(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5688087号
(P5688087)
(45)発行日　平成27年3月25日(2015.3.25)　(24)登録日　平成27年1月30日(2015.1.30)

(51)Int.Cl.		F I		
G06F 21/33	(2013.01)	G06F	21/33	
H04L 9/32	(2006.01)	H04L	9/00	675Z
H04L 9/08	(2006.01)	H04L	9/00	601A

請求項の数 19　(全 21 頁)

(21)出願番号　特願2012-529721 (P2012-529721)
(86)(22)出願日　平成21年9月14日 (2009.9.14)
(65)公表番号　特表2013-504832 (P2013-504832A)
(43)公表日　平成25年2月7日 (2013.2.7)
(86)国際出願番号　PCT/US2009/056823
(87)国際公開番号　WO2011/031272
(87)国際公開日　平成23年3月17日 (2011.3.17)
審査請求日　平成24年5月14日 (2012.5.14)

(73)特許権者　510030995
インターデイジタル　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　スイート　３００
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(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
(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)【特許請求の範囲】
【請求項１】
ユーザー・プラットフォームからの信頼されている認証およびアクセスのための方法であって、
前記ユーザー・プラットフォームが、アイデンティティ・プロバイダーに関連付けられている識別子および前記ユーザー・プラットフォームの証明アイデンティティ鍵（ＡＩＫ）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、前記ユーザー・プラットフォームは、前記識別子によって示される前記アイデンティティ・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、ステップと、
前記ユーザー・プラットフォームが、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、
前記ユーザー・プラットフォーム上に存在する信頼されているモジュールを介して、証明機関による前記証明アイデンティティ鍵の証明を示す証明書を取得するステップと、
前記信頼されているモジュールにおいて、前記アイデンティティ・プロバイダーにおける前記ユーザー・プラットフォームの認証のためのチケットを生成するステップであって、前記チケットは、前記証明機関による前記証明アイデンティティ鍵の前記証明を示す前記証明書を備える、ステップと、
前記信頼されているモジュールから、前記ユーザー・プラットフォームの構成を記述する１つまたは複数のプラットフォーム構成レジスタ（ＰＣＲ）値の署名された引用を検索するステップであって、前記引用は、前記証明アイデンティティ鍵によって署名される、

ステップと、
前記認証チャレンジに応答して、前記チケットおよび前記署名された引用を、前記ユーザー・プラットフォームの前記認証のために前記アイデンティティ・プロバイダーに送信するステップと、
前記チケットおよび前記署名された引用の成功した検証を受信すると、前記サービス・プロバイダーにアクセスし、それによって前記ユーザー・プラットフォームのユーザーが正当であり、および、前記ユーザー・プラットフォームが信頼できることを保証するステップと
を備えることを特徴とする方法。
【請求項２】
前記アイデンティティ・プロバイダーに関連付けられた前記識別子は、ユニバーサルリソース識別子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】
前記チケットは、前記ユーザー・プラットフォームおよび前記チケットの信頼性を正当であると確認するデータを備えてい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、少なくとも前記アイデンティティ・プロバイダーに関連付けられた前記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請求項１に記載の方法。
【請求項５】
前記ユーザー・プラットフォームが、前記識別子および前記サービス要求を署名するために、証明された署名鍵を生成す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】
前記ユーザー・プラットフォームが、前記識別子に対応する前記証明アイデンティティ鍵に対するパスワード、および、前記信頼されている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ることを特徴とする請求項１に記載の方法。
【請求項７】
前記証明書は、前記証明アイデンティティ鍵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８】
以前に獲得された証明書が利用できないという条件にて、前記証明書が取得されることを特徴とする請求項７に記載の方法。
【請求項９】
前記アイデンティティ・プロバイダーから受信された前記認証チャレンジに応答して、肯定的なチャレンジ確認応答を送信するステップと、
前記アイデンティティ・プロバイダーに送信された前記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と、
前記署名された引用を生成するステップであって、前記署名された引用は、前記証明アイデンティティ鍵によって署名され、および、前記ノンスを含む、ステップと
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、証明された署名鍵（ＣＳＫ）署名された所定の識別、ＣＳＫの署名された要求、ＣＳＫ公開鍵、および前記証明書をさらに備え、ならびに、前記証明書は、プライバシー認証局（ＰＣＡ）の発行されたＡＩＫ証明書を備えることを特徴とする請求項１に記載の方法。
【請求項１１】
前記認証チャレンジに応答して、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、前記信頼されているモジュールからの前記ＰＣＲ値の前

記署名された引用、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１０に記載の方法。
【請求項１２】
前記成功したチケット検証は、前記アイデンティティ・プロバイダーが、前記証明書のタイムスタンプを正当であると確認し、前記証明書上の前記証明機関の署名を検証し、前記ＣＳＫ公開鍵上のＡＩＫ署名を検証し、前記ＣＳＫの署名された所定の識別を検証し、前記ＣＳＫの署名された要求を検証し、前記測定ログを正当であると確認し、および、前記引用を検証したことを示すことを特徴とする請求項１１に記載の方法。
【請求項１３】
前記ユーザー・プラットフォームが、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１４】
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。
【請求項１５】
前記ユーザー・プラットフォームが、証明チャレンジ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１６】
信頼されている認証およびアクセスを支援するためのユーザー・プラットフォームであって、
アイデンティティ・プロバイダーに関連付けられている識別子および前記ユーザー・プラットフォームの証明アイデンティティ鍵（ＡＩＫ）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、前記ユーザー・プラットフォームは、前記識別子によって示される前記アイデンティティ・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、インターフェイス・モジュールと、
証明機関による前記証明アイデンティティ鍵の証明を示す証明書を取得するように構成された信頼されているモジュールであって、前記ユーザー・プラットフォームは、前記アイデンティティ・プロバイダーにおいて前記ユーザー・プラットフォームの認証のためのチケットを生成するように構成され、前記チケットは、前記証明機関による前記証明アイデンティティ鍵の前記証明を示す前記証明書を備えている、信頼されているモジュールと、
前記信頼されているモジュールから、前記ユーザー・プラットフォームの構成を記述する１つまたは複数のプラットフォーム構成レジスタ（ＰＣＲ）値の、前記証明アイデンティティ鍵によって署名された引用を検索することによって、ならびに、前記チケットおよび前記署名された引用を送信することによって、前記アイデンティティ・プロバイダーから受信された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、
前記チケットおよび前記署名された引用の成功した検証を受信して前記サービス・プロバイダー上のサービスにアクセスし、それによって、前記ユーザー・プラットフォームのユーザーが正当であり、および、前記ユーザー・プラットフォームが信頼できることを保証するように構成された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ユーザー・プラットフォーム。
【請求項１７】
前記チケットは、証明された署名鍵（ＣＳＫ）の署名された所定の識別、ＣＳＫの署名された要求、ＣＳＫ公開鍵、および、前記証明書を含み、ならびに、前記証明書は、プライバシー認証局（ＰＣＡ）の発行されたＡＩＫ証明書を備えることを特徴とする請求項１６に記載のユーザー・プラットフォーム。
【請求項１８】
前記チケット・サーバーは、前記信頼されているモジュールからのＡＩＫの署名された

引用、および測定ログを取得するようにさらに構成されていることを特徴とする請求項１７に記載のユーザー・プラットフォーム。

【請求項１９】

前記チケット・サーバーは、ノンスを受信し、および、前記信頼されているモジュールからのＡＩＫの署名された引用を生成するようにさらに構成されており、ならびに、前記ＡＩＫの署名された引用は、前記ノンスを含むことを特徴とする請求項１６に記載のユーザー・プラットフォーム。

【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。ただ一つのディ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。ディ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、ユーザーがディ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欲したとき、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充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。

【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。

【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。

【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される。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。この組み合わさ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、ＰＣＡ１３０と通信状態にあり、ＰＣＡ１３０は例えば証明を保存する格納媒体１６０と通信状態にある。

【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ＴＰＭ１１５を含む。ＴＰＭ１１５は、鍵、パスワード、ディ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。ＴＰＭ１１５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、ＴＰＭ１１５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。

【００１３】

ＴＰＭ１１５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の公開の部分は一般に、証明の目的のためのＥＫ証明書によってＰＣＡ１３０によって既知である。一般にＴＰＭ１１５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ＰＣＡ１３０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。ＰＣＡ１３０はその一覧表中にこのＥＫを見出したなら、ＰＣＡ１３０はＴＰＭ１１５のＡＩＫに関する証明書を発行する。そしてＴＰＭ１１５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。

【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、ＴＰＭ１１５によって制限される。したがって、ＣｅｒｔｉｆｙＫｅｙ動作と呼ばれる間接的解決方法を使用して、署名鍵が、ＴＰＭ１１５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。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ＴｉｃｋｅｔＳｅｒｖｅｒ１５０を含む。ＴｉｃｋｅｔＳｅｒｖｅｒ１５０はユーザーを認証する。ＴｉｃｋｅｔＳｅｒｖｅｒ１５０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。ＴｉｃｋｅｔＳｅｒｖｅｒ１５０は現在の非信頼済みＯｐｅｎＩＤ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す。より多くのセキュリティ重要情報および動作がＴｉｃｋｅｔＳｅｒｖｅｒ１５０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。

【００１６】

ユーザーは、ＴＰＭ１１５において生成されたＡＩＫを証明するためにＰＣＡ１３０を選択せねばならない。ＰＣＡ１３０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。ＰＣＡ１３０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。

【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、ＰＣＡ１３０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。ＰＣＡ１３０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。

【００１８】

ＰＣＡ１３０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、ＴＰＭ１１５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）。

【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ＯｐｅｎＩＤ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。

【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。

【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。

【００２３】

次にＯｐｅｎＩＤプロバイダー２２０は、ｐｒｏｖｉｄｅｒ．ｊｓｐウェブページ２４５からｐｒｏｖｉｄｅｒ＿ａｕｔｈｏｒｉｚａｔｉｏｎ．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＿ａｕｔｈｏｒｉｚａｔｉｏｎ．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ＴＴｖｅｒｉｆｉｅｒ２５８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＿ａｕｔｈｏｒｉｚａｔｉｏｎ．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ＴＴｖｅｒｉｆｉｅｒ２５８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。

【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へのアクセスを許可する。

【００２５】

ここで図３（ａ）および図３（ｂ）を参照すると、ＴｉｃｋｅｔＳｅｒｖｅｒ３０５およびＴｉｃｋｅｔ　Ｃｈａｌｌｅｎｇｅｒ３１０の間の信号フローチャート３００が示される。ＴｉｃｋｅｔＳｅｒｖｅｒ３０５、ならびにＰＣＡ３１５、証明格納媒体３２０、およびＴＰＭ３２５の間の信号フローもまた示される。

【００２６】

ＴｉｃｋｅｔＳｅｒｖｅｒ３０５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ＴｉｃｋｅｔＳｅｒｖｅｒ３０５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ＴＰＭ３２５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コマンド中に含められる。そしてＴｉｃｋｅｔＳｅｒｖｅｒ３０５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ＴＣＴｉｃｋｅｔ生成３５０のために必要である。証明書は、ＰＣＡ３１５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ＰＣＡ３１５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ＰＣＡ３１５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、ＴＰＭ３２５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、ＴＰＭ３２５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ＴｉｃｋｅｔＳｅｒｖｅｒ３０５からＴＰＭ３２５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　Ｃｈａｌｌｅｎｇｅｒ３１０はランダムなノンス３３７を生成する。ＴｉｃｋｅｔＳｅｒｖｅｒ３０５は、ノンス・メッセージ３３９を介してＴｉｃｋｅｔ　Ｃｈａｌｌｅｎｇｅｒ３１０からランダムなノンス３３７を受信する。ノンスを含む、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、ＴＰＭ３２５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】
ＴｉｃｋｅｔＳｅｒｖｅｒ３０５は次に、集合的に３５０として示されるようにＴＣＴｉｃｋｅｔを生成する。ＴＣＴｉｃｋｅｔ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、ＣｅｒｔｉｆｙＫｅｙ動作を使用して、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Ｔｉｃｋｅｔ　Ｃｈａｌｌｅｎｇｅｒ３１０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Ｔｉｃｋｅｔ　Ｃｈａｌｌｅｎｇｅｒ３１０に送り返される。ＣＨ＿ＲＥＳＰＯＮＳＥ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Ｔｉｃｋｅｔ　Ｃｈａｌｌｅｎｇｅｒ３１０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ＴＴ　Ｖｅｒｉｆｉｅｒ　Ｔｈｒｅａｄ２５８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でなければならない。

【００３１】
メッセージ３５５を介してＴＣＴｉｃｋｅｔ３５０を確認すると、ここでＴｉｃｋｅｔ　Ｃｈａｌｌｅｎｇｅｒ３１０は、以下のデータを有する。すなわち：アンチリプレイプロテクション（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、Ｔｉｃｋｅｔ　Ｃｈａｌｌｅｎｇｅｒ３１０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。

【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ー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。

【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機能性を使用するかすることができる。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。

【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　ＯｐｅｎＩＤ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、ＯｐｅｎＩＤ実施方法はＯｐｅｎＩＤ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ＯｐｅｎＩＤ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ＯｐｅｎＩＤ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ＯｐｅｎＩＤ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ＯｐｅｎＩＤ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ＯｐｅｎＩＤ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。

【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ＴｉｃｋｅｔＳｅｒｖｅｒ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。

【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ＯｐｅｎＩＤ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ＴｉｃｋｅｔＳｅｒｖｅｒに対して新しいチャレンジを生成する。信頼できるＴｉｃｋｅｔＳｅｒｖｅｒ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。ＴｉｃｋｅｔＳｅｒｖｅｒ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、ＴｉｃｋｅｔＳｅｒｖｅｒ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実にするように、生体認証が為される。

【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ＴｉｃｋｅｔＳｅｒｖｅｒ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。ＴｉｃｋｅｔＳｅｒｖｅｒ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（ｄａｓｈｂｏａｒｄ）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ＯｐｅｎｌＤ／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ＴＰＭ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、説明された方法は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をウェブ・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。

【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ケージを可能にする。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することができるように、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ー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ー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。ブラウザー拡張は、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ー拡張に返送する。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ー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。

【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。

【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、認証チャレンジが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応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。

【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・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、明らかであるべきである。

【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ー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。プロセッサー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、プロセッサー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およびプロセッサー５１６に電力を供給する。

【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ー５１７、送受信機５１９、およびアンテナ５２１を含む。プロセッサー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、プロセッサー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ー５３３を含む、ＭＭＥ／Ｓ－ＧＷ４３０に接続される。

【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。

【００５７】

３．前記認証チャレンジに応答して、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 Ｍｏ

ｄｕｌｅ：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応答して、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。

【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。

【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。

【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応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。

【００７７】

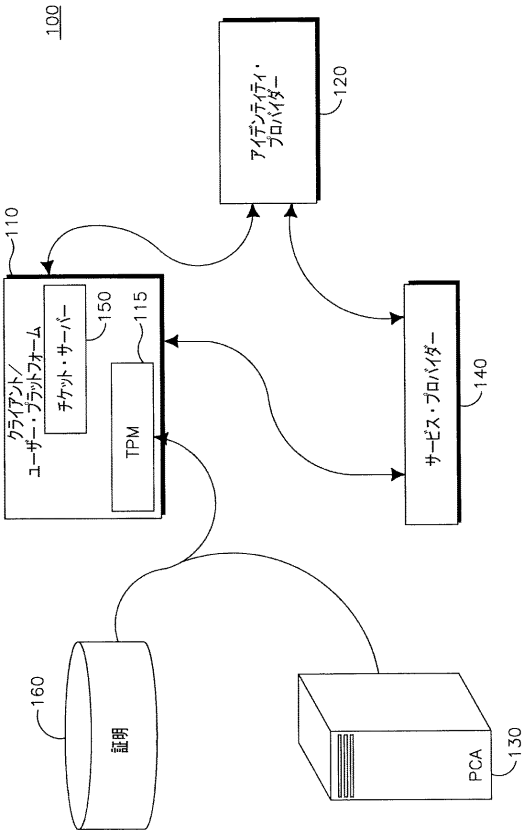
２３．前記チケット・サーバーは、ＣＳＫ（Ｃｅｒｔｉｆｉｅｄ Ｓｉｇｎｉｎｇ Ｋｅｙ：証明された署名鍵）によって署名された予め定められた識別子、ＣＳＫによって署名された要求、ＣＳＫ公開鍵、およびＰＣＡ（Ｐｒｉｖａｃｙ Ｃｅｒｔｉｆｉｃａｔｉｏｎ Ａｕｔｈｏｒｉｔｙ：プライバシー認証局）によって発行されたＡＩＫ（Ａｔｔｅｓｔａｔｉｏｎ Ｉｄｅｎｔｉｔｙ Ｋｅｙ：証明アイデンティティ鍵）証明書を含むチケットを生成させるようにさらに構成されることを特徴とする実施形態２０乃至２２の内の何れかに記載の装置。

【００７８】

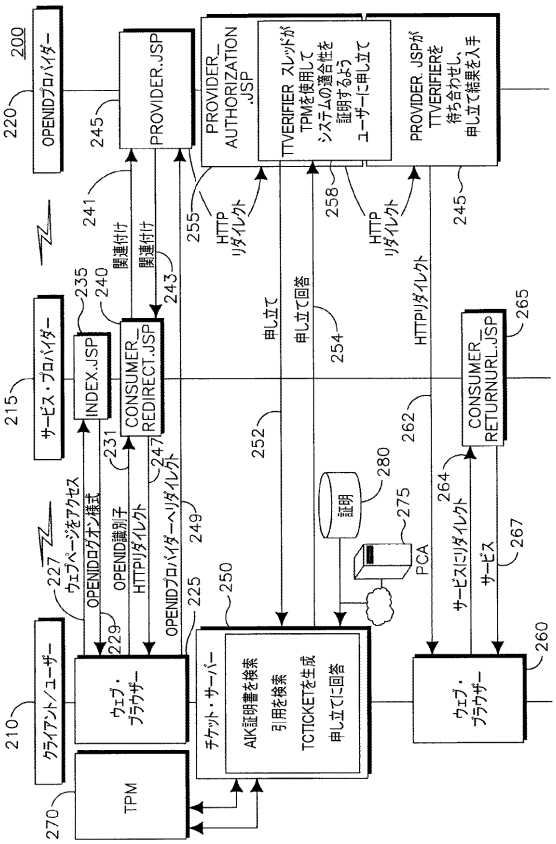
２４．前記チケット・サーバーは、前記ＴＰＭからのＡＩＫ（Ａｔｔｅｓｔａｔｉｏｎ Ｉｄｅｎｔｉｔｙ Ｋｅｙ：証明アイデンティティ鍵）によって署名された引用、および測定ログを獲得するようにさらに構成されることを特徴とする実施形態２０乃至２３の内の何れかに記載の装置。

【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ー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：ディジタル多用途ディスク）などの光学媒体が含まれる。
【００８１】
適当なプロセッサーの例としては、汎用プロセッサー、専用プロセッサー、従来のプロセッサー、ＤＳＰ（Ｄｉｇｉｔａｌ Ｓｉｇｎａｌ Ｐｒｏｃｅｓｓｏｒ：ディジタル・シグナル・プロセッサー）、複数のマイクロプロセッサー、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ー、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。
【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ー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、ディ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。

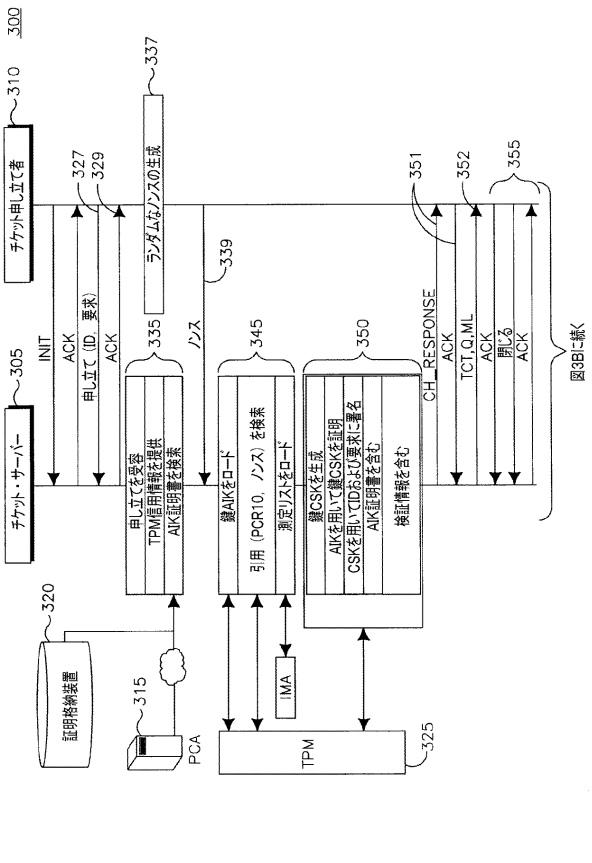
【図１】


100
110
クライアント/
ユーザー・プラットフォーム
チケット・サーバー
150
TPM
115
アイデンティティ・
プロバイダー
120
サービス・プロバイダー
140
証明
160
PCA
130

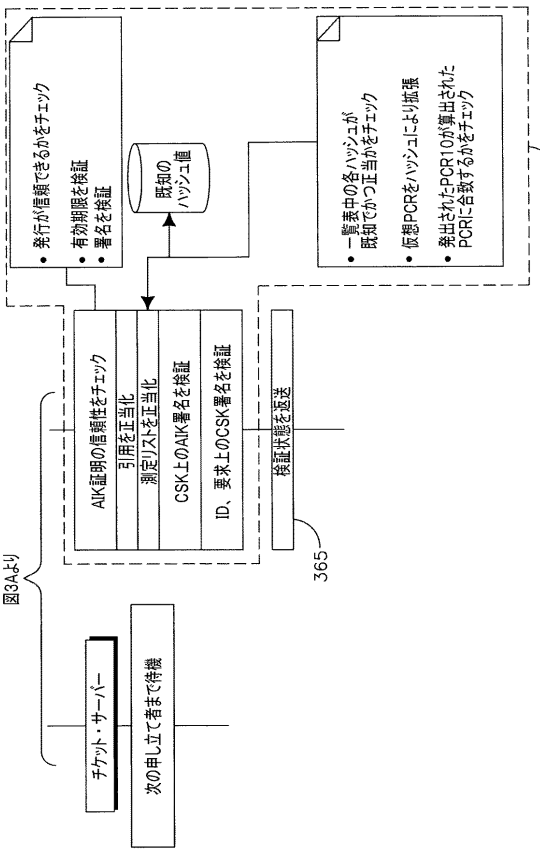
【図２】


200
OPENIDプロバイダー
220
PROVIDER.JSP
245
PROVIDER_
AUTHORIZATION
JSP
TTVERIFIER スレッドが
TPMを使用して
システムの適合性を
証明するよう
ユーザーに申し立て
PROVIDER.JSPが
TTVERIFIERを
待ち合わせし
申し立て結果を入手
241
関連付け
235
240
INDEX.JSP
CONSUMER_
REDIRECT.JSP
243
255
HTTP
リダイレクト
258
254
申し立て
申し立て回答
HTTP/リダイレクト
265
CONSUMER_
RETURNURL.JSP
262
264
サービスにリダイレクト
サービス
267
260
ウェブ・
ブラウザー
215
サービス・プロバイダー
231
247
252
280
証明
275
PCA
227
ウェブページをアクセス
OPENIDログオン/識別
229
OPENID識別子
HTTP/リダイレクト
249
OPENIDプロバイダーへリダイレクト
225
250
210
クライアント/ユーザー
ウェブ・
ブラウザー
チケット・サーバー
AIK証明書を検索
引用を検索
TCTICKETを生成
申し立てに回答
270
TPM

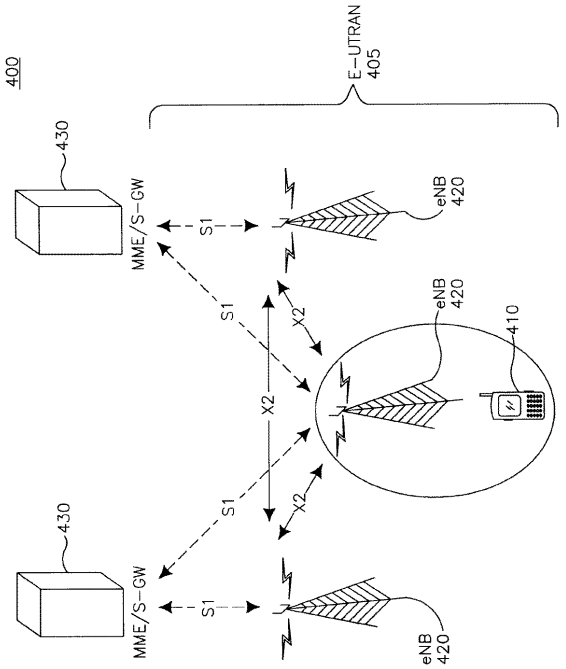
【図３（ａ）】


300
310
チケット申し立て者
337
327
329
ランダムなノンスの生成
305
INIT
ACK
申し立て（ID、要求）
ACK
335
339
ノンス
345
350
351
352
355
CH_RESPONSE
ACK
TCT,Q,ML
ACK
閉じる
ACK
チケット・サーバー
申し立てを受領
TPM情報を提供
AIK証明書を検索
鍵AIKをロード
引用（PCR10、ノンス）を検索
測定リストをロード
鍵CSKを生成
AIKを用いて鍵CSKを証明
CSKを用いてIDおよび要求に署名
AIK証明書を含む
検証情報を含む
図3Bに続く
320
証明格納装置
315
PCA
IMA
TPM
325

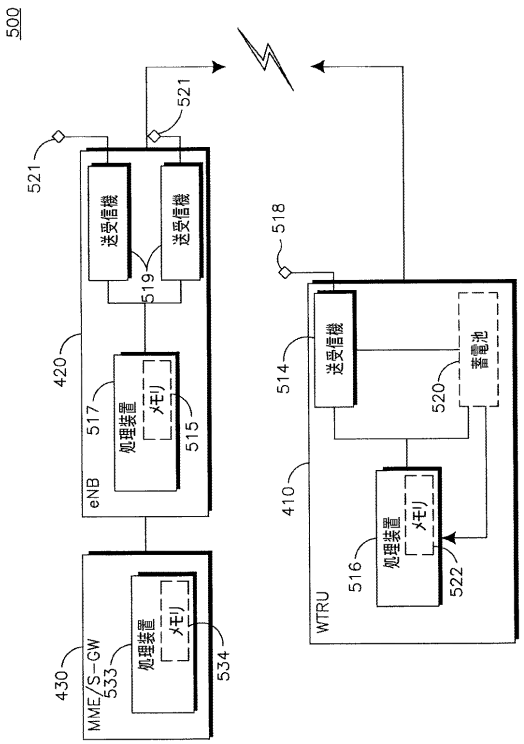
【図３（ｂ）】


• 発行が信頼できるかをチェック
• 有効期限を検証
• 署名を検証
既知の
ハッシュ値
• 一覧表中の各ハッシュが
既知でかつ正当かをチェック
• 仮想PCRをハッシュにより拡張
• 算出されたPCR10が算出された
PCRに合致するかをチェック
360
図3Aより
AIK証明の信頼性をチェック
引用を正当化
測定リストを正当化
CSK上のAIK署名を検証
ID、要求上のCSK署名を検証
検証状態を返送
365
チケット・サーバー
次の申し立て者まで待機

【図４】


400
E-UTRAN
405
430
MME/S-GW
S1
eNB
420
X2
410
430
MME/S-GW
S1
eNB
420

【図５】


500
521
送受信機
519
420
517
処理装置
メモリ
515
eNB
430
MME/S-GW
533
処理装置
メモリ
534
518
514
送受信機
520
蓄電池
410
516
処理装置
メモリ
522
WTRU

フロントページの続き

審査官　戸島　弘詩

(56)参考文献　特開２００８－０３３５１２（ＪＰ，Ａ）
特表平１１－５０７７５２（ＪＰ，Ａ）
国際公開第２００９／１０５５４２（WO，Ａ１）
特開２００７－２１９９３５（ＪＰ，Ａ）
米国特許第０５５９０１９９（ＵＳ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／３０－２１／４６
Ｈ０４Ｌ９／００