ラガワ

東京都港区芝五丁目7番1号 日本電気株式会社内

Fターム(参考) 5K201 AA02 AA09 BB03 BC23 CA01 CA04 CA07 CC02 CC04 EA05
EA07 EC06 ED04