(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2014-531163
(P2014-531163A)
(43)公表日　平成26年11月20日(2014.11.20)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675B	5J104
G06F 21/62	(2013.01)	G06F	21/24	163E	

審査請求 有　予備審査請求 未請求　（全 21 頁）

(21)出願番号	特願2014-536106 (P2014-536106)
(86)(22)出願日	平成24年10月19日 (2012.10.19)
(85)翻訳文提出日	平成26年6月17日 (2014.6.17)
(86)国際出願番号	PCT/CN2012/083219
(87)国際公開番号	WO2013/056674
(87)国際公開日	平成25年4月25日 (2013.4.25)
(31)優先権主張番号	201110319068.2
(32)優先日	平成23年10月20日 (2011.10.20)
(33)優先権主張国	中国 (CN)

(71)出願人　391030332
アルカテル－ルーセント
フランス国、９２１００・ブローニュ－ビヤンクール、ルート・ドゥ・ラ・レーヌ・１４８／１５２
(74)代理人　110001173
特許業務法人川口國際特許事務所
(72)発明者　フー，ジーユエン
中華人民共和国、シャンハイ・２０１２０６、プードン・ジンチャオ、ニンチャオ・ロード・ナンバー・３８８
(72)発明者　ルオ，ジガン
中華人民共和国、シャンハイ・２０１２０６、プードン・ジンチャオ、ニンチャオ・ロード・ナンバー・３８８

最終頁に続く

(54)【発明の名称】サードパーティーアプリケーションの集中型セキュアマネージメント方法、システム、および対応する通信システム

(57)【要約】
複数の実施形態が、サードパーティーアプリケーション上での集中型セキュアマネージメントを実行するための方法およびシステムを含む。この方法は、サードパーティーアプリケーションによって、その識別子、認証クレデンシャル、およびアクセス許可を区別可能な様式で集中型セキュアマネージメントシステムへ送信するステップと、サードパーティーアプリケーションを成功裏に認証した後に、集中型セキュアマネージメントシステムによって、識別子およびアクセス許可を許可サーバへ転送するステップと、アクセス許可が有効である場合には、許可サーバによって、保護されているリソースにアクセスするためのアクセストークンを、集中型セキュアマネージメントシステムを通じてサードパーティーアプリケーションに発行するステップとを含む。

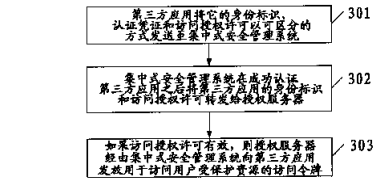


图3 / Fig. 3

301 TRANSMISSION BY THE THIRD PARTY APPLICATION OF THE IDENTITY MARKER, AUTHENTICATION CREDENTIAL, AND ACCESS LICENSE THEREOF IN THE DISTINGUISHABLE SCHEME TO THE CENTRALIZED SECURITY MANAGEMENT SYSTEM
302 FORWARDING BY THE CENTRALIZED SECURITY MANAGEMENT SYSTEM OF THE IDENTITY MARKER AND THE ACCESS LICENSE OF THE THIRD PARTY APPLICATION TO THE AUTHENTICATION SERVER WHEN THE THIRD PARTY APPLICATION IS AUTHENTICATED SUCCESSFULLY
303 IF THE ACCESS LICENSE IS VALID, THEN ISSUANCE BY THE AUTHENTICATION SERVER TO THE THIRD PARTY APPLICATION VIA THE CENTRALIZED SECURITY MANAGEMENT SYSTEM OF THE ACCESS TOKEN USED FOR ACCESSING THE PROTECTED RESOURCE

【特許請求の範囲】
【請求項１】
リソースサーバ内に格納されているユーザの保護されているリソースにアクセスするためにサードパーティーアプリケーション上での集中型セキュアマネージメントを実行するための方法であって、集中型マネージメントのためのサードパーティーアプリケーションの集中型セキュアマネージメントシステムが、サードパーティーアプリケーションのセキュリティーを検証すること、およびサードパーティーアプリケーションにデジタル署名することを担当し、集中型セキュアマネージメントシステムがサードパーティーアプリケーションを認証することができる認証クレデンシャルを発行し、当該方法が、
サードパーティーアプリケーションによって、その識別子、認証クレデンシャル、およびアクセス許可を区別可能な様式で集中型セキュアマネージメントシステムへ送信するステップと、
サードパーティーアプリケーションを成功裏に認証した後に、集中型セキュアマネージメントシステムによって、識別子およびアクセス許可を許可サーバへ転送するステップと、
アクセス許可が有効である場合には、許可サーバによって、ユーザの保護されているリソースにアクセスするためのアクセストークンを、集中型セキュアマネージメントシステムを通じてサードパーティーアプリケーションに発行するステップとを含むことを特徴とする、方法。
【請求項２】
アクセス許可およびアクセストークンが、ＩＥＴＦによって定義されている認証プロトコルＯＡｕｔｈ２．０に準拠しており、および／または認証クレデンシャルが、デジタル証明書、キー、またはパスワードのうちの１つである、
請求項１に記載の方法。
【請求項３】
サードパーティーアプリケーションがアクセスに関して許可される前に、ユーザが、サードパーティーアプリケーションがアクセス許可を使用することによってアクセストークンを入手する目的でアクセス許可を入手するように、許可サーバによって認証されなければならず、ならびに／または
許可サーバがアクセス許可をサードパーティーアプリケーションへ送信した後に、サードパーティーアプリケーションが、そのサードパーティーアプリケーションの識別子、認証クレデンシャル、およびアクセス許可を集中型セキュアマネージメントシステムへ送信する、
請求項１または２に記載の方法。
【請求項４】
サードパーティーアプリケーションが、リソースサーバ内に格納されているユーザの保護されているリソースにアクセスすることを要求したときに、サードパーティーアプリケーションが、有効なアクセストークンを有していない場合には、リソースサーバが、サードパーティーアプリケーションのアクセス要求をユーザエージェントへリダイレクトするステップ、および／または
許可サーバが、集中型セキュアマネージメントシステムを通じてサードパーティーアプリケーションにアクセストークンを発行した後に、サードパーティーアプリケーションが、ユーザの保護されているリソースにアクセスするためにアクセストークンをリソースサーバに提示するステップ
をさらに含む、請求項１から３のいずれか一項に記載の方法。
【請求項５】
許可サーバがユーザを認証することが、ユーザエージェントによって許可サーバに対して直接認証を行うことを介して行われ、
アクセス許可が、許可サーバによってユーザエージェントを通じてサードパーティーアプリケーションへ送信される、

請求項３に記載の方法。
【請求項６】
許可サーバがユーザを認証することが、ユーザエージェントによって認証のために集中型セキュアマネージメントシステムを通じて許可サーバへリダイレクトすることを介して行われ、
アクセス許可が許可サーバによって集中型セキュアマネージメントシステムおよびユーザエージェントを通じてサードパーティーアプリケーションへ送信されるステップ、またはアクセス許可が許可サーバによってユーザエージェントを通じてサードパーティーアプリケーションへ送信されるステップのうちの少なくとも１つが実行される、
請求項３に記載の方法。
【請求項７】
区別可能な様式が、サードパーティーアプリケーションが識別子、認証クレデンシャル、およびアクセス許可を個別にパッケージする様式、またはサードパーティーアプリケーションが識別子、認証クレデンシャル、およびアクセス許可を個別にマークする様式のうちの１つを含む、請求項１から３のいずれか一項に記載の方法。
【請求項８】
リソースサーバ内に格納されているユーザの保護されているリソースにアクセスするためにサードパーティーアプリケーション上での集中型セキュアマネージメントを実行するためのシステムであって、当該システムが、サードパーティーアプリケーションのセキュリティーを検証すること、およびサードパーティーアプリケーションにデジタル署名することを担当し、当該システムがサードパーティーアプリケーションを認証することができる認証クレデンシャルを発行し、当該システムが、
区別可能な様式でサードパーティーアプリケーションによって送信されたサードパーティーアプリケーションの識別子、認証クレデンシャル、およびアクセス許可を受信するための第１の受信デバイスと、
識別子、認証クレデンシャル、およびアクセス許可を受信した後に、識別子、認証クレデンシャルを使用してサードパーティーアプリケーションを認証するための第１の認証デバイスと、
サードパーティーアプリケーションを成功裏に認証した後に、サードパーティーアプリケーションの識別子およびアクセス許可を許可サーバへ転送するための第１の転送デバイスと、
許可サーバによって発行されたアクセストークンをサードパーティーアプリケーションへ転送するための第２の転送デバイスと含むことを特徴とする、システム。
【請求項９】
個人の開発者またはサービスプロバイダによって開発されて、デジタル署名のために個人の開発者またはサービスプロバイダのプライベートキーを使用するサードパーティーアプリケーションを受信するための第２の受信デバイスと、
個人の開発者またはサービスプロバイダによって開発されたデジタル証明書を使用して、第２の受信デバイスによって受信されたサードパーティーアプリケーションのデジタル署名を認証するための第２の認証デバイスと、
第２の認証デバイスの成功裏の認証の後に、サードパーティーアプリケーションが、悪意のあるコードまたはウイルスを含んでいるかどうかを検知するための安全チェックデバイスと、
サードパーティーアプリケーションを成功裏に安全チェックした後に、システムのプライベートキーを使用してサードパーティーアプリケーションにデジタル署名するためのデジタル署名デバイスと、
サードパーティーアプリケーションに関する識別子、認証クレデンシャル、および関連属性の均等な配布のマネージメントのためのサードパーティーアプリケーションレジストリ／マネージメントデバイスと、
すべての関連したデジタル証明書の均等なマネージメントのための証明書マネージメン

トデバイスと
をさらに含む、請求項８に記載のシステム。
【請求項１０】
アクセス許可およびアクセストークンが、ＩＥＴＦによって定義されている認証プロトコルＯＡｕｔｈ２．０に準拠しており、ならびに／または
認証クレデンシャルが、デジタル証明書、キー、もしくはパスワードのうちの１つであり、ならびに／または
デジタル証明書上での証明書マネージメントデバイスのマネージメントが、生成、発行、および取り消しを含む、
請求項８または９に記載のシステム。
【請求項１１】
すべての関連したデジタル証明書上での均等なマネージメントが、生成、発行、および取り消しを含み、ならびに／または
許可サーバがアクセス許可をサードパーティーアプリケーションへ送信した後に、サードパーティーアプリケーションが、そのサードパーティーアプリケーションの識別子、認証クレデンシャル、およびアクセス許可をシステムへ送信し、ならびに／または
サードパーティーアプリケーションがアクセスに関して許可される前に、ユーザが、サードパーティーアプリケーションがアクセス許可を用いてアクセストークンを入手する目的でアクセス許可を入手するように、許可サーバによってユーザエージェントを通じて認証されなければならず、ならびに／または
サードパーティーアプリケーションが、リソースサーバ内のユーザの保護されているリソースにアクセスすることを要求したときに、サードパーティーアプリケーションが、有効なアクセストークンを有していない場合には、リソースサーバが、サードパーティーアプリケーションのアクセス要求をユーザエージェントへリダイレクトし、ならびに／または
許可サーバが、システムを通じてサードパーティーアプリケーションにアクセストークンを発行した後に、サードパーティーアプリケーションが、ユーザの保護されているリソースにアクセスするためにアクセストークンをリソースサーバに提示する、
請求項８から１０のいずれか一項に記載のシステム。
【請求項１２】
許可サーバがユーザを認証することが、ユーザエージェントによって許可サーバに対して直接認証を行うことを介して行われ、
アクセス許可が、許可サーバによってユーザエージェントを通じてサードパーティーアプリケーションへ送信される、
請求項１１に記載のシステム。
【請求項１３】
許可サーバがユーザを認証することが、ユーザエージェントによって認証のためにシステムを通じて許可サーバへリダイレクトすることを介して行われ、
アクセス許可が許可サーバによってシステムおよびユーザエージェントを通じてサードパーティーアプリケーションへ送信されるステップ、またはアクセス許可が許可サーバによってユーザエージェントを通じてサードパーティーアプリケーションへ送信されるステップのうちの少なくとも１つが実行される、
請求項１１に記載のシステム。
【請求項１４】
区別可能な様式が、サードパーティーアプリケーションが識別子、認証クレデンシャル、およびアクセス許可を個別にパッケージする様式、またはサードパーティーアプリケーションが識別子、認証クレデンシャル、およびアクセス許可を個別にマークする様式のうちの１つを含む、請求項８から１０のいずれか一項に記載のシステム。
【請求項１５】
少なくとも１つの許可サーバと、

少なくとも１つのリソースサーバと、
ユーザエージェントと、
サードパーティーアプリケーションと、
請求項８から１４のいずれか一項に記載されている、リソースサーバ内に格納されているユーザの保護されているリソースにアクセスするためにサードパーティーアプリケーション上での集中型セキュアマネージメントを実行するためのシステムと
を含む、通信システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、通信に関し、詳細には、ユーザの保護されているリソースにアクセスするためにサードパーティーアプリケーション／クライアント上での集中型セキュアマネージメントを実行するためのテクノロジーに関する。

【背景技術】

【０００２】

現在、インターネットサービスどうしの統合が、必要なトレンドになってきている。よりよいサービスをユーザに提供するために、多くのサービスプロバイダは、サードパーティーアプリケーション／クライアントが、「オープンネットワークＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍｍｉｎｇ　Ｉｎｔｅｒｆａｃｅ）」を呼び出すことによってさらに多くのアプリケーションをユーザに提供することを可能にしている。オープンプラットフォームの本質的な問題は、ユーザ認証、承認、およびサードパーティーアプリケーション／クライアントがオープンネットワークＡＰＩを安全に使用しなければならないということである。ユーザにとっては一般に、ユーザとサードパーティーの両者が強い信頼関係にない限り、サードパーティーがユーザの保護されているネットワークリソースにアクセスする目的でユーザ自身のユーザ名およびパスワードを直接使用することができることをユーザは望まない。サービスどうしの統合中の「認証および承認」という本質的な問題を解決する目的で、ＯＡｕｔｈ（Ｏｐｅｎ　Ａｕｔｈｏｒｉｚａｔｉｏｎ）プロトコルが発表されている。

【０００３】

ＩＥＴＥ（すなわち、Ｉｎｔｅｒｎｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　Ｔａｓｋ　Ｆｏｒｃｅ）によって開発されたＯＡｕｔｈプロトコルは、現在国際的に一般的な様式であり、リソースの所有者を代理することによって、保護されているリソースにアクセスする方法をサードパーティーアプリケーション／クライアントに提供する。保護されているリソースにアクセスする前に、サードパーティーアプリケーション／クライアントは、はじめにリソースの所有者からの、すなわちアクセス許可（アクセス許可は、リソースの所有者によって提供されるに相当し、そのタイプは、サードパーティーアプリケーション／クライアントによって使用される入手様式、および許可サーバによってサポートされる様式に依存する）を入手し、次いで（アクセス許可のアクション範囲、持続時間、およびその他の属性を表す）アクセストークンをアクセス許可と交換しなければならない。サードパーティーアプリケーション／クライアントは、アクセストークンをリソースサーバに示すことによって、保護されているリソースにアクセスする。

【０００４】

ＯＡｕｔｈプロトコルの新たなバージョン、ＯＡｕｔｈ２．０は、実施を簡素化することを原則としており、より多くのアクセス形態をサポートし、たとえば、「ウェブアプリケーション、デスクトップアプリケーション、モバイル端末、ホームデバイス」などを同時にサポートする。ＯＡｕｔｈ２．０は、ユーザが、必ずしも自分の長期クレデンシャルを、または自分の識別子さえ明らかにすることなく、自分の保護されているリソースへのアクセスをサードパーティーアプリケーション／クライアントに許可することを可能にする。この方法においては、ユーザ機密情報のプライバシーが保護されることが可能である。

【０００５】
この目的のために、サービスプロバイダは、ユーザのリソースを管理しなければならず、下記を担当するＩＥＴＦ　ＯＡｕｔｈ２．０において定義されている許可サーバを構築しなければならない：
－　ユーザのマネージメント、
－　サードパーティーアプリケーション／クライアントのマネージメント、
－　サードパーティーアプリケーション／クライアントがアクセストークンを求める際に用いるアクセス許可（ＩＥＴＦ　ＯＡｕｔｈ２．０における定義を参照されたい）を発行すること、
－　許可サーバとユーザとの間における相互認証、
－　許可サーバとサードパーティーアプリケーション／クライアントとの間における相互認証、
－　アクセス許可の検証、および
－　サードパーティーアプリケーション／クライアントがユーザの保護されているリソースにアクセスすることができるアクセストークンを発行すること。
【０００６】
図１は、ＩＥＴＦ　ＯＡｕｔｈ２．０によるシステムおよびワークフローを概略的に示している。
【０００７】
図１において示されているワークフローは、下記のとおりである：
１．サードパーティーアプリケーション／クライアントが、リソースサーバ内に格納されているユーザの保護されているリソースにアクセスすることを計画し、
２．リソースサーバは、サードパーティーアプリケーション／クライアントが、有効なアクセストークンを有していないことに気づき、次いでユーザのを得るために、サードパーティーアプリケーション／クライアントをユーザエージェントへリダイレクトし、
３．ユーザは、許可アクセスを用いてサードパーティーアプリケーション／クライアントをする前に、許可サーバによってされなければならず、また同時に許可サーバを認証することを必要とする場合があり、
４．許可サーバは、ユーザエージェントを介してサードパーティーアプリケーション／クライアントへ許可アクセスを送信し、
５．サードパーティーアプリケーション／クライアントは、アクセストークンを求めるために、識別子、許可アクセス、および自分自身の認証クレデンシャルを許可サーバに提示し、
６．許可サーバとサードパーティーアプリケーション／クライアントとの間における相互認証の後に、かつ許可アクセスを検証した後に、許可サーバは、アクセストークンをサードパーティーアプリケーション／クライアントに発行し、
７．サードパーティーアプリケーション／クライアントは、ユーザのリソースにアクセスするために、アクセストークンをリソースサーバに提示し、
８．アクセストークンが有効である場合には、リソースサーバは、データをサードパーティーアプリケーション／クライアントに返す。
【発明の概要】
【発明が解決しようとする課題】
【０００８】
しかしながら、ＩＥＴＦ　ＯＡｕｔｈ２．０が非常に好ましいのは、いくつかの大規模サービスプロバイダにとってのみである。なぜなら、それらの大規模サービスプロバイダは、サードパーティーアプリケーション／クライアントのマネージメント（たとえば、識別子、認証、認証クレデンシャルマネージメントなど）を自分たち自身でまかなう余裕があるためである。しかしながら、小規模および中規模サービスプロバイダにとっては、これを行うのは容易ではない。なぜなら、サードパーティーアプリケーション／クライアントを管理することは、それらの小規模および中規模サービスプロバイダにとって非常に高

くつくことになるためである。その上、大規模サービスプロバイダたちは、内部で別々のリソースサーバを配備している場合には、サードパーティーウェブサイトおよびアプリケーション／クライアントを管理するための重複したコンポーネントを開発および配備しなければならない。

【０００９】

さらに、非常に多くのサードパーティーアプリケーション／クライアントが存在し、それらのうちのいくつかは個人によって開発および提供される場合があるため、攻撃者たちが、ネットワークＡＰＩを悪用することによってユーザのリソースに不正にアクセスするために悪意のあるネットワークＡＰＩを開発する可能性がある。したがって、すべてのサードパーティーアプリケーション／クライアントがセキュアで信頼されているということを、ユーザの保護されているリソースへのアクセスをそれらのサードパーティーアプリケーション／クライアントに許可する前に保証することは、容易ではない。

【課題を解決するための手段】

【００１０】

従来技術における上述の欠点に対処するために、本発明の第１の態様によれば、本発明は、リソースサーバ内に格納されているユーザの保護されているリソースにアクセスするためにサードパーティーアプリケーション上での集中型セキュアマネージメントを実行するための方法を明らかにする。この方法によれば、集中型マネージメントのためのサードパーティーアプリケーションの集中型セキュアマネージメントシステムが、サードパーティーアプリケーションを発行する前に、サードパーティーアプリケーションのセキュリティーを検証すること、およびサードパーティーアプリケーションにデジタル署名することを担当し、その集中型セキュアマネージメントシステムがサードパーティーアプリケーションを認証することができる認証クレデンシャルを発行する。この方法は、サードパーティーアプリケーションによって、その識別子、認証クレデンシャル、およびアクセス許可を区別可能な様式で集中型セキュアマネージメントシステムへ送信するステップと、サードパーティーアプリケーションを成功裏に認証した後に、集中型セキュアマネージメントシステムによって、アクセス許可を許可サーバへ転送するステップと、許可サーバがアクセス許可を有効なものとして成功裏に認証した場合には、許可サーバによって、ユーザの保護されているリソースにアクセスするためのアクセストークンを、集中型セキュアマネージメントシステムを通じてサードパーティーアプリケーションに発行するステップとを含む。

【００１１】

本発明の別の態様によれば、リソースサーバ内に格納されているユーザの保護されているリソースにアクセスするためにサードパーティーアプリケーション上での集中型セキュアマネージメントを実行するためのシステムが提供され、このシステムは、区別可能な様式でサードパーティーアプリケーションによって送信されたサードパーティーアプリケーションの識別子、認証クレデンシャル、およびアクセス許可を受信するための第１の受信デバイスと、識別子、認証クレデンシャル、およびアクセス許可を受信した後に、識別子および認証クレデンシャルを使用してサードパーティーアプリケーションを認証するための第１の認証デバイスと、サードパーティーアプリケーションを成功裏に認証した後に、サードパーティーアプリケーションのアクセス許可を許可サーバへ転送するための第１の転送デバイスと、許可サーバによって発行されたアクセストークンをサードパーティーアプリケーションへ転送するための第２の転送デバイスと含む。

【００１２】

好ましくは、本発明によるシステムは、個人の開発者またはサービスプロバイダによって開発されて、デジタル署名のために個人の開発者またはサービスプロバイダのプライベートキーを使用するサードパーティーアプリケーションを受信するための第２の受信デバイスと、個人の開発者またはサービスプロバイダによって開発されたデジタル証明書を使用して、第２の受信デバイスによって受信されたサードパーティーアプリケーションのデジタル署名を認証するための第２の認証デバイスと、第２の認証デバイスの成功裏の認証

の後に、サードパーティーアプリケーションが、悪意のあるコードまたはウイルスを含んでいるかどうかを検知するための安全チェックデバイスと、サードパーティーアプリケーションを成功裏に安全チェックした後に、システムのプライベートキーを使用してサードパーティーアプリケーションにデジタル署名するためのデジタル署名デバイスと、サードパーティーアプリケーションに関する識別子、認証クレデンシャル、および関連属性の均等な配布のマネージメントのためのサードパーティーアプリケーションレジストリ／マネージメントデバイスと、すべての関連したデジタル証明書の均等なマネージメント（生成、発行、および取り消しなど）のための証明書マネージメントデバイスとをさらに含む。

【００１３】

本発明のさらに別の態様によれば、少なくとも１つの許可サーバと、少なくとも１つのリソースサーバと、ユーザエージェントと、サードパーティーアプリケーションと、本発明による、リソースサーバ内に格納されているユーザの保護されているリソースにアクセスするためにサードパーティーアプリケーション上での集中型セキュアマネージメントを実行するためのシステムとを含む通信システムが提供される。

【００１４】

本発明のその他の特徴、目的、および利点は、添付の図面を参照しながら、非限定的な実施形態についての以降の詳細な説明を読むことによって、さらに明らかになるであろう。

【図面の簡単な説明】

【００１５】

【図１】従来技術におけるＩＥＴＦ　ＯＡｕｔｈ２．０によるシステムおよびワークフローを概略的に示す図である。

【図２】本発明による、サードパーティーアプリケーション上での集中型セキュアマネージメントを実行するためのシステムおよびワークフローを概略的に示す図である。

【図３】本発明の一実施形態による、サードパーティーアプリケーション上での集中型セキュアマネージメントの方法のフローチャートである。

【図４】本発明の一実施形態による、サードパーティーアプリケーション上での集中型セキュアマネージメントを実行するためのシステムのブロック図である。

【発明を実施するための形態】

【００１６】

本発明の基本的なアイディアは、リソースサーバ内に格納されているユーザの保護されているリソースにアクセスするためにサードパーティーアプリケーション／クライアント上での集中型セキュアマネージメントを実行することである。簡潔にするために、「サードパーティーアプリケーション／クライアント」は、以降の文章においては「サードパーティーアプリケーション」と示されることになる。図２は、サードパーティーアプリケーション上での集中型セキュアマネージメントを実行するためのシステムおよびワークフローを概略的に示している。図２において示されているように、図１における既存のソリューションと比較すると、集中型セキュアマネージメントシステムが付加されている。このシステムは、下記の機能を有する：

－　サードパーティーアプリケーションを正式にリリースする前に、

サードパーティーアプリケーションのトレーサビリティーを確保するための個人の開発者またはサービスプロバイダのキーを通じた署名に関してサードパーティーアプリケーションを認証するために個人の開発者またはサービスプロバイダのデジタル証明書を使用すること、

サードパーティーアプリケーションがセキュアであるか否かを検証すること（たとえば、アンチウイルス／アンチマルウェアをチェックすること）、

サービスプロバイダまたはエンドユーザが、サードパーティーアプリケーションのインストレーションの前にサードパーティーアプリケーションのセキュリティー、真正性、および信頼性を確認することができるように、サードパーティーアプリケーションにそのキーを用いて署名すること、

認証のために使用されるサードパーティーアプリケーションに対するクレデンシャル（たとえば、証明書またはキー）を発行すること、
－　サードパーティーアプリケーションを正式にリリースすること、
－　サードパーティーアプリケーションが、ユーザの保護されているリソースにアクセスする前に、このシステムは、下記の機能を有する：
集中型セキュアマネージメントシステムと、サードパーティーアプリケーションとの間における相互認証、
サードパーティーアプリケーションに関する識別子およびその認証クレデンシャルのマネージメント。

【００１７】
図１における既存のソリューションと比較すると、図２におけるサードパーティーアプリケーションは、本出願による集中型セキュアマネージメントサーバが、識別子、認証クレデンシャル、およびそのアクセス許可を個別に区別することができるように、それらの識別子、認証クレデンシャル、およびアクセス許可を個別にパックすること、または識別子、認証クレデンシャル、およびアクセス許可を個別にマークすることを必要とすることが可能である。

【００１８】
図２においては、許可サーバ＿１／リソースサーバ＿１、許可サーバ＿２／リソースサーバ＿２、および許可サーバ＿ｎ／リソースサーバ＿ｎは、下記のものに属する場合がある：
別々の小規模および中規模サービスプロバイダ、または
いくつかのリソースサーバを別々に配備した同じ大規模サービスプロバイダ。

【００１９】
図１における既存のソリューションと比較すると、許可サーバ＿ｉは、ステップ５のメッセージがサードパーティーアプリケーションから直接来ているのか、またはステップ５において示されているように集中型セキュアマネージメントシステムから来ているのかを区別するべきである。その区別は、たとえばフラグを通じて実施されることが可能である。ステップ５のメッセージがサードパーティーアプリケーションから直接来ている場合には、許可サーバ＿ｉは、サードパーティーアプリケーションを認証して、アクセス許可を検証すべきであり、ステップ５のメッセージが集中型セキュアマネージメントシステムから来ている場合には、許可サーバ＿ｉは、アクセス許可を検証することのみを行うべきである。

【００２０】
図１における既存のソリューションと比較すると、図５におけるワークフローの変更は、下記のとおり存在する：
－　ステップ５においては、サードパーティーアプリケーションの識別子、認証クレデンシャル、およびアクセス許可が、区別可能な様式で集中型セキュアマネージメントシステムへ送信されることが可能であり、区別可能な様式とは、集中型セキュアマネージメントシステムが、識別子、認証クレデンシャル、およびアクセス許可を区別することができるように、それらの識別子、認証クレデンシャル、およびアクセス許可が個別にパッケージされること、または個別にマークされることが可能であるということを意味している。
－　ステップ６においては、ステップ６は、下記のように２つのサブステップを含む：
６－１：　サードパーティーアプリケーションを成功裏に認証した後に、集中型セキュアマネージメントシステムは、アクセス許可を許可サーバ＿ｎへ転送する。アクセス許可が有効である場合には、許可サーバ＿ｎは、サードパーティーアプリケーションに対して発行されたアクセストークンを集中型セキュアマネージメントシステムへ送信する。本発明においては、アクセス許可およびアクセストークンは、たとえば、ＩＥＴＦによって定義されている認証プロトコルＯＡｕｔｈ２．０に準拠している。
６－２：　集中型セキュアマネージメントシステムは、アクセストークンをサードパーティーアプリケーションへ転送する。

【００２１】
さらに、本発明のソリューションによれば、サードパーティーアプリケーションが、有効なアクセストークンを有していない場合には、リソースサーバは、サードパーティーアプリケーションのアクセス要求をユーザエージェントへリダイレクトする。
【００２２】
指摘されなければならないこととして、本発明による集中型セキュアマネージメントシステムは、サーバグループを含み、そのサーバグループは、たとえば、証明書発行マネージメントサーバ、サードパーティーアプリケーションのセキュリティーチェッキングサーバ、サードパーティーアプリケーションのレジストリマネージメントサーバ、サードパーティーアプリケーションの認証サーバ、サードパーティーアプリケーションのストレージ／リリースサーバなどを含むことができる。
【００２３】
本発明においてさらに指摘されなければならないこととして、ユーザは、自分の保護されているリソースにサードパーティーアプリケーションがアクセスすることを許可すると想定される。自分の保護されているリソースにサードパーティーアプリケーションがアクセスすることをする前に、ユーザは、サードパーティーアプリケーションがアクセストークンを入手する目的でアクセス許可を入手するように、自分の識別子が真正であること、および自分の保護されているリソースにサードパーティーアプリケーションがアクセスすることを許可するための権限を有していることを確かにするために、許可サーバによって認証されなければならない。本発明のソリューションによれば、ユーザ認証は、ユーザエージェントと許可サーバとの間における通信によって直接、または集中型セキュアマネージメントシステムを通じたユーザエージェントによる許可サーバへのリダイレクトによって、実施されることが可能である。
【００２４】
同様に、アクセス許可は、許可サーバによってユーザエージェントを通じてサードパーティーアプリケーションへ送信されること、または許可サーバによって集中型セキュアマネージメントシステムおよびユーザエージェントを通じてサードパーティーアプリケーションへ送信されることが可能である。
【００２５】
さらに、本発明による集中型セキュアマネージメントシステムは、下記の機能を実施することができる：
－　個人の開発者またはサービスプロバイダのキーを使用した個人の開発者またはサービスプロバイダの署名およびサインによって開発されたサードパーティーアプリケーションが受信された場合には、サードパーティーアプリケーションのトレーサビリティーを確保するためのサードパーティーアプリケーションのデジタル署名を認証するために個人の開発者またはサービスプロバイダのデジタル証明書を使用すること、
－　認証が成功裏に実施された後に、サードパーティーアプリケーションが、悪意のあるコードまたはウイルスを含んでいるかどうかを検知すること、
－　安全検知がサードパーティーアプリケーション上で成功裏に実施された後に、サードパーティーアプリケーションがインストールされる際のそのセキュリティー、真正性、および信頼性を確かにする目的でサードパーティーアプリケーションにデジタル署名するために集中型セキュアマネージメントシステムのキーを使用すること、
－　サードパーティーアプリケーションに関する識別子、認証クレデンシャル、および関連属性の均等な配布のマネージメントを実行すること、
－　生成、発行、および取り消しなど、すべての関連したデジタル証明書上での均等なマネージメントを実行すること。
【００２６】
本発明による集中型セキュアマネージメントシステムを使用することによって、小規模および中規模サービスプロバイダにとっては、多額のコストを節約すること、および負担を低減することが可能であり（それは、ユーザおよび保護されているリソースのマネージ

メントを担当するだけですむということを意味し）、またさらに、大規模サービスプロバイダは、サードパーティーアプリケーション上での集中型マネージメントを伴って、それによって個別に配備される複数の内部リソースサーバを提供するようになることが可能である。さらに、本発明のソリューションを使用することによって、サードパーティーアプリケーションがさらにセキュアであり信頼できるということを確かにすることができる。なぜなら、そのサードパーティーアプリケーションは、信頼できるサードパーティーメカニズム（すなわち、本発明の集中型セキュアマネージメントシステム）によって安全管理されるためである。

【００２７】

以降では、本発明の一実施形態による、サードパーティーアプリケーション上での集中型セキュアマネージメントを実行するための方法が、図３を参照することによって説明される。この実施形態の方法は、上述の図２において示されているようなシステムに適合されることが可能であり、ここで上述のシステムの説明にさらに入り込むことはしない。

【００２８】

図３において示されているように、はじめに、ステップ３０１において、サードパーティーアプリケーションは、自分の識別子、認証クレデンシャル、およびアクセス許可を区別可能な様式で集中型セキュアマネージメントシステムへ送信する。認証クレデンシャルは、ここでは、たとえば、デジタル証明書、暗号、またはパスワードであることが可能であり、アクセス許可は、たとえば、ＩＥＴＦによって定義されている認証プロトコルＯＡｕｔｈ２．０に準拠することができる。区別可能な様式とは、集中型セキュアマネージメントシステムが、識別子、認証クレデンシャル、およびアクセス許可を区別することができるように、それらの識別子、認証クレデンシャル、およびアクセス許可が個別にパッケージされること、または個別にマークされることが可能であるということを意味している。上述したように、この実施形態においては、ユーザは、自分の保護されているリソースにサードパーティーアプリケーションがアクセスすることを許可すると想定される。サードパーティーアプリケーションが、リソースサーバ内のユーザの保護されているリソースにアクセスすることを要求したときに、サードパーティーアプリケーションが、有効なアクセストークンを有していない場合には、リソースサーバは、サードパーティーアプリケーションのアクセス要求をユーザエージェントへリダイレクトする。

【００２９】

指摘されなければならないこととして、アクセスに関してサードパーティーアプリケーションをする前に、ユーザは、サードパーティーアプリケーションがアクセス許可を使用することによってアクセストークンを入手する目的でアクセス許可を入手するように、許可サーバによって認証されなければならず、許可サーバによるユーザの認証は、許可サーバに対するユーザエージェントの認証によって直接、または認証のための集中型セキュアマネージメントシステムを通じたユーザエージェントによる許可サーバへのリダイレクトによって、実施されることが可能である。

【００３０】

さらに指摘されなければならないこととして、許可サーバがアクセス許可をサードパーティーアプリケーションへ送信した後に、サードパーティーアプリケーションは、そのサードパーティーアプリケーションの識別子、認証クレデンシャル、およびアクセス許可を集中型セキュアマネージメントシステムへ送信し、アクセス許可は、許可サーバによってユーザエージェントを通じてサードパーティーアプリケーションへ送信されること、または許可サーバによって集中型セキュアマネージメントシステムおよびユーザエージェントを通じてサードパーティーアプリケーションへ送信されることが可能である。

【００３１】

次いで、ステップ３０２において、集中型セキュアマネージメントシステムは、サードパーティーアプリケーションを成功裏に認証した後にアクセス許可を許可サーバへ転送する。ここで、アクセス許可は、たとえば、ＩＥＴＦによって定義されている認証プロトコルＯＡｕｔｈ２．０に準拠している。

【００３２】
次いで、ステップ３０３において、アクセス許可が有効である場合には、許可サーバは、ユーザの保護されているリソースにアクセスするためのアクセストークンを、集中型セキュアマネージメントシステムを通じてサードパーティーアプリケーションに発行する。ここで、アクセストークンは、たとえば、ＩＥＴＦによって定義されている認証プロトコルＯＡｕｔｈ２．０に準拠している。したがって、サードパーティーアプリケーションは、ユーザの保護されているリソースにアクセスするためにアクセストークンをリソースサーバに提示することができる。
【００３３】
この実施形態においては、集中型セキュアマネージメントシステム、ユーザエージェント、サードパーティーアプリケーション、許可サーバ、およびリソースサーバの間におけるインタラクティブなプロセスは、上述のＯＡｕｔｈ２．０などの（ただし、それには限定されない）任意の既存のおよび将来のソリューション、標準、および基準の様式に準拠することができる。
【００３４】
上述の説明においては、新たな集中型セキュアマネージメントシステムを既存のシステム内に付加することによって、この実施形態による、サードパーティーアプリケーション上での集中型セキュアマネージメントを実行する方法を使用すれば、小規模および中規模サービスプロバイダにとっては、多額のコストを節約すること、および負担を低減することが可能であり（それは、ユーザおよび保護されているリソースのマネージメントを担当するだけですむということを意味し）、またさらに、大規模サービスプロバイダは、サードパーティーアプリケーション上での集中型マネージメントを伴って、それによって個別に配備される複数の内部リソースサーバを提供するようになることが可能であるということがわかる。さらに、本発明のソリューションを使用することによって、サードパーティーアプリケーションがさらにセキュアであり信頼できるということを確かにすることができる。なぜなら、そのサードパーティーアプリケーションは、信頼できるサードパーティーメカニズム（すなわち、本発明の集中型セキュアマネージメントシステム）によって安全管理されるためである。
【００３５】
同じコンセプトのもとで、本発明の別の態様によれば、リソースサーバ内に格納されているユーザの保護されているリソースにアクセスするためにサードパーティーアプリケーション上での集中型セキュアマネージメントを実行するためのシステムが提供される。以降では、そのシステムが、図を参照することによって説明される。
【００３６】
図４は、本発明の一実施形態による集中型セキュアマネージメントシステム４００を示している。システム４００は、受信デバイス４０１、認証デバイス４０２、第１の転送デバイス４０３、および第２の転送デバイス４０４を含む。同様に、ユーザは、自分の保護されているリソースにサードパーティーアプリケーションがアクセスすることを許可すると想定される。具体的には、サードパーティーアプリケーションが、保護されているリソースにアクセスすることを要求した場合には、許可サーバがユーザを成功裏に認証して、アクセス許可をサードパーティーアプリケーションに発行した後に、受信デバイス４０１は、区別可能な様式でサードパーティーアプリケーションによって送信されたサードパーティーアプリケーションの識別子、認証クレデンシャル、およびアクセス許可を受信する。区別可能な様式とは、集中型セキュアマネージメントシステムが、識別子、認証クレデンシャル、およびアクセス許可を区別することができるように、それらの識別子、認証クレデンシャル、およびアクセス許可が個別にパッケージされること、または個別にマークされることが可能であるということを意味している。識別子、認証クレデンシャル、およびアクセス許可を受信した後に、認証デバイス４０２は、サードパーティーアプリケーションを認証するために、識別子、認証クレデンシャルを使用する。第１の転送デバイス４０３は、サードパーティーアプリケーションを成功裏に認証した後にサードパーティーア

プリケーションのアクセス許可を許可サーバへ転送し、第２の転送デバイス４０４は、許可サーバによって発行されたアクセストークンをサードパーティーアプリケーションへ転送する。したがって、サードパーティーアプリケーションは、アクセストークンをリソースサーバに提示することによって、ユーザの保護されているリソースにアクセスすることができる。

【００３７】

上述したように、集中型セキュアマネージメントシステム４００はさらに、下記の機能を実施する：

－　個人の開発者またはサービスプロバイダのキーを使用した個人の開発者またはサービスプロバイダの署名およびサインによって開発されたサードパーティーアプリケーションが受信された場合には、サードパーティーアプリケーションのトレーサビリティーを確保するためのサードパーティーアプリケーションのデジタル署名を認証するために個人の開発者またはサービスプロバイダのデジタル証明書を使用すること、

－　認証が成功裏に実施された後に、サードパーティーアプリケーションが、悪意のあるコードまたはウイルスを含んでいるかどうかを検知すること、

－　安全検知がサードパーティーアプリケーション上で成功裏に実施された後に、サードパーティーアプリケーションがインストールされる際のそのセキュリティー、真正性、および信頼性を確かにする目的でサードパーティーアプリケーションにデジタル署名するために集中型セキュアマネージメントシステムのキーを使用すること、

－　サードパーティーアプリケーションに関する識別子、認証クレデンシャル、および関連属性の均等な配布のマネージメントを実行すること、

－　生成、発行、および取り消しなど、すべての関連したデジタル証明書上での均等なマネージメントを実行すること。

【００３８】

指摘されなければならないこととして、サードパーティーアプリケーション上での集中型セキュアマネージメントシステムのセキュリティーチェックは、任意の既存のおよび将来のソリューション、標準、および基準の様式に準拠することができる。

【００３９】

実装においては、集中型セキュアマネージメントシステム４００、および、その集中型セキュアマネージメントシステム４００が含む受信デバイス４０１、認証デバイス４０２、第１の転送デバイス４０３、および第２の転送デバイス４０４は、ソフトウェア、ハードウェア、およびソフトウェアとハードウェアの組合せの形態で実装されることが可能である。たとえば、当業者なら、その手段を適切に実施するためのさまざまな種類のデバイス、たとえば、マイクロプロセッサ、マイクロコントローラ、特定用途向け集積回路（ＡＳＩＣ）、プログラマブルロジックデバイス（ＰＬＤ）、および／またはフィールドプログラマブルゲートアレイ（ＦＰＧＡ）などをよく知っている。この実施形態による集中型セキュアマネージメントシステムのそれぞれのコンポーネントは、物理的に個別に実現されて、互いに動作可能に接続されることが可能である。

【００４０】

オペレーションにおいては、上述の図４とともに説明されている実施形態の、リソースサーバ内に格納されているユーザの保護されているリソースにアクセスするためにサードパーティーアプリケーション上での集中型セキュアマネージメントを実行するためのシステムは、上述のサードパーティーアプリケーション上での集中型セキュアマネージメントを実行するための方法を実施することができる。このシステムを使用することによって、小規模および中規模サービスプロバイダにとっては、多額のコストを節約すること、および負担を低減することが可能であり（それは、ユーザおよび保護されているリソースのマネージメントを担当するだけですむということを意味し）、またさらに、大規模サービスプロバイダは、サードパーティーアプリケーション上での集中型マネージメントを伴って、それによって個別にデプロイされる複数の内部リソースサーバを提供するようになることが可能である。さらに、本発明のソリューションを使用することによって、サードパー

ティーアプリケーションがさらにセキュアであり信頼できるということを確かにすることができる。なぜなら、そのサードパーティーアプリケーションは、信頼できるサードパーティーメカニズム（すなわち、本発明の集中型セキュアマネージメントシステム）によって安全管理されるためである。

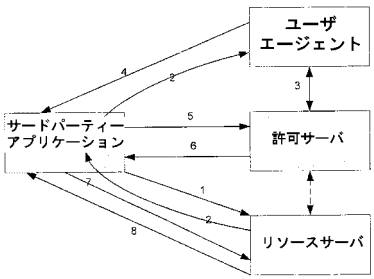
【００４１】

同じ本発明のコンセプトのもとで、本発明のさらに別の態様によれば、少なくとも１つの許可サーバと、少なくとも１つのリソースサーバと、ユーザエージェントと、サードパーティーアプリケーションと、本発明による、リソースサーバ内に格納されているユーザの保護されているリソースにアクセスするためにサードパーティーアプリケーション上での集中型セキュアマネージメントを実行するためのシステムとを含む通信システムが提供される。さらに、この通信システムは、その他のネットワーク要素、たとえばルータなどを含むことができる。

【００４２】

サードパーティーアプリケーション上での集中型セキュアマネージメントを実行するための方法、リソースサーバ内に格納されているユーザの保護されているリソースにアクセスするためにサードパーティーアプリケーション上での集中型セキュアマネージメントを実行するためのシステム、および、少なくとも１つの許可サーバと、少なくとも１つのリソースサーバと、ユーザエージェントと、サードパーティーアプリケーションと、本発明による、リソースサーバ内に格納されているユーザの保護されているリソースにアクセスするためにサードパーティーアプリケーション上での集中型セキュアマネージメントを実行するためのシステムとを含む通信システムが、いくつかの例示的な実施形態を用いて具体的に説明されているが、それらの実施形態は、限定的なものではなく、例示的なものとみなされるべきであり、当業者なら、本発明の趣旨および範囲内でさまざまな種類の変形および修正を実施することができる。したがって本発明は、それらの実施形態に限定されるものではなく、本発明の範囲は、添付の特許請求の範囲によってのみ画定される。

【図１】



PRIOR ART

Fig. 1

【図３】

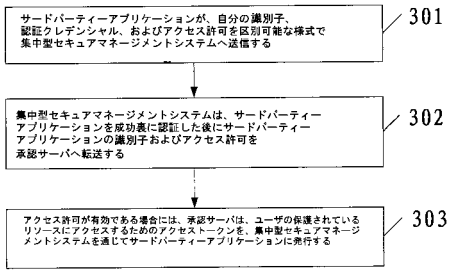


Fig. 3

【図２】

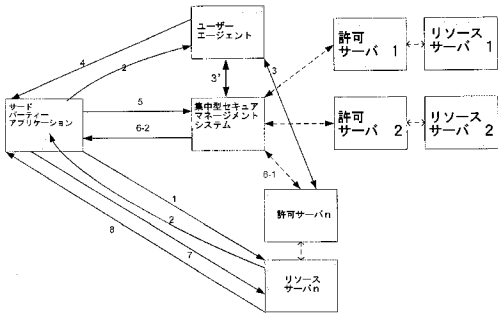


Fig. 2

【図４】

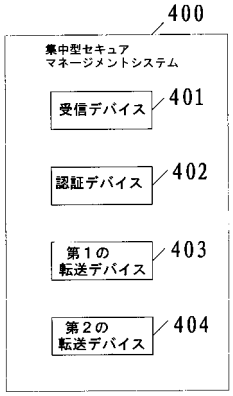


Fig. 4

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2012/083219

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet
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)

IPC: H04L; H04M

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)

CNPAT, CNTXT, WPI, EPODOC, CNKI, GOOGLE: security, authenticat+, authorizat+, access, visit, identity, ID, token, central+, manag+, resource, signature, third party

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101207485 A (SHENZHEN TONGZHOU ELECTRONIC CO., LTD.) 25 June 2008 (25.06.2008), the whole document	1-15
A	CN 101136928 A (BEIJING UNIVERSITY OF TECHNOLOGY) 03 May 2008 (03.05.2008), the whole document	1-15
A	CN 1889452 A (HUAWEI TECHNOLOGIES CO., LTD.) 03 Jan. 2007 (03.01.2007), the whole document	1-15
A	WO 2008/036569 A1 (SPRINT COMMUNICATIONS COMPANY L.P.) 27 Mar. 2008 (27.03.2008), the whole document	1-15
A	US 2006/0282886 A1 (LOCKHEED MARTIN CORPORATION) 14 Dec. 2006 (14.12.2006), the whole document	1-15

☐ 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
06 Jan. 2013 (06.01.2013)	07 Feb. 2013 (07.02.2013)

Name and mailing address of the ISA
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No. (86-10) 62019451

Authorized officer
LUO, Xiao
Telephone No. (86-10) 62413299

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2012/083219

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101207485 A	25.06.2008	NONE	
CN 101136928 A	05.03.2008	NONE	
CN 1889452 A	03.01.2007	EP 1746764 A2	24.01.2007
		US 2007022470 A1	25.01.2007
		WO 2007009350 A1	25.01.2007
		CN 101160775 A	09.04.2008
WO 2008036569 A1	27.03.2008	US 2008127337 A1	29.05.2008
US 2006282886 A1	14.12.2006	US 2007011349 A1	11.01.2007

Form PCT/ISA /210 (patent family annex) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2012/083219

A: CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i
H04L 12/24 (2006.01) n

国际检索报告	国际申请号 **PCT/CN2012/083219**

A. 主题的分类

参见附加页

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC：H04L；H04M

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNABS, CNTXT, WPI, EPODOC, CNKI, GOOGLE：安全，认证，验证，授权，权限，集中，统一，管理，访问，资源，第三方，签名，身份，标识，凭证，security, authenticat+, authorizat+, access, identity, ID, token, central+, manag+, third party

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN101207485A (深圳市同洲电子股份有限公司) 25.6 月 2008(25.06.2008), 全文	1-15
A	CN101136928A (北京工业大学) 05.3 月 2008(05.03.2008), 全文	1-15
A	CN1889452A (华为技术有限公司) 03.1 月 2007(03.01.2007), 全文	1-15
A	WO2008/036569A1 (SPRINT COMMUNICATIONS COMPANY L.P.) 27.3 月 2008(27.03.2008)，全文	1-15
A	US2006/0282886A1 (LOCKHEED MARTIN CORPORATION) 14.12 月 2006(14.12.2006)，全文	1-15

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
06.1 月 2013(06.01.2013)	**07.2 月 2013 (07.02.2013)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号：　(86-10)62019451	受权官员 罗啸 电话号码：(86-10) **62413299**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2012/083219

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101207485A	25.06.2008	无	
CN101136928A	05.03.2008	无	
CN1889452A	03.01.2007	EP1746764A2	24.01.2007
		US2007022470A1	25.01.2007
		WO2007009350A1	25.01.2007
		CN101160775 A	09.04.2008
WO2008036569A1	27.03.2008	US2008127337A1	29.05.2008
US2006282886A1	14.12.2006	US2007011349A1	11.01.2007

国际检索报告

国际申请号
PCT/CN2012/083219

A．主题的分类：
H04L 9/32 (2006.01)i
H04L 12/24 (2006.01)n

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,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,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,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,PA,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

(72)発明者 ワン，ヨンゲン
中華人民共和国、シャンハイ・２０１２０６、プードン・ジンチャオ、ニンチャオ・ロード・ナンバー・３８８

Ｆターム(参考) 5J104 AA07 AA16 AA32 EA04 EA19 JA21 KA01 KA06 NA02 NA37
NA38 PA07