(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2018-532301
(P2018-532301A)
(43)公表日　平成30年11月1日(2018.11.1)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675B	5J104
G06F 21/32	(2013.01)	G06F	21/32		
G06F 21/64	(2013.01)	H04L	9/00	673D	
		G06F	21/64		
		H04L	9/00	675D	

審査請求 未請求　予備審査請求 未請求　（全 22 頁）

(21)出願番号　特願2018-510966 (P2018-510966)
(86)(22)出願日　平成28年8月18日 (2016.8.18)
(85)翻訳文提出日　平成30年4月26日 (2018.4.26)
(86)国際出願番号　PCT/CN2016/095855
(87)国際公開番号　WO2017/032263
(87)国際公開日　平成29年3月2日 (2017.3.2)
(31)優先権主張番号　201510534755.4
(32)優先日　平成27年8月27日 (2015.8.27)
(33)優先権主張国　中国 (CN)

(71)出願人　505032849
アリババ　グループ　ホウルディング　リミテッド
英国領ケイマン諸島　グランド　ケイマン　ジョージ　タウン　ピーオーボックス　８４７　ワン　キャピタル　プレイス　フォース　フロア
(74)代理人　100097320
弁理士　宮川　貞二
(74)代理人　100100398
弁理士　柴田　茂夫
(74)代理人　100131820
弁理士　金井　俊幸
(74)代理人　100155192
弁理士　金子　美代子

最終頁に続く

(54)【発明の名称】本人認証方法及び装置

(57)【要約】
本願の実施例は本人認証方法及び装置に関する。当該方法は、端末デバイスによってサービス要求を受信し、前記サービス要求に従ってユーザの第１の生体認証情報を収集するステップと、前記第１の生体認証情報を、予め設定された生体認証情報と比較し、前記比較が前記第１の生体認証情報と前記予め設定された生体認証情報との一致を示す場合に、予め記憶されているデジタル署名証明プライベートキーを読み出すステップと、前記デジタル署名証明プライベートキーに従って前記サービス要求にデジタル署名し、生体情報検証メッセージを生成するステップと、前記生体情報検証メッセージをサーバへ送信することにより、前記サーバが、前記デジタル署名証明プライベートキーに対応する予め記憶されているデジタル署名証明パブリックキーを読み出し、前記デジタル署名証明パブリックキーに従って前記生体情報検証メッセージの検証及び署名を行った後に、認証結果情報を前記端末デバイスへ戻すステップとを備える。これにより、ユーザによる決済操作の安全性と利便性を向上することができる。

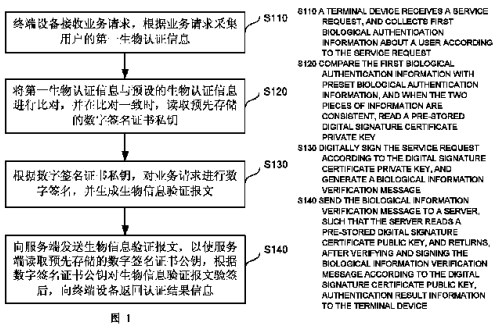

図１

【特許請求の範囲】
【請求項１】
端末デバイスによってサービス要求を受信し、前記サービス要求に従ってユーザの第１の生体認証情報を収集するステップと；
前記第１の生体認証情報を、予め設定された生体認証情報と比較し、前記比較が前記第１の生体認証情報と前記予め設定された生体認証情報との一致を示す場合に、予め記憶されているデジタル署名証明プライベートキーを読み出すステップと；
前記デジタル署名証明プライベートキーに従って前記サービス要求にデジタル署名し、生体情報検証メッセージを生成するステップと；
前記生体情報検証メッセージをサーバへ送信することにより、前記サーバが、前記デジタル署名証明プライベートキーに対応する予め記憶されているデジタル署名証明パブリックキーを読み出し、前記デジタル署名証明パブリックキーに従って前記生体情報検証メッセージの検証及び署名を行った後に、認証結果情報を前記端末デバイスへ戻す、ステップとを備える；
本人認証方法。
【請求項２】
前記デジタル署名証明プライベートキー及び前記デジタル署名証明パブリックキーを生成及び記憶するステップを更に備え；
前記デジタル署名証明プライベートキー及び前記デジタル署名証明パブリックキーを生成及び記憶する前記ステップは：
端末デバイスにより登録要求を受信し、前記登録要求に従って、前記ユーザの第２の生体認証情報を収集するステップと；
前記比較が前記第２の生体認証情報と前記予め設定された生体認証情報との一致を示す場合に、前記第２の生体認証情報に対応する前記デジタル署名証明プライベートキー及び前記デジタル署名証明パブリックキーを生成し、前記デジタル署名証明プライベートキーを記憶するステップと；
第１の予め設定されたプライベートキーに従って前記登録要求にデジタル署名した後に、前記デジタル署名証明パブリックキーを担持する登録要求メッセージを生成するステップと；
前記登録要求メッセージを前記サーバへ送信することにより、前記サーバが、前記第１の予め設定されたプライベートキーに対応する第１の予め設定されたパブリックキーに従って前記登録要求メッセージの検証及び署名が成功した後に、前記デジタル署名証明パブリックキーを記憶するステップとを備える；
請求項１に記載の方法。
【請求項３】
前記生体認証情報は、指紋情報、顔画像情報、及び音声情報のうち１つ以上を備える；
請求項１又は２に記載の方法。
【請求項４】
前記第２の生体認証情報に対応する前記デジタル署名証明プライベートキー及び前記デジタル署名証明パブリックキーを生成する前記ステップは：
前記ユーザのＩＤと、前記端末デバイスのＩＤと、一致を示す比較の結果情報とに従って、前記第２の生体認証情報に対応する前記デジタル署名証明プライベートキー及び前記デジタル署名証明パブリックキーを生成するステップを備える；
請求項２に記載の方法。
【請求項５】
前記端末デバイスよって登録要求を受信し、前記登録要求に従って前記ユーザの前記第２の生体認証情報を収集する前記ステップは：
前記端末デバイスにより、前記登録要求を前記サーバへ送信するステップと；
前記登録要求に従って前記サーバから戻された応答メッセージを受信するステップと；
前記応答メッセージの検証及び署名を行い、前記検証及び署名の成功後に、前記ユーザ

の前記第２の生体認証情報を収集するステップとを備える；
請求項２に記載の方法。
【請求項６】
前記登録要求メッセージを前記サーバへ送信する前記ステップは：
前記端末デバイスにより、前記ユーザが有効なユーザであるかどうかを検証するステップと；
前記ユーザが有効なユーザである場合には、オリジナルの決済パスワードをチェックし、前記チェックが成功した場合には、前記登録要求メッセージを前記サーバへ送信するステップとを備える；
請求項２に記載の方法。
【請求項７】
前記方法は決済中における本人認証に適用され、前記サービス要求は決済要求である；
請求項１、２、及び請求項４乃至６のいずれか１項に記載の方法。
【請求項８】
収集ユニット、読み出しユニット、生成ユニット、及び送信ユニットを備え；
前記収集ユニットは、サービス要求を受信し、前記サービス要求に従って、ユーザの第１の生体認証情報を収集するように構成され；
前記読み出しユニットは、前記収集ユニットが収集した前記第１の生態認証情報を予め設定された生体認証情報と比較し、前記比較が前記第１の生体認証情報と前記予め設定された生体認証情報との一致を示す場合に、予め記憶されているデジタル署名証明プライベートキーを読み出すように構成され；
前記生成ユニットは、前記読み出しユニットが読み出した前記デジタル署名証明プライベートキーに従って、前記サービス要求にデジタル署名し、生体情報検証メッセージを生成するように構成され；
前記送信ユニットは、前記生成ユニットが生成した前記生体情報検証メッセージをサーバへ送信し、これにより、前記サーバが、前記デジタル署名証明プライベートキーに対応する予め記憶されているデジタル署名証明パブリックキー読み出し、そして前記デジタル署名証明パブリックキーに従って前記生体情報検証メッセージの検証及び署名を行った後に、認証結果情報を端末デバイスへ戻すように構成される；
本人認証装置。
【請求項９】
前記収集ユニットは登録要求を受信し、前記登録要求に従って前記ユーザの第２の生体認証情報を収集するように更に構成され；
前記生成ユニットは、前記比較が、前記収集ユニットが収集した前記第２の生体認証情報と前記予め設定された生体認証情報とが一致することを示す場合に、前記第２の生体認証情報に対応するデジタル署名証明プライベートキー及びデジタル署名証明パブリックキーを生成し、前記デジタル署名証明プライベートキーを記憶するように更に構成され；
前記生成ユニットは、第１の予め設定されたプライベートキーに従って前記登録要求がデジタル署名された後に、前記デジタル署名証明パブリックキーを含む登録要求メッセージを生成するように更に構成され；
前記送信ユニットは、前記生成ユニットが生成した前記登録要求メッセージを前記サーバへ送信し、これにより、前記サーバが、第１の予め設定されたパブリックキーに従った前記登録要求メッセージの検証及び署名の成功後に、前記デジタル署名証明パブリックキーを記憶できるように更に構成され、前記第１の予め設定されたプライベートキーは前記第１の予め設定されたパブリックキーに対応する；
請求項８に記載の装置。
【請求項１０】
前記生体認証情報は、指紋情報、顔画像情報、及び音声情報のうち１つ以上を備える；
請求項８又は９に記載の装置。
【請求項１１】

前記生成ユニットは、具体的に：
前記第２の生体認証情報に対応する前記デジタル署名証明プライベートキー及び前記デジタル署名証明パブリックキーを、前記ユーザのＩＤと、前記端末デバイスのＩＤと、一致を示す比較の結果情報とに従って生成するように構成される；
請求項９に記載の装置。
【請求項１２】
前記収集ユニットは、具体的に：
前記登録要求を前記サーバへ送信し；
前記登録要求に従って前記サーバから戻された応答メッセージを受信し；
前記応答メッセージの検証及び署名を行い、前記検証及び署名の成功後に、前記ユーザの前記第２の生体認証情報を収集するように構成される；
請求項９に記載の装置。
【請求項１３】
前記送信ユニットは、具体的に：
前記ユーザが有効なユーザであるかどうかを検証し；
前記ユーザが有効なユーザである場合に、オリジナルの決済パスワードをチェックし、前記チェックが成功した場合に、前記登録要求メッセージを前記サーバへ送信するように構成される；
請求項９に記載の装置。
【請求項１４】
前記装置は決済中の本人認証に適用され、前記サービス要求は決済要求である；
請求項８、９、及び請求項１１乃至１３のいずれか１項に記載の装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本願はコンピュータ技術の分野に関し、詳しくは本人認証方法及び装置に関する。
【背景技術】
【０００２】
従来技術においては、一般的に、ユーザが入力したパスワード（例えば６桁の数字列）を検証することによりユーザの身元を認証し、ユーザはこの身元認証後にサービスオペレーションを実行することができる。しかし、この場合、ユーザは普段からパスワードを憶えておかねばならないため、ユーザによる使用の利便性は大きく削がれてしまう。そのうえ、このパスワードは本質的に固定パスワードのままであるため、パスワードが盗難に遭った場合、盗難後のユーザの資産の安全に重大な脅威を引き起こすことがある。
【発明の概要】
【０００３】
本願の実施の形態は、ユーザが実行するサービスオペレーションの安全性と利便性を向上させることができる本人認証方法及び装置を提供する。
【０００４】
第１の態様に係る本人認証方法が提供される。当該方法は、端末デバイスによってサービス要求を受信し、前記サービス要求に従ってユーザの第１の生体認証情報を収集するステップと、前記第１の生体認証情報を、予め設定された生体認証情報と比較し、前記比較が前記第１の生体認証情報と前記予め設定された生体認証情報との一致を示す場合に、予め記憶されているデジタル署名証明プライベートキーを読み出すステップと、前記デジタル署名証明プライベートキーに従って前記サービス要求にデジタル署名し、生体情報検証メッセージを生成するステップと、前記生体情報検証メッセージをサーバへ送信することにより、前記サーバが、前記デジタル署名証明プライベートキーに対応する予め記憶されているデジタル署名証明パブリックキーを読み出し、前記デジタル署名証明パブリックキーに従って前記生体情報検証メッセージの検証及び署名を行った後に、認証結果情報を前

記端末デバイスへ戻すステップとを備える。
【０００５】
第２の態様に係る本人認証装置が提供される。当該装置は、収集ユニット、読み出しユニット、生成ユニット、及び送信ユニットを備え、前記収集ユニットは、サービス要求を受信し、前記サービス要求に従って、ユーザの第１の生体認証情報を収集するように構成され、前記読み出しユニットは、前記収集ユニットが収集した前記第１の生態認証情報を予め設定された生体認証情報と比較し、前記比較が前記第１の生体認証情報と前記予め設定された生体認証情報との一致を示す場合に、予め記憶されているデジタル署名証明プライベートキーを読み出すように構成され、前記生成ユニットは、前記読み出しユニットが読み出した前記デジタル署名証明プライベートキーに従って、前記サービス要求にデジタル署名し、生体情報検証メッセージを生成するように構成され、前記送信ユニットは、前記生成ユニットが生成した前記生体情報検証メッセージをサーバへ送信し、これにより、前記サーバが、前記デジタル署名証明プライベートキーに対応する予め記憶されているデジタル署名証明パブリックキー読み出し、そして前記デジタル署名証明パブリックキーに従って前記生体情報検証メッセージの検証及び署名を行った後に、認証結果情報を端末デバイスへ戻すように構成される。
【０００６】
本願が提供する本人認証方法及び装置によれば、収集された生体認証情報を、予め設定された生体認証情報と比較することにより、両者の一致が判明すると、端末デバイスは、予め記憶されているデジタル署名証明プライベートキーを用いて署名された生体情報検証メッセージをサーバへ送信し、続いてサーバが、予め記憶されているデジタル署名証明パブリックキーに従って生体情報検証メッセージの検証及び署名を行うことで、ユーザの身元検証が達成される。これにより、ユーザが実行するサービス操作の安全性と利便性を向上させることができる。
【図面の簡単な説明】
【０００７】
【図１】本願の実施の形態による本人認証方法のフローチャートである。
【図２】本願の別の実施の形態による本人認証方法の情報のやり取りの概略図である。
【図３】本願の更に別の実施の形態による本人認証装置の概略図である。
【発明を実施するための形態】
【０００８】
本願の実施の形態の目的、技術的解決策、及び利点をもっと明瞭にするために、添付の図面を参照しながら、本願の実施の形態における技術的解決策を明瞭且つ完全に以下説明する。ここに記載する実施の形態は、明らかに本願の全ての実施の形態ではなく、そのうちのいくつかである。当業者が、創造的な努力をともなうことなく本願の実施の形態に基づいて得たその他の実施の形態は、全て本願の保護範囲に属する。
【０００９】
本願の実施の形態を理解し易くすることを目的に、特定の実施の形態を添付の図面を併用して以下説明するが、これらの実施の形態は本願の実施の形態を限定するものではない。
【００１０】
本願の実施の形態で提供される本人認証方法及び装置は、サービスオペレーションを実行するユーザの身元を認証するシナリオに適用される。このシナリオは、例えば、決済システムを用いて決済操作を実行するユーザの身元を認証できるシナリオである。
【００１１】
本願の実施の形態では、決済工程におけるユーザの身元の認証を一実施例（例えば、サービス要求は決済要求である）として用い、その他のサービスオペレーションを実行するユーザの身元の認証方法も同様であることに注目されたい。そのため、本願では詳細について述べない。
【００１２】

決済システムは決済クライアントと決済サーバとを含む。決済クライアントには第１のセキュリティコンポーネントがパックされている。第１のセキュリティコンポーネントはセキュリティクライアントとも呼ばれる、又は「決済セキュリティチェックサービス」（すなわち「ａｌｉｐａｙＳｅｃモジュール」）と呼ばれ、デジタル署名アルゴリズム、セキュリティクライアントプライベートキー、セキュリティサーバパブリックキー、及び新たに生成されたデジタル署名証明プライベートキーを記憶するように構成される。端末デバイスが生体認証情報の識別をサポートしているか、生体認証情報が記録されているか、及び、ユーザが入力した生体認証情報が検証されたかどうか、並びに、情報及びアルゴリズムへの安全なアクセスをチェックするべく収集モジュールを呼び出すために、セキュリティクライアントはオペレーティングシステムを用いて端末デバイスの収集モジュール（例えば、指紋センサ）と直接通信しても良く、又は、端末デバイス提供者によって提供された信頼された実行環境と直接通信しても良い。

【００１３】

加えて、決済サーバには第２のセキュリティコンポーネントもパックされている。第２のセキュリティコンポーネントはセキュリティサーバ又は「生体コア」（すなわち「ｂｉｃ　ｓｙｓｔｅｍ」）とも呼ばれ、認証チャレンジ情報を生成するように構成され、更に、デジタル署名アルゴリズム、セキュリティクライアントパブリックキー、セキュリティサーバプライベートキー、ポエダー（ｐｏｅｄｅｒ）システムにて書かれた生体認証情報の登録合意書（例えば、指紋の登録合意書）、及び新たに生成されたデジタル署名証明パブリックキーを記憶するように構成される。セキュリティサーバはセキュリティクライアントに対応する。

【００１４】

本願にて提供される端末デバイスには、限定されないが、モバイルフォン、モバイルコンピュータ、タブレットコンピュータ、パーソナルデジタルアシスタント（ＰＤＡ）、メディアプレーヤ、スマートテレビ、スマートウォッチ、スマートグラス、スマートリストバンド等が含まれる。端末デバイス上のオペレーティングシステムは、ＩＯＳシステム、Ａｎｄｒｏｉｄシステム、又はその他のシステムであってよい。加えて、本願の端末デバイスには決済クライアントがインストールされており、更に、収集モジュールを実装している。収集モジュールは、具体的には、オペレーティングシステムに配設されたハードウェアデバイスであってよく、又、指紋センサ、カメラ、マイクロフォン等であってよい。

【００１５】

図１は、本願の実施の形態による本人認証方法のフローチャートである。この方法は、処理機能を有するデバイス、すなわちサーバ、又はシステム、又は装置により実行されてもよい。図１に示すように、この方法は具体的に以下を含む。

【００１６】

ステップ１１０。端末デバイスがサービス要求を受信し、このサービス要求に従ってユーザの第１の生体認証情報を収集する。

【００１７】

つまり、端末デバイスの決済クライアントがサービス要求を受信し、セキュリティクライアントを用いて第１の収集命令を収集モジュールへ送信することで、収集モジュールがユーザの第１の生体認証情報を収集し、セキュリティクライアントへ戻すことができるようになる。

【００１８】

サービス要求は決済要求であることが好ましい。実施において、決済要求は、ユーザが決済クライアントの「決済（Ｐａｙ）」ボタンをクリックすることでトリガされてよい。

【００１９】

ここで述べる生体認証情報とは、指紋情報、顔画像情報、及び音声情報のうち１つ以上を含む。本明細書では、指紋情報を生体認証情報として用いて説明する。予め設定された生体認証情報は、端末デバイスの収集モジュールによって事前に収集され、ユーザを一意に識別できる情報であってよい。例えば、予め設定された生体認証情報が、予め設定され

た指紋情報である場合、端末デバイスは、指紋センサを用いて事前にユーザの指紋情報を収集し、この収集した指紋情報を、予め設定した指紋情報としてローカルに記憶する。ここで述べる予め設定した指紋情報は、収集した実際の指紋情報を、予め設定されたアルゴリズムに従い対応して計算することで得られることが分かるであろう。例えば、指紋センサは１０本の指の指紋情報を事前に収集し、次に、１０本の指の指紋情報の平均値を計算し、最終的に予め設定された指紋情報を得ることができる。

【００２０】

オプションではあるが、本方法は、ステップ１１０の前に、デジタル署名証明プライベートキー及びデジタル署名証明パブリックキーを生成し、これらを記憶するステップを更に含んでもよい。このステップでは、ユーザの生体認証情報を決済サーバにアップロードするのではなく端末デバイスでローカルな記憶のみ行い、決済工程にてユーザの身元を認証することもできる。

【００２１】

具体的なステップは次の通りである：

【００２２】

ステップ１１０１。端末デバイスが登録要求を受信し、この登録要求に従ってユーザの第２の生体認証情報を収集する。

【００２３】

ステップ１１０１において、端末デバイスによって登録要求を受信し、この登録要求に従ってユーザの第２の生体認証情報を収集するステップは、具体的に以下のステップ含んでもよい：

【００２４】

ステップＡ：端末デバイスが登録要求をサーバへ送信する。

【００２５】

すなわち、端末デバイスの決済クライアントが登録要求を決済サーバへ送信すると、この登録要求を受信した決済サーバが、セキュリティサーバを呼び出すことによって認証チャレンジ情報を読み出す。認証チャレンジ情報は、セキュリティサーバが、登録要求のために生成されたランダム文字列に、予め設定されたセキュリティサーバプライベートキーを用いてデジタル署名を行った後に生成されてよい。

【００２６】

ステップＢ：登録要求に従ってサーバから戻された応答メッセージを受信する。

【００２７】

ここで決済クライアントは応答メッセージを受信できる。好ましくは、応答メッセージは、決済サーバがセキュリティサーバを用いて読み出した認証チャレンジ情報であってよい。

【００２８】

ステップＣ：応答メッセージの検証及び署名を行い、更に、検証及び署名の成功後に、ユーザの第２の生体認証情報を収集する。

【００２９】

すなわち、決済クライアントは、セキュリティクライアントを呼び出すことで、受信した認証チャレンジ情報を検証し、これに署名する。具体的には、セキュリティクライアントは、予め設定されたセキュリティサーバパブリックキーに従って認証チャレンジ情報の検証及び署名を行い、更に、この検証及び署名の成功後に、第２の収集命令を収集モジュールへ送信することで、収集モジュールが、第２の収集命令に従ってユーザの第２の生体認証情報を収集できるようになる。

【００３０】

生体認証情報が指紋情報である実施例を用いて説明する。決済クライアントは、まず、ユーザが入力した登録要求を受信し、この登録要求の受信後に第１の呼び出しメッセージをセキュリティクライアントへ送信する。ここで、第１の呼び出しメッセージを用いて、ユーザが現在用いている端末デバイスが指紋決済をサポートしているかどうか、予め設定

された指紋情報が指紋センサに記憶されているかどうかを調べるべく、セキュリティクライアントにチェックを行うよう命令する。ここで、セキュリティクライアントは、具体的には、サービスhardwarePayExecute(type=QUICKPAY_REQUEST_TYPE_INIT)を呼び出すことで、ユーザが現在用いている端末デバイスが指紋決済をサポートしているかどうか、予め設定された指紋情報が指紋センサに記憶されているかどうかをチェックする。端末デバイスが指紋決済をサポートしており、予め設定された指紋情報が指紋センサに記憶されている場合には、セキュリティクライアントが、指紋決済がサポートされていることを示す情報を決済クライアントへ戻すことで、決済クライアントがスライドボタンをユーザに対して表示できるようにする。決済クライアントは、スライドボタンに対してなされたスライド命令（すなわち、ユーザが指紋決済の機能を登録したい）を受信すると、ユーザに対して法的文書を表示する。

【００３１】

ユーザが入力した承認命令を決済クライアントが受信した場合、表示された法的文書をユーザが閲覧し、「理解しました」を選択すると、承認命令がトリガされる。決済クライアントは登録要求を決済サーバへ送信する。すなわち、決済クライアントが、サービスgetBiometricRegRequestPRC（デバイスＩＤ、モバイルフォンのデバイスモデル、及びログイン済みユーザのユーザＩＤ）を呼び出すことにより登録要求を決済サーバへ送信することで、決済サーバは、セキュリティサーバへ第２の呼び出しメッセージを送信できるようになる。例えば、決済サーバは、サービスmobileBiometricService.getRegRequestを呼び出すことによって第２の呼び出しメッセージを送信する。セキュリティサーバは、第２の呼び出しメッセージを受信すると、現在のタイムスタンプ等の情報に従ってランダム文字列を生成し、セキュリティサーバに予め記憶されているセキュリティサーバプライベートキー（つまり、予め設定されたセキュリティサーバプライベートキー）を用いて、上記で生成されたランダム文字列にデジタル署名し、認証チャレンジ情報を生成し、更に、この生成した認証チャレンジ情報を決済サーバへ戻す。決済サーバは、認証チャレンジ情報を読み出した後、これを決済クライアントへ転送する。セキュリティクライアントは、今受信した認証チャレンジ情報がセキュリティサーバから送信されたものであるかどうかを判定するために、又、今受信した認証チャレンジ情報が修正されているかどうかを判定するために、認証チャレンジ情報を検証し、これに署名する。セキュリティクライアントが、今受信した認証チャレンジ情報がセキュリティサーバから送信されたものであり、送信された認証チャレンジ情報が修正されていないと判定した場合には、セキュリティクライアントとセキュリティサーバとの間のデータチャネルが安全であることを示す。これにより、指紋センサ（つまり収集モジュール）へ第２の収集命令を送信することができ、この第２の収集命令を受信した収集モジュールがユーザの第２の生体認証情報を収集する。

【００３２】

ステップ１１０２。第２の生体認証情報が予め設定された生体認証情報と一致することが比較によって示された場合には、第２の生体証明情報に対応するデジタル署名証明プライベートキー及びデジタル署名証明パブリックキーを生成し、デジタル署名証明プライベートキーを記憶する。

【００３３】

すなわち、収集モジュールは、収集命令に従ってユーザの第２の生体認証情報を収集した後、セキュリティクライアントが、第２の生体認証情報を、予め設定された生体認証情報と比較できるように、第２の生体認証情報をセキュリティクライアントへ戻し、第２の生体認証情報と予め設定された生体認証情報との一致が比較によって示された場合には、第２の生体認証情報に対応するデジタル署名証明プライベートキー及びデジタル署名証明パブリックキーを生成し、デジタル署名証明プライベートキーを記憶する。

【００３４】

セキュリティクライアントが、第２の生体認証情報に対応するデジタル署名証明プライベートキー及びデジタル署名証明パブリックキーを生成するステップを実行する前に、本方法は：

セキュリティクライアントが、決済クライアントから送信された第１のメッセージを受信するステップを更に含む。この第１のメッセージは、ユーザの一意の識別子（ＩＤ）及び端末デバイスのＩＤを含む。

【００３５】

第２の生体認証情報に対応するデジタル署名証明プライベートキー及びデジタル署名証明パブリックキーを生成するステップは：

セキュリティクライアントが、ユーザのＩＤと、端末デバイスのＩＤと、一致を示す比較の結果情報とに従って、第２の生体認証情報に対応するデジタル署名証明プライベートキー及びデジタル署名証明パブリックキーを生成するステップを含む。

【００３６】

ここでユーザのＩＤは決済システムによって生成され、ユーザを一意に識別するために用いられる情報であってよい。実施において、ユーザのＩＤはセッションから直接読み出してよい。端末デバイスのＩＤは、国際移動体識別番号（ＩＭＥＩ）であってよい。加えて、セキュリティクライアントによる比較が第２の生体認証情報と予め設定された生体認証情報との一致を示す場合には、デジタル署名証明パブリックキー及びデジタル署名証明プライベートキーを生成する。そのため、デジタル署名証明プライベートキー及びデジタル署名証明パブリックキーは、第２の生体認証情報に対応するデジタル署名証明プライベートキー及びデジタル署名証明パブリックキーとも呼ばれる。一致を示す比較の結果情報は、第２の生体認証情報と予め設定された生体認証情報との一致を示す比較の結果情報であることに更に注目されたい。

【００３７】

デジタル署名証明パブリックキー及びデジタル署名証明プライベートキーの生成後に、セキュリティクライアントがデジタル署名証明プライベートキーを記憶する。実施において、端末デバイスのオペレーションシステムがアンドロイド（Ａｎｄｒｏｉｄ）システムである場合、デジタル署名証明プライベートキーをセキュリティクライアントのＴＥＥに記憶することができる。

【００３８】

当然ながら、実際の使用では、指紋決済、画像認識決済、及び音声決済を最初に登録すると、端末デバイスは、第２の生体認証情報を収集した後に、この生体認証情報に対応するデジタル署名証明パブリックキー及びデジタル署名証明プライベートキーを直接的に生成できるが、第２の生体認証情報を予め設定された生体認証情報と比較する必要はなく、この比較が第２の生体認証情報と予め設定された生体認証情報との一致を示す場合に限って生成ステップを実行する。

【００３９】

ステップ１１０３。第１の予め設定されたプライベートキーに従って登録要求にデジタル署名した後に、登録要求メッセージを生成する。ここで登録要求メッセージはデジタル署名証明パブリックキーを含む。

【００４０】

ここでは、第１の予め設定されたプライベートキーは予め設定されたセキュリティクライアントプライベートキーであってよい、すなわち、セキュリティクライアントは、予め設定されたセキュリティクライアントプライベートキーを用いて登録要求にデジタル署名した後に、登録要求メッセージを生成する。

【００４１】

留意すべきは、登録要求は同時に認証チャレンジ情報を含んでよいということであり、それは、すなわち認証チャレンジ情報及びデジタル署名証明パブリックキーを同時にデジタル署名してから、登録要求メッセージを生成するということである。

【００４２】

ステップ１１０４。登録要求メッセージをサーバへ送信し、サーバが、第１の予め設定されたパブリックキーに従って登録要求メッセージの検証及び署名を行った後に、デジタル署名証明パブリックキーを記憶できるようにする。ここで、第１の予め設定されたパブ

リックキーには第１の予め設定されたプライベートキーが対応する。
【００４３】
ここで第１の予め設定されたパブリックキーは予め設定されたセキュリティクライアントパブリックキーであってよい、つまり、セキュリティクライアントが登録要求メッセージを決済クライアントへ送信し、決済クライアントが決済サーバを介して登録要求メッセージをセキュリティサーバへ転送し、次に、セキュリティサーバが、予め設定されたセキュリティクライアントパブリックキーに従って登録要求メッセージの検証及び署名を行い、検証及び署名の成功後に、デジタル署名証明パブリックキーを記憶する。
【００４４】
オプションではあるが、ステップ１１０４にて、登録要求メッセージをサーバへ送信するステップは以下のステップを含む：
端末デバイスによって、ユーザが有効なユーザであるかどうかを検証するステップ。及び、
ユーザが有効なユーザの場合にはオリジナルの決済パスワードをチェックし、チェックの成功後に登録要求メッセージをサーバへ送信するステップ。
【００４５】
実施例において、決済クライアントは、まず現在のユーザにバインドされているモバイルフォン番号を取得して、そのモバイルフォン番号のモバイルフォンへショートメッセージを送信し、その後、承認を示すメッセージを受信したら、ユーザが入力したオリジナル決済パスワードを受信し、このオリジナル決済パスワードのチェックの成功後に、決済サーバを用いて登録要求メッセージをセキュリティサーバへ転送できる。これにより、現在のユーザが決済クライアントのユーザであるかどうかを検証できるため、決済操作の安全性を向上させることができる。
【００４６】
ここで決済クライアントは、具体的に、サービスregisterBiometricPRC（デバイスＩＤ、モバイルフォンデバイスモデル、指紋登録メッセージ、ログイン済みユーザのＵＩＤ）を呼び出すことにより、登録要求メッセージを決済サーバへ送信できる。決済サーバが登録要求メッセージをセキュリティサーバへ転送した後に、セキュリティサーバは、予め設定されたセキュリティクライアントパブリックキーに従って登録要求メッセージの検証及び署名を行い、検証及び署名の成功後に、デジタル署名証明パブリックキーを登録要求メッセージに記憶する。ここで、予め設定されたセキュリティクライアントプライベートキーは、予め設定されたセキュリティクライアントパブリックキーに対応する。加えて、登録要求メッセージの検証及び署名の成功後に、検証及び署名の成功を示すメッセージを決済サーバへ戻すこともできる。次に、決済サーバが、検証及び署名が成功した旨を示すメッセージを決済クライアントへ戻す。これにより、決済クライアントは、指紋情報、顔画像情報、及び音声情報等を入力することで決済工程にて本人身元が認証される旨、及び、決済金額は別の端末デバイスのセキュリティレベルに対応する旨をユーザに表示できる。
【００４７】
デジタル署名証明プライベートキー及びデジタル署名証明パブリックキーを生成及び記憶するステップを実行した後、ユーザは、決済システムを用いて注文決済を行う際に、指紋情報、顔画像情報、及び音声情報を入力することによって本人身元を認証でき、本人認証の成功後に決済操作を実行できる。
【００４８】
ステップ１２０。第１の生体認証情報を予め設定された生体認証情報と比較し、この比較が、第１の生体認証情報と予め設定された生体認証情報との一致を示す場合には、予め記憶されているデジタル署名証明プライベートキーを読み出す。
【００４９】
すなわち、セキュリティクライアントは、第１の生体認証情報を、予め設定された生体認証情報と比較し、この比較が第１の生体認証情報と予め設定された生体認証情報との一致を示す場合に、予め記憶されているデジタル署名証明プライベートキーを読み出す。

【００５０】
ステップ１３０。デジタル署名証明プライベートキーに従ってサービス要求にデジタル署名し、生体情報検証メッセージを生成する。
【００５１】
決済シナリオの下では、サービス要求は決済要求であってよい。つまり、セキュリティクライアントは、読み出したデジタル署名証明プライベートキーに従って決済要求にデジタル署名して、生体情報検証メッセージを生成し、次に、生成した生体情報検証メッセージを決済クライアントへ送信する。
【００５２】
ステップ１４０。生体情報検証メッセージをサーバへ送信する。これにより、サーバが、デジタル署名証明プライベートキーに対応する予め記憶されているデジタル署名証明パブリックキーを読み出し、次に、デジタル署名証明パブリックキーに従って生体情報検証メッセージに検証及び署名を行った後に、認証結果情報を端末デバイスへ戻す。
【００５３】
決済クライアントが、生体情報検証メッセージを決済サーバへ送信する。これにより、決済サーバは、デジタル署名証明プライベートキーに対応する予め記憶されているデジタル署名証明パブリックキーをセキュリティサーバから読み出し、デジタル署名証明パブリックキーに従って生体情報検証メッセージの検証及び署名を行った後に、認証結果情報を決済クライアントへ戻すことができる。
【００５４】
当然ながら、実際の使用では、決済クライアントが送信されたサービス要求を暗号化している場合には、決済サーバは更に、デジタル署名証明パブリックキーに従って生体情報検証メッセージの検証及び署名を行った後に、この暗号化されたサービス要求を予め設定されたアルゴリズムに従って復号化し、復号化が成功した場合に限って、認証が成功したかどうかの結果情報を決済クライアントへ戻す必要がある。
【００５５】
ここで、本願に関与するデジタル署名と、デジタル署名の検証とは先行技術に属するものであり、デジタル署名及び検証する対象のみが異なることに留意すべきである。当業者は先行技術を参照して実施を達成することができる。そのため、本願ではこの工程についての説明を繰り返さない。
【００５６】
本願で提供される本人認証方法及び装置に従って、端末デバイスは、収集した生体認証情報が、予め設定された生体認証情報と一致することを比較により示された場合に、予め記憶されているデジタル署名証明プライベートキーを用いて署名された生体情報検証メッセージをサーバへ送信し、次に、サーバが、予め記憶されているデジタル署名証明パブリックキーに従ってこの生体情報検証メッセージの検証及び署名を行うことで、ユーザの身元の検証の目的を達成する。これにより、ユーザが実行するサービス操作の安全性と利便性を向上させることができる。
【００５７】
以下の実施の形態を、指紋決済を登録し、指紋決済の登録後に、指紋情報の検証によってユーザの身元を証するという実施例を用いて説明する。
【００５８】
図２は、本願の別の実施の形態による本人認証方法の情報のやり取りの図である。図２に示すように、この方法は具体的に以下のステップを含んでよい：
【００５９】
ステップ２１０。決済クライアントは、受信した登録要求に従って、第１の呼び出しメッセージをセキュリティクライアントへ送信する。
【００６０】
第１の呼び出しメッセージは、現在、ユーザが用いている端末デバイスが指紋決済をサポートしているかどうか、又、予め設定された指紋情報が指紋センサに記憶されているか

どうかをチェックするようにセキュリティクライアントに命令するために用いられる。
【００６１】
セキュリティクライアントは、具体的に、サービスhardwarePayExecute（type=QUICKPAY_REQUEST_TYPE_INIT）を呼び出すことで、現在、ユーザが用いている端末デバイスが指紋決済をサポートしているかどうか、そして、予め設定された指紋情報が指紋センサに記憶されているかどうかをチェックする。
【００６２】
ステップ２２０。セキュリティクライアントは、サポートの情報を決済クライアントへ戻す。
【００６３】
ステップ２３０。決済クライアントは登録要求を決済サーバへ送信する。
【００６４】
決済クライアントは、サービスgetBiometricRegRequestPRC（デバイスＩＤ、モバイルフォンデバイスモデル、ログイン済みユーザのユーザＩＤ）を呼び出すことで、登録要求を決済サーバへ送信する。
【００６５】
ステップ２４０。決済サーバは、受信した登録要求に従って、第２の呼び出しメッセージをセキュリティサーバへ送信する。
【００６６】
決済サーバは、サービスmobileBiometricService.getRegRequestを呼び出すことで、第２の呼び出しメッセージをセキュリティサーバへ送信する。
【００６７】
ステップ２５０。セキュリティサーバはランダム文字列を生成し、生成したこのランダム文字列に、予め設定されたセキュリティサーバプライベートキーを用いてデジタル署名した後に、認証チャレンジ情報を生成する。
【００６８】
ステップ２６０。セキュリティサーバが、生成された認証チャレンジ情報を決済サーバへ戻す。
【００６９】
ステップ２７０。決済サーバは、認証チャレンジ情報を決済クライアントへ転送する。
【００７０】
ステップ２８０。決済クライアントは、認証チャレンジ情報をセキュリティクライアントへ送信する。
【００７１】
決済クライアントは、具体的に、サービスhardwarePayExecute（type=QUICKPAY_REQUEST_TYPE_REGISTER,data＝認証チャレンジ情報）を呼び出すことにより、認証チャレンジ情報をセキュリティクライアントへ送信しても良い。
【００７２】
ステップ２９０。セキュリティクライアントは、予め設定されたセキュリティサーバパブリックキーに従って認証チャレンジ情報の検証及び署名を行い、検証及び署名の成功後に、第２の収集命令を端末デバイスの指紋センサへ送信する。
【００７３】
ステップ２１００。端末デバイスの指紋センサは、ユーザがリアルタイムで収集した第１の指紋情報をセキュリティクライアントへ送信する。
【００７４】
ステップ２１１０。比較が、リアルタイムで収集した第１の指紋情報と予め設定された指紋情報との一致を示す場合に、セキュリティクライアントは、ユーザの第１の指紋情報に対応するデジタル署名証明プライベートキー及びデジタル署名証明パブリックキーを生成し、デジタル署名証明プライベートキーを記憶する。
【００７５】

オプションではあるが、セキュリティクライアントは、決済クライアントが送信した第１のメッセージを受信する。ここで第１のメッセージは、ユーザの一意の識別子ＩＤと、端末デバイスのＩＤとを担持し；

第１の指紋情報に対応するデジタル署名証明プライベートキー及びデジタル署名証明パブリックキーを生成するステップは：

セキュリティクライアントにより、ユーザの第１の指紋情報に対応するデジタル署名証明プライベートキー及びデジタル署名証明パブリックキーを、ユーザのＩＤと、端末デバイスのＩＤと、一致を示す比較の結果情報とに従って生成するステップを含む。

【００７６】

一致を示す比較の結果情報は、リアルタイムで収集した第１の指紋情報と予め設定された指紋情報との一致を示す比較の結果情報であることに留意すべきである。

【００７７】

ステップ２１２０。セキュリティクライアントは、予め設定されたセキュリティクライアントプライベートキーを用いて認証チャレンジ情報にデジタル署名した後に、登録要求メッセージを生成する。ここで登録要求メッセージはデジタル署名証明パブリックキーを含む。

【００７８】

ステップ２１３０。セキュリティクライアントは、登録要求メッセージを決済クライアントへ送信する。

【００７９】

ステップ２１４０。決済クライアントは、検証要求を端末デバイスへ送信する。

【００８０】

ステップ２１５０。端末デバイスは、承認を示す応答メッセージを決済クライアントへ送信する。

【００８１】

ステップ２１６０。決済クライアントは、ユーザが入力したオリジナルの決済パスワードを受信し、オリジナルの決済パスワードが正しい場合に、決済サーバを用いて登録要求メッセージをセキュリティサーバへ転送する。

【００８２】

ステップ２１７０。セキュリティサーバは、予め設定されたクライアントサーバパブリックキーに従って登録要求メッセージの検証及び署名に成功した後に、登録要求メッセージに記憶されたデジタル署名証明パブリックキーを記憶する。

【００８３】

ステップ２１８０。セキュリティサーバは、検証及び署名が成功したことを示すメッセージを決済サーバへ戻す。

【００８４】

ステップ２１９０。決済サーバは、検証及び署名が成功したことを示すメッセージを決済クライアントへ転送する。

【００８５】

ステップ２２００。決済クライアントは、受信した決済要求に従って、第１の収集命令を、セキュリティクライアントを介して端末デバイスの指紋センサへ送信する。

【００８６】

第１の収集命令を用いて、ユーザの第２の指紋情報を収集してセキュリティクライアントへ戻すように、指紋センサに対して命令する。

【００８７】

ステップ２２１０。セキュリティクライアントは、指紋センサがリアルタイムで収集した第２の指紋情報を受信し、第２の指紋情報を、予め設定された指紋情報と比較する。

【００８８】

ステップ２２２０。第２の指紋情報と予め設定された指紋情報とが一致することを比較が示す場合に、予め記憶されているデジタル署名証明プライベートキーを読み出し、次に

デジタル署名証明プライベートキーを用いて決済要求メッセージにデジタル署名した後に、生体情報検証メッセージを生成する。

【００８９】

ステップ２２３０。セキュリティクライアントは決済クライアントを用いて、生体情報検証メッセージを決済サーバへ送信する。

【００９０】

ステップ２２４０。決済サーバは、事前に記憶されたデジタル署名証明パブリックキーをセキュリティサーバから読み出し、このデジタル署名証明パブリックキーに従って、生体情報検証メッセージの検証及び署名を行う。

【００９１】

ステップ２２５０。決済クライアントは、決済サーバから戻された、認証が成功であるかどうかを示すメッセージを受信し、認証が成功であることを示すメッセージの受信後に、決済操作を実行する。

【００９２】

要約すると、本願が提供する本人認証方法によれば、ユーザの指紋情報を収集するときに、セキュリティクライアントに記憶されたデジタル署名証明プライベートキーがアンロックされ、本人認証の最中に、指紋情報に代えてデジタル署名証明プライベートキーを用いて検証を実行し、これにより、オリジナルの決済パスワードを置き換える目的が達成され、ユーザによる決済操作の安全性と利便性を向上させることができる。

【００９３】

本願の実施の形態におけるステップ２１０乃至ステップ２１９０は、指紋決済登録手順と呼ぶこともできる。指紋決済登録手順は、任意の生体認証及び本人認証工程、例えば、虹彩、顔、リストバンドを用いた様々な安全性レベルにおける本人認証、に適用できることに更に留意されたい。

【００９４】

本人認証方法に対応して、本願の実施の形態は本人認証装置を更に提供する。図３に示すように、本装置は、収集ユニット３０１、読み出しユニット３０２、生成ユニット３０３、及び送信ユニット３０４を含む。

【００９５】

収集ユニット３０１は、サービス要求を受信し、このサービス要求に従ってユーザの第１の生体認証情報を収集するように構成される。

【００９６】

生体認証情報は、指紋情報、顔画像情報、及び音声情報のうちの一つ以上を含む。

【００９７】

読み出しユニット３０２は、収集ユニット３０１によって収集した第１の生体認証情報を、予め設定された生体認証情報と比較し、この比較が第１の生体認証情報と予め設定された生体認証情報との一致を示す場合には、予め記憶されているデジタル署名証明プライベートキーを読み出すように構成される。

【００９８】

生成ユニット３０３は、読み出しユニット３０２が読み出したデジタル署名証明プライベートキーに従ってサービス要求にデジタル署名し、生体情報検証メッセージを生成するように構成される。

【００９９】

送信ユニット３０４は、生成ユニット３０３により生成された生体情報検証メッセージをサーバへ送信することで、サーバがデジタル署名証明プライベートキーに対応する予め記憶されているデジタル署名証明パブリックキーを読み出し、更に、サーバが、デジタル署名証明パブリックキーに従って生体情報検証メッセージの検証及び署名を行った後に、認証結果情報を端末デバイスへ戻すことができるように、構成される。

【０１００】

収集ユニット３０１は更に、登録要求を受信し、この登録要求に従って、ユーザの第２

の生体認証情報を収集するように構成されても良い。
【０１０１】
収集ユニット３０１は、具体的には、登録要求をサーバへ送信し、この登録情報に従ってサーバから戻された応答メッセージを受信し、応答メッセージの検証及び署名を行い、検証及び署名の成功後にユーザの第２の生体認証情報を収集するように構成される。
【０１０２】
生成ユニット３０３は、比較により、収集ユニット３０１が収集した第２の生体認証情報と予め設定された生体認証情報との一致が示される場合に、第２の生体認証情報に対応するデジタル署名証明プライベートキー及びデジタル署名証明パブリックキーを生成し、デジタル署名証明プライベートキーを記憶するように更に構成される。
【０１０３】
生成ユニット３０３は、具体的には、ユーザのＩＤと、端末デバイスのＩＤと、一致を示す比較の結果情報とに従って、第２の生体認証情報に対応するデジタル署名証明プライベートキー及びデジタル署名証明パブリックキーを生成するように構成される。
【０１０４】
生成ユニット３０３は、第１のプライベートキーに従って登録要求にデジタル署名した後に、登録要求メッセージを生成するように更に構成される。ここで、登録要求メッセージはデジタル署名証明パブリックキーを含む。
【０１０５】
送信ユニット３０４は、生成ユニット３０３が生成した登録要求メッセージをサーバへ送信するように更に構成される。これにより、サーバは、第１の予め設定されたパブリックキーに従って登録要求メッセージの検証及び署名を行った後に、デジタル署名証明パブリックキーを記憶できる。ここで、第１の予め設定されたプライベートキーは第１の予め設定されたパブリックキーに対応する。
【０１０６】
送信ユニット３０４は、具体的に、ユーザが有効なユーザであるかどうかを検証し、ユーザが有効なユーザである場合にはオリジナルの決済パスワードをチェックし、更に、チェックが成功した場合には登録要求メッセージをサーバへ送信するように構成される。
【０１０７】
本人認証装置を、決済中における本人認証に適用しても良く、サービス要求は決済要求であっても良い。
【０１０８】
本願のこの実施の形態の装置における機能モジュールの機能は、この方法の実施の形態の様々なステップを介して実施できる。そのため、ここでは、本願にて提供される装置の特定の作動工程についての説明は繰り返さない。
【０１０９】
本願にて提供される本人認証装置によれば、収集ユニット３０１がサービス要求を受信し、このサービス要求に従ってユーザの第１の生体認証情報を収集する；読み出しユニット３０２が第１の生体認証情報を予め設定された生体認証情報と比較し、この比較が第１の生体認証情報と予め設定された生体認証情報との一致を示す場合には、予め記憶されているデジタル署名証明プライベートキーを読み出す；生成ユニット３０３が、デジタル署名証明プライベートキーに従ってサービス要求にデジタル署名し、生体情報検証メッセージを生成する；送信ユニット３０４が生体情報検証メッセージをサーバへ送信する。これにより、サーバがデジタル署名証明プライベートキーに対応する予め記憶されているデジタル署名証明パブリックキーを読み出せるようになり、次に、サーバが、デジタル署名証明パブリックキーに従って生体情報検証メッセージの検証及び署名を行った後に、認証結果情報を端末デバイスへ戻す。これにより、ユーザによる決済操作の安全性と利便性を向上させることができる。
【０１１０】
専門家は、ここで開示された実施の形態の中で述べた実施例を組み合わせることで、目

的及びアルゴリズムステップを、電子ハードウェア、コンピュータソフトウェア、又はこれらの組み合わせによって実施できることを更に理解すべきである。ハードウェアとソフトウェアの相互交換性を明確に説明するために、上記では、例示の組み合わせ及びステップを機能ごとに総体的に述べた。機能をハードウェア方式で実行するかソフトウェア方式で実行するかは、技術的解決策の特定の用途及び設計上の制約条件によって異なる。当業者は、ここで述べた機能を、特定の用途のための異なる方法を用いて実施できるが、この実施は本願の範囲を超えるものとみなすべきではない。

【０１１１】

ここで開示された実施の形態との組み合わせにおいて述べた方法ステップ又はアルゴリズムステップは、ハードウェア、プロセッサにより実行されるソフトウェアモジュール、又はこれらの組み合わせによって実施できる。ソフトウェアモジュールは、ランダムアクセスメモリ（ＲＡＭ）、メモリ、読み出し専用メモリ（ＲＯＭ）、消去可能なプログラマブルＲＯＭ（ＥＰＲＯＭ）、電気的に消去可能なプログラマブルＲＯＭ（ＥＥＰＲＯＭ）、レジスタ、ハードディスク、リムーバブルハードディスク、ＣＤ－ＲＯＭ、又は、当該技術で周知な他のいずれかの形態の記憶媒体に搭載できる。

【０１１２】

上で述べた特定の実施は、本願の目的、技術的解決策、有益な効果を詳細に更に説明している。上で述べた説明は、本願の特定の実施にすぎず、本願の保護範囲を限定するためではないことを理解すべきである。本願の主旨及び原理の範囲におけるあらゆる変更、均等物の置き換え、改良などは、全て本願の保護範囲に含まれる。

【図１】

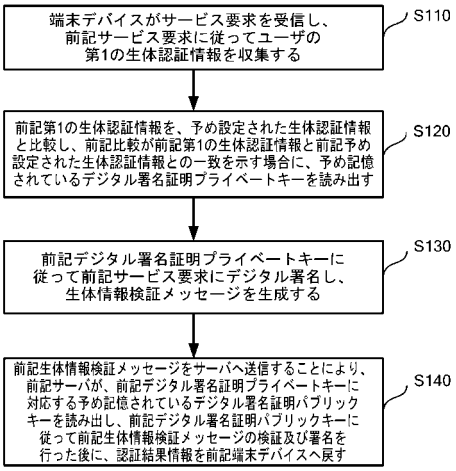

図 1

【図２】

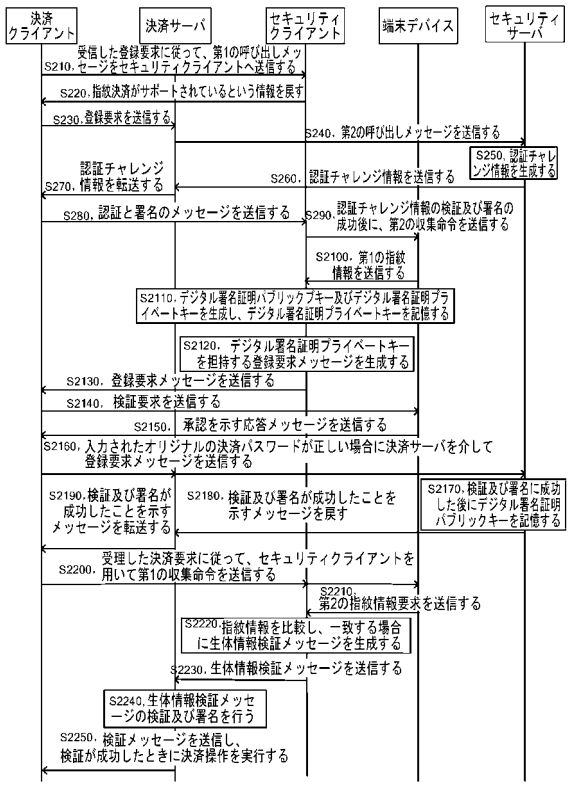

図 2

【図３】

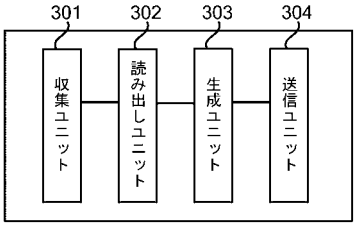

図 3

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/095855

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) 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)

H04L; G06Q

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

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

CNPAT, CNKI, WPI, EPODOC: creature, attestation, attest, authentication, authenticate, validate, validation, biologic, fingerprint, sound, voice, voiceprint, face, iris, private key, public key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102880960 A (SHENZHEN ARATEK BIOMETRICS TECHNOLOGY CO., LTD.), 16 January 2013 (16.01.2013), description, paragraphs 0038-0065	1-14
X	CN 101101686 A (SHANGHAI JIAO TONG UNIVERSITY et al.), 09 January 2008 (09.01.2008), abstract, and claims 1-13	1-14
X	CN 101340285 A (MIAXIS BIOMETRICS CO., LTD.), 07 January 2009 (07.01.2009), description, page 7, paragraph 3 to page 11, paragraph 6	1-14
A	US 2006176146 A1 (KRISHAN, B. et al.), 10 August 2006 (10.08.2006), the whole document	1-14

☐ 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
11 October 2016 (11.10.2016)	**11 November 2016 (11.11.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **HE, Xijia** Telephone No.: (86-10) **62413281**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/095855

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102880960 A	16 January 2013	None	
CN 101101686 A	09 January 2008	None	
CN 101340285 A	07 January 2009	None	
US 2006176146 A1	10 August 2006	JP 2006268831 A	05 October 2006

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

国际检索报告

国际申请号
PCT/CN2016/095855

A. 主题的分类
H04L 9/32(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)
H04L;G06Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)
CNPAT, CNKI, WPI, EPODOC：认证，验证，生物，指纹，声音，声纹，面部，脸，虹膜，私钥，公钥，attestation, attest, authentication, authenticate, validate, validation, biologic, fingerprint, sound, voice, voiceprint, face, iris, private key, public key

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 102880960 A (深圳市亚略特生物识别科技有限公司) 2013年 1月 16日 (2013-01-16) 说明书第0038-0065段	1-14
X	CN 101101686 A (上海交通大学 等) 2008年 1月 9日 (2008-01-09) 说明书摘要、权利要求1-13	1-14
X	CN 101340285 A (杭州中正生物认证技术有限公司) 2009年 1月 7日 (2009-01-07) 说明书第7页第3段-第11页第6段	1-14
A	US 2006176146 A1 (KRISHAN, BALDEV等) 2006年 8月 10日 (2006-08-10) 全文	1-14

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：
"A" 认为不特别相关的表示了现有技术一般状态的文件
"E" 在国际申请日的当天或之后公布的在先申请或专利
"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）
"O" 涉及口头公开、使用、展览或其他方式公开的文件
"P" 公布日先于国际申请日但迟于所要求的优先权日的文件
"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件
"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性
"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性
"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 10月 11日	2016年 11月 11日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 贺希佳 电话号码 (86-10)62413281

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/095855

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	102880960	A	2013年 1月 16日	无			
CN	101101686	A	2008年 1月 9日	无			
CN	101340285	A	2009年 1月 7日	无			
US	2006176146	A1	2006年 8月 10日	JP	2006268831	A	2006年 10月 5日

表 PCT/ISA/210（同族专利附件）（2009年7月）

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

（特許庁注：以下のものは登録商標）
１．ＡＮＤＲＯＩＤ
２．アンドロイド

(72)発明者 ジョン，ハオジエ
中華人民共和国 ３１００９９，ハンヂョウ，ナンバー１８ ワンタン ロード，フアンロン タイムズ プラザ，ビルディング ビー １７エフ，アンツ パテント チーム内
(72)発明者 ヂャオ，シアンユー
中華人民共和国 ３１００９９，ハンヂョウ，ナンバー１８ ワンタン ロード，フアンロン タイムズ プラザ，ビルディング ビー １７エフ，アンツ パテント チーム内
(72)発明者 ヂャン，シュリー
中華人民共和国 ３１００９９，ハンヂョウ，ナンバー１８ ワンタン ロード，フアンロン タイムズ プラザ，ビルディング ビー １７エフ，アンツ パテント チーム内

Ｆターム(参考) 5J104 AA07 AA09 AA16 KA01 KA05 KA06 KA16 LA03 LA06 MA01
NA02 NA37 NA38 PA07

【要約の続き】
【選択図】図１