

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2017-139026

(P2017-139026A)

(43) 公開日 平成29年8月10日(2017.8.10)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 21/33 (2013.01)	G06F 21/33	5 J 1 0 4
H04L 9/08 (2006.01)	H04L 9/00 6 0 1 F	
H04L 9/32 (2006.01)	H04L 9/00 6 7 5 B	
	H04L 9/00 6 7 5 D	

審査請求 有 請求項の数 12 O L 外国語出願 (全 23 頁)

(21) 出願番号	特願2017-94260 (P2017-94260)	(71) 出願人	510030995 インターデジタル パテント ホールディングス インコーポレイテッド アメリカ合衆国 19809 デラウェア州 ウィルミントン ベルビュー パークウェイ 200 스위트 300
(22) 出願日	平成29年5月10日 (2017.5.10)	(74) 代理人	110001243 特許業務法人 谷・阿部特許事務所
(62) 分割の表示	特願2015-11333 (P2015-11333)の分割	(72) 発明者	アンドレアス レイチェル ドイツ 60488 フランクフルト アム マイン ギースフェルトストラッセ 2
原出願日	平成21年9月14日 (2009.9.14)	(72) 発明者	アンドレアス ユー. シュミット ドイツ 65929 フランクフルト アム マイン トイトーネンウェグ 37 最終頁に続く

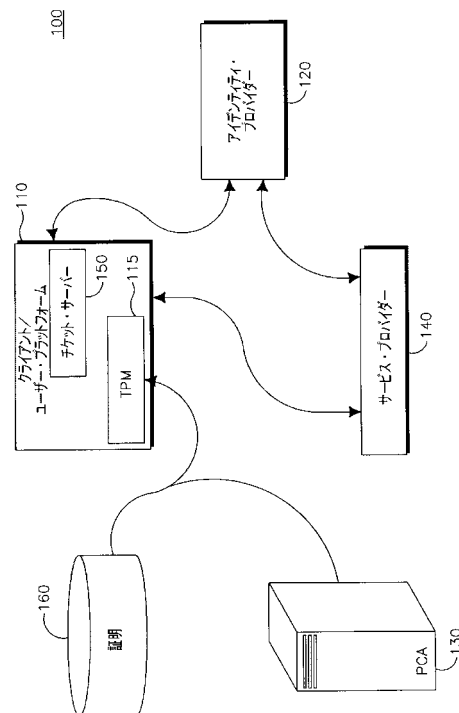
(54) 【発明の名称】 信頼できる認証およびログオンのための方法および装置

(57) 【要約】

【課題】 信頼できる認証およびログオンのための方法および装置が開示される。

【解決手段】 TPM (Trusted Platform Module: トラステッド・プラットフォーム・モジュール) 準拠のログオン方法が認証およびアクセスに対して提示される。ユーザーは、ユーザーの特定のプラットフォーム、例えば TPM に緊密に結合したアイデンティティ・プロバイダーを用いて識別子を登録する。ユーザーが、例えばこの識別子を使用してサービス・プロバイダーにログインしようと決めたなら、アイデンティティ・プロバイダーは、ユーザーが正しい信用情報を提供することを申し立て (challenge) する。信用情報は、TPM によって生成されたチケット、すなわち信用情報チェーンから成る。これによりユーザーは、アイデンティティ・プロバイダーにてパスワードの必要性なしでログインが可能となる。

【選択図】 図 1



【特許請求の範囲】

【請求項 1】

予め定められた識別子を使用してサービス・プロバイダーにログオンするステップであって、ユーザー・プラットフォームは、前記予め定められた識別子によって指し示されるアイデンティティ・プロバイダーに前記サービス・プロバイダーによってリダイレクトされることと、

前記アイデンティティ・プロバイダーから認証チャレンジを受信するステップと、

前記認証チャレンジに対応して、前記ユーザー・プラットフォームは前記認証チャレンジを受容したという条件にて、TPM (Trusted Platform Module: トラステッド・プラットフォーム・モジュール) に準拠したチケットを送信するステップと、

前記アイデンティティ・プロバイダーから成功したチケット検証を受信した際に、前記サービス・プロバイダーにアクセスするステップと
を備えることを特徴とする方法。

【請求項 2】

前記予め定められた識別子は、URI (Universal Resource Identifier) によって表されることを特徴とする請求項 1 に記載の方法。

【請求項 3】

前記ユーザー・プラットフォームおよびチケットを正当化する前記チケットを生成させるステップをさらに備えることを特徴とする請求項 1 に記載の方法。

【請求項 4】

前記認証チャレンジは、少なくとも前記予め定められた識別子およびサービス要求の種類を含むことを特徴とする請求項 1 に記載の方法。

【請求項 5】

前記予め定められた識別子および前記サービス要求に署名するために、証明された署名鍵を生成させるステップをさらに備えることを特徴とする請求項 4 に記載の方法。

【請求項 6】

前記予め定められた識別子に対応する AIK (Attestation Identity Key: 構成証明アイデンティティ鍵) のためのパスワード、および TPM 利用を認証するためのストレージ・ルート鍵パスワードを提供するステップをさらに備えることを特徴とする請求項 1 に記載の方法。

【請求項 7】

AIK (Attestation Identity Key: 構成証明アイデンティティ鍵) に対応する証明書を獲得するステップをさらに備えることを特徴とする請求項 1 に記載の方法。

【請求項 8】

以前に取得した証明書が入手不可という条件にて、証明書を生成させるステップをさらに備えることを特徴とする請求項 7 に記載の方法。

【請求項 9】

肯定的なチャレンジ確認に対応してノンスを受信するステップと、

AIK (Attestation Identity Key: 構成証明アイデンティティ鍵) によって署名された引用を前記 TPM から生成させるステップであって、前記 AIK によって署名された引用は、前記ノンスを含むことと
をさらに備えることを特徴とする請求項 1 に記載の方法。

【請求項 10】

前記チケットは、CSK (Certified Signing Key: 証明済み署名鍵) によって署名された予め定められた識別子、CSK によって署名された要求、CSK 公開鍵、および PCA (Privacy Certification Authority: プライバシー認証局) によって発行された AIK (Attestation Identity Key: 構成証明アイデンティティ鍵) 証明書、をさらに備えることを

10

20

30

40

50

特徴とする請求項 1 に記載の方法。

【請求項 1 1】

前記認証チャレンジに対応して、前記ユーザー・プラットフォームが前記認証チャレンジを受容したという条件にて、前記 TPM からの PCR (Platform Configuration Register : プラットフォーム構成レジスタ) の AIK によって署名された引用、および測定ログを送信するステップをさらに備えることを特徴とする請求項 1 0 に記載の方法。

【請求項 1 2】

前記成功したチケット検証は、前記 AIK 証明書のタイムスタンプの正当化、前記 AIK 証明書上の PCA 署名の検証、前記 CSK 公開鍵上の AIK 署名の検証、前記 CSK によって署名された予め定められた識別子の検証、前記 CSK によって署名された要求の検証、前記測定ログの正当化、および前記引用の検証、を含むことを特徴とする請求項 1 1 に記載の方法。

10

【請求項 1 3】

その後のサービス・プロバイダー・アクセスのために、証明された署名鍵によって保護された暗号化されたクッキーを受信するステップをさらに備えることを特徴とする請求項 1 に記載の方法。

【請求項 1 4】

前記認証チャレンジは、認可チャレンジを含むことを特徴とする請求項 1 に記載の方法。

20

【請求項 1 5】

構成証明チャレンジをさらに備えることを特徴とする請求項 1 に記載の方法。

【請求項 1 6】

信頼できる認証およびアクセスを支援するための装置であって、プラットフォームは、

予め定められた識別子を使用してサービス・プロバイダーにアクセスするように構成されたインターフェイス・モジュールであって、前記装置は、前記予め定められた識別子によって指し示されるアイデンティティ・プロバイダーに前記サービス・プロバイダーによってリダイレクトされることと、

認証チャレンジが受容されたという条件にて、TPM (Trusted Platform Module : トラステッド・プラットフォーム・モジュール) に準拠したチケットを送信することによって前記認証チャレンジに応答するように構成されたチケット・サーバーと、

30

前記アイデンティティ・プロバイダーから成功したチケット検証を受信し、および前記サービス・プロバイダーにおけるサービスにアクセスするように構成される前記インターフェイス・モジュールとを備えることを特徴とする装置。

【請求項 1 7】

前記チケット・サーバーは、CSK (Certified Signing Key : 証明済み署名鍵) によって署名された予め定められた識別子、CSK によって署名された要求、CSK 公開鍵、および PCA (Privacy Certification Authority : プライバシー認証局) によって発行された AIK (Attestation Identity Key : 構成証明アイデンティティ鍵) 証明書を含むチケットを生成させるようにさらに構成されることを特徴とする請求項 1 6 に記載の装置。

40

【請求項 1 8】

前記チケット・サーバーは、前記 TPM からの AIK (Attestation Identity Key : 構成証明アイデンティティ鍵) によって署名された引用、および測定ログを獲得するようにさらに構成されることを特徴とする請求項 1 7 に記載の装置。

【請求項 1 9】

前記チケット・サーバーは、ノンスを受信し、そして AIK (Attestation Identity Key : 構成証明アイデンティティ鍵) によって署名された引用を前

50

記TPMから生成させるようにさらに構成されることであって、前記AIKによって署名された引用は、前記ノンスを含むことを特徴とする請求項16に記載の装置。

【発明の詳細な説明】

【技術分野】

【0001】

本願は、認証(authentication)およびアクセスに関する。

【背景技術】

【0002】

識別子管理、ならびにユーザー認証およびアクセスは、ウェブ利用、移動体サービス、無線通信、および他のサービスのための重大な問題である。多くの認証およびアクセス・プロトコルがある。例えばOpenIDは、ユーザー認証およびアクセス管理のための、開かれた、分散型の枠組みおよび方法である。ただ一つのデジタル識別子により、ユーザーが、一度ログオンし、そして複数のサービスへのアクセスを得ることが可能である。デジタル識別子は一般には、アイデンティティ・プロバイダーによって通常提供される一意なユニバーサルリソースロケータ(URL: Universal Resource Locator)の形式である。アイデンティティ・プロバイダーは、ユーザーがデジタル識別子によりサービス・プロバイダーにアクセスしようとしたとき、ユーザーを認証する。OpenIDの枠組みは、ユーザーを認証するための種々の認証方法を可能にさせる。アイデンティティ・プロバイダーにて識別子を主張する(claim)ために、いくつかの方法を使用することが可能である。最も一般的なのは、ユーザーがパスワードを提供するログオン形式の使用である。しかしながら、信頼できるシステムの使用なくしては、認証信用情報を発出する通信相手と信頼関係を確立するための十分な根拠を依存する側が獲得することはないであろう。ユーザー信用情報(例えば、ユーザー名/パスワードの組み合わせの形式の)は、プラットフォームに結合している訳ではないため、盗用されているかもしれない。攻撃者は、正規のユーザーの名を借りてサービスにアクセスするために盗用された信用情報を使用するかもしれない。OpenIDプロトコルのための認証信用情報をプラットフォームおよびその信頼に値する状態に結合することによって、OpenIDプロトコルのセキュリティおよび安全性を高めることができる。

10

20

【0003】

チケット準拠の認証および認可プロトコルにおいては、単一のエンティティ/ユーザーの識別子を立証するためにソフトウェア・トークン(すなわちチケット)が使用される。これらのトークンに準拠することで、ある特定のシステムへのアクセスは、適切なトークンを生成するエンティティ/ユーザーに制限される。さらに加えて、単なる認証以外にトークン準拠のアクセス管理方式を可能にする認可制御を実施するために、トークン中に一体化されたデータを使用することができる。

30

【0004】

別の認証および認可プロトコルでは、チケット・システムにおいて信用情報を識別する際に、信頼できるコンピューティング環境におけるTPM(Trusted Platform Module: トラステッド・プラットフォーム・モジュール)により生成されたAIK(Attestation Identity Key: 証明アイデンティティ鍵)を使用する。AIKは、信頼性測定に署名し、そしてTPMによって生成された鍵を証明するために使用される。このような信頼できるチケット準拠のシステムの現在の実施方法は、チケットの暗号化のために、集中データベースを使用し、共有された鍵データベースまたはPKI(Public Key Infrastructure: 公開鍵暗号基盤)を維持することを必要とし、そしてすべてのサービス・プロバイダーを、受信したチケットを審査しそして受容するように変更する必要がある。

40

【発明の概要】

【0005】

信頼できる認証およびログオンのための方法および装置が開示される。TPM準拠のログオン方法が認証およびアクセスに対して提示される。ユーザーは、ユーザーの特定のプ

50

プラットフォーム、例えばTPMに緊密に結合したアイデンティティ・プロバイダーを用いて識別子を登録する。ユーザーが、例えばこの識別子を使用してサービス・プロバイダーにログインしようとしたら、アイデンティティ・プロバイダーは、ユーザーが正しい信用情報を提供することをチャレンジ(challenge)する。この方法においては、信用情報は、暗号信用情報チェーンを組み込んだ、TPMによって生成されたチケットから成る。これによりユーザーは、アイデンティティ・プロバイダーにてパスワードの必要性なしでログインが可能となる。ユーザーの特定のプラットフォームでのローカルなパスワードは、ローカルな攻撃から識別子を保護するために依然として使用することができる。

【0006】

ログオンは、特定のプラットフォームの完全性検証と組み合わせられる。システム構成を安全に保存する、TPMのPCR(Platform Configuration Register:プラットフォーム構成レジスタ)上のTPMによって署名されたステートメントを使用して、アイデンティティ・プロバイダーは、報告されたシステム状態を以前に生成された参照値と比較することができ、これによりログインしそして識別子を請求するために信頼に値するプラットフォームを正規のユーザーのみが使用することを可能とする。この組み合わせられた認証および証明(attestation)は、特定のプラットフォームのみではなく、信頼に値すると考えられる事前に定義されたシステム状態にも認証データを結合することによってきめ細かいアクセス管理を可能とする。これにより、システムの拡張されたセキュリティおよび安全性を必要とし、そして信頼に値しないシステムの原因となる何れの修正をも許容しないであろう、認証およびアクセス方法のための新しい用途を可能にする。

【図面の簡単な説明】

【0007】

添付図面に関連して例として与えられた以下の説明から、より詳細な理解を得ることができる。

【0008】

【図1】認証およびアクセス・システムのための高位な構造の一例を示す図である。

【図2】認証およびアクセス方法のための高位な信号フローの一例を示す図である。

【図3(a)】認証およびアクセス方法のための信号フローの一例を示す図である。

【図3(b)】認証およびアクセス方法のための信号フローの一例を示す図である。

【図4】LTE(Long Term Evolution)の無線通信システム/アクセス・ネットワークの一実施形態を示す図である。

【図5】LTE無線通信の無線送受信ユニットおよび基地局の例を示すブロック図である。

【発明を実施するための形態】

【0009】

後述される、用語「WTRU(Wireless Transmit/Receive Unit:無線送受信ユニット)」は、限定的ではなく、UE(User Equipment:ユーザー機器)、移動体端末、固定型または移動体の加入者ユニット、ページャー、携帯電話、PDA(Personal Digital Assistant:携帯情報端末)、コンピューター、または無線環境において動作する能力のある他の如何なる種別のデバイスをも含む。後述される、用語「基地局(base station)」は、限定的ではなく、ノードB(Node-B)、発展型ノードB(evolved Node-B)、サイトコントローラー、AP(Access Point:アクセス・ポイント)、または無線環境において動作する能力のある他の如何なる種別のインターフェイス・デバイスをも含む。

【0010】

本明細書における開示は、認証およびアクセス・システムの一例としてOpenIDプロトコルを使用し、そして他の認証およびアクセス・システムにも適用可能である。基本

10

20

30

40

50

的エンティティおよびそれらの高位のフローが最初に説明され、方法の詳細な論議があとに続く。

【0011】

図1は、限定的ではなく、クライアント/ユーザー・プラットフォーム110、アイデンティティ・プロバイダー120、PCA (Privacy Certification Authority: プライバシー認証局) 130、およびサービス・プロバイダー140を含む認証およびアクセス・システム100の一例である。クライアント/ユーザー・プラットフォーム110、アイデンティティ・プロバイダー120、およびサービス・プロバイダー140は、何れかの組み合わせの無線および有線の通信システムを通して互いに通信状態にある。クライアント/ユーザー・プラットフォーム110はさらに、PCA 130と通信状態にあり、PCA 130は例えば証明を保存する格納媒体160と通信状態にある。

10

【0012】

クライアント/ユーザー・プラットフォーム110は、WTRU、基地局、コンピューティング・プラットフォーム、または認証を必要とする場合がある何れのデバイスでもあることができる。クライアント/ユーザー・プラットフォーム110は、限定的ではなく、クライアント/ユーザー・プラットフォーム110のためのデータに対する、遠隔証明機能ならびにシール機能および結合機能を提供するTPM 115を含む。TPM 115は、鍵、パスワード、デジタル証明書を保存するマイクロコントローラーであり、そして暗号化鍵を生成させることが可能である。これはマザーボードに取り付けられるか、またはシステムのチップセットに集積され、そしてこれらの機能を必要とする何れのコンピューティング・デバイスにおいても使用することができる。TPM 115は、外部のソフトウェア攻撃および物理的改ざん、ならびに盗聴から、そこに保存された情報をより安全にすることを確実にする。ブート・シーケンスの間に構成要素に関して採られた測定値が参照測定値に対して予期された通りでないなら、TPM 115またはクライアント/ユーザー・プラットフォーム110の中のデータおよび秘密へのアクセスを拒絶することができる。その結果、安全な電子メール、安全なウェブ・アクセス、およびデータのローカルな保護などの重要なアプリケーションおよび能力をより以上に安全にする。本明細書においては信頼できるプラットフォーム・モジュールが議論されるが、例えば移動体の信頼できるモジュールなどの、他の代替の信用センターを使用することができる。

20

30

【0013】

TPM 115は2048ビットのRSA公開および秘密鍵の組であるEK (Endorsement Key: エンドースメント鍵) を使用し、これは製造時にチップ上にランダムに生成されそして変更することはできない。秘密鍵はチップから決して分離せず、一方公開鍵はチップに送られた機密データの証明のためおよび暗号化のために使用される。EKの公開の部分は一様に、証明の目的のためのEK証明書によってPCA 130によって既知である。一般にTPM 115が、例えばアイデンティティ・プロバイダーなどの検証機構に対して自身を認証する必要があるときは常に、それは、AIKと呼ばれる第2のRSA鍵の組を生成させ、AIK公開鍵をPCA 130に送り、そして対応するEKに対してこの公開鍵を認証する。PCA 130はその一覧表中にこのEKを見出したなら、PCA 130はTPM 115のAIKに関する証明書を発行する。そしてTPM 115は、アイデンティティ・プロバイダー120にこの証明書を提供し、そして自身を認証することができる。

40

【0014】

本明細書において述べられるように、AIK (少なくともAIK中に一体化された識別子) は少なくとも本明細書において説明されるチケットの一部を表す。AIKのチケットとしての利用はしかしながら、TPM 115によって制限される。したがって、Certify Key 動作と呼ばれる間接的解決方法を使用して、署名鍵が、TPM 115によって生成され、そしてAIKを用いてそれに署名することによって証明される。この鍵は、CSK (Certified Signing Key: 証明された署名鍵) と呼ばれる

50

。CSKおよびAIKは、AIKの正当性を保証するPCAと共に、本明細書において説明されるチケットの一部を構成する。

【0015】

クライアント/ユーザー・プラットフォーム110はまた、サービス・アクセスに対する信用情報またはチケットを生成させるTicket Server 150を含む。Ticket Server 150はユーザーを認証する。Ticket Server 150は、プラットフォーム証明の信頼できるコンピューティングを使用して、クライアント/ユーザー・プラットフォーム110およびそれ自身を、アイデンティティ・プロバイダー120に向かって正当化する。Ticket Server 150は現在の非信頼済みOpen ID構造においては存在せず、単純にローカルな信用情報格納装置としての役割を果たす。より多くのセキュリティ重要情報および動作がTicket Server 150に集中化されているため、AIK証明書およびCSKを適切に取り扱いそしてそれらを他のプラットフォームに拡散させることがないこと、チケットおよび信用情報を保護すること、ユーザー承認によりすべての信用情報に関するセキュリティに緊要な何れの動作をも保護すること、一般的ウェブ・ブラウザーに直接的に統合されそしてそれらによってアクセスされるべき安全なオプションを提供すること、およびプラットフォーム正当化データを収集し、処理し、送付すること、が信頼できねばならない。本明細書においてはこれがさらに詳細に開示される。

10

【0016】

ユーザーは、TPM 115において生成されたAIKを証明するためにPCA 130を選択せねばならない。PCA 130は、すべての識別子関連情報を保持することができ、そしてこの識別子関連情報の非公開性を確実にするために契約上の方策が講じられねばならない。PCA 130にてAIKを証明した後に、ユーザーはアイデンティティ・プロバイダー120を選択し、主張された識別子を提供させることができる。請求された識別子は、ユーザーによって選択されたURIによって表される。そのような請求された識別子を登録するために、ユーザーは正当なAIK証明書をアイデンティティ・プロバイダー120に提供せねばならない。これは本明細書においてさらに詳細に開示される。

20

【0017】

アイデンティティ・プロバイダー120には、最少量の識別子関連情報のみしか提示されない場合がある。ユーザーは、PCA 130にて提供された何れの情報をアイデンティティ・プロバイダー120に露出することができ、露出することになるかを決定することができる。関係者の間の協調を確実にするために契約上の方策が講じられねばならず、そうでなければ不正なPCAが相違するユーザーのものである識別子を証明してしまうかも知れない。PCA 130はアイデンティティ・プロバイダー120にユーザーの実際の識別子を露出することにはならないため、アイデンティティ・プロバイダー120は種々の要求を一つの識別子にリンクさせることはできないであろう。

30

【0018】

PCA 130は、主張された識別子を実際の識別子に転換することが可能な唯一の事例(instance)である。(一意な)EK証明書をAIKに対応付ける安全にされたデータベースを保つことによって、容易にこれを為すことができる。AIK証明の間に使用されるEK証明書は、TPM 115すなわちクライアント/ユーザー・プラットフォーム110の疑う余地のない識別を可能とする(1人のユーザーのみが、これがそのユーザーに転換するプラットフォーム110への物理的アクセス権を有すると仮定して)。

40

【0019】

サービス・プロバイダー140のみが、アイデンティティ・プロバイダーがサイトに対してログインすることを可能にさせる。サービス・プロバイダー140は例えば、最初のページ上にOpen IDログイン・ロゴを有することができる。ユーザー/クライアントによって使用されるアイデンティティ・プロバイダー120は、サービス・プロバイダー140の既知のかつ受容されたアイデンティティ・プロバイダーの一覧表中になければならない。

50

【0020】

ここで図2を参照すると、図1において開示されたシステム100に対する高位の信号フロー200の一例が示される。本明細書において議論されるように、クライアント/ユーザーまたはユーザー・プラットフォーム210、サービス・プロバイダー215、およびアイデンティティ・プロバイダー220（OpenID Providerの一例として示される）が互いの間の通信のために構成される。

【0021】

クライアント/ユーザー・プラットフォーム210は、ウェブ・ブラウザー225を使用して、アクセス・ウェブページ・メッセージ227を介してサービス・プロバイダー・ウェブページ（index.jsp235と識別して）にアクセスする。クライアント/ユーザー210が彼の、例えばOpenID URIを使用してログインすることを欲したなら、サービス・プロバイダー215でのindex.jspページ235は、OpenIDログオン様式メッセージ229を介してそのURIを要求し、そしてその結果OpenID識別子メッセージ231を介して請求された識別子を提供するOpenIDプロバイダー220のアドレスを検索する。

10

【0022】

次にサービス・プロバイダー215は、OpenIDプロバイダー220とのアソシエーション（association）の形成を試みる。OpenIDプロトコルに従って、サービス・プロバイダー215は、アソシエーションメッセージ241を介してOpenIDプロバイダー220とアソシエーションする。アソシエーションメッセージ241は、要求、主張された識別子、および認証に成功した場合に、クライアント/ユーザー・プラットフォーム210に対してそこにOpenIDプロバイダー220がリダイレクト・メッセージ247を送ることになる、アソシエーションメッセージ243を介するリターンURL、の安全な交換を含む。これは、サーバー・プロバイダー215にてconsumer_redirect.jsp240により、およびOpenIDプロバイダー220にてprovider.jsp245によって実行される。アソシエーションの後に、クライアント/ユーザー・プラットフォーム210は、OpenIDプロバイダーへのリダイレクト・メッセージ249を介してOpenIDプロバイダー220のprovider.jspウェブページ245にリダイレクトされる。

20

【0023】

次にOpenIDプロバイダー220は、provider.jspウェブページ245からprovider_authentication.jspウェブページ255に切り替わり、クライアント/ユーザー・プラットフォーム210を認証する。ユーザーは、provider_authentication.jspウェブページ255上のリンクをクリックすることによって、要求を起動する。これは新しい背景のスレッドTVerifier258を始動し、チャレンジメッセージ252を介してTicketServer250にチャレンジする。provider_authentication.jspウェブページ255は、クライアント/ユーザー・プラットフォーム210をprovider.jspウェブページ245にリダイレクトして戻し、そこでTVerifier258を待って、チャレンジ応答メッセージ254において提供されたチャレンジの結果を完成させそして審査する。本明細書において説明されるように、TicketServer250は、TPMの機能性を使用して、チケットを含む適切な応答を生成させ、そして一般に、TPM250、PCA275、および例えば証明を保持する格納媒体280と対話する。

30

40

【0024】

認証に成功したと仮定すると、provider.jspウェブページ245は、リダイレクション・メッセージ262をクライアント/ユーザー・プラットフォーム210に送る。リダイレクション・メッセージ262は、サービス・メッセージ264へのリダイレクトを介して、サービス・プロバイダー215にてconsumer_returnurl.jspページ265にクライアント/ユーザー・プラットフォーム210をリダイ

50

レクトする。consumer_returnurl.jsp ページ 265 は、リダイレクトが関連 OpenID プロバイダー 220 から来ていることをチェックし、そしてサービス・メッセージ 267 を介してクライアント/ユーザー・プラットフォーム 210 にアクセスを与える。

【0025】

ここで図 3 (a) および図 3 (b) を参照すると、Ticket Server 305 および Ticket Challenger 310 の間の信号フローチャート 300 が示される。Ticket Server 305、ならびに PCA 315、証明格納媒体 320、および TPM 325 の間の信号フローもまた示される。

【0026】

Ticket Server 305 は、クライアント側にてサービス・アプリケーションとして動作する。それは、予め定義されたポート上にてリッスンし、チャレンジを待ち受ける。チャレンジメッセージ 327 (ユーザーが例えば OpenID 中にて使用することを欲した識別子、およびサービス・プロバイダーにて発行されたサービス要求を含む) を受信次第、ユーザーは、確認応答 (acknowledge) メッセージ 329 を使用してチャレンジを明示的に許可することを要求される。ユーザーには、チャレンジを否定するオプションがある。否定されると、OpenID 認証は失敗することになる。

【0027】

チャレンジが受け入れられたなら、ユーザーは、所与の識別子に対応する AIK に対してパスワードを入力し、かつ Ticket Server 305 にて SRK (Storage Root Key: ストレージ・ルート鍵) パスワードを入力することによって TPM 325 利用を認証するように指示 (prompt) される。そして SRK は、TPM の安全にされた鍵にアクセスすることが可能な TPM コマンド中に含まれる。そして Ticket Server 305 は、証明書格納媒体 320 から、この識別子に対して以前取得された AIK 証明書を検索しようとする。これは集合的に 335 として示され、本明細書において議論するように、システム状態情報検索 345 および TC Ticket 生成 350 のために必要である。証明書は、PCA 315 などの PCA を用いて以前の AIK 証明から来る場合があり、その結果、証明格納媒体 320 などのシステム上のローカルな証明書格納装置から検索することが可能であり、あるいは証明書がローカルな格納装置において利用可能でない (またはローカルな格納装置における AIK に対する証明書が期限切れかもしくは何れかの理由により無効になっている) なら、AIK によって表された識別子に対する新しい証明書を PCA 315 から要求することが可能である。具体的に言うと、証明書格納媒体 320 において証明書を見出すことができないなら、ユーザーは PCA 315 を選択し、AIK 証明処理を経て、そして AIK に対する証明書を獲得するために接続することができる。したがってユーザーは、TPM 325 の正しい所有者パスワードを提供せねばならない。これが、TPM 325 の所有者以外の人々による不正な識別子の生成を防止する。以下に示されるように、ユーザー入力は Ticket Server 305 から TPM 325 に転送され、そこでパスワードが審査される。

【0028】

チャレンジを受け入れたことに応答して、Ticket Challenger 310 はランダムな nons 337 を生成する。Ticket Server 305 は、 nons ・メッセージ 339 を介して Ticket Challenger 310 からランダムな nons 337 を受信する。 nons を含む、システム構成について記述する PCR 値の AIK によって署名された引用 (quote) Q が、TPM 325 から検索され、集合的に 345 として示されるシステムの状態に関するステートメントが作成される。

【0029】

Ticket Server 305 は次に、集合的に 350 として示されるように TC Ticket を生成する。TC Ticket 生成 350 は、要求および識別子に署名するために使用することができる TPM による新しい鍵 (RSA 鍵の組) の生成にかかわる。本明細書において説明されるように、この新しい鍵は、Certify Key 動作を使用し

10

20

30

40

50

て、AIKを用いて証明される。すなわち、TPMはこの新たに生成された鍵の組に対する機能CertifyKeyを使用し、証明ステートメントおよび結合を生成させる。ここで結合とは、PCAからの、AIKへのおよびAIK証明書への信用のチェーンを結合することを意味する。新たに生成された鍵が成功裏に証明された場合に、それはCSKと呼ばれる。TPM中には複数のCSKおよび複数のAIKがある（またはTPMによって保護された安全な格納装置においてTPMにより安全にされている）場合がある。

【0030】

TCTicket350を検証するために必要とされる情報はTCTicket350に含まれ、受信した側（図3（a）および図3（b）においてはTicketChallenger310により表される）がTCTicket350を容易に検証することができる。平文（plain text）ML（Measurement Log：測定ログ）および引用Qと共に、TCTicket350を含む応答がTCT, Q, MLメッセージ352を介してTicketChallenger310に送り返される。CHRESPONSEおよびACKメッセージ（集合的に351）は、次のメッセージがTCTicket350、引用、およびMLを含むことになるということを、受信側、すなわちTicketChallenger310に通知するための、プロトコル信号方式メッセージである。この処理時点にては、図3（a）および図3（b）が図2におけるTTVerifierThread258の内部動作を表すことに注意するべきである。OpenIDプロバイダーは同時に複数の要求を扱うことができるため、リプレイアタック（replay attack）を防止するために、要求するクライアントの何れもが、新しく、新鮮、かつ一意なチャレンジを持つことが確実になければならない。

10

20

【0031】

メッセージ355を介してTCTicket350を確認すると、ここでTicketChallenger310は、以下のデータを有する。すなわち：アンチリプレイロテクション（anti-replay protection）としてのノンス337を含む、TPM325からのAIKによって署名された引用、平文測定ファイル、署名された識別子文字列、署名された要求文字列、CSKの公開鍵部分、CSKの公開鍵部分上のAIK署名、およびPCA315によって発行されたAIK証明書を含むTCTicket350、である。クライアントを認証するために、TicketChallenger310は、集合的に360として示された以下の情報をチェックする。すなわち：AIK証明書の正当化（タイムスタンプ）、AIK証明書上のPCA署名の検証、TCTicket350中のCSK公開鍵ハッシュ上のAIK署名の検証、TCTicket350中のサービス要求および識別子上の署名の検証、測定一覧表中のエントリーの正当化、および実際の（引用された）PCRの値がML（Measurement List：測定リスト）に対応することの検証、である。

30

【0032】

この検証処理における何かの項目が不良となると、そのクライアントは認証されないことになる。TicketServer305およびPCA315によって、特定の信用情報チェーン、すなわちAIK証明書 - 証明済みCSK - 署名済み要求が構築される。検証状態メッセージ365がユーザーに送られる。これはまた、例えば図2中のリダイレクション・メッセージ262により示される。この場合においては、メッセージ262が、サービス・プロバイダーのreturn_urlにユーザーのブラウザをリダイレクトすることができるか、またはサービス・プロバイダーにてユーザーが認証される。上の検証の何れかが不良（証明書不良またはシステム完全性不良）となると、リダイレクトはOpenIDプロバイダーの「認証失敗（authentication failed）」ページにユーザーを送ることになる。代替手段として、認証失敗の場合においてはOpenIDプロバイダーにて失敗の原因を示す、カスタム設計された結果ページを生成することが可能である場合がある。これは、何れのモジュールまたはソフトウェアが完全性チェックに失敗したかをユーザーに示すことを含むことができ、そしてこれを利用して、彼のシステムを信頼に値する状態に戻すための次のステップをユーザーに提案するシステムに

40

50

できるかも知れない。

【0033】

本明細書における開示から見て、例えばPCA275などのPCAの役割は、信頼できるコンピューティングを採用する現今のチケット・システムにおいて果たされるものとは異なる。例えばPCA275は、特定のサービス・プロバイダー215によって使用される何れの部分的識別子に対しても一回だけ呼び出される必要があるようにすることができる。新規登録においては、クライアント/ユーザー・プラットフォーム210が、自身のプラットフォーム識別子を仮名の(pseudonymous)部分的識別子に関連付ける。PCA275は、この仮名の識別子に対して証明書を提供し、そしてプラットフォーム識別子への仮名の関連付けを保存する。このデータは、個人的機密情報であり、そして従って保護されねばならない。別の例においては、PCA275の位置付けが、現今のチケット・システムと比較した上での追加的オプションを可能とする。本明細書において開示される信用モデルおよび方法は、アイデンティティ・プロバイダー220およびユーザー選択以外の場所でのPCA275の設置を可能とする。

10

【0034】

開示された方法および構造においてはユーザーは、アイデンティティ・プロバイダーによってAIK証明書が受容された任意の外部PCAを選択するか、またはアイデンティティ・プロバイダーによって直接的にもしくは間接的に提供されたPCA機能性を使用することができる。この後者の例においては、PCAまたはPCA機能性がアイデンティティ・プロバイダー中に設置され、複雑性を減少させ、そしてウェブ様式を介してアイデンティティ・プロバイダーを用いての登録の継ぎ目のない置き換えを提供することができる。

20

【0035】

その特定のセキュリティ構造により本開示は、識別子関連情報の暗号化に依存する信頼できるコンピューティングを採用する識別子管理システムに対する特定の脅威を軽減する。例えばTrusted Open IDにおいては、AIK証明書は、クライアントにとって既知でありそして視認可能であり、したがってAIK証明書は、プライバシーを脅かす隠された情報を含むことはできない。

【0036】

別の例においては、Open ID実施方法はOpen IDプロバイダー・ログイン様式をユーザーに提示する。ユーザーがその人の信用情報を入力し、そしてOpen IDプロバイダーがクライアントにクッキーを発行する。次にこのクッキーはあらゆるその後のOpen IDによって可能にされたサービス・アクセスに使用される。これはOpen IDプロトコルに対するいくつかの攻撃の原因となる場合がある：すなわち、(1)クライアントのOpen IDプロバイダーへログインするために使用されるユーザー信用情報への直接攻撃(偽のOpen IDプロバイダー・ページによるフィッシング(phishing)は多量のユーザー信用情報を露出させ、なりすまし犯罪を可能にすることになる)、および、(2)認証後のクライアントのコンピューターからのクッキーの再使用、コピー、および盗用にかかわる、なりすまし犯罪の原因となる攻撃、である。

30

【0037】

両方の攻撃は、本明細書において提示される開示によって軽減される。すべてのユーザー・パスワードは、ローカルであり、ローカルな信頼できるTicket Serverのみに提供され、信用情報フィッシングの問題は排除される。その上仮名の識別子をプラットフォーム、例えばTPMに結合し、その結果別のデバイスにそれらをコピーできないようにする。

40

【0038】

その上クッキーはクライアントのプラットフォームに保存されることはない。これにより、ローカルな再使用の脅威を回避する。例えば複数の人々によって共有されたコンピューターを考慮されたい。人Aが、彼のOpen IDアカウントにログインし、そして署名して退出することを忘れると、人Bは、保存されたクッキーを使用し、Aになりすますか

50

もしれない。オプションとして、ここで開示された認証方法をWeb Browserと
継ぎ目なく統合することができる。ユーザーが、本明細書において開示される信頼できる
方法を使用してサービスにアクセスすることを欲したときは常に、アイデンティティ・プ
ロバイダーはTicket Serverに対して新しいチャレンジを生成する。信頼でき
るTicket Serverアプリケーションからの、チャレンジに答えるために必要な
ローカルのAIKパスワードをクライアントに求める指示を、ユーザーは見るだけである
。Ticket ServerはこのAIK認証秘密を保存することはない。同じプラット
フォームの別のユーザーBがサービスにアクセスすることを欲したなら、Ticket S
erverは再びアイデンティティ・プロバイダーによってチャレンジされ、そしてBは
AのローカルのAIKパスワード（Bはこれを知らない）を提供せねばならない。狙いは
、クライアントのプラットフォームに永久に保存されることのない一時的クッキーを持つ
ことである。あるいは、デバイスへのユーザー認証の結合を生体認証を通して容易にする
ことができる。統合されたデバイスにおいては、透過的に、動的に、そしてしばしば、デ
バイスが常に真正の（bona-fida）ユーザーによって使用されていることを確定
にするように、生体認証が為される。

10

20

30

40

50

【0039】

本明細書における開示は、目標プラットフォーム（アイデンティティ・プロバイダーの
視点から見るとユーザー・プラットフォーム）およびユーザーがそれを解読し、そして認
証トークンとしてそれを使用することができるような方法にて、発行されたクッキー上の
暗号化を使用することができる。アイデンティティ・プロバイダーは、秘密鍵を使用して
クッキーを暗号化し、クライアント側のTicket Serverに、公開のCSKによ
って保護されて、それを送る。CSKは任意の量のデータの全体の暗号化を意味するもの
ではないが、クッキーを暗号化するために使用される秘密鍵を暗号化するためにはそれを
使用することができる。秘密鍵は、対称の、または非対称の鍵であることができる。

【0040】

そして必要であるときに、TPMを使用してクッキーを解読することができる。解読は
、CSK利用に対してユーザーが（ローカルの）CSK秘密を用いて認証することを必要
とする。Ticket Serverは、クッキーが暗号化された状態で保存され、そして
必要な場合にのみ、解読されることを確実にする。

【0041】

さらなるアプリケーションにおいては、開示された認証およびアクセス方法は、結合さ
れた認証ならびにアクセスおよび認可方法に対して使用することができる。ある主要検索
エンジン会社は、最近、ウェブ・サービスにアクセスするときに、継ぎ目のないユーザー
体験を提供するために、API認可方法の一例である、OAuthに対する支援を発表し
た。ユーザーは、サービス・プロバイダーが提供するアクセス・リンクを使用して、ウェブ
・サービスにアクセスし、そして同時に、例えばOAuthを介してそのサービス・プ
ロバイダーが提供するサービスへのウェブ・アプリケーションのアクセスを許可すること
になる。OpenIDは、集中的に保存された識別子を用いてユーザーを認証するために
使用される。OAuthは、ウェブ・サービスがカレンダー、docs、などのユーザー
のデータにアクセスすることを認可するために使用される。一つのステップにおける両方
のプロトコルの組み合わせは、ユーザー経験に関する一元化署名を改善し、かつ異なった
利用者データ、例えば、マッシュアップ（mash-up）、ダッシュボード（dash
board）などへのアクセスを必要とする、新しいウェブ・サービスを可能にする。

【0042】

ユーザーのTPMを、例えばOpenIDチャレンジのみとしてアイデンティティ・プ
ロバイダーに署名させる代わりに、TPMは、ウェブ・アプリケーションの要求を通して
アイデンティティ・プロバイダーによって提示される、結合された、例えばOpenID
/OAuthチャレンジに署名することになる。データへのアクセスの受容と並んで、ユ
ーザー識別および認可がTPMによって安全に署名される。本明細書において開示される
ように、ユーザーのためのセキュリティは、（1）ログインおよび認可をハードウェアT

PMに結合すること、および(2)クライアント上にて動作する悪意のあるソフトウェアによる機密のデータの盗用を回避するために、OpenID/OAuthプロバイダーによるプラットフォーム完全性検証を提供すること、によって改善される。完全性検証はまた、ウェブ・アプリケーションに対するセキュリティの水準を増大させる。完全性検証が証明された状態にあるクライアントのみに、ウェブ・サービスへのアクセス権を与えることができる。これにより、セキュリティおよび秘密が重要なアプリケーションに対して新しいウェブ・サービスの確立を可能にする。例えばOAuthの、認可プロバイダーのトークン・アクセスが、一意に特定可能なTPMによって署名されるという事実から、説明された方法が否認防止を提供する。これは、ウェブ・アプリケーションのサービス・プロバイダーが実施することができる課金処理を容易にする。署名により、ユーザーがウェブ・サービスを要求しそしてアクセスしたということウェブ・アプリケーション・プロバイダーが立証することを可能にする。

10

20

30

40

50

【0043】

TPM準拠のユーザー認証は、プラットフォームの識別子およびアイデンティティ・プロバイダーの間のリンクを可能にする。アイデンティティ・プロバイダーは、所与のプラットフォームに対して登録された識別子のデータベースを維持することが必要である。登録された識別子の内の1つを使用する別のプラットフォームからのログインの試みが検出されたときは常に、アイデンティティ・プロバイダーは：(1)認証を拒否することが可能である/拒否せねばならない、または(2)正規の所有者にその識別子を通知することができる。アイデンティティ・プロバイダーは、所与のプラットフォーム信用情報により攻撃者から正規のユーザーを容易に区別することが可能である。

【0044】

さらなる例においては、方法は証明(attestation)メカニズムを含むことができる。アイデンティティ・プロバイダーは、ユーザー・プラットフォームのシステム状態についての情報を提供するようにユーザーにチャレンジすることができる。システムが信頼に値する状態にあるなら、アクセスは許可されることになる。これにより、「信頼に値する(trustworthy)」システムだけがウェブ・サービスにアクセスできるように、ウェブ・アプリケーションのためのセキュリティをてこ入れする。

【0045】

さらなる例においては、ユーザー側にて、入来する識別子認証要求をリッスンし、そしてそれらをTPMに転送するサービス・アプリケーションを有する代わりに、継ぎ目のないブラウザ統合を使用することができる。適切な機能性を実施するブラウザ拡張を使用することによって、これを達成することができる。アイデンティティ・プロバイダーは、サインイン(sign-in)・ページのHTMLコード内にてチャレンジを発行する。ブラウザ拡張は、この情報を読み出し、そして必要なデータをTPMに転送することができる。TPMは、今度は署名されたチケットを生成し、そしてそれをブラウザ拡張に返送する。次に拡張は署名されたチケットを含む正しいHTTPS応答をアイデンティティ・プロバイダーに発行することができる。この場合において、図3(a)および図3(b)のフローは、別個の拡張ではなく継ぎ目のない統合ブラウザ拡張により扱われるであろう。この解決方法は、より優れた携帯性(portability)およびより良いユーザー体験を可能にする。

【0046】

一般に、ユーザー・プラットフォームからの信頼できる認証およびアクセスのための方法は、予め定められた識別子を使用してサービス・プロバイダーにログオンすることを備え、ここで、ユーザー・プラットフォームはその予め定められた識別子によって指し示されたアイデンティティ・プロバイダーの方に、サービス・プロバイダーによってリダイレクトされる。方法はさらに、アイデンティティ・プロバイダーから認証チャレンジを受信すること、そしてその認証チャレンジに対応して、ユーザー・プラットフォームが認証チャレンジを受け入れたという条件にてTPMに準拠したチケットを送信することを含む。方法はさらに、アイデンティティ・プロバイダーから成功したチケット検証を受信した際

に、サービス・プロバイダーにアクセスすることを含む。予め定められた識別子は、ユニバーサルリソース識別子 (URI: universal resource identifier) によって表される。方法はさらに、ユーザー・プラットフォームおよびチケットを正当化するチケットを生成させることを含む。認証チャレンジは、少なくとも予め定められた識別子およびサービス種別要求を含む。方法はさらに、予め定められた識別子およびサービス要求に署名するための証明された署名鍵を生成させることを備える。

【0047】

方法は、予め定められた識別子に対応するAIKに対するパスワード、およびTPM利用を認証するための格納ルート鍵パスワードを提供することを備える。またそれは、AIKに対応する証明書を獲得することを含む。方法はさらに、以前に取得した証明書が入手不可という条件にて、証明書を生成させることを備える。方法はさらに、肯定的なチャレンジ確認応答 (acknowledgement) に対応してノンスを受信すること、およびAIKによって署名された引用 (quote) をTPMから生成させることを備え、ここでAIKによって署名された引用はノンスを含む。チケットはさらに、CSKによって署名された予め定められた識別子、CSKによって署名された要求、CSK公開鍵、およびPCAによって発行されたAIK証明書、を備える。

10

【0048】

方法はさらに認証チャレンジに対応して、ユーザー・プラットフォームが認証チャレンジを受け入れたという条件にて、TPMからのPCRのAIKによって署名された引用、および測定ログを送信することを備える。成功したチケット検証は、AIK証明書のタイムスタンプの正当化、AIK証明書上のPCA署名の検証、CSK公開鍵上のAIK署名の検証、CSKによって署名された予め定められた識別子の検証、CSKによって署名された要求の検証、測定ログの正当化、および引用の検証、を含む。

20

【0049】

方法はさらに、その後のサービス・プロバイダー・アクセスに対して、証明された署名鍵によって保護された、暗号化されたクッキーを受信することを備える。認証チャレンジは認可チャレンジを含む。方法はさらに、証明 (attestation) チャレンジを備える。

【0050】

信頼できる認証およびアクセスを支援するための装置は、予め定められた識別子を使用するサービス・プロバイダーにアクセスするように構成されたインターフェイス・モジュールを含み、ここで装置は、その予め定められた識別子によって指し示されたアイデンティティ・プロバイダーの方に、サービス・プロバイダーによって、リダイレクトされる。装置はまた、認証チャレンジを受け入れられたという条件にて、TPMに準拠したチケットを送信することによって認証チャレンジに回答するように構成されたチケット・サーバーを含む。インターフェイス・モジュールはまた、アイデンティティ・プロバイダーから成功したチケット検証を受信し、そしてサービス・プロバイダー上のサービスにアクセスするように構成される。チケット・サーバーはさらに、CSKによって署名された予め定められた識別子、CSKによって署名された要求、CSK公開鍵、およびPCAによって発行されたAIK証明書を含む、チケットを生成させるように構成される。チケット・サーバーはさらに、TPMからのAIKによって署名された引用、および測定ログを獲得するように構成される。チケット・サーバーはさらに、ノンスを受信し、そしてTPMからAIKによって署名された引用を生成させるように構成され、ここでAIKによって署名された引用がノンスを含む。

30

40

【0051】

本明細書において開示されるように、ユーザー・クライアント/プラットフォームは、例えば無線通信システムにおいて使用することができるWTRUまたは基地局であることができる。一例であり、他の無線通信システムにもまた適用可能であるが、図4は、E-UTRAN (Evolved-Universal Terrestrial Radio Access Network) 405を含むLTE無線通信システム/アクセス・

50

ネットワーク400を示す。E-UTRAN405は、WTRU410および幾つかのeNB(evolved Node-B:発展形ノードB)420を含む。WTRU410は、eNB420と通信状態にある。eNB420はX2インターフェイスを使用して互いにインターフェイスする。それぞれのeNB420は、S1インターフェイスを通してMME(Mobility Management Entity:モビリティ管理エンティティ)/S-GW(Serving Gateway:サービング・ゲートウェイ)430とインターフェイスする。図4においては1つのWTRU410および3つのeNB420が示されるが、無線通信システム・アクセス・ネットワーク400においては、無線のそして有線のデバイスの何れの組み合わせをも含むことができることは、明らかである。

10

【0052】

図5は、WTRU410、eNB420、およびMME/S-GW430を含む、LTE無線通信システム500の代表的ブロック図である。図5に示されるように、WTRU410、eNB420、およびMME/S-GW430は、リンケージを使用するBD(Blind Decoding:ブラインド・デコード)の複雑性削減の方法を実行するように構成される。

【0053】

典型的なWTRUにおいて見出すことができる構成要素に加えてWTRU410は、随意的に接続されたメモリ522を有するプロセッサ516、少なくとも1つの送受信機514、随意的な蓄電池520、およびアンテナ518を含む。プロセッサ516は、本明細書において開示される方法を実行するように構成される。送受信機514は、プロセッサ516およびアンテナ518と通信状態にあり、無線通信の送信および受信を容易にする。蓄電池520がWTRU410において使用される場合には、送受信機514およびプロセッサ516に電力を供給する。

20

【0054】

典型的なeNBにおいて見出すことができる構成要素に加えてeNB420は、随意的に接続されたメモリ515を有するプロセッサ517、送受信機519、およびアンテナ521を含む。プロセッサ517は、本明細書において開示される方法を実行するように構成される。送受信機519は、プロセッサ517およびアンテナ521と通信状態にあり、無線通信の送信および受信を容易にする。eNB420は、随意的に接続されたメモリ534を有するプロセッサ533を含む、MME/S-GW430に接続される。

30

【0055】

実施形態

1. 予め定められた識別子を使用してサービス・プロバイダーにログオンするステップであって、ユーザー・プラットフォームは、前記予め定められた識別子によって指し示されるアイデンティティ・プロバイダーに前記サービス・プロバイダーによってリダイレクトされることを備えることを特徴とする前記ユーザー・プラットフォームからの信頼できる認証およびアクセスのための方法。

【0056】

2. 前記アイデンティティ・プロバイダーから認証チャレンジを受信するステップを備えることを特徴とする実施形態1に記載の方法。

40

【0057】

3. 前記認証チャレンジに回答して、前記ユーザー・プラットフォームが前記認証チャレンジを受け入れたという条件にて、TPM(Trusted Platform Module:トラステッド・プラットフォーム・モジュール)に準拠したチケットを送信するステップを備えることを特徴とする先行する実施形態の内の何れか1つに記載の方法。

【0058】

4. 前記アイデンティティ・プロバイダーから成功したチケット検証を受信した際に、前記サービス・プロバイダーにアクセスするステップを備えることを特徴とする先行する

50

実施形態の内の何れか1つに記載の方法。

【0059】

5. 前記予め定められた識別子がユニバーサルリソース識別子 (URI: Universal Resource Identifier) によって表されることを特徴とする先行する実施形態の内の何れか1つに記載の方法。

【0060】

6. 前記ユーザー・プラットフォームおよびチケットを正当化する前記チケットを生成させるステップを備えることを特徴とする先行する実施形態の内の何れか1つに記載の方法。

【0061】

7. 前記認証チャレンジは、少なくとも前記予め定められた識別子およびサービス要求の種別を含むことを特徴とする先行する実施形態の内の何れか1つに記載の方法。

【0062】

8. 前記予め定められた識別子および前記サービス要求に署名するために、証明された署名鍵を生成させるステップを備えることを特徴とする先行する実施形態の内の何れか1つに記載の方法。

【0063】

9. 前記予め定められた識別子に対応するAIK (Attestation Identity Key: 証明アイデンティティ鍵) のためのパスワード、およびTPM利用を認証するための格納ルート鍵パスワードを提供するステップを備えることを特徴とする先行する実施形態の内の何れか1つに記載の方法。

【0064】

10. AIK (Attestation Identity Key: 証明アイデンティティ鍵) に対応する証明書を獲得するステップを備えることを特徴とする先行する実施形態の内の何れか1つに記載の方法。

【0065】

11. 以前に取得した証明書が入手不可という条件にて、証明書を生成させるステップを備えることを特徴とする先行する実施形態の内の何れか1つに記載の方法。

【0066】

12. 肯定的なチャレンジ確認応答に応答してノンスを受信するステップを備えることを特徴とする先行する実施形態の内の何れか1つに記載の方法。

【0067】

13. AIK (Attestation Identity Key: 証明アイデンティティ鍵) によって署名された引用を前記TPMから生成させるステップであって、前記AIKによって署名された引用が前記ノンスを含むことを備えることを特徴とする先行する実施形態の内の何れか1つに記載の方法。

【0068】

14. 前記チケットは、CSK (Certified Signing Key: 証明された署名鍵) によって署名された予め定められた識別子、CSKによって署名された要求、CSK公開鍵、およびPCA (Privacy Certification Authority: プライバシー認証局) によって発行されたAIK (Attestation Identity Key: 証明アイデンティティ鍵) 証明書、をさらに備えることを特徴とする先行する実施形態の内の何れか1つに記載の方法。

【0069】

15. 前記認証チャレンジに回答して、前記ユーザー・プラットフォームが前記認証チャレンジを受け入れたという条件にて、前記TPMからのPCR (Platform Configuration Register: プラットフォーム構成レジスタ) のAIK (Attestation Identity Key: 証明アイデンティティ鍵) によって署名された引用、および測定ログを送信するステップを備えることを特徴とする先行する実施形態の内の何れか1つに記載の方法。

10

20

30

40

50

【0070】

16．前記成功したチケット検証は、前記AIK証明書のタイムスタンプの正当化、前記AIK証明書上のPCA署名の検証、前記CSK公開鍵上のAIK署名の検証、前記CSKによって署名された予め定められた識別子の検証、前記CSKによって署名された要求の検証、前記測定ログの正当化、および前記引用の検証、を含むことを特徴とする先行する実施形態の内の何れか1つに記載の方法。

【0071】

17．その後のサービス・プロバイダー・アクセスのために、証明された署名鍵によって保護された暗号化されたクッキーを受信するステップを備えることを特徴とする先行する実施形態の内の何れか1つに記載の方法。

10

【0072】

18．前記認証チャレンジは、認可チャレンジを含むことを特徴とする先行する実施形態の内の何れか1つに記載の方法。

【0073】

19．証明チャレンジを備えることを特徴とする先行する実施形態の内の何れか1つに記載の方法。

【0074】

20．信頼できる認証およびアクセスを支援するための装置であって、前記プラットフォームが、予め定められた識別子を使用してサービス・プロバイダーにアクセスするように構成されたインターフェイス・モジュールを備えることであって、前記装置が、前記予め定められた識別子によって指し示されるアイデンティティ・プロバイダーに前記サービス・プロバイダーによってリダイレクトされること、を特徴とする装置。

20

【0075】

21．認証チャレンジが受け入れられたという条件にて、TPM(Trusted Platform Module: トラステッド・プラットフォーム・モジュール)に準拠したチケットを送信することによって前記認証チャレンジに回答するように構成されたチケット・サーバーを備えることを特徴とする実施形態20に記載の装置。

【0076】

22．前記インターフェイス・モジュールは、前記アイデンティティ・プロバイダーから成功したチケット検証を受信し、そして前記サービス・プロバイダーにおけるサービスにアクセスするように構成されることを備えることを特徴とする実施形態20または21の何れかに記載の装置。

30

【0077】

23．前記チケット・サーバーは、CSK(Certified Signing Key: 証明された署名鍵)によって署名された予め定められた識別子、CSKによって署名された要求、CSK公開鍵、およびPCA(Privacy Certification Authority: プライバシー認証局)によって発行されたAIK(Attestation Identity Key: 証明アイデンティティ鍵)証明書を含むチケットを生成させるようにさらに構成されることを特徴とする実施形態20乃至22の内の何れかに記載の装置。

40

【0078】

24．前記チケット・サーバーは、前記TPMからのAIK(Attestation Identity Key: 証明アイデンティティ鍵)によって署名された引用、および測定ログを獲得するようにさらに構成されることを特徴とする実施形態20乃至23の内の何れかに記載の装置。

【0079】

25．前記チケット・サーバーは、ノンスを受信し、そしてAIK(Attestation Identity Key: 証明アイデンティティ鍵)によって署名された引用を前記TPMから生成させるようにさらに構成されることであって、前記AIKによって署名された引用が前記ノンスを含むことを特徴とする実施形態20-24の内の何れかに

50

記載の装置。

【0080】

特徴および要素が上で特定の組み合わせにて記述されているが、それぞれの特徴または要素は、他の特徴および要素なしで単独にて、または他の特徴および要素のあるなしに拘わらず様々な組み合わせにて使用することができる。本明細書において提供される方法またはフローチャートは、汎用目的のコンピューターまたはプロセッサによる実行のための、コンピューターにて読み取り可能な記憶装置媒体に組み込まれたコンピューター・プログラム、ソフトウェア、またはファームウェアにて実施することができる。コンピューターにて読み取り可能な記憶装置媒体の例としては、ROM (Read Only Memory: リード・オンリー・メモリ)、RAM (Random Access Memory: ランダム・アクセス・メモリ)、レジスタキャッシュ・メモリ、半導体メモリ・デバイス、内蔵ハード・ディスクおよび着脱可能ディスクなどの磁気媒体、磁気 - 光学媒体、ならびにCD-ROMディスクおよびDVD (Digital Versatile Disk: デジタル多用途ディスク)などの光学媒体が含まれる。

10

【0081】

適当なプロセッサの例としては、汎用プロセッサ、専用プロセッサ、従来プロセッサ、DSP (Digital Signal Processor: デジタル・シグナル・プロセッサ)、複数のマイクロプロセッサ、DSPコアに関連付けられた1つまたは複数のマイクロプロセッサ、コントローラー、マイクロコントローラー、ASIC (Application Specific Integrated Circuit: 特定用途向け集積回路)、FPGA (Field Programmable Gate Array: フィールド・プログラマブル・ゲートアレイ)回路、他の何れかの種別のIC (Integrated Circuit: 集積回路)、および/または状態マシンが含まれる。

20

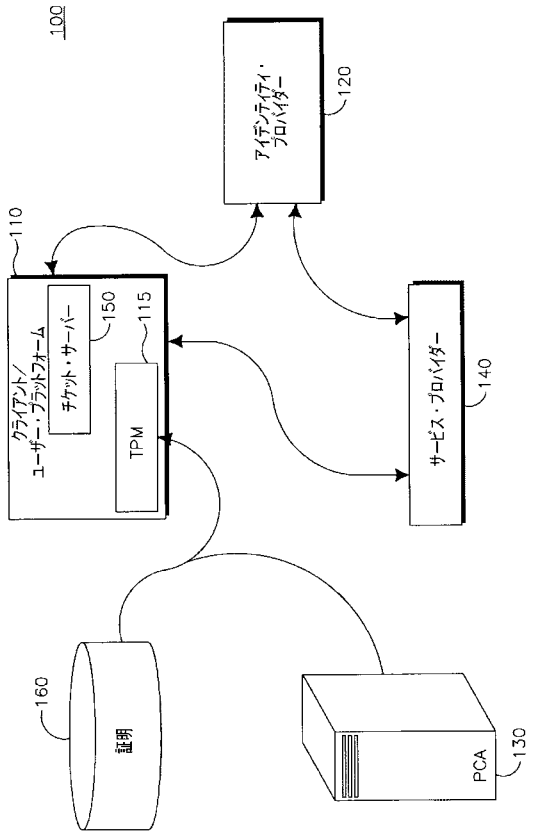
【0082】

ユーザー・プラットフォームは、WTRUを含む多くのプラットフォームの内の何れであることもできる。WTRU、UE、端末、基地局 (base station)、RNC (Radio Network Controller: 無線ネットワークコントローラー)、または任意のホスト・コンピューターにおいて使用するための無線周波数送受信機を実施するために、ソフトウェアに関連付けられたプロセッサを使用することができる。WTRUは、ハードウェアおよび/またはソフトウェアにて実施され、カメラ、ビデオ・カメラ・モジュール、テレビ電話、スピーカーフォン、振動デバイス、スピーカー、マイクロホン、テレビ送受信機、ハンズフリー受話器、キーボード、ブルートゥース (Bluetooth (登録商標))モジュール、FM (Frequency Modulated: 周波数変調)無線ユニット、LCD (Liquid Crystal Display: 液晶ディスプレイ)表示ユニット、OLED (Organic Light-Emitting Diode: 有機発光ダイオード)表示ユニット、デジタル音楽プレーヤー、メディア・プレーヤー、テレビゲーム・プレーヤー・モジュール、インターネット・ブラウザー、および/または任意のWLAN (Wireless Local Access Network: 無線ローカル・エリア・ネットワーク)モジュールもしくはUWB (Ultra Wide Band: 超広帯域)モジュールなどのモジュールと連動して使用することができる。

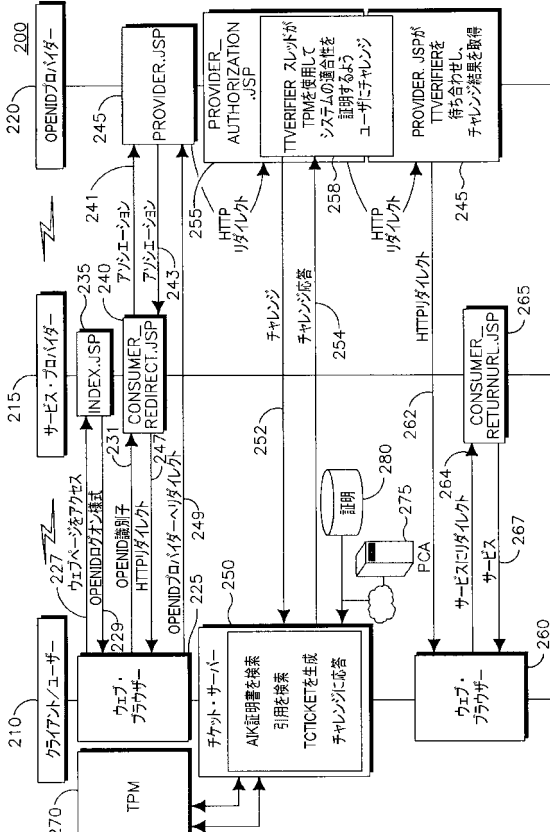
30

40

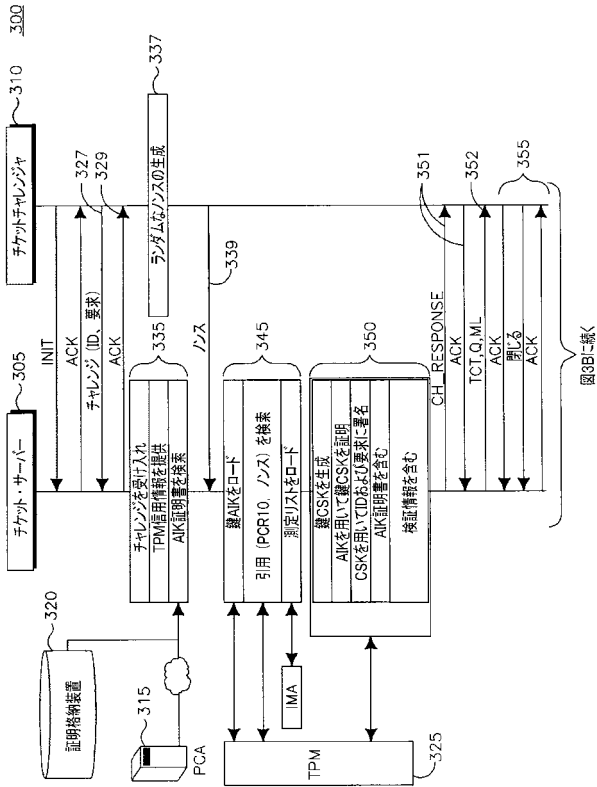
【 図 1 】



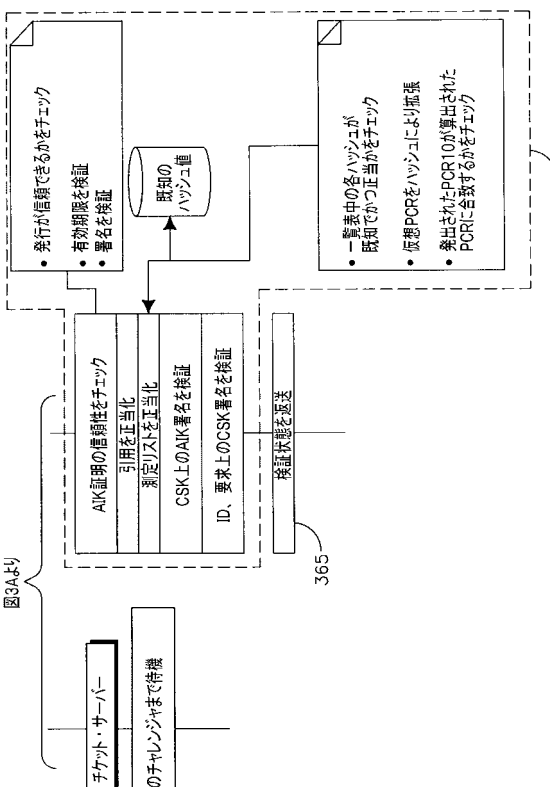
【 図 2 】



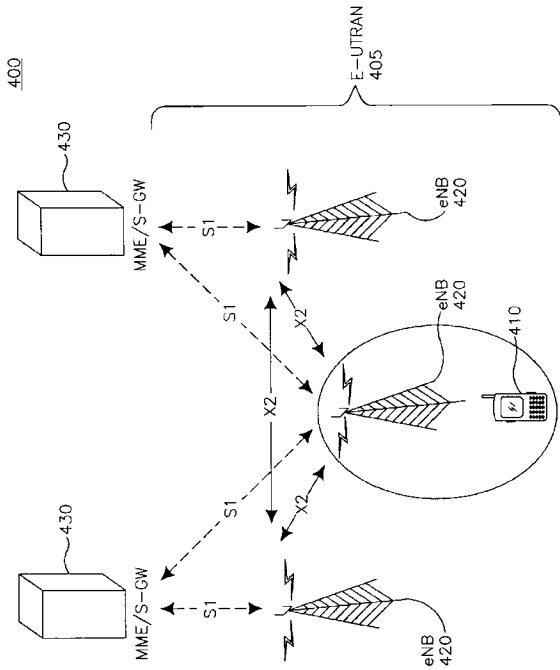
【 図 3 (a) 】



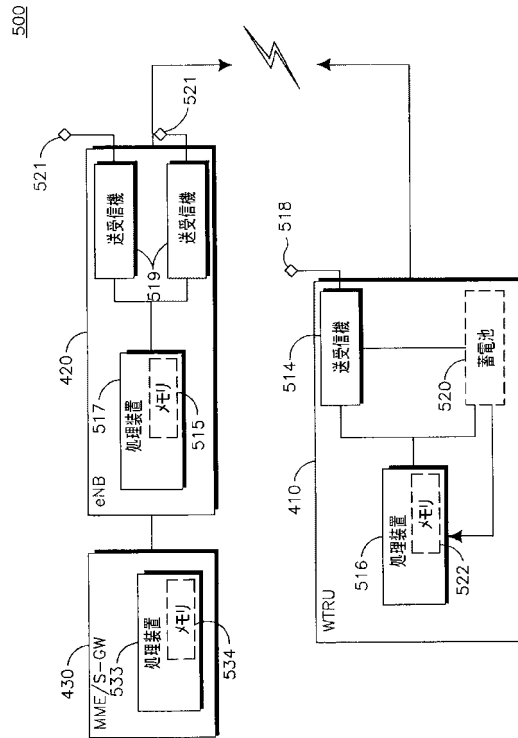
【 図 3 (b) 】



【 図 4 】



【 図 5 】



【 手続 補正 書 】

【 提出 日 】 平成 29 年 6 月 9 日 (2017.6.9)

【 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 】

トラステッドモジュールを含むユーザプラットフォームによって、サービスプロバイダからのサービスにアクセスする方法であって、

ユーザ識別を使用して、前記サービスプロバイダにログオンするステップと、

前記ユーザプラットフォームが認証チャレンジを前記サービスプロバイダから受信するステップと、

前記認証チャレンジに回答して、前記トラステッドモジュールにおいて、前記認証チャレンジへの認証応答を生成するステップであって、前記認証応答は、認証証明または前記認証証明への参照を含むことができる、ステップと、

前記認証応答の検証が成功するとき、前記サービスプロバイダからの前記サービスにアクセスするステップと

を備えたことを特徴とする方法。

【 請 求 項 2 】

前記認証チャレンジにさらに回答して、ユーザのローカル認証を実行するステップをさらに備えたことを特徴とする請求項 1 に記載の方法。

【 請 求 項 3 】

前記ユーザの前記ローカル認証は、前記ユーザの 1 つまたは複数の生体認証を使用して

実行されることを特徴とする請求項 2 に記載の方法。

【請求項 4】

前記検証が失敗する場合、認証失敗メッセージを受信するステップをさらに備えたことを特徴とする請求項 1 に記載の方法。

【請求項 5】

前記ユーザ識別は鍵に対応し、前記方法は、
前記鍵を使用して、前記認証証明を前記トラステッドモジュールから取り出すステップをさらに備えたことを特徴とする請求項 1 に記載の方法。

【請求項 6】

前記サービスプロバイダからの前記サービスにアクセスするとき、ユーザと関連付けられたデータにアクセスするために前記サービスプロバイダを認可するステップをさらに備えたことを特徴とする請求項 1 に記載の方法。

【請求項 7】

前記認証応答は、チケットの真正を立証するデータを含む前記チケットを含むことを特徴とする請求項 1 に記載の方法。

【請求項 8】

前記認証チャレンジは、少なくとも前記ユーザ識別およびサービス要求のタイプを含むことを特徴とする請求項 1 に記載の方法。

【請求項 9】

前記ユーザ識別および前記サービス要求を署名するための証明された署名鍵を生成するステップをさらに備えたことを特徴とする請求項 8 に記載の方法。

【請求項 10】

前記ユーザ識別は、証明アイデンティティ鍵 (A I K) とさらに関連付けられ、前記方法は、

前記ユーザ識別に対応する前記 A I K に対するパスワード、および前記トラステッドモジュールの使用を認証するためのストレージルート鍵パスワードを提供するステップをさらに備えたことを特徴とする請求項 1 に記載の方法。

【請求項 11】

前記ユーザ識別は、証明アイデンティティ鍵 (A I K) とさらに関連付けられ、および前記認証証明は、前記 A I K に対応することを特徴とする請求項 1 に記載の方法。

【請求項 12】

前記認証証明は、前に取得された認証証明が利用可能でないことを条件に取得されることを特徴とする請求項 11 に記載の方法。

フロントページの続き

Fターム(参考) 5J104 AA16 EA16 LA03 MA01 NA02 NA38

【外国語明細書】
2017139026000001.pdf