(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2017-519412
(P2017-519412A)
(43)公表日　平成29年7月13日(2017.7.13)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601B	5J104
H04L 9/32	(2006.01)	H04L	9/00	601F	
G06F 21/31	(2013.01)	H04L	9/00	675B	
G06F 21/33	(2013.01)	H04L	9/00	673D	
		G06F	21/31		

審査請求 未請求　予備審査請求 未請求　（全 25 頁）　最終頁に続く

(21)出願番号　特願2016-566924 (P2016-566924)
(86)(22)出願日　平成27年5月1日(2015.5.1)
(85)翻訳文提出日　平成28年11月2日(2016.11.2)
(86)国際出願番号　PCT/US2015/028927
(87)国際公開番号　WO2015/168644
(87)国際公開日　平成27年11月5日(2015.11.5)
(31)優先権主張番号　14/268,619
(32)優先日　平成26年5月2日(2014.5.2)
(33)優先権主張国　米国(US)

(71)出願人　516329587
ノック　ノック　ラブズ，　インコーポレイテッド
アメリカ合衆国　カリフォルニア州　９４３０３　パロ　アルト　ジェン　ロード　２１００　スイート　１０５
(74)代理人　100086771
弁理士　西島　孝喜
(74)代理人　100088694
弁理士　弟子丸　健
(74)代理人　100094569
弁理士　田中　伸一郎
(74)代理人　100067013
弁理士　大塚　文昭

最終頁に続く

(54)【発明の名称】認証装置の登録のための強化されたセキュリティ

(57)【要約】
登録時の強化されたセキュリティのためのシステム、装置、方法、及び機械可読媒体が説明される。例えば、方法の一実施形態は、依拠当事者側で認証部を登録するための要求を受信することと、ユーザから認証されたアウトオブバンド通信チャネルを介して依拠当事者にコードを送信することと、コードを使用してユーザのアイデンティティを検証し、肯定的な検証に応答して認証部を応答性良く登録することと、を含む。

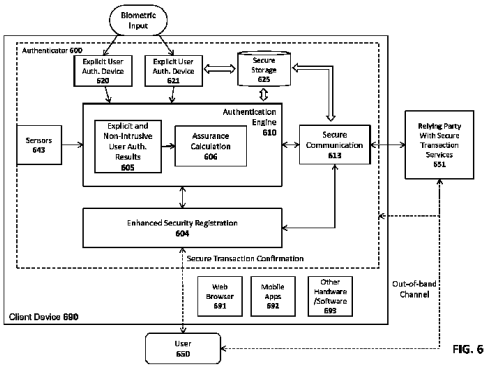


FIG. 6

【特許請求の範囲】
【請求項１】
依拠当事者側で、ユーザから認証部を登録するための要求を受信することと、
認証されたアウトオブバンド通信チャネルを介して前記ユーザから前記依拠当事者へ、又は前記依拠当事者から前記ユーザへ、コードを送信することと、
前記コードを使用して前記ユーザのアイデンティティを検証し、肯定的な検証に応答して前記認証部を応答性良く登録することと、を含む、方法。
【請求項２】
前記コードを前記検証することが、
前記ユーザの認証部のセキュアディスプレイ内に前記コードを表示することと、前記セキュアディスプレイ上に表示された前記コードを前記認証されたアウトオブバンド通信チャネルを介して送信するよう前記ユーザに求めることと、を含む、セキュアトランザクション確認操作を遂行することを更に含む、請求項１に記載の方法。
【請求項３】
前記コードが、前記ユーザの認証部によって生成された秘密コードである、請求項１に記載の方法。
【請求項４】
前記認証部を登録するための前記要求に応答して、前記認証部に関連付けられた公開鍵を生成することと、前記公開鍵を前記依拠当事者に伝送することと、を更に含む、請求項１に記載の方法。
【請求項５】
前記公開鍵に対してハッシュ操作を遂行することによって前記コードを生成することを更に含む、請求項４に記載の方法。
【請求項６】
前記ハッシュ操作が、ＳＨＡ－２５６、ＳＨＡ－１、又はＳＨＡ－３ハッシュ操作を含む、請求項５に記載の方法。
【請求項７】
前記アウトオブバンド通信チャネルが、郵便、電子メール、又はショートメッセージサービス（ＳＭＳ）メッセージを含む、請求項１に記載の方法。
【請求項８】
セキュアトランザクション確認操作を遂行することが、
前記依拠当事者に関連付けられた前記ユーザのアカウントに関する識別コードを表示することを更に含む、請求項２に記載の方法。
【請求項９】
前記コードが、前記ユーザの電子識別証を使用して認証／署名された電子メッセージから抽出される、請求項１に記載の方法。
【請求項１０】
前記セキュアディスプレイ内に表示される内容が、前記内容にわたってハッシュを生成すること、及び得られたハッシュ値を前記依拠当事者に提供することによって保護され、前記依拠当事者が、前記ハッシュ値を有効化することによって前記内容を有効性を確認する、請求項２に記載の方法。
【請求項１１】
依拠当事者側で、ユーザから認証部を登録するための要求を受信することと、
前記認証部内でコードを生成することと、
前記コードを前記ユーザにセキュアに表示することと、
認証されたアウトオブバンド通信チャネルを介して前記ユーザから前記依拠当事者へ前記コードを送信することと、
前記コードを使用して前記ユーザのアイデンティティを検証し、肯定的な検証に応答して前記認証部を応答性良く登録することと、を含む、方法。
【請求項１２】

前記依拠当事者に前記コードをセキュアに提供することが、
前記ユーザの認証部のセキュアディスプレイ内に前記コードを表示することを含むセキュアトランザクション確認操作を遂行することを含む、請求項１１に記載の方法。
【請求項１３】
前記認証部を登録するための前記要求に応答して、前記認証部に関連付けられた公開鍵を生成することと、前記公開鍵を前記依拠当事者に伝送することと、を更に含む、請求項１１に記載の方法。
【請求項１４】
前記公開鍵に対してハッシュ操作を遂行することによって前記コードを生成することを更に含む、請求項１３に記載の方法。
【請求項１５】
前記ハッシュ操作が、ＳＨＡ－２５６、ＳＨＡ－１、又はＳＨＡ－３ハッシュ操作を含む、請求項１４に記載の方法。
【請求項１６】
前記アウトオブバンド通信チャネルが、郵便、電子メール、又はショートメッセージサービス（ＳＭＳ）メッセージを含む、請求項１１に記載の方法。
【請求項１７】
セキュアトランザクション確認操作を遂行することが、
前記依拠当事者に関連付けられた前記ユーザのアカウントに関する識別コードを表示することを更に含む、請求項１２に記載の方法。
【請求項１８】
前記コードが、前記ユーザの電子識別証を使用して認証／署名された電子メッセージから抽出される、請求項１１に記載の方法。
【請求項１９】
前記セキュアディスプレイ内に表示される内容が、前記内容にわたってハッシュを生成すること、及び得られたハッシュ値を前記依拠当事者に提供することによって保護され、前記依拠当事者が、前記ハッシュ値を有効化することによって前記内容を有効性を確認する、請求項１２に記載の方法。
【請求項２０】
依拠当事者側で、ユーザから認証部を登録するための要求を受信することであって、前記要求が、前記ユーザの既存の資格証明書を識別する識別情報を含む、受信することと、
前記ユーザのクライアント側で認証オブジェクトを作成することであって、前記認証オブジェクトは、前記ユーザの前記既存の資格証明書と関連付けられた公開鍵を使用して生成された署名を含む、作成することと、
前記依拠当事者側で前記署名を検証し、肯定的な検証に応答して前記認証部を応答性良く登録することと、を含む、方法。
【請求項２１】
前記認証部に関連付けられた公開鍵／秘密鍵のペアを生成することと、前記公開鍵を前記依拠当事者に送信することと、を更に含む、請求項２０に記載の方法。
【請求項２２】
前記認証オブジェクトが、前記依拠当事者における前記ユーザのアカウントに関連付けられた識別コードと、前記秘密鍵によって生成された前記公開鍵のハッシュと、前記秘密鍵によって生成された前記署名と、を含む、請求項２１に記載の方法。
【請求項２３】
前記署名を検証することが、前記オブジェクトから抽出された前記公開鍵ハッシュを、登録時に前記ユーザから受信した前記公開鍵に関して計算された前記ハッシュ値と比較することを含む、請求項２２に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、概して、データ処理システムの分野に関する。より具体的には、本発明は、認証装置のセキュアな登録のための装置及び方法に関する。

【背景技術】

【０００２】

システムはまた、バイオメトリックセンサを使用してネットワーク上でセキュアなユーザ認証を提供するために設計されている。そのようなシステムにおいて、認証部によって生成されたスコア、及び／又は他の認証データは、遠隔サーバでユーザを認証するためにネットワークを介して送信され得る。例えば、特許出願第２０１１／００８２８０１号（「第‘８０１号出願」）は、強力な認証（例えば、アイデンティティ盗難やフィッシングに対する保護）、セキュアトランザクション（例えば、「ブラウザにおけるマルウェア」及びトランザクションについての「中間者」攻撃に対する保護）、並びに、クライアント認証トークンの登録／管理（例えば、指紋リーダ、顔認識装置、スマートカード、トラステッドプラットフォームモジュールなど）を提供するネットワーク上のユーザ登録及び認証のためのフレームワークについて記載している。

【０００３】

本出願の譲受人は、第‘８０１号出願に記載された認証フレームワークに対する様々な改善を開発している。これらの改善のうちいくつかは、本件の譲受人に譲渡された以下の一群の米国特許出願（「同時係属出願」）に記載されている：第１３／７３０，７６１号、Ｑｕｅｒｙ Ｓｙｓｔｅｍ ａｎｄ Ｍｅｔｈｏｄ ｔｏ Ｄｅｔｅｒｍｉｎｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃａｐａｂｉｌｉｔｉｅｓ；第１３／７３０，７７６号、Ｓｙｓｔｅｍ ａｎｄ Ｍｅｔｈｏｄ ｆｏｒ Ｅｆｆｉｃｉｅｎｔｌｙ Ｅｎｒｏｌｌｉｎｇ，Ｒｅｇｉｓｔｅｒｉｎｇ，ａｎｄ Ａｕｔｈｅｎｔｉｃａｔｉｎｇ Ｗｉｔｈ Ｍｕｌｔｉｐｌｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｄｅｖｉｃｅｓ；第１３／７３０，７８０号、Ｓｙｓｔｅｍ ａｎｄ Ｍｅｔｈｏｄ ｆｏｒ Ｐｒｏｃｅｓｓｉｎｇ Ｒａｎｄｏｍ Ｃｈａｌｌｅｎｇｅｓ Ｗｉｔｈｉｎ ａｎ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｆｒａｍｅｗｏｒｋ；第１３／７３０，７９１号、Ｓｙｓｔｅｍ ａｎｄ Ｍｅｔｈｏｄ ｆｏｒ Ｉｍｐｌｅｍｅｎｔｉｎｇ Ｐｒｉｖａｃｙ Ｃｌａｓｓｅｓ Ｗｉｔｈｉｎ ａｎ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｆｒａｍｅｗｏｒｋ；第１３／７３０，７９５号、Ｓｙｓｔｅｍ ａｎｄ Ｍｅｔｈｏｄ ｆｏｒ Ｉｍｐｌｅｍｅｎｔｉｎｇ Ｔｒａｎｓａｃｔｉｏｎ Ｓｉｇｎａｌｉｎｇ Ｗｉｔｈｉｎ ａｎ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｆｒａｍｅｗｏｒｋ；第１４／２１８，５０４、Ａｄｖａｎｃｅｄ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｔｅｃｈｎｉｑｕｅｓ ａｎｄ Ａｐｐｌｉｃａｔｉｏｎｓ（以下「第’５０４号出願」）。

【０００４】

簡潔に述べると、同時係属出願は、ユーザがクライアント装置上のバイオメトリック装置（例えば、指紋センサ）などの認証装置（又は認証部）に登録する認証技術を記載している。ユーザがバイオメトリック装置に登録すると、バイオメトリック基準データが認証装置のバイオメトリックセンサによって捕捉される（例えば、指をスワイプし、写真を撮影し、音声を録音することなどによって）。ユーザは、その後、認証装置をネットワークを介して１つ以上のサーバ（例えば、同時係属出願に記載されているようなセキュアトランザクションサービスを備えたウェブサイト又は他の依拠当事者）に登録し、その後、登録プロセスの間に交換したデータ（例えば、認証装置内にプロビジョンされた暗号鍵）を使用してそれらのサーバに登録することができる。認証されると、ユーザは、ウェブサイト又は他の依拠当事者と１つ以上のオンライントランザクションを実行することが許可される。同時係属出願に記載されたフレームワークにおいて、ユーザを固有に識別するために使用可能な指紋データ及び他のデータなどの機密情報は、ユーザのプライバシーを保護するためにユーザの認証装置上でローカルに保持されてもよい。第’５０４号出願は、ほんの２～３の例を挙げると、複合的な認証部を設計し、認証の保証レベルをインテリジェントに生成し、非侵襲型ユーザ検証を使用し、認証データを新しい認証装置に転送し、認証データをクライアントリスクデータによって増強し、認証ポリシーを適応的に適用し、

かつ信頼の輪を築くための技術を含む様々な追加の技術を記載している。
【図面の簡単な説明】
【０００５】
本発明のより良好な理解は、以下の図面と共に以下の詳細な説明から得ることができる。
【図１Ａ】セキュアな認証システムアーキテクチャの２つの異なる実施形態を図示している。
【図１Ｂ】セキュアな認証システムアーキテクチャの２つの異なる実施形態を図示している。
【図２】鍵を認証装置に登録することができる方法を示すトランザクション図である。
【図３Ａ】セキュアディスプレイを使用するセキュアトランザクション確認の実施形態を図示している。
【図３Ｂ】セキュアディスプレイを使用するセキュアトランザクション確認の実施形態を図示している。
【図４】依拠当事者に登録するための本発明の一実施形態を図示している。
【図５】本発明の一実施形態におけるクエリポリシーの登録操作が実装される方法を示すトランザクション図を図示している。
【図６】強化されたセキュリティを有する登録のアーキテクチャの一実施形態を図示している。
【図７】セキュアな登録方法の一実施形態を図示している。
【図８Ａ】セキュアな登録方法の異なる実施形態を図示している。
【図８Ｂ】セキュアな登録方法の異なる実施形態を図示している。
【図９】秘密がユーザから依拠当事者に送信される方法の別の実施形態を図示している。
【図１０】ユーザの既存の資格証明書が登録のために使用される方法の別の実施形態を図示している。
【図１１】本発明の実施形態を実行するためのコンピュータシステムの例示的な実施形態を図示している。
【図１２】本発明の実施形態を実行するためのコンピュータシステムの例示的な実施形態を図示している。
【発明を実施するための形態】
【０００６】
以下に説明するものは、高度な認証技術及び関連するアプリケーションを実行するための装置、方法及び機械可読媒体の実施形態である。説明を通して、説明の目的のために、多数の具体的な詳細が本発明の完全な理解を提供するために記載されている。しかしながら、本発明が、これらの具体的な詳細の一部がなくても実施され得ることは当業者にとって明らかであろう。他の例において、周知の構造及び装置は示されていないか、又は、本発明の基本原理を曖昧にすることを避けるためにブロック図の形態で示されている。
【０００７】
以下に説明する本発明の実施形態には、バイオメトリック装置又はＰＩＮ入力などのユーザ検証機能を備えた認証装置が含まれる。これらの装置は、「トークン」、「認証装置」、又は「認証部」と称される場合もある。特定の実施形態は、顔認識ハードウェア／ソフトウェア（例えば、ユーザの顔を認識してユーザの眼の動きを追跡するためのカメラ及び関連するソフトウェア）に焦点を当てているが、いくつかの実施形態は、例えば、指紋センサ、音声認識ハードウェア／ソフトウェア（例えば、マイクロフォン及びユーザの音声を認識するための関連するソフトウェア）、及び光学的認識機能（例えば、ユーザの網膜をスキャンするための光学スキャナ及び関連するソフトウェア）を含む、追加のバイオメトリック装置を利用することができる。ユーザ検証機能は、ＰＩＮ入力のような、非バイオメトリック様相を含んでもよい。認証部は、トラステッドプラットフォームモジュール（ＴＰＭ）、スマートカード、及びセキュアな要素などの装置を暗号操作のために使用し得る。

【０００８】
モバイルバイオメトリックの実装において、生体認証装置は、依拠当事者から遠隔にあってもよい。本明細書では、「遠隔」という用語は、バイオメトリックセンサが通信可能に結合されているコンピュータのセキュリティ区域の一部ではない（例えば、依拠当事者のコンピュータと同じ物理的筐体内に埋め込まれていない）ことを意味する。一例として、バイオメトリック装置は、ネットワーク（例えば、インターネット、無線ネットワークリンクなど）を介して又はＵＳＢポートなどの周辺入力を介して依拠当事者に結合することができる。これらの条件下では、その装置が依拠当事者（例えば、認証強度及び完全性保護の許容可能なレベルを提供するもの）によって認証されるものであるかどうか及び／又はハッカーがバイオメトリック装置を侵害したかどうか若しくは更には交換したかどうかを依拠当事者が知る方法はない可能性がある。バイオメトリック装置における信頼は、装置の特定の実装に依存する。

【０００９】
「ローカル」という用語は、ユーザが現金自動預け払い機（ＡＴＭ）又は店舗販売時点情報管理（ＰＯＳ）小売チェックアウトの位置などの特定の位置において個人がトランザクションを完了していることを意味するために本明細書において使用される。しかしながら、以下に説明するように、ユーザを認証するために用いられる認証技術は、遠隔サーバ及び／又は他のデータ処理装置とのネットワークを介した通信などの非位置要素を含むことができる。更に、具体的な実施形態が（ＡＴＭや小売店など）本明細書において記載されるが、本発明の基礎原理は、トランザクションがエンドユーザによってローカルに開始される任意のシステムのコンテキスト内で実装されてもよいことに留意すべきである。

【００１０】
「依拠当事者」という用語は、単にユーザのトランザクションを実行しようとしているエンティティ（例えば、ユーザトランザクションを実行するウェブサイト又はオンラインサービス）のみならず、本明細書に記載された基礎となる認証技術を実行することができるそのエンティティの代わりに実装されるセキュアトランザクションサーバを指すために本明細書において使用される場合もある。セキュアトランザクションサーバは、所有される及び／又は依拠当事者の制御下にあってもよく、又は、事業構成の一部として依拠当事者に対してセキュアトランザクションサービスを提供する第三者の制御下にあってもよい。

【００１１】
「サーバ」という用語は、クライアントからネットワークを介してリクエストを受信し、応答として１つ以上の操作を実行し、クライアントに通常は操作の結果を含む応答を伝送するハードウェアプラットフォーム上で（又は複数のハードウェアプラットフォームにわたって）実行されるソフトウェアを指すために本明細書において使用される。サーバは、クライアントに対してネットワーク「サービス」を提供する又は提供するのに役立つように、クライアントのリクエストに応答する。重要なことは、サーバが単一のコンピュータ（例えば、サーバソフトウェアを実行する単一のハードウェア装置）に限定されるものではなく、実際には、潜在的に複数の地理的位置における複数のハードウェアプラットフォームにまたがってもよいということである。

【００１２】
例示的なシステムアーキテクチャ
図１Ａ及び図１Ｂは、ユーザ認証に関して、クライアント側及びサーバ側の構成要素を含むシステムアーキテクチャの２つの実施形態を例示する。図１Ａに示される実施形態は、ウェブサイトと通信するためのウェブブラウザプラグインベースのアーキテクチャを用いる一方で、図１Ｂで示される実施形態は、ブラウザを必要としない。ユーザを認証装置に登録すること、認証装置をセキュアなサーバに登録すること、及びユーザを検証することなどの、本明細書に記載の様々な技術は、これらのシステムアーキテクチャのうちのどちらにも実装され得る。このため、図１Ａに示されるアーキテクチャは、以下に説明される実施形態のうちのいくつかの動作を実証するために使用されているものの、同じ基本原

則は、図１Ｂに示されるシステムに容易に実装され得る（例えば、サーバ１３０とクライアント上のセキュアトランザクションサービス１０１との間の通信手段としてのブラウザプラグイン１０５を削除することによって）。

【００１３】

先ず図１Ａを参照すると、図示されている実施形態は、エンドユーザを登録及び検証するための１つ以上の認証装置１１０～１１２（当該技術分野では、「トークン」又は「認証部」と称される場合もある）を備えたクライアント１００を含む。上述したように、認証装置１１０～１１２は、指紋センサ、音声認識ハードウェア／ソフトウェア（例えば、ユーザの音声を認識するためのマイクロフォン及び関連するソフトウェア）、顔認識ハードウェア／ソフトウェア（例えば、ユーザの顔を認識するためのカメラ及び関連するソフトウェア）、及び光学認識機能（ユーザの網膜をスキャンするための光スキャナ及び関連するソフトウェア）などのバイオメトリック装置、並びにＰＩＮ検証などの非バイオメトリック様相のサポートを含むことができる。認証装置は、トラステッドプラットフォームモジュール（ＴＰＭ）、スマートカード、又はセキュアな要素を暗号操作及び鍵記憶のために使用してもよい。

【００１４】

認証装置１１０～１１２は、セキュアトランザクションサービス１０１によって露出されたインターフェース１０２（例えば、アプリケーションプログラミングインターフェース又はＡＰＩ）を介してクライアントに通信可能に接続されている。セキュアトランザクションサービス１０１は、ネットワークを介して１つ以上のセキュアトランザクションサーバ１３２～１３３と通信を行い、かつウェブブラウザ１０４のコンテキスト内で実行されるセキュアトランザクションプラグイン１０５とインターフェースするためのセキュアアプリケーションである。図示されたように、インターフェース１０２はまた、装置識別コード、ユーザ識別コード、認証装置によって保護されるユーザ登録データ（例えば、スキャンされた指紋又は他のバイオメトリックデータ）などの認証装置１１０～１１２のそれぞれに関連する情報と、認証装置によって覆い包まれている本明細書に記載されたセキュア認証技術を実行するために使用される鍵とを記憶するクライアント１００におけるセキュア記憶装置１２０に対するセキュアアクセスを提供することができる。例えば、以下に詳細に説明するように、固有の鍵は、認証装置のそれぞれに記憶され、インターネットなどのネットワークを介してサーバ１３０と通信するときに使用することができる。

【００１５】

後述するように、特定の種類のネットワークトランザクションは、ウェブサイト１３１又は他のサーバとのＨＴＴＰ又はＨＴＴＰＳトランザクションなどのセキュアトランザクションプラグイン１０５によって、サポートされる。一実施形態において、セキュアトランザクションプラグインは、セキュアエンタープライズ又はウェブデスティネーション１３０内のウェブサーバ１３１（以下では単に「サーバ１３０」と称される場合もある）によってウェブページのＨＴＭＬコード内に挿入された特定のＨＴＭＬタグに応答して開始される。そのようなタグを検出することに応答して、セキュアトランザクションプラグイン１０５は、処理のために、セキュアトランザクションサービス１０１に、トランザクションを転送することができる。更に、特定の種類のトランザクション（例えば、セキュア鍵交換などの）について、セキュアトランザクションサービス１０１は、オンプレミストランザクションサーバ１３２（すなわち、ウェブサイトと同じ位置に配置された）又はオフプレミストランザクションサーバ１３３との直接の通信チャンネルを開くことができる。

【００１６】

セキュアトランザクションサーバ１３２～１３３は、ユーザデータ、認証装置データ、鍵、及び、後述するセキュア認証トランザクションをサポートするために必要な他のセキュア情報を記憶するためにセキュアトランザクションデータベース１２０に結合される。しかしながら、本発明の基本原理は、図１Ａに示されるセキュアエンタープライズ又はウェブデスティネーション１３０内の論理的な構成要素の分離を必要としないことに留意す

べきである。例えば、ウェブサイト１３１及びセキュアトランザクションサーバ１３２～１３３は、単一の物理サーバ又は他の物理サーバ内に実装されてもよい。更に、ウェブサイト１３１及びトランザクションサーバ１３２～１３３は、以下に説明する機能を実行するための１つ以上のサーバ上で実行される統合されたソフトウェアモジュール内に実装されてもよい。

【００１７】

上述したように、本発明の基本原理は、図１Ａに示されるブラウザベースアーキテクチャに限定されるものではない。図１Ｂは、スタンドアロンアプリケーション１５４がネットワークを介してユーザを認証するためにセキュアトランザクションサービス１０１によって提供される機能を利用する代替の実施形態を示している。一実施形態において、アプリケーション１５４は、以下に詳細に説明したユーザ／クライアント認証技術を実行するためのセキュアトランザクションサーバ１３２～１３３に依存する１つ以上のネットワークサービス１５１との通信セッションを確立するように設計されている。

【００１８】

図１Ａ及び図１Ｂに示された実施形態のどちらにおいても、セキュアトランザクションサーバ１３２～１３３は、次いでセキュアトランザクションサービス１０１に対してセキュアに伝送され、かつセキュア記憶装置１２０内の認証装置に記憶される鍵を生成することができる。更に、セキュアトランザクションサーバ１３２～１３３は、サーバ側のセキュアトランザクションデータベース１２０を管理する。

【００１９】

装置の登録及びトランザクションの確認

本発明の一実施形態は、登録中にセキュアトランザクション確認技術を用いる。したがって、様々な登録及びセキュアトランザクションの操作が図２～５を参照して最初に説明され、認証装置のセキュアな登録のための本発明の実施形態の詳細な説明がそれに続く。

【００２０】

図２は、認証装置を登録するための一連のトランザクションを図示している。登録時に、鍵は認証装置とセキュアトランザクションサーバ１３２～１３３のうちの１つとの間で共有される。鍵は、クライアント１００のセキュア記憶装置１２０及びセキュアトランザクションサーバ１３２～１３３によって使用されるセキュアトランザクションデータベース１２０内に記憶される。一実施形態において、鍵は、セキュアトランザクションサーバ１３２～１３３のいずれかによって生成された対称鍵である。しかしながら、以下に説明する他の実施形態において、非対称鍵を使用することができる。本実施形態において、公開鍵は、セキュアトランザクションサーバ１３２～１３３によって記憶され得、第２の関連する秘密鍵は、クライアントのセキュア記憶装置１２０に記憶され得る。更に、別の実施形態において、鍵（複数可）は、（例えば、セキュアトランザクションサーバ１３２～１３３よりもむしろ認証装置又は認証装置インターフェースによって）クライアント１００上に生成され得る。本発明の基本原理は、任意の特定の種類の鍵又は鍵の生成方法に限定されるものではない。

【００２１】

動的対称鍵プロビジョニングプロトコル（ＤＳＫＰＰ）などのセキュア鍵プロビジョニングプロトコルはセキュア通信チャンネルを介してクライアントと鍵を共有するために使用することができる（例えば、コメントについての要求（ＲＦＣ）６０６３を参照）。しかしながら、本発明の基本原理は、いかなる特定の鍵プロビジョニングプロトコルにも限定されるものではない。

【００２２】

図２に示される具体的な詳細を参照すると、ひとたびユーザ登録又はユーザ検証が完了すると、サーバ１３０は、装置登録の間にクライアントによって提出されなければならないランダム生成チャレンジ（例えば、暗号化ナンス）を生成する。ランダムチャレンジは、限られた期間について有効であり得る。セキュアトランザクションプラグインは、ランダムチャレンジを検出し、それをセキュアトランザクションサービス１０１に転送する。

それに応答して、セキュアトランザクションサービスは、サーバ１３０（例えば、アウトオブバンドトランザクション）とのアウトオブバンドのセッションを開始し、鍵プロビジョニングプロトコルを使用してサーバ１３０と通信する。サーバ１３０は、ユーザ名によってユーザを捜し出し、ランダムチャレンジを有効化し、装置の認証コードが送信された場合にその認証コードを有効化し、セキュアトランザクションデータベース１２０にユーザのための新たなエントリを作成する。それはまた、鍵を生成し、データベース１２０に鍵を書き込み、鍵プロビジョニングプロトコルを使用してセキュアトランザクションサービス１０１に鍵を返送することができる。完了すると、認証装置及びサーバ１３０は、対称鍵が使用された場合には同じ鍵を共有し、非対称鍵が使用された場合には異なる鍵を共有する。

【００２３】

図３Ａは、ブラウザベースの実装のためのセキュアトランザクションの確認を図示している。ブラウザベースの実装が図示されているものの、同じ基本原則は、スタンドアロンアプリケーション又はモバイル装置のアプリケーションを使用して実装され得る。

【００２４】

セキュアトランザクション確認は、特定の種類のトランザクション（例えば、金融トランザクション）についてより強力なセキュリティを提供するように設計されている。図示された実施形態において、ユーザは、トランザクションを委任する前に各トランザクションを確認する。図示された技術を使用して、ユーザは、彼／彼女が委任したいものを正確に確認し、彼／彼女がグラフィカルユーザインターフェース（ＧＵＩ）のウィンドウ３０１に表示されているのを見るものを正確に委任する。換言すれば、本実施形態は、ユーザが確認しなかったトランザクションを委任するためにトランザクションテキストが「中間者」（ＭＩＴＭ）又は「マンインザブラウザ攻撃」（ＭＩＴＢ）によって変更されることがないことを保証する。

【００２５】

一実施形態において、セキュアトランザクションプラグイン１０５は、トランザクションの詳細を示すためにブラウザコンテキスト内にウィンドウ３０１を表示する。セキュアトランザクションサーバ１０１は、ウィンドウに表示されるテキストが誰かによって改竄されていないことを定期的に（例えば、ランダムな間隔で）検証する。異なる実施形態において、認証装置は、トラステッドユーザインターフェース（例えば、ＧｌｏｂａｌＰｌａｔｆｏｒｍのＴｒｕｓｔｅｄＵＩに適合するＡＰＩを提供する）を有する。

【００２６】

以下の例は、この実施形態の動作を強調するために役立つ。ユーザは、商人のサイトから購入する項目を選択し、「チェックアウト」を選択する。商人のサイトは、本明細書に記載された発明の１つ以上の実施形態を実装するセキュアトランザクションサーバ１３２～１３３を有するサービスプロバイダ（例えば、ＰａｙＰａｌ）にトランザクションを送信する。商人のサイトは、ユーザを認証し、トランザクションを完了する。

【００２７】

セキュアトランザクションサーバ１３２～１３３は、トランザクション詳細（ＴＤ）を受信し、ＨＴＭＬページにおいて「セキュアトランザクション」要求を作成し、クライアント１００に送信する。セキュアトランザクション要求は、トランザクション詳細及びランダムチャレンジを含む。セキュアトランザクションプラグイン１０５は、トランザクションの確認メッセージの要求を検出し、セキュアトランザクションサービス１０１に全てのデータを転送する。ブラウザやプラグインを使用していない実施形態において、情報は、セキュアトランザクションサーバからクライアント１００上のセキュアトランザクションサービスに対して直接送信することができる。

【００２８】

ブラウザベースの実装については、セキュアトランザクションプラグイン１０５は、（例えば、ブラウザコンテキスト内で）ユーザにトランザクション詳細を有するウィンドウ３０１を表示し、トランザクションを確認するために認証を提供するようにユーザに要求

する。ブラウザやプラグインを使用していない実施形態において、セキュアトランザクションサービス１０１、アプリケーション１５４（図１Ｂ）、又は認証装置１１０は、ウィンドウ３０１を表示することができる。セキュアトランザクションサービス１０１は、タイマを起動し、ユーザに表示されているウィンドウ３０１の内容を検証する。検証期間は、ランダムに選択することができる。セキュアトランザクションサービス１０１は、ユーザがウィンドウ３０１内に有効なトランザクション詳細を見ること（例えば、詳細に関するハッシュを生成し、正確な内容のハッシュと比較することによって内容が正確であることを検証すること）を保証する。それは、内容が改竄されていることを検出した場合、確認トークン／署名が生成されるのを防止する。

【００２９】

ユーザが有効な検証データ（例えば、指紋センサ上で指をスワイプすることによって）を提供した後、認証装置は、ユーザを検証し、トランザクション詳細やランダムチャレンジによって暗号化署名（「トークン」と称される場合もある）を生成する（すなわち、署名は、トランザクション詳細及びナンスにわたって計算される）。これは、トランザクションの詳細がサーバとクライアントの間で変更されていないことをセキュアトランザクションサーバ１３２～１３３が確認するのを可能にする。セキュアトランザクションサービス１０１は、セキュアトランザクションサーバ１３２～１３３に署名を転送するセキュアトランザクションプラグイン１０５に対して生成された署名及びユーザ名を送信する。セキュアトランザクションサーバ１３２～１３３は、ユーザ名によってユーザを識別し、署名を検証する。検証が成功すると、確認メッセージがクライアントに送信され、トランザクションが処理される。

【００３０】

本発明の一実施形態は、セキュアトランザクションサーバが、サーバによって許容される認証機能を示すサーバポリシーをクライアントに伝送するクエリポリシーを実装する。次いで、クライアントは、サーバポリシーを分析して、サーバポリシーがサポートし、かつ／又はユーザが使用する願望を示した認証機能のサブセットを識別する。次いで、クライアントは、提供されたポリシーに一致する認証トークンのサブセットを使用してユーザを登録及び／又は認証する。したがって、クライアントは、その認証機能についての網羅的な情報（例えば、その認証装置の全て）又はクライアントを一意的に識別するために使用され得る他の情報を伝送する必要がないことから、クライアントのプライバシーに対する影響度はより低くなる。

【００３１】

限定としてではなく例示として、クライアントは、例を挙げると、指紋センサ、音声認識機能、顔認識機能、眼／光学的認識機能、ＰＩＮ検証などの多くユーザ検証機能を含むことができる。しかしながら、プライバシー上の理由から、ユーザは、要求サーバに対してその機能の全ての詳細を明かすことを望まないかもしれない。このため、本明細書に記載された技術を使用して、セキュアトランザクションサーバは、例えば、指紋、光学的又はスマートカード認証をサポートすることを示すサーバポリシーをクライアントに対して伝送することができる。次いで、クライアントは、独自の認証機能に対してサーバポリシーを比較し、利用可能な認証オプションを１つ以上選択することができる。

【００３２】

本発明の一実施形態は、クライアントとのセッションを維持するためにいかなるトランザクション状態もサーバにおいて維持される必要がないように、セキュアトランザクションサーバにおいてトランザクション署名を用いる。特に、ウィンドウ３０１内に表示されるトランザクションのテキストなどのトランザクション詳細は、サーバによって署名されたクライアントに送信され得る。次いで、サーバは、クライアントによって受信された署名されたトランザクション応答が署名を検証することで有効であることを検証することができる。サーバは、持続的にトランザクションの内容を記憶する必要がなく、多くのクライアントのための記憶スペースのかなりの量を消費し、サーバにおけるサービス種類攻撃の拒否の可能性を開く。

【００３３】
クライアント１００とのトランザクションを開始するウェブサイト又は他のネットワークサービス３１１を示す本発明の一実施形態が図３Ｂに示されている。例えば、ユーザは、ウェブサイト上で購入するための物品を選択している可能性があり、チェックアウトして支払う準備ができている。図示された例において、ウェブサイト又はサービス３１１は、（本明細書に記載される）署名を生成して検証するための署名処理ロジック３１３と、（例えば、上述した認証技術を使用して）クライアント認証３１４を実行するための認証ロジックとを含むセキュアトランザクションサーバ３１２にトランザクションをハンドオフする。
【００３４】
一実施形態において、クライアント１００に対してセキュアトランザクションサーバ３１２から送信された認証要求は、（上述したように）暗号化ナンスなどのランダムチャレンジと、トランザクション詳細（例えば、トランザクションを完了するために提示される特定のテキスト）と、（セキュアトランザクションサーバによってのみ知られている）秘密鍵を使用してランダムチャレンジ及びトランザクション詳細を介して署名処理ロジック３１３によって生成された署名とを含む。
【００３５】
上記情報がクライアントによって受信されると、ユーザは、トランザクションを完了するためにユーザ検証が必要とされるという指示を受信することができる。これに応答して、ユーザは、例えば、指紋スキャナにわたって指をスワイプする、画像をスナップする、マイクに発話する又は所定のトランザクションについて許可された他の種類の認証を行うことができる。一実施形態において、ひとたびユーザが認証装置１１０によって成功裡に検証されると、クライアントは、以下のものをサーバに伝送する：（１）ランダムチャレンジ及びトランザクションテキスト（両方とも、サーバによってクライアントに以前提供されたもの）、（２）ユーザが成功裡に認証を完了したことを証明するデータ、並び（３）署名、である。
【００３６】
次いで、セキュアトランザクションサーバ３１２における認証モジュール３１４は、ユーザが正しく認証されたことを確認することができ、署名処理ロジック３１３は、秘密鍵を使用してランダムチャレンジ及びトランザクションのテキストにわたって署名を再生成する。署名がクライアントから送信されたものと一致した場合、サーバは、トランザクションのテキストがウェブサイト又はサービス３１１から当初受信したときのものと同じであることを検証することができる。セキュアトランザクションサーバ３１２は、セキュアトランザクションデータベース１２０内にトランザクションのテキスト（又は他のトランザクションデータ）を持続的に記憶する必要がないため、記憶及び処理リソースは保存される。
【００３７】
図４は、これらの技術を実装するためのクライアント－サーバアーキテクチャの一実施形態を図示している。図示されたように、クライアント１００に実装されたセキュアトランザクションサービス１０１は、サーバ１３０によって提供されたポリシーを分析し、登録及び／又は認証に使用される認証機能のサブセットを識別するためのポリシーフィルタ４０１を含む。一実施形態において、ポリシーフィルタ４０１は、セキュアトランザクションサービス１０１のコンテキスト内で実行されるソフトウェアモジュールとして実装される。しかしながら、更に本発明の基本原理を順守しながら、ポリシーフィルタ４０１は、任意の方法で実装されてもよく、ソフトウェア、ハードウェア、ファームウェア又はそれらの任意の組み合わせを含むことができることに留意すべきである。
【００３８】
図４に示される特定の実装は、上述した技術を使用してセキュア企業又はウェブデスティネーション１３０（単に「サーバ１３０」又は「依拠当事者」１３０と称される場合もある）との通信を確立するためのセキュアトランザクションプラグイン１０５を含む。例

えば、セキュアトランザクションプラグインは、ウェブサーバ１３１によってＨＴＭＬコードに挿入された特定のＨＴＭＬタグを識別することができる。このため、本実施形態において、サーバポリシーは、ポリシーフィルタ４０１を実装するセキュアトランザクションサービス１０１にそれを転送するセキュアトランザクションプラグイン１０５に提供される。

【００３９】

ポリシーフィルタ４０１は、クライアントのセキュア記憶領域４２０から機能を読み出すことによって、クライアント認証機能を決定することができる。上述したように、セキュア記憶装置４２０は、全てのクライアントの認証機能（例えば、認証装置の全ての識別コード）のレポジトリを含むことができる。ユーザが既にその認証装置にユーザを登録している場合、ユーザの登録データは、セキュア記憶装置４２０内に記憶される。クライアントが既にサーバ１３０に認証装置を登録している場合、セキュア記憶装置はまた、各認証装置に関連する暗号化された秘密鍵を記憶することができる。

【００４０】

セキュア記憶装置４２０から抽出される認証データ及びサーバによって提供されるポリシーを使用して、ポリシーフィルタ４０１は、その後、使用される認証機能のサブセットを識別することができる。構成に応じて、ポリシーフィルタ４０１は、クライアント及びサーバの双方によってサポートされている認証機能の完全なリストを識別することができるか又は完全なリストのサブセットを識別することができる。例えば、サーバが認証機能Ａ、Ｂ、Ｃ、Ｄ、及びＥをサポートし、クライアントが認証機能Ａ、Ｂ、Ｃ、Ｆ、及びＧを有する場合、ポリシーフィルタ４０１は、共通の認証機能の全サブセット（Ａ、Ｂ、及びＣ）をサーバに識別することができる。代替的に、図４におけるユーザ選好４３０によって示されるように、より高水準のプライバシーが所望される場合、認証機能のより限定的なサブセットがサーバに識別され得る。例えば、ユーザは、単一の共通の認証機能がサーバ（例えば、Ａ、Ｂ又はＣのいずれか）に対して識別されるべきであるにすぎないことを示すことができる。一実施形態において、ユーザは、クライアント１００の認証機能の全てについて優先順位付け方式を確立することができ、ポリシーフィルタは、サーバ及びクライアントの双方に共通の優先順位の最も高い認証機能（又はＮ個の認証機能の優先順位のセット）を選択することができる。

【００４１】

何の動作がサーバ１３０（登録又は認証）によって開始されかに応じて、図４に示されるように、セキュアトランザクションサービス１３０は、認証装置のフィルタリングされたサブセット（１１０～１１２）においてその動作を実行し、セキュアトランザクションプラグイン１０５を介してサーバ１３０に動作応答を返送する。代替的に、ウェブブラウザのプラグイン１０５構成要素に依存しない実施形態において、情報は、セキュアトランザクションサービス１０１からサーバ１３０に対して直接送られてもよい。

【００４２】

図５は、クエリポリシートランザクションを有する例示的な一連の登録についての追加の詳細を示すトランザクション図を示している。図示された実施形態において、ユーザは、サーバ１３０に装置を以前に登録していない。したがって、５０１において、ユーザは、５０２においてクライアントブラウザ１０４を介してサーバ１３０に転送される最初のワンタイム認証工程としてユーザ名とパスワードを入力することができる。しかしながら、ユーザ名及びパスワードは、本発明の基本原理を順守するために必要とされないことに留意すべきである。

【００４３】

ユーザは、５０３において判定されたように強化されたセキュリティに以前に登録していないことから、サーバ１３０は、５０４においてクライアントに対してそのサーバポリシーを伝送する。上述したように、サーバポリシーは、サーバ１３０によってサポートされている認証機能の指示を含むことができる。図示された例において、サーバポリシーは、トランザクション５０６を介してセキュアトランザクションサービス１０１に渡される

。
【００４４】
トランザクション５０７において、セキュアトランザクションサービス１０１は、認証機能のフィルタリングされたリストに到達するために、クライアントの機能（及び上述したような装置の優先順位方式及び／又はユーザ選好などの潜在的に他の情報）とサーバポリシーを比較する。次に、装置（１０２）のフィルタリングされたリストは、トランザクション５０８及び５０９で鍵のペアを生成し、これらの鍵のペアの公開部分をセキュアトランザクションサービス１０１に対して提供し、セキュアトランザクションサービス１０１は、５１０において、これらを登録応答としてサーバ１３０に返送する。サーバは、認証装置を証明し、セキュアトランザクションデータベース内に公開鍵を記憶する。ここで用いられるトークン証明は、登録中に、認証装置アイデンティティを有効化する処理である。それは、クライアントによって報告された装置が実際に主張されたとおりのものであることをサーバ１３０が暗号的に確認することを可能にする。
【００４５】
代替的に又は追加的に、５０７において、ユーザは、リストを確認し及び／又はこの特定のサーバ１３０で使用される特定の認証機能を選択する機会を提供することができる。例えば、フィルタリングされたリストは、指紋スキャン、顔認識及び／又は音声認識による認証を使用するための選択肢を示すことができる。次いで、ユーザは、サーバ１３０による認証時にこれらの選択肢の１つ以上を使用するために選択することができる。
【００４６】
クライアントにおいてサーバポリシーをフィルタリングするための上述した技術は、上述した一連のトランザクションの様々な異なる段階（例えば、装置検出、装置登録、装置プロビジョニング、ユーザ認証などの際）で実施することができる。すなわち、本発明の基本原理は、図５に記載された特定のセットのトランザクション及び特定のトランザクションの順序に限定されるものではない。
【００４７】
更に、上述したように、ブラウザプラグインアーキテクチャは、本発明の基本原理を遵守するために必要とされない。ブラウザ又はブラウザプラグイン（例えば、スタンドアロンアプリケーション又はモバイル装置のアプリケーションなど）を伴うアーキテクチャについて、図５に示されるトランザクション図（及び本明細書に開示された残りのトランザクション図）は、ブラウザ１０４が削除され、セキュアトランザクションサービス１０１がサーバ１３０と直接通信するように簡略化することができる。
【００４８】
強化されたセキュリティを有する装置登録
欧州中央銀行（ＥＣＢ）及び連邦金融検査協議会（ＦＦＩＥＣ）を含む様々な組織は、金融取引のために強力な認証を使用することを推奨している。更に、欧州ネットワーク・情報セキュリティ機関（ＥＮＩＳＡ）は、金融機関は全ての顧客装置を侵害されたものとして取り扱うべきであると最近提案した。上記のセキュアトランザクション確認方法は、侵害された顧客の場合でさえ（認証装置が侵害されていない限り）、十分な保護を提供するものの、認証装置をネットワークを介して登録するための上記の登録技術は、一般にセキュアであるものの、顧客装置が侵害されているという想定の下に動作しておらず、したがって装置上のマルウェアに対して無防備であり得る。
【００４９】
装置登録時のセキュリティを強化するため、本発明の一実施形態は、アウトオブバンド通信チャネルを含み、使用して、秘密コードを依拠当事者からユーザへ、又はユーザから依拠当事者へ、送信する。このアウトオブバンド通信チャネルは、認証部を登録するために１回のみ使用される。次いで、認証部は、このチャネルの使用を義務付けることなく、後続の認証又はトランザクション確認のために使用され得る。更に、セキュアディスプレイの使用を含むセキュアトランザクション確認技術は、ユーザがアウトオブバンド伝送を介して送信された秘密コードを確認することを可能にするために、使用され得る（例えば

、図３Ａ及び図３Ｂに関して上記されたように）。

【００５０】

図６は、本明細書に記載の強化されたセキュリティ技術を実装するための強化されたセキュリティ登録モジュール６４０を含む認証部６００を含むか、又は認証部６００に接続される、例示的なクライアント装置６９０を図示している。図示されている実施形態は、正当なユーザがクライアント装置６００を所有している保証レベルを生成するための保証レベル計算モジュール６０６を有する認証エンジン６１０も含む。例えば、明示的かつ非侵襲的な結果６０５は、明示的なユーザ認証装置６２０～６２１、１つ以上のセンサ６４３（例えば、位置センサ、加速度計など）、及びクライアント装置６００の現在の認証状況に関する他のデータ（例えば、前回の明示的な認証からの時間など）を使用して収集される。

【００５１】

明示的な認証は、例えば、バイオメトリック技術を使用して（例えば、指紋認証装置上で指をスワイプすることによって）、及び／又はユーザが秘密コードを入力することによって、遂行され得る。非侵襲的な認証技術は、クライアント装置６００の現在の検出された位置（例えば、ＧＰＳセンサを介して）、他の感知されたユーザ挙動（例えば、ユーザの足取りを加速度計によって測定すること）、及び／又は前回の明示的な認証以来の時間などの変数などのデータに基づいて遂行され得る。どのように認証結果６０５が生成されるかということにかかわらず、保証計算モジュール６０６は、その結果を使用して、正当なユーザ６５０がクライアント装置６００を所有している可能性を表す保証レベルを決定する。セキュア通信モジュール６１３は、（例えば、本明細書で上述したようにセキュアな暗号化鍵を使用して）依拠当事者６１３とのセキュアな通信を確立する。公開鍵／秘密鍵のペア又は対称鍵は、暗号的にセキュアなハードウェア装置（例えば、セキュリティチップ）として実装され得るセキュア記憶装置６２５内に、又はセキュアなハードウェア及びソフトウェアの任意の組み合わせを使用して、記憶することができる。

【００５２】

図６に図示されるように、クライアント装置６９０は、ウェブブラウザ６９１、様々なモバイルアプリケーション６９２、及び他のハードウェア／ソフトウェアコンポーネントなどの様々な追加の構成要素を含み得る。本明細書に記載の実施形態のうちのいくつかにおいて、認証部６００は侵害されていると仮定され、それによって本明細書に記載のセキュアな登録技術を必要とする。しかしながら、この仮定は、通常本発明の基本原理に影響を与えることなく動作し得るクライアント装置６９０の残余のハードウェア／ソフトウェア構成要素には、いかなる影響も与えない可能性がある。

【００５３】

強化されたセキュリティによって登録を遂行するための方法の一実施形態が図７に示されている。７０１において、ユーザは、認証装置をオンラインサービス（本明細書に記載のようなセキュアトランザクションサービスを有する依拠当事者など）に登録することを試みる。例えば、ユーザは、新しい指紋認証部などの新しい認証装置／機能を有する新しい装置を購入した可能性がある。代替的に、ユーザは、既存のクライアント装置上に新しい認証部をインストールした可能性があり、かつ／又は既存の認証部を使用して初めてオンラインサービスにアクセスしている可能性がある。

【００５４】

７０２において、認証の試みに応答して、秘密コードがサービスからユーザへ、又はユーザからサービスへアウトオブバンド通信チャネルを介して、送信される。例えば、一実施形態において、登録プロセスの間に生成された公開鍵のハッシュ（例えば、図５のトランザクション５１０を参照されたい）を使用して秘密コードを生成し、これは、次いで、アウトオブバンドチャネルを介して送信される。１つの特定の実施形態において、ＳＨＡ－２５６、ＳＨＡ－１、又はＳＨＡ－３ハッシュ操作などのハッシュ操作が公開鍵に適用され、ハッシュ値を含む秘密コードを生成する。

【００５５】

一実施形態において、秘密コードは、依拠当事者によって生成され、アウトオブバンドチャネルを介してユーザに送信される（例えば、標準的な郵便又は電子メールなどを介して）。別の実施形態において、秘密は、セキュアトランザクション確認操作を使用してクライアント装置上にセキュアに表示される。次いで、ユーザは、セキュアに表示された秘密コード（例えば、公開鍵のハッシュ）をコピーし、それをアウトオブバンド通信チャネルを介して依拠当事者に送信する。

【００５６】

様々な異なる種類のアウトオブバンドチャネルが用いられ得る。本明細書で使用される場合、「アウトオブバンド」チャネルは、標準的な登録及び認証に使用されるものとは異なる種類の通信チャネルである。一実施形態において、アウトオブバンドチャネルは、非電子メールを含む。例えば、依拠当事者は、郵便サービスを使用してユーザの既知の住所にハッシュ値を郵送してもよい。別の実施形態において、アウトオブバンドチャネルは、電子メール、テキストメッセージング（例えば、ショートメッセージサービス（ＳＭＳ））、インスタントメッセージなどの電子的チャネル、又は依拠当事者側で知られているユーザと関連付けられた宛先住所を使用する任意の他の種類の通信チャネルを含み得る。

【００５７】

どのアウトオブバンドチャネルが使用されるかにかかわらず、７０３において、秘密コード（例えば、アウトオブバンドチャネルを通じて受信された公開鍵ハッシュ）を使用して、登録を検証する。例えば、公開鍵ハッシュがクライアント上にセキュアに表示される実施形態において、ユーザは、セキュアディスプレイ上に表示される公開鍵ハッシュをアウトオブバンドチャネルを介して提出する。コードが依拠当事者からクライアントにアウトオブバンドチャネルを介して送信される実施形態において、ユーザは、クライアント上で秘密コードを確認してもよい（例えば、セキュアトランザクション確認操作を介して）。一実施形態において、本明細書に記載のセキュアトランザクション確認技術（例えば、図３Ａ及び図３Ｂ並びに関連するテキストを参照されたい）を使用して、ユーザの検証のために公開鍵ハッシュをディスプレイ上にセキュアに表示すること、及び／又はユーザが公開鍵ハッシュをコピーし、それをアウトオブバンドチャネルを介して依拠当事者に返送することを可能にすることができる。

【００５８】

７０４において検証が成功したと判定された場合（例えば、登録７０１の一環として受信された公開鍵が、アウトオブバンドチャネルを介して送信された公開鍵に一致する場合）、登録は７０５で確認される。しかしながら、公開鍵が位置しない場合、又は公開鍵ハッシュがアウトオブバンドチャネルを介して受信される前にしきい値の時間が経過した場合、登録は、７０６で拒絶される。

【００５９】

一実施形態において、ユーザが登録プロセスの間に検証するように、様々な他のデータが表示され得る。例えば、一実施形態において、依拠当事者におけるユーザのアカウントに関連付けられた一意的なコードもまた、トランザクション確認及びセキュア表示技術を使用して表示され（かつユーザによって検証され）る。ユーザを依拠当事者と関連付けるこの一意的なコードは、本明細書において「ＡｐｐＩＤ」と称される場合もある。依拠当事者が複数のオンラインサービスを提供する幾つかの実施形態において、ユーザは、単一の依拠当事者との間で複数のＡｐｐＩＤを有し得る（依拠当事者によって提供されるサービスごとに１つずつ）。

【００６０】

ユーザが依拠当事者に前もって知られている登録後の実施形態、依拠当事者がユーザを識別する（例えば、それぞれの「自分の顧客を知る」（ＫＹＣ）規則に従って）より前にユーザが依拠当事者に登録する事前登録の実施形態、及び準同時的な登録を伴うハイブリッド型実施形態（例えば、ユーザと依拠当事者との両方によって知られている既存のコードを使用する）を含め、様々な異なる実装が用いられ得る。

【００６１】

１．事後登録

図８Ａは、ユーザが依拠当事者に知られている登録後プロセスの一実施形態を図示している。例えば、ユーザは、ユーザが登録を遂行する前に、「自分の顧客を知る」（ＫＹＣ）規則に従って、依拠当事者によって以前識別されたことがあり得る。８０１において、ユーザは、依拠当事者によって識別され（例えば、ＫＹＣを使用して）、依拠当事者は、このユーザのための電子記録をそのデータベース内に作成する。

【００６２】

８０２において、ユーザは、依拠当事者のウェブサイトを訪問し、依拠当事者のウェブアプリケーションは、ユーザの装置が強化された認証機能（例えば、ネットワークを介した遠隔認証のための本明細書に記載されているものなど）を備えていることを検出する。

【００６３】

８０３において、ユーザは、依拠当事者への登録を開始する。例えば、認証部のための公開鍵／秘密鍵のペアを生成するために、図５に示されているような一連のトランザクションが遂行され得る。８０４において、依拠当事者は、アウトオブバンド方法（例えば、郵便、電子メール、ＳＭＳなど）を使用して秘密（例えば、登録された公開鍵のハッシュ）をユーザに送付する。

【００６４】

８０５において、依拠当事者は、セキュアトランザクション確認操作をトリガする。例えば、一実施形態において、秘密及び一意的なアカウントＩＤコードを潜在的に含むメッセージがユーザに表示され得、情報（例えば、「アウトオブバンド方法を通じて受領した暗号鍵ハッシュは、今回私のセキュアディスプレイ上に表示されたものと同一であること、及びそれがそこに示されているＡｐｐＩＤに登録されたことを私は確認します」）を確認することをユーザに求める。次いで、８０６において、ユーザは、秘密及びＩＤコードがセキュアディスプレイ内に表示されたものに一致する場合、トランザクションを許容することができ、それによって８０７において登録を確認する。ユーザが８０６においてトランザクションを拒絶する場合（例えば、表示された情報が秘密及び／又はＩＤコードに一致しないため）、登録は、８０８において拒絶される。

【００６５】

図８Ｂは、ユーザが依拠当事者に知られている登録後プロセスの別の実施形態を図示している。この場合も、ユーザは、ユーザが登録を遂行する前に、「自分の顧客（ＫＹＣ）を知る」規則に従って依拠当事者によって以前識別されたことがあり得る。８１１において、ユーザは、依拠当事者によって識別され（例えば、ＫＹＣを使用して）、依拠当事者は、このユーザのための電子記録をそのデータベース内に作成する。

【００６６】

８１２において、ユーザは、依拠当事者のウェブサイトを訪問し、依拠当事者のウェブアプリケーションは、ユーザの装置が強化された認証機能（例えば、ネットワークを介した遠隔認証のための本明細書に記載されているものなど）を備えていることを検出する。

【００６７】

８１３において、ユーザは、依拠当事者への登録を許容する。例えば、認証部のための公開鍵／秘密鍵のペアを生成するために、図５に示されているような一連のトランザクションが遂行され得る。８０４において、依拠当事者は、セキュアトランザクション確認操作をトリガする。例えば、一実施形態において、一意的なアカウントＩＤコードを潜在的に含むメッセージがユーザに表示され得、情報（例えば、「私は、登録内容を確認し、以下に示される公開鍵ハッシュに署名したものを認証されたアウトオブバンドチャネルを介して送付します」）を確認することをユーザに求める。

【００６８】

８１５において、ユーザは、セキュアディスプレイ上に示された公開鍵ハッシュを、認証されたアウトオブバンドチャネル（例えば、署名されたレター）を介して送信する。８１６において、依拠当事者は、８１５において送信された公開鍵ハッシュを工程８１３で受信した公開鍵ハッシュによって検証し、８１７において登録を許容し得る。値が一致し

ない場合、依拠当事者は、８１８において登録を拒絶する。
【００６９】
２．事前登録
図９は、依拠当事者が（例えば、それぞれのＫＹＣ規則に従って）ユーザを識別する前にユーザが依拠当事者への登録を遂行するプロセスの一実施形態を図示している。９０１において、ユーザは、依拠当事者のウェブサイトを訪問し、依拠当事者のウェブアプリケーションは、ユーザの装置が強化された認証機能（例えば、ネットワークを介した遠隔認証のための本明細書に記載されているものなど）を備えていることを検出する。
【００７０】
９０２において、ユーザは、依拠当事者への登録を開始する。例えば、認証部のための公開鍵／秘密鍵のペアを生成するために、図５に示されているような一連のトランザクションが遂行され得る。９０３において、依拠当事者は、登録要求に関してトランザクション確認操作をトリガする。例えば、ユーザが依拠当事者に登録することを希望する旨の確認を要求するメッセージがセキュアディスプレイ内に表示され得る（例えば、「私は、＜依拠当事者＞に登録することを希望し、後ほどＫＹＣを受けます」）。更に、セキュアディスプレイは、コード（例えば、公開鍵のハッシュ）及びＡｐｐＩＤを表示し得る。このコードは「秘密」コードであってもよく、そうでなくてもよいことに留意されたい。
【００７１】
９０４において、ユーザは、認証されたアウトオブバンド機構を使用して、依拠当事者にコードを送信する。例えば、一実施形態において、ユーザは、ハッシュのプリントアウトを依拠当事者の支社に物理的に持参し、それをＫＹＣ確認の一環として提示してもよい。代替的に、ユーザは、識別手順の一部をなす様式にコードを記入してもよい。代替的に、ユーザは、秘密を電子メール、郵便、ＳＭＳ、又は任意の他の種類の認証されたアウトオブバンドチャネルを介して送付してもよい。
【００７２】
９０５において、依拠当事者は、コードの検証を遂行する（例えば、公開鍵ハッシュを、登録中にユーザから受領した公開鍵に基づいて計算された値と比較する）。９０６において一致が確認された場合、９０７において登録が確認される。一致が確認されなかった場合、９０８において登録が拒絶される。
【００７３】
３．準同時登録
一部のユーザは、アイデンティティ証明書を含む電子ＩＤカードなどの資格証明書を既に有している。このアイデンティティ証明書を使用すれば、アウトオブバンド方法を、図１０に図示されているような電子ＩＤカードを使用する電子的方法によって置き換えることができる。
【００７４】
１００１において、ユーザは、依拠当事者のウェブサイトを訪問し、依拠当事者のウェブアプリケーションは、ユーザの装置が強化された認証機能（例えば、ネットワークを介した遠隔認証のための本明細書に記載されているものなど）を備えていることを検出する。
【００７５】
１００２において、ユーザは、依拠当事者への登録を許容する。例えば、認証部のための公開鍵／秘密鍵のペアを生成するために、図５に示されているような一連のトランザクションが遂行され得る。１００３において、依拠当事者は、登録要求に関してトランザクション確認操作をトリガする。例えば、トランザクション確認のセキュアディスプレイは、ユーザが既存の資格証明書を使用して依拠当事者に登録することを希望する旨の確認を要求するメッセージを表示し得る（例えば、「私は、＜依拠当事者＞に登録することを希望し、私のｅＩＤカードに基づく身分証明を使用します」）。更に、セキュアディスプレイは、秘密（例えば、公開鍵のハッシュ）及びＡｐｐＩＤをユーザに対して表示し得る。
【００７６】

１００４において、ユーザは、ＡｐｐＩＤ及び公開鍵のハッシュを含む認証オブジェクト（例えば、文書又はバイナリファイル）を作成し、既存の資格証明書（例えば、ユーザの電子ＩＤカード上のアイデンティティ証明書）に関係する秘密鍵を使用してこのオブジェクトに署名する。１００５において、依拠当事者は、署名されたオブジェクトを検証し、資格証明書（例えば、アイデンティティ証明書）からアイデンティティデータを抽出する。更に、依拠当事者は、署名されたオブジェクトから抽出されたこの公開鍵ハッシュを、登録時にそのユーザから受領した公開鍵に基づいて計算されたハッシュ値と比較する。１００６で判定されたときにそれらが一致する場合、１００７において登録が確認される。そうでない場合、登録は、１００８において拒絶される。

【００７７】

例示的なデータ処理装置

図１１は、本発明のいくつかの実施形態において使用することができる例示的なクライアント及びサーバを図示するブロック図である。図１１は、コンピュータシステムの様々な構成要素を図示しているが、そのような詳細は本発明に適切でないため、構成要素を相互接続する任意の特定のアーキテクチャ又は方法を表すことを意図するものではないことを理解すべきである。より少ない構成要素又は複数の構成要素を有する他のコンピュータシステムもまた、本発明によって使用可能であることが理解されるであろう。

【００７８】

図１１に示されるように、データ処理システムの形態であるコンピュータシステム１１００は、処理システム１１２０に結合されているバス１１５０と、電源１１２５と、メモリ１１３０と、不揮発性メモリ１１４０（例えば、ハードドライブ、フラッシュメモリ、相変化メモリ（ＰＣＭ）など）とを含む。バス１１５０は、当該技術分野において周知であるように、様々なブリッジ、コントローラ及び／又はアダプタを介して互いに接続され得る。処理システム１１２０は、メモリ１１３０及び／又は不揮発性メモリ１１４０から命令を取得することができ、上述したように動作を実行するための命令を実行することができる。バス１１５０は、上記構成要素を一体に相互接続し、また、任意のドック１１６０、ディスプレイコントローラ及びディスプレイ装置１１７０、入力／出力装置１１８０（例えば、ＮＩＣ（ネットワークインターフェースカード）、カーソル制御（例えば、マウス、タッチスクリーン、タッチパッドなど）、キーボードなど）及び任意の無線送受信機１１９０（例えば、ブルートゥース（登録商標）、ＷｉＦｉ、赤外線など）にそれらの構成要素を相互接続する。

【００７９】

図１２は、本発明のいくつかの実施形態において使用され得る例示的なデータ処理システムを図示するブロック図である。例えば、データ処理システム１２００は、ハンドヘルドコンピュータ、パーソナルディジタルアシスタント（ＰＤＡ）、携帯電話、ポータブルゲームシステム、ポータブルメディアプレーヤ、タブレット、又は、携帯電話、メディアプレーヤ及び／又はゲームシステムを含むことができるハンドヘルドコンピューティング装置とすることができる。他の例として、データ処理システム１２００は、ネットワークコンピュータ又は他の装置内の埋め込み処理装置とすることができる。

【００８０】

本発明の一実施形態によれば、データ処理システム１２００の例示的なアーキテクチャは、上述した携帯機器のために使用することができる。データ処理システム１２００は、集積回路上の１つ以上のマイクロプロセッサ及び／又はシステムを含むことができる処理システム１２２０を含む。処理システム１２２０は、メモリ１２１０、（１つ以上のバッテリを含む）電源１２２５、オーディオ入力／出力１２４０、ディスプレイコントローラ及びディスプレイ装置１２６０、任意の入力／出力１２５０、入力装置１２７０及び無線送受信機１２３０に連結されている。図１２には示されていない追加の構成要素はまた、本発明の特定の実施形態においてデータ処理システム１２００の一部であってもよく、本発明の特定の実施形態において図１２に示されるよりも少ない構成要素が使用可能であることが理解されるであろう。更に、図１２には示されていない１つ以上のバスは、当該技

術分野において周知であるように様々な構成要素を相互接続するために使用することができることが理解されるであろう。

【００８１】

メモリ１２１０は、データ処理システム１２００による実行のためのデータ及び／又はプログラムを記憶する。オーディオ入力／出力１２４０は、例えば、音楽を再生するためにマイクロフォン及び／又はスピーカを含むことができ、並びに／又はスピーカ及びマイクロフォンを介して電話機能を提供することができる。ディスプレイコントローラ及びディスプレイ装置１２６０は、グラフィカルユーザインターフェース（ＧＵＩ）を含むことができる。無線（例えば、ＲＦ）送受信機１２３０（例えば、ＷｉＦｉ送受信機、赤外線送受信機、ブルートゥース（登録商標）送受信機、無線携帯電話送受信機など）は、他のデータ処理システムと通信するために使用することができる。１つ以上の入力装置１２７０は、ユーザがシステムに入力を提供するのを可能にする。これらの入力装置は、キーパッド、キーボード、タッチパネル、マルチタッチパネルなどであってもよい。任意の他の入力／出力１２５０は、ドック用コネクタであってもよい。

【００８２】

上述したように、本発明の実施形態は、様々な工程を含んでもよい。工程は、汎用又は特殊目的のプロセッサに特定の工程を実行させる機械実行可能な命令で具現化され得る。代替的に、これらの工程は、工程を実行するためのハードワイヤードロジックを含む特定のハードウェア構成要素によって又はプログラミングされたコンピュータ構成要素及びカスタムハードウェア構成要素の任意の組み合わせによって実行することができる。

【００８３】

本発明の要素はまた、機械実行可能なプログラムコードを記憶する機械可読媒体として提供することができる。機械可読媒体としては、フロッピーディスク、光ディスク、ＣＤ－ＲＯＭ及び光磁気ディスク、ＲＯＭ、ＲＡＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、磁気若しくは光カード、又は、電子プログラムコードを記憶するのに適した他の種類の媒体／機械可読媒体を挙げることができるが、これらに限定されるものではない。

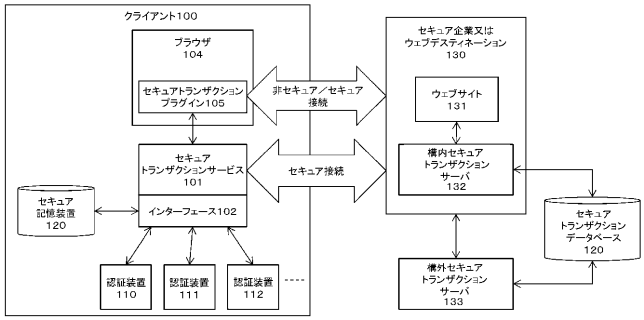
【００８４】

上記の説明全体を通じて、説明の目的のために、多数の具体的な詳細が本発明の完全な理解を提供するために記載された。しかしながら、本発明は、これらの具体的な詳細の一部がなくても実施され得ることは、当業者にとって明らかであろう。例えば、本明細書に記載された機能モジュール及び方法は、ソフトウェア、ハードウェア又はそれらの任意の組み合わせとして実装されてもよいことは、当業者にとって容易に明らかであろう。更に、本発明のいくつかの実施形態は、モバイルコンピューティング環境のコンテキストで本明細書において記載されているが、本発明の基本原理は、モバイルコンピューティングの実装に限定されるものではない。実質的に任意の種類のクライアント又はピアデータ処理装置は、例えば、デスクトップ又はワークステーションコンピュータを含むいくつかの実施形態で使用することができる。したがって、本発明の範囲及び趣旨は、以下の特許請求の範囲の観点から判断されるべきである。

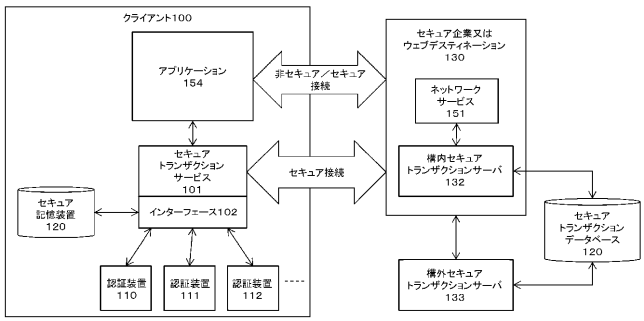
【００８５】

上述したように、本発明の実施形態は、様々な工程を含んでもよい。工程は、汎用又は特殊目的のプロセッサに特定の工程を実行させる機械実行可能な命令で具現化され得る。代替的に、これらの工程は、工程を実行するためのハードワイヤードロジックを含む特定のハードウェア構成要素によって又はプログラミングされたコンピュータ構成要素及びカスタムハードウェア構成要素の任意の組み合わせによって実行することができる。

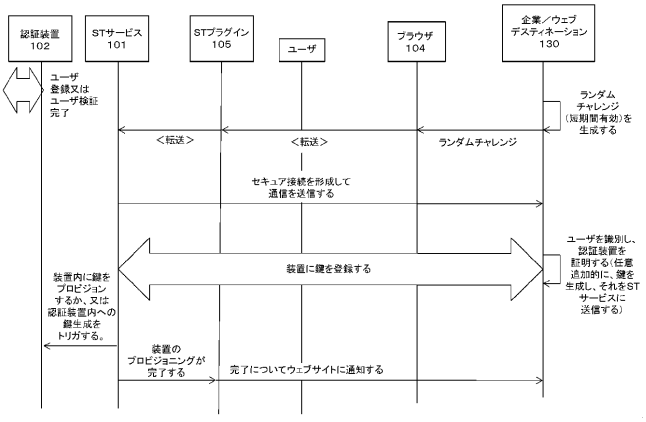
【図１Ａ】



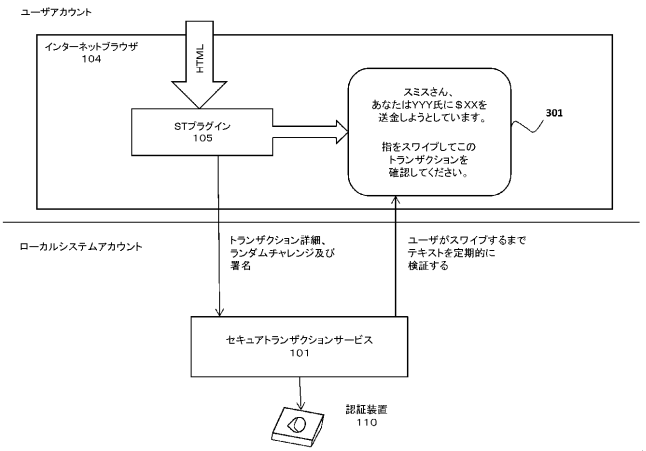
【図１Ｂ】



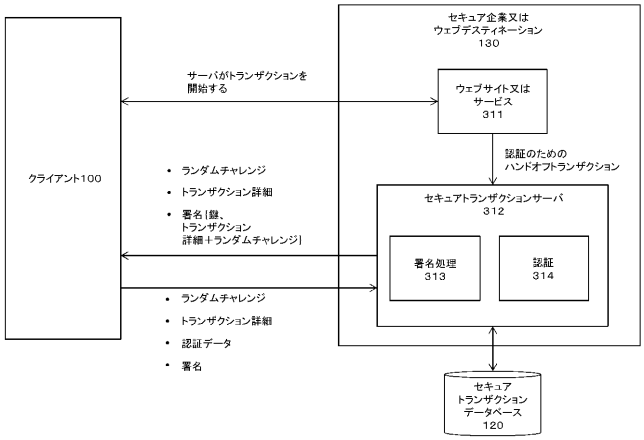
【図２】



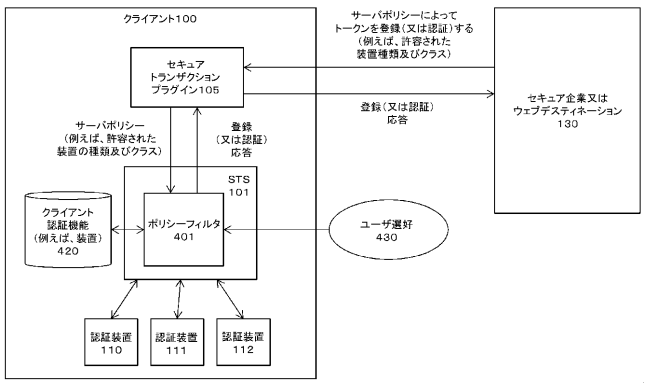
【図３Ａ】



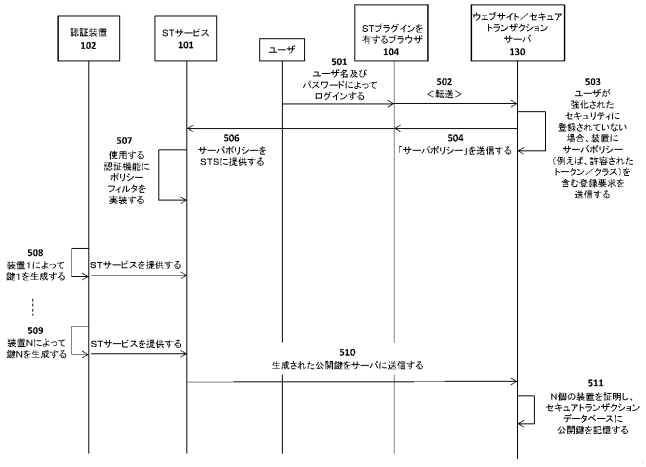
【図３Ｂ】



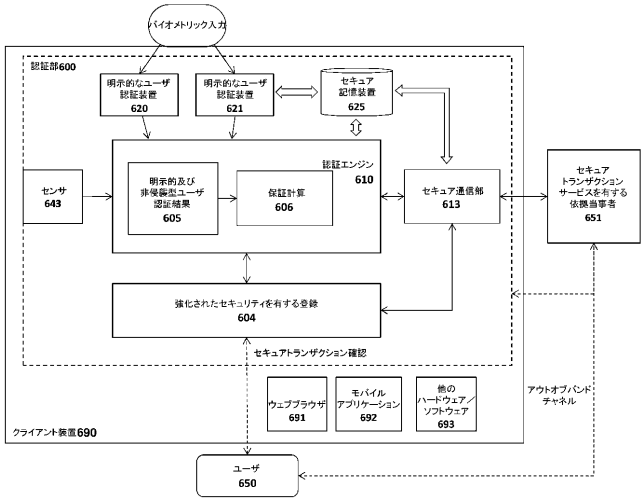
【図４】



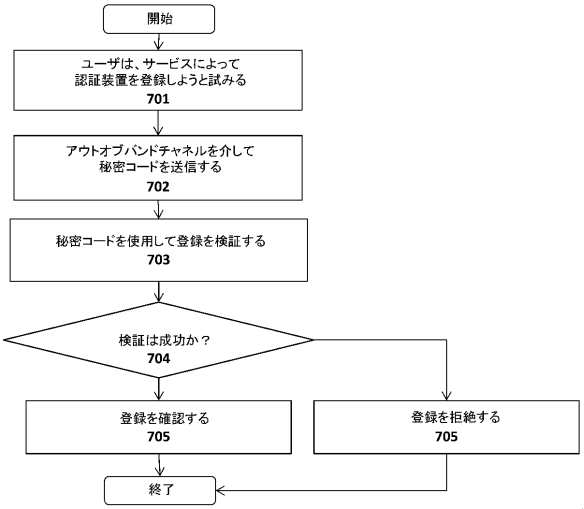
【図５】



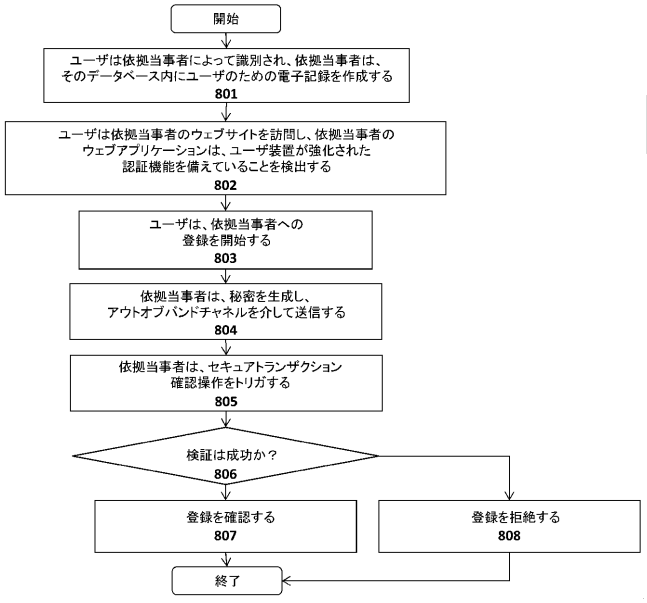
【図６】


バイオメトリック入力
認証部600
明示的なユーザ認証装置 620
明示的なユーザ認証装置 621
セキュア記憶装置 625
センサ 643
明示的及び非侵襲性ユーザ認証結果 605
認証エンジン 610
保証計算 606
セキュア通信部 613
セキュアトランザクションサービスを有する依拠当事者 651
強化されたセキュリティを有する登録 604
セキュアトランザクション確認
ウェブブラウザ 691
モバイルアプリケーション 692
他のハードウェア／ソフトウェア 693
クライアント装置690
アウトオブバンドチャネル
ユーザ 650

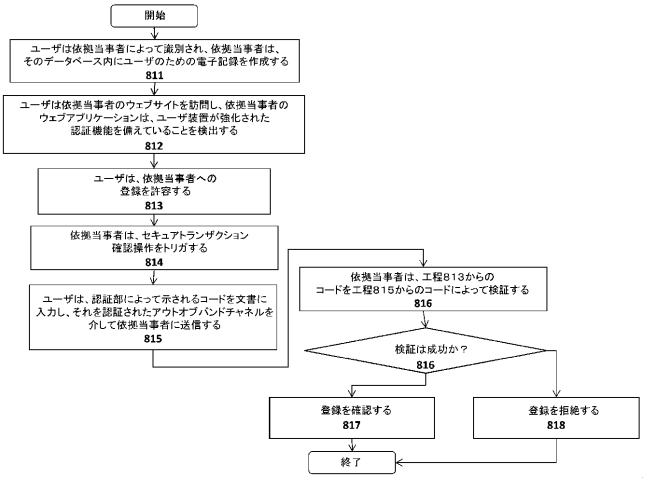
【図７】


開始
ユーザは、サービスによって認証装置を登録しようと試みる 701
アウトオブバンドチャネルを介して秘密コードを送信する 702
秘密コードを使用して登録を検証する 703
検証は成功か？ 704
登録を確認する 705
登録を拒絶する 705
終了

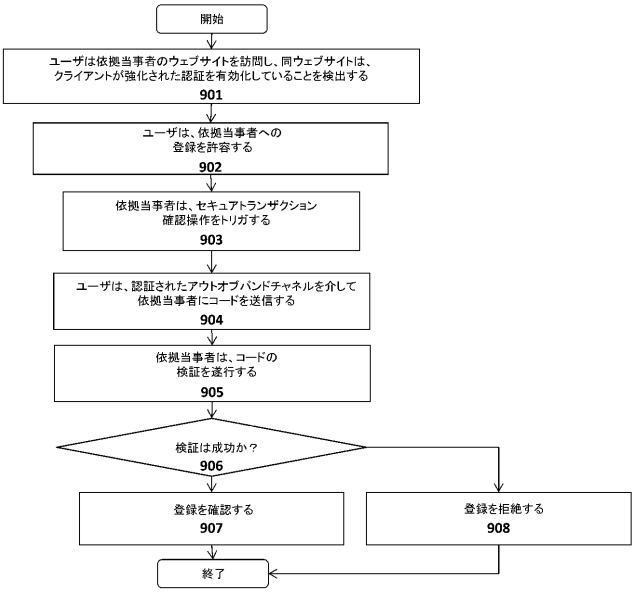
【図８Ａ】


開始
ユーザは依拠当事者によって識別され、依拠当事者は、そのデータベース内にユーザのための電子記録を作成する 801
ユーザは依拠当事者のウェブサイトを訪問し、依拠当事者のウェブアプリケーションは、ユーザ装置が強化された認証機能を備えていることを検出する 802
ユーザは、依拠当事者への登録を開始する 803
依拠当事者は、秘密を生成し、アウトオブバンドチャネルを介して送信する 804
依拠当事者は、セキュアトランザクション確認操作をトリガする 805
検証は成功か？ 806
登録を確認する 807
登録を拒絶する 808
終了

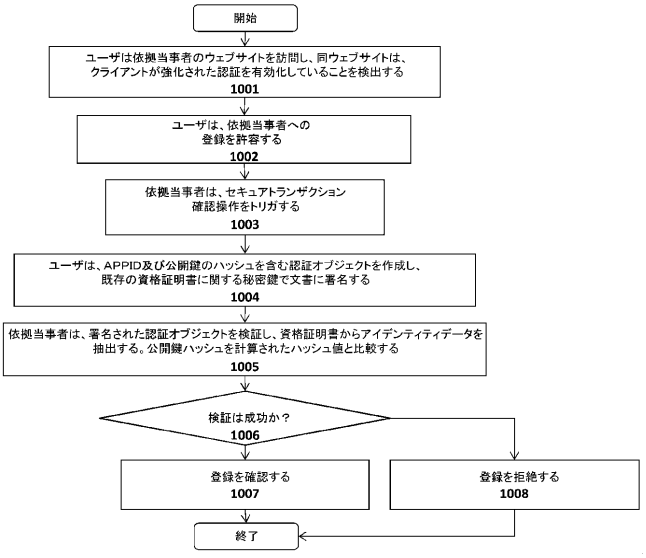
【図８Ｂ】


開始
ユーザは依拠当事者によって識別され、依拠当事者は、そのデータベース内にユーザのための電子記録を作成する 811
ユーザは依拠当事者のウェブサイトを訪問し、依拠当事者のウェブアプリケーションは、ユーザ装置が強化された認証機能を備えていることを検出する 812
ユーザは、依拠当事者への登録を許容する 813
依拠当事者は、セキュアトランザクション確認操作をトリガする 814
ユーザは、認証部によって示されるコードを文書に入力し、それを認証されたアウトオブバンドチャネルを介して依拠当事者に送信する 815
依拠当事者は、工程813からのコードを工程815からのコードによって検証する 816
検証は成功か？ 816
登録を確認する 817
登録を拒絶する 818
終了

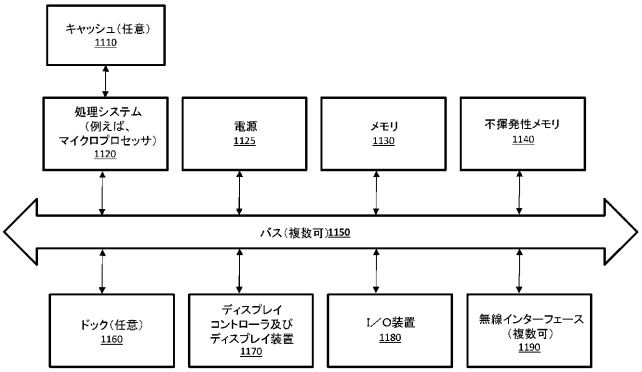
【図９】



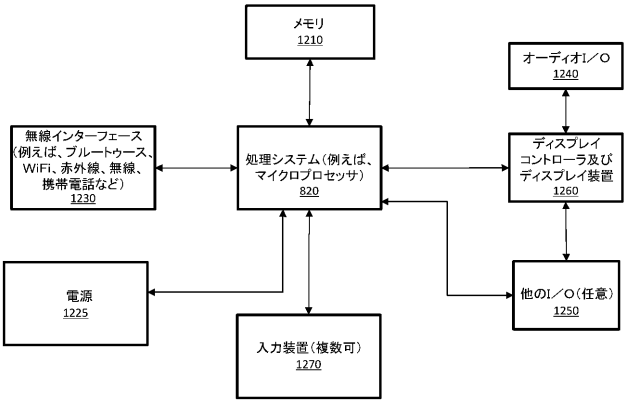
【図１０】



【図１１】



【図１２】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/028927

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 29/06 (2015.01)
CPC - H04L 63/08 (2015.04)
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(8) - G06F21/00, G06F17/30, G06F15/16, G06F7/04, H04L9/32, H04L29/06 (2015.01)
USPC - 713/151, 153, 155, 166, 168, 170, 182, 184, 185; 726/19, 21, 26, 3,5, 6, 7, 9

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC - (See Page 3)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Orbit, Google Patents, Google Scholar, Google.
Search terms used: security, authenticator, authentication device, registration, user, request, out-of-band, communication, code, PIN, SHA, hash operation, public key, private key, pair

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- Y	US 8,713,325 B2 (GANESAN) 29 April 2014 (29.04.2014) entire document	1-5, 7-14, 16-23 --- 6, 15
Y	US 2010/0042848 A1 (ROSENER) 18 February 2010 (18.02.2010) entire document	6, 15
A	US 8,060,922 B2 (CRICHTON et al.) 15 November 2011 (15.11.2011) entire document	1-23
A	US 8,245,030 B2 (LIN) 14 August 2012 (14.08.2012) entire document	1-23
A	US 2014/0068746 A1 (GONZALEZ MARTÍNEZ et al.) 06 March 2014 (06.03.2014) entire document	1-23
A,P	US 2014/0189779 A1 (BAGHDASARYAN et al.) 03 July 2014 (03.07.2014) entire document	1-23
A,P	US 8,719,905 B2 (GANESAN) 06 MAY 2014 (06.05.2014) entire document	1-23

☐ 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
09 July 2015	30 JUL 2015
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Blaine Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2015/028927

CPC - G06F17/30861, G06F21/30, G06F21/31, G06F21/32, G06F21/33, G06F21/34, G06F21/43, G06F21/72, G06F21/83, G06F21/84, G06F21/85, G06F2221/2107, G08Q20/12, G06Q20/40, G06Q30/06, H04L2463/082, H04L63/0428, H04L63/0435, H04L63/0442, H04L63/06, H04L63/062, H04L63/08, H04L63/0807, H04L63/0823, H04L63/083, H04L63/0838, H04L63/0846, H04L63/0853, H04L63/0861, H04L63/0884, H04L63/10, H04L63/105, H04L63/126, H04L63/1441, H04L63/1483, H04L63/18, H04L67/02, H04L67/2814, H04L9/0819, H04L9/32, H04L9/3213, H04L9/3215, H04L9/3228, H04L9/3231, H04L9/3234, H04L9/3271, H04L9/3281, H04W12/04 (2015.04) (keyword delimited)

フロントページの続き

(51)Int.Cl.	FI	テーマコード（参考）
	G06F 21/33	

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

(74)代理人 100109070
弁理士 須田 洋之
(74)代理人 100109335
弁理士 上杉 浩
(74)代理人 100120525
弁理士 近藤 直樹
(72)発明者 リンデマン ロルフ
アメリカ合衆国 カリフォルニア州 ９４３０３ パロ アルト ジェン ロード ２１００ スイート １０５

Ｆターム(参考) 5J104 AA07 AA16 EA01 EA04 EA20 KA01 KA05 KA06 KA16 NA02
NA37 PA07