(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6977158号
(P6977158)
(45)発行日　令和3年12月8日(2021.12.8)　(24)登録日　令和3年11月12日(2021.11.12)

(51)Int.Cl.　F I
G06Q 20/22 (2012.01)　G06Q 20/22 300

請求項の数 13 (全 12 頁)

(21)出願番号　特願2020-520157(P2020-520157)
(86)(22)出願日　平成30年9月28日(2018.9.28)
(65)公表番号　特表2020-537247(P2020-537247A)
(43)公表日　令和2年12月17日(2020.12.17)
(86)国際出願番号　PCT/US2018/053293
(87)国際公開番号　WO2019/074686
(87)国際公開日　平成31年4月18日(2019.4.18)
審査請求日　令和2年5月27日(2020.5.27)
(31)優先権主張番号　17195532.1
(32)優先日　平成29年10月9日(2017.10.9)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)

(73)特許権者　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　ミハイル　ブリノフ
アイルランド国　ダブリン　ダン　レアリー　アッシュグローブ　５
最終頁に続く

(54)【発明の名称】ピアツーピア移転を実行するシステム及び方法

(57)【特許請求の範囲】
【請求項１】
ピアツーピア移転を実行するために、トランザクションの当事者によって操作されるコンピューティング装置上にインストールされたアプリケーションによって実行される方法であって、前記アプリケーションが、
第１の当事者モードにおいて、
前記当事者をアイデンティティサーバに対し認証することと、
前記当事者と相手方との間で移転される資金の金額を前記当事者から取得することと、
前記アイデンティティサーバに、前記トランザクションに関する情報を記憶するためのセッションを確立させることと、
前記セッションに関連して記憶するために、前記アイデンティティサーバに前記金額を提供することと、
前記セッションに関連して記憶するために、前記アイデンティティサーバに前記当事者についてのアカウント情報を提供することと、
前記アイデンティティサーバから前記トランザクションに固有のトークンを取得することと、
前記相手方の連絡先情報を取得することと、
前記連絡先情報を用いて、前記トークンを含むメッセージを前記相手方に提供し、前記相手方に前記トランザクションが開始されたことを示すことと、
第２の相手方モードにおいて、

トランザクションの第１の当事者からメッセージを受信することであって前記メッセージはトランザクションのトークンを含む、ことと、
前記アイデンティティサーバに対して前記相手方を認証することと、
前記相手方が前記トランザクションを完了しようとすることを判定することと、
前記判定に応答して、前記トランザクションにつき確立されたセッションに関連して記憶するために、前記トークンを使用して前記相手方のアカウント情報を前記アイデンティティサーバに提供し、前記アイデンティティサーバが前記トランザクションを完了することを可能にすることと、
前記アイデンティティサーバから、任意の完了したトランザクションの結果を受信することと、
を含み、
前記第１の当事者モードにおいて、前記アプリケーションは、前記トランザクションの前記相手方についての認証基準を指定するように構成され、前記認証基準は、前記相手方が所有することを前記当事者が期待する情報として、前記当事者によって指定される、方法。
【請求項２】
前記メッセージを提供することは、前記アプリケーションが前記コンピューティング装置にインストールされたメッセージングアプリケーションのためのアプリケーションプログラミングインタフェース（ＡＰＩ）を使用して前記メッセージを送信することを含み、
前記メッセージを受信することは、前記コンピューティング装置にインストールされたメッセージングアプリケーションから、前記アプリケーションのためのアプリケーションプログラミングインタフェース（ＡＰＩ）を使用して前記アプリケーションが起動されることによって、前記メッセージを受信することを含む、請求項１に記載の方法。
【請求項３】
前記メッセージを提供することは前記アプリケーションが前記アイデンティティサーバを介して前記メッセージを送信することを含み、
前記メッセージを受信することは、前記アプリケーションが前記アイデンティティサーバから前記メッセージを受信することを含む、請求項１に記載の方法。
【請求項４】
前記認証はＦＩＤＯ（Fast IDentity Online）プロトコルに基づいて実行される、請求項１に記載の方法。
【請求項５】
前記第１の当事者は支払者または受領者の一方であり、前記相手方は前記支払者および前記受領者の他方である、請求項１に記載の方法。
【請求項６】
前記アプリケーションが、資金移転以外の機能を提供するアプリケーション内に統合される、請求項１に記載の方法。
【請求項７】
前記アプリケーションは、電子ウォレットと協働して、前記当事者及び／又は相手方についての前記アカウント情報を検索する、請求項１に記載の方法。
【請求項８】
前記メッセージは、相手方が前記アプリケーションを自身の装置にインストールすることを可能にするための命令を含む、請求項１に記載の方法。
【請求項９】
前記メッセージングアプリケーションは、ＳＭＳアプリケーション、インスタントメッセンジャーアプリケーション、またはeメールアプリケーションのうちのいずれか１つを含む、請求項２に記載の方法。
【請求項１０】
前記連絡先情報を取得することは、前記アプリケーションが前記第１の当事者の連絡先一覧から連絡先情報を取得することと、相手方の連絡先の選択のために前記連絡先一覧を

表示することとを含む、請求項１に記載の方法。
【請求項１１】
命令が格納されたコンピュータ可読媒体であって、前記命令は、コンピューティング装置上で実行されると、請求項１に記載のステップを実行するように構成される、コンピュータ可読媒体。
【請求項１２】
スタンドアロンのクライアントアプリケーションとして、またはブラウザベースのアプリケーションとして実行可能な命令を含む、請求項１１に記載のコンピュータ可読媒体。
【請求項１３】
ピアツーピア移転を実行するためのコンピューティング装置であって、請求項１に記載の方法を実行するように構成されたアプリケーションを含む、コンピューティング装置。
【発明の詳細な説明】
【関連出願の相互参照】
【０００１】
本出願は、2017年10月9日に出願された欧州特許出願第17195532.1号の利益と優先権を主張するものである。上記出願の開示全体は、参照により本明細書に組み込まれる。
【技術分野】
【０００２】
本願はピアツーピア移転を実行するシステムに関する。
【背景技術】
【０００３】
支払人と受取人との間のピアツーピア支払いを可能にするために、スマートフォン，タブレット端末または汎用コンピュータなどのエンドユーザ装置にインストールすることができる支払アプリケーションは一般に、支払人によって支払いが開始されたときに受取人の詳細が提供されることを必要とする。これは、すべての支払人が、支払いをしたい受取人の銀行アカウント詳細を入手し、入力し、記憶する必要があるか、またはそれらを提供するために一般的なシステムに依拠する必要があることを意味する。
【０００４】
特に、前者については、支払人に潜在的に多くの異なった受取人からの比較的長い数を伴うことがあるアカウント詳細を受け取らせるという負荷が、そのような支払いアプリケーションの採用に対する1つの障壁として働いてきた。
したがって、驚くべきことに、ピアツーピア支払いのための市場は、まだうまく行っていない。比較的低い市場浸透または使用を有するSkypeまたはPaypalのような多くのアプリケーションが存在する。
【発明の概要】
【０００５】
本発明によれば、請求項1に記載のピアツーピア移転を実行する方法が提供される。
【０００６】
第２の態様では、命令が格納されたコンピュータ可読媒体を含むコンピュータプログラムプロダクトが提供される。命令は、コンピュータシステムで実行されると、請求項１に記載のピアツーピア移転を実行する方法を実行するよう構成される。
【０００７】
第３の態様では、請求項１に記載のピアツーピア移転を実行する装置が提供される。
【０００８】
本実施形態は、使い易さ及び採用の容易さと、ユーザに対する高度の信頼性及び安全性とを兼ね備えている。
【０００９】
実施形態は必ずしもアカウントを作成したり、アカウントにログインしたりする必要なく、ピア間での資金移転を可能にする。参加当事者(送金人および受取人)は、トランザクションごとに変化する一時的なセッションキーを介して相関させることができる。

【００１０】
実施形態は新しいユーザ名またはパスワードを生成または記憶するユーザの必要性を回避するために、生体認証に基づくことができる。
実施形態は、二段階支払戦略に基づく。これは、支払いが開始されたときに、一方の当事者の支払い証明書が相手方当事者に知られたり開示されたりする必要がないことを意味する。このようなシステムの更なる利点は、支払詳細を中央に記憶する必要がないことである。
【００１１】
エンドユーザアプリケーションはスタンドアロンの資金移転アプリケーションとして実装することもできるし、機能を、例えば、顧客から顧客への電子的支払だけでなく顧客から販売者への電子的支払、または販売者から販売者への電子的支払を容易にするために、電子商取引またはMコマースアプリケーションなどの他のアプリケーション内に組み込むこともできる。したがって、多くの様々な動作者間で支払いを容易にすることができる。
【図面の簡単な説明】
【００１２】
以下、添付図面を参照して、本発明の実施形態を例示的に説明する。
【図１】図1は、本実施形態による支払システムの相互動作する構成要素を示す図である。
【図２】図2は、図1のアイデンティティサーバと通信して、支払人(送金人)が操作するアプリケーションによって実行されるステップを示す。
【図３】図3は図1の受領者(受取人)によって操作されるアプリケーションとの通信においてアイデンティティサーバによって実行されるステップを示す。
【図４】図4は、図1の支払ゲートウェイとの通信においてアイデンティティサーバによって実行されるステップを示している。
【発明を実施するための形態】
【００１３】
ここで図1を参照すると、本実施形態による支払システムでは、支払いを開始することを望む装置のユーザがまず、支払いアプリケーションを自分の装置にインストールする。
【００１４】
理解されるように、装置がアンドロイドまたはiOSオペレーティングシステムに基づく典型的なスマートフォンまたはタブレット端末である場合、ユーザは、そのようなアプリケーションをアプリケーションストア110からダウンロードすることができる。あるいは特に装置がWindowsベースのデスクトップまたはラップトップ装置であるとき（しかしこれがスマートフォンであってもよい）、ユーザはアプリケーションプロバイダーのWebサイトからアプリケーションをダウンロードすることができる。さらに別の変形例では、スタンドアロンのクライアントアプリケーションではなく、アプリケーションは、ブラウザベースのアプリケーションとして実装することができる。
【００１５】
いずれにせよ、開始ユーザは支払人(送金人)または受領者(受取人)のいずれであってもよく、以下の例は送金人によって開始される支払に関して説明される。
【００１６】
ここで、図2を参照すると、送金人は最初にアプリケーション100-Aを装置上で実行するとき、アイデンティティサーバ120にそれらのアイデンティティを登録する。一実施形態では、それらは、FIDOアライアンスによって定義されたFIDO(「Fast IDentity Online」)プロトコルに基づいてそうする。FIDOプロトコルは、標準的な公開鍵暗号技術を使用して認証を提供する。アイデンティティサーバ120への登録中に、ユーザのアプリケーション100-Aは、新しいキーペアを作成する。アプリケーション100-Aは秘密鍵を保持し、公開鍵をオンラインサーバ120に登録する。その後の認証は、アプリケーション100Aを介してユーザによって行われ、チャレンジに署名することによって、サーバに対して秘密鍵の所有を証明する。クライアントの秘密鍵は、ユーザによって装置上でローカルにロック解除さ

れた後でのみ使用できる。ローカルロック解除は、指をスワイプすること、ＰＩＮを入力すること、マイクに話すこと、第2要素装置を挿入すること、またはボタンを押すこと、または実際には生体情報の任意の形態または組合せを使用することなど、ユーザに優しく安全な動作によって達成される。

【００１７】

FIDOプロトコルは、ユーザのプライバシーを保護するために設計されている。というのも、それらは、サービス間でユーザを連携及び追跡するためにさまざまなオンラインサービスによって使用可能な情報を提供しないからである。

生体情報は、使用される場合、ユーザの装置を離れることはない。

【００１８】

したがって、ステップ[001]において、送金人のアプリケーション100-Aはアイデンティティサーバ120に接続し、ステップ[002]においてアイデンティティサーバによって提供される登録要求によってチャレンジを要求する。チャレンジを受信すると、アイデンティティサーバ120から、送金人のアプリケーション100-Aは、必要なユーザの生体認証であるステップ[003]を捕捉する。示されるように、これは、指をスワイプすること、暗証番号を入力すること、マイクに話すこと、第２要素装置を挿入すること、またはボタンを押すことなどの任意の組合せを含むことができる。ステップ[0004]で、ユーザのバイオメトリクスに基づく送金人のための公開鍵を含む応答がアイデンティティサーバ120に戻される。公開鍵が登録されると、これは、ステップ[005]で、アイデンティティサーバ120によって送金人アプリケーション100-Aに確認される。

【００１９】

ここで、送金人はその後の任意の時間に、アプリケーション100-Aのインスタンスを使用して送金することを判定することができる。(実際、後述するように、アプリケーション100-Aのインスタンスをインストールし、アイデンティティサーバ120に登録すると、潜在的受取人から要求を受け取ることもできる）

【００２０】

図2の例では、送金人アプリケーション100-Aが電話番号を識別子とするモバイル(セルラ)装置にインストールされ、そのため、電話番号に基づくセキュアチャネルが、送金人アプリケーション100-Aと、その識別子に基づくアイデンティティサーバ120との間に確立することができる（ステップ[007]）。送金人アプリケーション100-Aが非移動装置上にインストールされる他の実施形態では、等価のセキュアチャネルが他のメカニズムを使用して、または例えばMAC識別子のような他の識別子に基づいて確立することができることが理解されるであろう。いずれにせよ、チャネルの確立に応じて、セッションを確立し、ステップ[008]を行い、アイデンティティサーバ[120]によって送金人アプリケーション100-Aへ確認されることができる（ステップ[009]）。見てわかるように、アイデンティティサーバ120内に確立されたセッションは、任意の所与のトランザクションに必要な情報のプレースホルダ（代替）として機能する。

【００２１】

実施形態では送金人アプリケーション100-Aがセッションの確立の通知を受信すると、アプリケーション100-Aは送金人に対して、支払に関連するメッセージの入力を促すことができる（ステップ[010]）。例えば、ステップ[011]で、ユーザは自由形式メッセージとして「こんにちは、これは私が借りている20米ドルです」と入力する。ステップ[012]及び[013]において、ユーザは実際に移転されるべき金額を入力する。もちろん、ユーザが行われるべき支払いの金額を判定し、支払いに添付されるべきメッセージを判定することを可能にするために、任意の好適な機構を採用することができることが理解されるであろう。

【００２２】

ステップ[014]および[015]において、アイデンティティサーバ120および送金人アプリケーション100-Aは、資金が移転される元の送金人の銀行アカウント詳細をそれぞれ要求及び提供する。

【００２３】
したがって、ユーザが銀行アカウント詳細をアプリケーションにまだ格納していない場合、それらを行うように促され、複数のアカウントの詳細をアプリケーション100-Aに提供している場合、これらの詳細がアイデンティティサーバ120に返されるまでにアカウントを選択するように促される。
【００２４】
これで、ユーザは、ステップ[016]から[021]を介して、アイデンティティサーバ120 に対して自身を認証できるようになる。見てわかるように、認証のためにユーザによって提供されるべき情報は、それらが採用している装置の任意の組み合わせ、ユーザのプロファイル、およびアイデンティティサーバ120と協働する認証規則エンジン130によって判定される移転金額に基づくことができる。このようなポリシーベースの認証は例えば、Dan Holdings Limitedの名義の欧州特許出願公開第EP2605567号公報に開示されている。
【００２５】
送金人が認証されると、送金人アプリケーション100-Aは、ステップ[010]から[015]までで収集されたデータを、アイデンティティサーバ120に送信する（ステップ[022]）。この点に関して、ステップ[010]～[015]のいずれも、認証ステップ[016]～[021]に続くことができることが分かるであろう。
【００２６】
アイデンティティサーバ120はステップ[008]で作成されたセッションの情報を、ステップ[023]の送金人アプリケーション100-Aから受信したトランザクションデータで更新し、ステップ[024]で移転のための一意トークンを生成する。したがって、トークンは、トランザクションのためのセッションに対する短期鍵として機能する。トークンはステップ[025]で送金人アプリケーション100-Aに提供され、送金人アプリケーション100Aはこのトークンを使用して、トランザクションを完了するために受取人に提供されるべきメッセージを生成することができる。
【００２７】
一実施形態ではアプリケーション100-Aが装置にインストールされた連絡先一覧にアクセスすることができ、ユーザは通常、SMSまたはインスタントメッセンジャ(IM)メッセージを生成し、コール（呼）を開始し、および/または電子メールを生成し、あるいは実際には様々なソーシャルネットワークとの任意の相互作用を容易にするために使用する。
【００２８】
したがって、アイデンティティサーバ120からトークンを受信すると、アプリケーション100-Aは受取人のために生成する必要があるメッセージのタイプを判定するために、送金人が連絡先一覧から連絡先を選択することを要求することができる（ステップ[027]）。
送金人の電話番号が連絡先リストから選択されるとき、アプリケーションは、ステップ[011]および[013]で入力されたメッセージと金額を含むSMSまたはIMメッセージと、アイデンティティサーバによって提供されたトークンからステップ[026]で生成されたURLとを生成できる。URLは、メッセージの受取人がアプリケーションとは別個の装置上でアプリケーションのインスタンスを自動的に起動し、次いで、支払いメッセージおよびトークンによって識別されるトランザクションの他の詳細を表示することを可能にする。
【００２９】
もし送金人が彼らの連絡先一覧から受取人の電子メールアドレスを選択するなら、ステップ[028]で生成されたメッセージは電子メールメッセージを構成するだろう。これにより、支払いアプリケーションに関連する情報、又は、たとえば、支払いアプリケーションを装置にインストールしていないユーザがそのようにするためのリンクなど、完全な情報をメッセージに含めることができる。
【００３０】
いずれにせよ、一旦メッセージがステップ[028]で生成されると、送金人アプリケーションは、対応するメッセージングの装置に送金人によって公開された適切なAPI、あるい

はe-メールアプリケーション170-Aを使って、メッセージを送信することができる（ステップ[029]）。

【００３１】

なお、図2の例では、登録と認証は別々に行われる。しかしながら、ユーザが最初にアイデンティティサーバ120に登録し、(支払人または受取人のいずれかとして)即座に支払いを開始することを望む場合、ステップ[016]～[021]を実行する必要がない場合があることが理解されよう。

【００３２】

図3は、装置に支払いアプリケーションを以前にインストールしていない受取人によって実行されるステップを示す。

【００３３】

ステップ[030]は支払人によって送信されたメッセージの受信を示し、理解されるように、これは、受取人が装置にインストールしたメッセージングアプリケーション、IMアプリケーション、または電子メール受信ボックス170-Bのいずれかに現れる可能性がある。

【００３４】

ユーザが装置にアプリケーションをインストールしていない場合は、アプリケーションストア110またはアプリケーションソフトウェアの任意のリポジトリにアプリケーションへの直接リンクを含めることによって、それらのアプリケーションを有効にすることができる。

【００３５】

アプリケーション100-Bがインストールされると、例えば、ステップ[026]で生成されたメッセージ内のURLをクリックすることによって、ステップ[031]のメッセージから起動することができる。

【００３６】

ユーザが以前にアプリケーション100-Bにインストールされておらず登録されていない場合はステップ[001]～[005]の送金人と同様に、ステップ[034]～[038]で登録する。

【００３７】

この場合も、受取人アプリケーション100-Bとアイデンティティサーバとの間にセキュアチャネルが確立され（ステップ[032]および[033]）、これらのステップはステップ[034]から[038]の前後のいずれかで実行することができるが、FIDO登録はセキュアチャネル上で実行することが好ましいことが分かるのであろう。

【００３８】

ステップ[030]で受信されたメッセージからの元のトークンは現在、アプリケーション100-Bによって、トランザクションが関係するセッションをアイデンティティサーバ120に示すために、および、アイデンティティサーバ120によって記憶されたセッションデータから支払データを取り出すために、使用することができる（ステップ[039]から[041]）。

【００３９】

ここで、アプリケーション100-Bは送金人の詳細、支払いの説明および金額を表示することができ（ステップ[042]）、受取人が支払いを承認する(または拒否する)ことを可能にする。

【００４０】

受取人が支払いを承認し、彼らが受取人アプリケーション100-Bに対して自身を認証していない場合、彼らは、ステップ[045]から[050]において、再度、認証規則エンジン130を使用して、受取人によって提供される生体情報を判定することができる。

【００４１】

ここでも、図3の例では、登録と認証は別々に実行される。しかしながら、ユーザが最初にアイデンティティサーバ120に登録し、(支払人または受取人のいずれかとして)即座に支払を完了したい場合、ステップ[045]～[050]を実行する必要がないことが理解されよう。

【００４２】

再度、ステップ[051]および[052]において、アイデンティティサーバ120要求および受取人アプリケーション100-Bは、資金が移転される受取人の銀行アカウント詳細を提供する。

【００４３】

したがって、受取人が銀行アカウント詳細をアプリケーション100-Bにまだ記憶していない場合、そのようにするように促され、複数のアカウントの詳細をアプリケーション100-Bに提供した場合、ステップ[030]で受信した元のメッセージで提供されたトークンと共に、ステップ[053]でこれらの詳細がアイデンティティサーバ120に返されるまでに、アカウントを選択するように促される。

【００４４】

これにより、アイデンティティサーバ120は送金人によって最初に確立されたセッションデータに受取人詳細を追加し（ステップ[054]）、このデータを照合することができる（ステップ[055]）。

【００４５】

図4を参照すると、決済のデータが相関されて完了すると、アイデンティティサーバ120は支払ゲートウェイに情報を提供できるようになる。

例示的なゲートウェイは、Mastercardによって提供され、MC送信140と呼ばれ、このゲートウェイは送金人および受取人のアカウント詳細およびゲートウェイによって実行されるトランザクション金額を含むトランザクション詳細を提供するために、様々な他の形式のアプリケーションを可能にするAPIを公開する。

【００４６】

このようなゲートウェイを使用することにより、様々なタイプのトランザクションを完了することができ、したがって、例えば、送金人または受取人のいずれかがクレジットカード、デビットカード、または銀行アカウント詳細を指定することができる。マスターカードによって提供されるような支払ゲートウェイは、クレジットカードまたはデビットカードと、または送金人および/または受取人によって指定されたアカウントに対応する銀行とのための発行者150への適切なメッセージを開始することによって、それに応答して資金の移転を完了することができる。

【００４７】

その前に、支払ゲートウェイ140は、MastercardまたはKountによって提供されるタイプの詐欺規則エンジン(ゲートキーパ)160を用いてトランザクションを検査することができる。ゲートキーパサーバは、典型的には販売者がカードが有効であるか否かを検査することを可能にすることによって、クレジットカード詐欺を防止するために使用される。それらは、本質的に、失われた、ブロックされた、または盗まれた支払いカードのリストを記憶することができる、不正な、または潜在的に無効な支払いカードの使用および/またはデータベースを識別するための規則ベースのエンジンを備える。これらの規則は、有効であっても、特定のタイプの支払カードが所与の販売者によって受け入れられることができるかどうかを分析するための規則を含むことができる。

【００４８】

いずれにせよ、検査が順序通りであれば、支払ゲートウェイ140は支払いを確定することができる(ステップ[058])。一旦完成すると、支払ゲートウェイ140はステップ[059]において、支払いが完了したかどうかについてアイデンティティサーバ120に通知し、この情報は送金人および受取人アプリケーションの各々に順番に通知され（ステップ[060]）、これらはステップ[061]および[062]において、それぞれ送金人および受取人に通知する。ステップ[008]で確立されたセッションは、アイデンティティサーバ120によって終了できるようになる（ステップ[063]）。

【００４９】

上述のように、アプリケーション100の実装は、資金の潜在的受取人が移転を開始することを可能にするように拡張できることが理解されるのであろう。このケースでは、装置でアイデンティティサーバ120に一旦認証されると、潜在的受取人は(ステップ[029]のよ

うに)潜在的送金人に送信されるメッセージをアプリケーションが生成できるように、(ステップ[027]のように)潜在的送金人を選択するだけでなく、(ステップ[010]から[014]のように)メッセージと金額を指定することができる。この場合、アイデンティティサーバ120内でセッションを確立し、送金人アプリケーションのインスタンスとともにセッションのためのデータを生成及び提供して、その後にそれらのデータを提供して、セッションに必要な情報を完成させて移転を実行可能とするのは、受取人アプリケーションである。

【００５０】

上記の実施形態の多くの変形が可能であることが理解されるであろう。例えば支払アプリケーションの外部のメッセージングサービスを用いて連絡先に送信されるメッセージを生成する（ステップ[028]及び[029]のように）のではなく、支払アプリケーションは代わりに、相手方（すなわち送金人又は受取人）のための識別子、例えば電話番号、eメールアドレス、ユーザ名/ニックネーム、又はアイデンティの他の形態（例えばGoogle handle）を、アイデンティティサーバ120に提供することができる、

【００５１】

このようなメッセージを受信すると、アイデンティティサーバ120は相手方が登録されているかどうか、すなわち、アプリケーションをインストールしてアプリケーションに登録したかどうかを判断することができる。この場合、アイデンティティサーバ120がトークンを含むプッシュ通知を直接的に相手方装置に送信することができ、したがって、相手方装置がステップ[032]、[033]および[039]～[042]を自動的に実行することを可能にする。

【００５２】

別の変形例では、送金人は、アイデンティティサーバ120が受取人のクレデンシャルをより安全に確立できるように、資金の潜在的な受取人に関する付加的な情報を提供することができる。したがって、トランザクションを完了する前に、送金人および受取人は他の支払詳細と共にトランザクション開始部によって送信される秘密トランザクション特定符号語を確立するために、帯域外で互いに通信することができる。

【００５３】

あるいは合意された付加的な情報を使用するのではなく、開始当事者は相手当事者が所有することを期待する追加の認証情報を指定することができる。

【００５４】

他の変形例において、送金人は、受取人について、より強いもしくは弱い認証ポリシーを要求する可能性がある。あるいは又は加えて、送金人は例えば、電話番号を提供することによって特定の装置上で認証を行わなければならないことを要求することができる。この場合、受取人がそのセキュアセッションを確立する数が、指定された数と一致することをアプリケーションが検査してから、トランザクションを続行する。

【００５５】

他の変形例では、アプリケーション100およびアイデンティティサーバ120のインスタンスがオンラインウォレットとともに動作することができ、参加者は、アイデンティティサーバ120が送金人または受取人アカウントのいずれかの支払詳細を検索することができるオンラインウォレットへのアクセス詳細を提供する。

【００５６】

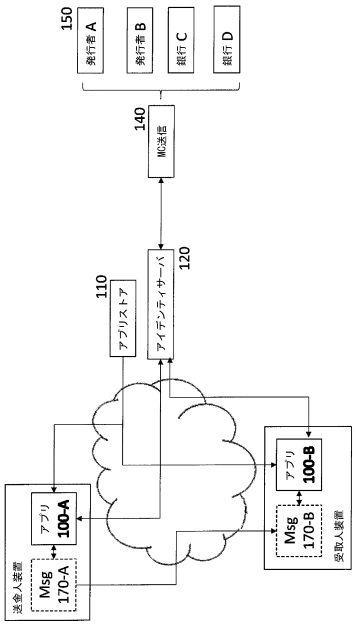
トランザクションの各当事者によって操作されるアプリケーションは、同じアプリケーションのインスタンスであってもよいし、またはアプリケーションについて上述した機能は、ある場合にはある当事者が所与のトランザクションを完了するために別の当事者とは別のアプリケーションを操作してもよいように、eコマースまたはmコマースアプリケーションなどの多機能プラットホーム内に統合されてもよいことが理解されるであろう。

【００５７】

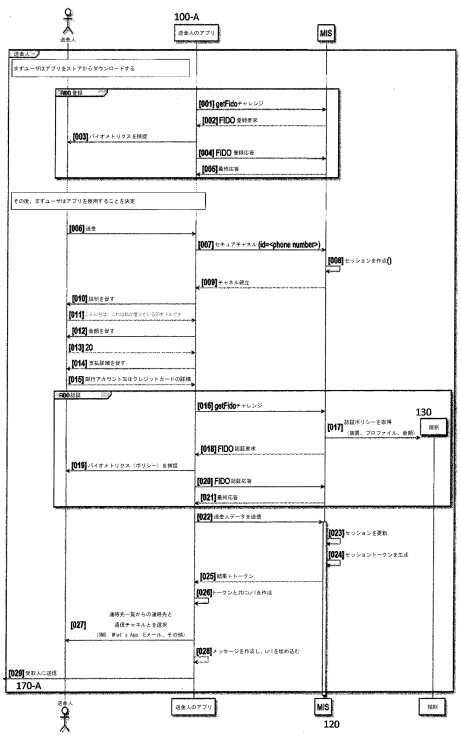
FIDO登録/認証は、上述のようなスタンドアロンアプリケーション100を介してではなく、ブラウザを介して実行することも可能であることに留意されたい。このように、特定の関係者、例えば販売者が、専用のアプリケーションではなくブラウザベースのアプリケー

ションを介してシステム内で動作することができる。

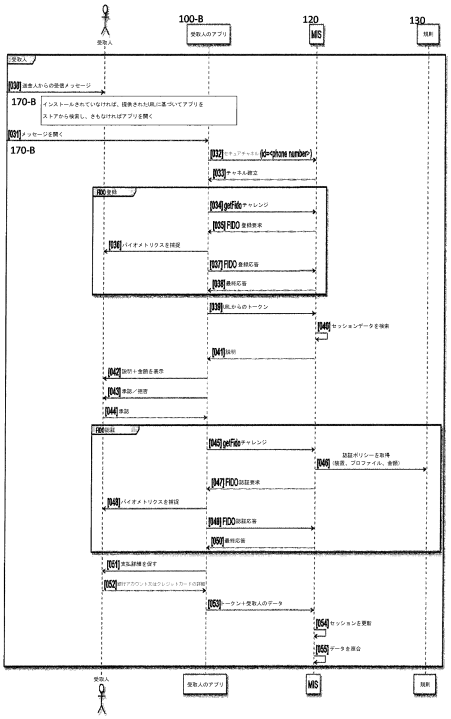
【図１】



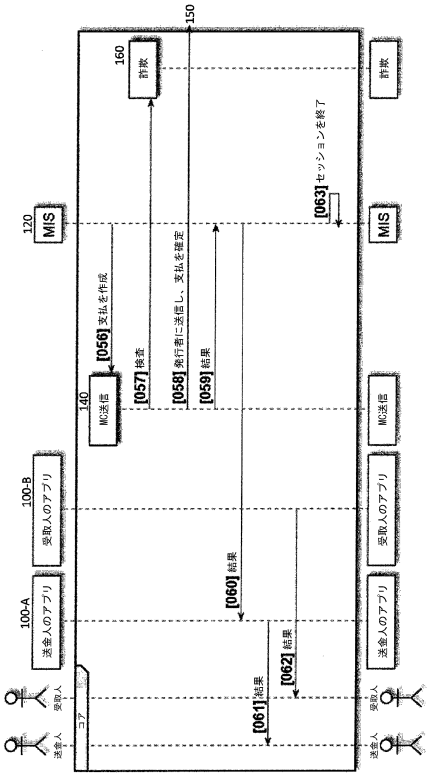
【図２】



【図３】


受取人
100-B
受取人のアプリ
120
MIS
130
銀行
受取人
[038] 送金人からの招待メッセージ
170-B
インストールされていなければ、提供された URL に基づいてアプリを
ストアから検索し、さもなければアプリを開く
[031] メッセージを開く
170-B
[032] (id=phone number)
[033] チャネル確立
FIDO 登録
[034] getFido チャレンジ
[035] FIDO 登録要求
[036] バイオメトリクスを検証
[037] FIDO 登録応答
[038] 最終応答
[039] MIS からのトークン
[040] セッションデータを検索
[041] 認証
[042] 振替口 + 金額を表示
[043] 承認／拒否
[044] 承認
FIDO 認証
[045] getFido チャレンジ
[046] 認証ポリシーを取得
(振替、プロファイル、金額)
[047] FIDO 認証要求
[048] バイオメトリクスを検証
[049] FIDO 認証応答
[050] 最終応答
[051] 支払詳細を保存
[052] 銀行アカウントまたはクレジットカードの詳細
[053] トークン + 受取人のデータ
[054] セッションを更新
[055] データを返す
受取人
受取人のアプリ
MIS
銀行

【図４】


150
160
詐欺
詐欺
[063] セッションを終了
120
MIS
MIS
[056] 支払を作成
[057] 検査
[058] 銀行に送信し、支払を確定
[059] 結果
140
MC送信
MC送信
100-B
受取人のアプリ
受取人のアプリ
[060] 結果
100-A
送金人のアプリ
送金人のアプリ
[062] 結果
[061] 結果
コア
受取人
送金人
受取人
送金人

フロントページの続き

(72)発明者 ダウィド ノワァク
アイルランド国 ダブリン １５ オンガー チェイス ブラックウッド ミューズ ３
(72)発明者 ヴラダド ドルータ
アイルランド国 ダブリン １ アッパー ガーディナー ストリート ドーセット スクウェア ４１
(72)発明者 キアン バーンズ
アイルランド国 ダブリン １６ バリンディァ クロネア ６１
(72)発明者 エイダン カニョン
アイルランド国 ダブリン ６ダブリュ テレニュア ウェインズフォート ロード １６

審査官 岡北 有平

(56)参考文献 米国特許出願公開第２０１４／０１７２７１６（ＵＳ，Ａ１）
特表２０１４－５２３５９１（ＪＰ，Ａ）
国際公開第２０１６／０５７０３５（WO，Ａ１）
米国特許出願公開第２０１６／０１０４１３２（ＵＳ，Ａ１）
国際公開第２０１７／０７２５８９（WO，Ａ２）
特開２０１６－１８１１９２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ １０／００ － ９９／００