(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2018-522353
(P2018-522353A)
(43)公表日　平成30年8月9日(2018.8.9)

(51)Int.Cl.		F I			テーマコード（参考）
G06Q 20/40	***(2012.01)***	G06Q	20/40	300	5J104
H04L 9/08	***(2006.01)***	H04L	9/00	601B	5L055
H04L 9/32	***(2006.01)***	H04L	9/00	601E	
		H04L	9/00	675A	

審査請求 有　予備審査請求 未請求　（全 51 頁）

(21)出願番号　特願2018-502105 (P2018-502105)
(86)(22)出願日　平成28年6月13日 (2016.6.13)
(85)翻訳文提出日　平成30年3月7日 (2018.3.7)
(86)国際出願番号　PCT/US2016/037159
(87)国際公開番号　WO2017/014863
(87)国際公開日　平成29年1月26日 (2017.1.26)
(31)優先権主張番号　14/802,210
(32)優先日　平成27年7月17日 (2015.7.17)
(33)優先権主張国　米国 (US)

(71)出願人　500557864
マスターカード　インターナショナル　インコーポレーテッド
アメリカ合衆国　ニューヨーク州　１０５７７－２５０９　パーチェス　パーチェス　ストリート　２０００
(74)代理人　100147485
弁理士　杉村　憲司
(74)代理人　230118913
弁護士　杉村　光嗣
(74)代理人　100192924
弁理士　石井　裕充
(72)発明者　クリスチャン　ラデュ
ベルギー国　１３２０　ボーヴシェン　リュ　ド　トゥランヌ　２

最終頁に続く

(54)【発明の名称】サーバベースド支払のための認証システム及び方法

(57)【要約】
２要素認証機構を利用する支払トランザクション実行方法を開示する。該方法は、秘密鍵がエンコードされた暗号関数を用いて暗号処理を行うことを含む。暗号関数はコンピューティング装置内に格納されている。秘密鍵は第１の認証要素として機能する。該方法は、支払トランザクションの実行に際して第２の認証要素を活用することをさらに含む。

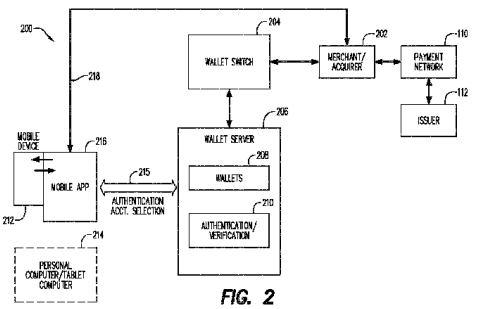


FIG. 2

【特許請求の範囲】
【請求項１】
２要素認証を利用する支払トランザクションを実行する方法であって、該方法は、
秘密鍵がエンコードされた暗号関数を用いて暗号処理を行うステップであって、前記暗号関数はコンピューティング装置内に格納されており、前記秘密鍵は第１の認証要素として機能する、ステップと、
前記支払トランザクションを実行するに際して第２の認証要素を活用するステップ
とを含む、方法。
【請求項２】
前記第２の認証要素は前記コンピューティング装置のユーザのバイオメトリック特徴である、請求項１に記載の方法。
【請求項３】
前記第２の認証要素は前記コンピューティング装置のユーザに知られている秘密コードである、請求項１に記載の方法。
【請求項４】
前記コンピューティング装置は、携帯電話とパソコンとタブレットコンピュータとからなる群から選択される、請求項３に記載の方法。
【請求項５】
前記秘密鍵は、前記コンピューティング装置内で実行される支払アプリケーションの初期化時に前記暗号関数にエンコードされる、請求項４に記載の方法。
【請求項６】
前記秘密鍵は、前記初期化時に前記支払アプリケーションによってランダムに生成される、請求項５に記載の方法。
【請求項７】
前記暗号処理を行うステップは、遠隔サーバから前記コンピューティング装置へと前記支払トランザクションの一部として送信された暗号化一回用鍵を復号するために前記秘密鍵を用いることを含む、請求項５に記載の方法。
【請求項８】
前記コンピューティング装置のユーザが、前記支払トランザクションに際して、前記ユーザに割り当てられており且つ遠隔ウォレットサーバにてホスティングされているデジタルウォレットにアクセスすることを許可される、請求項１に記載の方法。
【請求項９】
コンピューティング装置を用いて一連の支払トランザクションを実行する方法であって、前記一連の支払トランザクションは第１の支払トランザクションと第２の支払トランザクションとを含み、前記第２の支払トランザクションは前記一連の支払トランザクションにおいて前記第１の支払トランザクションの直後に続き、各支払トランザクションはそれぞれについての装置認証段階とそれぞれについてのユーザ認証段階とを含んでおり、該方法は、
前記第１の支払トランザクションの前記装置認証段階を行うステップと、
第１のセッション暗号鍵を用いて前記第１の支払トランザクションの前記ユーザ認証段階を行うステップと、
前記第１の支払トランザクションの前記ユーザ認証段階の一環として、第２のセッション暗号鍵の生成のために用いられるべき入力を受信するステップと、
前記第２のセッション暗号鍵を、前記第２の支払トランザクションの前記装置認証段階の一環として行われる暗号オペレーションのための入力値として、用いるステップと、
第３のセッション暗号鍵を用いて前記第２の支払トランザクションの前記ユーザ認証段階を行うステップであって、前記第１、第２及び第３のセッション暗号鍵は全て互いに異なっている、ステップ
とを含む、方法。
【請求項１０】

前記第２のセッション暗号鍵の生成のために用いられるべき入力を前記コンピューティング装置内にて所定期間格納するステップであって、前記所定期間は前記第１の支払トランザクションの完了後及び前記第２の支払トランザクションの開始前である、ステップをさらに含む、請求項９に記載の方法。

【請求項１１】

前記第１の支払トランザクションの前記ユーザ認証段階の一環として前記コンピューティング装置にてチャレンジ値を受信するステップであって、前記チャレンジ値は遠隔サーバによって前記コンピューティング装置に提供される、ステップをさらに含む、請求項１０に記載の方法。

【請求項１２】

前記チャレンジ値を、前記第２の支払トランザクションの前記装置認証段階の一環として行われる暗号オペレーションのための入力値として、用いるステップをさらに含む、請求項１０に記載の方法。

【請求項１３】

前記チャレンジ値を前記コンピューティング装置内にて前記所定期間格納するステップをさらに含む、請求項１２に記載の方法。

【請求項１４】

第１の一回用鍵を復号して前記第１のセッション暗号鍵を取得するステップであって、前記第１の一回用鍵は前記第１の支払トランザクションとの関連で遠隔サーバから前記コンピューティング装置に提供される、ステップと、

第２の一回用鍵を復号して前記第２のセッション暗号鍵を取得するステップであって、前記第２の一回用鍵は前記第１の支払トランザクションの一環として前記遠隔サーバから前記コンピューティング装置に提供される、ステップ

とをさらに含む、請求項９に記載の方法。

【請求項１５】

前記コンピューティング装置は、携帯電話とパソコンとタブレットコンピュータとからなる群から選択される、請求項９に記載の方法。

【請求項１６】

前記第１及び第２の支払トランザクションのそれぞれについてのユーザ認証段階との関連で秘密コードが前記コンピューティング装置に入力され、前記秘密コードは前記第１及び第２の支払トランザクションのそれぞれについてのユーザ認証段階との関連で前記コンピューティング装置によって行われるそれぞれの暗号処理の入力値として前記コンピューティング装置によって用いられる、請求項９に記載の方法。

【請求項１７】

前記コンピューティング装置のユーザが、前記第１及び第２の支払トランザクションに際して、前記ユーザに割り当てられており且つ遠隔ウォレットサーバにてホスティングされているデジタルウォレットにアクセスすることを許可される、請求項９に記載の方法。

【請求項１８】

現在の支払トランザクションを実行する方法であって、

認証リクエストをコンピューティング装置から遠隔サーバへと送信するステップであって、前記認証リクエストは、前記コンピューティング装置のユーザを識別するユーザ識別データと、前記コンピューティング装置を識別する装置識別データと、前記認証リクエストのために前記コンピューティング装置内にてランダムに生成された第１のチャレンジ値とを含む、ステップと、

前記遠隔サーバとＴＬＳ（トランスポート層セキュリティ）ハンドシェーク処理を行って前記コンピューティング装置と前記遠隔サーバとの間でのトンネリング通信チャネルを開設するステップであって、前記ＴＬＳハンドシェーク処理は前記遠隔サーバから応答を受信することを含み、前記応答は第２のチャレンジ値とデジタル証明書と前記遠隔サーバによって提案された暗号処理アルゴリズムについての識別子とを含み、前記ＴＬＳハンドシェーク処理は前記遠隔サーバによって提案された暗号処理アルゴリズムと合致する暗号

処理アルゴリズムを選択することをさらに含み、前記ＴＬＳハンドシェーク処理は前記遠隔サーバから受信された前記デジタル証明書を検証することをさらに含み、前記ＴＬＳハンドシェーク処理は前記遠隔サーバと関連付けられている公開暗号化鍵にアクセスすることをさらに含み、前記ＴＬＳハンドシェーク処理は秘密の値をランダムに生成することをさらに含み、前記ＴＬＳハンドシェーク処理は前記公開暗号化鍵で前記秘密の値を暗号化してデジタルエンベロープを生成することをさらに含み、前記ＴＬＳハンドシェーク処理は前記デジタルエンベロープを前記遠隔サーバへと送信することをさらに含み、前記ＴＬＳハンドシェーク処理はサーバ信頼性証明値を前記遠隔サーバから受信することをさらに含み、前記ＴＬＳハンドシェーク処理は前記秘密の値と前記第１のチャレンジ値と前記第２のチャレンジ値とに基づいてセキュアチャンネル鍵Ｋを計算することをさらに含み、前記ＴＬＳハンドシェーク処理は前記セキュアチャンネル鍵Ｋと前記第１のチャレンジ値と前記第２のチャレンジ値とを入力として受ける暗号処理を介して前記サーバ信頼性証明値を検証することをさらに含む、ステップと、

前記セキュアチャンネル鍵Ｋを用いて前記遠隔サーバと装置認証処理段階を行うステップであって、前記装置認証処理段階は前記コンピューティング装置内に格納された暗号化データベースから第１のハッシュ値と第１の暗号化一回用鍵と第３のチャレンジ値とを検索することを含み、前記第１の暗号化一回用鍵は以前の支払トランザクションのユーザ認証処理段階において前記コンピューティング装置によって受信され、前記以前の支払トランザクションは前記コンピューティング装置によって行われた一連の支払トランザクションにおいて前記現在の支払トランザクションの直前にあり、前記第１の暗号化一回用鍵は前記コンピューティング装置内に格納された支払アプリケーション内にエンコードされた鍵と同一であるトランスポート鍵を用いて暗号化され、前記第３のチャレンジ値は前記以前の支払トランザクションのユーザ認証段階との関連で前記コンピューティング装置によって前記遠隔サーバから受信され、前記第１のハッシュ値は装置フィンガプリントデータ及び第１のソルト値に第１のハッシュ関数を適用することによって計算され、前記装置認証処理段階は前記支払アプリケーション内にエンコードされた前記鍵を用いて前記第１の暗号化一回用鍵を復号することをさらに含み、前記装置認証処理段階は第１のセッション鍵と前記第２のチャレンジ値とトランザクションカウンタ値とを含む入力に基づいて第１の暗号を生成することをさらに含み、前記第１のセッション鍵は前記復号された第１の一回用鍵と前記第１のハッシュ値と前記第３のチャレンジ値とから導出され、前記装置認証処理段階は前記第１の暗号を前記コンピューティング装置から前記遠隔サーバへと送信することをさらに含む、ステップと、

前記装置認証処理段階に続いて前記セキュアチャンネル鍵Ｋを用いて前記現在の支払トランザクションのユーザ認証処理段階を行うステップであって、前記現在の支払トランザクションのユーザ認証段階は前記遠隔サーバから第２の暗号化一回用鍵と第３の暗号化一回用鍵と第４のチャレンジ値とを受信することを含み、前記現在の支払トランザクションのユーザ認証段階は前記第２の暗号化一回用鍵と前記第４のチャレンジ値とを前記暗号化データベースに格納することをさらに含み、前記現在の支払トランザクションのユーザ認証段階は第２のソルト値を前記暗号化データベースから検索することをさらに含み、前記現在の支払トランザクションのユーザ認証段階はユーザに対してＰＩＮ（暗証番号）を入力するように促すことをさらに含み、前記現在の支払トランザクションのユーザ認証段階は前記ユーザのＰＩＮを表すユーザ入力を受信することをさらに含み、前記現在の支払トランザクションのユーザ認証段階は前記支払アプリケーション内にエンコードされた前記鍵を用いて前記第３の暗号化一回用鍵を復号することをさらに含み、前記現在の支払トランザクションのユーザ認証段階は第２のセッション鍵と前記第４のチャレンジ値とトランザクションデータとを含む入力に基づいて第２の暗号を生成することをさらに含み、前記第２のセッション鍵は前記ユーザ入力を用いて前記復号された第３の一回用鍵から導出され、前記現在の支払トランザクションのユーザ認証段階は前記第２の暗号を前記コンピューティング装置から前記遠隔サーバへと送信することをさらに含む、ステップと、

前記コンピューティング装置を介して前記ユーザのデジタルウォレットへのアクセスを

受信するステップ
とを含む、方法。
【請求項１９】
前記ユーザのデジタルウォレットは前記遠隔サーバ上にて維持される、請求項１８に記載の方法。
【請求項２０】
前記コンピューティング装置は、携帯電話とパソコンとタブレットコンピュータとからなる群から選択される、請求項１８に記載の方法。
【請求項２１】
第１の支払トランザクションと第２の支払トランザクションとの関係でサーバコンピュータ内にて認証サービスを行うステップであって、前記第１及び第２の支払トランザクションはコンピューティング装置によって要求されており、前記第１の支払トランザクションは前記コンピューティング装置によって要求された一連の支払トランザクションにおいて前記第２の支払トランザクションの直前にある、ステップを含む方法であって、
前記認証サービスは、
（ｉ）前記第１の支払トランザクションの装置認証処理段階であって、前記サーバコンピュータは前記第１の支払トランザクションの装置認証処理段階中に第１の暗号を受信及び検証する、処理段階と、
（ｉｉ）前記第１の支払トランザクションのユーザ認証処理段階であって、前記サーバコンピュータは（ａ）第１の一回用鍵と第２の一回用鍵とを計算し、且つ、（ｂ）前記第１及び第２の一回用鍵を前記第１の支払トランザクションの前記ユーザ認証処理段階の一環として前記コンピューティング装置へと送信する、処理段階と、
（ｉｉｉ）前記第２の支払トランザクションの装置認証処理段階であって、前記サーバコンピュータは前記第２の支払トランザクションの装置認証処理段階中に第２の暗号を受信及び検証し、前記第２の暗号を検証することは第１のセッション鍵を計算することを含み、前記第１のセッション鍵は前記第１の支払トランザクションの前記ユーザ認証処理段階の前記ユーザ認証処理段階中に計算された前記第２の一回用鍵を生成するのに前記サーバコンピュータによって用いられた第２のセッション鍵と同一である、処理段階と、
（ｉｖ）前記第２の支払トランザクションのユーザ認証処理段階
とを含む、
方法。
【請求項２２】
前記サーバコンピュータは前記第１及び第２の一回用鍵を暗号化形式で前記コンピューティング装置へと送信する、請求項２１に記載の方法。
【請求項２３】
前記サーバコンピュータは前記コンピューティング装置のユーザのためのデジタルウォレットを維持する、請求項２１に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、サーバベースド支払のための認証システム及び方法に関する。
【０００２】
関連出願の相互参照
本願は、２０１５年７月１７日に出願された米国特許出願１４／８０２，２１０号に基づく優先権を主張するものであり、その内容は参照によって本明細書に全て取り込まれるものである。
【背景技術】
【０００３】
クレジットカード口座やデビットカード口座等の支払口座は、広範に用いられている。支払口座をアクセスする１つの従来的な態様においては、口座保有者が、小売店内のＰＯ

Ｓ（point of sale）端末でプラスチック製のカードを提示する。ＰＯＳ端末は、カードから口座情報を（例えば、磁気ストライプを介して、又は、カード内の集積回路との無線通信を通じて、又は、カード上の電気接点を介する等して）読み取り、そして、カードから読み取られた情報を用いて支払口座トランザクションを開始する。

【０００４】

支払口座は、電子商取引においても広範に用いられている。例えば、口座保有者は、パソコン又はスマートフォンを用いて業者（商人、販売者）のオンラインストアのウェブページにアクセスする。購入する商品を選んで、そして「チェックアウト」を選択した後、口座保有者に対して入力催促がなされるのであり、該催促では口座保有者自身の支払口座情報を、自身のコンピュータ（又はスマートフォン）にダウンロードされたデータ入力画面内へと入力するように促される。そして、業者の電子商取引用ホストコンピュータは、口座保有者によって入力された情報を用いて支払口座トランザクションを開始する。

【０００５】

支払口座のユーザの多くが複数のそのような口座を保有していることからして、所謂デジタルウォレットに関する提言がなされている。提案されている１つの案によると、ウォレットサービスプロバイダ（ＷＳＰ、wallet service provider）が多数のユーザのためにデジタルウォレットを維持する。各ユーザは自己の支払口座の幾つか又は全てを自己のデジタルウォレットに登録するのであり、ＷＳＰは各々のユーザの専用データパーティションに対応する情報を格納し、これによって各自のデジタルウォレットが形成される。電子商取引購買トランザクションの最終段階にてユーザがチェックアウトを希望する際に、ＷＳＰにある自己のウォレットにアクセスする選択肢がユーザに対して与えられる。ユーザのコンピュータ／スマートフォンと、業者の電子商取引ホストコンピュータと、ＷＳＰのコンピュータとの間でのデータ通信がなされるのであり、ユーザに対しては、現在の電子商取引トランザクションに使用するための自己の登録済み口座を１つ選ぶ選択肢が与えられる。これとの関連でのユーザに掛かる負担は、極僅かなものであることができる。ユーザが所望の支払口座を自己のデジタルウォレットから選んだらば、業者は、対応する口座情報を用いることができ、ユーザによって選ばれた口座を用いた支払口座トランザクションを開始することができる。このような案ではユーザ／オンライン購買者に対して多大な利便性をもたらすことができる。なぜならば、電子商取引トランザクションの一部として支払口座情報についての詳細事項を入力する手間から各人が解放されるからである。同時に、様々な支払口座から口座を選ぶ選択肢がユーザに与えられており、また、業者の電子商取引コンピュータ上での格納のために自己の支払口座情報を預けることが不要とされる。

【０００６】

デジタルウォレットに関する別の案は、支払可能スマートフォン又は類似の携帯機器に基づいている。支払可能スマートフォン内に単一の支払口座クレデンシャル（証明書）のセットを格納する代わりに、支払可能スマートフォン内に複数の異なる支払口座に関する情報をユーザが入力することできる。スマートフォンはウォレットアプリケーションを実行しており、該アプリケーションはスマートフォン内に格納された支払カード口座情報へのユーザアクセスを管理する。スマートフォン内のウォレット機能に対応する口座情報は、スマートフォン内の所謂「セキュア要素」（ＳＥ、secure element）内に格納されていることができる。ＰＯＳにてユーザは、スマートフォンのユーザインターフェースを介してスマートフォンウォレットアプリケーションと対話して、スマートフォン内に情報が格納されている支払口座の１つを選ぶ。そして、スマートフォンは、選ばれた支払口座についての情報を、近距離無線通信（ＮＦＣ、Near Field Communication）又は他の標準化された通信プロトコルを用いて、ＰＯＳ端末へと無線送信する。例えば、スマートフォンは支払口座アプリ（app、application program）を実行することができるのであり、該アプリはＰＯＳ端末とＩＣ支払カードとの対話をエミュレートする。そして、ＰＯＳ端末は、スマートフォンから受信した支払カード口座情報に基づいて支払カード口座トランザクションを開始する。

【０００７】
スマートフォンのＳＥ機能を遠隔的にエミュレートする案も提案されており、これによってデジタルウォレット機能を提供するスマートフォンのハードウェアコスト及びハードウェア複雑度を下げることができる。ＳＥはモバイルネットワークオペレータ（ＭＮＯ、Mobile Network Operator）又は装置製造者の支配下にある故に、カードをホスティングしているＷＳＰ又はカード発行者はＭＮＯ又は装置製造者に依存せざるを得なくなる。
【０００８】
経営上の配慮及び一部の領域における規制上の要求によって、デジタルウォレットへのユーザアクセスを不正利用から保護することが要求されるのであり、これを高度のセキュリティでなすことを要する。同時に、他の経営上の配慮からすれば、既存の技術的プラットフォーム及びディストリビューションシステムに基づいて、装置製造者やＭＮＯ等の主体に面倒な又は金銭的に厳しい負担を負わせずにセキュリティ対策を容易に且つ経済的に策定・実施することができることを要する。即ち、最重要なのは、適切なレベルのセキュリティ対策を講じつつ、ウォレットトランザクションの実行に際して単純かつ簡単なユーザエクスピリエンスを提供することの望ましさなのかもしれない。
【図面の簡単な説明】
【０００９】
本発明の特徴及び長所並びにこれらが実現される態様は、以下の発明についての詳細な説明と添付の図面とを参照することによってより明らかになるのであり、該図面は好適な又は例示的な実施形態を示すものでありこれらは縮尺通りに描写されているとは限らない。
【００１０】
【図１】従来型支払システムについてのブロック図である。
【図２】本発明の諸側面に基づいてもたらされる支払システムについてのブロック図である。
【図３】図２のシステムの一部として提供されまた本発明の諸側面に基づくコンピュータシステムについてのブロック図である。
【図４】図２のシステム内での支払トランザクションとの関連で用いることができる携帯型機器についてのブロック図である。
【図５】図２のシステムにて実装される認証機能についての概略図である。
【図６】図２のシステムのユーザ装置にて実装され得るホワイトボックス暗号化手法を表す図である。
【図７】ユーザ装置へ認証クレデンシャルを提供するための従来的手法についての概略図である。
【図８】本発明の諸側面による、認証クレデンシャル提供のための手法について示す図である。
【図９】図２のシステムで認証手続を実装するためのアーキテクチャについて示す図である。
【図１０】一部の実施形態による、認証クレデンシャル提供のための手法について示す図である。
【図１１】他の実施形態による、認証クレデンシャル提供のための手法について示す図である。
【図１２】図２のシステムについての一部の実施形態との関係で、ユーザ及び装置の認証を取り扱うための構造及び手順について示す図である。
【図１３】図２のシステムで認証プロセスのために一回用（シングルユース）鍵が生成されるプロセスについて示す図である。
【図１４】図２のシステムのユーザ装置にて利用されるホワイトボックス暗号化手法についての概略図である。
【図１５】図２のシステムの他の実施形態による、ユーザ及び装置の認証プロセスの概要について示す図である。

【図１６】図１５のプロセスの初期的段階の詳細について示す図である。
【図１７】図１５のプロセスの装置認証プロセス段階に関連するプロセス段階について示すフローチャートである。
【図１８】図１５のプロセスの一部としてセッション鍵の生成及び配布との関連で中央サーバにて行われるプロセス段階について示すフローチャートである。
【図１９】図１５のプロセスのユーザ認証プロセス段階に関連するプロセス段階について示すフローチャートである。
【図２０】図２のシステムのユーザ装置にて提供される暗号化データベースに関して行われる操作について示す図である。
【図２１】一部の実施形態による、図２０の暗号化データベースの例示的内容について示す図である。
【図２２】図２のシステムのユーザ装置にてホワイトボックス暗号化機能を初期化するためのプロセスについて示すフローチャートである。
【図２３】図２のシステムのユーザ登録プロセスについて示す図である。
【図２４】図２のシステムのユーザ装置に支払機能をインストールするプロセスについて示す図である。
【図２５】図２のシステムのユーザ装置での支払アプリケーションの初期化との関連でウォレットサーバにて行われるプロセス段階について示すフローチャートである。
【図２６】図２５にて参照される支払アプリケーションの初期化との関連でユーザ装置にて行われるプロセス段階について示すフローチャートである。
【図２７】図２５にて参照される支払アプリケーションの初期化との関連でウォレットサーバにて行われる更なるプロセス段階について示すフローチャートである。
【発明を実施するための形態】
【００１１】
一般論として、また、本発明の実施形態の諸概念についての紹介として述べるに、ウォレットアクセス／支払トランザクションのための２要素認証機構を提供する。２つの認証要素には次のものが含まれ得る：（ａ）スマートフォンやパソコン（ＰＣ）等のユーザ装置のユーザに知られており該ユーザによって入力される秘密のＰＩＮ；及び（ｂ）ユーザ装置内において保護された態様でセキュアに格納されている装置特有な暗号鍵。第２の認証要素（「あなたが有する何か」）は、ソフトウェアセキュリティ手法のみで実装することができ、また、ユーザ装置内にハードウェア型セキュア要素を含めずに実装することができ、また、ユーザ装置内にトラステッド実行環境をインストールせずに実装することができる。また、ウォレットアクセス／支払トランザクション実行中に、ユーザがユーザ装置以外の装置を所持したり操作したりすることは必要とされない。
【００１２】
一部の実施形態では、装置特有の鍵は、ユーザ装置の支払機能の初期化中にユーザ装置内で実装される暗号関数内にエンコードされていることができる。ホワイトボックス暗号化手法（white box cryptographic technique）を利用してユーザ装置内の秘密鍵について適切な水準のセキュリティを提供することができる。秘密鍵は、支払トランザクション中に、ユーザ装置とウォレットサーバとの間での暗号化データ通信の交換のための輸送鍵（transport key）として利用されることができ、主として一回用認証鍵（SUK_AU、Single Use Key for Authentication）のインポートのために用いられる。
【００１３】
一部の実施形態では、ウォレットサーバからユーザ装置へ向かって、毎回のトランザクションに際して、次のトランザクションで使用するためのユーザ装置内にて格納する暗号化された一回用鍵を、供することができ、これによって強化されたセキュリティを提供することができる。したがって、格納された一回用鍵は、ソフトウェアだけで実装された「あなたが有する何か」型の認証要素による強化されたセキュリティレベルをユーザ装置内にて提供する。
【００１４】

１つの強化セキュリティ体制においては、各支払トランザクションは装置認証フェーズとユーザ認証フェーズとを含む。装置認証フェーズは、先行トランザクションからのセッション鍵について行うユーザ装置からウォレットサーバへと向かっての暗号的に隠蔽された提示行為、及び、ウォレットサービスによるセッション鍵の検証行為を含む。ユーザ認証フェーズは、次のトランザクションのための装置認証セッション鍵についてのウォレットサーバからユーザ装置へと向かってなされる提供行為、及び、現在のトランザクションのためのユーザ認証セッション鍵の提供行為を含む。ユーザ認証フェーズはユーザによる秘密ＰＩＮの入力をさらに含み、該ＰＩＮはユーザ認証のためのセッション鍵を抽出するためにユーザ装置内で使用される。ユーザ認証フェーズは暗号的に隠蔽された形式でのデータ提出行為をさらに含むことができ、該提出行為はユーザ装置からウォレットサーバへと向かってなされるのでありまたウォレットサーバによる検証のためになされる。

【００１５】

本開示にて説明した認証手法は、支払トランザクションに際しての簡単で便利なユーザエクスピリエンスを提供することができる。さらに、これらの手法は、トランザクション及びクレデンシャルについてのセキュリティ関連の厳格な規制上の要件の遵守を実現し得る。また、本開示にて説明する様々な手法は費用／資源消費 対 提供セキュリティ度合いに関して有利なバランシングをもたらし得るのであり、また、説明する他の手法は費用効果的でありつつ支払インフラに対しての相当に洗練された攻撃に対しても保護を提供し得るものである。本開示にて説明した手法の他の利点の１つとしては、複雑又は困難となり得る装置製造者及びモバイルネットワークオペレータ（ＭＮＯ）との提携やこれら主体の関与を回避しつつ、ユーザ装置へソフトウェアを配布するための商業的に利用可能な販路を活用できることが挙げられる。

【００１６】

背景として、従来型支払システムについて先ず簡単に説明する。図１は従来型支払システム１００についてのブロック図である。

【００１７】

システム１００は、従来型の支払カード／装置１０２を含む。当業者には自明であるように、支払カード／装置１０２は、例えば磁気ストライプカード、ＩＣ（集積回路）カード、fob、支払可能スマートフォン等であることができる。

【００１８】

システム１００は、ＰＯＳ端末１０６と関連付けられた読み出しコンポーネント１０４をさらに含む。読み出しコンポーネント１０４は、（支払カード／装置１０２の種類に応じて）何らかの既知の態様で、支払カード／装置１０２から支払口座番号及びその他の情報を読み取ることができる。

【００１９】

読み出しコンポーネント１０４及びＰＯＳ端末１０６は、小売店の敷地内に配置されていることができ、小売業者の店員（即ち、商人）によって小売トランザクションの処理のために運用されることができる。図１においては、支払カード／装置１０２が、そのようなトランザクションの実行のために、読み出しコンポーネント１０４及びＰＯＳ端末１０６と相互作用している様子が示されている。

【００２０】

図１のシステム１００の一部として、アクワイアラ（acquirer、即ち取得側金融機関等）によって運用されるコンピュータ１０８が示されている。アクワイアラコンピュータ１０８は、従来的な態様で作動して、トランザクションについてのＰＯＳ端末１０６からの承認リクエスト（authorization request）を受信することができる。アクワイアラコンピュータ１０８は、承認リクエストを、支払ネットワーク１１０を介して、支払カード／装置１０２と関連付けられている支払カード口座のイシュア（issuer、カード発行会社）によって運用されるサーバコンピュータ１１２へと、ルーティングすることができる。また、よく知られているように、支払カードイシュアサーバコンピュータ１１２によって生成された承認応答は、支払ネットワーク１１０及びアクワイアラコンピュータ１０８を介

してＰＯＳ端末１０６へと戻るようにルーティングされることができる。
【００２１】
支払ネットワークとしてよく知られたものの１例が「Banknet」（登録商標）システムであり、これは本件譲受人たるMasterCard International Incorporatedによって運営されている。
【００２２】
支払カードイシュアサーバコンピュータ１１２は、個々のユーザに対して支払口座を発行する金融機関（ＦＩ、financial institution）によって又は該機関の代理として、運用されていることができる。例えば、支払カードイシュアサーバコンピュータ１１２は次のような機能を実行することができる：（ａ）ＦＩによって発行された支払口座に課金すべき支払口座トランザクションについての承認リクエストを受信し及びこれに応答すること；並びに（ｂ）トランザクションについて追跡と格納を行うこと及び口座記録を維持すること。
【００２３】
図１に示すシステム１００のコンポーネントは、単一のトランザクションを処理するために必要なものだけを含んでいる。典型的な支払システムは（同時的になされるトランザクションを含めて）多数の購入トランザクションを処理することができ、またシステムは、相当な数の支払口座イシュア及びそれらのコンピュータと、相当な数のアクワイアラとそれらのコンピュータと、無数の商人及びそれらのＰＯＳ端末及び関連付けられている近接読み取りコンポーネントとを含むことができる。システムは非常に多数の支払口座保有者を含んでいることができ、これら保有者は支払トランザクションを開始するための支払カード又は他の装置を携帯しており、これらトランザクションの開始は対応づけられた支払口座番号をＰＯＳ端末の読み取りコンポーネントに提示することによってなされる。
【００２４】
上述の支払システム１００についての概要では、例示的に示されたトランザクションは店舗内（in-store）購入トランザクションであった。しかし、当業者及び消費者が良く知っているように、多くの支払口座トランザクションはオンラインショッピングトランザクション等の電子商取引トランザクションとの関連で行われる。これらのトランザクションに関しては、商人の役割を電子商取引サーバコンピュータ（不図示）によって代替することができ、該サーバコンピュータが図１のコンポーネント１０４，１０６を代替することができる。したがって、電子商取引サーバが、従来型の図１にて言及されたトランザクション承認リクエストメッセージ（transaction authorization request message）を発することができる。また、ショッピングウェブページとの対話をする為に、スマートフォン等のモバイルブラウザが実行される装置又はパソコン、ラップトップコンピュータ若しくはタブレット等の装置を、ユーザが操作することを、トランザクションが伴う場合があり、該ウェブページは上述の商人の電子商取引サーバ上にホスティングされている。直前のセンテンスにおいて参照されたユーザ装置の諸タイプは、図１の符号１０２の箇所について実質的な代役たり得る。
【００２５】
図２は、本発明の諸側面に基づいてもたらされる支払システム２００についてのブロック図である。（図１の場合と同様に、単一のトランザクションを処理するために必要なコンポーネントだけを含んでいる場合の支払システムが図２に図示されており、実際においてはそして後述のように、支払システム２００は少なくとも幾つかのコンポーネントについて遙かに多い個数のインスタンスを含んでいることができる。）
【００２６】
図１と同様に、図２は上述したような支払ネットワーク１１０とイシュアサーバコンピュータ１１２とを含んでいる。一部の実施形態では、これら２つのシステムコンポーネントは大体において従来的態様で動作することができ、支払口座システムトランザクション承認リクエスト（payment account system transaction authorization request）及びトランザクション承認応答（transaction authorization response）を受信及びルーティン

グすることができる。

【００２７】

図示の簡潔性のために、支払システム２００の商人及びアクワイアラの諸観点は単一のブロック２０２によって表されている。商人／アクワイアラブロック２０２（即ち、商人又はアクワイアラ又はこれらのどちらかのためにサービス提供者によって運用されている装置）は、ウォレットスイッチ２０４と通信可能なものとして表されている。顧客がＷＳＰにアクセスしてトランザクションのための支払を提供したいと商人に対して知らせた場合、ウォレットスイッチ２０４は、商人／アクワイアラブロック２０２から通信を受信することができる。実効的には、ウォレットスイッチ２０４は、商人から発せられるトランザクション詳細事項をウォレットサーバ２０６へと中継することによってウォレットサーバ２０６をトランザクションに参加させることができる。ウォレットサーバ２０６の詳細は後述する。ウォレットサーバ２０６が提供する主要な働きには、支払システム２００の多数のユーザのためにデジタルウォレット２０８を格納すること及び図２のブロック２１０に示されているユーザ及び装置認証サービスの提供機能が含まれる。後者の機能は、本願開示の教示事項に従って提供されることができ、また、重要な側面に関して従来提案されてきた認証慣行から逸脱することができる。また、コンポーネント２０２は、ウォレットサーバとして機能することができることに加えて、遠隔認証サーバとしても機能することができることに留意されたい。

【００２８】

トランザクションに関しての認証は、ウォレットサーバ２０６／認証機能２１０と、商人と購入トランザクションを行うユーザによって操作されるユーザ／支払装置（参照符号２１２）との間で行われる処理を介して、なされることができる。図２ではユーザ／支払装置２１２はスマートフォン等のモバイル装置として図示されているが、例えば他の場合においては、ユーザ／支払装置２１２は、現在のトランザクションのためにブラウザプログラムを介して電子商取引サイトにアクセスするために用いられているパソコン、ラップトップコンピュータ、タブレットコンピュータ等であることができる。ユーザ装置２１２についての非スマートフォン型の事例は破線でブロック２１４として図示されており、一部の事例においては明示的に図中に示されているユーザ装置２１２を代替することができる。図２に示す特定の例においては、ユーザ装置２１２は、モバイル認証アプリ（アプリケーションプログラム）２１６を介してウォレットサーバ２１２と相互作用２１５を行っているものとして示されている。

【００２９】

ウォレットサーバ２０６とユーザ装置２１２との間の相互作用２１５には、ウォレットサーバ２０６内に格納されたユーザのデジタルウォレットからの口座についての認証及び選定が、含まれることができる。認証は、装置認証及びユーザ認証を含むことができ、また、後述のように、相当な厳密性又は極め高度な厳密性を伴って運用される２要素認証機構を伴って実装されることができる。

【００３０】

図２において接続２１８によって概略的に図示されているように、モバイルアプリ２１６は、オンライン購買「バスケット」（買い物籠）についての支払段階が完了し得ることを商人／アクワイアラ２０２に対して効果的に知らせることができるのであり、バスケット合計がユーザに知られている場合には、モバイルアプリ２１６は、現在のトランザクションについて特定のウォレットのブランドを選好支払方法としてユーザが選定したことを指示することもできる。

【００３１】

システム２００の実際的な実施形態に含まれる、図２に示す各コンポーネントの実際の個数は、１を超えることができることに留意されたい。例えば、システムに参加する商人が多数存在することができ、また、トランザクション認証をなすようにプログラムされているユーザ装置や他のユーザ／支払装置を操作している個人がさらに多く存在することができる。相当数のアクワイアラ及びイシュアが存在することができ、幾つかのウォレット

サーバが存在していることがあり、潜在的には１つより多くの支払ネットワークが存在することができる。従来型の支払システム１００についての上記の記述から分かるように、図２に示す支払システム２００は、同時的なトランザクションを含めて多数のトランザクションを処理することができる。

【００３２】

支払システム２００の典型的な構成においては、ウォレットサーバ２０６は商人及びユーザ装置２１２の双方との関係で遠隔に配置されている。

【００３３】

図３は、図２に示されており本発明の諸観点に基づくウォレットサーバ２０６についての例示的実施形態を示すブロック図である。

【００３４】

図３を参照するに、ウォレットサーバ２０６は、ハードウェアの観点からは従来的であることが可能であるが、ソフトウェアによって制御されて本明細書にて説明するように機能するように構成されていることができる。例えば、ウォレットサーバ２０６はサーバコンピュータ用ハードウェアで構成されていることができる。

【００３５】

ウォレットサーバ２０６は、通信装置３０１、記憶装置３０４、入力装置３０６及び出力装置３０８と連携動作可能に接続されたコンピュータプロセッサ３００を含むことができる。

【００３６】

コンピュータプロセッサ３００は、１以上の従来的プロセッサによって構成されていることができる。プロセッサ３００はその動作に際して、以下において説明されるプログラム命令に含まれたプロセッサによって実行可能な諸ステップを実行するのであり、これによってウォレットサーバ２０６を制御して所望の機能を提供する。

【００３７】

通信装置３０１は、例えば（ウォレットスイッチ２０４やユーザ装置２１２等の）他の装置との通信を促進するために用いることができる。例えば、通信装置３０１は、次のような通信を促進するための種々の通信ポート及びインターフェースを含むことができる：（ｉ）支払システム２００の数多くのユーザによって操作されるユーザ装置たるモバイル装置との間でなされる１以上のモバイル通信ネットワーク（不図示）を介した無線通信；及び／又は（ｉｉ）インターネットを介したＰＣ等との通信。

【００３８】

入力装置３０６は、コンピュータ内へとデータを入力するために典型的に用いられる任意のタイプの周辺機器を１以上備えることができる。例えば、入力装置３０６は、キーボード及びマウスを含むことができる。出力装置３０８は、例えばディスプレイ及び／又はプリンタを備えることができる。

【００３９】

記憶装置３０４は、任意の適切な情報記憶装置を備えることができ、これには次の装置の組合せが含まれる：磁気記憶装置（例えば、ハードディスクドライブ）、例えばＣＣＤ及び／若しくはＤＶＤ等の光学記憶装置、並びに／又はランダムアクセスメモリ（ＲＡＭ）や読み出し専用メモリ（ＲＯＭ）や所謂フラッシュメモリ等の半導体メモリ装置。このような情報記憶装置の１以上は、コンピュータ可読記憶媒体又はコンピュータ使用可能媒体若しくはメモリであるものとみなされることができる。

【００４０】

記憶装置３０４は、プロセッサ３００を制御するための１以上のプログラムを記憶している。プログラムは（コンピュータ可読プログラムコード手段とも称される）プログラム命令を含んでおり、該命令はプロセッサ３００によって実行されるウォレットサーバ２０６のプロセッサ実行可能処理ステップを含んでおり、該ステップはウォレットサーバ２０６に本明細書で説明する機能を行わせるものである。

【００４１】

プログラムは、プロセッサ３００を制御する１以上の従来的オペレーティングシステム（不図示）を含むことができ、これによってウォレットサーバ２０６内での活動及びリソース共有を管理し及び調和させて、ウォレットサーバ２０６上で実行されるアプリケーションプログラム（後述）のためのホストとして稼働することができる。

【００４２】

記憶装置３０４によって記憶されているプログラムには、例えばユーザ登録アプリケーションプログラム３１０が含まれていることができる。ユーザ登録アプリケーションプログラム３１０は、プロセッサ３００を制御して、ウォレットサーバ２０６がユーザからの要求を捌けるようにして、ウォレットサーバ２０６によって提供されるウォレットサービスに登録できるようにすることができる。例えば、これには少なくとも次の動作が含まれることができる：ウォレットサーバ２０６上にユーザ口座を開設することと；ユーザの支払口座の幾つかをウォレットサーバ２０６上でユーザに提供されるためのデジタルウォレットに編入すること。ユーザの支払カード口座の登録は、少なくとも一部の場合においては、問題となる支払カード口座を識別するプライマリ口座番号（ＰＡＮ、primary account number）を介してなされるか、及び／又は、２０１３年にMasterCard International Incorporated、Visa及びAmerican Expressによって公表された「Payment Token Interoperability Standard」（支払トークン相互運用基準）において言及されるタイプの支払トークンを介してなされることができる。

【００４３】

ユーザのデジタルウォレットを確立するための、ユーザとウォレットサーバ２０６との相互作用は、例えば、ウォレットサーバ２０６によってホスティングされたウェブサイトへのアクセスを介してなされることができる。

【００４４】

また、記憶装置３０４は、次の動作をウォレットサーバ２０６にさせるようにプロセッサ３００を制御するウォレットメンテナンスアプリケーションプログラム３１２をも記憶していることができる：ウォレットサーバ２０６内にユーザ達によって確立されたデジタルウォレットを格納及び維持すること。

【００４５】

また、記憶装置３０４は、次の動作をウォレットサーバ２０６にさせるために必要なプログラム命令３１４を記憶していることができる：本明細書にて詳述されるような態様で遠隔認証サーバとして稼働すること。

【００４６】

また、記憶装置３０４は、支払トランザクション取り扱いプログラム３１６をも記憶していることができ、該プログラムはプロセッサ３００を制御してウォレットサーバ２０６がウォレットスイッチ２０４からウォレットサーバ２０６へと差し向けられた多数のトランザクションについてウォレット口座選定を行うことができるようにするものである。一部の実施形態では、プログラム３１４，３１６の機能は、単一のプログラムに併合されるか、又は、関連するプログラム間の協調を包括することができる。

【００４７】

また、記憶装置３０４は不図示の他のプログラムをも記憶することができ、また、ウォレットサーバ２０６は不図示の他のプログラムをも実行することができる。例えば、これらのプログラムには報告アプリケーションが含まれることができ、該アプリケーションはウォレットサーバ２０６によって行われた活動についての報告を求めるシステム管理者からの要求に応答することができる。他のプログラムには１以上の次のようなものも含まれ得る：データ通信プログラム、ウェブサイトホスティングプログラム、データベース管理プログラム、デバイスドライバ等。

【００４８】

また、記憶装置３０４は、ウォレットサーバ２０６の稼働に必要な１以上のデータベース３１８を記憶していることができる。このようなデータベースは、例えば、ユーザ／カード保持者のためにウォレットサーバ２０６内にて維持されるデジタルウォレット及び関

連する支払口座情報に対応するデータを格納するための（図３において別個に図示はされていない）データベースを含むことができる。ウォレットサーバ２０６は、自己の認証機能との関係で、後述のように、１以上の他の（図３において符号３１８としてしか示されていない）データベースを活用することができるのであり、例えば認証目的のためのユーザデータベースや認証目的のための装置データベースがそれである。

【００４９】

上述のように、スマートフォン、パソコン、ラップトップコンピュータ、タブレットコンピュータ等を含むインターネット接続を有する様々な異なるタイプの装置を、ウォレットベースド（ウォレットを基礎とした）支払トランザクションにおいてユーザ／支払装置として活用することができる。多くの場合において、スマートフォン等のモバイル装置をそのような役割で用いることができるということからして、そのような装置の諸観点について示すことが有益なのであり、図４にてこれが示されている。

【００５０】

図４は、図２の支払システム２００でなされる支払／ウォレットアクセストランザクションとの関連で用いられ得るモバイル装置（本図に関しては、参照符号４００が付与されている）についての実施形態についてのブロック図である。

【００５１】

１つの例示的実施形態では、モバイル装置４００はハードウェアの観点において及びソフトウェアの観点の殆どにおいて典型的なスマートフォンであることができるも、本明細書にて説明されているように例えば商人側装置及びウォレットサーバ２０６と相互作用できるようにするために当該モバイル装置４００は適切にプログラミングされていることができる。端的には、モバイル装置４００は、商人側装置に対して自己についての識別事項を提示し、また、ウォレットサーバ２０６との関係で次の動作を行うことができる：装置認証、ユーザ認証、ウォレットデータの受領及びウォレット口座についての選定。これらの動作の詳細については後述するが、モバイル機器４００の重要な側面についての概要に関してはこれから述べる。

【００５２】

モバイル機器４００はハウジング４０２を含むことができる。多くの実施形態では、ハウジングの前面の主要部はタッチスクリーンで構成されており、これがモバイル機器４００のユーザインターフェース４０４の主要要素である。

【００５３】

モバイル機器４００は、従来的なモバイルプロセッサ／制御回路４０６をさらに含んでおり、これらはハウジング内に格納されている。また、モバイル機器４００内には記憶／メモリ装置が１つ又は複数含まれている（参照符号４０８）。記憶／メモリ装置はプロセッサ／制御回路４０６と通信可能であり、また、プロセッサ／制御回路４０６を制御してモバイル機器４００の様々な機能を管理及び実行するためのプログラム命令を含んでいることができる。周知のように、このような機能には、携帯電話ネットワーク（不図示）との相互作用を介してなされる携帯型音声通信装置としての運用が含まれる。さらなる従来的機能としては、モバイルデータ通信装置としての運用が含まれ、さらには幾つかのアプリケーションプログラム（「アプリ」とも称する）によるプログラミングによるポケットに収まる程の大きさのパソコンとしての実質的運用も含まれる。（アプリは図４ではブロック４１０として表されており、運用においてはブロック４０８内に格納されていることができ、種々の態様でプロセッサ／制御回路４０６をプログラミングすることができる。）上述のモバイル通信機能はブロック４１２として表されており、プログラミングされた制御機能に加えて、これらのモバイル通信機能はアンテナ、トランシーバ回路、マイクロフォン、拡声器等の（不図示の）ハードウェア機能に依存している。

【００５４】

図４のブロック４１４は、モバイル機器４００が支払システム２００に参加するための機能を表しており、該参加の態様については後述する。これにはウォレットアプリ（支払アプリ又は支払アプリケーションとも称する。）の関与がある場合があり、該アプリは本

願開示の教示事項において示された機能に即する機能を有していることができる。また、後述から分かるように、支払機能４１４は記憶部／メモリ４０８を管理することができ、モバイル機器４００内に１以上の特化したデータベース（図４においては別個には図示されていない）をもたらすことを可能とし得る。

【００５５】

上述から次のことが分かるであろう：即ち、モバイル機器４００のコンポーネントとして図４にて表されたブロックは実質的に互いに重複し得るものであり、及び／又は、ブロック間には図示はされていない機能的な連関があり得る、ということ。

【００５６】

モバイル機器４００はスマートフォンとして体現され得ると述べられているも、該仮定は限定的なものとしては意図されておらず、モバイル機器４００は少なくとも一部の場合においては代替的には、モバイル通信機能を持たされたタブレットコンピュータとして又は他のタイプのモバイルコンピューティング装置として構成され得る。上述のように、本発明の諸観点に即して他のタイプのモバイルコンピューティング装置をユーザ装置として活用することができる。

【００５７】

図５は、図２のシステムの一部の実施形態における認証機能の実装例について概略的に示す図である。

【００５８】

本発明の諸観点によれば、ユーザ装置２１２，２１４（実際にはそれらは内なるソフトウエアエンティティを伴っている）とウォレットサーバ２０６の認証／検証機能５１２（図５）との間で強力な認証方法が提供される。一部の観点においては、図５に提示されるアーキテクチャは、本件譲受人たるMasterCard International Incorporatedによって制定されたＤＳＲＰ（Digital Secure Remote Payment、デジタルセキュア遠隔支払）システムのモデルに準拠することができる。開示する認証方法は、電子商取引支払トランザクションに関して（例えば、ヨーロッパ中央銀行（ＥＣＢ）体制等の）規制体制との関連での完全遵守をもたらし得るのであり、同時に、少なくとも毎回のトランザクションに関してＩＣ支払カードや個人カードリーダ（ＰＣＲ、personal card reader）等のハードウェア要素を伴わずにしてユーザに便利且つ簡単なエクスピリエンスを提供することができる。代わりに、一部の実施形態では、特定のカード／支払口座を自身のデジタルウォレットに追加するという局面のみにおいて、自身のＩＣ支払カード及びＰＣＲを使用することがユーザに義務づけられる（これは、例えば、資金洗浄防止／テロ資金対策（ＡＭＬ／ＣＴＦ、Anti-Money Laundering/Counter Terrorism Funding）関連のＥＣＢ要求を満たすためのものたり得る。）。他の実施形態では、デジタルウォレットに支払口座を編入する場合やウォレットトランザクションを行う場合との関連で、ＩＣ支払カード及び／又はＰＣＲを使用することをユーザに義務づけない場合もある。開示される認証方法は、既に提案されてきた他のユーザ認証方法が伴うような複雑なインフラへの依存を回避することができる。

【００５９】

図５に示したアーキテクチャの１つの特徴としては、ユーザに便利な態様での強力なユーザ認証の提供が挙げられ、即ち購買エクスピリエンスがもたらされた際のチャンネルと同一のチャンネルでこれを提供し得る。例えば、モバイル機器２１２内のモバイルウォレットアプリ５０２を介して「inApp inChannel」型認証を提供することができ、あるいは、ユーザ装置がパソコン２１４等である場合には、inApp inChannel型認証はパソコン２１４上で実行されるオペレーティングシステムと互換性を有するアプリケーションプログラムを介して提供されることができる。５０４で表されるように、モバイルウォレットアプリ５０２は本願開示の教示事項による認証機能５０４を組み込むことができ、モバイル機器２１２内にて「ソフトウェアオンリー」な認証トークンを実装することができる。

【００６０】

代替的には、本発明の諸観点によれば、モバイル機器２１２又はパソコン２１４内にお

いて「inBrowser inChannel」型認証機能を提供することができ、例えばブラウザ拡張５０６又はブラウザ（例えば、パソコンブラウザ５０８又はモバイルブラウザ５１０）内にて実行されているウェブページを介して提供がなされ得る。

【００６１】

また、認証機能５０４／ブラウザ拡張５０６のどちらかがウォレットサーバ２０６の認証／検証機能５１２と相互作用しているものとして表されており、該サーバはウォレットサービスを提供するに際して慣例となっている「登載済みカード」（ＣｏＦ、card on file）機能５１４をも組み込んでいることができる。

【００６２】

ソフトウェアオンリーな認証トークンを用いることによって、さもなければ生じていたであろう次の側面における潜在的な不便さ又は困難性を回避し得る：（ａ）ＭＮＯによって提供されたＳＩＭカード上に認証トークンをホスティングすること（即ち、ＭＮＯの協力を取り付けることを要さないということ。）；（ｂ）支払セキュリティ目的で専用のハードウェアセキュア要素（ＳＥ、secure element）を提供すること（即ち、機材製造者の協力を得る必要性が減るか無くなるということ。）；又は（ｃ）装置内に信頼済み実行環境（ＴＥＥ、Trusted Execution Environment）回路の組み込み（即ち、機材製造者の協力を得る必要性が減るか無くなるということ。）

【００６３】

ソフトウェアオンリーな認証トークンの実装を支援するために「不正耐性」特性を付与するために用いることのできる手法は、例えば図６に示されている静的な又は動的なホワイトボックス暗号（ＷＢＣ、white box cryptography）の両者を用いることができる（該図の上部６０２が静的ＷＢＣを表し、下部６０４が動的ＷＢＣを表している。）。

【００６４】

静的ＷＢＣ実装例（６０２の部分）では、秘密鍵Ｋは固定されているがブロック暗号構造内にエンコードされており、攻撃者によって逆算できないようになっている。当該鍵は、ウォレットアプリのコンパイル時に、ウォレットアプリの実装の一体的な部分と化する。

【００６５】

図６の下部６０４は動的ホワイトボックス（ＤＷＢ、Dynamic White Box）の実装例を示しており、鍵Ｋはウォレットアプリの呼び出し毎に変化することができる。このような実装では、動的鍵Ｋはパラメータとして渡されるが、保護されていない環境へと送信される前にセキュアな態様に先ず変換される。可能な変換タイプには以下のものが含まれる：

【００６６】

・　キーイングされていないｔ変換ｏ（Ｋ）。このタイプではセキュリティは変換の秘匿性に依存しており、ｏ（Ｋ）は難読化関数（obfuscation function）と見なされることができる。これは、秘密のエンコーディング／デコーディングテーブルを有する難読化変換として実装されることができる。したがって、o^{-1}（Ｋ）は、非セキュアな環境を経た後に宛先においてセッション鍵の復元を可能とする逆難読化変換である。

【００６７】

・　汎用的な暗号化／復号化アルゴリズムｅＲ（Ｋ）を伴う暗号化。生成された実装例では鍵Ｒが用いられるのであり、該鍵はユーザ／モバイル機器のそれぞれについて固有なものであり、該鍵は動的鍵Ｋの生成後にそれを暗号化するために用いられるのであり、該鍵はそれを内部的に復号して暗号化アルゴリズムＥによって使用されるべきＤＷＢ（Ｅ）プリミティブを得るために用いられるのである。

【００６８】

（例えば、「アプリストア」等からの）各ユーザ装置へ向かっての頒布時においては、各装置内のＷＢＣ構造についてはコーディングが同じであることができるが、後においては、各ユーザに特有なセッショントランスポート鍵（session transport key）を用いて個々のユーザ装置のＷＢＣ構造を初期化することができる。したがって、ＷＢＣ構造と特有化されたＷＢＣが実行されているハードウェア／ソフトウェアプラットフォームとがな

す組合せが、「あなたが有する何か」（即ち、認証要素に対しての所有）と同視されることができる。

【００６９】

認証トークンの不正耐性を支援するために用いられ得る別の手法は、後述の図８に示すプロビジョニングアプローチに基づいていることができ、ホワイトボックス暗号手法によって構築されることができる。先ず図７を参照するのであり、同図は典型的なプロビジョニングアプローチを表しており、ここでは（７０２にて示されているように）パラメータ／鍵が認証前に１回プロビジョニングされるのであり、鍵は格納されて多数回使用されるのであり、鍵はハードウェアの不正耐性を有している認証トークン７０４内に格納される。格納されたパラメータの後程における複数回の使用は、図７においては符号７０６で表されている。

【００７０】

対照的に、本願開示の教示事項によれば、そして図８に示されている事項によれば、認証用の秘密パラメータ／認証鍵は「クラウド」内でウォレットサーバ認証サービス機能によって新規に生成されるのであり、図８の８０２で示されているようにこれらは認証自体が行われるのに先んじて各セッションにおいて提供される。また、秘密パラメータ／認証鍵はＰＩＮ又はパスワードによって保護されていることができ、これによって第２の認証要素たる「知識」型／「あなたが知っている何か」型の認証要素が提供される。

【００７１】

さらに、一部の実施形態では、セッション認証鍵が実行環境内で平文のまま開示されることは絶対になされない。むしろ、セッション鍵は、動的ホワイトボックス暗号プリミティブ内でそれをウォレットアプリ内で用いている認証機能と一緒にサンドボックス化される。

【００７２】

一部の規制上の要求又はセキュリティ目標を達成するためには、ウォレットサーバ内のデジタルウォレットにカード／支払口座を追加する操作の段階においては、別個のユーザ認証インフラを用いることが望ましい場合があり、追加後に関しては、当該口座データを用いるトランザクションとの関係では、そのような別個のユーザ認証インフラを用いることが必要なくなる場合がある。

【００７３】

図９は、図２のシステム内で認証手順を実施するためのアーキテクチャの概要を示す図である。このアーキテクチャは、サーバベースド（サーバを基礎とした）ＤＳＲＰモデルで強力なユーザ認証サービスを提供するために望ましいものであり得るのであり、上述において望ましい目標として言及されているようなソフトウェアだけで実装された２要素認証を組み込んだものである。図９の機構は、パソコンやタブレットコンピュータやスマートフォン等の非セキュアなメモリ内においてホスティングされ得るソフトウェアオンリーな環境として実装されることができる。図９の要素については後述するのであり、説明はＯＡＴＨ（Initiative for Open Authentication）フレームワークに従ってなされる。

【００７４】

図９を参照するに、認証トークン（参照符号９０２）は、動的ＷＢＣで作成されたソフトウェア型不正耐性環境内の暗号学的に耐性を有しているワンウェイ関数（ＯＷＦ、One Way Function）９０４を伴って実装され得る。認証方法（９０６）は、クライアントアプリケーション９１０とのチャレンジ／応答プロトコル９０８を伴って実装されることができる。クライアントアプリケーション９１０は、認証トークン９０２内のＯＷＦ９０４とウォレットサーバ２０６内の認証検証サーバ機能９１２との間の透過的プロキシとされることができる。クライアントアプリケーション９１０は、例えば次のようなものとして実装されることができる：モバイルウォレットアプリ、従来的なパソコンオペレーティングシステムと互換なパソコンタイプのアプリケーション、ブラウザ拡張、又はパソコン／タブレット／モバイルブラウザに提供されるＨＴＭＬ５型のウェブページ。

【００７５】

トークンインターフェース（参照符号９１４）は、例えばＥＭＶプロトコル（及びそのＡＰＤＵ（アプリケーションプロトコルデータユニット））をエミュレートするプロプライエタリなＡＰＩ（アプリケーションプログラミングインターフェース）（参照符号９１６）であることができ、又は、代替的には、認証方法９０６を実施可能な他の任意のＡＰＩであることができる。

【００７６】

ウェブサービスはウォレットサーバ２０６を介して実装されることができ、ユーザに対して顧客データベース９１８内の自己のチェックアウトデータ／登載済みカード（ＣｏＦ）を提供することができ、これは認証検証サーバ機能９１２によって適正な認証がなされた後になされるのであり、これに際しては該サーバ機能９１２が認証トークン９０２からサーバ機能９１２へと伝達された「認証符号」（即ちデータエンティティ）を検証しているものとする。

【００７７】

図９のアーキテクチャ内のプロビジョニング及び管理サービスは、ウォレットサーバ２０６と関連付けられたトークン管理エンティティを含むことができる。トークン管理エンティティは、システムに登録されている各認証トークン９０２について、認証のための固有なトークンマスター鍵（ＴＭＫ＿ＡＵ、token master key for authentication）を生成して格納することができる。プロビジョニング及び管理サービスは、トークンクレデンシャルエンティティ９２２をさらに含むことができ、該エンティティは各認証セッションに際してトークンマスター鍵ＴＭＫ＿ＡＵから新たな認証用のセッション鍵ＳＫ＿ＡＵ（session key for authentication）を導出する。

【００７８】

後述の記載においては、認証トークン９０２及び認証方法９０６を実施するための機構として２以上の具体的機構について述べる。

【００７９】

本願開示の教示事項による比較的に単純なユーザ認証モデルは、図１０に示されている。図１０のモデルは、ユーザ認証のための鍵及び／又は他のパラメータのプロビジョニング（参照符号１００２）並びにユーザ認証それ自体（参照符号１００４）を含む。このモデルの説明には、後述の図１２～１４についての説明が伴う。

【００８０】

本願開示の他の態様による強化されたセキュリティ機能を有する認証モデルは、図１１に示されている。図１１のモデルは、ユーザなりすまし、装置なりすまし、強化暗号化等の広範な攻撃手法に対して保護をもたらすことができる。後者のモデルは、ユーザ認証のための鍵をプロビジョニング（参照符号１１０２）することと、次のユーザ認証セッションにて装置認証のための鍵をさらにプロビジョニング（参照符号１１０４）することと、装置及びユーザの両者について認証（参照符号１１０６）することとを含み、前者の認証は以前のセッションからの鍵を用いるのであり、後者のそれは現在のセッションの鍵を用いる。図１１のモデルの説明には、後述の図１５～１９についての説明が伴う。

【００８１】

図１２は、図１０との関連で若干説明した認証モデルを実施するための、（ソフトウェアベースドな）認証トークン１２０２と認証検証サーバ１２０４との間の相互作用を示す図である。

【００８２】

図１２をなおも参照するに、以下認証トークン１２０２の構造について説明する。

【００８３】

認証トークン１２０２は認証符号生成器を含むことができ、これは暗号学的に耐性を有しているＯＷＦ１２０６の形式を取ることができる。ＯＷＦ１２０６は、認証符号生成器として機能するのであり、ユーザの信頼性を評価するために用いられるべき認証符号（認証検証サーバ１２０４へと提出すべきデータエンティティ）をもたらす。ＯＷＦ／認証符号生成器１２０６は次式に従って認証符号（Authenticator）を計算することができる：

[数１]
Authenticator = OWF[SK_AU, Token Profile](Challenge, Session Data, Token Data)

【００８４】
本願開示の後程で説明するように、ＯＷＦは、数学的関数ｆを用いて実装されることができる。後述のように、関数は、暗号鍵とトークンプロファイルとをもってパラメータ化されることができる。ＯＷＦは、認証データを入力として受け付けて、認証符号をもたらす。認証データの例の詳細は、本願開示の後程の表にて説明されている。一部の実施形態では、認証データは、認証検証サーバによってもたらされた新たなチャレンジ値、及び、クライアントと認証検証サーバとの間で確立された接続から収集されたセッションデータを、常に含んでいる。

【００８５】
前段落で言及されたトークンプロファイルは認証トークンのための個人化データを含むことができ、該データは特定のユーザに特有なものである。この個人化データはトークン識別番号（ＴＩｄＮ、token identification number）を含むことができ、該番号は問題となる認証トークンをウォレットサーバ及び／又はウォレットサーバの運営者の技術的・管理的な境界内で識別するための固有な番号であることができる。

【００８６】
個人化データは失効日をさらに含むことができ、該日付はトークンが認証システム内で有効として扱われなくなる日を特定するものである。

【００８７】
個人化データはトークン属性をさらに含むことができるのであり、該属性は認証トークンが有効とみなされるための具体的な条件を記述し得るものである（例えば、どのタイプの装置で生成されたか、どのタイプのトランザクションに用いられることができるか等）。

【００８８】
一部の実施形態では、２以上の異なるタイプのトークンプロファイルがあることができる。例えば、一方ではトークンプロファイル「ＴＰ－ＭＡ」があり、これは認証トークン機能を伴うモバイルウォレットアプリ（mobile wallet app）に対応し得るのでありＴＩｄＮ１によって表され得るのであり、他方ではトークンプロファイル「ＴＰ－ＢＥ」があり、これは認証トークン機能を伴うブラウザ拡張（browser extension）又はウェブページに対応し得るのでありＴＩｄＮ２によって表され得る。

【００８９】
さらに、認証トークンは鍵コンテナを含むことができ、これは暗号鍵を用いてのＯＷＦのパラメータ化のために用いられることができる。暗号鍵は、図１２においてはＳＫ＿ＡＵ（参照符号１２０８）と呼ばれ、認証セッション鍵（authentication session key）とも呼ばれ得る。

【００９０】
鍵コンテナに（トランザクション毎に多様化させ得る）「カードマスター」鍵を恒久的に格納させる代わりに、新たな認証用一回用鍵（ＳＵＫ＿ＡＵ、single-use key for authentication）を鍵コンテナに提供することができるのであり、該提供動作はウォレットサーバのトークンクレデンシャルサービスによって（図８，１０において概略的に示されている）各ユーザ認証セッションの開始時においてなされる。この手法は、モバイル（ウォレット）アプリ又はブラウザ拡張／ウェブページのソフトウェアオンリーな環境におけるセキュリティの潜在的な欠如への対処態様としては、適切たり得る。

【００９１】
一部の実施形態では、トークンクレデンシャルサービスによってもたらされたＳＵＫ＿ＡＵは、ＯＷＦにて暗号鍵として直接的には用いられず、代わりに、ユーザによってクライアントソフトウェアのＰＩＮパッドソフトウェアエミュレータ部に打鍵入力されたＰＩＮ又はパスワードと組み合わされて、セッション鍵ＳＫ＿ＡＵをもたらし得る。

【００９２】

一部の実施形態では、ＯＷＦは、以下の特性を有し得る。

【００９３】

暗号学的な耐性を有するＯＷＦたるｆは以下の特性を有し得る：

（ａ）ｆの表現が公知であること；

（ｂ）所与の入力ｘに対してｆ（ｘ）を計算するのは容易であるが、ｆの値域内の全ての像ｙについてｙ＝ｆ（ｘ）となるような入力ｘを導出することが計算量的に実現不可能であること（この特性は第１原像耐性（first pre-image resistance）とも呼ばれる。）；

（ｃ）ｆ（ｘ）＝ｆ（ｘ’）且つｘ≠ｘ’である引数があったとしても、ペアたる（ｘ，ｆ（ｘ））についてｆ（ｘ）＝ｆ（ｘ’）となるようなｘ’を発見することは計算量的に実現不可能であること（この特性は第２原像耐性（second pre-image resistance）とも呼ばれる。）；

（ｄ）ｆ（ｘ）＝ｆ（ｘ’）且つｘ≠ｘ’である引数を発見することが計算量的に実現不可能であること（この場合、関数は衝突耐性を有しているという。）。

【００９４】

これらの特性の１以上は、ペアたる（ｘ，ｆ（ｘ））の観測のみできるがｘの選定に関して影響力を及ぼすことができないような外部攻撃者に対する防護としては効果的である傾向が認められ得る。これらの特性の１以上は、後日において自己が実際に認証されたトランザクションの責任を逃れようとする不誠実なユーザのような内部攻撃者に対する防護としては効果的である傾向が認められ得る。

【００９５】

一部の実施形態では、ＯＷＦは、アンキード（un-keyed）関数とするか、又は、対称鍵を有するキード（keyed）関数とするように選択されることができる。

【００９６】

一部の実施形態では、アンキード関数としてのＯＷＦは、以下のように実装されることができる。

【００９７】

関数ｆはアンキード関数として選定されることができるのであり、即ち関数をパラメータ化するのに暗号キーを要しない場合である。ユーザの秘密情報は（それがセッション鍵であるか直接的にパスワードであるかを問わずに）、関数ｆの引数内で直接的に渡されることができるのであり、即ち次式のとおりである。

[数２]

$$\text{Authenticator} = f[SK\_AU](\text{Challenge}, \text{Session Data}) = H(SK\_AU, \text{Challenge}, \text{Session Data}).$$

【００９８】

通常、この分類においては、ハッシュ関数Ｈを選択することができる。エンティティ認証サービスの実装においてハッシュ関数を用いる際の基本的な思想は、任意の長さを持つ属性セットの信頼性をそのハッシュコードの信頼性に転換する、ということである。

【００９９】

アンキードＯＷＦについて例を２つ挙げる：（１）ＯＡＴＨコンソーシアムによって提案されたＨＭＡＣ系ワンタイムパスワード（ＨＯＴＰ、HMAC-Based One-Time Password）アルゴリズム；及び（ｂ）ＳＨＡ－２５６系ハッシュ関数。

【０１００】

一部の実施形態では、秘密対称キード関数としてのＯＷＦを次のように実装することができる。

【０１０１】

関数ｆがメッセージ認証コード（ＭＡＣ、Message Authentication Code）である場合、データの信頼性は、データの出所を保証する秘密鍵（secret key）ＳＫ＿ＡＵの秘密性及び信頼性に依存する。

【０１０２】

秘密対称キード関数の例として頻繁に挙げられるものとしては、広く知られたＥＭＶ支

払トランザクションプロトコルで用いられる関数がある。これは通常アプリケーション暗号（Application Cryptogram）と称され、一般的にはＡＣと略される。

[数３]

Authenticator = AC = MAC[SK_AU](Challenge, Session Data)

【０１０３】

これは、通常セッション鍵（session key）SK_{AC}と称される５６ビットの対称鍵を伴うＤＥＳ系ＭＡＣである。これは、アプリケーションによる、マスター鍵（master key）からの鍵導出の結果であり、MK_{AC}と称される。

【０１０４】

ユーザ装置のクライアントと認証トークンと認証検証サーバとがチャレンジ／応答認証方法に参加して、ユーザ認証サービスを実行することができる。これは、次のようにして行われ得る。

【０１０５】

クライアントは、ユーザをウォレットサーバのユーザデータベース内において一意的に識別するＵｓｅｒ＿ＩＤを、送ることができる。クライアントは、装置データベース内において一意的にユーザの装置を識別するＤｅｖｉｃｅ＿ＩＤを送ることもできるのであり、即ち、これによってユーザによって使用される装置を一意的に識別してウォレットサーバの認証に供する。

【０１０６】

Ｕｓｅｒ＿ＩＤ／Ｔｏｋｅｎ＿ＩＤに基づいて、認証検証サーバは、認証用トークンマスター鍵（ＴＭＫ＿ＡＵ）を検索してそれを用いて認証プロトコルの現在の実行回のためのユーザ認証セッション鍵（ＳＫ＿ＡＵ）を生成する。セッション鍵は、ユーザ装置によって提供された認証符号を検証するために用いられる。

【０１０７】

認証検証サーバは、新たなチャレンジ値を（例えば、ランダムな値又は疑似ランダムに生成された値として）生成し、ユーザ装置のクライアントとの接続上で交換された現在の認証セッションデータを収集する。これらのデータ全てをクライアントへと送るのであり、該クライアントは認証コマンドの要求を発するのであり、これにはチャレンジ及びセッションデータが認証トークンのパラメータとして伴う。

【０１０８】

クライアントはユーザ装置にＰＩＮパッドソフトウェアエミュレータも提供するのであり、ユーザの秘密知識即ちＰＩＮ又はパスワードを入力するようにユーザに対して促す。

【０１０９】

ユーザがＰＩＮ／パスワードを入力した後、同じセッション中にウォレットサーバのトークンクレデンシャルサービスから受信された認証用一回用鍵（ＳＵＫ＿ＡＵ、single-use key for authentication）を復号して、認証符号の生成のために使用されるべき認証セッション鍵（ＳＫ＿ＡＵ、authentication session key）を生成することができる。認証符号は、チャレンジ／応答枠組み内において、認証検証サーバのチャレンジに対しての応答として送信されるべきものとされる。

【０１１０】

認証トークンによって演算／計算された認証符号は、ユーザ装置のクライアントを経て認証検証サーバへと送信される。

【０１１１】

認証検証サーバは以前に導出されたセッション鍵ＳＫ＿ＡＵを検索して、セッションデータ及びチャレンジに関してauthenticator_witnessを演算／計算して、authenticator_witnessをユーザ装置から受信された認証符号と比較する。authenticator_witnessが認証符号に符合する場合、認証は成功したものとみなされ、ユーザの登載済みカードウォレットデータ（card-on-file wallet data）を有するウォレットパーティションへのアクセスをユーザに許す。

【０１１２】

認証符号の演算は、以下の態様でなされることができる。

【０１１３】

認証符号生成器はＳＫ＿ＡＵを用いて認証符号ＡＵ＿Ｃｒを計算するのであり、これは認証検証サーバによる検証のためにウォレットサーバのトークントランザクション処理エンティティへと送られるべきものである。

[数４]

AU_Cr = MAC(SK_AU)[Auth_Data]

【０１１４】

認証データ（Auth_Data）は、例えば次表のデータ要素の１以上を含むことができるのであり、それらの構成例も表されている：

【表１】

Amount, Authorized (Numeric) 承認された量（数値）	'000000000000'	6
Amount, Other (Numeric) その他の量（数値）	'000000000000'	6
Terminal Country Code 端末国コード	'0000'	2
Terminal Verification Results 端末検証結果	'0000000000'	5
Transaction Currency Code トランザクション通貨コード	'0000'	2
Transaction Date トランザクション日付	'000000'	3
Transaction Type トランザクション種別	'00'	1
Unpredictable Number 予測不能数	ウォレットサーバによって送られたRAND	4
Application Interchange Profile アプリケーション交換プロファイル	MPP Lite [AU]でパーソナライズされたAIP	2
Application Transaction Counter アプリケーショントランザクションカウンタ	MPP Lite [AU]で保たれたATC	2
Card Verification Results カード検証結果	'A50000000000'	6

【０１１５】

一部の実施形態では、認証検証サーバによって量及びトランザクション通貨コードが提供されるか否かによって、これらのデータアイテムはAuth_Dataにおいてゼロとは異なる値として提示され得る。

【０１１６】

一部の実施形態では、ＡＵ＿Ｃｒは、第１のＡＣ生成コマンドに対しての応答のタグ「９Ｆ２６」内で送られることができる。

【０１１７】

一部の実施形態では、ＭＡＣ機能は、ＥＭＶ支払トランザクションプロトコルにおいて定義されるＥＭＶ暗号プリミティブとして実装することができる。

【０１１８】

図１３は、一部の実施形態による、認証セッション鍵の導出及びそのセキュア送信を示す図である。図１３に示されている処理／演算の入力の１つはＷＳＰ＿ＭＫ＿ＡＵ（参照符号１３０２）であり、これはウォレットサービスプロバイダ（wallet service provide

r）によって維持されている（即ち、ウォレットサーバのオペレータによって維持されている）認証サービス（authentication service）のための専用システムマスター鍵（master key）である。

【０１１９】

ＷＳＰ＿ＭＫ＿ＡＵは、トークナイゼーション／デジタイゼーションサービス等と合意されたウォレットサービスプロバイダによって認証用途のために予約された特殊ＢＩＮ（銀行識別番号、bank identification number）レンジから割り当てることのできる専用のＴＩｄＮを伴う各々の認証トークンのための認証用トークンマスター鍵（ＴＭＫ＿ＡＵ、token master key for authentication；参照符号１３０４）に多様化される。トークン属性も多様化データに含めることができる。

【０１２０】

ウォレットサーバへ向かってのユーザ認証のための認証用セッション鍵ＳＫ＿ＡＵは、認証トークンの認証符号トランザクションカウンタ（ＡＴＣ、authenticator transaction counter；参照符号１３０６）をダイバーシファイアとして使用することによって、ＴＭＫ＿ＡＵから生成されることができる。ＡＴＣは認証セッション毎にインクリメントされ、また、認証検証サーバはこの値と各Ｕｓｅｒ＿ＩＤ／Ｄｅｖｉｃｅ＿ＩＤの認証トークンとの同期を維持する。一部の実施形態では、既知のＥＭＶ　ＣＳＫセッション鍵アルゴリズムを用いることができる。

【０１２１】

ＳＫ＿ＡＵはハッシュ値と組み合わされて、後述の関数ＦｎＨを用いて認証用一回用鍵（ＳＵＫ＿ＡＵ）を生成する。一部の実施形態では、ＳＫ＿ＡＵ自体の代わりに、ＳＵＫ＿ＡＵを認証トークンへと送信する。

【０１２２】

これに対応して、認証トークンによって受信されたＳＵＫ＿ＡＵは、ハッシュ値と組み合わされて、関数ＦｎＨを後述のような態様で用いることによって当初のＳＫ＿ＡＵを復元する。

【０１２３】

ハッシュ値は次式に従って計算できる：

[数５]

HASH = H1[RAND, H2(WSP_AU_PIN, SALT)]

ここで、以下の点に留意する：

【０１２４】

・　ＷＳＰ＿ＡＵ＿ＰＩＮは、ユーザが使う４～６桁の長さのＰＩＮであり、ユーザ自身のチェックアウト資源／ＣｏＦに関する認証のために使われるものである。ＷＳＰ＿ＡＵ＿ＰＩＮは、ユーザのみに知られたる「復号鍵」とみなされることができ、これは自己の知識の証左として提供されるものであり、認証符号の生成のために用いられるべき（ＳＵＫ＿ＡＵからの）ＳＫ＿ＡＵの復元を可能とするためのものである。

・　ＳＡＬＴは、各ユーザについてＰＩＮ登録又はＰＩＮ変更の際に自動生成されるダイバーシファイアである。これは、ウォレットサーバの「ソルテッドＰＩＮ（salted PIN）」テーブルに対しての総当たり攻撃の難度を増大させるために用いられる。「ソルテッドＰＩＮ」テーブルは、ユーザデータベース内の各々のユーザのレコード内においてフィールドたるH2(WSP_AU_PIN, SALT)を有している。

【０１２５】

一回用鍵ＳＵＫ＿ＡＵは、トークンクレデンシャル９２２（図９）からユーザのモバイルアプリ又はブラウザ拡張又はウェブページへと送信される。この文脈では、ＳＵＫ＿ＡＵはＡＥＳ２５６－Ｅ暗号アルゴリズム（参照符号１３０８、図１３）で暗号化されるのであり、該暗号化はユーザ装置に特有のトランスポート鍵を用いてなされるのであり、該トランスポート鍵はK_{TR}（transport key；参照符号１３１０）と称され、処理は次式に従って為される：

[数６]

ESUK = AES256-E[K_{TR}](SUK_AU)

【０１２６】

一部の実施形態では、トランスポート鍵K_{TR}はウォレットサービスプロバイダに特有の導出プロセスを介してトークン保管庫（token vault）にて生成されるのではなく、むしろトランスポート鍵は初期化段階においてランダムでユーザのアプリ／ブラウザ拡張／ウェブページによって生成されるのであり、セキュアな態様でウォレットサーバへと送信されるのであり、トランスポートサービス鍵（transport service key）としてユーザデータベースで更新される。

【０１２７】

一部の実施形態では、認証セッション鍵の生成のためのセキュリティパラメータは次のようにすることができる：

・　Ｈ２＝ＳＨＡ－２５６

・　Ｈ１＝ＳＨＡ－２５６の４バイトについての打ち切り出力。

関数ＦｎＨ（ｎＫｅｙ，Ｈ１）を用いてＳＫ＿ＡＵ鍵及び４バイトのＨ１値からのＳＵＫ＿ＡＵの変換をサポートする。

【０１２８】

入力は次のとおりである：

・　Ｈ１は（８ニブルまでの）１６進数及び１６バイトのデータブロックとして表され、

・　ｎＫｅｙは変換されるべき、鍵の１６バイトのデータブロックを表す

【０１２９】

出力は１６バイトのデータブロックである。

【０１３０】

関数は次のようにコーディングされる：

```
for(i=0; i < H1Length; i++)
{
nKey[i] ^= (sH1[i] << 1); // 鍵の左部分
nKey[(i+8)] ^= (sH1[i] << 1); // 鍵の右部分
}
```

ここで：

・　^ はＸＯＲ演算子であり、

・　<< 1 は１ビットの左シフト（バイトベースド）であり、

・　[i] は変数の第ｉ番目のバイトであり、

・　H1Length はＨ１の長さ（＝桁数＝８）であり、

・　sH1 はＨ１値のＡＳＣＩＩ表現である。

【０１３１】

本願開示の以下の部分は認証セッション鍵のプロビジョニングに関する。

【０１３２】

ウォレットサーバ２０６のプロビジョニングサーバ機能の認証クレデンシャルブロック９２２（図９）は、暗号化を伴うセキュアチャンネルを用いて、ありとあらゆる認証セッションの実行に際してＳＵＫ＿ＡＵを認証トークンに提供することができる。

【０１３３】

これに関しては、各認証トークンを特有のトランスポート鍵K_{TR}で初期化することができ、認証トークンが、プロビジョニングサーバから受信した暗号化ＥＳＵＫ値を、復号モードのＡＥＳ２５６－Ｉブロックサイファを用いて正しく復号できるようにする。

[数７]

SUK_AU = AES256-I[K_{TR}](ESUK)

【０１３４】

本願開示の以下の部分は認証符号の計算についてのＤＷＢ暗号実装に関する。

【０１３５】

上述のように、一部の実施形態では、認証符号（ＡＵ＿Ｃｒ）の計算は「アプリ」内で

実行できる。アプリは次のようにすることができる：
・　アプリストアからダウンロードされた汎用的モバイルトランザクションアプリケーション；
・　ウェブストアからダウンロードされたブラウザ拡張；
・　セキュアなサーバからダウンロードされたＨＴＭＬ５ウェブページ。
【０１３６】
アプリのソフトウェアオンリーなセキュリティを実装するために、図１４に示すように、２つのソフトウェアコンポーネントを重畳して用いることができる。図１４の構成では、認証符号の計算は、グレーボックスとＤＷＢＣ（dynamic white box cryptography）とを組み合わせた認証トークン内で行われることができる。グレーボックス（参照符号１４０２、図１４）及びＤＷＢ１４０４（図１４）両者の特徴については、後述する。
【０１３７】
アプリの全体の基礎としては、ソフトウェア難読化によるグレーボックスアプローチを使うことができるのであり、これによってソフトウェア全体と暗号関連のコンストラクト類（含む、ＤＷＢ）と機密なオペレーティングパラメータとを保護するのであり、該パラメータとしては例えば次のようなものが含まれる：アプリ内に格納されている間のＳＡＬＴや、クライアントのＰＩＮパッドソフトウェアエミュレータにタイプされてアプリに送信される迄の間のＷＳＰ＿ＡＵ＿ＰＩＮや、更にはＰＩＮパッドエミュレータを表示せずにアクションを惹起させるための「タッチ」だけによる高度に利便的でストリームライン化されたＵＸを提供するためのアプリ内に格納されたＷＳＰ＿ＡＵ＿ＰＩＮ。もっとも、何らの暗号鍵もグレーボックスオンリーの保護下に放置される訳ではなく、これらは後述するＤＷＢ暗号コンストラクトを伴う第２のレベルの保護下に置かれるのである。
【０１３８】
アプリのソフトウェアオンリーなセキュリティコンポーネントは例えば図６の６０４で概略的に示されたようなＤＷＢ暗号コンストラクトも含むことができ、変換Ｔ（）は対称鍵復号プリミティブである。
【０１３９】
一部の実施形態では、同じ汎用アプリを用いつつも、アプリのユーザ初期化が行われるか否か又はユーザ装置によってサポートされているか否かによって、（より低位なレベルの）ＳＷＢセキュリティレベル又は（より高位なセキュリティレベルの）ＤＷＢセキュリティレベルを達成することができる。
【０１４０】
復号アルゴリズムは、固有システム鍵（K_{SYS}）をエンコードする静的ホワイトボックス（ＳＷＢ、Static White Box）ＡＥＳ２５６－Ｉアルゴリズムを用いて実装することができる。この場合において実装はＳＷＢセキュリティレベルのものであり、全てのユーザ装置にシステムワイドな鍵が配布されるのであるが、初期化段階においてユーザ及びウォレットサーバを関与させなくて良いという利点がある。
【０１４１】
ユーザによってアプリ上でウォレットサーバ／ＷＳＰを組み合わせて行われた初期化段階中に、ＳＷＢ　ＡＥＳ２５６－ＩのK_{SYS}が装置又はユーザに特有なトランスポーテーション鍵K_{TR}と置換された場合、ＤＷＢにおける増強されたセキュリティレベルが提供され得る。
【０１４２】
ＤＷＢの利点は、システム鍵K_{SYS}をアプリによってランダムに生成された具体的なトランスポート鍵K_{TR}に変更した後においては、グレーボックス保護が仮に回避されたとしても、攻撃者が効果的にコードリフティング攻撃又はデータリフティング攻撃を行うことを妨げられる、という点にある。なぜならば、攻撃者は自己のハードウェア上で関連あるプロセスを再現できないからであるからである。これは、K_{TR}が利用不可能であることに起因する。
【０１４３】

この構成においては、初期化プロセス中にユーザ装置にてランダムに生成された鍵K_{TR}との関係でＤＷＢコンストラクトはユーザ／装置に特有なものと化するのであり、該鍵は、ウォレットサーバからアプリ内へと機密な認証セッション鍵を取り込むために使われるトランスポート鍵として用いられる。基本的な動作原理としては、初期化手順が呼び出された時のみにランダム鍵K_{TR}をモバイルトランザクションアプリケーションにインスタンス化する。この鍵は敵対的な環境の中でＳＵＫ＿ＡＵ鍵を輸送するためのトランスポート鍵として用いられるのであり、これはＳＵＫ＿ＡＵを暗号化形式ＥＳＵＫにしてなされ、ウォレットサーバのトークンクレデンシャルサーバ内での生成から認証符号のＭＡＣ計算での使用時迄に及ぶ。そして、ＤＷＢ実装例では復号を行ってＳＵＫ＿ＡＵを復元し、さらに後においてHASH = H1[RAND, H2(WSP_AU_PIN, SALT)]としたＦｎＨ変換を行ってＳＫ＿ＡＵを復元する。

【０１４４】

一部の実施形態では、認証トークン構造内のグレーボックス及び／又はＤＷＢ部分を初期化するに際して、モバイルフィンガプリント又は他の装置特有的データを活用することができる。

【０１４５】

一部の実施形態では、本明細書にて開示したＤＷＢのための動的鍵の生成のためのサーバベースドセキュリティの代替として、ユーザ装置内のクロック機能からＤＷＢのための動的鍵を生成することができる。本明細書にて説明しているように、いずれの場合であっても、動的鍵は、ローカルな暗号化データベース（「ＤＢＥ」、「database encrypted」とも称する）内に格納することができる。

【０１４６】

以下の説明は、強化されたセキュリティ対策が講じられている支払システム２００についての実施形態に関する。

【０１４７】

図１５は、高度にセキュアなユーザ認証プロセスのためのトランザクションフローについての概要を示す。更なる詳細は後述するも、高レベルで述べればプロセスフローは次の事項を含む：（ａ）認証トークンからウォレットサーバ（認証サービス）への認証リクエスト（参照符号１５０２）；（ｂ）認証トークンとウォレットサーバとの間でのセキュア通信チャネルの確立（参照符号１５０４）；並びに（ｃ）次のことを含むトンネリング認証セッション（参照符号１５０６）：（ｉ）装置認証段階１５０８；（ｉｉ）セッション鍵の生成及び（ウォレットサーバから認証トークンへなされる）送信１５１０；及び（ｉｉｉ）ユーザ認証段階１５１２。

【０１４８】

以下においては、セキュアチャンネルの確立、装置認証、セッション鍵の生成及び配布、並びにユーザ認証についての詳細について述べる。

【０１４９】

図１５に示すトランザクションフローは、認証トークンによってなされるトークンクレデンシャルサーバの認証で始まり、続いてトークンクレデンシャルサーバと認証トークンとの間のセキュアチャンネルの確立がなされる。この段階においては、認証トークンがクライアントの役割を果たし、他方でトークンクレデンシャルサーバがサーバの役割を果たす。

【０１５０】

ＴＬＳ（トランスポート層セキュリティ）ハンドシェークプロトコルは、サーバがクライアントに認証することを可能とする。また、該プロトコルは、対応する暗号鍵を伴う対称暗号アルゴリズムのネゴシエーションを可能とする。ネゴシエーションされた鍵は、クライアントとサーバとの間でのセキュアセッション中に確立された任意の接続のためのレコードプロトコルオペレーションのために供される。ハンドシェークプロトコルについては、本願開示の認証機構によって必要とされ得る要素を伴って後述しており、概略的には図１６に示してある。

【０１５１】
一部の実施形態では、支払ネットワークオペレータ（図中及び以降の説明においては、ＭＣＷと称する。）は、認証トークン及びトークンクレデンシャルサーバの双方によって信頼されている証明機関（certification authority）として機能できる。
【０１５２】
認証トークンは、ＫＶ＿ＭＣＷ（ＭＣＷ公開検証鍵）で初期化される。
【０１５３】
自己の番になると、トークンクレデンシャルは次のものを伴って初期化される：
・　ＫＶ＿ＭＣＷ　－ＭＣＷ公開検証鍵
・　Ｃｅｒｔ＿Ｓｅｒｖｅｒ＝Ｃｅｒｔ＿ＭＣＷ（ＫＥ）　－トークンクレデンシャルサーバのためにＭＣＷによって発行された公開暗号鍵証明書（public encryption key certificate）
・　ＫＥ　－トークンクレデンシャルサーバの公開暗号鍵（Public encryption key）
・　ＫＤ　－トークンクレデンシャルサーバの秘密復号鍵（Private decryption key）
【０１５４】
ハンドシェークプロトコルの第１段階では、ウォレットサーバインフラにおいて、ユーザの認証トークンとトークンクレデンシャルサーバとは、次のような若干修正されたＴＬＳハンドシェークプロトコルを行う：
【０１５５】
・　ステップ１６０２－－認証トークンが、認証リクエストをトークンクレデンシャルサーバへと転送する。このコマンドのパラメータとして以下のものが提供される：
□　ユーザデータベース内のユーザの識別子（Ｕｓｅｒ＿ＩＤ）
□　装置データベース内の（認証トークンをホスティングしている）ユーザ装置の識別子Ｄｅｖｉｃｅ＿ＩＤ
□　サポートされる暗号化アルゴリズムの識別子を伴ったCipherSuiteClient提案のセット（トークンクレデンシャルの可能性と同調されるべきものであり、　－システム内で２つの主体は互いを知っているが故にマッチングアルゴリズムは予め確立しておくことができることに留意されたい。）
□　サーバへ差し向けられたクライアントチャレンジの一環としての乱数Ｒ＿Ｃ
【０１５６】
・　ステップ１６０４－－認証リクエスト受信後、トークンクレデンシャルサーバは次のオペレーションを行う：
□　Ｕｓｅｒ＿ＩＤを用いてシステムにおけるユーザの登録状態を確認し、また、ユーザデータベースからそのユーザの暗号パラメータを検索するのであって、該パラメータは次のとおり：
　　{TIdN, Token_Attributes, H_2U = H2(WSP_AU_PIN, SALT_U)}
□　Ｄｅｖｉｃｅ＿ＩＤを用いてユーザ装置の登録状態を確認し、これに基づいてトークンクレデンシャルサーバは装置の暗号パラメータを装置データベースから検索し及び格納するのであり、該パラメータは次のとおりである：
　　{H_2D = H2(MD_Fingerprint, SALT_D)} 。
□　自己のCipherSuiteServerを検索して、CipherSuiteServerの記述に従って認証トークンにサポートされている暗号アルゴリズムとマッチングを行うのであり、　－例えばＲＳＡとすることもできるが、代替的には他のアルゴリズムもサポートできる。
□　クライアントへ差し向けられたサーバチャレンジの一環としての乱数Ｒ＿Ｓを生成する。
□　公開暗号鍵証明書Cert_Server = Cert_MCW (KE)を検索する。
□　次のロードを形成してクライアントに送る：
　　サーバ応答 {R_S, Cert_Server, CipherSuiteServer }
【０１５７】
・　ステップ１６０６－－トークンクレデンシャルサーバからサーバ応答を受信後、認証

トークンは次のオペレーションを行う：
□　トークンクレデンシャルのCipherSuiteServerを検索して、自己のCipherSuiteClientを伴って共通にサポートされた暗号アルゴリズムとしてＲＳＡを識別する。
□　受信されたCert_Serverのピニング（pinning）が、認証トークンの初期化以来認証トークン内で格納されていた、トークンクレデンシャルサーバの公開暗号鍵証明書に対応する証拠的ピニングトレース（witness pinning trace）に対応することを検証する。
□　ＭＣＷ公開検証鍵ＫＶ＿ＭＣＷを用いてCert_Serverを検証してトークンクレデンシャルサーバの公開暗号鍵ＫＥの真正なコピーを取得する。
□　ランダムでプリマスター秘密（pms、pre-master secret）を生成する。
□　ＫＥを用いてpmsについてのデジタルエンベロープ（ＤＥ、Digital Envelope）を計算するものであって（即ち、DE= RSA(KE)[pms]）それをサーバへと送る。
【０１５８】
・　ステップ１６０８――デジタルエンベロープ（デジタル封筒）を認証トークンから受信した後、サーバは次のオペレーションを行う：
□　ＫＤを用いて、ｐｍｓを復元するためにＤＥを開封する、即ちpms= RSA(KD)[DE]。
□　ＴＬＳの記録プロトコルによって使用されるべきセキュアチャンネル鍵Ｋを、認証トークンによって提案されたｐｍｓ値及びセッション中に交換された乱数（Ｒ＿Ｃ，Ｒ＿Ｓ）から、計算すること、即ち：

K = SHA(pms, R_C, R_S)

□　鍵コンファメーション値V = SHA(K,R_C,R_S)を計算して、これを認証トークンへと送る。
・　（ステップ１６０８の続き）――鍵コンファメーション値Ｖをトークンクレデンシャルから受信した後、認証トークンは、サーバと同じ式K = SHA(pms, R_C, R_S)を用いてセキュアチャネル鍵Ｋについての自己のコピーを作成して、これを自己の計算結果と対比して検証（verify）する、即ち：
Verify V ?= SHA(K,R_C,R_S)
【０１５９】
検証が成功裏に終わった場合、トークンクレデンシャルサーバは真正なものであるとみなされ、セキュアチャネル鍵Ｋは、トークンクレデンシャルサーバとのセッションが終了する迄の以後のデータ交換全てについての暗号化に関する記録プロトコルへと、渡される。
【０１６０】
図１７は、図１５のステップ１５０８（装置認証）の詳細を示すフローチャートである。以下の説明では、「ＡＴＣ」は認証符号トランザクションカウンタ（authenticator transaction counter）の現在値を示し、「ＡＴＣ－１」はユーザ認証プロトコルの以前（直前）の実行回／セッションにおける該カウンタの値を示す。
【０１６１】
ステップ１７０２、図１７――認証トークンが暗号化データベース（ＤＢＥ、Database Encrypted）を読んで以下を検索する：
・　プロトコルの全ての実行に用いられる共通の値、即ち：
□　H_2D = H2(MD_Fingerprint, SALT_D)
□　SALT_U
備考：
パスワードについての辞書攻撃を抑制するためのＳＡＬＴは装置認証について異なる値を有しているのであり、装置データベースの装置フィンガプリントテーブルに保持されている値とされるのであり、即ち：

H_2D = H2(MD_Fingerprint, SALT_D)

であり、ユーザ認証についてはユーザデータベース内に保持されている値とされるのであり、即ち：

H_2U=H2(WSP_AU_PIN, SALT_U)

・　「ＡＴＣ－１」に対応する、ＤＢＥ内のメモリインデックスにて格納された、鍵の生成及び配布に関しての以前のセッションの値、即ち：
□　ESUK*_MD = AES256-E[KTR](SUK*_MD)
□　RAND* －以前のユーザ認証セッションで使用されたランダムな（チャレンジ）値
備考：　以下のアルゴリズムはＡＴＣ＞０の場合に機能する。ＡＴＣ＝０の場合、装置認証は、ＷＳＰによって初期化段階において配布された認証コード（Authentication Code）に頼ってなされるのであり、その使用態様については後述する。

【０１６２】
ステップ１７０４、図１７－認証トークンは、ＤＷＢコンストラクトを用いて以下を計算する：

DA_Cryptogram = MAC [SK*_MD](R_S, ATC)

ここで：
・　Ｒ＿Ｓは、ハンドシェーク段階においてトークンクレデンシャルサーバによって認証トークンへと送られたチャレンジ値であり（ステップ１６０４、図１６）、
・　ＡＴＣ－認証符号トランザクションカウンタ（ＡＴＣ）の現在値（ATC_crt）であり、
・　SK*_MD = SUK*_MD FnH H1(RAND*, H_2D)であり、ここでRAND*及びH_2DはＤＢＥから検索された値であり、
・　SUK*_MD = AES256-I[ESUK*_MD]であり、ここでESUK*_MDはＤＢＥから検索された値である。

【０１６３】
ステップ１７０６、図１７－認証トークンは、装置の信頼性の証明の検証のためにDA_Cryptogramをトークンクレデンシャルサーバへと送信する。

【０１６４】
ステップ１７０８、図１７－トークンクレデンシャルサーバは、装置認証用トークンマスター鍵ＴＭＫ＿ＭＤを次のようにして計算するようにトークン管理保管庫（Token Management Vault）に依頼する：

TMK_MD = 3DES[WSP_MK_MD](Device_ID, MD_Fingerprint)

ここで、
・　WSP_MK_MDは、装置認証サービスについてのＷＳＰのシステム鍵であり、
・　Device_IDは、装置データベースに記録されている装置の識別子であり、
・　MD_Fingerprintは、認証トークンソフトウェア構成についてモバイルＯＳ又はブラウザ拡張によって計算された一意的なトレースである。

【０１６５】
トークンクレデンシャルサーバは、以前の実行回において用いられた装置認証のためのセッション鍵を計算するために、ＴＭＫ＿ＭＤを用いるのであり、即ちセッション鍵は次の通りである：

SK*_MD = 3DES[TMK_MD](ATC-1)

【０１６６】
そしてこの段階になれば、トークンクレデンシャルサーバは、装置認証符号の証拠的値（witness value）を計算することができ、これを受信された値DA_Cryptogramと比較するのであり、即ち：

MAC[SK*_MD](R_S, ATC) ?= DA_Cryptogram

【０１６７】
等式が真となる場合、装置は真正のものであるとみなされ、ユーザ認証プロトコルの以下の段階を実行することができる。

【０１６８】
トークンクレデンシャルサーバは、ステップ１５０４（図１５）でデータベースから検索されたユーザ及び装置パラメータを用いるのであり、後続のチャレンジ／応答の実行（即ち、図１５のステップ１５１０）のための新たなＲＡＮＤ（チャレンジ値）を生成する

ようにトークントランザクション処理に要請する。したがって、次の値がプロトコルの次段階において利用可能である：

・ {TIdN, Token_Attributes, H_2U = H2(WSP_AU_PIN, SALT_U)}
・ {H_2D = H2(MD_Fingerprint, SALT_D)}
・ RAND

【０１６９】

本願開示のこの箇所で説明される消費者認証システムは、特殊な、鍵についてなされる生成及び配布に関する、スキーマに依拠しており、該スキーマによれば、ソフトウェアオンリーなセキュリティモデルをとった場合の、セキュリティサービスの実現のためになされる暗号鍵の格納についての、潜在的な脆弱性を緩和し得る。

【０１７０】

一部の実施形態において、後述の鍵の生成は、装置毎に（セキュア要素の片割れとして）何らかの暗号化データベースにて格納される１つの長期的サービス鍵の使用に依存はしていないのであり、認証トークンによる多様化が想起され、それぞれのサービスの実行のためのセッション鍵の実現にＡＴＣが伴う。

【０１７１】

代わりに、これらの実施形態のための仕組みにおいては、２つの「ワンタイム」セッション鍵が用いられるべきものとして提案され、図１１でこのことが概略的に示されており、以下のように要約される：

【０１７２】

（１） 装置認証セキュリティサービスのため、当事者はＳＫ＿ＭＤと称する装置認証用セッション鍵（session key for Device Authentication）を用いるのであり、これは現在のユーザ認証トランザクションにてトークンクレデンシャルサーバによって作られ、次期ユーザ認証セッションでの装置認証サービスの実現のために認証トークンによって使用されるためのものである。この鍵ＳＫ＿ＭＤは、ＡＴＣ＝０の場合の認証トークンの初期化時に、認証コードの値の箇所にて認証トークン内にてセットされる。

【０１７３】

（２） ユーザ認証サービスのため、当事者はＳＫ＿ＡＵと称するユーザ認証用セッション鍵（session key for user authentication）を用いるのであり、これは現在のユーザ認証トランザクションにてトークンクレデンシャルサーバによって作られ、同じユーザ認証セッションでのユーザ認証サービスの実現のために認証トークンによって使用されるためのものである。この鍵ＳＫ＿ＡＵは、認証トークン内に格納されることはない。

【０１７４】

図１８は、図１５のステップ１５１０の詳細を示すものであり、これは先程説明した２つの鍵の生成に関連する事柄である。次に、図１８を参照するに以下のとおりである：

【０１７５】

ステップ１８０２、図１８－トークンクレデンシャルサーバは、ユーザ認証の次期実行セッションにて用いられるべき装置認証用セッション鍵を計算するために、ステップ１７０８（図１７）で取得した鍵ＴＭＫ＿ＭＤを再利用するのであり、次のようにする：

SK*_MD = 3DES[TMK_MD](ATC)

【０１７６】

ステップ１８０４、図１８－トークンクレデンシャルサーバは、消費者認証用トークンマスター鍵ＴＭＫ＿ＡＵを次のようにして計算するように依頼する：

TMK_AU = 3DES[WSP_MK_AU](TIdN,Token_Attributes)

ここで：

・ WSP_MK_AUは、ユーザ認証サービスについてのＷＳＰのシステム鍵であり、
・ TIdNは、ユーザデータベースに記録されている認証トークン識別子であり、
・ Token_Attributesは、トークンが、ユーザ認証プロトコルのためのみに用いて宜しく、支払トランザクションそれ自体のためには用いられてはならぬことを記述するための属性のセットである。

【０１７７】
トークンクレデンシャルサーバは、ユーザ認証プロトコルの現在の実行回において用いられるべきユーザ認証用セッション鍵を計算するために、ＴＭＫ＿ＡＵを用いるのであり、次のようにする：

SK_AU = 3DES[TMK_AU](ATC)

【０１７８】
ステップ１８０６、図１８－トークンクレデンシャルサーバは、（暗号化されたＴＬＳトンネルが既になされているという意味で）「過剰」にセキュアな輸送のための「隠蔽」パラメータ（例えば、ハッシュ値）を計算するのであり、セッション鍵のセキュアな送達は意図された受信者、即ちユーザと同人の装置、のみに対して差し向けられており（なお、一意的なトランスポート鍵K_{TR}に頼っているＤＷＢコンストラクトを伴って初期化される）、次のようにする：

・ HASH_U = H1[RAND, H2(WSP_AU_PIN, SALT_U)]－ユーザ認証用セッション鍵ＳＫ＿ＡＵのための隠蔽パラメータ。
・ HASH_D= H1[RAND, H2(MD_Fingerprint, SALT_D)]－装置認証用セッション鍵ＳＫ＊＿ＭＤのための隠蔽パラメータ。

【０１７９】
ステップ１８０８、図１８－トークンクレデンシャルサーバは、認証トークンへとセキュアに配布されるべきセッション鍵を計算するのであり、該鍵は次の「隠蔽」パラメータを介して変形された一回用鍵（ＳＵＫ、Single-Use Keys）とされる：

・ SUK_AU = SK_AU FnH HASH_U 。SK_AUは、現在のユーザ認証セッションを完遂するために認証トークンによって使用される。
・ SUK*_MD = SK*_MD FnH HASH_D 。SK*_MDは、先ず認証トークンのＤＢＥ内に格納されるのであり、次期ユーザ認証セッションでの装置認証段階を完遂するために認証トークンによって使用される。

【０１８０】
ステップ１８１０、図１８－認証トークンのＤＷＢコンストラクトによって許された第３のレベルの暗号化を行うために、トークンクレデンシャルサーバは、最後にもう一回、一回用鍵（SUK_AU, SUK*_MD）を暗号化することができる。暗号化は、装置に特有なトランスポーテーション鍵（transportation key）K_{TR}を用いてなされる。したがって、一回用鍵（ＳＵＫ＿ＡＵ）は、ＤＷＢコンストラクトによってK_{TR}をランダムに初期化時において生成したユーザの認証トークンのみによって、セキュアに送達され得るのであり、次のようになる：

・ ESUK = AES256-E[KTR](SUK_AU)
・ ESUK*_MD = AES256-E[KTR](SUK*_MD)

【０１８１】
ステップ１８１２、図１８－－トークンクレデンシャルサーバは、ESUK、ESUK*_MD、及びRANDを認証トークンへと送信する。

【０１８２】
本願開示の次の部分は、装置／ユーザ認証セッションのユーザ認証段階に関する。

【０１８３】
図１９は、図１５のステップ１５１２の詳細を示すフローチャートである。

【０１８４】
ステップ１９０２、図１９－－認証トークンは、ＤＢＥ内にESUK*_MD及びRANDを格納するのであり、これはユーザ認証プロトコルの次期実行時の装置認証段階の達成のためになされる。

【０１８５】
ステップ１９０４、図１９－－認証トークンは、ＳＡＬＴ＿ＵをＤＢＥから検索する（ＳＡＬＴ＿Ｕは、後述のように、暗号化の演算／計算のための入力データとしての役割を果たすことになる）。

【０１８６】
ステップ１９０６、図１９－－認証トークンは、仮想ＰＩＮパッド（virtual PINPad）をポップアップさせて、ウォレット認証のための消費者のＰＩＮ即ちWSP_AU_PINを求める。ユーザは、要求された秘密を打ち込む（即ち、ＰＩＮについてのユーザ入力を求めて、これを受信する）。
【０１８７】
ステップ１９０８、図１９－－認証トークンは次のものを計算する：

AU_Cr = MAC(SK_AU)[Auth_Data]

ここで、Auth_Dataは、図１２についての記述に続く本願開示の上述のセクションにて説明されている。
【０１８８】
認証用セッション鍵ＳＫ＿ＡＵは認証トークンによって検索され、ＤＷＢコンストラクトは次の通りである：

SK_AU = SUK_AU FnH HASH_U

ここで：
・ HASH_U = H1[RAND, H2(WSP_AU_PIN, SALT_U)]であり、WSP_AU_PINは認証証拠としてユーザによって提供されたものであり、
・ SUK_AU = AES256-I[K_{TR}](ESUK)であり、これは、ユーザ装置のＤＷＢコンストラクトによって、トークンクレデンシャルサーバから受信されたエンベロープＥＳＵＫから、復号されたものである。
【０１８９】
ステップ１９１０、図１９－－認証トークンは、暗号ＡＵ＿Ｃｒを、ウォレットサーバ構成内のトークントランザクション処理へと送る。
【０１９０】
ステップ１９１２、図１９－－トークントランザクション処理は次の処理を行う：
・ ステップ１７０８（図１７）の完了後にトークンクレデンシャルサーバのために生成した初期ＲＡＮＤ（チャレンジ値）を検索する。
・ ステップ１８０４（図１８）で計算されたＳＫ＿ＡＵを、トークンクレデンシャルサーバから受信する。
・ （図１２についての説明に続く本願開示の部分に記載されているように、）ＲＡＮＤ及びＡＴＣから出発して認証トークンが行ったのと同じ態様で、Auth_Dataを再コンパイルする。
・ 受信された次のものについて比較を行う：AU_Cr ? = MAC(SK_AU)[Auth_Data] 。２つの値が等しい場合、トークントランザクション処理サーバは、ユーザの信頼性を受け入れる。
【０１９１】
装置認証及びユーザ認証の両方について成功裏に完了した場合、ウォレットサーバは、ユーザがユーザ装置を介して自己のデジタルウォレットにアクセスすることを許可することができる。例えば、現在の購買トランザクションで使うために、１つの支払口座を選択することをユーザが許されることとすることができ、ここでは支払口座はユーザのデジタルウォレット内の幾つかの「登載済みカード」（cards on file）に含まれているものとされる。そして、支払トランザクションを進行させることができ、トランザクションについての課金を選択された支払口座に対して行うことになる。
【０１９２】
少なくとも幾つかの用途に関しては、装置認証フェーズ又は段階の完了後に生じる、図１５の処理の全部は、処理のユーザ認証フェーズ又は段階の一部とみなされ得る
【０１９３】
本願開示の以下の部分は、ソフトウェアオンリーな認証システムのために必要な様々なエンティティのセットアップオペレーションについての概要を提供するのであり、例えば、ＭＰＡ／ＢＥ（モバイル支払アプリケーション（mobile payment application）／ブラ

ウザ拡張（browser extension））やトークンクレデンシャルサーバのデータベースが含まれる。

【０１９４】

後述の１つのセクションは、ユーザ装置内についてのＤＢＥ（暗号化データベース）のために使用される仕組みについて言及している。静的ホワイトボックス手法を用いることによって、ユーザ装置内の潜在的には攻撃されやすいパラメータについて、比較的単純で効果的な保護をもたらすことができる。

【０１９５】

装置特有的な／装置固有的なトランスポート鍵を伴っての、ユーザ装置内でのＤＷＢコンストラクトの初期化に関する更なる詳細事項が、後述の別のセクションで提供されており、これによって、一部の実施形態では、ユーザ装置が「あなたが有する何か」型認証要素として機能することになる。この手法によれば、あらゆるユーザ装置（即ち、標準的なダウンロード可能なウォレット／支払アプリ／ＭＰＡ／ＢＥ）内に単一のコードシーケンスを用いることが可能となり得るのであり、各ユーザ装置での、装置のオペレーションの初期化段階に際して、各ユーザについて異なる態様でアプリの初期化をなすことになる。

【０１９６】

後述のまた別のセクションでは、システム２００におけるユーザ登録段階についての概要を提供し、また、他の追加的セクションはユーザ装置にＭＰＡ／ＢＥをインストールして初期化することについて言及している。以降における説明を簡略化するために、ＭＰＡについてのみ述べるが、ＭＰＡに妥当する説明はＢＥにも妥当するものとして解されるべきである。

【０１９７】

説明の以下のセクションは、上述のＤＢＥについての記述を含む。図２０は、（図６の部分たる６０２による）静的ホワイトボックス（ＳＷＢ、static white-box）暗号コンストラクトの詳細を概略的に示す図であり、これ用いてＤＢＥにおいて必要とされる変換を提供することができる。

【０１９８】

図２０の左側（参照符号２００２）には書き込みオペレーションが示されており、－ここで指数ｉ及びＡＴＣ値はＳＷＢアルゴリズムに対する入力であり、該アルゴリズムでは、埋め込まれたK_{SYS}を使ってその指数値についての鍵Ｋｉを作成するのであり、これをモバイルフィンガプリント（MD_Fingerprint）と組み合わせてモバイル機器に合わせてパーソナライズするのであり、これによってＫ’ｉを得る。そして、パラメータPARAMiを暗号化するためにＫ’ｉを用いるのであり、これによって暗号化されたパラメータEPARAMiが形成され、これをその指数ｉの下に格納する。

【０１９９】

読み出しオペレーションは書き込み手続の逆であり、図２０の右側（参照符号２００４）に示されている。Ｋ’ｉを作るのに用いられたのと同じ手順を用いてＫ’ｉを再計算する。そして、EPARAMiを復号するためにＫ’ｉを用いてPARAMiを再作成する。

【０２００】

図２０の手順全ては、ソフトウェア難読化によって更に保護されることができる－つまり、このプロセスの全体が「グレーボックス」内で行われ得る。

【０２０１】

図２０のアプローチは、ＭＰＡについてユーザカスタマイゼーションがなされていないことを仮定しているのであり、－即ちモバイルフィンガプリントはＭＰＡが実行されている間に提供されており、－－該ＭＰＡは純然に汎用的である。

【０２０２】

ユーザ認証プロトコルの用途に関して、ＤＢＥは、次のようにして削減した個数のパラメータを格納している（詳細は図２１に示される）：

・　－－書き込み及び読み出しオペレーションの両者について、指数＝１、ＡＴＣ＝０の場合　－－適切なＫ’ｉ鍵たるPARAM11 = SALT_U（参照符号２１０２）及びPARAM12= H2_

D（参照符号２１０４）を伴う暗号化された値が格納されている。
・　指数＝２の場合で、書き込みについてはＡＴＣ＝ＡＴＣ＿ｃｒｔである時及び読み出しについてはＡＴＣ＝ＡＴＣ＿ｃｒｔ－１である時は、PARAM21 = ESUK*_MD（参照符号２１０６）及びPARAM22=RAND*（参照符号２１０８）が格納されている。ＤＢＥ内に格納されるべき初期パラメータPARAM21は、図１８との関係で上述したようにトークンクレデンシャルサーバによって装置特有的なトランスポーテーション鍵K_{TR}を伴って作成された暗号に既になっている。ＤＢＥ内にEPARAM21として格納されると、ＡＴＣの現在値によって決定される鍵Ｋ’ｉの下で二重暗号化される。

【０２０３】
本願開示の次のセクションは、ユーザ装置内でのＤＷＢコンストラクトの初期化に関する。

【０２０４】
ＤＷＢコンストラクトの機能についての当該説明は、図１４との関連性を有している。また、以下の記載は、図６の下部６０４に示されているアプローチの実装例をも示すものである。後述の実装例では、図６の下部６０４にて示される変換は、K_{TR}（「トランスポート鍵（transport key）」を意味する）と称される鍵を伴っての復号処理であることができる。

【０２０５】
図２０、２１との関連で説明されたＳＷＢコンストラクトに関して述べるに、そのプロセスの全体をグレーボックス環境内で処理することが望ましいかもしれないのであり、この場合はHASH = H1[RAND, H2(WSP_AU_PIN, SALT)]の計算の全てをソフトウェア難読化によって保護することができる。ＤＷＢコンストラクト内で実装される復号化アルゴリズムは、ＤＷＢコンストラクトのホワイトボックス保護環境内のパラメータとしてセットされた鍵ＫＴＲを伴うパラメータ化AES256-Iアルゴリズムとすることができる。

【０２０６】
ユーザによってなされる初期化段階において述べるに、アプリケーションストアからダウンロードされた汎用的ＭＰＡは、初期化前においてはシステム鍵K_{SYS}をSWB AES256-Iのために有していることができ、初期化後においては装置特有的なブロックAES256-Iのための装置鍵K_{TR}で先のものを代替することができる。

【０２０７】
様々な実施形態では、同じ汎用的ＭＰＡを用いてＳＷＢのセキュリティレベル又はＤＷＢのセキュリティレベルを達成することができるのであり、これはＭＰＡ初期化が行われるか否かという点や、それらがモバイルコンピューティング装置によってサポートされているか否かという点に依存する。

【０２０８】
鍵がK_{SYS}からK_{TR}に変更された後においては、たとえＭＰＡのグレーボックス保護が迂回されたとしても、攻撃者は効果的にコードリフティング攻撃又はデータリフティング攻撃を行うことがもはやできなくなる。なぜならば、攻撃者は自己のハードウェア上で関連あるプロセスを再現できないからであるからである。これは、K_{TR}が利用不可能であることに起因する。

【０２０９】
つまり、実効的には復号化ブロックSWB AES256-Iは装置特有的になったのであり、ランダム鍵K_{TR}を伴ったＤＷＢ実装例たるAES256-Iとして生成される。トークンクレデンシャルサーバは、ＳＵＫ＿ＡＵが生成された時点から、それがトランスポート鍵K_{TR}によって暗号化される時点迄、ＳＵＫ＿ＡＵを保護している。

【０２１０】
基本的な動作原理としては、一部の実施形態では、初期化手順が呼び出された時のみにランダム鍵K_{TR}をＭＰＡにインスタンス化する（図２５－２７に関連する後述の記載も参照）。この鍵は敵対的な環境の中で運用中のＳＵＫ＿ＡＵ鍵を暗号化形式で輸送するためのトランスポート鍵として用いられるのであり、該暗号化は、トークンクレデンシャル

サーバ内での生成時から、ＭＰＡによってなされるＳＫ＿ＡＵの計算での使用時迄に及ぶ。そして、ＭＰＡのＤＷＢ実装例では、トランスポート鍵K_{TR}を用いて復号オペレーションを行ってＳＵＫ＿ＡＵを取得し、該取得は、この鍵についてのいかなる情報をもホワイトボックスで強化したサンドボックスの外に露出させない態様でなされる。

【０２１１】

ＤＷＢ初期化シーケンスは、復号のためのクリプトＡＰＩ対しての次のような例示的な呼び出しを伴う：

【０２１２】

図２２はＤＷＢ初期化シーケンスを示すフローチャートである。

【０２１３】

・　（ステップ２２０２、図２２）　トランスポーテーション鍵ktrを１６バイトで生成する、即ちktr = RANDOM (16)とする。

【０２１４】

・　（ステップ２２０４、図２２）　（図２０、２１との関連で述べられた）ＭＰＡのネーティブSWB-E K_{SYS}コンストラクトを用いて、トークンクレデンシャルサーバのためのktrを含むエンベロープを作成する、即ちEKTR = SWB-E[K_{SYS}](ktr)とする。これは次のようなコーディングの例をもたらし得る：

EKTR=NativeS_Encrypt_WBC(ktr,16) 。

このエンベロープは、初期化段階において、トークンクレデンシャルサーバへと送られる。

【０２１５】

・　（ステップ２２０６、図２２）　ＤＷＢコンストラクトで用いるための鍵ktrを伴ってＳＷＢ復号化関数S_Decrypt_WBCを作成する、即ち次のようにする：

S_Decrypt_WBC (input, size)

ここで：

○　inputは、ktrを伴う暗号化エンベロープESUKであり、これが一回用鍵ＳＵＫ＿ＡＵを輸送する。

○　sizeは、それのバイト長である（例えば、１６バイト）。

【０２１６】

この関数は、初期化段階において１回だけ作成されるのであり、例えば次のようなＡＰＩ呼び出しによって作成される：

Create Static WBC (decrypt, ktr, S_decrypt_WBC(), AES256)

関数たるS_Decrypt_WBCは、装置特有的トランスポート鍵ktrを、AES256-I内のホワイトボックス暗号モード内に埋め込まれた静的な鍵として使用する。

【０２１７】

・　（ステップ２２０８、図２２）　ＤＷＢコンストラクトを（例えば、）ＭＡＣとして作成するのであり、これは、ＥＭＶ支払プロトコルの特徴に準拠してなされたり、及び／又は周知の基準たるISO 9797-1に準拠してなされることができるのであり、即ち次のようにし得る：

D_MAC_WBC (key, vector, combination, input, size)

ここで、

○　keyは、動的鍵ＳＵＫ＿ＡＵであり、トランスポート鍵ktrを用いてS_Decrypt_WBCを介してなされるＥＳＵＫの送達に関するものであり；

○　vectorは、セッション鍵ＳＫ＿ＡＵを得るためにＳＵＫ＿ＡＵ鍵と組み合わされることができるコンポーネントであり、即ちvectorについては次のようにする：HASH_U = H1[RAND, H2(WSP_AU_PIN, SALT_U)] ；

○　combinationは、結果として生じるＭＡＣ秘密を得るためのアルゴリズムであり、次のようにする：

combination[key, vector] ；

例えば、combinationは、セキュリティパラメータとの関連で上記のセクションで述べたF

nH(nKey,H1)とすることができ；
○　inputは、ＭＡＣ化すべき認証データストリングであり；
○　sizeは、そのバイト長である。
【０２１８】
この関数は次のようなＡＰＩ呼び出しで作成することができる：
Create Dynamic WBC (ktr, S_Decrypt_WBC(ESUK), D_MAC_WBC(), “ISO9797-1”)
【０２１９】
以上のように、上述下ステップ２２０４に準拠した態様で各装置のトランスポーテーション鍵ktrの暗号を含むエンベロープ全てを受信及び記録できるようにするためには、トークンクレデンシャルサーバをK_{SYS}で初期化することを要する場合があり得る。
【０２２０】
本願開示の以下の部分は、ウォレットサーバでのユーザ登録に関する。この段階の概要は図２３に示されている。
【０２２１】
ユーザ登録段階においては、静的なユーザ認証クレデンシャル即ち（User_ID, password）を用いて、管理用ブラウジングセッション内で、ユーザはウォレットサーバに接続する。
【０２２２】
ユーザは、管理用ウェブサイトで、「ソフトウェアオンリー認証符号に関して登録する」との機能を選択する。
【０２２３】
この動作によって、サーバには登録リクエストが送られる。そして、サーバは、ランダムな認証コード（ＡＣ、Authentication Code）を生成して、これはユーザに送り戻されることになる。サーバは、（消費者データベース（ＣＤＢ、Consumers Database）とも呼ぶ）ユーザデータベース内のユーザレコードについて、ＡＣ値を更新する。
【０２２４】
ＡＣをウォレットサーバから受信した後、ユーザはこれを任意の従来的なセキュアな方法を用いて保管するのであり、後程の初期化段階においてこれを初期のユーザ認証及び装置認証として提出する（図２５－２７についての後述の記載も参照）。
【０２２５】
これによってユーザ登録段階が終わる。
【０２２６】
本願開示の次なるセクションは、ユーザ装置上にＭＰＡをインストールすることに関する。図２４はＭＰＡインストール段階の概要を示す。
【０２２７】
ソフトウェアオンリーな認証サービスへの登録とは独立して、ユーザは自己の装置にＭＰＡ（又はＢＥ）をインストールする手続に進むことができる。
【０２２８】
この点、ユーザは、アプリストアからＭＰＡアプリケーションを選択（ＢＥの場合は、ウェブストアから選択）することができ、自己の装置にこれをダウンロードすることができる。本願開示では、ダウンロードが無料であり、初期ユーザ（及び装置）認証の証拠としてＡＣを提示することをユーザが義務づけられないことを仮定する。
【０２２９】
ダウンロードされたＭＰＡは「初期化されていない」状態にあり、次の標準的コンテンツが伴う：
□　トークンクレデンシャルサーバとの関係で用いられるべき、ＭＰＡの初期化段階のための初期化ＵＲＬ。
□　Cert_Server = Cert_MCW(KE)　－ウォレットサーバのトークンクレデンシャルサーバのためにＭＣＷによって発行される公開暗号鍵証明書（図１５との関連も参照）。

□　バリデーションピニング　－Cert_Serverのピニング値であり、これは初期においてはＭＰＡに知られており、弱化したサーバ認証のためのものである。
□　トークンクレデンシャルサーバに対してなされる、ＤＷＢコンストラクトのトランスポーテーション鍵K_{TR}の初期のセキュアな引き渡しのための、SWB-E K_{SYS}コンストラクト。
□　システム鍵K_{SYS}を伴う「初期化されていない」ＤＷＢコンストラクト
【０２３０】
本願開示の次のセクションは、ＭＰＡの初期化（又は、明示的に述べられていないものの、ＢＥの初期化）に関する。
【０２３１】
初期化段階においては、ＭＰＡは「初期化されていない」状態から処理を開始し、初期化ＵＲＬに接続し、－例えば図１５及び１６との関連で説明されたような－セキュアチャンネルを確立するのであり、ユーザは従来的な（User_ID, password）を用いてトークンクレデンシャルサーバに対して認証をする。サーバは、ユーザデータベース／消費者データベース（ＣＤＢ）内の対応するユーザレコードを検索する。
【０２３２】
成功裏なユーザ認証の後に、サーバは、ＭＰＡ／ユーザに対して、装置識別子（Device_ID）と装置フィンガプリント（例えば、簡潔性のためにモバイル機器フィンガプリント（MD_Fingerprint）という）との関連で、初期の認証コード（ＡＣ）を提示するように要求する（もっとも、他の実施形態では、このことをブラウザ拡張（ＢＥ）についても可能とすることが望ましいかもしれない）。この点、ＭＰＡは、適切なDevice_ID値及びMD_Fingerprint値が生成されるようにするためにモバイルＯＳを呼び出すのであり、これらをＡＣと共にパッケージ化するのであり、これらをサーバへと送る。
【０２３３】
図２５は、ウォレットサーバによって後に行われることができるプロセスを表すフローチャートである。
【０２３４】
ウォレットサーバは、以下の処理を行うことができる：
【０２３５】
（ステップ２５０２、図２５）ＣＤＢのユーザレコードから証拠的ＡＣ（これはユーザ登録段階に格納されたものである、－図２３の説明も参照）を検索し、ユーザによってＭＰＡ内に提供された受信済みＡＣと比較する。２つの値が同一の場合には処理が続行される。
【０２３６】
（ステップ２５０４）SALT_Uを生成してこれを、ＣＤＢ内のUser_IDの隣のユーザレコード内に格納する。
【０２３７】
（ステップ２５０６）与えられたDevice_ID及びMD_Fingerprintについて、装置データベース（ＤＤＢ）内にユーザ装置についてのエントリを作成する。
【０２３８】
（ステップ２５０８、２５１０）SALT_Dを生成して、H_2D = H2(MD_Fingerprint, SALT_D)を計算する（図１７のステップ１７０２に関する説明も参照）。
【０２３９】
（ステップ２５１２）(H2_D, SALT_D)をＤＤＢ内のDevice_IDと対応するレコードに記録する。
【０２４０】
（ステップ２５１４）図１７のステップ１７０８の説明に準拠してTMK_MDを計算する。
【０２４１】
（ステップ２５１６）ATC = 0の場合においてSK*_MDを計算するのにTMK_MDを用いるのであって、一部の実施形態では、上述の図１８のステップ１８０２の説明のようにするこ

とができる。
【０２４２】
（ステップ２５１８）ウォレットサーバのトークントランザクション処理に対して、新たなチャレンジ値RANDを生成するように依頼する。
【０２４３】
（ステップ２５２０）HASH_D =H1(RAND, H2_D)を計算するのであり、これは上述の図１８のステップ１８０６についての説明に準拠してなされることができる。
【０２４４】
（ステップ２５２２）SUK*_MD = SK*_MD FnH HASH_Dを計算するのであり、これは上述の図１８のステップ１８０８についての説明に準拠してなされることができる。
【０２４５】
（ステップ２５２４）SALT_U及びH2_DをＭＰＡ／ユーザ装置へと送信する。
【０２４６】
図２６は、ＭＰＡ／ユーザ装置によって後に行われることができるプロセスを表すフローチャートである。
【０２４７】
{SALT_U, H2_D}をサーバから受信した後に、ＭＰＡ／ユーザ装置は、以下の処理を行うことができる。
【０２４８】
「初期化されていない」の状態で処理を開始する。
【０２４９】
（ステップ２６０２、図２６）ＡＴＣ＝０の場合、指数＝１にてＤＢＥ内で書き込みオペレーションを行って、{SALT_U, H2_D}を格納する。
【０２５０】
（ステップ２６０４）セキュアなエミュレートされたＰＩＮＰａｄをポップアップさせて、認証に付するべきウォレットＰＩＮを選択させて、これをWSP_AU_PINの第１の値として捕捉する。
【０２５１】
（ステップ２６０６）ユーザにＰＩＮの選択を確認させて、WSP_AU_PINの第２の値を捕捉する。
【０２５２】
（ステップ２６０６の続き；ステップ２６０８）WSP_AU_PINについて捕捉された２つの値を比較し、これらが合致する場合には、つぎのように計算：

H2_U = H2(WSP_AU_PIN, SALT_U)

【０２５３】
（ステップ２６１０）ＤＷＢコンストラクトの初期化を実行するのであり、これは、図２２の説明で言及された手法及び本願開示の図２２以前の説明の手法に従ってなされることができるのであり；一部の実施形態では、EKTR = SWB-E[K_{SYS}](K_{TR})は次のようにしてより正確に表現できる：

EKTR = AES256-E[K_{SYS}](K_{TR}, SALT_U, H2_D, H2_U)

【０２５４】
（ステップ２６１２）ＥＫＴＲをサーバへと送信する。
【０２５５】
図２７は、ウォレットサーバによって後に行われることができるプロセスを表すフローチャートである。
【０２５６】
ＥＫＴＲを受信する際には、ウォレットサーバは以下の処理を行うことができる：
【０２５７】
（ステップ２７０２、図２７）以前に初期化したシステム鍵K_{SYS}を用いてデジタルエンベロープＥＫＴＲを開封して、ストリングたるＳを得る：

S = AES256-I[KSYS](EKTR)

【０２５８】

（ステップ２７０４）ストリングＳにおいて、SALT_U及びH2_Dとして表される既知のパターンを識別する。これら復元された２つの値が以前送られたものに等しい場合にのみ続行する。

【０２５９】

（ステップ２７０６）消費者装置に対応するトランスポート鍵K_{TR}をH2_Uと共に検索する。

【０２６０】

（ステップ２７０８）Device_IDと関連付けてＤＤＢ内にK_{TR}をセキュアな態様で格納する。

【０２６１】

（ステップ２７１０）ＣＤＢ内において、H2_UをSALT_Uの隣に格納する。

【０２６２】

（ステップ２７１２）ESUK*_MD = AES256-E[KTR](SUK*_MD)を計算するのであり、これは、上述において図１８のステップ１８１０との関連で述べられた態様でなされ得る。

【０２６３】

（ステップ２７１４）サーバはESUK*_MDをＭＰＡ／ユーザ装置へと送る。

【０２６４】

ESUK*_MDをサーバから受信した後、ＭＰＡ／ユーザ装置は、（現在はゼロである）ＡＴＣ＝ＡＴＣ＿ｃｒｔの場合、これを指数＝２においてＤＢＥに書き込む。この暗号がユーザ認証プロトコルの第１回目の実行時に役割を果たすのであり、強化された装置認証機能を行うための暗号鍵を提供することになる。ＭＰＡは「初期化段階は完了されたのでＯＫです」とのメッセージをサーバに送り、自身の内部状態を「初期化されていない」から「初期化された」に変更する。

【０２６５】

成功したＭＰＡ初期化についてのコンファメーションを受信した後、サーバはＤＤＢ内のDevice_IDに対応するレコードをバリデートし、ＣＤＢ内のUser_IDを有するユーザレコードに追加された新たなアイテムをバリデートする。両方のレコードに対して、状態フィールドに「ACTIVE」との値を記録する。これによって、ウォレットサーバ内でのユーザ及びその者の装置についての初期化が完了する。

【０２６６】

本願開示のユーザ及び装置認証処理は、オンライン支払セキュリティに関する関連規則や要求を便利で費用対効果に優れる態様で満たすことができるのであり、同時に簡単で不必要に複雑化していないユーザエクスピリエンスを提供できる。また、開示した少なくとも幾つかの処理においては、埋め込み型セキュア要素やＳＩＭカード上での支払セキュリティ実装等のハードウェアベースドセキュリティ機能につきまとう費用及び負担をもたらさずにして、極めて高度なセキュリティ及び信頼性を提供できる。また、開示した諸々の処理は既存の支払インフラを様々な観点から新規な態様で活用することができるのであり、開示したユーザ／装置認証ソリューションの費用対効果にさらに貢献し得る。

【０２６７】

ユーザ及び／又は装置認証はオンライン購入トランザクションとの関連で上述したが、一部の実施形態では、同一の又は類似のユーザ及び／又は装置認証プロトコルを次のような店舗内（in-store）購入トランザクションに適用することができる：「店舗通路内（in-aisle）」型トランザクション又はＰＯＳ端末に向かっている顧客／ユーザのための小売店ロケーション内におけるＰＯＳ端末活用型トランザクション。

【０２６８】

開示された例示的実施形態においては、２要素認証アプローチが提示されており、該アプローチでは「あなたが有する何か」（コンピューティング装置内に格納された装置に特有なソフトウェアオンリーな認証データを、有するコンピューティング装置）と「あなた

が知っている何か」（ＰＩＮ又は他の秘密の情報／パスワード等）とが要求される。もっとも、他の実施形態では、「あなたが知っている何か」型認証要素の代わりに又はそれに加えて、「あなたが何であるか」／バイオメトリック型認証要素を用いることができる。例えば、ユーザ装置は指紋スキャン機能を有していることができ、ユーザ証明データ（ＰＩＮ型ユーザ認証の場合には、WSP_AU_PINと表記。）は、ユーザの指紋をスキャンすることによって得られた結果から導出された１以上の標準形式のデータ要素を含むことができる。他のタイプのバイオメトリック測定値を追加的に又は代替的に使用することもできる。

【０２６９】

本明細書及び添付の特許請求の範囲で使用される「秘密コード」という用語は、（装置ユーザによって一般的には秘密とされている）装置ユーザに知られているＰＩＮ、パスワード、又は他の一連の文字を含み、ウォレットサーバによって提供されるサービスにアクセスするために用いられる装置内に格納されているか否かは問われない。開示された多数の実施形態では、ＰＩＮは次の期間以外にはユーザ装置内に格納されないことに留意されたい：認証セッション中の限られた期間であって、ＰＩＮの入力後から、ユーザ装置内での暗号処理の入力としてＰＩＮが用いられる迄の期間。

【０２７０】

本明細書及び添付の特許請求の範囲で使用される「直前」又は「直後」という用語は、一連の事象における事象の相対位置を表すものであり、必ずしも時間的な近接性を示唆するわけではない。

【０２７１】

本明細書及び添付の特許請求の範囲で使用される「支払アプリケーション」という用語は、コンピューティング装置にダウンロードされたモバイルウォレットアプリケーション、ブラウザ拡張又はウェブページを含む。

【０２７２】

「コンピューティング装置」という用語は、パソコン、タブレットコンピュータ及びスマートフォンを含む。

【０２７３】

「パソコン」又は「ＰＣ」という用語は、ラップトップコンピュータ及びノートブックコンピュータを含む。

【０２７４】

開示された処理においては、現在のトランザクションと後続のトランザクションとは、所与のユーザ装置による一連のトランザクションにおいて互いに隣り合っていることができるが、時間（hour）単位又は日（day）単位で時間的に離隔されていることがあることに留意されたい（例えば、２４時間以上離れていることがある。）。

【０２７５】

本明細書及び添付の特許請求の範囲で使用される「電子商取引」という用語は、商人のオンラインストアを介して及び／若しくは「店舗通路内」購買／支払を介してなされる購入又はインターネットを介して又は遠隔サーバ若しくは他のコンピュータとのモバイルアプリケーションの対話を介して支払がなされる類いの他のトランザクションを含む。

【０２７６】

本明細書及び添付の特許請求の範囲で使用される「コンピュータ」という用語は、単一のコンピュータ又は２以上の相互通信するコンピュータを包括するものと解されるべきである。

【０２７７】

本明細書及び添付の特許請求の範囲で使用される「プロセッサ」という用語は、単一のプロセッサ又は２以上の相互通信するプロセッサを包括するものと解されるべきである。

【０２７８】

本明細書及び添付の特許請求の範囲で使用される「メモリ」という用語は、単一のメモリ若しくは記憶装置又は２以上のメモリ若しくは記憶装置を包括するものと解されるべき

である。

【０２７９】

本明細書及び添付の特許請求の範囲で使用される「サーバ」という用語は、サービス要求を送出するクライアントたる他の装置からの多数のサービス要求に応答するコンピュータ装置又はシステムを含む。

【０２８０】

本明細書にて開示されるフローチャート及び説明に関して、開示される方法のステップの実施順序が限定されないことを理解されたい。むしろ、実行可能な任意の順序で方法のステップを実施することができるのであり、少なくとも一部のステップを同時に実施することも可能である。

【０２８１】

本明細書及び添付の特許請求の範囲で使用される「支払カードシステム口座」という用語は、クレジットカード口座、口座保有者がデビットカード使用時にアクセスする入金口座、プリペイドカード口座、又は、支払トランザクションを完結させることができる任意の他のタイプの口座を含む。「支払カードシステム口座」、「支払カード口座」及び「支払口座」という用語は本明細書では可換なものとして用いられる。「支払カード口座番号」という用語には、支払カードシステム口座を識別する番号又は支払カードが保持する番号、又は、デビットカード及び／若しくはクレジットカードトランザクションを扱う支払システム内でトランザクションをルーティングするために使用される番号が含まれる。「支払カード」という用語には、クレジットカード、デビットカード、プリペイドカード、又は他のタイプの支払手段（それが実際に物理的なカードであるか仮想的なものであるかは問わない）。

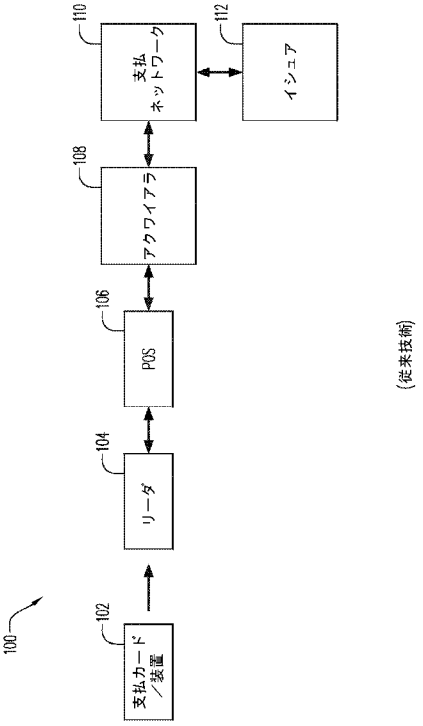
【０２８２】

本明細書及び添付の特許請求の範囲で使用される「支払カードシステム」という用語は、購入トランザクション及び関連トランザクションを取り扱うためのシステムを意味する。このようなシステムの一例としては、本件譲受人たるMasterCard International Incorporatedによって運営されているシステムを挙げることができる。一部の実施形態では、「支払カードシステム」との用語は、加盟金融機関が個人、事業体及び／又は他の団体に対して支払カード口座を与えるシステムに限定され得る。

【０２８３】

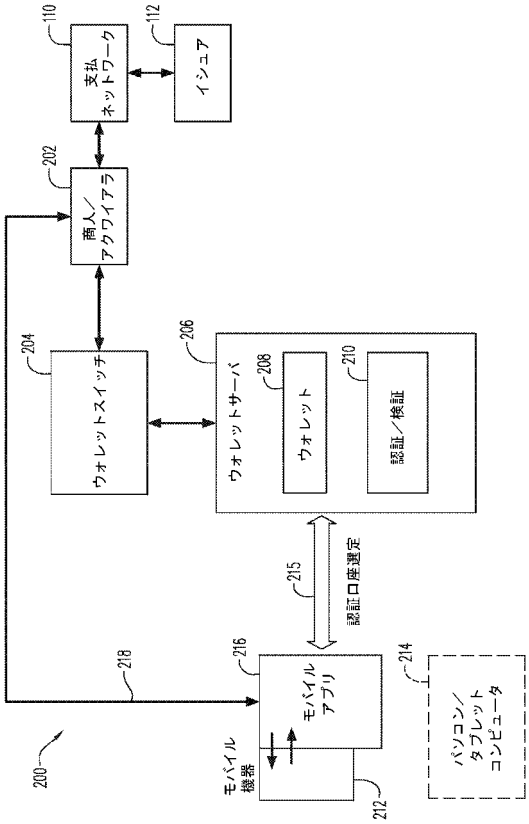
特定の例示的な実施形態と関連付けて本発明を説明したが、添付の特許請求の範囲に記載した本発明の精神及び範囲から逸脱することなく、開示された実施形態に当業者に明らかな様々な変更、置換、及び改変を行うことができることを理解されたい。

【図１】

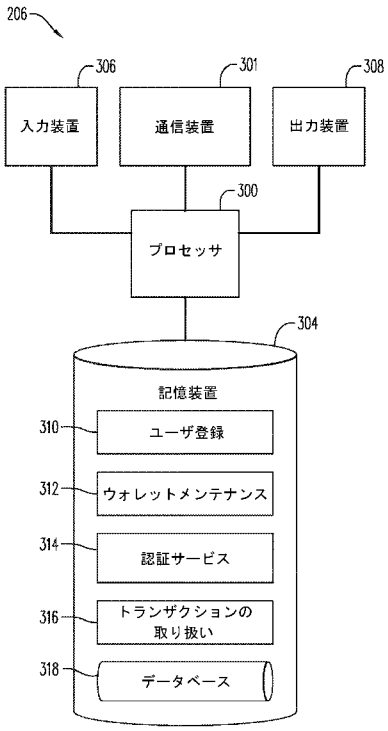


（従来技術）

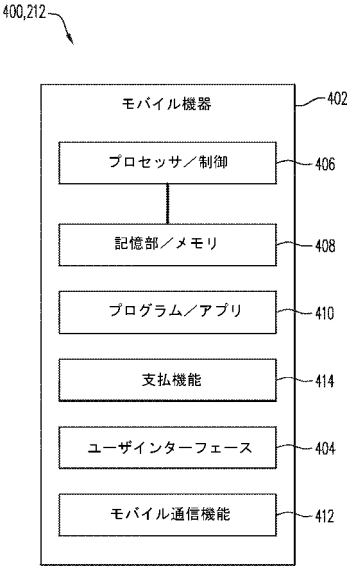
【図２】



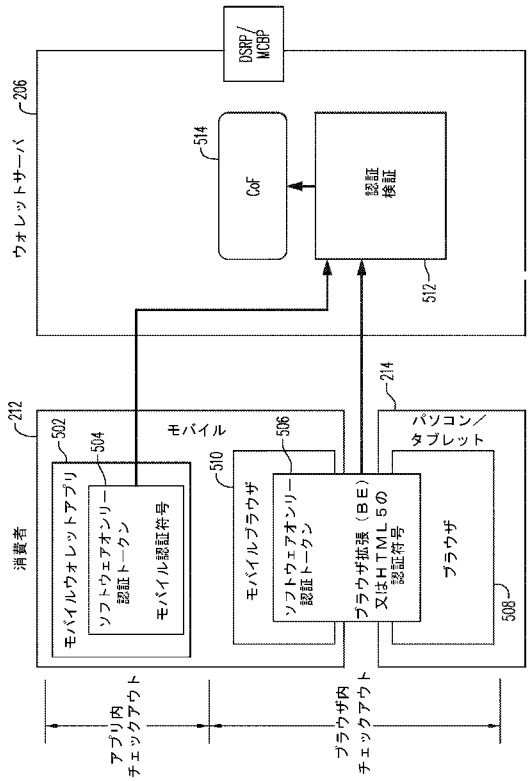
【図３】



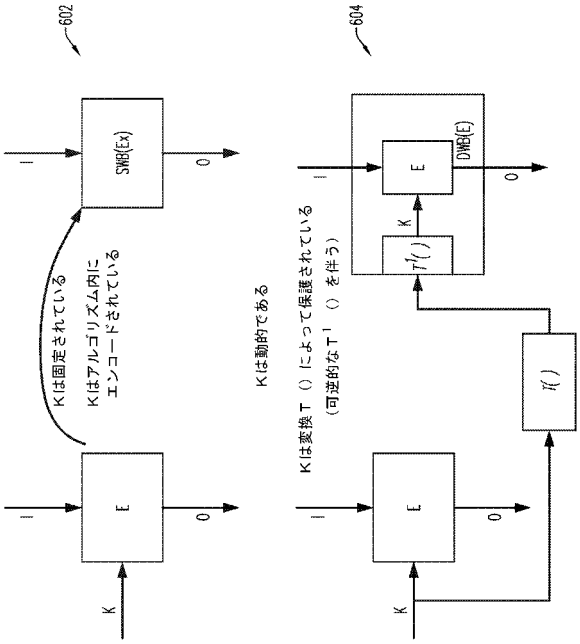
【図４】



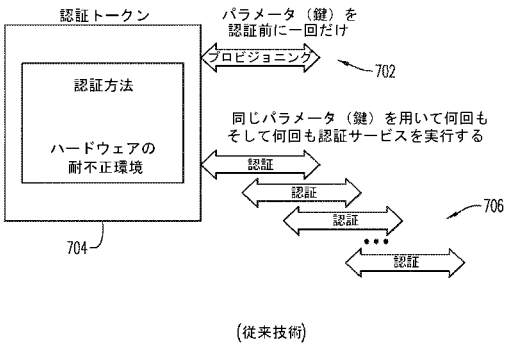
【図５】



【図６】

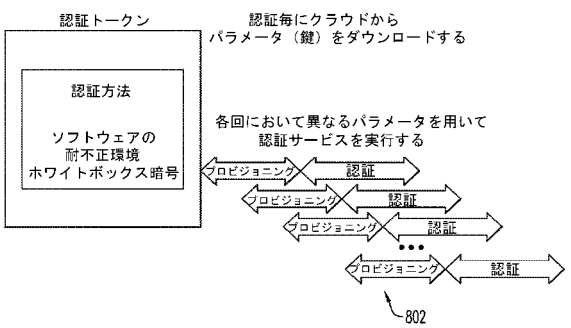


【図７】

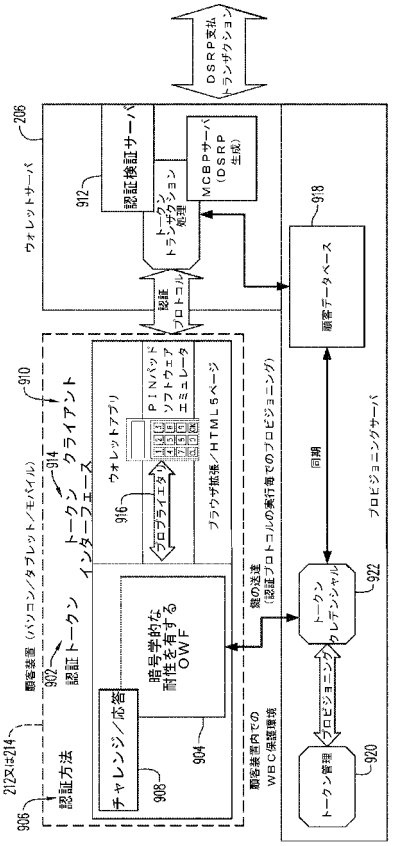


(従来技術)

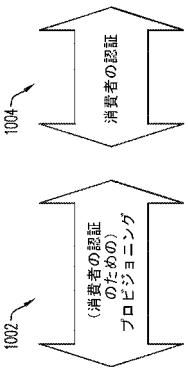
【図８】



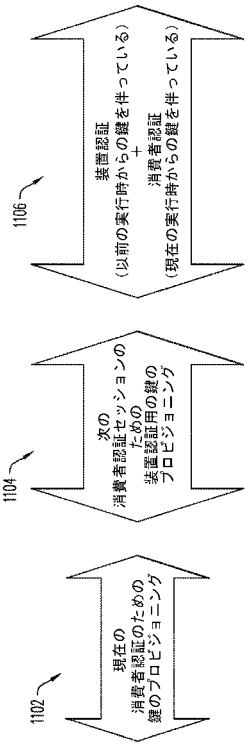
【図９】



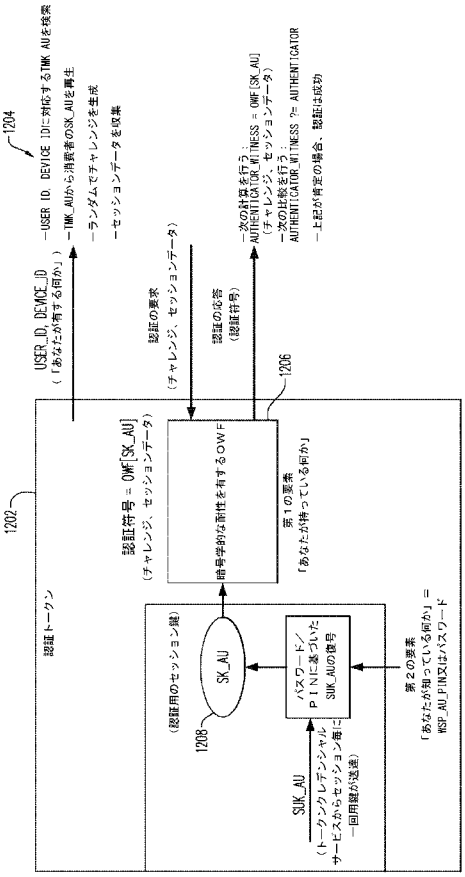
【図１０】



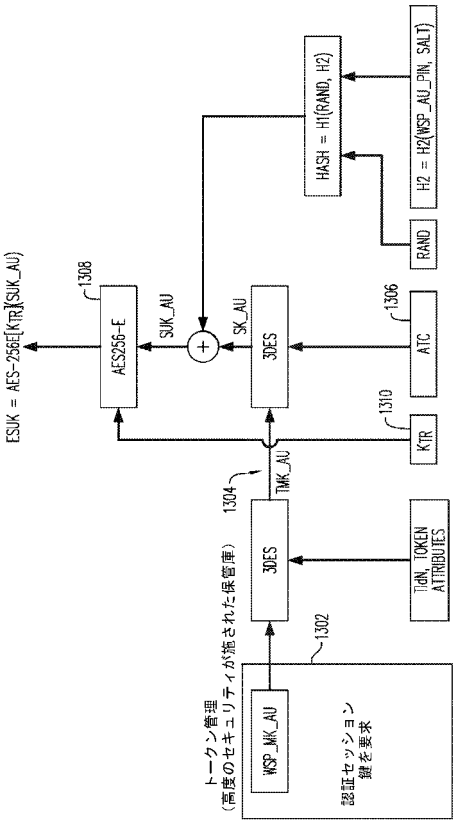
【図１１】



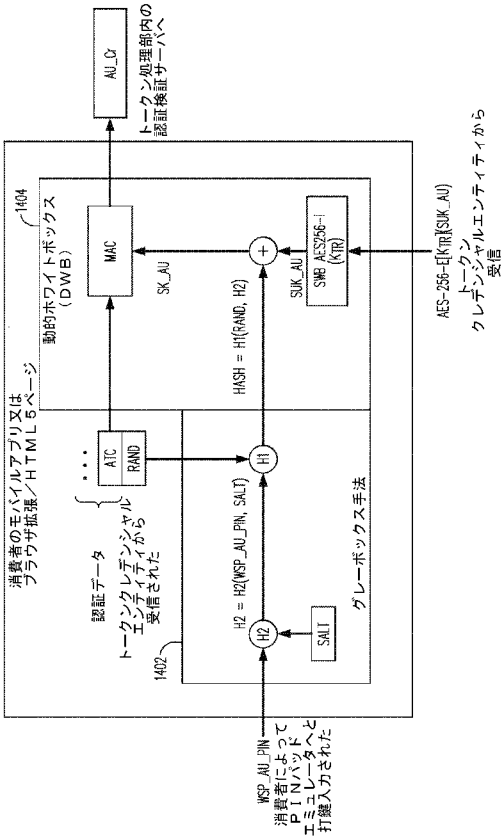
【図１２】



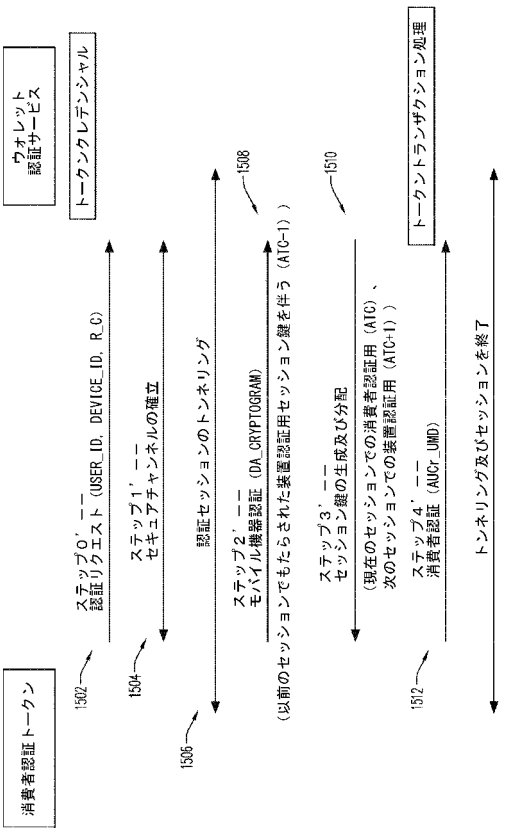
【図１３】



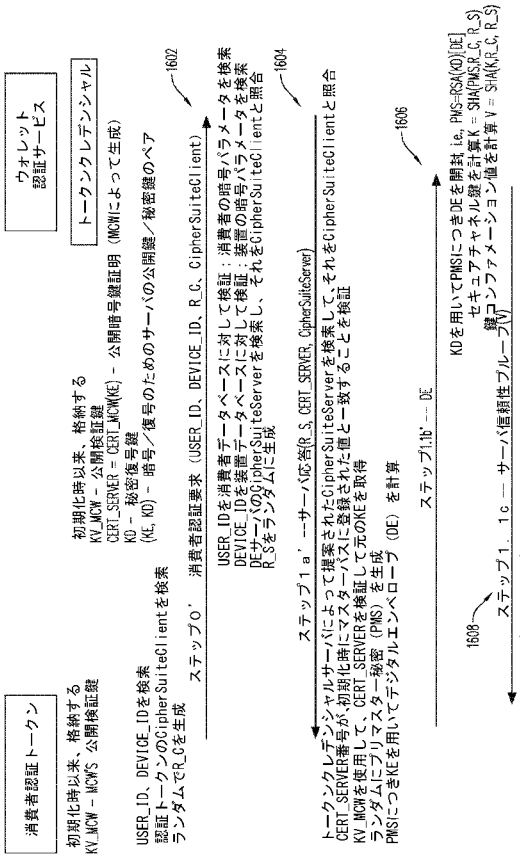
【図１４】



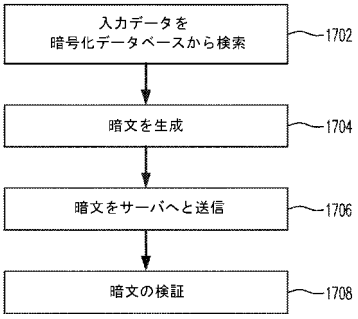
【図１５】



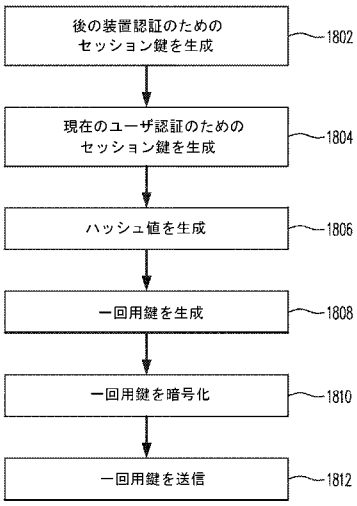
【図１６】



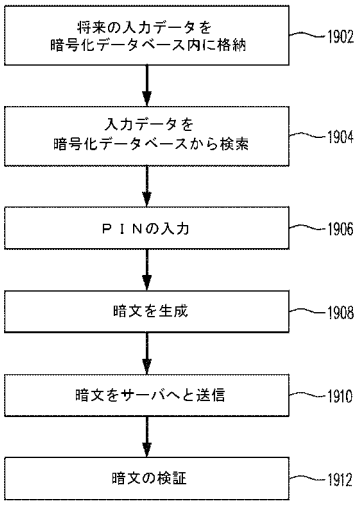
【図１７】



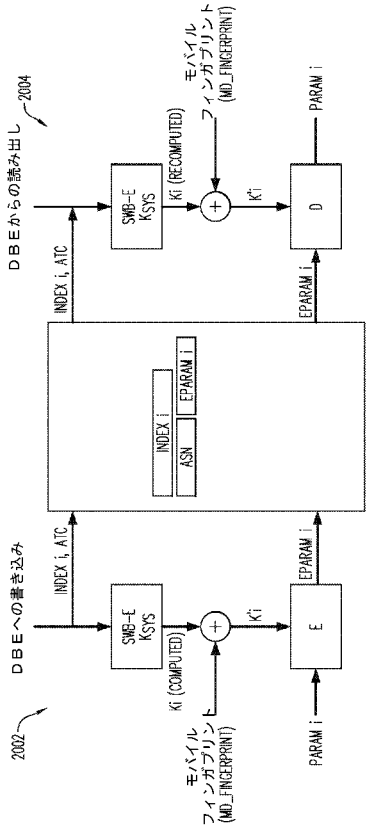
【図１８】



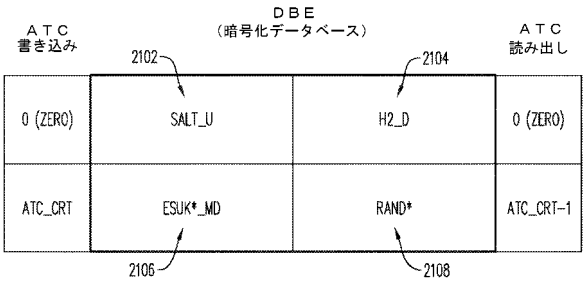
【図１９】



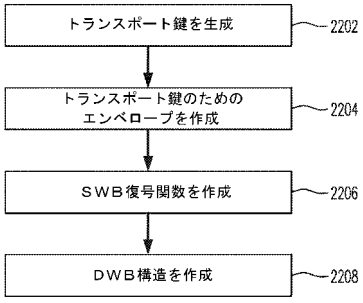
【図２０】



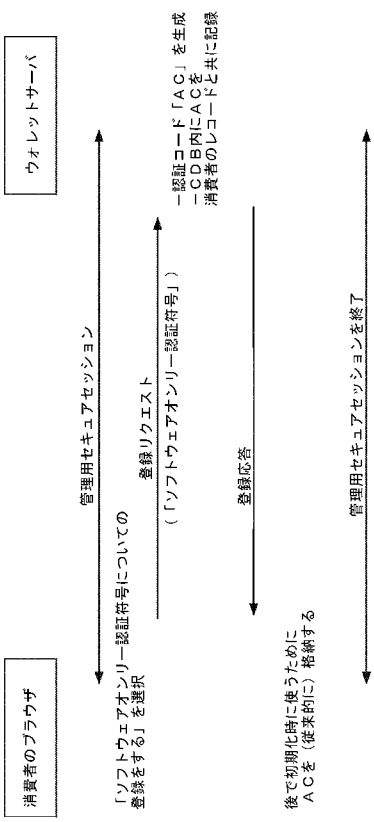
【図２１】



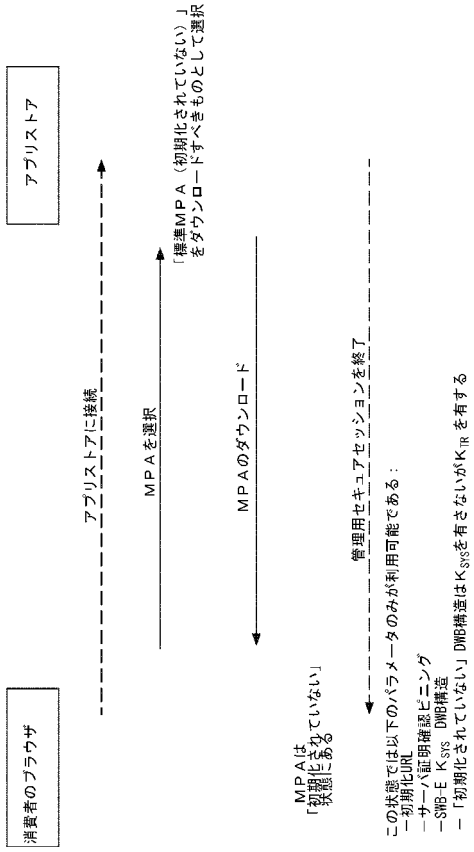
【図２２】



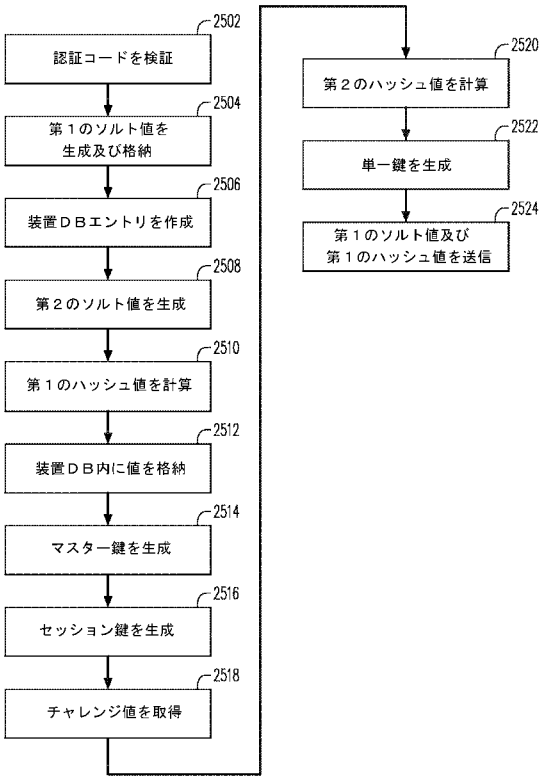
【図２３】



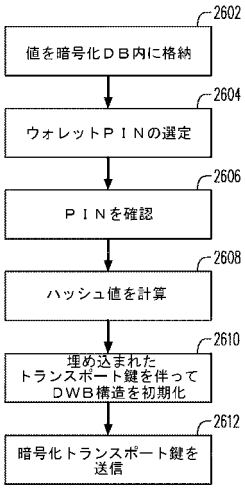
【図２４】



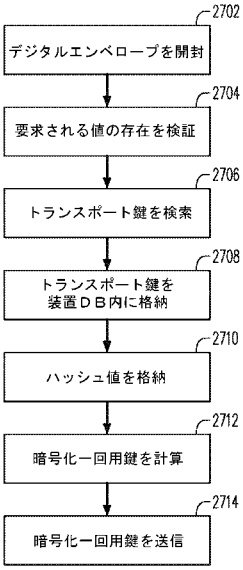
【図２５】



【図２６】



【図２７】


2702
デジタルエンベロープを開封
2704
要求される値の存在を検証
2706
トランスポート鍵を検索
2708
トランスポート鍵を
装置ＤＢ内に格納
2710
ハッシュ値を格納
2712
暗号化一回用鍵を計算
2714
暗号化一回用鍵を送信

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/037159

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06Q20/40(2012.01)i

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)

Int.Cl. G06Q20/40

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2016
Registered utility model specifications of Japan 1996-2016
Published registered utility model applications of Japan 1994-2016

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	US 2014/0358796 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 2014.12.04, paragraphs [0032], [0050] & GB 2514780 A & WO 2014/195320 A1 & EP 3005264 A1 & CA 2914042 A1 & CN 105593886 A	1,4 2-3,5-8,15 18-23
Y	US 2015/0124963 A1 (CERTIVOX LTD.) 2015.05.07, paragraphs [0139], [0401] & WO 2014/191768 A2 & EP 3005608 A2 & KR 10-2016-0013905 A	2-3,5-8, 16-17
Y	US 2007/0255661 A1 (YOSHIDA, Takuya) 2007.11.01, paragraphs [0078], [0083] & JP 2006-119771 A & CN 1773546 A	5-7

☑ 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
28.09.2016	11.10.2016

Name and mailing address of the ISA/JP
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan

Authorized officer
YAMAMOTO, Masashi 5L 3786
Telephone No. +81-3-3581-1101 Ext. 3562

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/037159

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2011/0004557 A1 (Ynjiun P.Wang) 2011.01.06, paragraph [0056] & JP 2003-517658 A & WO 2001/069388 A1 & EP 1272933 A1 & TW 560159 B & AU 2002247213 A	6-7
X Y	WO 2009/051989 A1 (DRESSER, INC.) 2009.04.23, page 18, line 33 - page 19, line 2, Figs.1-4, claims 1-44 & EP 2210392 A1 & CA 2702833 A1 & US 2009/0103725 A1	9-10 7, 11-17
Y	JP 2015-95208 A (TOPPAN PRINTING CO., LTD) 2015.05.18, paragraph [0053] (No Family)	11-13
Y	US 2015/0156176 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 2015.06.04, Fig.13 & WO 2015/084755 A1 & AU 2014357343 A & CA 2932105 A1	14

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

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,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

Fターム(参考) 5J104 AA07 AA16 EA17 KA01 KA02 KA04 KA21 MA05 NA02 NA03
NA37 PA07 PA10
5L055 AA75