

(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2014-509162

(P2014-509162A)

(43) 公表日 平成26年4月10日(2014.4.10)

(51) Int.Cl.	F I	テーマコード (参考)
H04L 9/32 (2006.01)	H04L 9/00 675B	5J104
G06F 21/44 (2013.01)	H04L 9/00 673B	
	G06F 21/20 144C	

審査請求 有 予備審査請求 未請求 (全 15 頁)

(21) 出願番号	特願2013-557929 (P2013-557929)	(71) 出願人	507364838
(86) (22) 出願日	平成24年3月9日 (2012.3.9)		クアルコム, インコーポレイテッド
(85) 翻訳文提出日	平成25年9月27日 (2013.9.27)		アメリカ合衆国 カリフォルニア 921
(86) 国際出願番号	PCT/US2012/028611		21 サン ディエゴ モアハウス ドラ
(87) 国際公開番号	W02012/122529		イブ 5775
(87) 国際公開日	平成24年9月13日 (2012.9.13)	(74) 代理人	100108453
(31) 優先権主張番号	61/450,956		弁理士 村山 靖彦
(32) 優先日	平成23年3月9日 (2011.3.9)	(74) 代理人	100163522
(33) 優先権主張国	米国 (US)		弁理士 黒田 晋平
(31) 優先権主張番号	13/213,401	(72) 発明者	アナンド・パラニグンダー
(32) 優先日	平成23年8月19日 (2011.8.19)		アメリカ合衆国・カリフォルニア・921
(33) 優先権主張国	米国 (US)		21・サン・ディエゴ・モアハウス・ドラ
			イブ・5775

最終頁に続く

(54) 【発明の名称】 セキュアエレメントを用いたリモート局の認証方法

(57) 【要約】

セキュアエレメントを用いた管理局によるリモート局の認証方法が開示される。この方法では、リモート局は、セキュアエレメントからID要求を受信する。このID要求には、管理局によってセキュアエレメントに提供された第1のチャレンジが含まれる。リモート局は、ID応答をセキュアエレメントに転送する。このID応答には、リモート局の鍵によって署名された第1のチャレンジに対する応答が含まれ、第1のチャレンジに対する署名された応答は、リモート局を認証するために管理局が用いるためのものである。

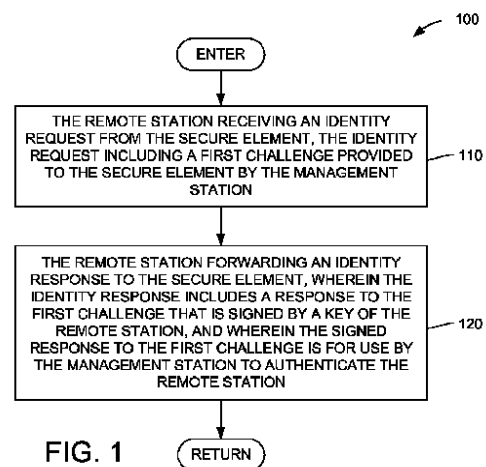


FIG. 1

【特許請求の範囲】**【請求項 1】**

セキュアエレメントを用いた管理局によるリモート局の認証方法であって、
前記管理局によって前記セキュアエレメントに提供された第1のチャレンジを含むID要求を、前記リモート局が前記セキュアエレメントから受信するステップと、
前記リモート局を認証するために前記管理局が用いるための、前記リモート局の鍵によって署名された前記第1のチャレンジに対する応答を含むID応答を、前記リモート局が前記セキュアエレメントに転送するステップと
を含む、認証方法。

【請求項 2】

前記セキュアエレメントが、前記リモート局に組み込まれたスマートカードである、請求項1に記載の認証方法。

【請求項 3】

前記セキュアエレメントが、前記リモート局から取外し可能なスマートカードである、請求項1に記載の認証方法。

【請求項 4】

前記セキュアエレメントが、前記リモート局に内蔵されたトラステッドプロセッサモジュールである、請求項1に記載の認証方法。

【請求項 5】

前記リモート局がワイヤレスモバイルデバイスである、請求項1に記載の認証方法。

【請求項 6】

前記リモート局の前記鍵が、前記管理局にとって利用可能な公開鍵に対応する私有鍵である、請求項1に記載の認証方法。

【請求項 7】

前記ID応答が、前記公開鍵を含む証明書を含む、請求項6に記載の認証方法。

【請求項 8】

前記リモート局の前記鍵が、前記管理局によって共有される秘密鍵である、請求項1に記載の認証方法。

【請求項 9】

前記ID応答が、前記リモート局に固有のID値を含む、請求項1に記載の認証方法。

【請求項 10】

前記第1のチャレンジが第1のナンスである、請求項1に記載の認証方法。

【請求項 11】

前記ID応答が、前記管理局を認証する際に用いるために前記リモート局によって生成された第2のチャレンジを含む、請求項1に記載の認証方法。

【請求項 12】

リモート局であって、
管理局によってセキュアエレメントに提供された第1のチャレンジを含むID要求を前記セキュアエレメントから受信するための手段と、
前記リモート局を認証するために前記管理局が用いるための、前記リモート局の鍵によって署名された前記第1のチャレンジに対する応答を含むID応答を前記セキュアエレメントに転送するための手段と
を含む、リモート局。

【請求項 13】

前記セキュアエレメントが、前記リモート局に組み込まれたスマートカードである、請求項12に記載のリモート局。

【請求項 14】

前記セキュアエレメントが、前記リモート局から取外し可能なスマートカードである、請求項12に記載のリモート局。

【請求項 15】

前記セキュアエレメントが、前記リモート局に内蔵されたトラステッドプロセッサモジュールである、請求項12に記載のリモート局。

【請求項16】

前記リモート局がワイヤレスモバイルデバイスである、請求項12に記載のリモート局。

【請求項17】

前記リモート局の前記鍵が、前記管理局にとって利用可能な公開鍵に対応する私有鍵である、請求項12に記載のリモート局。

【請求項18】

前記ID応答が、前記公開鍵を含む証明書を含む、請求項17に記載のリモート局。

【請求項19】

前記リモート局の前記鍵が、前記管理局によって共有される秘密鍵である、請求項12に記載のリモート局。

【請求項20】

前記ID応答が、前記リモート局に固有のID値を含む、請求項12に記載のリモート局。

【請求項21】

前記第1のチャレンジが第1のナンスである、請求項12に記載のリモート局。

【請求項22】

前記ID応答が、前記管理局を認証する際に用いるために前記リモート局によって生成された第2のチャレンジを含む、請求項12に記載のリモート局。

【請求項23】

リモート局であって、

管理局によってセキュアエレメントに提供された第1のチャレンジを含むID要求を前記セキュアエレメントから受信し、

前記リモート局を認証するために前記管理局が用いるための、前記リモート局の鍵によって署名された前記第1のチャレンジに対する応答を含むID応答を前記セキュアエレメントに転送する

ように構成されたプロセッサと、

前記リモート局の前記鍵を記憶するように構成されたメモリと

を含む、リモート局。

【請求項24】

前記セキュアエレメントが、前記リモート局に組み込まれたスマートカードである、請求項23に記載のリモート局。

【請求項25】

前記セキュアエレメントが、前記リモート局から取外し可能なスマートカードである、請求項23に記載のリモート局。

【請求項26】

前記セキュアエレメントが、前記リモート局に内蔵されたトラステッドプロセッサモジュールである、請求項23に記載のリモート局。

【請求項27】

前記リモート局がワイヤレスモバイルデバイスである、請求項23に記載のリモート局。

【請求項28】

前記リモート局の前記鍵が、前記管理局にとって利用可能な公開鍵に対応する私有鍵である、請求項23に記載のリモート局。

【請求項29】

前記ID応答が、前記公開鍵を含む証明書を含む、請求項28に記載のリモート局。

【請求項30】

前記リモート局の前記鍵が、前記管理局によって共有される秘密鍵である、請求項23に記載のリモート局。

【請求項31】

前記ID応答が、前記リモート局に固有のID値を含む、請求項23に記載のリモート局。

10

20

30

40

50

【請求項 3 2】

前記第1のチャレンジが第1のナンスである、請求項23に記載のリモート局。

【請求項 3 3】

前記ID応答が、前記管理局を認証する際に用いるために前記リモート局によって生成された第2のチャレンジを含む、請求項23に記載のリモート局。

【請求項 3 4】

管理局によってセキュアエレメントに提供された第1のチャレンジを含むID要求を、コンピュータに前記セキュアエレメントから受信させるためのコードと、
前記コンピュータを認証するために前記管理局が用いるための、前記コンピュータに関連する鍵によって署名された前記第1のチャレンジに対する応答を含むID応答を、コンピュータに前記セキュアエレメントに転送させるためのコードと
を含む、コンピュータプログラム。

10

【請求項 3 5】

前記セキュアエレメントがスマートカードである、請求項34に記載のコンピュータプログラム。

【請求項 3 6】

前記セキュアエレメントが取外し可能なスマートカードである、請求項34に記載のコンピュータプログラム。

【請求項 3 7】

前記セキュアエレメントがトラステッドプロセッサモジュールである、請求項34に記載のコンピュータプログラム。

20

【請求項 3 8】

前記鍵が、前記管理局にとって利用可能な公開鍵に対応する私有鍵である、請求項34に記載のコンピュータプログラム。

【請求項 3 9】

前記鍵が、前記管理局によって共有される秘密鍵である、請求項34に記載のコンピュータプログラム。

【請求項 4 0】

前記第1のチャレンジが第1のナンスである、請求項34に記載のコンピュータプログラム。

30

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

関連出願の相互参照

本出願は、参照によって本明細書に組み込まれている、2011年3月9日に提出された米国仮出願第61/450,956号の利益を主張するものである。

【0 0 0 2】

本発明は、概してリモート局の認証に関する。

【背景技術】

【0 0 0 3】

リモート局は、ワイヤレスネットワークのオペレータによって提供されるユーザサービスをホスティングすることができる。GSM(登録商標)、UMTS、LTE、およびcdma2000のシステムでは、ユーザサービスはスマートカードを用いて可能となり得る。スマートカードの例は、ユニバーサル集積回路カード(UICC)であってもよい。UICCは取外し可能であってもよく、別の局または別のデバイスに移すことができる。ワイヤレスネットワークのオペレータは、ホスティングするリモート局の認証を過度の出費をせずに望むことがある。

40

【発明の概要】

【発明が解決しようとする課題】

【0 0 0 4】

したがって、リモート局を認証するための効果的な技術が必要とされている。

50

【課題を解決するための手段】

【0005】

本発明における一態様は、セキュアエレメントを用いた管理局によるリモート局の認証方法にあり得る。この方法では、リモート局は、セキュアエレメントからID要求を受信する。このID要求には、管理局によってセキュアエレメントに提供された第1のチャレンジが含まれる。リモート局は、ID応答をセキュアエレメントに転送する。このID応答には、リモート局の鍵によって署名された第1のチャレンジに対する応答が含まれる。第1のチャレンジに対する署名された応答は、リモート局を認証するために管理局が用いるためのものである。

【0006】

本発明におけるより詳細な態様では、セキュアエレメントは、リモート局に組み込まれ、そのリモート局から取外し可能なスマートカードでもよく、または、リモート局に内蔵されたトラステッドプロセッサモジュール(Trusted Processor Module)でもよい。リモート局は、ワイヤレスモバイルデバイスでもよい。リモート局の鍵は、管理局にとって利用可能な公開鍵に対応する私有鍵でもよく、ID応答は、公開鍵を含む証明書を含み得る。あるいは、リモート局の鍵は、管理局によって共有される秘密鍵でもよい。ID応答は、リモート局に固有のID値を含み得る。第1のチャレンジは、第1のナンスでもよい。また、ID応答は、管理局を認証する際に用いるためにリモート局によって生成された第2のチャレンジを含み得る。

【0007】

本発明における別の態様は、管理局によってセキュアエレメントに提供された第1のチャレンジを含むID要求をセキュアエレメントから受信するための手段と、リモート局を認証するために管理局が用いるための、リモート局の鍵によって署名された第1のチャレンジに対する応答を含むID応答をセキュアエレメントに転送するための手段とを含み得るリモート局にあり得る。

【0008】

本発明における別の態様は、管理局によってセキュアエレメントに提供された第1のチャレンジを含むID要求をセキュアエレメントから受信するように構成されているとともに、リモート局を認証するために管理局が用いるための、リモート局の鍵によって署名された第1のチャレンジに対する応答を含むID応答をセキュアエレメントに転送するように構成されたプロセッサと、リモート局の鍵を記憶するように構成されたメモリとを含み得るリモート局にあり得る。

【0009】

本発明における別の態様は、管理局によってセキュアエレメントに提供された第1のチャレンジを含むID要求を、コンピュータにセキュアエレメントから受信させるためのコードと、コンピュータを認証するために管理局が用いるための、コンピュータに関連する鍵によって署名された第1のチャレンジに対する応答を含むID応答を、コンピュータにセキュアエレメントに転送させるためのコードとを含むコンピュータ可読記憶媒体を備えるコンピュータプログラム製品にあり得る。

【図面の簡単な説明】

【0010】

【図1】本発明による、セキュアエレメントを用いた管理局によるリモート局の認証方法の流れ図である。

【図2】セキュアエレメントを用いた管理局によるリモート局の認証のためのコールフローの流れ図である。

【図3】プロセッサとメモリとを含むコンピュータのブロック図である。

【図4】ワイヤレス通信システムの一例におけるブロック図である。

【発明を実施するための形態】

【0011】

「例示的」という語は、本明細書では「例、実例、または具体例として働く」ことを意

10

20

30

40

50

味するように用いられている。「例示的」として本明細書で説明される任意の実施形態は、他の実施形態に比べて好ましいか、または有利であると必ずしも解釈されるべきではない。

【0012】

図1および図2を参照すると、本発明の一態様は、セキュアエレメント230を用いた管理局220によるリモート局210の認証方法100にあり得る。この方法では、リモート局は、セキュアエレメントからID要求REQ IDを受信する(ステップ110)。このID要求には、管理局によってセキュアエレメントに提供された第1のチャレンジ(N1)が含まれる。リモート局は、ID応答ID RESをセキュアエレメントに転送する(ステップ120)。このID応答には、リモート局の鍵Kによって署名された第1のチャレンジに対する応答が含まれる。署名された応答は、リモート局を認証するために管理局が使用するためのものである。

10

【0013】

本発明におけるより詳細な態様では、セキュアエレメント230は、リモート局210に組み込まれ、そのリモート局から取外し可能なスマートカードでもよく、または、リモート局に内蔵されたトラステッドプロセッサモジュールでもよい。リモート局は、ワイヤレスデバイスなどのモバイルユーザ機器(UE)を含み得る。リモート局の鍵Kは、管理局にとって利用可能な公開鍵に対応する私有鍵 K_{PRI} でもよく、ID応答は、公開鍵を含む証明書CERTを含み得る。あるいは、リモート局の鍵は、管理局220によって共有される秘密鍵 K_{SH} でもよい。ID応答は、国際移動体装置識別番号(IMEI)、または、移動体装置識別番号(MEID)、または、リモート局を常に一意に識別する任意の他のIDなどの、リモート局に固有のID値を含み得る。そのようなIDの他の例には、限定されないが、EUI-48もしくはEUI-64などのIEEEによって割り当てられたハードウェア識別子、または、リモート局の製造業者によって割り当てられたハードウェア識別子が含まれ得る。第1のチャレンジN1は、第1のナンスでもよい。また、ID応答は、管理局を認証する際に用いるためにリモート局によって生成された、第2のナンスなどの第2のチャレンジを含み得る。

20

【0014】

さらに図3を参照すると、本発明における別の態様は、リモート局210にあり得る。このリモート局210は、手段(プロセッサ310)を含むことができ、この手段310は、管理局によってセキュアエレメントに提供された第1のチャレンジを含むID要求をセキュアエレメントから受信するためのものであり、さらに、リモート局を認証するために管理局が用いるための、リモート局の鍵によって署名された第1のチャレンジに対する応答を含むID応答をセキュアエレメントに転送するためのものである。

30

【0015】

本発明における別の態様は、リモート局210にあり得る。このリモート局210は、管理局によってセキュアエレメントに提供された第1のチャレンジを含むID要求をセキュアエレメントから受信するように構成されているとともに、リモート局を認証するために管理局が用いるための、リモート局の鍵によって署名された第1のチャレンジに対する応答を含むID応答をセキュアエレメントに転送するように構成されたプロセッサ310と、リモート局の鍵を記憶するように構成されたメモリとを含み得る。

40

【0016】

本発明における別の態様は、コンピュータプログラム製品にあり得る。このコンピュータプログラム製品は、管理局によってセキュアエレメントに提供された第1のチャレンジを含むID要求を、コンピュータ300にセキュアエレメントから受信させるためのコードと、コンピュータを認証するために管理局が用いるための、コンピュータに関連する鍵によって署名された第1のチャレンジに対する応答を含むID応答を、コンピュータにセキュアエレメントに転送させるためのコードとを含む非一時的なコンピュータ可読記憶媒体320を備えている。

【0017】

リモート局210またはリモート装置は、プロセッサ310と、メモリおよび/またはディスクドライブなどの記憶媒体320と、セキュアモジュール330とを含むコンピュータ300、デ

50

イスプレイ340、たとえばキーボード350と、マイクロホンと、スピーカと、カメラとである入力デバイスなどを含み得る。リモート局は、ワイヤレス接続360を含み得る。さらに、リモート局は、USB、イーサネット(登録商標)、および類似のインターフェースも含み得る。

【0018】

図2を再度参照すると、高レベルのコールフロー200は、管理局220によるホストリモート局の認証のための手順を示している。セキュアエレメント230は、リモート局210に取り付けられ、管理局のアドレスをプロビジョニングされたスマートカードでもよい。リモート局は、たとえば、3GPPのTS33.320などのトラステッド環境(TrE)である、セキュア記憶および実行環境330を有する、モバイル機器などのホストモジュールでもよい。リモート局は、デバイスIDとしてのIMEIなどのデバイスクレデンシャルと、安全に記憶されたデバイスの私有鍵、または共有の秘密鍵とをプロビジョニングされてもよい。デバイスの私有鍵に対応する公開鍵は、デバイスの私有鍵を用いてなされた署名の検証を望む者に(たとえば、証明書CERTから)アクセス可能であってもよい。共有の秘密鍵が用いられる場合には、その秘密鍵が同様に管理局によって安全に記憶されることになる。管理局は、ネットワークアクセスアプリケーション(NAA)をセキュアエレメントに提供するセキュアエレメントマネージャ(secure element manager)でもよい。NAAは、ワイヤレスネットワークまたはワイヤラインネットワークなどのアクセスネットワークからサービスを得るために用いられる。

【0019】

たとえば、セキュアエレメント230は、導入前にネットワークオペレータのデータでカスタマイズされてはいけないスマートカード(たとえば、SIM、UICC/eUICC、またはR-UIM)またはトラステッドプロセッサモジュール(TPM)でもよい。スマートカードまたはTPMは、それらにネットワークアクセスのクレデンシャル情報がプロビジョニングされる前に、それらが証明および/または認証されたホスト(セルラーモジュール/モバイル機器)に取り付けられていることを検証することが望ましい場合がある。また、ネットワークのオペレータは、スマートカードまたはTPMがホストリモート局210に依然として取り付けられていることを定期的に検証することを望む場合がある。たとえば、ネットワークのオペレータは、ネットワークアクセスを不正に受け入れるか、または、ネットワークのオペレータもしくは政府当局の追跡を避ける認証されていない別のホストリモート局と、スマートカードまたはTPMとのペアリング(pairing)の防止を望む場合がある。スマートカードまたはTPMを用いることによって、特定のトランスポートアクセスネットワーク(すなわち、LTE/UMTS、cdma2000、または、そのような他のワイヤレスアクセスネットワーク、もしくはさらにワイヤラインアクセスネットワーク)のプロトコルに対する変更を要することなく、ホストリモート局の認証が可能となり得る。

【0020】

ホストリモートデバイスのIDは、デバイスの私有鍵/公開鍵のペア、または共有の秘密鍵に関連し得る任意のデバイスIDでもよい。IMEIに加えて、他の例には、MEID、EUI-64、EUI-48、または任意である他の固有のデバイスIDが含まれ得る。

【0021】

管理局220は、セキュアエレメント230に対するオーバージエア(OTA)管理プラットフォームを動作させるエンティティでもよい。セキュアエレメントは、ETSI SCP/3GPPによって規定された既存のUICC/SIMカードのプロトコルを用いてもよく、または、グローバルプラットフォームのプロトコルもしくは他の好適なプロトコルを用いてもよい。

【0022】

コールフロー200では、セキュアエレメント230は、リモート局210との接続を開き、管理局220とのトランスポート接続(transport connection)の確立をリモート局に要求することができる(ステップ250)。セキュアエレメントとリモート局との間の接続は、セキュアエレメントとリモート局との間に挿入される攻撃者からの攻撃を防止するように安全に保護され得る。リモート局は、管理局とのトランスポート接続を確立するためにトランス

ポートシステム240を選択する(ステップ252)。このトランスポートシステムは、ワイヤレスワイドエリアアクセスネットワークWWAN(たとえば、cdma2000、または、GSM/GPRS/UMTS/LTEなどの3GPPのアクセスシステム)でもよく、ワイヤレスローカルエリアネットワークWLAN(たとえば、IEEE802.11a/b/g/nのワイヤレスネットワーク)でもよく、または、固定ネットワーク(たとえば、PSTN、xDSL、ケーブル、イーサネット(登録商標)、ファイバ)によって提供される固定IPサービスでもよい。トランスポート接続は、IP、またはSMS、またはそのような任意のトランスポートプロトコルを用いることができる。トランスポート接続が確立される(ステップ254)。セキュアエレメントおよび管理局220は、プロビジョニングまたは管理メッセージ交換のためにトランスポートプロトコルを介して安全につながる
10
ことができる(ステップ256)。セキュアエレメントと管理局との間でトランスポートされるメッセージは、認証されたHTTPS/TLS、または、暗号および/もしくは完全性(integrity)によって強化されたSMSなどを用いて、暗号化されてもよく、ならびに完全性をもって保護されてもよい。

【0023】

管理局220は、署名されたホストリモート局のIDの要求を求める要求REQ ID REQをセキュアエレメント230に送る(ステップ258)。この要求はナンスN1を含む。セキュアエレメントは、ナンスN1を含む、署名されたホストリモート局のIDを求める要求をホストリモート局210に送る(ステップ260)。リモート局は、自身のID(たとえば、自身のIMEI)、ナンス、および署名を含む、署名されたID応答ID RESをセキュアエレメントに返す(ステップ262)。
20
署名されたID応答は、管理局を認証するためのチャレンジとして第2のナンスN2をさらに含み得る。署名は、リモート局を認証するために管理局が使用するためのものである。

【0024】

リモート局210は、私有鍵/公開鍵のペアを用いる場合には、メッセージのハッシュ値を求め、それを私有鍵を用いて暗号化する。管理局220は、リモート局を認証するためにリモート局の公開鍵を用いて、暗号化されたハッシュを復号化する(ステップ266)。メッセージの完全性は、受信したメッセージのハッシュ値を再度求め、それを署名ハッシュと比較することによって検証される。

【0025】

リモート局210は、共有の秘密鍵を用いる場合には、共有鍵を用いて署名(MAC)を生成する(MAC=HMAC(共有鍵、メッセージ))。管理局220は、共有鍵を用いて署名(MAC)を再度生成し、それを受信したMACと比較する(ステップ266)。次いで、受信したIDによってホストリモート局が特定される。
30

【0026】

ホストリモート局210の認証が成功した後、管理局220は、次いで、リモート局にサービスを提供するためのNAAまたは他のクレデンシャルをセキュアエレメント230に安全にプロビジョニングし、そのセキュアエレメント230をアクティブ化することができる(ステップ268)。ホストリモート局の認証が失敗した場合、管理局は、そのリモート局をブラックリストに載せ、サービスプロバイダからのサービスを得るためにリモート局によって必要とされるNAAまたは他のクレデンシャル情報をそのリモート局にプロビジョニングしないように
40
することができる。また、管理局は、ホストリモート局による、ネットワークアクセスのクレデンシャル情報の使用を、その情報がセキュアエレメントに存在する場合には許可しないようにセキュアエレメントに命令することもできる。

【0027】

管理局220は、ホストリモート局の認証を定期的に要求することができる。たとえば、管理局は、進行中の管理セッションの間における認証を要求することができる。あるいは、管理局は、セキュアエレメント230におけるポリシーを構成して、構成された時間の終了時、ホストリモート局において変更を検出した時(たとえば、新たなデバイスがペアリングされた時)、または、ホストリモート局における毎回の電源投入時に、認証ステップ
50
を実行することができる。

【0028】

10

20

30

40

50

図4を参照すると、ワイヤレスリモート局(RS)402(またはUE)は、ワイヤレス通信システム400における1つまたは複数の基地局(BS)404と通信することができる。さらに、RSは、ワイヤレスピアデバイスとペアになってもよい。ワイヤレス通信システム400は、1つまたは複数の基地局コントローラ(BSC)406と、コアネットワーク408とをさらに含んでもよい。コアネットワークは、好適なバックホールを介して、インターネット410および公衆交換電話網(PSTN)412に接続されていてもよい。典型的なワイヤレス移動局は、携帯電話またはラップトップコンピュータを含み得る。ワイヤレス通信システム400は、符号分割多元接続(CDMA)、時間分割多元接続(TDMA)、周波数分割多元接続(FDMA)、空間分割多元接続(SDMA)、偏波分割多元接続(PDMA)、または当技術分野で知られている他の変調技術などの、いくつかの多元接続技術のうちのいずれか1つを用いてもよい。

10

【0029】

当業者は、情報および信号が、様々な異なる技術および技法のいずれかを用いて表され得ることを理解するであろう。たとえば、上記の説明全体にわたって言及され得るデータ、命令、コマンド、情報、信号、ビット、シンボル、およびチップは、電圧、電流、電磁波、磁界または磁性粒子、光場または光学粒子、あるいはそれらの任意の組合せによって表されてもよい。

【0030】

さらに、当業者は、本明細書で開示された実施形態に関連して説明された様々な例示的な論理ブロック、モジュール、回路、およびアルゴリズムのステップが、電子的なハードウェア、コンピュータのソフトウェア、または両方の組合せとして実装され得ることを理解するであろう。例示的な様々な構成要素、ブロック、モジュール、回路、およびステップは、ハードウェアおよびソフトウェアにおけるこの互換性を明確に示すために、それらの機能に関して上記では概略的に説明されている。そのような機能をハードウェアとして実装するか、またはソフトウェアとして実装するかは、特定の用途と、システム全体に課された設計の制約とに依存する。当業者は、説明された機能を特定の用途ごとに様々な方法で実施することができるが、そのような実施の決定は、本発明の範囲からの逸脱を生じさせるものと解釈されるべきではない。

20

【0031】

本明細書で開示された実施形態に関連して説明された例示的な様々な論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理デバイス、ディスクリートゲートもしくはトランジスタロジック、ディスクリートのハードウェア部品、または、本明細書で説明された機能を実行するように設計されたそれらの任意の組合せによって実施または実行されてもよい。汎用プロセッサは、マイクロプロセッサでもよいが、代替として、そのプロセッサは、従来の任意のプロセッサ、コントローラ、マイクロコントローラ、またはステートマシンでもよい。また、プロセッサは、コンピューティングデバイスの組合せ、たとえば、DSPとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つまたは複数のマイクロプロセッサ、あるいはそのような任意の他の構成として実装されてもよい。

30

【0032】

本明細書で開示された実施形態に関連して説明された方法またはアルゴリズムのステップは、ハードウェアで直接実施されてもよく、プロセッサによって実行されるソフトウェアモジュールで実施されてもよく、またはその2つの組合せで実施されてもよい。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、取外し可能ディスク、CD-ROM、または当技術分野で知られている任意の他の形態の記憶媒体の中にあってもよい。例示的な記憶媒体は、記憶媒体から情報を読み出し、記憶媒体に情報を書き込むことができるプロセッサに接続されている。代替形態では、記憶媒体はプロセッサと一体であってもよい。プロセッサおよび記憶媒体は、ASICの中にあってもよい。ASICはユーザ端末の中にあってもよい。代替形態では、プロセッサおよび記憶媒体は、ユーザ端末の中にディスクリート部品としてあって

40

50

もよい。

【0033】

1つまたは複数の例示的实施形態では、説明された機能は、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組合せで実装されてもよい。コンピュータプログラム製品としてソフトウェアで実装される場合、機能は、1つもしくは複数の命令またはコードとしてコンピュータ可読媒体に記憶されるか、あるいはコンピュータ可読媒体を介して送信されてもよい。コンピュータ可読媒体は、ある場所から別の場所へのコンピュータプログラムの転送を容易にする任意の媒体を含む、コンピュータ記憶媒体とコンピュータ通信媒体の両方を含む。記憶媒体は、コンピュータによってアクセスされ得る任意の利用可能な媒体でもよい。限定ではなく例として、そのようなコンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMもしくは他の光ディスクストレージ、磁気ディスクストレージもしくは他の磁気ストレージデバイス、または、命令もしくはデータ構造の形態の所望のプログラムコードを伝送もしくは記憶するために使用でき、またコンピュータによってアクセスされ得る任意の他の媒体を含み得る。また、正確にはいかなる接続もコンピュータ可読媒体と呼ばれる。たとえば、ソフトウェアが、同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者回線(DSL)、または赤外線、無線、およびマイクロ波などのワイヤレス技術を用いて、ウェブサイト、サーバ、または他のリモートソースから送信される場合、同軸ケーブル、光ファイバケーブル、ツイストペア、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、媒体の定義に含まれる。本明細書で用いられる場合、ディスク(disk)およびディスク(disc)は、コンパクトディスク(CD)、レーザーディスク、光ディスク、デジタル多用途ディスク(DVD)、フレキシブルディスク、およびブルーレイディスクを含み、このうちディスク(disk)は、通常、データを磁氣的に再生し、ディスク(disc)は、データをレーザーで光学的に再生する。上記の組合せもコンピュータ可読媒体の範囲の中に含まれるべきである。

【0034】

開示された実施形態における上記の説明は、いかなる当業者も本発明を製造または使用することができるように提供されている。これらの実施形態に対する様々な変更は、当業者には容易に明らかとなり、本明細書で定義される全体的な原理は、本発明の趣旨および範囲から逸脱することなく他の実施形態に適用され得る。したがって、本発明は、本明細書で示された実施形態に限定されるようには考えられておらず、本明細書で開示された原理および新規性のある特徴と矛盾することのない最も広い範囲を与えられるべきである。

【符号の説明】

【0035】

- 100 方法
- 200 コールフロー
- 210 リモート局
- 220 管理局
- 230 セキュアエレメント
- 240 トランスポートシステム
- 300 コンピュータ
- 310 プロセッサ
- 320 記憶媒体
- 330 セキュアモジュール
- 400 ワイヤレス通信システム
- 402 ワイヤレスリモート局
- 404 基地局
- 406 基地局コントローラ
- CERT 証明書
- K 鍵
- K_{PRI} 私有鍵

10

20

30

40

50

K_{SH}

秘密鍵

N1

第1のチャレンジ

N2

第2のチャレンジ

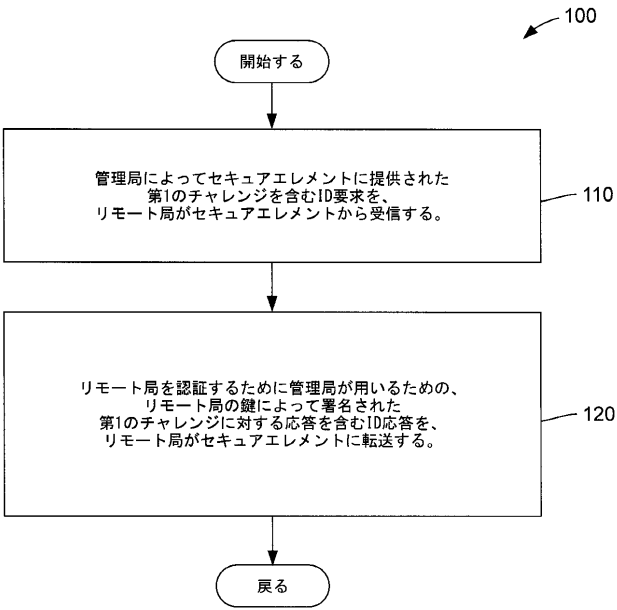
REQ ID

ID要求

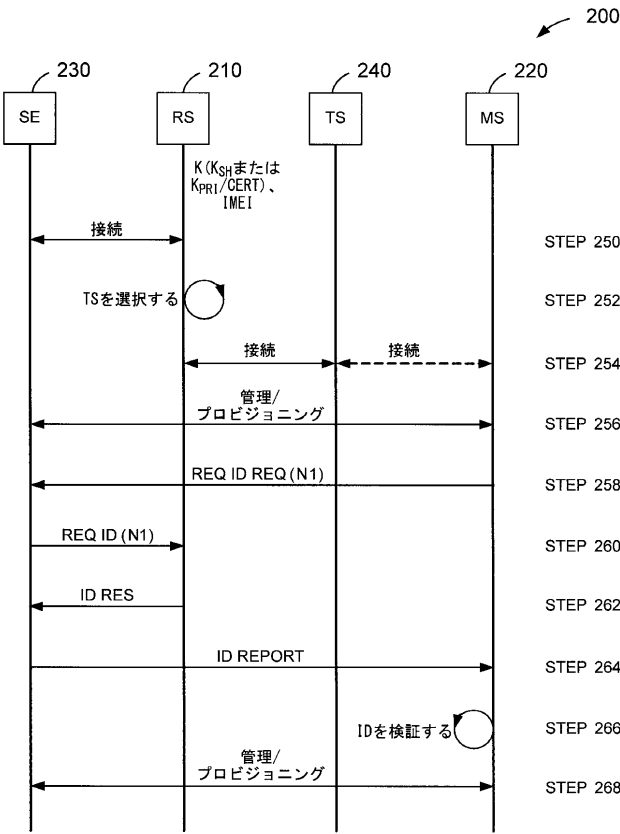
ID RES

ID応答

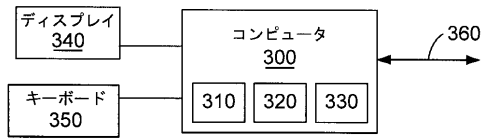
【 図 1 】



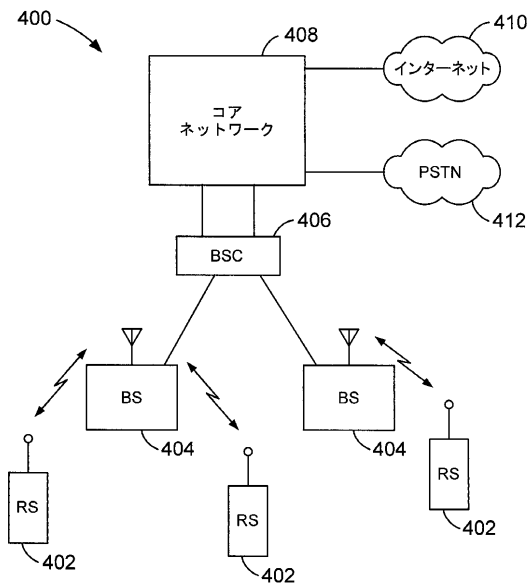
【 図 2 】



【図 3】



【図 4】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2012/028611

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04W12/06
ADD.

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)

H04W H04L H04Q G06F

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, COMPENDEX, INSPEC, 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	US 2004/111616 A1 (ADI WAEL [DE]) 10 June 2004 (2004-06-10) paragraphs [0057], [0059] - [0068], [0073] - [0094] figures 1-6 -----	1-40
X	US 2007/142086 A1 (BOURSIER CARINE [FR] ET AL) 21 June 2007 (2007-06-21) paragraphs [0026] - [0039] figures 1-2 -----	1-40
X	EP 2 291 015 A1 (GEMALTO SA) 2 March 2011 (2011-03-02) paragraphs [0097] - [0103], [0108] - [0121] figures 1,2 -----	1-40

☐ 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

2 May 2012

Date of mailing of the international search report

23/05/2012

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

Ghomrasseni, Z

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2012/028611

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004111616 A1	10-06-2004	DE 10026326 A1 EP 1290905 A2 JP 4819286 B2 JP 2003535497 A US 2004111616 A1 WO 0191478 A2	29-11-2001 12-03-2003 24-11-2011 25-11-2003 10-06-2004 29-11-2001
US 2007142086 A1	21-06-2007	AT 386408 T DE 602004011836 T2 EP 1709827 A1 FR 2864410 A1 US 2007142086 A1 WO 2005069658 A1	15-03-2008 09-04-2009 11-10-2006 24-06-2005 21-06-2007 28-07-2005
EP 2291015 A1	02-03-2011	EP 2291015 A1 WO 2011023819 A1	02-03-2011 03-03-2011

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, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN

(72)発明者 エドワード・ジョージ・タイドマン
アメリカ合衆国・カリフォルニア・92121・サン・ディエゴ・モアハウス・ドライブ・5775

(72)発明者 ジョン・ウォレス・ナシエルスキー
アメリカ合衆国・カリフォルニア・92121・サン・ディエゴ・モアハウス・ドライブ・5775

Fターム(参考) 5J104 AA07 AA16 AA32 EA05 EA08 EA19 JA21 KA02 NA02 NA36
NA37 NA38 PA07