(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2024-527492
(P2024-527492A)
(43)公表日　令和6年7月25日(2024.7.25)

(51)国際特許分類			FI		
H04L	*9/10*	*(2006.01)*	H04L	9/10	A
G06F	*21/33*	*(2013.01)*	G06F	21/33	
H04L	*9/32*	*(2006.01)*	H04L	9/32	２００Ｂ
G06F	*21/44*	*(2013.01)*	G06F	21/44	

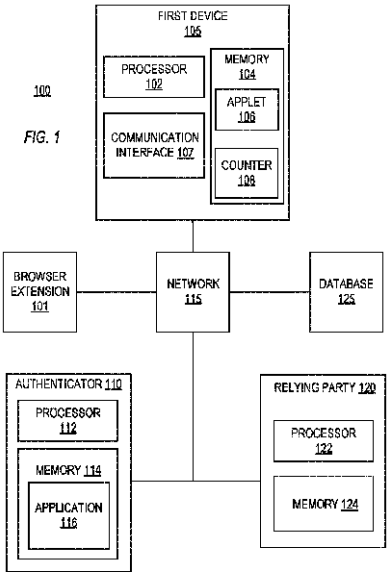
審査請求　未請求　予備審査請求　未請求　（全35頁）

(21)出願番号　特願2023-577529(P2023-577529)
(86)(22)出願日　令和4年6月16日(2022.6.16)
(85)翻訳文提出日　令和6年1月23日(2024.1.23)
(86)国際出願番号　PCT/US2022/033724
(87)国際公開番号　WO2022/266283
(87)国際公開日　令和4年12月22日(2022.12.22)
(31)優先権主張番号　17/352,181
(32)優先日　令和3年6月18日(2021.6.18)
(33)優先権主張国・地域又は機関
米国(US)
(81)指定国・地域　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,
最終頁に続く

(71)出願人　519111877
キャピタル・ワン・サービシーズ・リミテッド・ライアビリティ・カンパニー
Ｃａｐｉｔａｌ Ｏｎｅ Ｓｅｒｖｉｃｅｓ，ＬＬＣ
アメリカ合衆国２２１０２バージニア州マクリーン、キャピタル・ワン・ドライブ１６８０番
(74)代理人　100145403
弁理士　山尾 憲人
(74)代理人　100135703
弁理士　岡部 英隆
(72)発明者　ルール，ジェフリー
アメリカ合衆国２２１０２バージニア州マクリーン、キャピタル・ワン・ドライ
最終頁に続く

(54)【発明の名称】　非接触型カード通信及びマルチ装置鍵ペア暗号認証のためのシステム及び方法

(57)【要約】
認証のためのシステム及び方法は、認証装置を含むことができる。認証装置は、プロセッサとメモリを含むことができる。プロセッサは、第１の命令を生成し、第１の命令は、第１のＦＩＤＯ（Ｆａｓｔ Ｉｄｅｎｔｉｔｙ Ｏｎｌｉｎｅ）鍵を取得する要求を含み、第１の命令を送信し、第１のＦＩＤＯ鍵を受信し、第１のＦＩＤＯ鍵を用いて、１つ又は複数のチャレンジに署名し、第２のＦＩＤＯ鍵を用いた検証のために、１つ又は複数の署名されたチャレンジを送信する。



【特許請求の範囲】
【請求項１】
メモリとプロセッサとを備える認証装置であって、
前記プロセッサは、
１つ又は複数のチャレンジを受信し、
第１の命令を生成するように構成され、前記第１の命令は、第１のＦＩＤＯ（Ｆａｓｔ Ｉｄｅｎｔｉｔｙ Ｏｎｌｉｎｅ）鍵を取得する要求を含み、
前記プロセッサは、
前記第１の命令を送信し、
前記第１のＦＩＤＯ鍵を受信し、
前記第１のＦＩＤＯ鍵を用いて、１つ又は複数のチャレンジに署名し、
第２のＦＩＤＯ鍵を用いた検証のために、１つ又は複数の署名されたチャレンジを送信するように構成される、認証装置。
【請求項２】
前記第１の命令は、第１のＦＩＤＯ鍵を生成する要求を含む、
請求項１に記載の認証装置。
【請求項３】
前記第１の鍵は、１つ又は複数の暗号アルゴリズムを用いて、マスター鍵と認証要求に関連付けられた識別子に基づいて生成される、
請求項２記載の認証装置。
【請求項４】
前記第１のＦＩＤＯ鍵は帯域外チャンネルを介して送信される、
請求項１に記載の認証装置。
【請求項５】
前記第１の命令は、前記第１のＦＩＤＯ鍵を再生成する要求を含む、
請求項１に記載の認証装置。
【請求項６】
前記１つ又は複数のチャレンジは、ＦＩＤＯウェブサイト登録のための認証要求に基づいて受信される、
請求項１に記載の認証装置。
【請求項７】
前記プロセッサは、バイオメトリックデータ及びクレデンシャルデータのグループから選択される少なくとも１つを含む入力データを受信するようにさらに構成される、
請求項１に記載の認証装置。
【請求項８】
前記第１のＦＩＤＯ鍵は、通信フィールドへの通信インターフェースの入力により取得される、
請求項１に記載の認証装置。
【請求項９】
前記入力データは、１つ又は複数の条件の決定後に送信される、
請求項７に記載の認証装置。
【請求項１０】
認証方法であって、
前記認証方法は、
プロセッサが、１つ又は複数のチャレンジを受信することと、
前記プロセッサが、第１のＦＩＤＯ（Ｆａｓｔ Ｉｄｅｎｔｉｔｙ Ｏｎｌｉｎｅ）鍵を取得する要求を含む第１の命令を生成することと、
前記プロセッサが、第１の命令を送信することと、
第１のＦＩＤＯ鍵を受信することと、
前記プロセッサが、前記第１のＦＩＤＯ鍵を用いて、１つ又は複数のチャレンジに署名

することと、
前記プロセッサが、第２のＦＩＤＯ鍵を用いた検証のために、１つ又は複数の署名されたチャレンジを送信することと、
を含む、認証方法。
【請求項１１】
前記第１の命令は、前記第１のＦＩＤＯ鍵を生成する要求を含む、
請求項１０に記載の方法。
【請求項１２】
前記第１のＦＩＤＯ鍵は、１つ又は複数の暗号化アルゴリズムを用いて、第３の鍵と、認証要求に関連付けられた識別子に基づいて生成される、
請求項１１に記載の方法。
【請求項１３】
帯域外チャンネルを介して第１のＦＩＤＯ鍵を送信することをさらに含む、
請求項１０に記載の方法。
【請求項１４】
前記第１の命令は、前記第１のＦＩＤＯ鍵を再生成する要求を含む、
請求項１０に記載の方法。
【請求項１５】
前記１つ又は複数のチャレンジは、ＦＩＤＯウェブサイト登録のための認証要求に基づいて受信される、
請求項１０に記載の方法。
【請求項１６】
前記プロセッサが、バイオメトリックデータ及びクレデンシャルデータの群から選択される少なくとも１つを含む入力データを受信することをさらに含む、
請求項１０に記載の方法。
【請求項１７】
前記第１のＦＩＤＯ鍵は、通信フィールドへの通信インターフェースの入力により取得される、
請求項１０に記載の方法。
【請求項１８】
前記入力データは、１つ又は複数の条件の決定後に送信される、
請求項１６に記載の方法。
【請求項１９】
少なくとも１つの条件は、所定の期間にわたる認証要求のしきい値数を決定することを含む、
請求項１８に記載の方法。
【請求項２０】
コンピュータにより実行可能な命令を含む、コンピュータ可読非一時的媒体であって、
前記命令はプロセッサ上で実行されると、所定のステップを含む手順を実行し、
前記ステップは、
１つ以上のチャレンジを受信することと、
第１のＦＩＤＯ（Ｆａｓｔ　Ｉｄｅｎｔｉｔｙ　Ｏｎｌｉｎｅ）鍵を取得する要求を含む第１の命令を生成することと、
前記第１の命令を送信することと、
前記第１のＦＩＤＯ鍵を受信することと、
前記第１のＦＩＤＯ鍵を用いて１つ又は複数のチャレンジに署名することと、
第２のＦＩＤＯ鍵を用いた検証のために、１つ又は複数の署名されたチャレンジを送信することと、
を含むコンピュータ可読非一時的媒体。
【発明の詳細な説明】

【技術分野】
【０００１】
本開示は、非接触型カード通信のためのシステム及び方法に関し、より具体的には、複数の装置を使用する非接触型カードの鍵ペア暗号認証のためのシステム及び方法に関する。
【０００２】
関連出願との相互参照
本出願は、２０２１年６月１８日に出願された米国特許出願第１７／３５２，１８１号の優先権を主張するものであり、その開示内容は参照によりその全体が本明細書に組み込まれる。
【背景技術】
【０００３】
カードを使った業務では、サーバ装置や他の機器との通信にカードを使うことが多い。このような通信を傍受や不正アクセスから保護することが必要である。しかし、ハッカーやその他の不正行為者によって採用される可能性のあるデータ傍受、数多くの洗練された方法が存在する。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
例えば、暗号化又は他の保護手段を用いないデータ伝送は、中間者攻撃、フィッシング攻撃、リプレイ攻撃、及び他の攻撃の影響を受けやすく、他の脆弱性の影響を受信する可能性があり、その結果、セキュリティリスクが増大し、アカウント又はカードが悪用されるリスクが増大する。これらのリスクは、他の装置と無線通信を行う非接触型カードの使用によりさらに高まる可能性があり、その結果、伝送中にデータが傍受される可能性にさらされる。
【０００５】
暗号化など、セキュリティリスクに対処するために取られる措置は、システムリソースを消費し、業務効率を妨げる可能性がある。操作回数が多い場合、システムリソースの消費量や操作効率の阻害が増大し、操作に失敗して満足なパフォーマンスが得られない可能性がある。また、セキュアな認証装置へのアクセスが制限されて利用できない場合もあり、これにより、安全な暗号化、データ伝送、安全な登録と認証へのアクセスに悪影響が及び、不正取引や口座乗っ取りに利用される危険な口座につながる可能性がある。
【０００６】
このような欠陥やその他の欠陥が存在する。従って、安全で信頼性の高い方法で通信を傍受や不正アクセスから保護することにより、複数装置の鍵ペア暗号認証を効果的に利用し、安全かつ迅速に発信者を特定し、その真正性を判断することで、これらの欠陥を克服する認証のためのシステムや方法が必要とされている。
【課題を解決するための手段】
【０００７】
本開示の実施形態は、認証装置を提供する。認証装置は、プロセッサとメモリとを含むことができる。プロセッサは、１つ又は複数のチャレンジを受信するように構成されてもよい。プロセッサは、第１の命令を生成するように構成されてもよい、第１の命令は、第１のＦＩＤＯ（Ｆａｓｔ　Ｉｄｅｎｔｉｔｙ　Ｏｎｌｉｎｅ；高速識別オンライン）鍵を取得する要求を含む。プロセッサは、第１の命令を送信するように構成されてもよい。プロセッサは、第１のＦＩＤＯ鍵を受信するように構成されてもよい。プロセッサは、第１のＦＩＤＯ鍵を用いて１つ又は複数のチャレンジに署名するように構成される。プロセッサは、第２のＦＩＤＯ鍵を用いた検証のために、１つ又は複数の署名されたチャレンジを送信するように構成される。
【０００８】
本開示の実施形態は、認証方法を提供する。本方法は、プロセッサにおいて、１つ又は

複数のチャレンジを受信することを含む。本方法は、プロセッサによって、第１のＦＩＤＯ（Ｆａｓｔ　Ｉｄｅｎｔｉｔｙ　Ｏｎｌｉｎｅ）鍵を取得する要求を含む第１の命令を生成することを含む。本方法は、プロセッサにより、第１の命令を送信することを含む。本方法は、第１のＦＩＤＯ鍵を受信することを含む。本方法は、プロセッサにより、第１のＦＩＤＯ鍵を用いて１つ又は複数のチャレンジに署名することを含む。本方法は、プロセッサにより、第２のＦＩＤＯ鍵を用いた検証のために、１つ又は複数の署名されたチャレンジを送信することを含む。

【０００９】

本開示の実施形態は、以下のコンピュータ実行可能命令を含むコンピュータ可読非一時的媒体を提供し、プロセッサ上で実行されると、以下のステップを含む手順を実行する。前記ステップは、１つ又は複数のチャレンジを受信し、第１のＦＩＤＯ（Ｆａｓｔ　Ｉｄｅｎｔｉｔｙ　Ｏｎｌｉｎｅ）鍵を取得する要求を含む第１の命令を生成することと、前記第１の命令を送信することと、第１のＦＩＤＯ鍵を受信することと、第１のＦＩＤＯ鍵を用いて１つ又は複数のチャレンジに署名することと、第２のＦＩＤＯ鍵を用いた検証のために、１つ又は複数の署名されたチャレンジを送信することとを含む。

【００１０】

本開示の様々な実施形態は、さらなる目的及び利点とともに、添付の図面と併せて取られる以下の説明を参照することによって最もよく理解され得る。

【図面の簡単な説明】

【００１１】

【図１】例示的な実施形態に係る認証システムを示す。

【図２Ａ】例示的な実施形態に係る第１の装置の説明図である。

【図２Ｂ】例示的な実施形態に係る第１の装置の接触パッドの説明図である。

【図３】例示的な実施形態に係る認証方法を示す。

【図４】例示的な実施形態に係る認証プロセスのシーケンス図である。

【図５】例示的な実施形態に係る認証方法を示す。

【図６】例示的な実施形態に係る認証方法を示す。

【発明を実施するための形態】

【００１２】

詳細説明

以下の実施形態の説明は、本発明の異なる態様の特徴及び教示を特に説明するために数字を参照する非限定的な代表例を提供する。説明される実施形態は、実施形態の説明から、別個に、又は他の実施形態と組み合わせて実施することが可能であると認識されるべきである。実施形態の説明を検討する当業者は、本発明の異なる記載された態様を学び理解することができるはずである。実施形態の記載は、具体的に網羅されていないが、実施形態の記載を読んだ当業者の知識の範囲内にある他の実施態様が、本発明の適用と一致すると理解される程度に、本発明の理解を容易にするものでなければならない。

【００１３】

本明細書において開示するシステム及び方法は、認証フレームワーク（ＦＩＤＯ認証、ＦＩＤＯ２認証、ＷｅｂＡｕｔｈｎ、ＣＴＡＰ（Ｃｌｉｅｎｔ　ｔｏ　Ａｕｔｈｅｎｔｉｃａｔｏｒ　Ｐｒｏｔｏｃｏｌ）ＦＩＤＯ、その他の認証実装を含むが、これらに限定されない）を補完するために使用することができる。本明細書で採用されるシステム及び方法は、この機能をサポートするために、分散記憶装置、クラウドベースの記憶装置、及び他の形態の記憶装置とともに実装され得る。本明細書で開示するシステム及び方法は、ブラウザにおけるＦａｓｔ　Ｉｄｅｎｔｉｔｙ　Ｏｎｌｉｎｅ　２（ＦＩＤＯ２）認証において、装置がローミング認証装置として機能することを可能にする。以下にさらに説明するように、ユーザは、実装されたシステム及び方法を用いて、パスワードなしの環境でウェブサイトと認証することができる。ウェブサイトにログインするために、ウェブサイトの登録プロセス中に秘密鍵が装置に保存されてもよい。ユーザがウェブサイトへの再ログインを希望する場合、装置は、タップ、スワイプ、ウェーブなどを含むがこれらに限定さ

れない１つ又は複数のジェスチャを用いてモバイル装置のような通信フィールドに入ることができる。その後、秘密鍵は、第１の装置から、認証装置能を含むがこれに限定されない、モバイル装置上で実行するための命令を含むアプリケーションに送信される可能性がある。認証装置は、ウェブサイトが発行したチャレンジに秘密鍵を用いて署名するよう構成される。署名されたチャレンジは、依拠当事者サーバ装置に送信され、保存されている公開鍵を用いて検証される。このように、この認証は、ユーザをログインさせるための一次認証として機能する。さらに、この認証を、例えばモバイル装置に入力されたバイオメトリクスやクレデンシャルなどの二次要素認証と組み合わせて使用することもできる。

【００１４】

本明細書で開示されるシステム及び方法の利点には、通信を傍受や不正アクセスから保護し、発信者を安全かつ迅速に特定し、その真正性を判定することによる認証の向上が含まれる。

本明細書で開示するシステム及び方法により、ｉＯＳ（登録商標）やＡｎｄｒｏｉｄ（登録商標）が装置上で実行されている場合に限らず、ラップトップブラウザ、タブレットブラウザ、デスクトップブラウザなどのブラウザ上でＦＩＤＯ２認証を行う際の認証装置として使用することで、条件付き多要素認証を実装して、中間者攻撃やフィッシング攻撃の回避、リプレイ攻撃の防止、認証装置のアクセシビリティとセキュリティの向上、安全な暗号化とデータ伝送、他のセキュリティ上の脆弱性の低減が可能になる。

【００１５】

さらに、ＦＩＤＯ２フレームワークやその他の認証フレームワークで懸念されるのは、認証プロセスを実行しようとするユーザの身元を確立することである。本明細書で説明するシステム及び方法は、資格情報を登録し、フレームワークを用いて認証しようとするユーザが、そのユーザであると主張し、認証プロセスを実行することを許可されたユーザであることを確認することによって、この脆弱性を低減することができる。そうすることで、フレームワークのセキュリティと、権限のないユーザを排除する能力を高めることができる。従って、セキュリティリスクはさらに軽減され、様々な装置間の互換性や取引効率はさらに改善される可能性がある。いくつかの例では、１つ又は複数のＦＩＤＯ鍵を認証装置内で生成する代わりに、１つ又は複数のＦＩＤＯ鍵を取得又は生成するよう第１の装置に命令する場合、認証装置の計算処理が削減される。

【００１６】

これらの機能は、ユーザに不必要なセキュリティタスクを負わせることによってユーザエクスペリエンスを低下させることなく実装することができる。さらに、これらの機能は、ユーザの期待やトランザクション要件に適合するように、トランザクションの時間効率的な実行を可能にする方法で実行することができる。

【００１７】

従って、ここに開示されたシステムと方法は、例えばカード又はカードに関連する口座の不正使用などためのリスクを軽減する。同時に、認証装置への安全なアクセスと暗号化されたデータ伝送を改善する。本明細書で開示されるシステム及び方法は、安全な認証を欠く実装を改善する。これらの利点は、システム効率を促進し、ユーザエクスペリエンスの低下を回避し、多数の装置間の互換性を促進しながら、有利に達成され得る。

【００１８】

図１は、認証システム１００を示す。システム１００は、ブラウザ拡張機能１０１、第１の装置１０５、認証装置１１０又は第２の装置、ネットワーク１１５、依拠当事者装置又はサーバ装置１２０、及びデータベース１２５から構成される。図１は、システム１００のコンポーネントの単一インスタンスを図示すが、システム１００は、任意の数のコンポーネントを含むことができる。

【００１９】

システム１００は、ブラウザ拡張機能１０１を含むことができる。ブラウザ拡張機能１０１は、Ｃｈｒｏｍｅ（登録商標）、Ｉｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒ（登録商標）、Ｆｉｒｅｆｏｘ（登録商標）、又はＳａｆａｒｉ（登録商標）で構成されてもよい。ブ

ラウザ拡張機能以外のソフトウェアアプリケーション（スタンドアローンのソフトウェアアプリケーションを含む）を利用することができることを理解されたい。これに限定されることなく、ウェブサイト登録などの認証要求は、ブラウザ拡張機能１０１に関連付けられたラップトップやデスクトップを含むがこれに限定されない、任意の装置上で行われる可能性がある。モバイルベースのブラウザ拡張機能１０１、又はタブレットベースのブラウザ拡張機能１０１、又はラップトップベースのブラウザ拡張機能１０１、又はデスクトップベースのブラウザ拡張機能１０１は、以下にさらに説明するように、１つ又は複数のリクエストを送信及び受信するように構成されてもよい。

【００２０】

システム１００は、第１の装置１０５を含むことができる。限定するものではないが、第１の装置１０５は、非接触型カード、接触型カード、ネットワーク対応コンピュータ、又は本明細書で説明する他の装置で構成することができる。本明細書で言及するように、ネットワーク対応コンピュータには、コンピュータ装置、又は通信装置が含まれるが、これらに限定されるものではない。これらの装置には、例えば、サーバ装置、ネットワークアプライアンス、パーソナルコンピュータ、ワークステーション、電話、ハンドヘルドＰＣ、パーソナルデジタルアシスタント、非接触型カード、シンクライアント、ファットクライアント、インターネットブラウザ、キオスク、タブレット、端末、その他の装置が含まれる。図２Ａ～図２Ｂで以下にさらに説明するように、第１の装置１０５は、１つ又は複数のプロセッサ１０２、及びメモリ１０４を含むことができる。メモリ１０４は、１つ又は複数のアプレット１０６と、１つ又は複数のカウンタ１０８とを含むことができる。各カウンタ１０８はカウンタ値を含んでもよい。メモリ１０４は、カウンタ値、送信データ、及び少なくとも１つの鍵を含んでもよい。

【００２１】

第１の装置１０５は、通信インターフェース１０７を含むことができる。通信インターフェース１０７は、物理インターフェース及び非接触インターフェースとの通信機能を含んでいてもよい。例えば、通信インターフェース１０７は、例えば、カードスワイプインターフェースを介してスワイプし、現金自動預け払い機（ＡＴＭ）又は物理的なインターフェースを介して通信するように構成された他の装置に見られるカードチップリーダーに挿入することによって、物理インターフェースと通信するように構成される。他の例では、通信インターフェース１０７は、ＮＦＣ、ブルートゥース（登録商標）、Ｗｉ－Ｆｉ、ＲＦＩＤなどの近距離無線通信方式を用いて、カード読み取り装置と非接触通信を確立するように構成することができる。図１に示すように、通信インターフェース１０７は、ネットワーク１１５を介して、認証装置１１０又は第２の装置、依拠当事者装置又はサーバ装置１２０、及び／又はデータベース１２５と直接通信するように構成されてもよい。

【００２２】

第１の装置１０５は、システム１００の任意の数のコンポーネントとデータ通信を行ってよい。例えば、第１の装置１０５は、ネットワーク１１５を介して、認証装置１１０又は第２の装置、及び／又は依拠当事者装置又はサーバ装置１２０にデータを送信することができる。第１の装置１０５は、ネットワーク１１５を介してデータベース１２５にデータを送信してもよい。いくつかの例では、第１の装置１０５は、任意の装置の１つ又は複数の通信フィールドへのエントリ後に、ネットワーク１１５を介してデータを送信するように構成されてもよい。限定されないが、各入力は、タップ、スワイプ、ウェーブ、及び／又はそれらの任意の組み合わせに関連付けられ得る。

【００２３】

システム１００は、認証装置１１０を含むことができる。認証装置１１０は、他のクライアント装置に対するローミング認証装置を構成することができる。いくつかの例では、認証装置１１０は、ラップトップ、デスクトップ、又はタブレットに対するローミング認証装置として機能するモバイル装置を含むことができる。クライアント装置はこのような装置に限定されるものではなく、他のクライアント装置も本発明の範囲内であることを理解されたい。

【００２４】
一例として、認証装置１１０は、第２の装置を構成することができる。認証装置１１０は、１つ又は複数のプロセッサ１１２、及びメモリ１１４を含むことができる。メモリ１１４は、アプリケーション１１６を含むがこれに限定されず、１つ又は複数のアプリケーションを含んでもよい。認証装置１１０は、システム１００の任意の数の構成要素とデータ通信を行うことができる。例えば、認証装置１１０は、ネットワーク１１５を介してサーバ装置１２０にデータを送信することができる。認証装置１１０は、ネットワーク１１５経由でデータベース１２５にデータを送信してもよい。限定するものではないが、認証装置１１０はネットワーク対応コンピュータであってもよい。本明細書で言及するように、ネットワーク対応コンピュータには、コンピュータ装置、又は通信装置が含まれるが、これらに限定されるものではない。これらの装置には、例えば、サーバ装置、ネットワークアプライアンス、パーソナルコンピュータ、ワークステーション、電話、ハンドヘルドＰＣ、パーソナルデジタルアシスタント、非接触型カード、シンクライアント、ファットクライアント、インターネットブラウザ、キオスク、タブレット、端末、その他の装置が含まれる。認証装置１１０は、モバイル装置であってもよく、例えば、モバイル装置には、Ａｐｐｌｅ（登録商標）のｉＰｈｏｎｅ（登録商標）、ｉＰｏｄ（登録商標）、ｉＰａｄ（登録商標）、又はＡｐｐｌｅのｉＯＳ（登録商標）オペレーティングシステムを実行する他のモバイル装置、ＭｉｃｒｏｓｏｆｔのＷｉｎｄｏｗｓ（登録商標）Ｍｏｂｉｌｅオペレーティングシステムを実行する装置、ＧｏｏｇｌｅのＡｎｄｒｏｉｄ（登録商標）オペレーティングシステムを実行する装置、及び／又は他のスマートフォン、タブレット、又は同様のウェアラブルモバイル装置が含まれる。

【００２５】
認証装置１１０は、処理回路を含むことができ、追加の構成要素を含むことができ、追加の構成要素は、プロセッサ、メモリ、エラー及びパリティ／ＣＲＣチェッカ、データエンコーダ、アンチコリジョンアルゴリズム、コントローラ、コマンドデコーダ、セキュリティプリミティブ及び改ざん防止ハードウェアを含み、本明細書で説明する機能を実行するために必要なものである。認証装置１１０は、ディスプレイ及び入力装置をさらに含むことができる。ディスプレイは、例えばコンピュータのモニター、フラットパネルディスプレイ、モバイル機器の画面など、液晶ディスプレイ、発光ダイオードディスプレイ、プラズマパネル、ブラウン管ディスプレイなどであり、視覚情報を表示する装置であればどのようなものでもよい。入力装置には、例えば、タッチスクリーン、鍵ボード、マウス、カーソル制御装置、タッチスクリーン、マイク、デジタルカメラ、ビデオレコーダー、ビデオカメラなど、ユーザの装置で利用可能でサポートされている、ユーザの装置に情報を入力するための任意の装置を含めることができ、これらの機器は、情報を入力したり、本明細書で説明するソフトウェアや他の機器と相互作用したりするために使用することができる。

【００２６】
システム１００は、ネットワーク１１５を含み得る。いくつかの例では、ネットワーク１１５は、無線ネットワーク、有線ネットワーク、又は無線ネットワークと有線ネットワークの任意の組み合わせのうちの１つ又は複数であってよく、システム１００の構成要素のうちの任意の１つに接続するように構成されてよい。例えば、第１の装置１０５は、ネットワーク１１５を介して依拠当事者装置又はサーバ装置１２０に接続するように構成され得る。いくつかの例では、ネットワーク１１５は、光ファイバネットワーク、パッシブ光ネットワーク、ケーブルネットワーク、インターネットネットワーク、衛星ネットワーク、無線ローカルエリアネットワーク（ＬＡＮ）、移動通信グローバルシステム、パーソナル通信サービス、パーソナルエリアネットワーク、ワイヤレスアプリケーションプロトコル、マルチメディアメッセージングサービス、エンハンストメッセージングサービス、ショートメッセージサービス、時分割多重化ベースのシステム、符号分割多重アクセスベースのシステム、Ｄ－ＡＭＰＳ、Ｗｉ－Ｆｉ、固定無線データ、ＩＥＥＥ８０２．１１ｂ、８０２．１５．１、８０２．１１ｎ及び８０２．１１ｇ、ブルートゥース（登録商標）

、ＮＦＣ、ＲＦＩＤ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）、Ｗｉ－Ｆｉなどである。

【００２７】

さらに、ネットワーク１１５は、限定するものではないが、電話回線、光ファイバ、ＩＥＥＥイーサネット９０２．３、広域ネットワーク、無線パーソナルエリアネットワーク、ＬＡＮ、又はインターネットのようなグローバルネットワークを含むことができる。さらに、ネットワーク１１５は、インターネットネットワーク、無線通信ネットワーク、セルラーネットワークなど、又はそれらの任意の組み合わせをサポートすることができる。ネットワーク１１５は、さらに、独立したネットワークとして、又は互いに協力して動作し、１つのネットワーク、又は上述の例示的なタイプのネットワークの任意の数を含むことができる。ネットワーク１１５は、通信可能に結合されている１つ又は複数のネットワーク要素の１つ又は複数のプロトコルを利用することができる。ネットワーク１１５は、他のプロトコルからネットワーク装置の１つ又は複数のプロトコルへ、又は他のプロトコルからネットワーク装置の１つ又は複数のプロトコルへ変換することができる。ネットワーク１１５は単一のネットワークとして図示されているが、１つ又は複数の実施例によれば、ネットワーク１１５は、例えば、インターネット、サービスプロバイダのネットワーク、ケーブルテレビネットワークなど、企業ネットワークであって、例えば、クレジットカード協会ネットワークやホームネットワークなどである、複数の相互接続されたネットワークから構成され得ることが理解されるべきである。

【００２８】

システム１００は、サーバ装置１２０を含んでもよく、例えば、限定するものではないが、サーバ装置１２０は依拠当事者装置を構成してもよい。いくつかの例では、サーバ装置１２０は、メモリ１２４に結合された１つ又は複数のプロセッサ１２２を含むことができる。限定するものではないが、サーバ装置１２０はクラウドベースの認証装置を構成することができる。サーバ装置１２０は、複数のワークフロー動作を実行するために、異なる時間に様々なデータを制御し、呼び出すための中央システム、サーバ装置、又はプラットフォームとして構成されてもよい。サーバ装置１２０は、第１の装置１０５に接続するように構成されてもよい。サーバ装置１２０は、アプレット１０６及び／又はアプリケーション１１６とデータ通信を行ってもよい。例えば、サーバ装置１２０は、１つ又は複数のネットワーク１１５を介してアプレット１０６とデータ通信を行ってもよい。第１の装置１０５は、１つ又は複数のネットワーク１１５を介して１つ又は複数のサーバ装置１２０と通信してよく、サーバ装置１２０とのそれぞれのフロントエンド対バックエンド対として動作してよい。第１の装置１０５は、例えばその上で実行されるアプレット１０６から、１つ又は複数の要求をサーバ装置１２０に送信してもよい。１つ以上のリクエストは、サーバ装置１２０からデータを取得することに関連してもよい。サーバ装置１２０は、第１の装置１０５から１つ又は複数の要求を受信してもよい。アプレット１０６からの１つ又は複数の要求に基づいて、サーバ装置１２０は、要求されたデータを取得するように構成されてもよい。サーバ装置１２０は、受信されたデータをアプレット１０６に送信するように構成されてもよく、受信されたデータは、１つ又は複数の要求に応答する。

【００２９】

いくつかの例では、サーバ装置１２０は、ブレードサーバ装置などの専用サーバ装置コンピュータとすることができ、もしくは、サーバ装置１２０は、パーソナルコンピュータ、ラップトップコンピュータ、ノートブックコンピュータ、パームトップコンピュータ、ネットワークコンピュータ、モバイル装置、ウェアラブル装置、又はシステム１００をサポートすることができる任意のプロセッサ制御装置とすることができる。図１は、単一の依拠当事者装置又はサーバ装置１２０を示す。他の実施形態では、ユーザをサポートするために必要又は所望に応じて複数のサーバ装置又は複数のコンピュータシステムを使用することができ、特定のサーバ装置に障害が発生した場合のネットワークのダウンタイムを防止するためにバックアップ又は冗長サーバ装置を使用することもできることを理解されたい。

【００３０】
サーバ装置１２０は、その上で実行するための命令を含むアプリケーションを含むことができる。例えば、アプリケーションは、サーバ装置１２０上で実行するための命令を含んでもよい。サーバ装置１２０のアプリケーションは、システム１００の任意の構成要素と通信してもよい。例えば、サーバ装置１２０は、例えば、システム１００の１つ又は複数の構成要素とのネットワーク及び／又はデータ通信を可能にし、データを送信及び／又は受信する１つ又は複数のアプリケーションを実行してもよい。限定するものではないが、サーバ装置１２０は、ネットワーク対応コンピュータであってもよい。本明細書で言及するように、ネットワーク対応コンピュータには、コンピュータ装置、又は通信装置が含まれるが、これらに限定されるものではない。これらの装置には、例えば、サーバ装置、ネットワークアプライアンス、パーソナルコンピュータ、ワークステーション、電話、ハンドヘルドＰＣ、パーソナルデジタルアシスタント、非接触型カード、シンクライアント、ファットクライアント、インターネットブラウザ、又はその他の装置が含まれる。サーバ装置１２０はまた、モバイル装置であってもよく、例えば、モバイル装置は、Ａｐｐｌｅ（登録商標）のｉＰｈｏｎｅ（登録商標）、ｉＰｏｄ（登録商標）、ｉＰａｄ（登録商標）、又はＡｐｐｌｅのｉＯＳ（登録商標）オペレーティングシステムを実行する任意の他のモバイル装置、ＭｉｃｒｏｓｏｆｔのＷｉｎｄｏｗｓ（登録商標）Ｍｏｂｉｌｅオペレーティングシステムを実行する任意の装置、ＧｏｏｇｌｅのＡｎｄｒｏｉｄ（登録商標）オペレーティングシステムを実行する任意の装置、及び／又は任意の他のスマートフォン、タブレット、又は同様のウェアラブルモバイル装置を含み得る。

【００３１】
サーバ装置１２０は、処理回路を含むことができ、追加のコンポーネントを含むことができ、本明細書で説明する機能を実行するために必要な追加コンポーネントは、プロセッサ、メモリ、エラー及びパリティ／ＣＲＣチェッカ、データエンコーダ、アンチコリジョンアルゴリズム、コントローラ、コマンドデコーダ、セキュリティプリミティブ、改ざん防止ハードウェアなどである。サーバ装置１２０は、ディスプレイ及び入力装置をさらに含むことができる。ディスプレイは、コンピュータモニタ、フラットパネルディスプレイ、モバイル装置の画面など、液晶ディスプレイ、発光ダイオードディスプレイ、プラズマパネル、陰極線管ディスプレイを含む、視覚情報を提示するための任意のタイプの装置であってもよい、入力装置には、ユーザの装置で利用可能でサポートされている、ユーザの装置に情報を入力するための任意の装置を含めることができ、例えば、タッチスクリーン、鍵ボード、マウス、カーソル制御装置、タッチスクリーン、マイク、デジタルカメラ、ビデオレコーダー、ビデオカメラなどである。これらの機器は、情報を入力したり、本明細書で説明するソフトウェアや他の機器と相互作用したりするために使用することができる。

【００３２】
システム１００は、１つ又は複数のデータベース１２５を含んでもよい。データベース１２５は、リレーショナルデータベース、非リレーショナルデータベース、又は他のデータベース実装、及びそれらの任意の組み合わせから構成されてもよく、これらは、複数のリレーショナルデータベース及び非リレーショナルデータベースを含む。いくつかの例では、データベース１２５は、デスクトップデータベース、モバイルデータベース、又はインメモリデータベースで構成される。さらに、データベース１２５は、第１の装置１０５やサーバ装置１２０など、システム１００の任意のコンポーネントによって内部的にホストされてもよい、又はデータベース１２５は、システム１００のコンポーネントの外部でホストされ、これは、クラウドベースのプラットフォーム、又は第１の装置１０５やサーバ装置１２０とデータ通信を行う任意の記憶装置などである。いくつかの例では、データベース１２５は、システム１００の任意の数のコンポーネントとデータ通信を行うことができる。例えば、サーバ装置１２０は、アプレット１０６によって送信されるデータベース１２５から要求されたデータを取得するように構成されてもよい。サーバ装置１２０は、ネットワーク１１５を介してデータベース１２５からアプレット１０６に受信されたデ

ータを送信するように構成されてもよく、受信されたデータは、送信された１つ又は複数の要求に応答する。他の例では、アプレット１０６は、ネットワーク１１５を介してデータベース１２５から要求されたデータに対する１つ又は複数の要求を送信するように構成されてもよい。

【００３３】

いくつかの例では、本明細書に記載される本開示に従った例示的な手順は、処理配置及び／又は計算配置（例えば、コンピュータハードウェア配置）によって実行され得る。このような処理／計算配置は、例えば、全体又はその一部とすることができ、又は、例えば、１つ又は複数のマイクロプロセッサを含むことができ、コンピュータアクセス可能な媒体（例えば、ＲＡＭ、ＲＯＭ、ハードドライブ、又は他の記憶装置）に記憶された命令を使用するコンピュータ／プロセッサを含むことができるが、これらに限定されない。例えば、コンピュータアクセス可能な媒体は、第１の装置１０５、認証装置１１０、サーバ装置１２０、及び／又はデータベース１２５のメモリの一部、あるいは他のコンピュータハードウェア配置とすることができる。

【００３４】

いくつかの例では、コンピュータがアクセス可能な媒体（例えば、本明細書で上述したように、以下の記憶装置であってもよく、例えば、ハードディスク、フロッピーディスク、メモリースティック、ＣＤ－ＲＯＭ、ＲＡＭ、ＲＯＭなど、又はそれらの集合体など）を（例えば、処理配置と通信可能に）設けることができる。コンピュータアクセス可能な媒体には、実行可能な命令を含めることができる。加えて、あるいは代替的に、コンピュータアクセス可能な媒体とは別に記憶装置を設けることができ、この記憶装置は、本明細書で説明するように、特定の例示的な手順、プロセス、及び方法を実行するように処理装置を構成するように、処理装置に命令を提供することができる。

【００３５】

サーバ装置１２０のプロセッサ１２２は、認証要求を受信するように構成されてもよい。例えば、認証要求は、ブラウザ拡張機能１０１から受信されてもよい。一部の例では、認証要求は、ＦＩＤＯ２（Ｆａｓｔ　Ｉｄｅｎｔｉｔｙ　Ｏｎｌｉｎｅ　２）ウェブサイト登録の要求で構成されてもよい。プロセッサ１２２は、１つ又は複数のチャレンジを生成するように構成されてもよい。例えば、プロセッサ１２２は、第１のチャレンジを生成するように構成されてもよい。いくつかの例では、プロセッサ１２２は、認証装置１１０にログインを要求するように構成される。第１のチャレンジは、適切なＦＩＤＯ鍵ペアを選択するために使用される、ユーザ識別子やサイト識別子などの識別子を含むことができる。第１のチャレンジは、リプレイを防止するために使用される、サーバ装置１２０によって与えられる可能性のある予測不可能な番号をさらに含むことができる。例えば、認証のインスタンスごとに、新しい予測不可能な番号が必要となるため、予測不可能な番号は毎回異なる。こうすることで、予測不可能な古い番号の署名を利用することを避け、代わりに認証のインスタントセッションにその番号を利用する。

【００３６】

モバイル装置のプロセッサ１１２などの認証装置１１０は、第１の装置１０５の１つ又は複数の入力を促すように構成されてもよい。例えば、１つ又は複数のエントリは、タップ、スワイプ、ウェーブなどのグループから選択された少なくとも１つ、及び／又はそれらの任意の組み合わせを含むことができる。従って、第１の装置１０５の通信インターフェース１０７は、モバイル装置の通信フィールドなどの認証装置１１０の通信フィールドに入力することができる。第１の装置１０５は、認証装置１１０から受信した第１の命令に応じて、特定のユーザ又はサイトに関連付けられたＦＩＤＯ鍵ペアを生成又は取得するように構成されてもよい。生成又は取得されたＦＩＤＯ鍵ペアは、認証装置１１０によって読み取られる。ＦＩＤＯ鍵ペアは、認証装置１１０が第１の装置１０５から読み取ることができるＦＩＤＯ秘密鍵を含み、認証装置１１０が第１のチャレンジに署名するために使用することができる。ＦＩＤＯ秘密鍵は、第１の装置１０５の通信インターフェース１０７の通信フィールドへの入力を通じて取得されてもよい。いくつかの例では、ＦＩＤＯ

秘密鍵は、認証装置１１０に転送される前に、第１の装置１０５によって暗号化されてもよく、その場合、モバイル装置のプロセッサ１１２は、受信した暗号化されたＦＩＤＯ秘密鍵を復号化するように構成されてもよい。サーバ装置１２０は、モバイル装置のプロセッサ１１２などの認証装置１１０から署名付きチャレンジデータを受信することができる。サーバ装置１２０は、署名されたチャレンジデータの検証を行うことができる。例えば、サーバ装置１２０は、署名されたチャレンジデータを、ユーザがサイトに登録したときに保存されたＦＩＤＯ公開鍵で検証することができる。検証は、署名検証を含む認証プロセスの結果を構成することができる。

【００３７】

いくつかの例では、ＦＩＤＯ秘密鍵の第１の装置１０５から認証装置１１０への送信は防止される。例えば、第１の装置１０５が第１のチャレンジの署名を実行するとき、ＦＩＤＯ秘密鍵の無線（ＯＴＡ）送信は回避される。従って、第１のチャレンジとサイト又はユーザ識別子情報は、認証装置から第１の装置１０５に送信される。これにより、プロキシプロトコルを用いて近距離無線通信（ＮＦＣ）を用いて第１の装置１０５に計算を分配する。

【００３８】

いくつかの例では、ＦＩＤＯ秘密鍵は、１つ又は複数の暗号化アルゴリズムを用いて、マスター鍵及び認証要求に関連付けられた識別子に基づいて生成される。例えば、識別子はサイト識別子を含み、マスター鍵と組み合わされて別の鍵ペアが生成される。第１の装置１０５は、鍵を再生成する必要がないように、有限数の鍵をメモリ１０４に保存するよう構成される。他の例では、認証装置１１０からの第１の命令は、例えば、公開鍵／秘密鍵ペアの一部である秘密鍵などである、ＦＩＤＯ秘密鍵を再生成する要求を含んでもよい。

【００３９】

いくつかの例では、マスター鍵は、第１の装置１０５上のメモリ１０４に格納され、マスター鍵は、ＦＩＤＯ秘密鍵を生成するために第１の装置１０５上のサイト識別子と組み合わされる。他の例では、マスター鍵は、第１の装置１０５から認証装置１１０に転送され、認証装置１１０によってマスター鍵とサイト識別子の結合が行われ、ＦＩＤＯ秘密鍵が生成される。

【００４０】

いくつかの例では、ＦＩＤＯ秘密鍵は、第１の装置１０５内で生成又は保存されるのではなく、認証装置１１０に属するセキュアエレメント内で生成又は保存される。例えば、ＦＩＤＯ秘密鍵は、認証装置１１０が保持するセキュアエレメントに格納されてもよい。いくつかの例では、セキュアエレメントは、１つ又は複数の鍵が安全に保管され、サーバ装置１２０によって取り出される、耐タンパー性のセキュア記憶装置エリアを構成することができる。

【００４１】

命令生成後、認証装置１１０は、第１の命令を第１の装置１０５に送信するように構成される。認証装置１１０は、第１の命令に基づいて、第１の装置１０５からＦＩＤＯ秘密鍵を受信するように構成されてもよい。第１の命令は、認証装置１１０によって第１の装置１０５のプロセッサ１０２に送信されてもよい。例えば、第１の装置１０５のプロセッサ１０２は、ＦＩＤＯ秘密鍵を生成するように構成される。第１の装置１０５のプロセッサ１０２は、ＦＩＤＯ秘密鍵を送信するように構成されてもよい。例えば、第１の装置１０５のプロセッサ１０２は、ＦＩＤＯ秘密鍵を認証装置１１０に送信するように構成される、例えば、認証装置１１０上で実行するための命令を含むアプリケーション１１６などである。上述したように、認証装置１１０は、限定されるものではないが、ラップトップ、タブレット、電話などのモバイル装置であってもよい。一部の例では、ＦＩＤＯ秘密鍵は１つ又は複数のチャンネルを介して送受信されてもよい。例えば、ＦＩＤＯ秘密鍵は帯域外チャンネルを介して送受信される。第１の装置１０５のプロセッサ１０２は、通信インターフェース１０７の認証装置１１０の通信フィールドへのエントリにより、ＦＩＤＯ

秘密鍵を認証装置１１０に送信するように構成される。いくつかの例では、エントリは、１つ又は複数のタップ、スワイプ、ウェーブ、及び／又はそれらの任意の組み合わせを含むがこれらに限定されず、１つ又は複数のジェスチャに関連付けられてもよい。認証装置１１０は、検証のために、サーバ装置１２０のプロセッサ１２２に第１のＦＩＤＯ鍵を送信するように構成されてもよく、従って、認証装置１１０は、第１の装置１０５とサーバ装置１２０のプロセッサ１２２との間の仲介装置として機能するように構成されてもよい。

【００４２】

プロセッサ１２２は、第２のＦＩＤＯ鍵を用いて、認証装置１１０から送信された署名済みチャレンジデータを検証するよう構成されてもよく、第２のＦＩＤＯ鍵は、ＦＩＤＯ公開鍵のようなもので、上述したように、公開鍵と秘密鍵のペアの一部である可能性がある。例えば、認証装置１１０で実行するための命令を含むアプリケーション１１６は、ＦＩＤＯ秘密鍵を用いてウェブサイトによって発行された第１のチャレンジに署名するように構成される。チャレンジが認証装置１１０によって署名されると、サーバ装置１２０のメモリ１２４に保存されているＦＩＤＯ公開鍵を用いて検証するために、プロセッサ１２２に送信される。

【００４３】

プロセッサ１２２は、第２の命令を生成するように構成されてもよい。例えば、第２の命令は、入力データを送信する第２の要求を含むことができる。命令生成後、プロセッサ１２２は、第２の命令を送信するように構成されてもよい。例えば、プロセッサ１２２は、第２の命令を認証装置１１０に送信するように構成されてもよい。いくつかの例では、第２の命令は、プロセッサ１２２によって、１つ又は複数のプッシュ通知を用いてアプリケーション１１６に転送されてもよい。いくつかの例では、第２の命令は、プロセッサ１２２及び／又はデータベース１２５による１つ又は複数の条件の評価の後に、プロセッサ１２２によって送信され得る。例えば、１つ又は複数の条件の少なくとも１つは、所定の期間にわたる認証要求のしきい値数を決定することを含み得る。例えば、プロセッサ１２２及び／又はデータベース１２５は、異常な数のトランザクション又は要求が、任意の秒数、分数、時間数、日数、週数、月数、年数などの範囲内で実行されたかどうかを判定するように構成され得る。別の例では、１つ又は複数の条件の少なくとも１つは、アカウント及び／又はユーザに関連する不正使用又は詐欺が発生したかどうかを判定することを含み得る。例えば、プロセッサ１２２及び／又はデータベース１２５は、ユーザの取引履歴が過度の購入又は異常な場所を示すか否かを判定するように構成され得る。このように、条件付き多要素認証を実施してセキュリティを向上させ、入力データを受信するための第２の命令の送信をトリガすることができる。

【００４４】

プロセッサ１２２は、第２の命令に基づいて、入力データを受信するように構成されてもよい。プロセッサ１２２は、第２の装置上で実行するための命令を含むアプリケーション１１６などから、認証装置１１０から入力データを受信するように構成されてもよい。入力データは、バイオメトリクスデータ及びクレデンシャルデータのグループから選択された少なくとも１つを含むことができる。例えば、入力データは、バイオメトリックデータ、クレデンシャルデータ、及び／又はそれらの任意の組合せを含むことができる。限定されないが、バイオメトリックデータは、指紋、顔スキャン、網膜スキャン、音声認識、及び／又はそれらの任意の組み合わせのグループから選択される少なくとも１つを含むことができる。いくつかの例では、入力データは、追加的及び／又は代替的にクレデンシャルデータを含んでもよい。これらに限定されないが、ログインデータは、ユーザ名の入力、パスワード、アカウント番号、セキュリティコード、ワンタイムパスコード、セキュリティ質問に対する回答、及び／又はそれらの任意の組み合わせのグループから選択される少なくとも１つを含むことができる。

【００４５】

プロセッサ１２２は、入力データを認証することによって認証要求を完了するように構

成されてもよい。例えば、プロセッサ１２２は、受信した入力データを基準入力データと比較することによって、１つ又は複数の結果を生成するように構成されてもよい。いくつかの例では、参照入力データはサーバ装置１２０のメモリ１２４に格納されてもよい。他の例では、基準入力データは、プロセッサ１２２によって要求されてもよい。例えば、プロセッサ１２２は、１つ又は複数の要求を通じて、基準入力データを受信するように構成されてもよいし、代わりに、基準入力データと比較するための入力データをデータベース１２５に送信するように構成されてもよい。例えば、サーバ装置１２０のプロセッサ１２２は、受信した入力データと参照入力データとの比較に基づいて照合が成功した場合に、認証が成功したことを示す結果を生成するように構成される。別の例では、サーバ装置１２０のプロセッサ１２２は、受信した入力データと参照入力データとの比較に基づき、照合が失敗した場合に認証失敗の結果を生成するように構成されてもよい。認証に失敗したと判断された場合、サーバ装置１２０のプロセッサ１２２は、入力データの認証に成功する前に、所定の試行回数まで、及びその試行回数を含めて、入力データを再認証するように構成され得る。認証要求を完了するように、又は認証要求の完了を中止する。このように、システム１００は、前述の機能性をサポートするために、分散記憶装置、クラウドベースの記憶装置、及び他の形態の記憶装置を用いて実装することができる。

【００４６】

図２Ａは、１つ又は複数の第１の装置２００を示す。第１の装置２００は、図１に関して上記で説明したように、第１の装置１０５の同一又は類似の構成要素を参照することができる。図２Ａ及び図２Ｂは、第１の装置２００の構成要素の単一インスタンスを図示すが、任意の数の構成要素を利用することができる。

【００４７】

第１の装置２００は、システム１００の１つ又は複数の構成要素と通信するように構成されてもよい。第１の装置２００は、接触型カード（例えば、磁気ストライプのスワイプ又はチップリーダへの挿入によって読み取られるカード）又は非接触型カードで構成される。第１の装置２００は、第１の装置２００の前面又は背面に表示されたサービスプロバイダ２０５によって発行されたクレジットカード、デビットカード、ギフトカードなどの支払いカードで構成されてもよい。いくつかの例では、第１の装置２００は、決済カードとは関係なく、限定されないが、ＩＤカード、会員カード、及び交通カードで構成されてもよい。一部の例では、支払カードは、デュアルインターフェース非接触支払カードから構成されてもよい。

【００４８】

第１の装置２００は、プラスチック、金属、及び他の材料から構成される単層又は１つ又は複数の「積層された層」を含むことができる基板２１０から構成されることができる。例示的な基板には、ポリ塩化ビニル、ポリ塩化ビニルアセテート、アクリロニトリルブタジエンスチレン、ポリカーボネート、ポリエステル、陽極酸化チタン、パラジウム、金、カーボン、紙、生分解性材料などがある。いくつかの例では、第１の装置２００は、ＩＳＯ／ＩＥＣ７８１０規格のＩＤ－１フォーマットに準拠した物理的特性を有してもよく、第１の装置２００は、そうでなければＩＳＯ／ＩＥＣ１４４４３規格に準拠していてもよい。しかしながら、本開示による第１の装置２００は異なる特性を有してもよく、本開示は支払いカードへの実装を必要としないことが理解される。

【００４９】

第１の装置２００は、カードの前面及び／又は背面に表示される識別情報２１５と、接触パッド２２０も含むことができる。接触パッド２２０は、ユーザ機器、スマートフォン、ラップトップ、デスクトップ、又はタブレットコンピュータを含むがこれらに限定されない、他の通信機器との接触を確立するように構成され得る。第１の装置２００は、処理回路、アンテナ、及び図２Ａには示されていない他の構成要素も含むことができる。これらの構成要素は、接触パッド２２０の裏側又は基板２１０上の他の場所に配置することができる。第１の装置２００は、磁気ストリップ又はテープも含むことができ、これはカードの裏面に位置することができる（図２Ａには図示せず）。

【００５０】
図２Ｂに示されるように、図２Ａの接触パッド２２０は、情報を記憶し処理するための処理回路２２５を含むことができる、処理回路は、マイクロプロセッサなどのプロセッサ２３０とメモリ２３５を含む。処理回路２２５には、プロセッサ、メモリ、エラー及びパリティ／ＣＲＣチェッカ、データエンコーダ、アンチコリジョンアルゴリズム、コントローラ、コマンドデコーダ、セキュリティプリミティブ、改ざん防止ハードウェアなど、本明細書で説明する機能を実行するために必要な追加コンポーネントなどの、さらなる構成要素が含まれている可能性があることを理解されたい。
【００５１】
メモリ２３５は、例えば、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭなどの読み出し専用メモリ、書き込み一回読み出しマルチメモリ、又は読み出し／書き込みメモリであってよく、第１の装置２００は、これらのメモリのうちの１つ又は複数を含んでよい。読み出し専用メモリは、読み出し専用として工場でプログラム可能であってもよいし、１回限りのプログラム可能であってもよい。ワンタイムプログラマブルは、一度書き込んだ後に何度も読み出す機会を提供する。ライトワンス／リードマルチプルメモリは、メモリチップが工場から出荷された後の時点でプログラムすることができる。一度プログラムされたメモリは、書き直すことはできないが、何度でも読み出すことができる。読み出し／書き込みメモリは、工場出荷後に何度もプログラムされ、再プログラムされる可能性がある。また、何度も読み出すことができる。
【００５２】
メモリ２３５は、１つ又は複数のアプレット２４０、１つ又は複数のカウンタ２４５、及び顧客識別子２５０を記憶するように構成され得る。１つ又は複数のアプレット２４０は、Ｊａｖａカードアプレットなど、１つ又は複数の接触型カード又は非接触型カード上で実行されるように構成された１つ又は複数のソフトウェアアプリケーションで構成されてもよい。しかしながら、アプレット２４０は、Ｊａｖａカードアプレットに限定されるものではなく、その代わりに、接触型カード又は非接触型カード、又は限られたメモリを有する他の装置上で動作可能な任意のソフトウェアアプリケーションであってもよいことが理解される。１つ以上のカウンタ２４５は、整数を記憶するのに十分な数値カウンタで構成されてもよい。顧客識別子２５０は、第１の装置２００のユーザに割り当てられた一意の英数字識別子から構成されてもよく、識別子は、非接触型カードのユーザを他の非接触型カードのユーザから区別してもよい。いくつかの例では、顧客識別子２５０は、顧客とその顧客に割り当てられたアカウントとの両方を識別することができ、さらに、顧客のアカウントに関連付けられた非接触型カードを識別することができる。
【００５３】
前述の例示的な実施形態のプロセッサ及びメモリ要素は、接触パッドを参照して説明されているが、本開示はこれに限定されない。これらの要素は、接触パッド２２０の外部に実装されてもよいし、接触パッド２２０から完全に分離されてもよいし、接触パッド２２０内に配置されたプロセッサ２３０及びメモリ２３５要素に加えて、さらなる要素として実装されてもよいことが理解される。
【００５４】
いくつかの例では、第１の装置２００は１つ又は複数のアンテナ２５５を含んでいてもよい。１つ以上のアンテナ２５５は、第１の装置２００内で、接触パッド２２０の処理回路２２５の周囲に配置されてもよい。例えば、１つ又は複数のアンテナ２５５は処理回路２２５と一体であってもよく、１つ又は複数のアンテナ２５５は外部ブースターコイルと共に使用されてもよい。別の例として、１つ又は複数のアンテナ２５５は、接触パッド２２０及び処理回路２２５の外部にあってもよい。
【００５５】
一実施形態では、第１の装置２００のコイルは、空芯変圧器の二次側として機能してもよい。端末は、電力又は振幅変調を切断することによって第１の装置２００と通信してもよい。第１の装置２００は、第１の装置の電力接続のギャップを用いて、端末から送信さ

れたデータを推測してもよく、このギャップは、１つ又は複数のキャパシタを用いて機能的に維持されてもよい。第１の装置２００は、第１の装置のコイルの負荷を切り替えるか、又は負荷変調を行うことによって通信を返してもよい。負荷変調は、干渉によって端末のコイルで検出される場合がある。

【００５６】

図３は、認証方法３００を示す。図３は、図１のシステム１００、及び図２Ａ及び図２Ｂの第１の装置２００の同一又は類似の構成要素を参照することができる。

【００５７】

ブロック３０５において、方法３００は、プロセッサにおいて、１つ又は複数のチャレンジを受信することを含み得る。例えば、依拠当事者装置又はサーバ装置は、第１のチャレンジを生成するように構成されてもよい。いくつかの例では、依拠当事者装置は、モバイル装置のプロセッサなどの認証装置にログインをチャレンジするように構成されてもよい。第１のチャレンジは、適切なＦＩＤＯ鍵ペアを選択するために使用される、ユーザ識別子やサイト識別子などの識別子を含むことができる。第１のチャレンジは、さらに、リプレイを防ぐために使用される、依拠当事者装置によって与えられる予測不可能な番号を含むことができる。例えば、認証のインスタンスごとに、新しい予測不可能な番号が必要となり、そのため予測不可能な番号は毎回異なる。このようにして、古い予測不可能な番号の署名を利用することを回避し、代わりに認証のインスタントセッションの番号を利用する。

【００５８】

一部の例では、第１の要求は認証要求で構成される。認証要求は、ＦＩＤＯ２（Ｆａｓｔ Ｉｄｅｎｔｉｔｙ Ｏｎｌｉｎｅ ２）ウェブサイト登録要求を含む。プロセッサは、１つ又は複数の命令を生成するように構成されてもよい。例えば、プロセッサは、第１の命令を生成するように構成される。各命令は、１つ又は複数の要求を含むことができる。第１の命令は、第１の装置のプロセッサから第１の鍵を取得するための第１の要求を含むことができる。鍵はＦＩＤＯ鍵を含む。第１の鍵は、第１の装置の通信インターフェースの通信フィールドへの入力により取得されてもよい。いくつかの例では、第１の命令は、第１の装置のプロセッサによって第１の鍵を生成する要求を含む。他の例では、第１の命令は、第１のＦＩＤＯ鍵を再生成する要求を含むことができ、第１の装置のプロセッサは、公開鍵／秘密鍵ペアの一部である秘密鍵などを使用する。

【００５９】

ブロック３１０において、方法３００は、プロセッサによって、第１の装置から第１のＦａｓｔ Ｉｄｅｎｔｉｔｙ Ｏｎｌｉｎｅ（ＦＩＤＯ）鍵を取得する要求を含む第１の命令を生成することを含む場合がある。例えば、依拠当事者装置から受信した第１のチャレンジに基づき、モバイル装置のプロセッサなどの認証装置は、１つ又は複数の命令を生成することにより、第１の装置の１つ又は複数の入力を促すように構成される。例えば、１つ又は複数の入力は、タップ、スワイプ、ウェーブなどのグループから選択された少なくとも１つ、及び／又はそれらの任意の組み合わせを含むことができる。第１の命令は、第１の装置によって第１のＦＩＤＯ鍵を生成する要求を含む場合がある。いくつかの例では、第１のＦＩＤＯ鍵は、１つ又は複数の暗号アルゴリズムを用いて、マスター鍵と第１の要求に関連付けられた識別子に基づいて生成される。例えば、識別子はサイト識別子を含み、マスター鍵と組み合わされて鍵ペアを生成する。一部の例では、マスター鍵は第１の装置に保存され、マスター鍵は第１の装置上でサイト識別子と組み合わされて秘密鍵が生成される。他の例では、マスター鍵は、第１の装置から、第２の装置上で実行するための命令を含むアプリケーションに転送されてもよく、マスター鍵とサイト識別子の結合は、秘密鍵を生成するために第２の装置のアプリケーションによって実行される。一部の例では、ＦＩＤＯ秘密鍵を第１の装置で生成又は保存するのではなく、第１のＦＩＤＯ鍵を第２の装置に属するセキュアエレメントで生成又は保存してもよい。例えば、ＦＩＤＯ秘密鍵は第２の装置が保持するセキュアエレメントに格納される。いくつかの例では、セキュアエレメントは、１つ又は複数の鍵が安全に保管され、サーバ装置によって取り出され

る耐タンパー（不正改ざん）性のセキュア記憶装置エリアを構成することができる。
【００６０】
ブロック３１５において、方法３００は、プロセッサによって、第１の命令を送信することを含み得る。例えば、プロセッサは、第１の命令を第１の装置に送信するように構成されてもよい。いくつかの例では、第１の命令は、認証装置によって第１の装置のプロセッサに送信されてもよい。命令生成後、認証装置は、第１の命令を第１の装置に送信するように構成される。
【００６１】
ブロック３２０において、方法３００は、第１のＦＩＤＯ鍵を受信することを含み得る。例えば、第１の装置の通信インターフェースは、第１のＦＩＤＯ鍵を転送するために、モバイル装置の通信フィールドなど、認証装置の通信フィールドに入力することができる。第１の装置は、認証装置から受信した第１の命令に応じて、特定のユーザ又はサイトに関連するＦＩＤＯ鍵ペアを生成又は取得するように構成される。生成又は取得されたＦＩＤＯ鍵ペアは、認証装置によって読み取られる。ＦＩＤＯ鍵ペアは、認証装置が第１の装置から読み取ることができるＦＩＤＯ秘密鍵を含み、認証装置が署名されたチャレンジデータをもたらす第１のチャレンジに署名するために使用することができる。ＦＩＤＯ秘密鍵は、第１の装置の通信インターフェースが通信フィールドに入力されることにより取得される。一部の例では、ＦＩＤＯ秘密鍵は、認証装置に転送される前に、第１の機器によって暗号化されてもよく、この場合、モバイル機器のプロセッサは、受信した暗号化されたＦＩＤＯ秘密鍵を復号化するように構成されてもよい。
【００６２】
いくつかの例では、ＦＩＤＯ秘密鍵は、１つ又は複数の暗号化アルゴリズムを用いて、マスター鍵及び認証要求に関連付けられた識別子に基づいて生成される。例えば、識別子はサイト識別子を含み、マスター鍵と組み合わされて別の鍵ペアが生成される。第１の装置は、鍵を再生成する必要がないように、有限数の鍵をメモリに保存するように構成される。他の例では、認証装置からの第１の命令は、例えば、公開鍵／秘密鍵ペアの一部である秘密鍵など、ＦＩＤＯ秘密鍵を再生成する要求を含む。
【００６３】
いくつかの例では、マスター鍵は第１の装置上のメモリに保存され、マスター鍵は第１の装置上のサイト識別子と組み合わされてＦＩＤＯ秘密鍵が生成される。他の例では、マスター鍵は第１の装置から認証装置へ転送され、認証装置によってマスター鍵とサイト識別子の結合が行われ、ＦＩＤＯ秘密鍵が生成される。
【００６４】
いくつかの例では、第１の装置から認証装置へのＦＩＤＯ秘密鍵の送信は防止される。例えば、第１の装置が第１のチャレンジの署名を実行する際、ＦＩＤＯ秘密鍵のＯＴＡ（Ｏｖｅｒ　ｔｈｅ　Ａｉｒ）送信は回避される。従って、第１のチャレンジとサイト又はユーザ識別子情報は、認証装置から第１の装置に送信され、これにより、認証装置は、プロキシプロトコルを用いて近距離無線通信（ＮＦＣ）を用いて第１の装置に計算を配布する。
【００６５】
いくつかの例では、ＦＩＤＯ秘密鍵は、第１の装置において生成又は保存されるのではなく、認証装置に属するセキュアエレメントにおいて生成又は保存される。例えば、ＦＩＤＯ秘密鍵は、第２の装置が保持するセキュアエレメントに格納される。いくつかの例では、セキュアエレメントは、１つ又は複数の鍵が安全に保管され、依拠当事者装置によって取り出されうる、耐タンパー性の安全な保管領域を含んでいてもよい。
【００６６】
一部の例では、第１の装置のプロセッサは、ＦＩＤＯ秘密鍵を生成するように構成されてもよい。第１の装置のプロセッサは、ＦＩＤＯ秘密鍵を送信するように構成される。例えば、第１の装置のプロセッサは、例えば第２の装置上で実行するための命令を含むアプリケーションなどの、ＦＩＤＯ秘密鍵を認証装置に送信するように構成される。上述した

ように、認証装置は、限定するものではないが、ラップトップ、タブレット、電話などのモバイル装置であってもよい。いくつかの例では、ＦＩＤＯ秘密鍵は１つ又は複数のチャンネルを介して送受信される。例えば、ＦＩＤＯ秘密鍵は帯域外チャンネルを介して送受信される。第１の装置のプロセッサは、第１の装置の通信インターフェースから認証装置の通信フィールドへの入力により、ＦＩＤＯ秘密鍵を認証装置に送信するように構成される。いくつかの例では、エントリは１つ又は複数のジェスチャに関連付けられ、これらのジェスチャには、１つ又は複数のタップ、スワイプ、ウェーブ、及び／又はそれらの任意の組み合わせが含まれるが、これらに限定されない。

【００６７】

例えば、第１の装置のプロセッサは、第１のＦＩＤＯ鍵を生成するように構成されてもよい。第１の装置のプロセッサは、第１のＦＩＤＯ鍵を送信するように構成されてもよい。例えば、第１の装置のプロセッサは、第１のＦＩＤＯ鍵を、第２の装置上で実行するための命令を含むアプリケーションに送信するように構成されてもよい。上述したように、第２の装置は、限定されるものではないが、ラップトップやタブレット、電話などのモバイル装置であってもよい。一部の例では、第１のＦＩＤＯ鍵は１つ又は複数のチャンネルを介して送受信されてもよい。例えば、第１のＦＩＤＯ鍵は帯域外チャンネルを介して送受信される。第１の装置のプロセッサは、第２の装置の通信フィールドへの通信インターフェースのエントリにより、第１のＦＩＤＯ鍵を第２の装置のアプリケーションに送信するように構成されてもよい。いくつかの例では、エントリは１つ又は複数のジェスチャに関連付けられる、これらのジェスチャには、１つ又は複数のタップ、スワイプ、ウェーブ、及び／又はそれらの任意の組み合わせが含まれるが、これらに限定されない。第２の装置のアプリケーションは、検証のために第１のＦＩＤＯ鍵をサーバ装置のプロセッサに送信するように構成されてもよく、従って、第２の装置は、第１の装置とプロセッサとの間の仲介装置として機能するように構成されてもよい。

【００６８】

ブロック３２５において、方法３００は、プロセッサによって、第１のＦＩＤＯ鍵を用いて１つ又は複数のチャレンジに署名することを含むことができる。

【００６９】

ブロック３３０において、方法３００は、プロセッサによって、第２のＦＩＤＯ鍵を用いた検証のために、１つ又は複数の署名されたチャレンジを送信することを含み得る。例えば、プロセッサは、１つ又は複数の署名されたチャレンジを依拠当事者装置に送信するように構成される。依拠当事者装置は、モバイル装置のプロセッサなどの認証装置から署名済みチャレンジデータを受信することができる。依拠当事者装置は、署名されたチャレンジデータの検証を行ってもよい。例えば、依拠当事者装置は、署名されたチャレンジデータを、ユーザがサイトに登録した際に保存されたＦＩＤＯ公開鍵で検証することができる。検証は、署名検証を含む認証プロセスの結果で構成される。認証装置は、検証のために、依拠当事者装置のプロセッサに第１のＦＩＤＯ鍵を送信するように構成される場合があり、従って、認証装置は、第１の装置と依拠当事者装置のプロセッサとの間の仲介装置として機能するように構成されてもよい。

【００７０】

依拠当事者装置は、ウェブサイトのＦＩＤＯサービスを用いてＦＩＤＯ秘密鍵を検証するように構成される。依拠当事者装置は、上述した公開鍵／秘密鍵ペアの一部であるＦＩＤＯ公開鍵などの第２のＦＩＤＯ鍵を用いて、認証装置から送信された署名済みチャレンジデータを検証するように構成されてもよい。例えば、第２の装置上で実行するための命令を含むアプリケーションは、ＦＩＤＯ秘密鍵を用いてウェブサイトによって発行された第１のチャレンジに署名するように構成される。チャレンジがオーセンティケータによって署名されると、サーバ装置のメモリに保存されているＦＩＤＯ公開鍵を用いて検証するために、プロセッサに送信される。

【００７１】

依拠当事者装置は、第２の命令を生成するように構成されてもよい。例えば、第２の命

令は、入力データを送信する第２の要求を含むことができる。命令生成後、依拠当事者装置は、第２の命令を送信するように構成されてもよい。例えば、依拠当事者装置は、第２の命令を認証装置に送信するように構成される。一部の例では、第２の命令は、依拠当事者装置によって、１つ又は複数のプッシュ通知を用いてアプリケーションに転送される場合がある。いくつかの例では、第２の命令は、依拠当事者装置及び／又はデータベースによる１つ又は複数の条件の評価後に、依拠当事者装置によって送信される場合がある。例えば、１つ又は複数の条件の少なくとも１つは、所定の期間にわたる認証要求のしきい値数を決定することを含む場合がある。例えば、依拠当事者装置及び／又はデータベースは、異常な数のトランザクション又は要求が、任意の秒数、分数、時間数、日数、週数、月数、年数などの範囲内で実行されたかどうかを判断するように構成され得る。別の例では、１つ又は複数の条件の少なくとも１つは、アカウント及び／又はユーザに関連する不正使用又は詐欺が発生したかどうかを判断することを含む場合がある。例えば、依拠当事者装置及び／又はデータベースは、ユーザの取引履歴が過度の購入又は異常な場所を示すかどうかを判断するように構成されてもよい。このように、条件付き多要素認証を実施してセキュリティを向上させ、入力データを受信するための第２の命令の送信をトリガすることができる。

【００７２】

依拠当事者装置は、第２の命令に基づいて、入力データを受信するように構成され得る。依拠当事者装置は、第２の装置上で実行するための命令を含むアプリケーションからなど、認証装置から入力データを受信するように構成されてもよい。入力データは、バイオメトリクスデータ及びクレデンシャルデータのグループから選択された少なくとも１つを含むことができる。例えば、入力データは、バイオメトリックデータ、クレデンシャルデータ、及び／又はそれらの任意の組合せを含むことができる。限定されないが、バイオメトリックデータは、指紋、顔スキャン、網膜スキャン、音声認識、及び／又はそれらの任意の組み合わせの群から選択される少なくとも１つを含むことができる。いくつかの例では、入力データは追加的及び／又は代替的にクレデンシャルデータを含むことができる。限定するものではないが、ログインデータは、ユーザ名、パスワード、アカウント番号、セキュリティコード、ワンタイムパスコード、セキュリティ質問に対する回答、及び／又はそれらの任意の組み合わせの入力のグループから選択される少なくとも１つを含むことができる。

【００７３】

依拠当事者装置は、入力データを認証することによって認証要求を完了するように構成される。例えば、依拠当事者装置は、受信した入力データを参照入力データと比較することによって、１つ又は複数の結果を生成するように構成されてもよい。一部の例では、参照入力データは、依拠当事者装置のメモリに格納されてもよい。他の例では、参照入力データは、依拠当事者装置によって要求される場合がある。例えば、依拠当事者装置は、１つ又は複数の要求を通じて、基準入力データを受信するように構成されてもよいし、代わりに、基準入力データと比較するための入力データをデータベースに送信するように構成されてもよい。例えば、依拠当事者装置のプロセッサは、受信した入力データと参照入力データとの比較に基づいて照合が成功した場合に、認証が成功したことを示す結果を生成するように構成される。別の例では、依拠当事者装置のプロセッサは、受信した入力データと参照入力データとの比較に基づいて照合が失敗した場合、認証失敗の結果を生成するように構成される。認証に失敗したと判断された場合、前記依拠当事者装置のプロセッサは、前記入力データの認証に成功する前に、前記入力データを所定の試行回数まで再認証するように構成される場合があり認証要求を完了するように、又は認証要求の完了を中止する。このように、認証システムは、前述の機能性をサポートするために、分散記憶装置、クラウドベースの記憶装置、及び他の形式の記憶装置を実装することができる。

【００７４】

図４は、例示的な実施形態に係る認証プロセスのシーケンス図４００を示す。図４は、システム１００、図２Ａ及び図２Ｂの第１の装置２００、ならびに図３の方法３００の同

一又は類似の構成要素を参照することができる。

【００７５】

ステップ４０５で、プロセッサが認証要求を受信するように構成されてもよい。一例として、プロセッサは、依拠当事者装置又はサーバ装置の一部である場合がある。一部の例では、認証要求は、ＦＩＤＯ２（Ｆａｓｔ　Ｉｄｅｎｔｉｔｙ　Ｏｎｌｉｎｅ　２）ウェブサイト登録の要求で構成される。例えば、要求はブラウザ拡張機能から受信される。

【００７６】

ステップ４１０において、プロセッサは、認証要求に応答して、１つ又は複数のチャレンジを生成するように構成されてもよい。例えば、プロセッサは、第１のチャレンジを生成するように構成される。いくつかの例では、依拠当事者装置は、例えばモバイル装置のプロセッサなどがログインするなど、認証装置にチャレンジするように構成される、第１のチャレンジは、例えば、識別子を含むことができる。第１のチャレンジは、さらに、リプレイを防ぐために使用される、依拠当事者装置によって与えられる予測不可能な番号を含むことができる。例えば、認証のインスタンスごとに、新しい予測不可能な番号が必要となり、そのため予測不可能な番号は毎回異なる。このようにして、古い予測不可能な番号の署名を利用することを回避し、代わりに認証のインスタントセッションの番号を利用する。

【００７７】

ステップ４１５において、プロセッサは、第１のチャレンジを送信するように構成されてもよい。例えば、プロセッサは、第１の命令を認証装置に送信するように構成される、例えば、アプリケーションは装置上で実行するための命令を含んでおり、装置はモバイル装置を含むがこれに限定されない。

【００７８】

ステップ４２０において、第１の命令が第１の装置に送信されてもよい。例えば、第１の命令は、認証装置によって生成及び／又はカードのプロセッサに送信されてもよい。プロセッサは、１つ又は複数の命令を生成するように構成されてもよい。例えば、プロセッサは、第１の命令を生成するように構成されてもよい。各命令は、１つ又は複数の要求を含むことができる。第１の命令には、第１の装置のプロセッサから第１の鍵を取得するための第１の要求が含まれる。鍵はＦＩＤＯ鍵を含む。第１の鍵は、第１の装置の通信インターフェースから、認証装置の通信フィールドなどの通信フィールドに入力することで取得できる。いくつかの例では、第１の命令は、第１の装置のプロセッサによって第１の鍵を生成する要求を含むことができる。他の例では、第１の命令は第１のＦＩＤＯ鍵を再生成する要求を含み、第１の装置のプロセッサは、公開鍵／秘密鍵ペアの一部である秘密鍵などを使用する。

【００７９】

例えば、依拠当事者装置から受け取った第１のチャレンジに基づいて、モバイル装置のプロセッサなどの認証装置は、１つ又は複数の命令を生成することによって、第１の装置の１つ又は複数の入力を促すように構成されてもよい。例えば、１つ又は複数の入力は、タップ、スワイプ、ウェーブなどのグループから選択された少なくとも１つ、及び／又はそれらの任意の組み合わせを含むことができる。第１の命令は、第１の装置によって第１のＦＩＤＯ鍵を生成する要求を含む場合がある。いくつかの例では、第１のＦＩＤＯ鍵は、１つ又は複数の暗号アルゴリズムを用いて、マスター鍵と第１の要求に関連付けられた識別子に基づいて生成される。例えば、識別子はサイト識別子を含み、マスター鍵と組み合わされて鍵ペアを生成する。一部の例では、マスター鍵は第１の装置に保存され、マスター鍵は第１の装置上でサイト識別子と組み合わされて秘密鍵が生成される。

【００８０】

ステップ４２５において、第１の装置のプロセッサは、第１のＦＩＤＯ鍵を生成し、送信するように構成される。例えば、第１の装置の通信インターフェースは、第１のＦＩＤＯ鍵を転送するために、モバイル装置の通信フィールドなど、認証装置の通信フィールドに入力することができる。第１の装置は、認証装置から受信した第１の命令に応じて、特

定のユーザ又はサイトに関連するＦＩＤＯ鍵ペアを生成又は取得するように構成される。生成又は取得されたＦＩＤＯ鍵ペアは、認証装置によって読み取られる。ＦＩＤＯ鍵ペアは、認証装置が第１の装置から読み取ることができるＦＩＤＯ秘密鍵を含み、認証装置が第１のチャレンジに署名するために使用することができる。ＦＩＤＯ秘密鍵は、第１の装置の通信インターフェースが通信フィールドに入力されることで取得される。いくつかの例では、ＦＩＤＯ秘密鍵は、認証装置に転送される前に、第１の機器によって暗号化され、この場合、モバイル装置のプロセッサは、受信した暗号化されたＦＩＤＯ秘密鍵を復号化するように構成される。

【００８１】

いくつかの例では、ＦＩＤＯ秘密鍵は、１つ又は複数の暗号化アルゴリズムを用いて、マスター鍵及び認証要求に関連付けられた識別子に基づいて生成される。例えば、識別子はサイト識別子を含み、マスター鍵と組み合わされて別の鍵ペアが生成される。第１の装置は、鍵を再生成する必要がないように、有限数の鍵をメモリに保存するように構成される。他の例では、認証装置からの第１の命令は、例えば、公開鍵／秘密鍵ペアの一部である秘密鍵などの、ＦＩＤＯ秘密鍵を再生成する要求を含む。

【００８２】

いくつかの例では、マスター鍵は第１の装置上のメモリに保存され、マスター鍵は第１の装置上のサイト識別子と組み合わされてＦＩＤＯ秘密鍵を生成する。他の例では、マスター鍵は第１の装置から認証装置に転送され、ＦＩＤＯ秘密鍵を生成するために、マスター鍵とサイト識別子の結合が認証装置によって実行される。

【００８３】

いくつかの例では、第１の装置から認証装置へのＦＩＤＯ秘密鍵の送信は防止される。例えば、第１の装置が第１のチャレンジの署名を実行する際、ＦＩＤＯ秘密鍵のＯＴＡ（Ｏｖｅｒ　ｔｈｅ　Ａｉｒ）送信は回避される。このように、第１のチャレンジとサイト又はユーザ識別子情報は、認証装置から第１の装置に送信され、これにより、プロキシプロトコルを用いて近距離無線通信（ＮＦＣ）を通じて第１の装置に計算を分配する。

【００８４】

いくつかの例では、ＦＩＤＯ秘密鍵は、第１の装置において生成又は保存されるのではなく、認証装置に属するセキュアエレメントにおいて生成又は保存される。例えば、ＦＩＤＯ秘密鍵は、第２の装置が保持するセキュアエレメントに格納される。いくつかの例では、セキュアエレメントは、１つ又は複数の鍵が安全に保管され、依拠当事者装置によって取得される耐タンパー性のセキュア記憶装置エリアから構成される。

【００８５】

一部の例では、第１の装置のプロセッサは、ＦＩＤＯ秘密鍵を生成するように構成されてもよい。第１の装置のプロセッサは、例えば、第１の装置のプロセッサは、例えば、第２の装置上で実行するための命令を含むアプリケーションなどの、ＦＩＤＯ秘密鍵を認証装置に送信するように構成される。上述したように、認証装置は、限定するものではないが、ノートパソコン、タブレット、電話などのモバイル機器であってもよい。一部の例では、ＦＩＤＯ秘密鍵は１つ又は複数のチャンネルを介して送受信されてもよい。例えば、ＦＩＤＯ秘密鍵は帯域外チャンネルを介して送受信される。第１の装置のプロセッサは、第１の装置の通信インターフェースの認証装置の通信フィールドへのエントリにより、ＦＩＤＯ秘密鍵を認証装置に送信するように構成されてもよい。いくつかの例では、エントリは、１つ又は複数のジェスチャに関連付けられてもよく、これらのジェスチャには、１つ又は複数のタップ、スワイプ、ウェーブ、及び／又はそれらの任意の組み合わせが含まれるが、これらに限定されない。

【００８６】

ステップ４３０において、認証装置は、第１のＦＩＤＯ鍵を受信するように構成される。例えば、第２の装置のアプリケーションは、第１の装置のプロセッサから第１のＦＩＤＯ秘密鍵を受信するように構成される。認証装置は、受信した第１のＦＩＤＯ鍵を用いて第１のチャレンジに署名するように構成される。認証装置は、署名された第１のチャレン

ジを検証のために依拠当事者装置に送信するように構成される。
【００８７】
ステップ４３５において、依拠当事者装置又はサーバ装置のプロセッサは、署名された第１のチャレンジを検証するように構成されてもよい。例えば、依拠当事者装置又はサーバ装置のプロセッサは、認証装置から署名された第１のチャレンジを受信するように構成される。例えば、依拠当事者装置は、ユーザがサイトに登録したときに保存されたＦＩＤＯ公開鍵で、署名されたチャレンジデータを検証することができる。検証は、署名検証を含む認証プロセスの結果を構成することができる。認証装置は、検証のために、第１のＦＩＤＯ鍵を依拠当事者装置のプロセッサに送信するように構成されてもよく、従って、認証装置は、第１の装置と依拠当事者装置のプロセッサとの間の仲介装置として機能するように構成されてもよい。
【００８８】
ステップ４４０において、依拠当事者装置又はサーバ装置のプロセッサは、第２の命令を生成するように構成され得る。例えば、第２の命令は、入力データを送信する第２の要求を含むことができる。いくつかの例では、プロセッサは、１つ又は複数の条件を評価するように構成されてもよい。例えば、第２の命令は、１つ又は複数の条件の評価後にプロセッサによって送信される。例えば、１つ又は複数の条件の少なくとも１つには、所定の期間にわたる認証要求のしきい値数を決定することが含まれる。例えば、プロセッサは、異常な数のトランザクション又は要求が、任意の秒数、分数、時間数、日数、週数、月数、年数などの範囲内で実行されたかどうかを判定するように構成され得る。別の例では、１つ又は複数の条件の少なくとも１つは、アカウント及び／又はユーザに関連する不正使用又は詐欺が発生したかどうかを判定することを含むことができる。例えば、プロセッサは、ユーザの取引履歴が過度の購入又は異常な場所を示すかどうかを判定するように構成されてもよい。このようにして、セキュリティを向上させるために条件付き多要素認証が実装されてもよく、これにより、入力データを受信するための第２の命令の送信がトリガされてもよい。
【００８９】
ステップ４４５において、認証装置は、第２の命令を受信するように構成されてもよい。例えば、モバイル装置のプロセッサは、依拠当事者装置又はサーバ装置による１つ又は複数の条件の評価後に、依拠当事者装置又はサーバ装置のプロセッサから第２の命令を受信するように構成されてもよい。いくつかの例では、第２の命令は、例えば、１つ又は複数のプッシュ通知を用いてモバイル装置で実行するための命令を含むアプリケーションなどであり、依拠当事者装置又はサーバ装置のプロセッサによって認証装置に転送される。
【００９０】
ステップ４５０において、認証装置は、第２の命令に基づいて、入力データを送信するよう構成される。例えば、モバイル装置のプロセッサ又はアプリケーションは、入力データをサーバ装置のプロセッサなどの依拠当事者装置に送信するように構成することができる。入力データは、バイオメトリクスデータ及びクレデンシャルデータのグループから選択された少なくとも１つを含むことができる。例えば、入力データは、バイオメトリックデータ、クレデンシャルデータ、及び／又はそれらの任意の組合せを含むことができる。限定されないが、バイオメトリックデータは、指紋、顔スキャン、網膜スキャン、音声認識、及び／又はそれらの任意の組み合わせのグループから選択される少なくとも１つを含むことができる。いくつかの例では、入力データは、追加的及び／又は代替的に、クレデンシャルデータを含み得る。限定されないが、ログインデータは、ユーザ名、パスワード、口座番号、セキュリティコード、ワンタイムパスコード、セキュリティ質問に対する回答、及び／又はそれらの任意の組み合わせの入力のグループから選択される少なくとも１つを含むことができる。
【００９１】
ステップ４５５で、依拠当事者装置又はサーバ装置は、入力データを認証することによって認証要求を完了するように構成される。例えば、依拠当事者装置又はサーバ装置のプ

ロセッサは、例えば、モバイル機器の実行命令を構成するプロセッサやアプリケーションなどの、認証装置から入力データを受信するよう構成される。いくつかの例では、依拠当事者装置又はサーバ装置のプロセッサは、受信した入力データを参照入力データと比較することによって、１つ又は複数の結果を生成するように構成され得る。いくつかの例では、参照入力データは、依拠当事者装置又はサーバ装置によって記憶される場合がある。他の例では、参照入力データは、依拠当事者装置又はサーバ装置によって要求される場合がある。例えば、依拠当事者装置又はサーバ装置のプロセッサは、１つ又は複数の要求を通じて、基準入力データを受信するように構成されてもよいし、代わりに、基準入力データと比較するための入力データをデータベースに送信するように構成されてもよい。例えば、依拠当事者装置又はサーバ装置は、受信した入力データと参照入力データとの比較に基づいて照合が成功した場合、認証が成功したことを示す結果を生成するように構成される。別の例では、依拠当事者装置又はサーバ装置は、受信した入力データと参照入力データとの比較に基づいて照合が失敗した場合、認証失敗の結果を生成するように構成される。認証に失敗したと判断された場合、依拠当事者装置又はサーバ装置は、入力データの認証に成功する前に、認証要求を完了するように、又は認証要求の完了を中止するべく、所定の試行回数まで入力データを再認証するように構成することができる。このように、認証プロセスのシーケンス図４００は、前述の機能性をサポートするために、分散記憶装置、クラウドベースの記憶装置、及び他の形態の記憶装置を用いて実装することができる。

【００９２】

図５は、例示的な実施形態に係る認証の方法５００を示す。図５は、システム１００、図２Ａ及び図２Ｂの第１の装置２００、図３の方法３００、及び図４のシーケンス図４００の同一又は類似の構成要素を参照することができる。

【００９３】

ブロック５０５において、方法５００は、プロセッサにおいて、第１の命令を受信することを含み得る。プロセッサは、カードなどの第１の装置上で実行するための命令を含むアプリケーションを含むメモリに結合されてもよい。一部の例では、第１の命令は認証要求の完了に関連付けられてもよい。例えば、認証要求は、ＦＩＤＯ２（Ｆａｓｔ Ｉｄｅｎｔｉｔｙ Ｏｎｌｉｎｅ ２）ウェブサイト登録の要求で構成される。第１の命令は、例えば、クライアント装置やモバイル装置などの第２の装置上で実行するための命令を含むアプリケーションなどの、認証装置のプロセッサによって生成及び／又は送信される１つ又は複数の命令の一部である。例えば、認証装置のプロセッサは、第１の命令を生成するように構成される。各命令は、１つ又は複数の要求を含むことができる。第１の命令には、第１の装置のプロセッサから第１の鍵を生成又は取得するための第１の要求が含まれる。鍵は、ＦＩＤＯ秘密鍵などのＦＩＤＯ鍵から構成される。

【００９４】

第１の命令は、カードを含むがこれに限定されない第１の装置から第１のＦＩＤＯ（Ｆａｓｔ Ｉｄｅｎｔｉｔｙ Ｏｎｌｉｎｅ）鍵を取得する要求を含む場合がある。第１の命令は、第１の装置によって第１のＦＩＤＯ鍵を生成する要求を含む場合がある。一部の例では、第１のＦＩＤＯ鍵は、１つ又は複数の暗号アルゴリズムを用いて、マスター鍵及び第１の要求に関連付けられた識別子に基づいて生成される。例えば、識別子はサイト識別子を含み、マスター鍵と組み合わされて鍵ペアを生成する。一部の例では、マスター鍵は第１の装置に保存され、マスター鍵は第１の装置上でサイト識別子と組み合わされて秘密鍵が生成される。いくつかの例では、ＦＩＤＯ秘密鍵を第１の装置で生成又は保存するのではなく、第１のＦＩＤＯ鍵を、モバイル装置を含むクライアント装置などの認証装置又は第２の装置に属するセキュアエレメントで生成又は保存することができる。例えば、ＦＩＤＯ秘密鍵は、第２の装置が保持するセキュアエレメントに格納することができる。幾つかの例では、セキュアエレメントは、１つ又は複数の鍵が安全に保管され、認証装置又は依拠当事者装置サーバ装置によって取得される、耐タンパー性の安全な保管領域から構成される。例えば、認証装置は、第１の命令を第１の装置に送信するように構成され、認証装置は、第１の装置と依拠当事者装置又はサーバ装置との間の仲介装置として機能す

るように構成される。

【００９５】

ブロック５１０において、方法５００は、第１の鍵を生成することを含むことができる。例えば、第１の鍵は、第２の装置の通信インターフェースを、認証装置又はモバイル装置などのクライアント装置の通信フィールドに入力することによって取得される。いくつかの例では、第１の命令は、第１の装置による第１の鍵の生成要求を含む。他の例では、第１の命令は、例えば、公開鍵／秘密鍵ペアの一部である秘密鍵などの、第１のＦＩＤＯ鍵を再生成する要求を含むことができる。モバイル装置のプロセッサなどの認証装置は、第１の装置の１つ又は複数の入力を促すように構成されてもよい。例えば、１つ又は複数の入力は、タップ、スワイプ、ウェーブなどのグループから選択される少なくとも１つ、及び／又はそれらの任意の組み合わせを含むことができる。従って、第１の装置の通信インターフェースは、モバイル装置の通信フィールドなど、認証装置の通信フィールドに入ることができる。第１の装置は、認証装置から受信した第１の命令に基づいて、特定のユーザ又はサイトに関連付けられたＦＩＤＯ鍵ペアを生成又は取得するように構成される。第１の装置のプロセッサは、第１のエントリにより認証装置から第１の命令を受信し、第１の装置の通信インターフェースの第２のエントリにより認証装置の通信フィールドにＦＩＤＯ秘密鍵を送信するように構成されてもよい。いくつかの例では、１つ又は複数のエントリは、１つ又は複数のジェスチャに関連付けられてもよく、これらのジェスチャには、１つ又は複数のタップ、スワイプ、ウェーブ、及び／又はそれらの任意の組み合わせが含まれるが、これらに限定されない。

【００９６】

いくつかの例では、ＦＩＤＯ秘密鍵は、１つ又は複数の暗号化アルゴリズムを用いて、マスター鍵及び認証要求に関連付けられた識別子に基づいて生成される。例えば、識別子はサイト識別子を含み、マスター鍵と組み合わされて別の鍵ペアが生成される。第１の装置は、鍵を再生成する必要がないように、有限数の鍵をメモリに保存するように構成される。他の例では、認証装置からの第１の命令は、例えば、公開鍵／秘密鍵ペアの一部である秘密鍵などの、ＦＩＤＯ秘密鍵を再生成する要求を含む。

【００９７】

いくつかの例では、マスター鍵は第１の装置上のメモリに保存され、マスター鍵は第１の装置上のサイト識別子と組み合わされてＦＩＤＯ秘密鍵を生成する。他の例では、マスター鍵は第１の装置から認証装置に転送され、ＦＩＤＯ秘密鍵を生成するために、マスター鍵とサイト識別子の結合が認証装置によって実行される。

【００９８】

いくつかの例では、ＦＩＤＯ秘密鍵は、第１の装置において生成又は保存されるのではなく、認証装置に属するセキュアエレメントにおいて生成又は保存される。例えば、ＦＩＤＯ秘密鍵は、第２の装置が保持するセキュアエレメントに格納される。

【００９９】

ブロック５１５において、方法５００は、第１の鍵を暗号化することを含む。例えば、ＦＩＤＯ秘密鍵は、認証装置に転送される前に、第１の装置によって暗号化される。従って、モバイル装置のプロセッサは、１つ又は複数のチャレンジに署名する前に、受信した暗号化されたＦＩＤＯ秘密鍵を復号化するように構成される。

【０１００】

ブロック５２０において、方法５００は、検証のために暗号化された第１の鍵を送信することを含むことができる。例えば、第１の装置のプロセッサは、検証のために暗号化されたＦＩＤＯ秘密鍵を認証装置に送信するように構成される。生成又は取得されたＦＩＤＯ鍵ペアは、近距離無線通信（ＮＦＣ）を介することに限定されず、認証装置により読み取られる。ＦＩＤＯ鍵ペアは、認証装置が第１の装置から読み取ることができるＦＩＤＯ秘密鍵を含む。ＦＩＤＯ秘密鍵は、第１の装置の通信インターフェースから認証装置の通信フィールドへの１つ又は複数のエントリにより取得される。

【０１０１】

いくつかの例では、暗号化されたＦＩＤＯ秘密鍵の第１装置から認証装置への送信は防止される。例えば、第１の装置が第１のチャレンジの署名を実行するように構成されている場合、ＦＩＤＯ秘密鍵の無線（ＯＴＡ）送信は回避される。従って、第１のチャレンジとサイト又はユーザ識別子情報は、認証装置から第１の装置に送信され、これにより、認証装置は、プロキシプロトコルを用いて近距離無線通信（ＮＦＣ）を用いて第１の装置に計算を配布する。

【０１０２】

一部の例では、ＦＩＤＯ秘密鍵は１つ又は複数のチャンネルを介して送受信されてもよい。例えば、ＦＩＤＯ秘密鍵は帯域外チャンネルを介して送受信される。いくつかの例では、認証装置は、帯域外チャンネルを介して第１の装置からＦＩＤＯ秘密鍵を受信するように構成される。認証装置は、検証のために、依拠当事者装置のプロセッサに第１のＦＩＤＯ鍵を送信するように構成される場合があり、従って、認証装置は、第１の装置と依拠当事者装置のプロセッサとの間の仲介装置として機能するように構成されてもよい。

【０１０３】

いくつかの例では、依拠当事者装置は、１つ又は複数の第２の命令を生成及び／又は送信するように構成され得る。例えば、第２の命令は、入力データを送信する要求を含むことができる。第２の装置のプロセッサのような認証装置は、第２の命令を受信するように構成される。例えば、第２の装置のプロセッサは、依拠当事者装置又はサーバ装置のプロセッサから入力データを送信する要求を受信するように構成され得る。いくつかの例では、第２の命令は、依拠当事者装置又はサーバ装置のプロセッサから認証装置に転送され、１つ又は複数のプッシュ通知を用いて第２装置のプロセッサなどに通知される。いくつかの例では、第２の命令は、依拠当事者装置又はサーバ装置による１つ又は複数の条件の評価後に、認証装置によって受信されてもよい。例えば、１つ又は複数の条件の少なくとも１つは、所定の期間にわたる認証要求のしきい値数を決定することを含む。例えば、依拠当事者装置は、異常な数のトランザクション又は要求が、秒、分、時、日、週、月、年などの任意の時間内に実行されたかどうかを判断するように構成され得る。別の例では、１つ又は複数の条件の少なくとも１つは、アカウント及び／又はユーザに関連する不正使用又は詐欺が発生したかどうかを判断することを含む場合がある。例えば、依拠当事者装置は、ユーザの取引履歴が過剰な購入量や異常な場所を示すかどうかを判断するように構成されてもよい。このように、条件付き多要素認証を実施してセキュリティを向上させ、入力データを受信するための第２の命令の送信をトリガすることができる。

【０１０４】

図６は、例示的な実施形態に係る認証方法６００を示す。図６は、システム１００、図２Ａ及び図２Ｂの第１の装置２００、図３の方法３００、図４のシーケンス図４００、及び図５の方法５００の同一又は類似の構成要素を参照することができる。

【０１０５】

ブロック６１０において、方法６００は、プロセッサにおいて、認証要求を受信することを含み得る。例えば、プロセッサは、依拠当事者装置又はサーバ装置に属する場合がある。一部の例では、認証要求は、ＦＩＤＯ２（Ｆａｓｔ　Ｉｄｅｎｔｉｔｙ　Ｏｎｌｉｎｅ　２）ウェブサイト登録要求を含む。

【０１０６】

ブロック６２０において、方法６００は、プロセッサによって、第１のチャレンジを送信することを含み得る。例えば、プロセッサは、仲介の第２の装置又はクライアント装置上で実行するための命令を含むアプリケーションなどの認証装置に第１のチャレンジを送信するように構成される。いくつかの例では、プロセッサは、認証要求に応答して、１つ又は複数のチャレンジを生成するように構成され得る。例えば、プロセッサは、第１のチャレンジを生成するように構成される。いくつかの例では、依拠当事者装置は、モバイル装置のプロセッサなどの認証装置にログインを要求するように構成される。第１のチャレンジは、ユーザ識別子やサイト識別子などの識別子を含むことができ、これは、適切なＦＩＤＯ鍵ペアを選択するために使用できる。第１のチャレンジは、さらに、リプレイを防

ぐために使用される、依拠当事者装置によって与えられる予測不可能な番号を含むことができる。例えば、認証のインスタンスごとに、新しい予測不可能な番号が必要となり、そのため予測不可能な番号は毎回異なる。このようにして、古い予測不可能な番号の署名を利用することを回避し、代わりに認証のインスタントセッションの番号を利用する。

【０１０７】

ブロック６３０において、方法６００は、第１のチャレンジを検証することを含み得る。例えば、第１の命令が、認証装置によって第１の装置に送信されてもよい。いくつかの例では、第１の命令は、認証装置によってカードのプロセッサに生成及び／又は送信されてもよい。モバイル装置のプロセッサなどの認証装置は、１つ又は複数の命令を生成するように構成されている場合がある。例えば、モバイル機器のプロセッサは、第１の命令を生成するように構成され得る。各命令は、１つ又は複数の要求を含むことができる。第１の命令は、カードなどの第１の装置のプロセッサから第１の鍵を取得する第１の要求を含んでもよい。鍵は、ＦＩＤＯ鍵で構成されてもよい。ＦＩＤＯ秘密鍵は、第１の装置の通信インターフェースが、認証装置の通信フィールドなどの通信フィールドに入力されることによって取得される。いくつかの例では、第１の命令は、第１の装置のプロセッサによってＦＩＤＯ秘密鍵を生成する要求を含むことができる。他の例では、第１の命令は、例えばＦＩＤＯ秘密鍵である第１のＦＩＤＯ鍵を再生成する要求を含むことができ、ＦＩＤＯ秘密鍵は、公開鍵／秘密鍵ペアの一部である。

【０１０８】

例えば、認証装置は、依拠当事者装置又はサーバ装置のプロセッサから受信した第１のチャレンジに基づき、１つ又は複数の命令を生成することによって、第１の装置の１つ又は複数のエントリを促すように構成されてもよい。例えば、１つ又は複数の入力は、タップ、スワイプ、ウェーブなどのグループから選択された少なくとも１つ、及び／又はそれらの任意の組み合わせを含むことができる。第１の命令は、第１の装置によって第１のＦＩＤＯ鍵を生成する要求を含む場合がある。いくつかの例では、第１のＦＩＤＯ鍵は、１つ又は複数の暗号アルゴリズムを用いて、マスター鍵と第１の要求に関連付けられた識別子に基づいて生成される。例えば、識別子はサイト識別子を含み、マスター鍵と組み合わされて鍵ペアを生成する。一部の例では、マスター鍵は第１の装置に保存され、マスター鍵は第１の装置上でサイト識別子と組み合わされて秘密鍵が生成される。

【０１０９】

例えば、第１の装置のプロセッサは、第１のＦＩＤＯ鍵を生成し、送信するように構成される。例えば、第１の装置の通信インターフェースは、例えば、モバイル装置の通信フィールドなどの認証装置の通信フィールドに入ることができる。第１の装置は、認証装置から受信した第１の命令に応じて、特定のユーザ又はサイトに関連するＦＩＤＯ鍵ペアを生成又は取得するように構成される。生成又は取得されたＦＩＤＯ鍵ペアは、認証装置によって読み取られる。ＦＩＤＯ鍵ペアは、認証装置が第１の装置から読み取ることができるＦＩＤＯ秘密鍵を含み、認証装置が署名されたチャレンジデータをもたらす第１のチャレンジに署名するために使用することができる。ＦＩＤＯ秘密鍵は、第１の装置の通信インターフェースから通信フィールドに入力することで取得される。いくつかの例では、ＦＩＤＯ秘密鍵は、認証装置に転送される前に、第１の装置によって暗号化されてもよく、この場合、モバイル装置のプロセッサは、受信した暗号化されたＦＩＤＯ秘密鍵を復号化するように構成されてもよい。

【０１１０】

いくつかの例では、ＦＩＤＯ秘密鍵は、１つ又は複数の暗号化アルゴリズムを用いて、マスター鍵及び認証要求に関連付けられた識別子に基づいて生成される。例えば、識別子はサイト識別子を含み、マスター鍵と組み合わされて別の鍵ペアが生成される。第１の装置は、鍵を再生成する必要がないように、有限数の鍵をメモリに保存するように構成される。他の例では、認証装置からの第１の命令は、例えば、公開鍵／秘密鍵ペアの一部である秘密鍵などの、ＦＩＤＯ秘密鍵を再生成する要求を含む。

【０１１１】

いくつかの例では、マスター鍵は第１の装置上のメモリに保存され、マスター鍵は第１の装置上のサイト識別子と組み合わされてＦＩＤＯ秘密鍵を生成することができる。他の例では、マスター鍵は第１の装置から認証装置に転送され、ＦＩＤＯ秘密鍵を生成するために、マスター鍵とサイト識別子の結合が認証装置によって実行される。

【０１１２】

いくつかの例では、第１の装置から認証装置へのＦＩＤＯ秘密鍵の送信は防止される。例えば、第１の装置が第１のチャレンジの署名を実行する際、ＦＩＤＯ秘密鍵のＯＴＡ（Ｏｖｅｒ　ｔｈｅ　Ａｉｒ）送信は回避される。このように、第１のチャレンジとサイト又はユーザ識別子情報は、認証装置から第１の装置に送信され、これにより、プロキシプロトコルを用いて近距離無線通信（ＮＦＣ）を通じて第１の装置に計算を分配する。

【０１１３】

いくつかの例では、ＦＩＤＯ秘密鍵は、第１の装置において生成又は保存されるのではなく、認証装置に属するセキュアエレメントにおいて生成又は保存される。例えば、ＦＩＤＯ秘密鍵は、第２の装置が保持するセキュアエレメントに格納される。いくつかの例では、セキュアエレメントは、１つ又は複数の鍵が安全に保管され、依拠当事者装置によって取得される耐タンパー性のセキュア記憶装置エリアから構成される。

【０１１４】

一部の例では、第１の装置のプロセッサは、ＦＩＤＯ秘密鍵を生成するように構成されてもよい。第１の装置のプロセッサは、ＦＩＤＯ秘密鍵を送信するように構成される。例えば、第１の装置のプロセッサは、例えば第２の装置上で実行するための命令を含むアプリケーションなどの、ＦＩＤＯ秘密鍵を認証装置に送信するように構成される。上述したように、認証装置は、限定するものではないが、ノートパソコン、タブレット、電話などのモバイル機器であってもよい。一部の例では、ＦＩＤＯ秘密鍵は１つ又は複数のチャンネルを介して送受信されてもよい。例えば、ＦＩＤＯ秘密鍵は帯域外チャンネルを介して送受信される。第１の装置のプロセッサは、第１の装置の通信インターフェースが認証装置の通信フィールドに入力されることにより、ＦＩＤＯ秘密鍵を認証装置に送信するように構成される。いくつかの例では、エントリは１つ又は複数のジェスチャに関連付けられてもよく、これらのジェスチャには、１つ又は複数のタップ、スワイプ、ウェーブ、及び／又はそれらの任意の組み合わせが含まれるが、これらに限定されない。

【０１１５】

一部の例では、認証装置は、第１のＦＩＤＯ鍵を受信するように構成される。例えば、第２の装置のアプリケーションは、第１の装置のプロセッサから第１のＦＩＤＯ秘密鍵を受信するように構成される。認証装置は、受信した第１のＦＩＤＯ鍵を用いて第１のチャレンジに署名するように構成される。認証装置は、署名された第１のチャレンジを検証のために依拠当事者装置に送信するように構成される。依拠当事者装置又はサーバ装置のプロセッサは、署名された第１のチャレンジを検証するように構成される。例えば、依拠当事者装置又はサーバ装置のプロセッサは、署名された第１のチャレンジを認証装置から受信するように構成される。例えば、依拠当事者装置は、ユーザがサイトに登録したときに保存されたＦＩＤＯ公開鍵で、署名されたチャレンジデータを検証することができる。検証は、署名検証を含む認証プロセスの結果を構成することができる。認証装置は、検証のために、第１のＦＩＤＯ鍵を依拠当事者装置のプロセッサに送信するように構成されてもよく、従って、認証装置は、第１の装置と依拠当事者装置のプロセッサとの間の仲介装置として機能するように構成されてもよい。

【０１１６】

ブロック６４０において、方法６００は、プロセッサによって、１つ又は複数の条件を評価することを含み得る。例えば、１つ又は複数の条件の少なくとも１つは、所定の期間にわたる認証要求のしきい値数を決定することを含み得る。例えば、プロセッサは、異常な数のトランザクション又は要求が、任意の秒数、分数、時間数、日数、週数、月数、年数などの範囲内で実行されたかどうかを判定するように構成され得る。別の例では、１つ又は複数の条件のうちの少なくとも１つは、アカウント及び／又はユーザに関連する不正

使用又は詐欺が発生したかどうかを判定することを含み得る。例えば、プロセッサは、ユーザの取引履歴が過度の購入又は異常な場所を示すか否かを判定するように構成され得る。このように、条件付き多要素認証を実装することで、セキュリティを向上させることができ、これは、入力データを受信するための第２のチャレンジの送信をトリガする可能性がある。

【０１１７】

ブロック６５０において、方法６００は、プロセッサによって、第２のチャレンジを送信することを含み得る。例えば、依拠当事者装置又はサーバ装置のプロセッサは、第２のチャレンジを生成するように構成されてもよい。例えば、第２のチャレンジは、入力データを送信する第２の要求を含むことができる。いくつかの例では、依拠当事者装置又はサーバ装置のプロセッサは、上述したように、１つ又は複数の条件を評価するように構成されてもよい。いくつかの例では、第２のチャレンジは、１つ又は複数の条件の評価後にプロセッサによって送信されてもよい。

【０１１８】

一部の例では、認証装置は、第２のチャレンジを受信するように構成されてもよい。例えば、モバイル装置のプロセッサは、依拠当事者装置又はサーバ装置による１つ又は複数の条件の評価後に、依拠当事者装置又はサーバ装置のプロセッサから第２のチャレンジを受信するように構成されてもよい。いくつかの例では、第２のチャレンジは、例えば、１つ又は複数のプッシュ通知を用いてモバイル装置で実行するための命令を含むアプリケーションなどであり、依拠当事者装置又はサーバ装置のプロセッサによって認証装置に転送される。

【０１１９】

認証装置は、第２のチャレンジに基づき、入力データを送信するように構成される。例えば、モバイル装置のプロセッサ又はアプリケーションは、入力データをサーバ装置のプロセッサなどの依拠当事者装置に送信するように構成することができる。入力データは、バイオメトリクスデータ及びクレデンシャルデータのグループから選択された少なくとも１つを含むことができる。例えば、入力データは、バイオメトリックデータ、クレデンシャルデータ、及び／又はそれらの任意の組合せを含むことができる。限定されないが、バイオメトリックデータは、指紋、顔スキャン、網膜スキャン、音声認識、及び／又はそれらの任意の組み合わせのグループから選択される少なくとも１つを含むことができる。いくつかの例では、入力データは、追加的及び／又は代替的に、クレデンシャルデータを含み得る。これに限定されないが、ログインデータは、ユーザ名、パスワード、口座番号、セキュリティコード、ワンタイムパスコード、セキュリティ質問に対する回答、及び／又はそれらの任意の組み合わせの入力のグループから選択される少なくとも１つを含むことができる。

【０１２０】

ブロック６６０において、方法６００は、受信した入力データをプロセッサによって認証することを含むことができる。例えば、依拠当事者装置又はサーバ装置のプロセッサは、入力データを認証することによって認証要求を完了するように構成され得る。例えば、依拠当事者装置又はサーバ装置のプロセッサは、モバイル装置の実行命令を構成するプロセッサ又はアプリケーションなど、認証装置からの入力データを受信するように構成される。いくつかの例では、依拠当事者装置又はサーバ装置のプロセッサは、受信した入力データを参照入力データと比較することによって、１つ又は複数の結果を生成するように構成され得る。いくつかの例では、参照入力データは、依拠当事者装置又はサーバ装置によって記憶される場合がある。他の例では、参照入力データは、依拠当事者装置又はサーバ装置によって要求される場合がある。例えば、依拠当事者装置又はサーバ装置のプロセッサは、１つ又は複数の要求を通じて、基準入力データを受信するように構成されてもよいし、代わりに、基準入力データと比較するための入力データをデータベースに送信するように構成されてもよい。例えば、依拠当事者装置又はサーバ装置は、受信した入力データと参照入力データとの比較に基づいて照合が成功した場合、認証が成功したことを示す結

果を生成するように構成される。別の例では、依拠当事者装置又はサーバ装置は、受信した入力データと参照入力データとの比較に基づいて照合が失敗した場合、認証失敗の結果を生成するように構成される。認証に失敗したと判断された場合、依拠当事者装置又はサーバ装置は、入力データの認証に成功する前に、所定の試行回数まで入力データを再認証するように構成することができる。認証要求を完了するように、又は認証要求の完了を中止する。このように、認証プロセスのシーケンス図４００は、前述の機能性をサポートするために、分散記憶装置、クラウドベースの記憶装置、及び他の形態の記憶装置を用いて実装することができる。

【０１２１】

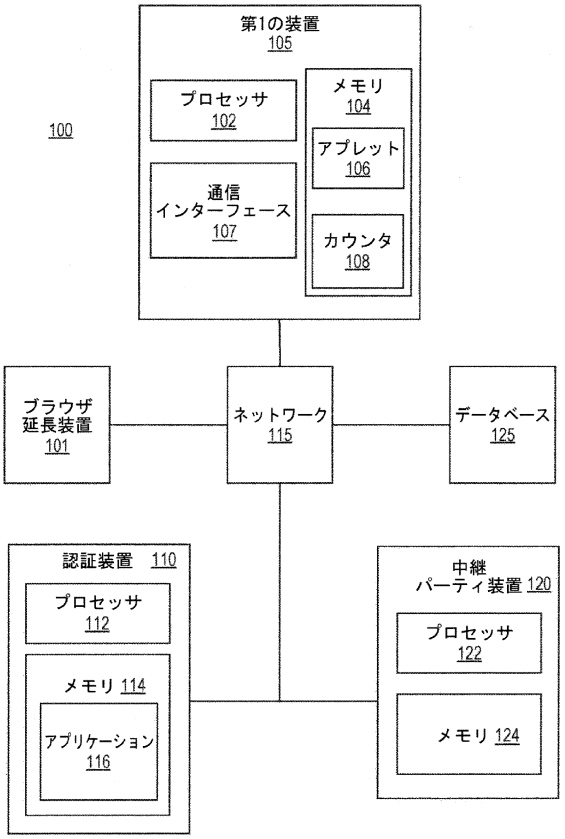
さらに、本明細書に記載されるシステム及び方法は、コンパクトディスク（ＣＤ）、デジタル多用途ディスク（ＤＶＤ）、フロッピーディスク、ハードドライブ、読み取り専用メモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、及びデータ記憶可能な他の物理的媒体のような（ただし、これらに限定されない）、１つ又は複数の物理的媒体に具体化され得ることに留意されたい。例えば、データ記憶装置には、ランダムアクセスメモリ（ＲＡＭ）や読み出し専用メモリ（ＲＯＭ）が含まれ、これらはデータや情報、コンピュータプログラム命令にアクセスして記憶するように構成される。データ記憶装置はまた、記憶媒体又は他の適切なタイプのメモリ（例えば、例えば、ＲＡＭ、ＲＯＭ、プログラマブルリードオンリーメモリ（ＰＲＯＭ）、消去可能プログラマブルリードオンリーメモリ（ＥＰＲＯＭ）、電気的消去可能プログラマブルリードオンリーメモリ（ＥＥＰＲＯＭ）、磁気ディスク、光ディスク、フロッピーディスク、ハードディスク、リムーバブルカートリッジ、フラッシュドライブ、任意のタイプの有形及び非一時的の記憶媒体など）を含み得るが、ここには、オペレーティングシステム、例えばウェブブラウザアプリケーション、電子メールアプリケーション及び／又はその他のアプリケーションを含むアプリケーションプログラム、及びデータファイルを構成するファイルが格納される。ネットワーク対応コンピュータシステムのデータ保存には、さまざまな方法で保存された電子情報、ファイル、文書が含まれ、ここで、データ記憶装置は、例えば、フラットファイル、インデックスファイル、階層型データベース、リレーショナルデータベースを含み、これらは、例えば、オラクル（登録商標）コーポレーション、マイクロソフト（登録商標）エクセルファイル、マイクロソフト（登録商標）アクセスファイルなどのソフトウェアで作成管理されたデータベースなどであって、データ記憶装置は、フラッシュアレイ、ハイブリッドアレイ、サーバ装置サイド製品などのソリッドステート記憶装置、オンライン記憶装置、クラウド記憶装置、その他の記憶装置機構を含むエンタープライズ記憶装置である。さらに、図には様々な構成要素（例えば、サーバ装置、コンピュータ、プロセッサなど）が個別に図示されている。様々な構成要素で実行されるものとして説明された機能は、他の構成要素で実行されてもよく、様々な構成要素は組み合わされても分離されてもよい。また、その他の変更も可能である。

【０１２２】

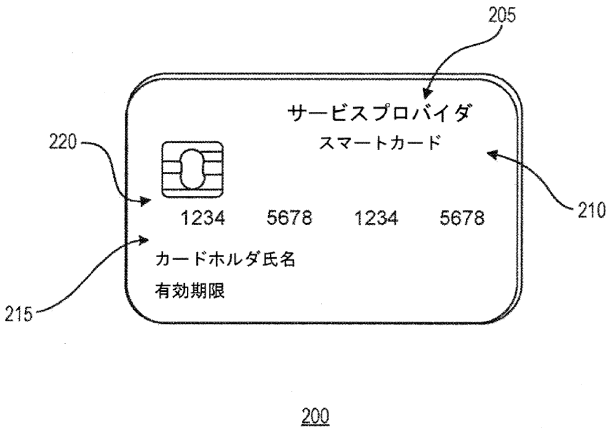
先の明細書では、添付図面を参照しながら様々な実施形態について説明した。しかしながら、以下に続く特許請求の範囲に規定される本発明の広範な範囲から逸脱することなく、様々な修正及び変更をそれらに加えることができ、追加の実施形態を実施することができることは明らかであろう。従って、本明細書及び図面は、制限的な意味ではなく例示的な意味としてみなされる。

【図面】

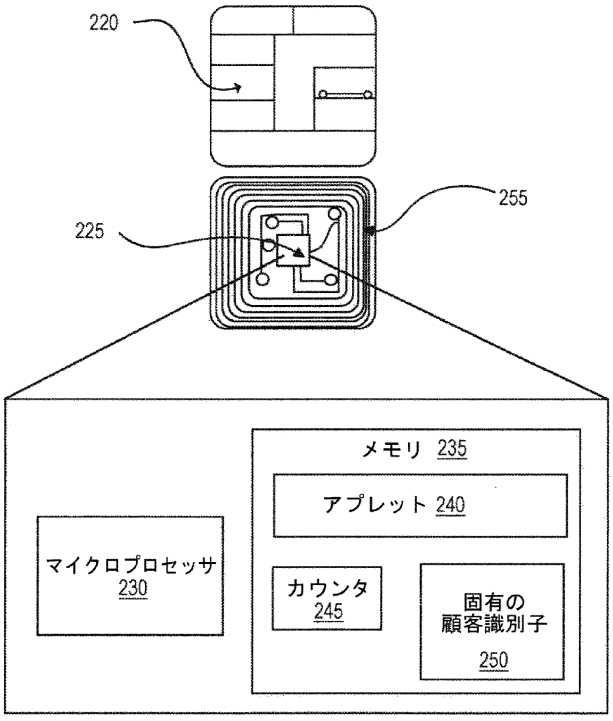
【図１】



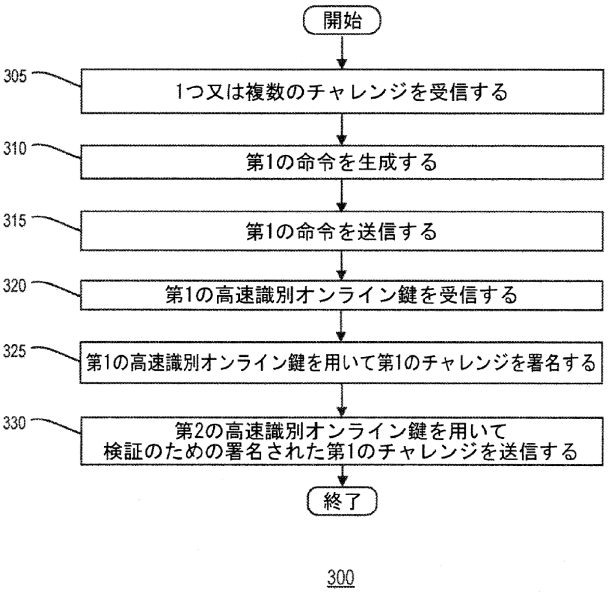
【図２Ａ】



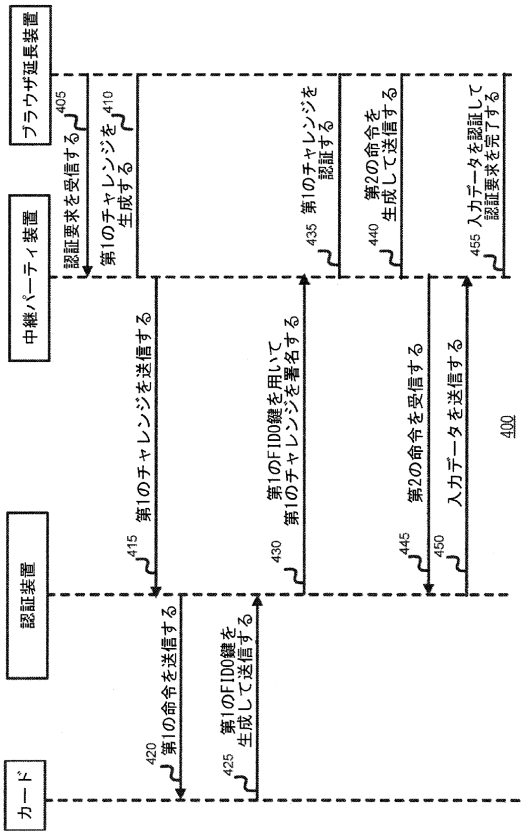
【図２Ｂ】



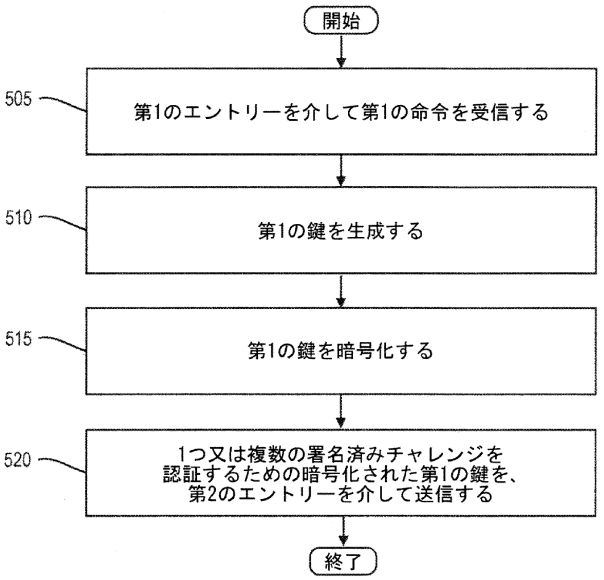
【図３】



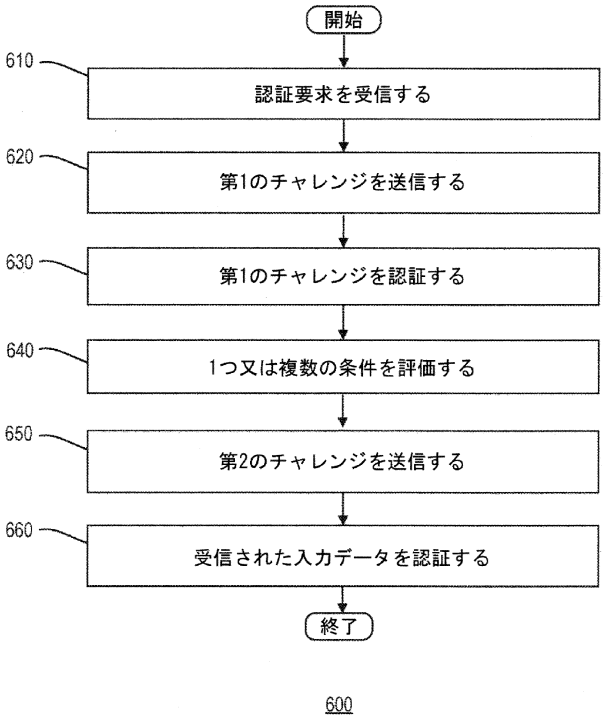
【図４】


ブラウザ延長装置
中継パーティ装置
認証装置
カード
405 認証要求を受信する
410 第1のチャレンジを生成する
435 第1のチャレンジを認証する
440 第2の命令を生成して送信する
455 入力データを認証して認証要求を完了する
415 第1のチャレンジを送信する
430 第1のFIDO鍵を用いて第1のチャレンジを署名する
445 第2の命令を受信する
450 入力データを送信する
420 第1の命令を送信する
425 第1のFIDO鍵を生成して送信する
400

【図５】


開始
505 第1のエントリーを介して第1の命令を受信する
510 第1の鍵を生成する
515 第1の鍵を暗号化する
520 1つ又は複数の署名済みチャレンジを認証するための暗号化された第1の鍵を、第2のエントリーを介して送信する
終了
500

【図６】


開始
610 認証要求を受信する
620 第1のチャレンジを送信する
630 第1のチャレンジを認証する
640 1つ又は複数の条件を評価する
650 第2のチャレンジを送信する
660 受信された入力データを認証する
終了
600

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/033724

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/31 H04L9/32
ADD.

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)
G06F H04L

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)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2020/127858 A1 (STÖHR VOLKER [DE] ET AL) 23 April 2020 (2020-04-23) abstract paragraphs [0001] - [0055] paragraphs [0065] - [0082] paragraphs [0110] - [0171] claims 18-34 figures 1-8	1-20
X	WO 2013/109932 A1 (ONEID INC [US]) 25 July 2013 (2013-07-25)	1-3, 5-12, 14-20
A	abstract paragraphs [0005] - [0017] paragraphs [0082] - [0161] paragraphs [0172] - [0173] claims 1-68 figures 1-19	4,13

-/--

[x] Further documents are listed in the continuation of Box C. [x] 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
29 September 2022	07/10/2022
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Bichler, Marc

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/033724

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2020/336308 A1 (DEUTSCHMANN INGO [DE] ET AL) 22 October 2020 (2020-10-22) abstract paragraphs [0002] - [0022] paragraph [0028] paragraphs [0042] - [0046] paragraphs [0052] - [0067] claims 1-16 figures 1-5 -----	1-20

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2022/033724

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2020127858 A1	23-04-2020	CN 110337797 A	15-10-2019
		DE 102017000768 A1	02-08-2018
		EP 3574610 A1	04-12-2019
		EP 3574625 A1	04-12-2019
		ES 2887258 T3	22-12-2021
		ES 2894480 T3	14-02-2022
		US 2019364032 A1	28-11-2019
		US 2020127858 A1	23-04-2020
		WO 2018137888 A1	02-08-2018
		WO 2018137889 A1	02-08-2018
WO 2013109932 A1	25-07-2013	US 11012240 B1	18-05-2021
		US 2013198516 A1	01-08-2013
		US 2013198834 A1	01-08-2013
		US 2013205136 A1	08-08-2013
		US 2016261413 A1	08-09-2016
		US 2022109578 A1	07-04-2022
		WO 2013109932 A1	25-07-2013
US 2020336308 A1	22-10-2020	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

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,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,IR,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,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,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）

１．ＪＡＶＡ

ブ１６８０

(72)発明者　オズボーン，ケビン

アメリカ合衆国２２１０２バージニア州マクリーン、キャピタル・ワン・ドライブ１６８０

(72)発明者　ルッツ，ウェイン

アメリカ合衆国２２１０２バージニア州マクリーン、キャピタル・ワン・ドライブ１６８０