(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2024-520925
(P2024-520925A)
(43)公表日　令和6年5月27日(2024.5.27)

(51)国際特許分類　FI
G06Q 20/40 (2012.01)　G06Q 20/40
H04L 9/32 (2006.01)　H04L 9/32 200B
G06F 21/35 (2013.01)　G06F 21/35

審査請求　未請求　予備審査請求　未請求　（全39頁）

(21)出願番号　特願2023-569960(P2023-569960)
(86)(22)出願日　令和4年3月22日(2022.3.22)
(85)翻訳文提出日　令和6年1月9日(2024.1.9)
(86)国際出願番号　PCT/US2022/021272
(87)国際公開番号　WO2022/240484
(87)国際公開日　令和4年11月17日(2022.11.17)
(31)優先権主張番号　17/317,262
(32)優先日　令和3年5月11日(2021.5.11)
(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
(74)代理人　100163902
弁理士　市川 奈月
(72)発明者　ルール，ジェフリー
最終頁に続く

(54)【発明の名称】　ユニフォームリソースロケータ内のアクティブリンクを利用して金銭授受を実施するシステムおよび技術

(57)【要約】
ペイメントカードをモバイルデバイスにタップするシステムが、別のユーザに金銭を送る、または他のユーザに金銭を要求するユーザを認証するために使用される。第１のユーザがペイメントカードを自身のデバイスにタッチすると、金銭を受け取る、または金銭要求を受け取るユーザのモバイルデバイスに、暗号化された文字列を有するＵＲＬが送信される。別のユーザのモバイルデバイスは、ＵＲＬを開いた結果として、銀行取引アプリを起動する。そのアプリは、暗号化された文字列を使用して、金銭を送るまたは要求する第１のユーザを認証する。

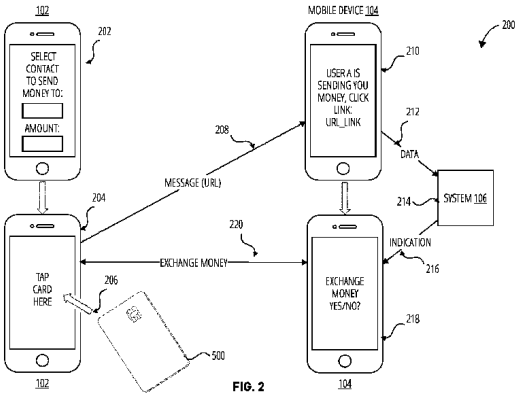


FIG. 2

【特許請求の範囲】
【請求項１】
モバイルデバイスであって、
ディスプレイデバイスと、
プロセッサと、
メモリとを含み、
前記メモリは、前記プロセッサによって実行されると、前記プロセッサに、
第１のユーザの第２のモバイルデバイスと金銭の電子授受を実施する入力を受信させ、
前記モバイルデバイス上に非接触カードを提供する指示を前記ディスプレイデバイスに提示させ、
前記非接触カードから、第２のユーザの秘密鍵で暗号化された第１のデータを受信させ、
前記第２のモバイルデバイスと送信する前記第１のデータを含み、前記第２のモバイルデバイスに、前記第１のデータを用いて前記第２のユーザの認証を実施させるユニフォームリソースロケータ（ＵＲＬ）を含むメッセージを生成させ、
前記メッセージを前記第２のモバイルデバイスに通信させ、
前記第２のユーザの前記認証に基づいて、前記金銭の電子授受をさせる、
命令を含む、
モバイルデバイス。
【請求項２】
前記メモリおよび前記プロセッサに結合された入力デバイスを備え、前記入力デバイスが、連絡先の選択、電子授受する金額の指示、またはそれらの組み合わせを含む前記入力を受信する、
請求項１に記載のモバイルデバイス。
【請求項３】
前記ＵＲＬが、前記金額を識別する第１の識別子と、前記第１のユーザを識別する第２の識別子とをさらに含む、
請求項２に記載のモバイルデバイス。
【請求項４】
前記プロセッサが、
近距離無線通信（ＮＦＣ）信号を介して、前記非接触カードを検出し、
前記非接触カードが前記モバイルデバイスの通信範囲内に入ることに基づいて、前記非接触カードとのＮＦＣ交換を開始し、かつ
前記ＮＦＣ交換を介して、前記非接触カードから前記第１のデータを受信する、
請求項１に記載のモバイルデバイス。
【請求項５】
前記ＵＲＬが、アクティブ化されると、前記第２のモバイルデバイス上でウェブページを起動して、前記第１のデータを用いて前記第２のユーザの前記認証を実施するリンクを含む、
請求項１に記載のモバイルデバイス。
【請求項６】
前記第１のデータが、前記非接触カードに記憶された前記秘密鍵で暗号化された文字列を含む、請求項１に記載のモバイルデバイス。
【請求項７】
前記秘密鍵が鍵ペアの一部であり、前記鍵ペアが、前記非接触カード、前記第１のユーザ、またはそれらの組み合わせに関連付けられた公開鍵をさらに含む、
請求項１に記載のモバイルデバイス。
【請求項８】
前記プロセッサが、前記第２のユーザが前記第２のモバイルデバイスから認証に成功したことを示す結果を受信し、前記結果に基づいて前記電子授受を引き起こす、請求項１に

記載のモバイルデバイス。
【請求項９】
前記プロセッサが、ショートメッセージサービス（ＳＭＳ）メッセージ、マルチメディアメッセージサービス（ＭＭＳ）メッセージ、またはリッチ通信サービス（ＲＣＳ）メッセージとして前記第２のモバイルデバイスに前記メッセージを送信する、請求項１に記載のモバイルデバイス。
【請求項１０】
モバイルデバイスであって、
入力デバイスと、
プロセッサと、
メモリとを含み、
前記メモリは、前記プロセッサによって実行されると、前記プロセッサに、
第２のモバイルデバイスから第１のデータを含み、前記モバイルデバイスに前記第１のデータを用いて第１のユーザの認証を実施させる、ユニフォームリソースロケータ（ＵＲＬ）を含むメッセージを受信させ、
前記入力デバイスを介して、前記ＵＲＬをアクティブ化する入力を検出させ、
前記入力に応答して、サーバと通信して、前記第１のデータを用いて前記第１のユーザの前記認証を実施するアプリケーションを起動させ、
前記第１のユーザが前記サーバによって認証されたという指示を受信させ、
前記第１のデータと、前記第１のユーザが認証されたという前記指示とに基づいて、金銭の授受の実施を行わせる、
命令を含む、
モバイルデバイス。
【請求項１１】
前記入力デバイスがタッチスクリーンインタフェースを備え、前記タッチスクリーンインタフェースが、ディスプレイデバイス上の前記ＵＲＬの選択を検出する、
請求項１０に記載のモバイルデバイス。
【請求項１２】
前記ＵＲＬが、選択されると、前記アプリケーションを起動するリンクを含む、
請求項１１に記載のモバイルデバイス。
【請求項１３】
グラフィカルユーザインタフェース（ＧＵＩ）ディスプレイに前記メッセージを提示するように構成されたディスプレイデバイスを備える、
請求項１０に記載のモバイルデバイス。
【請求項１４】
前記プロセッサが、前記第１のデータを前記サーバに通信して、前記第１のユーザの前記認証を実施する、
請求項１０に記載のモバイルデバイス。
【請求項１５】
前記ＵＲＬは、授受する金額の第１の識別子と、前記第１のユーザを識別する第２の識別子とをさらに含み、
前記プロセッサは、前記第１の識別子および前記第２の識別子の少なくとも一方を前記サーバに送信する、
請求項１４に記載のモバイルデバイス。
【請求項１６】
前記プロセッサは、前記金額および前記認証されている前記第１のユーザに基づいて、前記授受の前記実施を行わせる、
請求項１５に記載のモバイルデバイス。
【請求項１７】
第１のデータは、前記第１のユーザに関連付けられた暗号化された文字列を含み、

前記指示は、前記暗号化された文字列が前記第１のユーザに関連付けられた秘密鍵を用いた復号に成功したことを示す情報を含む、
請求項１０に記載のモバイルデバイス。
【請求項１８】
暗号化された文字列は、前記第１のユーザに関連付けられた非接触カードに記憶された秘密鍵で暗号化される、
請求項１７に記載のモバイルデバイス。
【請求項１９】
前記プロセッサは、ショートメッセージサービス（ＳＭＳ）メッセージ、マルチメディアメッセージサービス（ＭＭＳ）メッセージ、またはリッチ通信サービス（ＲＣＳ）メッセージとして前記メッセージを受信する、
請求項１０に記載のモバイルデバイス。
【請求項２０】
第１のユーザに関連付けられた第１のモバイルデバイスのプロセッサによって、第２のモバイルデバイスの第２のユーザと金銭を授受する要求を検出し、
ディスプレイデバイス上のプロンプトによって、前記第１のユーザデバイスに関連付けられた前記第１のユーザに、前記第１のユーザデバイスに非接触カードをタップするように要求し、
前記非接触カードから、前記第１のユーザに関連付けられた秘密鍵で暗号化された第１のデータを受信し、
第２のユーザデバイスに送信するために前記第１のデータをさらに含み、前記第２のモバイルデバイスに、前記第１のデータを用いて前記第１のユーザの認証を実施させるユニフォームリソースロケータ（ＵＲＬ）を含むテキストメッセージを生成し、
前記第２のモバイルデバイスに前記メッセージを通信し、
前記第１のユーザが認証されたことを示す指示を、前記第２のモバイルデバイスから受信し、
前記金銭を授受するために前記第２のモバイルデバイスと情報を交換する、
ことを含む、コンピュータに実行される方法。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願
本出願は、２０２１年５月１１日に出願された「ＳＹＳＴＥＭＳ ＡＮＤ ＴＥＣＨＮＩＱＵＥＳ ＴＯ ＵＴＩＬＩＺＥ ＡＮ ＡＣＴＩＶＥ ＬＩＮＫ ＩＮ Ａ ＵＮＩＦＯＲＭ ＲＥＳＯＵＲＣＥ ＬＯＣＡＴＯＲ ＴＯ ＰＥＲＦＯＲＭ Ａ ＭＯＮＥＹ ＥＸＣＨＡＮＧＥ」と題する米国特許出願第１７／３１７，２６２号の優先権を主張する。前述の出願の内容は、その全体が参照により本明細書に引用される。
【背景技術】
【０００２】
ユーザが他のユーザと金銭を授受することを可能にする多くの種類の電子決済システムが存在する（すなわち、ピアツーピア決済トランザクション）。理論的には、従来の電子決済システムは、ユーザ間で金銭の振替を行う便利な方法を提供する。しかしながら、従来の電子決済システムには、ユーザのフラストレーション、混乱を引き起こし、満足のいかない授受をもたらすことが多いいくつかの欠点がある。従来の電子決済システムのそのような欠点の１つは、電子決済システムが通常、送金者と受取人の両方が加入しなければならず、トランザクションを完了するためにユーザがいくつかのステップを行う必要があるスタンドアロンシステムであることである。場合によっては、送金者、受取人、またはその両方が、口座を設定し、システムを使用して別の銀行取引システムを介して決済を送る、または受け取るために機密の金融情報を提供する時間のかかるプロセスを経る必要があり得る。多くの場合、最初のトランザクション後に、ユーザがその電子決済システムを

使用することはほとんどない。

【０００３】

従来の電子決済システムの限られた性質はまた、不便を追加する。特に、従来の電子決済システムのスタンドアロンの性質は、通常、ユーザが決済を送る、または受け取るために、決済トランザクション専用の別個のアプリケーションを開くことを必要とする。従来の電子決済システムのスタンドアロンの性質の不便さは、そのようなシステムを使用するユーザを妨げる可能性がある。したがって、従来の電子決済システムおよび方法にはいくつかの欠点がある。

【発明の概要】

【０００４】

実施形態は、ディスプレイデバイス、プロセッサ、およびメモリを含むモバイルデバイスを含むシステム、デバイス、技術、および方法を含むことができる。メモリは、プロセッサによって実行されると、プロセッサに、第１のユーザの第２のモバイルデバイスと金銭の電子授受を実施する入力を受信させ、モバイルデバイス上に非接触カードを提供する指示をディスプレイデバイスに提示させ、非接触カードから、第２のユーザの秘密鍵で暗号化された第１のデータを受信させ、第２のモバイルデバイスに送信する第１のデータを含み、第２のモバイルデバイスに、第１のデータを用いて第２のユーザの認証を実施させるユニフォームリソースロケータ（ＵＲＬ）を含むメッセージを生成させ、メッセージを第２のモバイルデバイスに通信させ、かつ第２のユーザの認証に基づいて、金銭の電子授受（electronic exchange of money）をさせる、命令を含む。

【０００５】

実施形態はまた、入力デバイス、プロセッサ、およびメモリを含むモバイルデバイスを含むシステム、デバイス、技術、および方法を含む。メモリは、プロセッサによって実行されると、プロセッサに、第２のモバイルデバイスから第１のデータを含み、モバイルデバイスに第１のデータを用いて第１のユーザの認証を実施させるユニフォームリソースロケータ（ＵＲＬ）を含むメッセージを受信させ、入力デバイスを介して、ＵＲＬをアクティブ化する入力を検出させ、入力に応答して、サーバと通信して、第１のデータを用いて第１のユーザの認証を実施するアプリケーションを起動させ、第１のユーザがサーバによって認証されたという指示を受信させ、第１のデータと、第１のユーザが認証されたという指示とに基づいて、金銭の授受（exchange of money）の実施をさせる、命令を含む。

【０００６】

実施形態はまた、コンピュータに実行される方法を含むシステム、デバイス、技術、および方法を含み、コンピュータに実行される方法は、第１のユーザに関連付けられた第１のモバイルデバイスのプロセッサによって、第２のモバイルデバイスの第２のユーザと金銭を授受する要求を検出し、ディスプレイデバイス上のプロンプトによって、第１のユーザデバイスに関連付けられた第１のユーザに、第１のユーザデバイスに非接触カードをタップするように要求し、非接触カードから、第１のユーザに関連付けられた秘密鍵で暗号化された第１のデータを受信し、第２のユーザデバイスに送信するために第１のデータをさらに含み、第２のモバイルデバイスに、第１のデータを用いて第１のユーザの認証を実施させるユニフォームリソースロケータ（ＵＲＬ）を含むテキストメッセージを生成し、第２のモバイルデバイスにメッセージを通信し、第１のユーザが認証されたことを示す指示を、第２のモバイルデバイスから受信し、金銭を授受するために第２のモバイルデバイスと情報を交換することとを含む。

【図面の簡単な説明】

【０００７】

【図１】本明細書で説明する実施形態に係るシステム１００の一例を示す図である。

【図２】一実施形態に係る主題の態様を示す図である。

【図３】本明細書で説明する実施形態に係るルーチン３００を示す図である。

【図４】本明細書で説明する実施形態に係るルーチン４００を示す図である。

【図５】実施形態に係る非接触カード５００を示す図である。
【図６】実施形態に係るトランザクションカード構成要素６００を示す図である。
【図７】実施形態に係るシーケンスフロー７００を示す図である。
【図８】実施形態に係る鍵システム８００の図である。
【図９】実施形態に係る暗号文を生成するフローチャート９００の一例の図である。
【図１０】実施形態に係るフローチャート１０００の一例を示す図である。
【図１１】実施形態に係る１１００の一例を示す図である。
【図１２】一実施形態に係るコンピュータアーキテクチャ１２００を示す図である。
【図１３】一実施形態に係る通信アーキテクチャ１３００を示す図である。
【発明を実施するための形態】
【０００８】
本明細書で説明する実施形態は、一般に、ユーザが安全で合理化された方法で金銭を授受することを可能にするデバイス、システム、および技術に関することができる。例えば、モバイルデバイスを使用するユーザは、モバイルデバイスを介して別のユーザに金銭を送ることができる。授受は、送金者がモバイルデバイス上に銀行取引アプリケーションと対話することによって実施することができる。具体的には、銀行取引アプリケーションは、ユーザが人または連絡先を入力し、金額を入力し、特定の人物または連絡先に金銭を送ることを可能にすることができる。送金者の銀行取引アプリケーションは、送金者を識別する情報および金額を含むメッセージを生成することができる。メッセージは、授受を開始するために受取人のモバイルデバイスに送信することができる。場合によっては、メッセージは、情報が埋め込まれたユニフォームリソースロケータ（ＵＲＬ）を含んでもよい。ＵＲＬは、受取人のモバイルデバイス上で銀行取引アプリケーションを自動的に起動して、送金者を認証して授受を実施するために、受取人によって呼び出されてもよい。
【０００９】
以下の説明でより詳細に説明するように、技術は、送金者を認証するために送金者に関連付けられた安全なデータを含む非接触カードを利用するので、以前の解決策よりも安全で合理化されている。安全なデータは、ＵＲＬに埋め込まれ、メッセージ内の受取人のモバイルデバイスに送信することができる。受取人のモバイルデバイスは、送金者をローカルまたはサーバを介してリモートのいずれかで認証し、次いで認証プロセスの結果に基づいて授受の実施に進むことができる。
【００１０】
さらに、授受は、送金者および受取人によって実施される動作の数を最小限にして行うことができる。例えば、送金者は、連絡先を選択または入力し、金額を入力し、モバイルデバイス上に非接触カードをタップして授受を実施することができる。受取人は、メッセージを読んでＵＲＬをアクティブ化し、金銭の授受を確認することができる。授受は、送金者のモバイルデバイス、受取人のモバイルデバイス、および銀行取引システムまたは第三者システムによって実施される動作に基づいて行われ得る。詳細は以下の説明で説明する。
【００１１】
図１は、ユーザがモバイルデバイスを介して金銭を授受することを可能にすることを含む、本明細書で論じられる動作を実施するシステム１００の一例を示す。図示のシステム１００は、説明の目的のために限られた数の構成要素およびデバイスを含む。実施形態では、システム１００は、任意の数のユーザがデバイスを介して他のユーザに金銭を送ることを可能にする任意の数のサーバ、デバイス、ネットワーキング機器などを含む。
【００１２】
図１において、システム１００は、モバイルデバイス１０２と、モバイルデバイス１０４と、システム１０６とを含み、これらはすべて、例えばインターネットなどのネットワーク１０８を介して結合することができる。モバイルデバイスの例は、セルラー電話、携帯情報端末、タブレットコンピュータなどを含むことができ、セルラープロトコル、無線プロトコルなどに従って通信される。一例では、モバイルデバイスは、金属またはプラス

チックなどの材料で作られたハウジングを含むことができ、１つ以上のプロセッサ、メモリ、ストレージ、入力デバイス（タッチスクリーンインタフェース、ボタン、センサ、マイクロフォンなど）、出力デバイス（ディスプレイ、スピーカ、振動デバイス、ハプティクスデバイスなど）、短距離通信無線機、アンテナなどの構成要素を含むことができる。

【００１３】

図示の例では、モバイルデバイス１０２は、ネットワーク１０８を介してモバイルデバイス１０４と通信することができ、その逆も可能である。場合によっては、モバイルデバイスは、ローカルエリアネットワーク、無線ローカルエリアネットワーク、ワイドエリアネットワークなどの他のネットワークを介して互いに通信することができる。モバイルデバイスはまた、互いの間に安全なポイントツーポイント（Ｐ２Ｐ）接続または直接接続を確立してもよい。Ｐ２Ｐまたは直接接続は、例えばＢｌｕｅｔｏｏｔｈ　Ｌｏｗ　Ｅｎｅｒｇｙ（ＢＬＥ）、Ｂｌｕｅｔｏｏｔｈ、ワイヤレスフィディリティ（ＷｉＦｉ）、ＨａＬｏｗ（ＩＥＥＥ８０２．１１ａｈ）、Ｚ－ｗａｖｅ、またはＺｉｇｂｅｅなどのプロトコルを利用して確立することができる。

【００１４】

実施形態では、モバイルデバイスは、オペレーティングシステムおよびアプリケーションまたはアプリなどのソフトウェアを含む。オペレーティングシステムは、ＡＮＤＲＩＯＤ（登録商標）、ＩＯＳ（登録商標）、またはＷＩＮＤＯＷＳ（登録商標）などの任意の種類の動作であってもよく、モバイルデバイスのハードウェア、ソフトウェアリソースを管理し、他のアプリケーションにサービスを提供してもよい。アプリケーションは、モバイルデバイス上で動作し、ユーザにサービスおよび体験を提供するように設計されたソフトウェアアプリケーションであってもよい。アプリケーションの例には、生産性アプリケーション、例えば、Ｅメールアプリケーション、メッセージングアプリケーション、電話アプリケーション、連絡先データベース、カレンダーアプリケーションなどが含まれる。他のアプリケーションは、ゲームアプリケーション、地図アプリケーション、位置ベースのサービスなどを含むことができる。

【００１５】

本明細書で説明する実施形態では、モバイルデバイスはまた、１つ以上の銀行口座に関連付けられた銀行取引アプリケーションを含むことができ、ユーザが互いに金銭を送る／受け取ることを可能にすることを含む、ユーザに銀行サービスを提供する。銀行取引アプリケーションはまた、追加の銀行サービス、例えば、口座管理、請求書の支払い、口座審査などを提供してもよい。高レベルでは、銀行取引アプリケーションは、１つ以上のグラフィカルユーザインタフェース（ＧＵＩ）ディスプレイでユーザに情報を提示し、ユーザ入力および選択を処理し、他のアプリケーションと通信し、１つ以上のバックエンドシステム（銀行サーバ）およびサービスと通信するなどして、銀行サービスを提供することができる。

【００１６】

モバイルデバイス１０２および１０４はまた、ネットワーク１０８を介してシステム１０６と結合されてもよい。システム１０６は、１つ以上のサーバまたはコンピューティングデバイスを含み、モバイルアプリケーションが金銭を送る／受け取る１つ以上のサービスを提供することができる。一例では、システム１０６は、別のユーザに金銭を送ることを要求するユーザ、または別のユーザに金銭を要求するユーザを認証する認証動作を実施する銀行取引システムであってもよい。システム１０６はまた、一般的な銀行サービス、口座管理、決済サービスなどの追加のサービスを提供することができる。実施形態はこのように限定されない。場合によっては、システム１０６は、モバイルデバイス１０２と１０４との間の金銭の授受を処理してもよい。例えば、システム１０６は、送金者の口座から金銭を電子的に差し引き、受取人の口座に金銭を電子的に追加することができる。場合によっては、送金者は第１の銀行取引システムに関連付けられる場合があり、受取人は第２の銀行取引システムに関連付けられる場合がある。銀行取引システムは、金銭の授受を調整するために互いにデータを送信することができる。以下の説明において、図２は、シ

ステム１００を利用して金銭の振替を実施する追加の詳細を示す。
【００１７】
図２は、第１のモバイルデバイス１０２から第２のモバイルデバイス１０４に金銭を送るためにシステム１００で実施され得るシーケンス図２００の一例である。図２は１つの可能なシーケンスを示し、いくつかの実施形態では、１つ以上の動作が他の動作の前、後、および同時に行われ得ることに留意されたい。また、以下でより詳細に説明するように、ユーザは別のユーザにお金を要求することができる。
【００１８】
２０２において、モバイルデバイス１０２は、ユーザが金銭を送る（または金銭を要求する）情報を入力する１つ以上のＧＵＩディスプレイを提示することができる。具体的には、銀行取引アプリケーションまたはウェブブラウザなどの、モバイルアプリケーションを含むモバイルデバイス１０２は、１つ以上のＧＵＩディスプレイを提示する。ディスプレイは、ユーザが対話し、例えば選択を行い、オプションおよびメニューをナビゲートし、動作を実施することができる。ＧＵＩディスプレイは、任意の種類の入力要素、例えば、入力フィールド、ドロップダウンメニュー、タッチベースのメニューまたはボタンなどを含むことができ、モバイルデバイス１０２は、入力デバイス、例えば、ボタン、スクロールホイール、タッチスクリーンインタフェースなどによって検出されたユーザ入力を処理する。図示の例では、銀行取引アプリケーションは、ユーザが連絡先および金額を入力するエリアを提示する。テキストフィールドは、自動入力、サジェスチョンなどの機能を含み、例えば、Ｅメールアドレス、電話番号、ユーザ名などのいくつかの形式で連絡先を受け入れてもよい。実施形態は、図示された特定のＧＵＩディスプレイに限定されず、ディスプレイは別のフォーマットであってもよい。例えば、銀行取引アプリケーションは、モバイルデバイス１０２上の連絡先データベースから連絡先のリストを提供することができる。場合によっては、リストは、使用頻度、最も近い連絡先、友人対家族などの基準に基づいて順序付けられてもよい。場合によっては、モバイルアプリケーションは、２つ以上のＧＵＩディスプレイ、例えば、連絡先を入力する第１のＧＵＩディスプレイ（またはページ）、および金額を入力する第２のＧＵＩディスプレイを提示することができる。上述したように、場合によっては、ユーザは別のユーザにお金を要求する場合がある。これらの例では、ユーザに同様のＧＵＩディスプレイを提示することができるが、しかしながら、ＧＵＩディスプレイは、ユーザが金銭を送るのではなく、金銭を要求しているという指示を提供する。
【００１９】
２０２において、ユーザは、連絡先を選択または入力し、送る（または要求する）金額を提供することができる。モバイルデバイス１０２は、入力を処理して、選択された連絡先に関連付けられたデバイス、例えばモバイルデバイス１０４を決定することができる。モバイルデバイス１０２は、金銭を送るまたは要求するためにユーザを認証する認証動作を実施する。図示の例では、モバイルデバイス１０２は、ユーザに関連付けられた非接触カードを利用して認証を実施する。
【００２０】
２０４において、銀行取引アプリケーションを含むモバイルデバイス１０２は、モバイルデバイス１０２上にカードをタップするようにユーザに命令するＧＵＩディスプレイを提示することができる。場合によっては、ＧＵＩディスプレイは、特定の表面、例えば、モバイルデバイス１０２のディスプレイまたは背面上にカードをタップするようにユーザに命令することができる。モバイルデバイス１０２上にカードをタップすると、モバイルデバイス１０２とカードとの間のデータの交換が開始される。モバイルデバイス１０２および非接触カード５００の両方は、短距離通信プロトコルを利用して互いに通信する。例えば、非接触カードおよびモバイルデバイス１０２は、１回以上の近距離無線通信（ＮＦＣ）交換を実施することができる。交換の一部として、非接触カード５００は、ユーザを認証するために使用され得る情報およびデータを、１０２に送信することができる。例えば、２０６において、５００は、５００に記憶され、ユーザを一意に識別する文字列、例

えば英数字の文字列を送信することができる。場合によっては、非接触カード５００は、モバイルデバイス１０２によって実施された要求または読み取りに基づいて文字列を送信することができる。さらに、非接触カード５００は、非接触カード５００に記憶された秘密鍵を使用して文字列を暗号化し、暗号化された文字列として文字列をモバイルデバイス１０２に送信することができる。秘密鍵は、鍵ペアの一部であり、ユーザを認証するために使用され得る公開鍵に関連付けることができる。実施形態では、秘密鍵は、カードプロバイダによって生成され、カードプロバイダに関連付けられた独自の鍵であってもよい。他の例では、秘密鍵は、Ｅｕｒｏｐａｙ、Ｍａｓｔｅｒｃａｒｄ、Ｖｉｓａ（ＥＭＶ）規格に従って動作を実施することに関連付けられてもよい。

【００２１】

２０６において、モバイルデバイス１０２は、非接触カード５００から受信した情報を処理し、選択された連絡先に関連付けられたデバイス（モバイルデバイス１０４）に送信するメッセージを生成することができる。実施形態では、モバイルデバイス１０２は、連絡先の識別子または属性、例えば、電話番号、ユーザ名、電子メール（Ｅメール）アドレスなどを使用して、モバイルデバイスにメッセージを送信することを決定することができる。図示の例では、モバイルデバイス１０２は、例えばＳＭＳ、ＭＭＳ、ＲＣＳなどのテキストメッセージングプロトコルに従ってテキストメッセージを生成する。しかしながら、実施形態では、例えば電子メール、リアルタイムメッセージングなどの他のフォーマットが利用されてもよく、ユーザデータグラムプロトコル（ＵＤＰ）および伝送制御プロトコル（ＴＣＰ）などのプロトコルを使用してもよい。

【００２２】

メッセージは、別のユーザが金銭を送りたい（または金銭を要求したい）ことを受取人に示す情報、非接触カード５００から受信した情報、およびユーザ入力に基づく情報、例えば、選択された連絡先および入力された金額を含むことができる。実施形態では、メッセージはまた、アクティブリンクまたはアクティブＵＲＬを含むことができる。アクティブＵＲＬは、金銭の授受を容易にするために受取人によって使用することができる。例えば、受取人は、ＵＲＬを選択またはアクティブ化することができ、これにより、受取人のデバイスのモバイルアプリケーションが起動する。アクティブＵＲＬは、例えば、モバイルデバイス１０４上で銀行取引アプリまたはウェブページを起動するディープリンクであってもよい。実施形態では、ＵＲＬは、非接触カード５００によって生成された暗号化された文字列、受取人の識別子、金額の識別子、および送金者の識別子のうちの１つ以上を含む情報に埋め込まれてもよい。ＵＲＬは、１つ以上のオペレーティングシステムおよびＡＰＩに従ったフォーマットであってもよい。例えば、メッセージは、オペレーティングシステムＩＯＳ、ＡＮＤＲＯＩＤ、および／またはＭＩＣＲＯＳＯＦＴの規格およびＡＰＩに従ったフォーマットのＵＲＬを含むことができる。例示的なフォーマットは、「ａｐｐａｍ：／／＜ｓｔｒｉｎｇ＞　＜ｒｅｃｉｐｉｅｎｔ　ｉｄｅｎｔｉｆｉｅｒ＞　＜ａｍｏｕｎｔ　ｉｄｅｎｔｉｆｉｅｒ＞」または「ｈｔｔｐｓ：／／ｓｉｔｅ．ｃｏｍ／＜ｓｔｒｉｎｇ＞／＜ｒｅｃｉｐｉｅｎｔ　ｉｄｅｎｔｉｆｉｅｒ＞／＜ａｍｏｕｎｔ　ｉｄｅｎｔｉｆｉｅｒ＞」を含むことができるが、実施形態はこのように限定されない。

【００２３】

２０８において、モバイルデバイス１０２は、モバイルデバイス１０４、すなわち連絡先に関連付けられたデバイスにメッセージを送信することができる。メッセージは、メッセージの種類に基づいて、１つ以上の通信プロトコルに従って送信することができる。２１０において、モバイルデバイス１０４は、メッセージを受信し、ディスプレイデバイス上にメッセージを提示することができる。上述したように、メッセージは、モバイルデバイス１０４のユーザによって選択可能なアクティブＵＲＬを含むことができる。モバイルデバイス１０４は、メッセージングアプリケーションのＧＵＩディスプレイにメッセージを提示することができる。ユーザは、メッセージと対話し、ＵＲＬを選択またはクリックすることができる。モバイルデバイス１０４は、ユーザがＵＲＬを選択および／またはアクティブ化したことを検出し、ＵＲＬ内の情報に基づいてアプリケーションまたはウェブ

ページを起動する。モバイルデバイス１０４は、ウェブブラウザで銀行取引アプリケーションまたはウェブページなどのアプリケーションを起動することができる。実施形態では、アプリケーションを含むモバイルデバイス１０４はまた、ＵＲＬに埋め込まれた情報を処理する。例えば、アプリケーションは、２１２において、暗号化された文字列を処理し、暗号化された文字列をＡＰＩを介してシステム１０６に渡して送金者を認証することができる。実施形態では、アプリケーションはまた、送金者の識別子、受取人の識別子、および金額を含む他のデータをシステム１０６に送信することができる。

【００２４】

２１４において、システム１０６は、モバイルデバイス１０４から受信した情報に基づいて送金者を認証することができる。例えば、システム１０６は、送金者の識別子を利用して検索を実施し、データベースまたはデータストアから記憶された認証文字列を決定することができる。システム１０６はまた、送金者に関連付けられた公開鍵を決定し、文字列の復号を試みることができる。次いで、復号された文字列を認証文字列と比較して、それらが一致するかどうかを決定し、送金者を認証することができる。システム１０６が、文字列が一致すると決定した場合、送金者は認証され、一致しない場合、送金者は認証されない。

【００２５】

２１６において、システム１０６は、送金者が認証されたかどうかに関する比較または指示の結果を返すことができる。指示は、結果として、認証動作を実施するＡＰＩ呼び出しに通信されてもよい。２１８において、モバイルデバイス１０４は、ＧＵＩディスプレイで指示をユーザに提示することができる。場合によっては、モバイルデバイス１０４は、ユーザがお金を受け入れる、または拒否する選択肢を表示することができる。モバイルデバイス１０４は、授受を拒否するというユーザ入力を処理して動作を停止するか、または金銭を授受する追加の動作を実施しないことができる。代替的に、モバイルデバイス１０４は、２２０において、金銭の授受を受け入れる、または進めるというユーザ入力を処理して、授受を実施する追加の動作を実施することができる。例えば、モバイルデバイス１０４は、送金を進めるためにモバイルデバイス１０２に指示または通信を提供することができる。モバイルデバイス１０２は、受取人およびモバイルデバイス１０４に関連付けられた口座に金銭を電子的に振り替える指示を、銀行サーバなどの１つ以上のバックエンドサーバに送信することができる。他の例では、アプリケーションは、金銭の振替を進める指示を銀行サーバに送信することができる。

【００２６】

場合によっては、モバイルデバイス１０２とモバイルデバイス１０４との間に安全な接続を確立して、金銭を授受することができる。安全な接続は、モバイルデバイス１０２とモバイルデバイス１０４との間のＰ２Ｐローカライズされた接続であり得る。モバイルデバイス１０２は、金銭を電子トークンとしてモバイルデバイス１０４に送ることができる。モバイルデバイス１０４は、トークンを処理し、銀行サーバと通信して、振替の指示を提供することができる。トークンは、授受を完了するために銀行サーバによって使用され得る情報を含むことができる。情報は、送金者の識別子、受取人の識別子、金額などを含むことができる。実施形態はこのように限定されない。

【００２７】

図３は、システム１００によって実施され得る例示的なルーチン３００を示す。具体的には、ルーチン３００は、モバイルデバイスを介して別のユーザに金銭を送る（または金銭を要求する）モバイルデバイスによって実施されてもよい。

【００２８】

ブロック３０２において、ルーチン３００は、第１のユーザに関連付けられた第１のモバイルデバイスのプロセッサによって、第２のモバイルデバイスの第２のユーザと金銭を授受する要求を検出することを含む。例えば、モバイルデバイスは、ユーザがＰ２Ｐ授受を介して別の人物に金銭を送るまたは要求する１つ以上の選択肢を提示し得る銀行取引アプリケーションを含んでもよい。ユーザは、銀行取引アプリケーションを介して、金銭を

送るか、または金銭を要求するかを選択する入力を提供することができる。ユーザはまた、授受の追加情報を提供することができる。例えば、アプリケーションは、ユーザが、金銭を送るまたは要求する連絡先または人物、および授受する金額を入力することを可能にすることができる。モバイルデバイスは、例えば、別のユーザに金銭を送るためにタッチスクリーンインタフェースを介して入力選択を受信することができる。一例では、入力選択は、モバイルデバイスに記憶された連絡先リストからの連絡先の選択を含むことができる。他の例では、ユーザは、物理キーボードまたは仮想キーボードなどのキーボードを使用してフィールドに連絡先をタイプ入力することができる。他の例では、ユーザは、電話番号、Ｅメールアドレス、ユーザ名などの他の識別情報を提供することができる。実施形態は、これらの例に限定されなくてもよい。

【００２９】

金銭の授受を実施するために、ユーザは、第２のモバイルデバイスおよび第２のユーザに対して認証されなければならない。パスワードの提供、生体分析の実施、テキストメッセージでのコードの送信などを含む典型的な認証方法を利用することができる。しかしながら、本明細書で説明する実施形態は、非接触カードを利用することによって追加のセキュリティを提供することができる。図示のルーチン３００では、第１のユーザは、第１のユーザに関連付けられた非接触カードを利用して認証される。非接触カードを使用してユーザを認証することは、ユーザがカードを所有し、非接触カードがユーザに一意のトークンまたは文字列を含むことを保証することによって、他の技術を超える利点を提供する。より詳細に説明するように、トークンまたは文字列は、第三者、例えば銀行取引システムまたは他の第三者認証システムを介してユーザを認証するために使用することができる。場合によっては、第２のユーザは、ローカル認証文字列および第１のユーザに関連付けられた公開鍵を利用して第１のユーザを認証することができる。

【００３０】

非接触カードを用いて実施される認証動作は、モバイルデバイスが非接触カードと情報を交換することを含み、これは、ユーザが非接触カードをモバイルデバイスの通信範囲内（ＮＦＣ通信範囲は約１０ｃｍ）に持ち込むことによって開始することができる。ブロック３０４において、ルーチン３００は、ディスプレイデバイス上のプロンプトによって、第１のモバイルデバイスに関連付けられた第１のユーザに、第１のモバイルデバイス上に非接触カードをタップするように要求することを含む。非接触カードがモバイルデバイスの十分な範囲内に入ると、デバイスとカードとの間に接続を確立することができ、モバイルデバイスはカードとデータを交換することができ、カードはモバイルデバイスとデータを交換することができる。モバイルデバイス上にカードをタップするようにユーザに命令することは、カードが通信範囲内にあることを保証する。しかしながら、他の実施形態は、非接触カードをモバイルデバイスに接近、またはその近くに持ってくるようにユーザに命令することを含んでもよく、モバイルデバイスは、カードが通信範囲内にあるときに指示、例えば、メッセージまたはアイコンの表示、ＬＥＤの点灯などを提供することができる。

【００３１】

ブロック３０６において、ルーチン３００は、非接触カードからデータを受信することを含む。データは、第１のユーザに関連付けられ、非接触カードに安全に記憶された秘密鍵、例えば、独自の秘密鍵またはＥＭＶベースの秘密鍵で、非接触カードによって暗号化することができる。場合によっては、非接触カードは、１つ以上のＮＦＣデータ授受フォーマット（ＮＤＥＦ）メッセージでモバイルデバイスにデータを送信することができる。暗号化されたデータは、やはり非接触カードに安全に記憶されたトークンまたは文字列などの、第１のユーザを識別する情報を含むことができる。モバイルデバイスは、交換が完了したときに、メッセージが第２のモバイルデバイスに送信されるべきであるという指示をユーザに提供することができる。

【００３２】

実施形態では、モバイルデバイスは、金銭の授受の指示を生成し、第２のユーザに関連

付けられた第２のモバイルデバイスに送信することができる。例えば、ブロック３０８において、ルーチン３００は、授受の情報を含むテキスト、ユニフォームリソースロケータ（ＵＲＬ）、および非接触カードからのデータを含むテキストメッセージを生成することを含む。テキストは、送金者および金額を識別することができる。ＵＲＬは、受取人によってアクティブ化されると、受取人側モバイルデバイスにアプリケーションを起動させ、非接触カードからのデータを使用して第１のユーザの認証を実施させるアクティブＵＲＬまたはディープリンクであってもよい。実施形態では、モバイルデバイスは、メッセージを生成し、メッセージおよび／またはＵＲＬにデータを埋め込むことができる。例えば、暗号化された文字列を含むデータは、パラメータとしてＵＲＬに組み込まれてもよい。したがって、ＵＲＬがアクティブ化されると、暗号化された文字列が起動されたアプリケーションに渡される。場合によっては、モバイルデバイスは、送金者を識別する識別子、受取人を識別する識別子、および指定された授受する金額を含む追加情報をＵＲＬに含めることができる。識別子および指定された金額はまた、パラメータとして起動されたアプリケーションに渡されてもよく、授受を処理するためにアプリケーションによって使用されてもよい。

【００３３】

ブロック３１０において、ルーチン３００は、メッセージを第２のモバイルデバイスに送信することを含む。メッセージは、テキストメッセージであってもよく、関連付けられた電話番号に基づいて第２のモバイルデバイスに通信されてもよい。テキストメッセージは、ＳＭＳ、ＭＭＳ、およびＲＣＳなどの任意の種類のメッセージングプロトコルに従って送信することができる。場合によっては、メッセージ、Ｅメール、チャットアプリケーションなどを送信するために他の媒体が使用されてもよい。実施形態はこのように限定されない。

【００３４】

実施形態では、第２のモバイルデバイスは、メッセージを受信し、メッセージを処理することができる。例えば、第２のモバイルデバイスは、ＧＵＩディスプレイのディスプレイデバイス上に第２のユーザにメッセージを提示することができる。ＵＲＬが第２のユーザによってアクティブ化されると、第２のモバイルデバイスは、第１のユーザを認証することを含む追加の動作を実施することができる。場合によっては、認証は、第２のモバイルデバイスによってローカルに実施されてもよく、他の場合には、第２のモバイルデバイスは、第１のユーザを認証するために銀行取引システムまたは他の第三者システムを利用してもよい。第２のモバイルデバイスは、認証動作の結果を決定し、その結果を第１のモバイルデバイスに提供することができる。

【００３５】

ブロック３１２において、ルーチン３００は、第１のユーザが認証されたか否かを示す指示を第２のモバイルデバイスから受信することを含む。指示は、テキストメッセージまたは他の通信媒体で第２のモバイルデバイスから受信されてもよい。指示は、認証の結果と、第２のユーザが金銭の授受を受け入れるか拒否するかに関する指示とを含むことができる。第１のユーザを認証することができないか、または第２のユーザが授受を拒否した場合、第１および第２のモバイルデバイスは、金銭を授受する動作を停止することができる。代替的に、第１のユーザが認証され、第２のユーザが授受を受け入れる場合、デバイスは、金銭を授受する動作の実施を続けることができる。ブロック３１４において、ルーチン３００は、金銭を授受するために第２のモバイルデバイスと情報を交換することを含む。

【００３６】

場合によっては、例えば、第１のモバイルデバイスと第２のモバイルデバイスとが互いにリモート、例えば、ローカライズされたＰ２Ｐ接続を形成することができない場合、モバイルデバイスは、銀行取引システムを介して金銭の授受を実施することができる。一例では、送金者および受取人は、同じ銀行および銀行取引システムの口座を有してもよい。それぞれのデバイス上の銀行取引アプリケーションはまた、銀行取引システムと直接通信

されてもよい。この例では、第２のモバイルデバイスは、第１のユーザが認証され、第２のユーザが授受を受け入れる場合、授受が受け入れられたことを示す指示を銀行取引システムに送信することができる。指示は、第２のモバイルデバイス上の銀行取引アプリケーションから銀行取引システムへ、ＡＰＩ通信を介して送信されてもよい。次いで、銀行取引システムは、送金者の口座から金銭を引き落とし、受取人の口座に金銭を追加することによって、トランザクションを電子的に実施することができる。場合によっては、第１のモバイルデバイスは、第１のユーザが認証され、第２のユーザが授受を承認するという指示を受信すると、金銭の授受を開始および引き起こすことができる。同様に、第１のモバイルデバイスは、授受を引き起こすために、第１のモバイル上の銀行取引アプリケーションを介して銀行取引システムと通信することができる。次いで、銀行取引システムは、上述のように授受を実施することができ、例えば、送金者の口座から金銭を電子的に引き落とし、受取人の口座に金銭を追加することができる。

【００３７】

実施形態では、第１および第２のユーザは、異なる銀行取引システムを有する異なる銀行を利用することができ、銀行取引システムは、互いに通信して金銭の授受を実施することができる。例えば、第１のユーザは、第１のユーザの銀行取引システムを識別する識別子を第２のモバイルデバイスに提供することができる。授受が承認されると、第２のモバイルデバイスは、第２のユーザに関連付けられた銀行取引システムに情報を送信することができる。次いで、第２のユーザの銀行取引システムは、授受を実施するために第１のユーザの銀行取引システムと通信することができる。他の例では、第２のモバイルデバイスは、第２のユーザの銀行取引システムを識別する情報を、第１のモバイルデバイスに送信することができ、第１のモバイルデバイスは、第１のユーザの銀行取引システムと通信することによって授受を開始することができる。

【００３８】

いくつかの実施形態では、銀行取引アプリケーションは、第三者銀行取引アプリケーション、例えば、銀行取引システムによって直接操作されないアプリケーションであってもよい。第三者銀行取引アプリケーションは、第三者銀行取引アプリケーションと共に動作する１つ以上の銀行口座を有することを含めて、各モバイルデバイスとすることができる。授受が承認されると、送金者および受取人のデバイスのそれぞれの第三者アプリケーションは、授受を実施するためにそれぞれの銀行と通信することができる。場合によっては、第三者システムを含む第三者アプリケーションは、送金者の銀行取引システムと通信して、送金者の口座から金銭を引き落とすことができる。第三者システムは、料金または利子を獲得するために一定期間にわたって金銭を保持し、次いで金銭を受取人の口座に送ることができる。実施形態はこのように限定されない。

【００３９】

実施形態では、第１および第２のモバイルデバイスは、安全なＰ２Ｐ接続を介してデータを通信して金銭を授受することができる。例えば、第１のユーザが認証され、第２のユーザが授受を承認したことに応じて、第２のモバイルデバイスは、第１のモバイルデバイスと通信して、Ｐ２Ｐ接続を確立することができる。接続は、ＢＬＥ、Ｂｌｕｅｔｏｏｔｈ、ＺｉｇＢｅｅ、Ｗｉ－Ｆｉなどの特定のＰ２Ｐプロトコルに従って確立することができる。接続が確立されると、第１および／または第２のモバイルデバイスは、メッセージを送信することによって金銭の授受を開始することができる。例えば、第２のモバイルデバイスは、第１のモバイルデバイスに金銭を授受するデータまたはトークンの要求を送信することができる。第１のモバイルデバイスは、授受する金額の指示を有するトークンまたは安全な情報を含み得るデータを、第２のモバイルデバイスに送信することができる。第２のモバイルデバイスは、第１のユーザおよび第２のユーザの銀行口座間の授受を実施するために銀行取引システムと通信することができる。場合によっては、データはまた、送金者の識別子、受取人の識別子、送金者の銀行口座情報などを含んでもよい。データは安全に送信され、暗号化することができる。

【００４０】

図４は、システム１００によって実施され得る例示的なルーチン４００を示す。具体的には、ルーチン４００は、別のモバイルデバイスから通信を受信するモバイルデバイスによって実施されてもよく、通信は、別のユーザが金銭を送ること（または要求すること）を希望していることを示す。

【００４１】

ブロック４０２において、ルーチン４００は、第１のユーザに関連付けられた第１のモバイルデバイスによって、ユーザが金銭を送りたい（または金銭を要求したい）ことを示すテキストを含むメッセージと、ユニフォームリソースロケータ（ＵＲＬ）を含むデータを受信することを含む。テキストは、メッセージの送金者および金額を識別することができる。実施形態では、メッセージは、ＳＭＳ、ＭＭＳ、ＲＣＳ、または別のプロトコルなどの通信プロトコルを介して、第２のユーザに関連付けられた第２のモバイルデバイスから受信することができる。

【００４２】

実施形態では、ＵＲＬは、受取人によってアクティブ化されると、第２のモバイルデバイスにアプリケーションを起動させ、第１のモバイルデバイスから受信したデータおよび非接触カードを使用して第２のユーザの認証を実施させるアクティブＵＲＬまたはディープリンクであってもよい。実施形態では、データはトークンまたは暗号化された文字列を含み、ＵＲＬに埋め込まれてもよい。データは、第２のユーザの認証を実施するためにアプリケーションによって使用され得るパラメータとして、起動時にアプリケーションに渡されてもよい。第１および第２のユーザの識別子および授受する金額などの他の情報もＵＲＬに埋め込むことができる。

【００４３】

ブロック４０４において、ルーチン４００は、第１のモバイルデバイスによって、ＵＲＬをアクティブ化する入力を検出することを含む。例えば、第１のモバイルデバイスは、タッチスクリーンインタフェースなどの入力デバイスを含むことができ、ユーザは、ＵＲＬを選択または「クリック」することができる。実施形態はこの例に限定されず、入力は、例えばボタン、マイクロフォン（音声命令）などの別の入力デバイスを介して提供されてもよい。

【００４４】

ブロック４０６において、ルーチン４００は、第１のモバイルデバイスによって、入力に応答してアプリケーションを起動することを含み、アプリケーションは、データを用いて第２のユーザの認証を実施するためにサーバと通信する。上述したように、ＵＲＬは、あるロケーションを指し示すことができる、またはアプリケーションを起動するためにオペレーティングシステムによって処理される命令を提供するディープリンクであってもよい。例えば、ＵＲＬは、起動する特定のアプリケーションを示したり、ウェブブラウザで起動するウェブサイトを指し示したりすることができる。場合によっては、ＵＲＬは、アプリケーションを起動する指示を含むか、またはランディングスポットまたはロケーションを指定することができる。したがって、アプリケーションまたはウェブブラウザは、金銭の授受の情報、例えば、送金者／要求者の名前、連絡先情報、金額などを表示するＧＵＩディスプレイを開くことができる。実施形態では、ＵＲＬは、トークンまたは暗号化された文字列などのデータ、送金者を識別する識別子、受取人を識別する識別子、およびアプリケーションが起動されたときにパラメータとしてアプリケーションに渡され得る金額の指示を含むことができる。

【００４５】

実施形態では、起動されたアプリケーションを含む第１のモバイルデバイスは、ＵＲＬがアクティブ化されたときに第２のユーザを認証する認証動作を開始することができる。具体的には、起動されたアプリケーションは、ユーザを認証するために、ＵＲＬに埋め込まれた情報、例えばトークンまたは暗号化された文字列を利用することができる。場合によっては、アプリケーションは、暗号化された文字列を復号し、復号された文字列を認証された文字列と比較することによって、ローカルに認証動作を実施してもよい。場合によ

っては、第１のモバイルデバイスは、安全な通信で銀行取引システムから認証された文字列を最初に取得してもよい。

【００４６】

図示の例では、アプリケーションを含む第２のモバイルデバイスは、認証動作を実施するために、暗号化された文字列を銀行取引システムまたは第三者システムのサーバに送信することができる。アプリケーションは、暗号化された文字列を含むデータを、ＡＰＩ通信を介してサーバに送信することができる。サーバは、第２のユーザに関連付けられた公開鍵に基づいて暗号化された文字列を復号し、復号された文字列を銀行取引システムに記憶された認証文字列と比較することができる。文字列が一致する場合、第２のユーザを認証することができ、逆もまた同様である。

【００４７】

ブロック４０８において、ルーチン４００は、第１のモバイルデバイスによって、第２のユーザがサーバによって認証されたか否かの指示を受信することを含む。指示は、ＡＰＩ通信に応答してアプリケーションに返されてもよい。場合によっては、ＧＵＩディスプレイは、第２のユーザを認証するために認証動作が実施されているという指示を表示し、認証動作の結果が決定されるとその結果を表示することができる。ユーザを認証することができない場合、金銭を授受する動作は中止することができる。ユーザが認証された場合、アプリケーションは、金銭の授受を進めたいことに対する確認を第１のユーザに要求することができる。

【００４８】

第２のユーザが認証され、第１のユーザがトランザクションを確認したことに応答して、ブロック４１０において、ルーチン４００は、第１のモバイルデバイスによって、金銭の授受を実施することを含む。図３で上述したように、第１のモバイルデバイスは、金銭の授受を実施するために１つ以上の銀行取引システムと通信することができる。他の例では、第１のモバイルデバイスは、認証が成功し、第１のユーザが授受を承認したという指示を第２のモバイルデバイス（送金者のデバイス）に送信することができる。第２のモバイルデバイスは、授受を実施するために１つ以上の銀行取引システムと通信することができる。さらに別の例では、第１および第２のモバイルデバイス間でＰ２Ｐ接続を確立することができ、デバイス間でデータを交換して、授受を実施することができる。

【００４９】

図５は、非接触カード５００の例示的な構成を示し、非接触カード５００は、非接触カード５００の前面または背面にサービスプロバイダ証印５０２として表示されるように、サービスプロバイダによって発行された、非接触カード、クレジットカード、デビットカード、またはギフトカードなどのペイメントカードを含むことができる。いくつかの例では、非接触カード５００は、ペイメントカードに関連せず、限定はしないが、身分証明書を含むことができる。いくつかの例では、トランザクションカードは、デュアルインタフェース非接触ペイメントカード、報酬カードなどを含むことができる。非接触カード５００は、プラスチック、金属、および他の材料で構成された単層または１つ以上の積層を含み得る基板５０８を含むことができる。例示的な基板材料としては、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、炭素、紙、および生分解性材料が挙げられる。いくつかの例では、非接触カード５００は、ＩＳＯ／ＩＥＣ７８１６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、そうでなければ、トランザクションカードは、ＩＳＯ／ＩＥＣ１４４４３規格に準拠してもよい。しかしながら、本開示に係る非接触カード５００は、異なる特性を有してもよく、本開示は、ペイメントカードにトランザクションカードを実装することを必要としないことが理解される。

【００５０】

非接触カード５００はまた、カードの前面および／または背面に表示される識別情報５０６と、接触パッド５０４とを含むことができる。接触パッド５０４は、１つ以上のパッドを含んでもよく、トランザクションカードを介してＡＴＭ、ユーザデバイス、スマート

フォン、ラップトップ、デスクトップ、またはタブレットコンピュータなどの別のクライアントデバイスとの接触を確立することができる。接触パッドは、ＩＳＯ／ＩＥＣ７８１６規格などの１つ以上の規格に従って設計され、ＥＭＶプロトコルに従って通信を可能にすることができる。非接触カード５００はまた、図６でさらに説明するように、処理回路、アンテナ、および他の構成要素を含むことができる。これらの構成要素は、接触パッド５０４の背後または基板５０８上の他の場所、例えば基板５０８の異なる層内に配置されてもよく、接触パッド５０４と電気的および物理的に結合されてもよい。非接触カード５００はまた、カードの背面に配置され得る磁気ストリップまたはテープを含んでもよい（図５には示されていない）。非接触カード５００はまた、ＮＦＣプロトコルを介して通信することができるアンテナに結合された近距離無線通信（ＮＦＣ）デバイスを含むことができる。実施形態はこのように限定されない。

【００５１】

図５に示すように、非接触カード５００の接触パッド５０４は、プロセッサ６０２、メモリ６０４、および１つ以上のインタフェース６０６を含む、情報を記憶、処理、および通信する処理回路６１６を含むことができる。処理回路６１６は、本明細書に記載の機能を実施するために必要に応じて、プロセッサ、メモリ、エラーおよびパリティ／ＣＲＣチェック部、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、および改ざん防止ハードウェアを含む追加の構成要素を含み得ることが理解される。

【００５２】

メモリ６０４は、リードオンリーメモリ、ライトワンスリードメニー（ｒｅａｄ－ｍｕｌｔｉｐｌｅ）メモリ、またはリード／ライトメモリ、例えばＲＡＭ、ＲＯＭ、およびＥＥＰＲＯＭであってもよく、非接触カード５００は、これらのメモリのうちの１つ以上を含んでもよい。リードオンリーメモリは、読み取り専用またはワンタイムプログラマブルとして工場で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、１回書き込んだ後に何度も読み取る機会を提供する。ライトワンス／リードメニー（ｒｅａｄ－ｍｕｌｔｉｐｌｅ）メモリは、メモリチップが工場を出荷された後の時点でプログラムすることができる。メモリがプログラムされると、メモリは書き換えることができないが、何度も読み取ることができる。リード／ライトメモリは、工場出荷後に何度もプログラムおよび再プログラムすることができる。リード／ライトメモリはまた、工場出荷後に何度も読み取ることができる。場合によっては、メモリ６０４は、暗号化データに対してプロセッサ６０２によって実行される暗号化アルゴリズムを利用する暗号化メモリであってもよい。

【００５３】

メモリ６０４は、１つ以上のアプレット６０８、１つ以上のカウンタ６１０、トークンまたは文字列などの顧客識別子６１４、および仮想口座番号であり得る口座番号６１２を記憶することができる。１つ以上のアプレット６０８は、Ｊａｖａ（登録商標）カードアプレットなどの１つ以上の非接触カード上で実行する１つ以上のソフトウェアアプリケーションを含むことができる。しかしながら、アプレット６０８は、Ｊａｖａカードアプレットに限定されず、代わりに、非接触カードまたは限られたメモリを有する他のデバイス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６１０は、整数を記憶するのに十分な数値カウンタを含むことができる。顧客識別子６１４は、非接触カード５００のユーザに割り当てられた一意の英数字識別子、トークン、または文字列を含むことができ、識別子は、非接触カードのユーザを他の非接触カードユーザから区別することができる。いくつかの例では、顧客識別子６１４は、顧客とその顧客に割り当てられた口座の両方を識別することができ、顧客の口座に関連付けられた非接触カード５００をさらに識別することができる。場合によっては、メモリ６０４は、顧客識別子６１４と、顧客を識別するために使用され得る１つ以上のトークンまたは追加の文字列とを含むことができる。上述したように、口座番号６１２は、非接触カード５００に関連付けられた数千の使い捨て仮想口座番号を含むことができる。非接

触カード５００のアプレット６０８は、口座番号６１２を管理する（例えば、口座番号６１２を選択し、選択された口座番号６１２を使用済みとしてマークし、自動入力サービスによる自動入力のために口座番号６１２をモバイルデバイスに送信する）ことができる。

【００５４】

前述の例示的な実施形態のプロセッサ６０２およびメモリ要素は、接触パッド５０４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５０４の外部に実装されてもよく、もしくは接触パッド５０４から完全に分離されてもよく、または接触パッド内に配置されたプロセッサ６０２およびメモリ６０４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。

【００５５】

いくつかの例では、非接触カード５００は、１つ以上のアンテナ６１８を備えることができる。１つ以上のアンテナ６１８は、非接触カード５００内で接触パッド５０４の処理回路６１６の周囲に載置されてもよい。例えば、１つ以上のアンテナ６１８は処理回路６１６と一体であってもよく、１つ以上のアンテナ６１８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つ以上のアンテナ６１８は、接触パッド５０４および処理回路６１６の外部にあってもよい。

【００５６】

一実施形態では、非接触カード５００のコイルは、空芯変圧器の二次として機能することができる。端末は、切断電力（ｃｕｔｔｉｎｇ　ｐｏｗｅｒ）または振幅変調によって非接触カード５００と通信することができる。非接触カード１０１は、非接触カードの電力接続のギャップを使用して端末から送信されたデータを推測することができ、これは、１つ以上のコンデンサを介して機能的に維持することができる。非接触カード５００は、非接触カードのコイルの負荷を切り替えること、または負荷変調によって、通信を返すことができる。負荷変調は、干渉によって端末のコイルで検出することができる。より一般的には、アンテナ６１８、プロセッサ６０２、および／またはメモリ６０４を使用して、非接触カード１０１は、ＮＦＣ、Ｂｌｕｅｔｏｏｔｈ、および／またはＷｉ－Ｆｉ通信を介して通信する通信インタフェースを提供する。

【００５７】

上述したように、非接触カード５００は、スマートカード、またはＪａｖａＣａｒｄなどの限られたメモリを有する他のデバイス上で動作可能なソフトウェアプラットフォーム上に構築することができ、１つ以上のアプリケーションまたはアプレットを安全に実行することができる。様々なモバイルアプリケーションベースのユースケースにおける多要素認証（ＭＦＡ）のワンタイムパスワード（ＯＴＰ）を提供するために、非接触カードにアプレット６０８を追加することができる。アプレット６０８は、モバイルＮＦＣリーダ（例えば、モバイルデバイスまたは販売時点情報管理端末（ｐｏｉｎｔ－ｏｆ－ｓａｌｅ　ｔｅｒｍｉｎａｌ））などのリーダからの近距離無線データ交換要求などの１つ以上の要求に応答し、ＮＤＥＦテキストタグとして符号化された暗号的に安全なＯＴＰを含むＮＤＥＦメッセージを生成することができる。

【００５８】

ＮＤＥＦ　ＯＴＰの一例は、ＮＤＥＦショートレコードレイアウト（ＳＲ＝１）である。そのような例では、１つ以上のアプレット６０８は、ＯＴＰをＮＤＥＦタイプ４の周知の種類のテキストタグとして符号化することができる。いくつかの例では、ＮＤＥＦメッセージは、１つ以上のレコードを含んでもよい。アプレット６０８は、ＯＴＰレコードに加えて、１つ以上の静的タグレコードを追加することができる。

【００５９】

いくつかの例では、１つ以上のアプレット６０８は、ＲＦＩＤタグをエミュレートすることができる。ＲＦＩＤタグは、１つ以上の多形タグを含むことができる。いくつかの例では、タグが読み取られるたびに、非接触カードの信頼性を示すことができる異なる暗号化データが提示される。１つ以上のアプレット６０８に基づいて、タグのＮＦＣ読み取りを処理することができ、データを銀行取引システムのサーバなどのサーバに送信すること

ができ、データをサーバで検証することができる。

【００６０】

いくつかの例では、非接触カード５００およびサーバは、カードが適切に識別され得るように特定のデータを含むことができる。非接触カード５００は、例えばトークンまたは文字列（図示せず）などの、１つ以上の一意の識別子を含むことができる。読み取り動作が行われるたびに、カウンタ６１０はインクリメントを行うことができる。いくつかの例では、非接触カード５００からのデータが（例えば、モバイルデバイスによって）読み取られるたびに、カウンタ６１０は、検証のためにサーバに送信され、カウンタ６１０がサーバのカウンタと等しいかどうかを（検証の一部として）決定する。

【００６１】

１つ以上のカウンタ６１０は、リプレイ攻撃を防止することができる。例えば、暗号文が取得されてリプレイされた場合、その暗号文は、カウンタ６１０が読み取られたか、使用されたか、そうでなければ渡された場合に直ちに拒否される。カウンタ６１０が使用されていない場合、リプレイすることができる。いくつかの例では、カード上でインクリメントが行われるカウンタは、トランザクションのためにインクリメントが行われるカウンタとは異なる。非接触カード１０１は、非接触カード５００上のアプレット６０８間に通信がないため、アプリケーショントランザクションカウンタ６１０を決定することができない。

【００６２】

いくつかの例では、カウンタ６１０は同期しなくてもよい。いくつかの例では、ある角度での読み取りなど、トランザクションを開始する偶発的な読み取りを考慮するために、カウンタ６１０はインクリメントが可能であるが、アプリケーションはカウンタ６１０を処理しない。いくつかの例では、モバイルデバイス１０がウェイクアップされるとＮＦＣが有効にされてもよく、デバイス１１０は利用可能なタグを読み取ってもよいが、読み取りに応答してアクションは実行されない。

【００６３】

カウンタ６１０を同期したままにするために、モバイルデバイス１１０がウェイクアップしたときを検出し、検出に起因して発生したリードを示す銀行取引システムのサーバと同期して、その後カウンタ６１０を加算方向（ｆｏｒｗａｒｄ）に動かし得る、バックグラウンドアプリケーションなどのアプリケーションを実行することができる。他の例では、誤同期のウィンドウが受け入れられ得るように、ハッシュ化ワンタイムパスワードが利用されてもよい。例えば、１０の閾値内である場合、カウンタ６１０は、加算方向に動き得る。しかし、異なる閾値内、例えば１０または１２００内の場合、再同期を実施する要求が処理されてもよく、これは、ユーザのデバイスを介してユーザがタップ、ジェスチャ、または他の方法で１回以上指示する１つ以上のアプリケーションを介して要求する。カウンタ６１０が適切なシーケンスで増加する場合、ユーザはそのことを知ることができる。

【００６４】

カウンタ６１０、マスタ鍵、および多様化された鍵を参照して本明細書で説明される鍵多様化技術は、鍵多様化技術の暗号化および／または復号の一例である。この例示的な鍵多様化技術は、本開示が他の種類の鍵多様化技術にも等しく適用可能であるため、本開示を限定するものとみなすべきではない。

【００６５】

非接触カード５００の作成プロセス中に、カードごとに２つの暗号鍵を一意に割り当てることができる。暗号鍵は、データの暗号化および復号の両方で使用され得る対称鍵を含むことができる。トリプルＤＥＳ（３ＤＥＳ）アルゴリズムは、ＥＭＶにより使用することができ、非接触カード５００内のハードウェアによって実装される。鍵多様化プロセスを使用することによって、鍵を必要とする各エンティティの一意に識別可能な情報に基づいて、マスタ鍵から１つ以上の鍵を導出することができる。

【００６６】

いくつかの例では、脆弱性の影響を受けやすい３ＤＥＳアルゴリズムの欠点を克服するために、セッション鍵（セッションごとの一意の鍵など）を導出することができるが、マスタ鍵を使用するのではなく、一意のカード導出鍵およびカウンタを多様化データとして使用することができる。例えば、非接触カード１０１が動作中に使用されるたびに、メッセージ認証コード（ＭＡＣ）の作成および暗号化の実施に異なる鍵が使用されてもよい。これにより、暗号の三重層が得られる。セッション鍵は、１つ以上のアプレットによって生成され、（ＥＭＶ ４．３ Ｂｏｏｋ ２ Ａ１．３．１ Ｃｏｍｍｏｎ Ｓｅｓｓｉｏｎ Ｋｅｙ Ｄｅｒｉｖａｔｉｏｎに定義されているように）１つ以上のアルゴリズムを有するアプリケーショントランザクションカウンタを使用することによって導出することができる。

【００６７】

さらに、各カードのインクリメントは一意であってもよく、パーソナライズによって割り当てられてもよく、または何らかの識別情報によってアルゴリズム的に割り当てられてもよい。例えば、奇数番号のカードは２ずつインクリメントを行ってもよく、偶数番号のカードは５ずつインクリメントを行ってもよい。いくつかの例において、インクリメントはまた、１つのカードが１、３、５、２、２、…を繰り返すことによって順にインクリメントが行われ得るように、一連のリードで変動してもよい。特定のシーケンスまたはアルゴリズムシーケンスは、パーソナライズ時に、または一意の識別子から導出された１つ以上のプロセスから定義することができる。これにより、リプレイ攻撃者が少数のカードインスタンスから一般化することをより困難にすることができる。

【００６８】

認証メッセージは、１６進ＡＳＣＩＩフォーマットのテキストＮＤＥＦレコードのコンテンツとして配信することができる。別の例では、ＮＤＥＦレコードは１６進形式で符号化されてもよい。

【００６９】

図７は、本開示の１つ以上の実施形態に係る、データの交換を提供する例示的なシーケンスを示すタイミング図である。シーケンスフロー７００は、非接触カード５００と、アプリケーション７０２およびプロセッサ７０４を含み得るモバイルデバイスとを含み得る。

【００７０】

ライン７０８において、アプリケーション７０２は、（例えば、非接触カード５００の近くに持ってきた後に）非接触カード５００と通信する。アプリケーション７０２と非接触カード５００との間の通信は、アプリケーション７０２と非接触カード５００との間のＮＦＣデータ転送を可能にするために、非接触カード５００がモバイルデバイスのカードリーダ（図示せず）に十分に近いことを伴うことができる。

【００７１】

ライン７０６において、モバイルデバイスと非接触カード５００との間に通信が確立された後、非接触カード５００は、メッセージ認証コード（ＭＡＣ）暗号文を生成する。いくつかの例では、これは、非接触カード５００がアプリケーション７０２によって読み取られるときに起こり得る。特に、これは、ＮＦＣデータ交換フォーマットに従って作成され得る近距離無線データ交換（ＮＤＥＦ）タグのＮＦＣ読み取りなどの読み取り時に行われ得る。例えば、アプリケーション７０２などのリーダアプリケーションは、ＮＤＥＦ生成アプレットのアプレットＩＤを用いて、アプレット選択メッセージなどのメッセージを送信することができる。選択を確認すると、一連の選択ファイルメッセージとそれに続く読み取りファイルメッセージを送信することができる。例えば、シーケンスは、「ケーパビリティファイルを選択する」、「ケーパビリティファイルを読み込む」、および「ＮＤＥＦファイルを選択する」を含むことができる。この時点で、非接触カード５００によって維持されるカウンタ値は、更新またはインクリメントを行ってもよく、その後に「ＮＤＥＦファイルを読み取る」が続くことができる。この時点で、ヘッダと、トークンまたは文字列などの共有秘密とを含み得るメッセージを生成することができる。その後、セッシ

ョン鍵を生成することができる。ＭＡＣ暗号文は、ヘッダおよび共有秘密を含み得るメッセージから作成することができる。ＭＡＣ暗号文はその後、ランダムデータの１つ以上のブロックと連結することができ、ＭＡＣ暗号文および乱数（ＲＮＤ）はセッション鍵で暗号化することができる。その後、暗号文とヘッダとを連結し、ＡＳＣＩＩ　ｈｅｘとして符号化し、（「ＮＤＥＦファイルを読み取る」メッセージに応答して）ＮＤＥＦメッセージフォーマットで返すことができる。

【００７２】

いくつかの例では、ＭＡＣ暗号文は、ＮＤＥＦタグとして送信されてもよく、他の例では、ＭＡＣ暗号文は、ユニフォームリソースインジケータ（例えば、フォーマットされた文字列として）と共に含まれてもよい。いくつかの例では、アプリケーション７０２は、非接触カード５００に要求を送信してもよく、要求は、ＭＡＣ暗号文を生成する命令を含む。

【００７３】

ライン７１０において、非接触カード５００は、ＭＡＣ暗号文をアプリケーション７０２に送信する。いくつかの例では、ＭＡＣ暗号文の送信はＮＦＣを介して行われるが、本開示はこれに限定されない。他の例では、この通信は、Ｂｌｕｅｔｏｏｔｈ、Ｗｉ－Ｆｉ、または他の無線データ通信手段を介して行われてもよい。ライン７１２において、アプリケーション７０２はＭＡＣ暗号文をプロセッサ７０４に送信する。

【００７４】

ライン７１４において、プロセッサ７０４は、アプリケーション１２２からの命令に従ってＭＡＣ暗号文を検証する。例えば、以下に説明するように、ＭＡＣ暗号文を検証することができる。いくつかの例では、ＭＡＣ暗号文の検証は、モバイルデバイスとデータ通信する銀行取引システムのサーバなど、モバイルデバイス以外のデバイスによって実施されてもよい。例えば、プロセッサ７０４は、ＭＡＣ暗号文を検証し得る銀行取引システムのサーバに送信するために、ＭＡＣ暗号文を出力することができる。いくつかの例では、ＭＡＣ暗号文は、検証のデジタル署名として機能することができる。この検証を実施するために、公開鍵非対称アルゴリズムなどの他のデジタル署名アルゴリズム、例えばデジタル署名アルゴリズムおよびＲＳＡアルゴリズム、またはゼロ知識プロトコルを使用することができる。

【００７５】

図８は、本開示の１つ以上の実施形態を実行システム８００の図を示す。以下に説明するように、非接触カード作成プロセス中に、２つの暗号鍵をカードごとに一意に割り当てることができる。暗号鍵は、データの暗号化および復号の両方で使用され得る対称鍵を含むことができる。トリプルＤＥＳ（３ＤＥＳ）アルゴリズムは、ＥＭＶにより使用することができ、非接触カード内のハードウェアによって実行される。鍵多様化プロセスを使用することにより、鍵を必要とする各エンティティの一意に識別可能な情報に基づいて、マスタ鍵から１つ以上の鍵を導出することができる。

【００７６】

マスタ鍵管理に関しては、１つ以上のアプレットが発行されるポートフォリオの部分ごとに２つの発行者マスタ鍵８０２、８２６が必要とされる場合がある。例えば、第１のマスタ鍵８０２は発行者暗号文生成／認証鍵（Ｉｓｓ－Ｋｅｙ－Ａｕｔｈ）を含んでもよく、第２のマスタ鍵８２６は発行者データ暗号鍵（Ｉｓｓ－Ｋｅｙ－ＤＥＫ）を含んでもよい。本明細書でさらに説明するように、２つの発行者マスタ鍵８０２、８２６は、カードごとに一意のカードマスタ鍵８０８、８２０に多様化される。いくつかの例では、バックオフィスデータとしてのネットワークプロファイルレコードＩＤ（ｐＮＰＲ）５２２および導出鍵インデックス（ｐＤＫＩ）８２４を使用して、認証の暗号化プロセスでどの発行者マスタ鍵８０２、８２６を使用するかを識別することができる。認証を実施するシステムは、認証時に非接触カードのｐＮＰＲ８２２およびｐＤＫＩ８２４の値を取得してもよい。

【００７７】

いくつかの例では、解決策のセキュリティを高めるために、セッション鍵（セッションごとの一意の鍵など）を導出することができるが、上述したように、マスタ鍵を使用するのではなく、一意のカード導出鍵およびカウンタを多様化データとして使用することができる。例えば、カードが動作中に使用されるたびに、メッセージ認証コード（ＭＡＣ）の作成および暗号化の実施に異なる鍵を使用することができる。セッション鍵生成に関して、暗号文を生成し、１つ以上のアプレット内のデータを暗号化するために使用される鍵は、カード固有鍵（Ｃａｒｄ－Ｋｅｙ－Ａｕｔｈ８０８およびＣａｒｄ－Ｋｅｙ－Ｄｅｋ８２０）に基づくセッション鍵を含むことができる。セッション鍵（Ａｕｔ－Ｓｅｓｓｉｏｎ－Ｋｅｙ８３２およびＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙ８１０）は、１つ以上のアプレットによって生成され、１つ以上のアルゴリズムでアプリケーショントランザクションカウンタ（ｐＡＴＣ）８０４を使用することによって導出することができる。データを１つ以上のアルゴリズムに適合させるために、４バイトのｐＡＴＣ８０４の２つの下位バイトのみが使用される。いくつかの例では、４バイトのセッション鍵導出方法は、Ｆ１：＝ＰＡＴＣ（下位２バイト）｜｜「Ｆ０」｜｜「００」｜｜ＰＡＴＣ（４バイト）Ｆ１：＝ＰＡＴＣ（下位２バイト）｜｜「０Ｆ」｜｜「００」｜｜ＰＡＴＣ（４バイト）ＳＫ：＝｛（ＡＬＧ（ＭＫ）［Ｆ１］）｜｜ＡＬＧ（ＭＫ）［Ｆ２］｝を含むことができ、ＡＬＧは３ＤＥＳ　ＥＣＢを含むことができ、ＭＫはカード固有の導出マスタ鍵を含むことができる。

【００７８】

本明細書で説明されるように、ｐＡＴＣ８０４カウンタの下位２バイトを使用して、１つ以上のＭＡＣセッション鍵を導出することができる。非接触カードの各タップにおいて、ｐＡＴＣ８０４は更新され、カードマスタ鍵Ｃａｒｄ－Ｋｅｙ－ＡＵＴＨ７０４およびＣａｒｄ－Ｋｅｙ－ＤＥＫ８２０は、セッション鍵Ａｕｔ－Ｓｅｓｓｉｏｎ－Ｋｅｙ８３２およびＤＥＫ－Ｓｅｓｓｉｏｎ－ＫＥＹ８１０にさらに多様化される。ｐＡＴＣ８０４は、パーソナライズまたはアプレット初期化時に０に初期化されてもよい。いくつかの例では、ｐＡＴＣカウンタ８０４は、パーソナライズ時またはパーソナライズ前に初期化されてもよく、各ＮＤＥＦ読み取り時に１ずつインクリメントしてもよい。

【００７９】

さらに、各カードの更新は、一意であってもよく、パーソナライズによって割り当てられてもよく、またはｐＵＩＤもしくは他の識別情報によってアルゴリズム的に割り当てられてもよい。例えば、奇数番号のカードは２ずつインクリメントまたはデクリメントが行われてもよく、偶数番号のカードは５ずつインクリメントまたはデクリメントが行われてもよい。いくつかの例において、更新はまた、１つのカードが１、３、５、２、２、…を繰り返すことによって順にインクリメントが行われ得るように、一連のリードで変動してもよい。特定のシーケンスまたはアルゴリズムシーケンスは、パーソナライズ時に、または一意の識別子から導出された１つ以上のプロセスから定義することができる。これにより、リプレイ攻撃者が少数のカードインスタンスから一般化することをより困難にすることができる。

【００８０】

認証メッセージは、１６進ＡＳＣＩＩフォーマットのテキストＮＤＥＦレコードのコンテンツとして配信することができる。いくつかの例では、認証データ、および認証データのＭＡＣが続く８バイトの乱数のみが含まれてもよい。いくつかの例では、乱数は暗号文Ａの前にあってもよく、１ブロック長であってもよい。他の例では、乱数の長さに制限はなくてもよい。さらなる例では、総データ（すなわち、乱数に暗号文を加えたもの）はブロックサイズの倍数であってもよい。これらの例では、ＭＡＣアルゴリズムによって生成されたブロックと一致するように追加の８バイトブロックを追加してもよい。別の例として、使用されるアルゴリズムが１６バイトのブロックを使用した場合、そのブロックサイズの偶数倍が使用されてもよく、または出力をそのブロックサイズの倍数に自動的にもしくは手動でパディングしてもよい。

【００８１】

ＭＡＣは、ファンクション鍵（ＡＵＴ－Ｓｅｓｓｉｏｎ－Ｋｅｙ）８３２によって実施されてもよい。暗号文で指定されたデータは、ｊａｖａｃａｒｄ．ｓｉｇｎａｔｕｒｅ方法：ＡＬＧ＿ＤＥＳ＿ＭＡＣ８＿ＩＳＯ９７９７＿１＿Ｍ２＿ＡＬＧ３で処理されて、ＥＭＶ　ＡＲＱＣ検証方法と相関させることができる。この計算に使用される鍵は、先に説明したように、セッション鍵ＡＵＴ－Ｓｅｓｓｉｏｎ－Ｋｅｙ８３２を含んでもよい。上述したように、カウンタの下位２バイトを使用して、１つ以上のＭＡＣセッション鍵を多様化することができる。以下に説明するように、ＡＵＴ－Ｓｅｓｓｉｏｎ－Ｋｅｙ８３２はＭＡＣデータ８０６に使用することができ、結果として得られるデータまたは暗号文Ａｎ８１４および乱数ＲＮＤはＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙ８１０を使用して暗号化して、メッセージで送信される暗号文Ｂまたは出力８１８を作成することができる。

【００８２】

いくつかの例では、最後の１６（バイナリ、３２ｈｅｘ）バイトが、ゼロＩＶの乱数とそれに続くＭＡＣ認証データとを伴うＣＢＣモードを用いる３ＤＥＳ対称暗号化を含み得るように、１つ以上のＨＳＭコマンドを復号のために処理することができる。この暗号化に使用される鍵は、Ｃａｒｄ－Ｋｅｙ－ＤＥＫ８２０から導出されたセッション鍵ＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙ８１０を含んでもよい。この場合、セッション鍵導出のためのＡＴＣ値は、カウンタｐＡＴＣ８０４の最下位バイトである。

【００８３】

以下のフォーマットは、バイナリバージョンの例示的な実施形態を表す。さらに、いくつかの例では、先頭バイトはＡＳＣＩＩ「Ａ」に設定することができる。

【表１】

メッセージフォーマット				
1	2	4	8	8
０ｘ４３（メッセージタイプ「Ａ」）	バージョン	ｐＡＴＣ	ＲＮＤ	暗号文Ａ（ＭＡＣ）
暗号文Ａ（ＭＡＣ）	８バイト			
何のＭＡＣか				
2	8	4	4	１８バイト入力データ
バージョン	ｐＵＩＤ	ｐＡＴＣ	共有秘密	

メッセージフォーマット				
1	2	4	１６	
０ｘ４３（メッセージタイプ「Ａ」）	バージョン	ｐＡＴＣ	暗号文Ｂ	
暗号文Ａ（ＭＡＣ）	８バイト			
何のＭＡＣか				
2	8	4	4	１８バイト入力データ
バージョン	ｐＵＩＤ	ｐＡＴＣ	共有秘密	
暗号文Ｂ	１６			
何のＳｙｍ暗号化か				
8	8			
ＲＮＤ	暗号文Ａ			

【００８４】

別の例示的なフォーマットを以下に示す。この例では、タグは１６進形式で符号化することができる。

【表２】

メッセージフォーマット				
2	8	4	8	8
バージョン	ｐＵＩＤ	ｐＡＴＣ	ＲＮＤ	暗号文Ａ（ＭＡＣ）
8バイト				
8	8	4	4	１８バイト入力データ
ｐＵＩＤ	ｐＵＩＤ	ｐＡＴＣ	共有秘密	

メッセージフォーマット				
2	8	4	１６	
バージョン	ｐＵＩＤ	ｐＡＴＣ	暗号文Ｂ	
8バイト				
8		4	4	１８バイト入力データ
ｐＵＩＤ	ｐＵＩＤ	ｐＡＴＣ	共有秘密	
暗号文Ｂ	１６			
何のＳｙｍ暗号化か				
8	8			
ＲＮＤ	暗号文Ａ			

【００８５】

受信したメッセージのＵＩＤフィールドを抽出して、マスタ鍵Ｉｓｓ－Ｋｅｙ－ＡＵＴＨ５００およびＩｓｓ－Ｋｅｙ－ＤＥＫ８２６から、その特定のカードのカードマスタ鍵（Ｃａｒｄ－Ｋｅｙ－Ａｕｔｈ８０８およびＣａｒｄ－Ｋｅｙ－ＤＥＫ８２０）を導出することができる。カードマスタ鍵（Ｃａｒｄ－Ｋｅｙ－Ａｕｔｈ７０４およびＣａｒｄ－Ｋｅｙ－ＤＥＫ８２０）を使用して、受信したメッセージのカウンタ（ｐＡＴＣ）フィールドを使用して、その特定のカードのセッション鍵（Ａｕｔ－Ｓｅｓｓｉｏｎ－Ｋｅｙ８３２およびＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙ８１０）を導出することができる。暗号文Ｂ８１８は、ＤＥＫ－Ｓｅｓｓｉｏｎ－ＫＥＹを使用して復号して、暗号文Ａｎ８１４およびＲＮＤを生成することができ、ＲＮＤは破棄されてもよい。ＵＩＤフィールドは非接触カードの共有秘密を検索するために使用することができ、共有秘密は、メッセージのＶｅｒ、ＵＩＤ、およびｐＡＴＣフィールドと共に、ＭＡＣ’などのＭＡＣ出力を作成するために再作成されたＡｕｔ－Ｓｅｓｓｉｏｎ－Ｋｅｙを使用して暗号化ＭＡＣを介して処理され得る。ＭＡＣ’が暗号文Ａｎ８１４と同じである場合、これはメッセージ復号およびＭＡＣチェックがすべて合格であることを示す。次いで、ｐＡＴＣを読み取って、それが有効であるかどうかを決定することができる。

【００８６】

認証セッション中に、１つ以上のアプリケーションによって１つ以上の暗号文を生成することができる。例えば、１つ以上の暗号文は、ＩＳＯ９７９７－１のアルゴリズム３を、方法２のパディングと共に使用して、Ａｕｔ－Ｓｅｓｓｉｏｎ－Ｋｅｙ８３２などの１

つ以上のセッション鍵を介して３ＤＥＳ　ＭＡＣとして生成することができる。入力データ８０６は、以下の形式をとることができる：バージョン（２）、ｐＵＩＤ（８）、ｐＡＴＣ（４）、共有秘密（４）。いくつかの例では、括弧内の数字はバイト単位の長さを含むことができる。いくつかの例では、共有秘密は、１つ以上の安全なプロセスを介して、乱数が予測不可能であることを保証し得る１つ以上の乱数生成器によって生成することができる。いくつかの例では、共有秘密は、パーソナライズ時間にカードに注入されるランダムな４バイトの２進数を含むことができ、これは認証サービスに知られている。認証セッション中、共有秘密は、１つ以上のアプレットからモバイルアプリケーションに提供されなくてもよい。方法２のパディングは、入力データの最後に必須の０ｘ’８０’バイトを追加することと、８バイト境界まで結果データの最後に追加され得る０ｘ’００’バイトを追加することとを含むことができる。結果として得られる暗号文は、長さが８バイトであってもよい。

【００８７】

いくつかの例では、共有されていない乱数をＭＡＣ暗号文を用いて第１のブロックとして暗号化する利点の１つは、対称暗号化アルゴリズムのＣＢＣ（ブロック連鎖）モードを使用しながら初期化ベクトルとして機能することである。これにより、固定ＩＶまたは動的ＩＶのいずれかを事前に確立する必要なしに、ブロック間の「スクランブル」が可能になる。

【００８８】

ＭＡＣ暗号文に含まれるデータの一部にアプリケーショントランザクションカウンタ（ｐＡＴＣ）を含めることによって、認証サービスは、クリアデータで搬送された値が改ざんされているかどうかを決定することができる。さらに、１つ以上の暗号文にバージョンを含めることにより、暗号ソリューションの強度を低下させようとして攻撃者がアプリケーションバージョンを意図的に偽ることが困難になる。いくつかの例では、ｐＡＴＣは０から開始し、１つ以上のアプリケーションが認証データを生成するたびに１ずつ更新され得る。認証サービスは、認証セッション中に使用されるｐＡＴＣを追跡することができる。いくつかの例では、認証データが認証サービスによって受信された以前の値以下のｐＡＴＣを使用する場合、これは古いメッセージをリプレイしようとするものと解釈され、認証は拒否することができる。いくつかの例では、ｐＡＴＣが受信した以前の値よりも大きい場合、これを評価して、それが許容可能な範囲または閾値内にあるかどうかを決定し、それが範囲または閾値を超えるかまたは範囲または閾値外にある場合、検証は失敗したかまたは信頼できないとみなすことができる。ＭＡＣ動作８１２において、データ８０６は、Ａｕｔ－Ｓｅｓｓｉｏｎ－Ｋｅｙ８３２を使用してＭＡＣを介して処理され、暗号化されたＭＡＣ出力（暗号文Ａ）８１４を生成する。

【００８９】

カードの鍵を露出させる総当たり攻撃に対する追加の保護を提供するために、ＭＡＣ暗号文８１４は暗号化されることが望ましい。いくつかの例では、暗号文（ｃｉｐｈｅｒｔｅｘｔ）に含まれるデータまたは暗号文Ａｎ８１４は、乱数（８）、暗号文（８）を含み得る。いくつかの例では、括弧内の数字はバイト単位の長さを含むことができる。いくつかの例では、乱数は、１つ以上の安全なプロセスを介して、乱数が予測不可能であることを保証し得る１つ以上の乱数生成器によって生成することができる。このデータを暗号化するために使用される鍵は、セッション鍵を含み得る。例えば、セッション鍵は、ＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙ８１０を含み得る。暗号化動作８１６では、ＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙ７０６を使用してデータまたは暗号文Ａｎ８１４およびＲＮＤが処理されて、暗号化データ、暗号文Ｂ８１８が生成される。データ８１４は、暗号ブロック連鎖モードで３ＤＥＳを使用して暗号化され、攻撃者がすべての暗号文に対して攻撃を実行しなければならないことを保証することができる。非限定的な例として、高度暗号化標準（ＡＥＳ）などの他のアルゴリズムが使用されてもよい。いくつかの例では、０ｘ’０００００００００００００００’の初期化ベクトルを使用することができる。正しく復号されたデータがそのランダムな見た目のために不正確に復号されたデータと区別できないので

、このデータを暗号化するために使用される鍵を総当たりしようとする攻撃者は、正しい鍵がいつ使用されたかを決定することができない。

【００９０】

認証サービスが１つ以上のアプレットによって提供される１つ以上の暗号文を検証するためには、認証セッション中に１つ以上のアプレットからモバイルデバイスに以下のデータをクリアで搬送しなければならない：使用される暗号手法を決定するバージョン番号、および将来的に手法を変更することを可能にする暗号文を検証するメッセージフォーマット、暗号資産を取得し、カード鍵を導出するｐＵＩＤ、ならびに暗号文に使用されるセッション鍵を導出するｐＡＴＣ。

【００９１】

図９は、暗号文を生成する方法９００を示す。例えば、ブロック９０２において、ネットワークプロファイルレコードＩＤ（ｐＮＰＲ）および導出鍵インデックス（ｐＤＫＩ）を使用して、認証のために暗号化プロセスにおいてどの発行者マスタ鍵を使用すべきか識別することができる。いくつかの例では、本方法は、認証時に非接触カードのｐＮＰＲおよびｐＤＫＩの値を取得するために認証を実施することを含むことができる。

【００９２】

ブロック９０４において、発行者マスタ鍵は、発行者マスタ鍵を、カードの一意のＩＤ番号（ｐＵＩＤ）、および１つ以上のアプレット、例えば決済アプレットのＰＡＮシーケンス番号（ＰＳＮ）と組み合わせることによって多様化することができる。

【００９３】

ブロック９０６において、発行者マスタ鍵を多様化することによって、Ｃａｒｄ－Ｋｅｙ－ＡｕｔｈおよびＣａｒｄ－Ｋｅｙ－ＤＥＫ（一意のカード鍵）を作成して、ＭＡＣ暗号文を生成するために使用され得るセッション鍵を生成することができる。

【００９４】

ブロック９０８において、暗号文を生成し、１つ以上のアプレット内のデータを暗号化するために使用される鍵は、カード固有鍵（Ｃａｒｄ－Ｋｅｙ－ＡｕｔｈおよびＣａｒｄ－Ｋｅｙ－ＤＥＫ）に基づくブロック１２３０のセッション鍵を含むことができる。いくつかの例では、これらのセッション鍵は、１つ以上のアプレットによって生成され、ｐＡＴＣを使用して導出され、セッション鍵Ａｕｔ－Ｓｅｓｓｉｏｎ－ＫｅｙおよびＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙをもたらすことができる。

【００９５】

図１０は、一例に係る鍵の多様化を示す例示的なプロセス１０００を示す。最初に、送金者および受取人は、２つの異なるマスタ鍵でプロビジョニングされ得る。例えば、第１のマスタ鍵はデータ暗号化マスタ鍵を含むことができ、第２のマスタ鍵はデータ完全性マスタ鍵を含むことができる。送金者は、ブロック１００２において更新され得るカウンタ値と、他のデータ、例えば、受取人と安全に共有することができる保護されるべきデータなどとを有する。

【００９６】

ブロック１００４において、データ暗号化マスタ鍵を使用して送金者によってカウンタ値を暗号化して、データ暗号化導出セッション鍵を生成することができ、そして、データ完全性マスタ鍵を使用して送金者によってカウンタ値を暗号化して、データ完全性導出セッション鍵を生成することもできる。いくつかの例では、両方の暗号化中にカウンタ値全体またはカウンタ値の一部を使用することができる。

【００９７】

いくつかの例では、カウンタ値は暗号化されなくてもよい。これらの例では、カウンタは、送金者と受取人との間でクリアで、すなわち暗号化なしで送信することができる。

【００９８】

ブロック１００６において、保護されるべきデータは、送金者によって、データ完全性セッション鍵および暗号化ＭＡＣアルゴリズムを使用して暗号化ＭＡＣ動作で処理される。平文および共有秘密を含む保護されたデータは、セッション鍵のうちの１つ（ＡＵＴ－

Ｓｅｓｓｉｏｎ－Ｋｅｙ）を使用してＭＡＣを生成するために使用することができる。

【００９９】

ブロック１００８において、保護されるべきデータは、対称暗号化アルゴリズムと共にデータ暗号化導出セッション鍵を使用して、送金者によって暗号化することができる。いくつかの例では、ＭＡＣは、例えば各８バイト長など、等しい量のランダムデータと組み合わされ、次いで、第２のセッション鍵（ＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙ）を使用して暗号化される。

【０１００】

ブロック１０１０において、暗号文を検証するために、追加の秘密情報（例えば、共有秘密、マスタ鍵など）を識別するのに十分な情報と共に、暗号化されたＭＡＣが送金者から受取人に送信される。

【０１０１】

ブロック１０１２において、受取人は、上記で説明したように、受信したカウンタ値を使用して、２つのマスタ鍵から２つの導出されたセッション鍵を独立して導出する。

【０１０２】

ブロック１０１４において、データ暗号化導出セッション鍵は、保護されたデータを復号する対称復号動作と併せて使用される。次いで、交換されたデータに対する追加の処理が行われる。いくつかの例では、ＭＡＣが抽出された後、ＭＡＣを再現して一致することが望ましい。例えば、暗号文を検証する際には、適宜生成されたセッション鍵を用いて復号してもよい。保護されたデータは、検証のために再構築することができる。適切に生成されたセッション鍵を使用してＭＡＣ動作を実施して、復号されたＭＡＣと一致するかどうかを決定することができる。ＭＡＣ動作は不可逆的なプロセスであるため、検証する唯一の方法はソースデータから再作成を試みることである。

【０１０３】

ブロック１０１６において、保護されたデータが変更されていないことを検証するために、データ完全性導出セッション鍵が暗号化ＭＡＣ動作と併せて使用される。

【０１０４】

本明細書に記載された方法のいくつかの例は、有利には、以下の条件が満たされたときに認証の成功が決定されるときを確認することができる。第１に、ＭＡＣを検証する能力は、導出されたセッション鍵が適切であったことを示す。復号が成功し、適切なＭＡＣ値が得られた場合にのみ、ＭＡＣは正しい場合がある。復号の成功は、正しく導出された暗号鍵が暗号化ＭＡＣを復号するために使用されたことを示すことができる。導出されたセッション鍵は、送金者（例えば、送信デバイス）および受取人（例えば、受信デバイス）にのみ知られているマスタ鍵を使用して作成されるので、ＭＡＣを最初に作成し、ＭＡＣを暗号化した非接触カードが実際に本物であると信頼することができる。さらに、第１のセッション鍵および第２のセッション鍵を導出するために使用されるカウンタ値は、有効であることが示されてもよく、認証動作を実施するために使用されてもよい。

【０１０５】

その後、導出された２つのセッション鍵は破棄されてもよく、データ交換の次の反復はカウンタ値を更新し（ブロック１００２に戻る）、セッション鍵の新しいセットが作成されてもよい（ブロック１０１０）。いくつかの例では、結合されたランダムデータは破棄されてもよい。

【０１０６】

図１１は、例示的な実施形態に係るカードアクティブ化の方法１０００を示す。例えば、カードアクティブ化は、カード、デバイス、および１つ以上のサーバを含むシステムによって完了することができる。非接触カード、デバイス、および１つ以上のサーバは、非接触カード５００、モバイルデバイス、およびサーバなど、以前に説明したものと同じまたは類似の構成要素を参照することができる。

【０１０７】

ブロックにおいて、カードは、データを動的に生成することができる。いくつかの例で

は、このデータは、カードからデバイスに送信され得る口座番号、カード識別子、カード検証値、または電話番号などの情報を含むことができる。いくつかの例では、データの１つ以上の部分は、本明細書に開示されるシステムおよび方法を介して暗号化されてもよい。

【０１０８】

ブロック１１０４において、動的に生成されたデータの１つ以上の部分は、ＮＦＣまたは他の無線通信を介してデバイスのアプリケーションに送信することができる。例えば、デバイスに近接するカードのタップは、デバイスのアプリケーションが非接触カードに関連付けられたデータの１つ以上の部分を読み取ることを可能にすることができる。いくつかの例では、デバイスがカードのアクティブ化を支援するアプリケーションを備えていない場合、カードのタップは、カードをアクティブ化する関連アプリケーションをダウンロードするようにデバイスを誘導するか、またはソフトウェアアプリケーションストアに顧客を促すことができる。いくつかの例では、ユーザは、カードがデバイスの表面に向かって十分なジェスチャ、載置、または配向となるように促されてもよく、例えば、デバイスの表面の上、近く、または近接に、斜めにまたは平坦に載置される。カードの十分なジェスチャ、載置、および／または配向に応答して、デバイスは、カードから受信したデータの１つ以上の暗号化された部分を１つ以上のサーバに送信することに進むことができる。

【０１０９】

ブロック１１０６において、データの１つ以上の部分は、カード発行者サーバなどの１つ以上のサーバに送信することができる。例えば、データの１つ以上の暗号化部分は、カードのアクティブ化のためにデバイスからカード発行者サーバに送信されてもよい。

【０１１０】

ブロック１１０８において、１つ以上のサーバは、本明細書に開示されたシステムおよび方法を介してデータの１つ以上の暗号化部分を復号することができる。例えば、１つ以上のサーバは、デバイスから暗号化されたデータを受信することができ、受信されたデータを１つ以上のサーバがアクセス可能なレコードデータと比較するためにそれを復号することができる。１つ以上のサーバによるデータの１つ以上の復号された部分の比較の結果が一致の成功をもたらす場合、カードをアクティブ化することができる。１つ以上のサーバによるデータの１つ以上の復号された部分の比較の結果が一致の不成功をもたらした場合、１つ以上のプロセスを行うことができる。例えば、一致の不成功の決定に応答して、ユーザに、カードを再度タップ、スワイプ、またはウェーブジェスチャするように促すことができる。この場合、ユーザがカードをアクティブ化することを許可される試行回数を含む所定の閾値が存在してもよい。代替的に、ユーザは、カード検証の試みの失敗を示し、カードをアクティブ化する支援に関する関連サービスに電話、Ｅメールもしくはテキスト送信を行いなさいという自分のデバイスへのメッセージなどの通知、またはカード検証の試みの失敗を示し、カードをアクティブ化する支援に関する関連サービスに電話、Ｅメールもしくはテキスト送信を行いなさいという自分のデバイスへの電話などの別の通知、またはカード検証の試みの失敗を示し、およびカードをアクティブ化する支援に関する関連サービスに電話、Ｅメールもしくはテキスト送信を行いなさいというＥメールなどの別の通知を受信することができる。

【０１１１】

ブロック１１１０において、１つ以上のサーバは、カードのアクティブ化の成功に基づいてリターンメッセージを送信することができる。例えば、デバイスは、１つ以上のサーバによるカードのアクティブ化の成功を示す出力を１つ以上のサーバから受信することができる。デバイスは、カードのアクティブ化の成功を示すメッセージを表示することができる。カードがアクティブ化すると、カードは、不正使用を回避するためにデータの動的生成を中止することができる。このようにして、カードはその後アクティブ化されなくてもよく、１つ以上のサーバは、カードが既にアクティブ化されていることを通知される。

【０１１２】

図１２は、前述のような様々な実施形態の実行に適した例示的なコンピュータアーキテ

クチャ１２００の実施形態を示す。一実施形態では、コンピュータアーキテクチャ１２００は、本明細書で説明する１つ以上のシステムまたはデバイスを含むか、またはその一部として実装することができる。

【０１１３】

本出願で使用される場合、「システム」および「構成要素」という用語は、ハードウェア、ハードウェアとソフトウェアとの組み合わせ、ソフトウェア、または実行中のソフトウェアのいずれかのコンピュータ関連エンティティを指すことを意図しており、その例は、例示的なコンピューティングコンピュータアーキテクチャ１２００によって提供される。例えば、構成要素は、プロセッサ上で動作するプロセス、プロセッサ、ハードディスクドライブ、（光および／または磁気記憶媒体の）複数の記憶ドライブ、オブジェクト、実行可能ファイル、実行スレッド、プログラム、および／またはコンピュータであり得るが、これらに限定されない。例として、サーバ上で起動するアプリケーションおよびサーバの両方が構成要素であってもよい。１つ以上の構成要素は、プロセスおよび／または実行スレッド内に存在してもよく、構成要素は、１つのコンピュータ上にローカライズすることができ、および／または２つ以上のコンピュータ間に分散されてもよい。さらに、構成要素は、動作を調整するために様々な種類の通信媒体によって互いに通信可能に結合されてもよい。調整は、情報の単方向または双方向の交換を含むことができる。例えば、構成要素は、通信媒体を介して通信される信号の形態で情報を送信することができる。情報は、様々な信号線に割り当てられた信号として実装することができる。このような割り当てでは、各メッセージは信号である。しかしながら、さらなる実施形態は、代替的にデータメッセージを使用してもよい。このようなデータメッセージは、様々な接続を介して送信することができる。例示的な接続には、パラレルインタフェース、シリアルインタフェース、およびバスインタフェースが含まれる。

【０１１４】

コンピューティングコンピュータアーキテクチャ１２００は、１つ以上のプロセッサ、マルチコアプロセッサ、コプロセッサ、メモリユニット、チップセット、コントローラ、周辺機器、インタフェース、発振器、タイミングデバイス、ビデオカード、オーディオカード、マルチメディア入力／出力（Ｉ／Ｏ）構成要素、電源などの様々な一般的なコンピューティング要素を含む。しかしながら、実施形態は、コンピューティングコンピュータアーキテクチャ１２００による実行に限定されない。

【０１１５】

図１２に示すように、コンピューティングコンピュータアーキテクチャ１２００は、プロセッサ１２１２と、システムメモリ１２０４と、システムバス１２０６とを含む。プロセッサ１２１２は、様々な市販のプロセッサのいずれかとすることができる。

【０１１６】

システムバス１２０６は、システムメモリ１２０４を含むがこれに限定されないシステム構成要素のインタフェースをプロセッサ１２１２に提供する。システムバス１２０６は、様々な市販のバスアーキテクチャのいずれかを使用して、（メモリコントローラの有無にかかわらず）メモリバス、周辺バス、およびローカルバスにさらに相互接続することができるいくつかの種類のバス構造のいずれかとすることができる。インタフェースアダプタは、スロットアーキテクチャを介してシステムバス１２０６に接続することができる。例示的なスロットアーキテクチャは、限定はしないが、アクセラレーテッドグラフィックスポート（ＡＧＰ）、カードバス、（拡張）業界標準アーキテクチャ（（Ｅ）ＩＳＡ）、マイクロチャネルアーキテクチャ（ＭＣＡ）、ＮｕＢｕｓ、周辺構成要素相互接続（拡張）（ＰＣＩ（Ｘ））、ＰＣＩ　Ｅｘｐｒｅｓｓ、パーソナルコンピューターメモリーカード国際協会（ＰＣＭＣＩＡ）などを含むことができる。

【０１１７】

コンピュータアーキテクチャ１２００は、様々な製品を含むかまたは実装することができる。製品は、論理を記憶するコンピュータ可読記憶媒体を含むことができる。コンピュータ可読記憶媒体の例は、揮発性メモリまたは不揮発性メモリ、取り外し可能または取り

外し不能メモリ、消去可能または消去不能メモリ、書き込み可能または書き換え可能メモリなどを含む、電子データを記憶することができる任意の有形媒体を含むことができる。論理の例は、ソースコード、コンパイル済みコード、解釈済みコード、実行可能コード、静的コード、動的コード、オブジェクト指向コード、視覚的コードなどの任意の適切な種類のコードを使用して実装された実行可能コンピュータプログラム命令を含むことができる。実施形態はまた、本明細書に記載の動作の実施を可能にするために１つ以上のプロセッサによって読み取られて実行され得る非一時的コンピュータ可読媒体に含まれる命令または非一時的コンピュータ可読媒体上の命令として少なくとも部分的に実装されてもよい。

【０１１８】

システムメモリ１２０４は、リードオンリーメモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、ダイナミックＲＡＭ（ＤＲＡＭ）、ダブルデータレートＤＲＡＭ（ＤＤＲＡＭ）、シンクロナスＤＲＡＭ（ＳＤＲＡＭ）、スタティックＲＡＭ（ＳＲＡＭ）、プログラマブルＲＯＭ（ＰＲＯＭ）、消去可能プログラマブルＲＯＭ（ＥＰＲＯＭ）、電気的消去可能プログラマブルＲＯＭ（ＥＥＰＲＯＭ）、フラッシュメモリ、強誘電体ポリマーメモリなどのポリマーメモリ、オボニックメモリ（ｏｖｏｎｉｃ　ｍｅｍｏｒｙ）、相変化または強誘電体メモリ、シリコン酸化物窒化物酸化物シリコン（ＳＯＮＯＳ）メモリ、磁気または光カード、独立ディスク冗長アレイ（ＲＡＩＤ）ドライブなどのデバイスのアレイ、ソリッドステートメモリデバイス（例えば、ＵＳＢメモリ）、ソリッドステートドライブ（ＳＳＤ）、および情報を記憶するのに適した任意の他の種類の記憶媒体など、１つ以上の高速メモリユニットの形態の様々な種類のコンピュータ可読記憶媒体を含むことができる。図１２に示す図示の実施形態では、システムメモリ１２０４は、不揮発性メモリ１２０８および／または揮発性メモリ１２１０を含むことができる。基本入力／出力システム（ＢＩＯＳ）は、不揮発性メモリ１２０８に記憶することができる。

【０１１９】

コンピュータ１２０２は、内部（または外部）ハードディスクドライブ１２３０、リムーバブル磁気ディスク１２２０から読み書きする磁気ディスクドライブ１２１６、およびリムーバブル光ディスク１２３２（例えば、ＣＤ－ＲＯＭまたはＤＶＤ）から読み書きする光ディスクドライブ1を含む、１つ以上の低速メモリユニットの形態の様々な種類のコンピュータ可読記憶媒体を含むことができる。ハードディスクドライブ１２３０、磁気ディスクドライブ１２１６および光ディスクドライブ１２２８は、それぞれＨＤＤインタフェース１２１４、ＦＤＤインタフェース１２１８および光ディスクドライブインタフェース１２３４によってシステムバス１２０６に接続することができる。外部ドライブ実装のＨＤＤインタフェース１２１４は、ユニバーサルシリアルバス（ＵＳＢ）およびＩＥＥＥ１３９４インタフェース技術の少なくとも一方または両方を含むことができる。

【０１２０】

ドライブおよび関連するコンピュータ可読媒体は、データ、データ構造、コンピュータ実行可能命令などの揮発性および／または不揮発性ストレージを提供する。例えば、オペレーティングシステム１２２２、１つ以上のアプリケーション１２４２、他のプログラムモジュール１２２４、およびプログラムデータ１２２６を含む、いくつかのプログラムモジュールをドライブおよび不揮発性メモリ１２０８、ならびに揮発性メモリ１２１０に記憶することができる。一実施形態では、１つ以上のアプリケーション１２４２、他のプログラムモジュール１２２４、およびプログラムデータ１２２６は、例えば、本明細書で説明するシステムの様々なアプリケーションおよび／または構成要素を含むことができる。

【０１２１】

ユーザは、例えばキーボード１２５０およびマウス１２５２などのポインティングデバイスなどの、１つ以上の有線／無線入力デバイスを介してコンピュータ１２０２にコマンドおよび情報を入力することができる。他の入力デバイスは、マイクロフォン、赤外線（ＩＲ）リモコン、無線周波数（ＲＦ）リモコン、ゲームパッド、スタイラスペン、カードリーダ、ドングル、指紋リーダ、手袋、グラフィックタブレット、ジョイスティック、キ

ーボード、網膜リーダ、タッチスクリーン（例えば、容量性、抵抗性など）、トラックボール、トラックパッド、センサ、スタイラスなどを含むことができる。これらおよび他の入力デバイスは、システムバス１２０６に結合された入力デバイスインタフェース１２３６を介してプロセッサ１２１２に接続されることが多いが、パラレルポート、ＩＥＥＥ１３９４シリアルポート、ゲームポート、ＵＳＢポート、ＩＲインタフェースなどの他のインタフェースによって接続されてもよい。

【０１２２】

モニタ１２４４または他の種類のディスプレイデバイスも、ビデオアダプタ１２４６などのインタフェースを介してシステムバス１２０６に接続される。モニタ１２４４は、コンピュータ１２０２の内部または外部にあってもよい。モニタ１２４４に加えて、コンピュータは通常、スピーカ、プリンタなどの他の周辺出力デバイスを含む。

【０１２３】

コンピュータ１２０２は、リモートコンピュータ１２４８などの１つ以上のリモートコンピュータへの有線および／または無線通信を介した論理接続を使用してネットワーク環境で動作することができる。リモートコンピュータ１２４８は、ワークステーション、サーバコンピュータ、ルータ、パーソナルコンピュータ、ポータブルコンピュータ、マイクロプロセッサベースのエンターテイメント機器、ピアデバイス、または他の共通ネットワークノードとすることができ、典型的には、コンピュータ１２０２に関して説明した多くのまたはすべての要素を含むが、簡潔にするために、メモリおよび／または記憶デバイス１２５８のみが示されている。図示の論理接続は、ローカルエリアネットワーク１２５６および／またはより大きなネットワーク、例えばワイドエリアネットワーク１２５４への有線／無線接続を含む。そのようなＬＡＮおよびＷＡＮネットワーキング環境は、オフィスおよび企業において一般的であり、イントラネットなどの企業規模のコンピュータネットワークを容易にし、そのすべてが、例えばインターネットなどのグローバル通信ネットワークに接続することができる。

【０１２４】

ローカルエリアネットワーク１２５６のネットワーク環境で使用される場合、コンピュータ１２０２は、有線および／または無線通信ネットワークインタフェースまたはネットワークアダプタ１２３８を介してローカルエリアネットワーク１２５６に接続される。ネットワークアダプタ１２３８は、ローカルエリアネットワーク１２５６への有線および／または無線通信を容易にすることができ、ローカルエリアネットワークはまた、ネットワークアダプタ１２３８の無線機能と通信するためにその上に配置された無線アクセスポイントを含むことができる。

【０１２５】

ワイドエリアネットワーク１２５４のネットワーク環境で使用される場合、コンピュータ１２０２は、モデム１２４０を含むことができるか、またはワイドエリアネットワーク１２５４上の通信サーバに接続されるか、またはインターネットなどを介してワイドエリアネットワーク１２５４上で通信を確立する他の手段を有する。モデム１２４０は、内部または外部の有線および／または無線デバイスとすることができ、入力デバイスインタフェース１２３６を介してシステムバス１２０６に接続する。ネットワーク化された環境では、コンピュータ１２０２またはその一部に関して示されたプログラムモジュールは、リモートメモリおよび／または記憶デバイス１２５８に記憶することができる。図示のネットワーク接続は例示的なものであり、コンピュータ間の通信リンクを確立する他の手段を使用できることが理解されよう。

【０１２６】

コンピュータ１２０２は、無線通信で動作可能に配置された無線デバイス（例えば、ＩＥＥＥ８０２．１１無線変調技術）などのＩＥＥＥ８０２ファミリの規格を使用して、有線および無線デバイスまたはエンティティと通信するように動作可能である。これには、とりわけ、少なくともＷｉ－Ｆｉ（すなわちワイヤレスフィディリティ）、ＷｉＭａｘ、およびＢｌｕｅｔｏｏｔｈ（商標）無線技術が含まれる。したがって、通信は、従来のネ

ットワークと同様に事前定義された構造、または単に少なくとも２つのデバイス間のアドホック通信とすることができる。Ｗｉ－Ｆｉネットワークは、ＩＥＥＥ８０２．１１（ａ、ｂ、ｇ、ｎなど）と呼ばれる無線技術を使用して、安全で信頼性が高く高速な無線接続を提供する。Ｗｉ－Ｆｉネットワークを使用して、コンピュータを互いに、インターネットに、および（ＩＥＥＥ８０２．３関連の媒体および機能を使用する）有線ネットワークに接続することができる。

【０１２７】

本明細書で前述したようなデバイスの様々な要素は、様々なハードウェア要素、ソフトウェア要素、または両方の組み合わせを含むことができる。ハードウェア要素の例は、デバイス、論理デバイス、構成要素、プロセッサ、マイクロプロセッサ、回路、プロセッサ、回路要素（例えば、トランジスタ、抵抗器、コンデンサ、インダクタなど）、集積回路、特定用途向け集積回路（ＡＳＩＣ）、プログラマブル論理デバイス（ＰＬＤ）、デジタル信号プロセッサ（ＤＳＰ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、メモリユニット、論理ゲート、レジスタ、半導体デバイス、チップ、マイクロチップ、チップセットなどを含むことができる。ソフトウェア要素の例は、ソフトウェア構成要素、プログラム、アプリケーション、コンピュータプログラム、アプリケーションプログラム、システムプログラム、ソフトウェア開発プログラム、機械プログラム、オペレーティングシステムソフトウェア、ミドルウェア、ファームウェア、ソフトウェアモジュール、ルーチン、サブルーチン、関数、方法、プロシージャ、ソフトウェアインタフェース、アプリケーションプログラムインタフェース（ＡＰＩ）、命令セット、コンピューティングコード、コンピュータコード、コードセグメント、コンピュータコードセグメント、ワード、値、シンボル、またはそれらの任意の組み合わせを含むことができる。しかしながら、実施形態がハードウェア要素および／またはソフトウェア要素を使用して実行されるか否かの決定は、所与の実装に望まれる所望の計算速度、電力レベル、耐熱性、処理サイクルバジェット、入力データ速度、出力データ速度、メモリリソース、データバス速度、および他の設計または性能制約などの任意の数の要因に従って変化する場合がある。

【０１２８】

上述したデバイスの構成要素および特徴は、ディスクリート回路、特定用途向け集積回路（ＡＳＩＣ）、論理ゲートおよび／または単一チップアーキテクチャの任意の組み合わせを使用して実装されてもよい。さらに、デバイスの特徴は、適切な場合には、マイクロコントローラ、プログラマブル論理アレイおよび／もしくはマイクロプロセッサ、または前述の任意の組み合わせを使用して実装されてもよい。ハードウェア、ファームウェア、および／またはソフトウェア要素は、本明細書では集合的または個別に「論理」または「回路」と呼ばれる場合があることに留意されたい。

【０１２９】

図１３は、前述のような様々な実施形態の実行に適した例示的な通信アーキテクチャ１３００を示すブロック図である。通信アーキテクチャ１３００は、送信機、受信機、トランシーバ、無線機、ネットワークインタフェース、ベースバンドプロセッサ、アンテナ、増幅器、フィルタ、電源などの様々な一般的な通信要素を含む。しかしながら、実施形態は、本明細書で説明されるシステムおよびデバイスと一致し得る通信アーキテクチャ１３００による実装に限定されない。

【０１３０】

図１３に示すように、通信アーキテクチャ１３００は、１つ以上のクライアント１３０２およびサーバ１３０４を含む。サーバ１３０４は、本明細書で説明する１つ以上の機能および実施形態を実行することができる。クライアント１３０２およびサーバ１３０４は、クッキーおよび／または関連するコンテキスト情報などの、それぞれのクライアント１３０２およびサーバ１３０４に対してローカルな情報を記憶するために使用され得る、１つ以上のそれぞれのクライアントデータストア１３０６およびサーバデータストア１３０８に動作可能に接続される。

【０１３１】

クライアント１３０２およびサーバ１３０４は、通信フレームワーク１３１０を使用して互いに情報を送信することができる。通信フレームワーク１３１０は、任意の周知の通信技術およびプロトコルを実装することができる。通信フレームワーク１３１０は、パケット交換ネットワーク（例えば、インターネットなどのパブリックネットワーク、企業イントラネットなどのプライベートネットワークなど）、回線交換ネットワーク（例えば、公衆交換電話網）、またはパケット交換ネットワークと回線交換ネットワークとの組み合わせ（適切なゲートウェイおよび変換器を有する）として実装することができる。

【０１３２】

通信フレームワーク１３１０は、通信ネットワークを受け入れ、通信し、接続する様々なネットワークインタフェースを実装することができる。ネットワークインタフェースは、入力／出力（Ｉ／Ｏ）インタフェースの特殊な形態とみなすことができる。ネットワークインタフェースは、限定はしないが、直接接続、イーサネット（例えば、Ｔｈｉｃｋ、Ｔｈｉｎ、ツイストペア１０／１００／１２００Ｂａｓｅ　Ｔなど）、トークンリング、無線ネットワークインタフェース、セルラーネットワークインタフェース、ＩＥＥＥ８０２．１１ａ－ｘネットワークインタフェース、ＩＥＥＥ８０２．１６ネットワークインタフェース、ＩＥＥＥ８０２．２０ネットワークインタフェースなどを含む接続プロトコルを使用することができる。さらに、複数のネットワークインタフェースを使用して、様々な通信ネットワークタイプに関与することができる。例えば、ブロードキャスト、マルチキャスト、およびユニキャストネットワークを介した通信を可能にするために、複数のネットワークインタフェースを使用することができる。処理要件がより大きな量の速度および容量を要求する場合、分散型ネットワークコントローラアーキテクチャを同様に使用して、負荷をプールして分散し、他の方法でクライアント１３０２およびサーバ１３０４によって必要とされる通信帯域幅を増加させることができる。通信ネットワークは、直接相互接続、安全なカスタム接続、プライベートネットワーク（例えば、企業イントラネット）、パブリックネットワーク（例えば、インターネット）、パーソナルエリアネットワーク（ＰＡＮ）、ローカルエリアネットワーク（ＬＡＮ）、メトロポリタンエリアネットワーク（ＭＡＮ）、インターネット上のノードとしてのオペレーティングミッション（Ｏｐｅｒａｔｉｎｇ　Ｍｉｓｓｉｏｎｓ　ａｓ　Ｎｏｄｅｓ　ｏｎ　ｔｈｅ　Ｉｎｔｅｒｎｅｔ）（ＯＭＮＩ）、ワイドエリアネットワーク（ＷＡＮ）、無線ネットワーク、セルラーネットワーク、および他の通信ネットワークを含むがこれらに限定されない有線および／または無線ネットワークの任意の１つおよび組み合わせであってもよい。

【図面】

【図１】

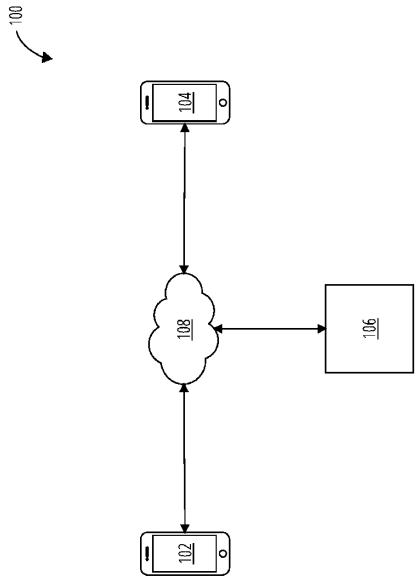
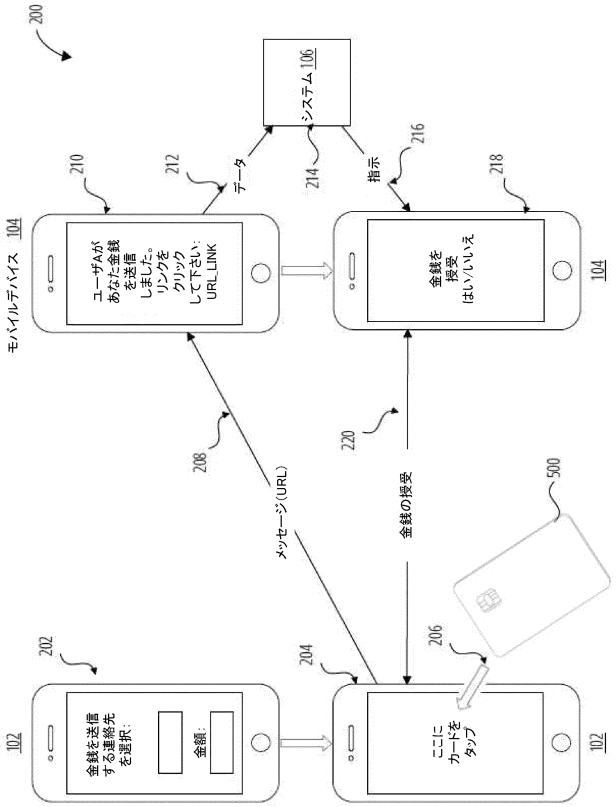
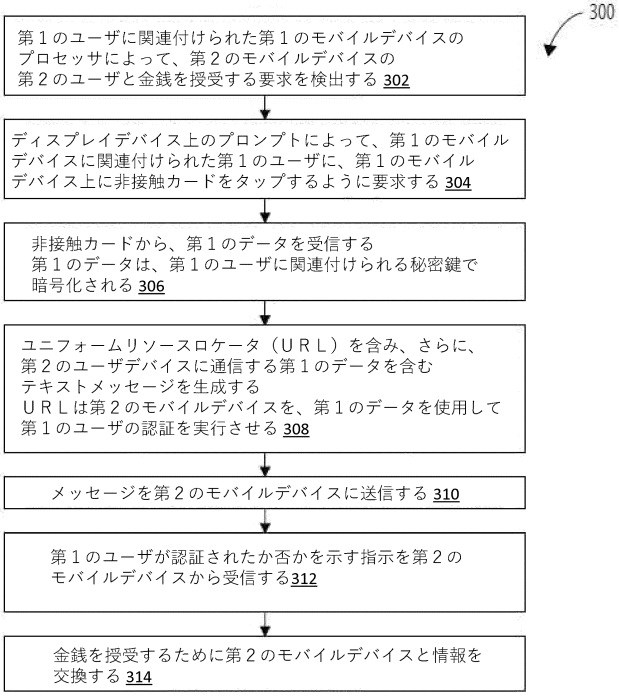


FIG. 1

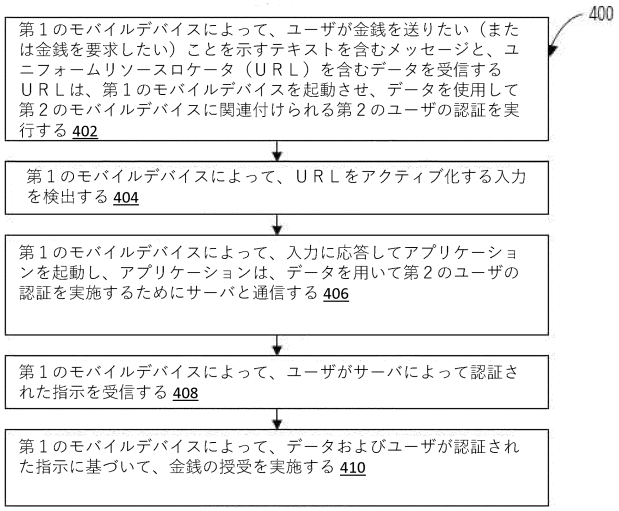
【図２】



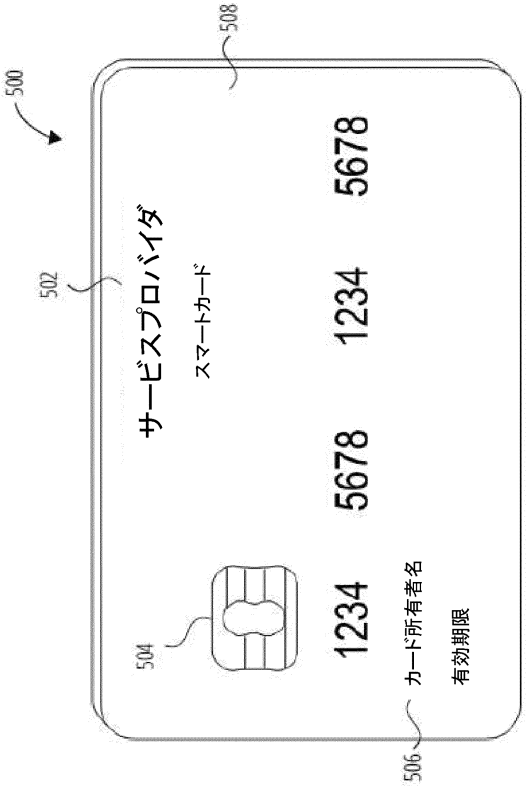
【図３】



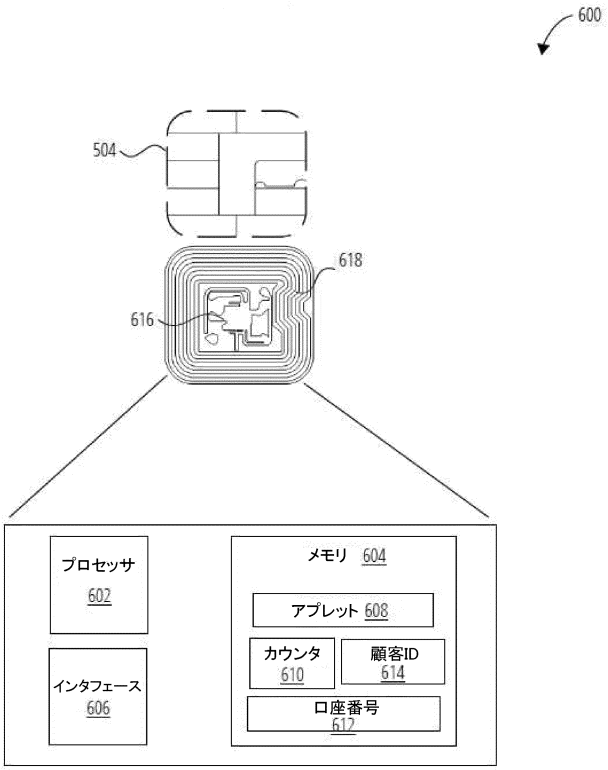
【図４】



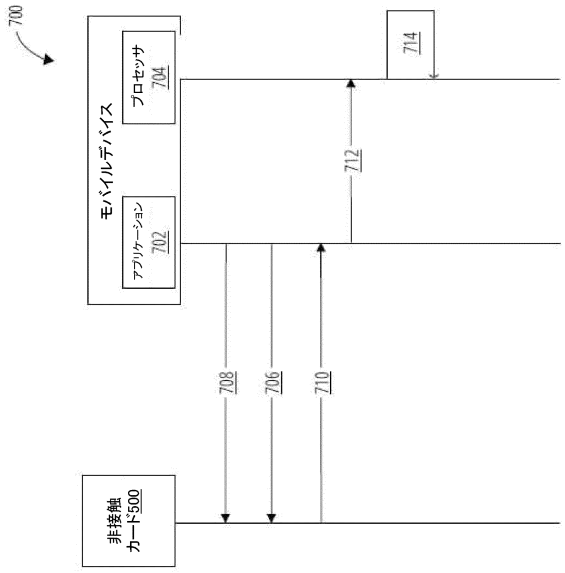
【図５】


500
502
504
506
508
サービスプロバイダ
スマートカード
5678
1234
5678
1234
カード所有者名
有効期限

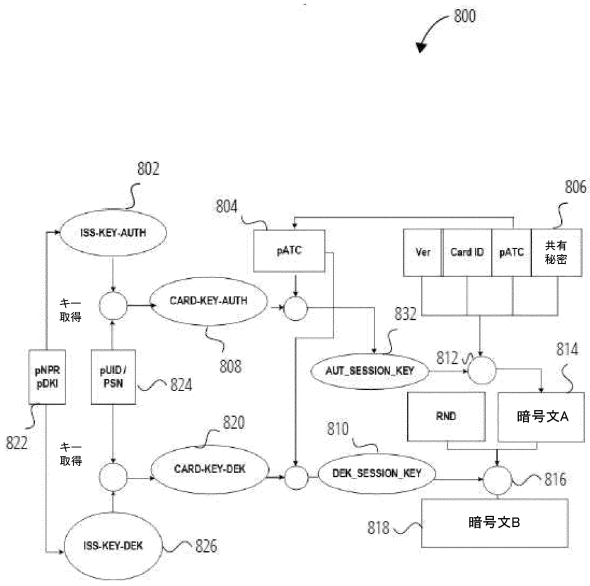
【図６】


600
504
616
618
プロセッサ
602
メモリ 604
アプレット 608
カウンタ
610
顧客ID
614
インタフェース
606
口座番号
617

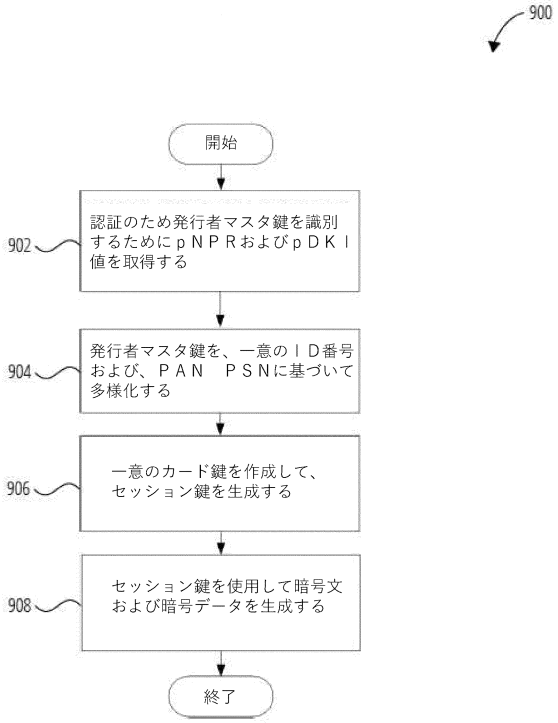
【図７】


700
モバイルデバイス
プロセッサ
704
アプリケーション
702
714
712
708
706
710
非接触
カード500

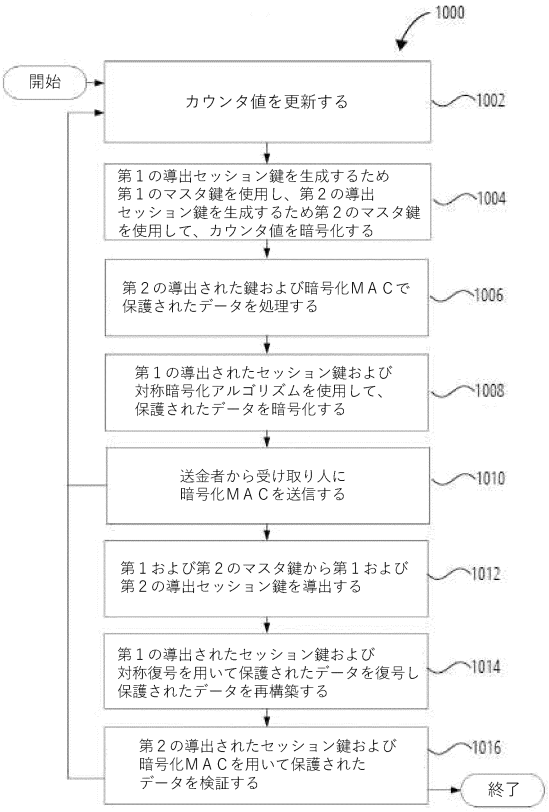
【図８】


800
802
ISS-KEY-AUTH
804
pATC
806
Ver
Card ID
pATC
共有秘密
キー取得
CARD-KEY-AUTH
808
832
AUT_SESSION_KEY
812
814
RND
暗号文A
pNPR
pDKI
pUID/
PSN
824
822
820
キー取得
CARD-KEY-DEK
810
DEK_SESSION_KEY
816
818
暗号文B
ISS-KEY-DEK
826

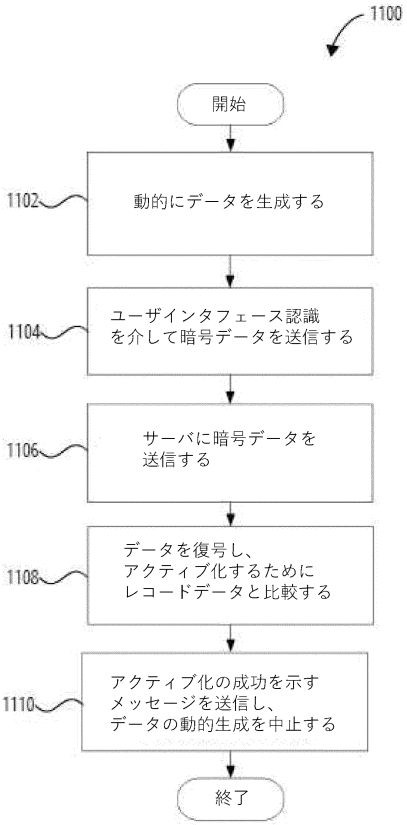
【図９】



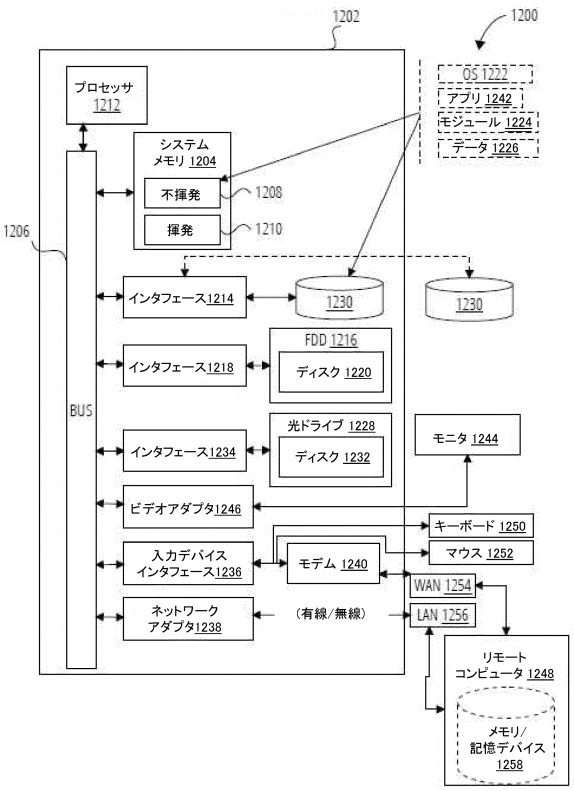
【図１０】



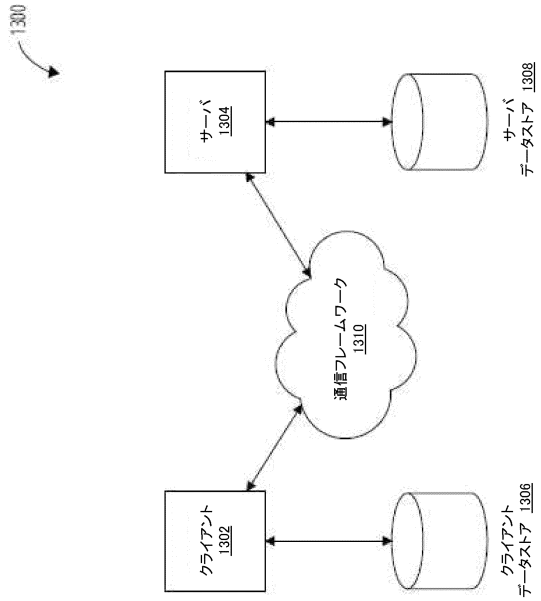
【図１１】



【図１２】



【図１３】


1300
サーバ
1304
サーバ
データストア
1308
通信フレームワーク
1310
クライアント
1302
クライアント
データストア
1306

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/021272

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/34 G06Q20/32 G06F16/955 G06F21/35 G06Q20/10
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)
G06Q G07G G06F

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 2020/106615 A1 (RULE JEFFREY [US] ET AL) 2 April 2020 (2020-04-02) paragraph [0030] - paragraph [0196]	1-20
X	EP 3 582 166 A1 (THALES DIS FRANCE SA [FR]) 18 December 2019 (2019-12-18) paragraph [0030] - paragraph [0129]	1-20
X	US 2020/250659 A1 (RULE JEFFREY [US] ET AL) 6 August 2020 (2020-08-06) paragraph [0012] - paragraph [0070]; figures 2B, 2C, 2D	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 June 2022	11/07/2022

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Pomocka, Marek

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2022/021272

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2020106615 A1	02-04-2020	CA 3115084 A1	09-04-2020
		US 2020106615 A1	02-04-2020
		US 2021203507 A1	01-07-2021
		WO 2020072440 A1	09-04-2020
EP 3582166 A1	18-12-2019	EP 3582166 A1	18-12-2019
		EP 3807831 A1	21-04-2021
		US 2021272098 A1	02-09-2021
		WO 2019238688 A1	19-12-2019
US 2020250659 A1	06-08-2020	AU 2020215026 A1	20-05-2021
		CA 3118911 A1	06-08-2020
		CN 113302954 A	24-08-2021
		EP 3918820 A1	08-12-2021
		JP 2022524269 A	02-05-2022
		KR 20210120978 A	07-10-2021
		SG 11202104525X A	28-05-2021
		US 10467622 B1	05-11-2019
		US 2020250659 A1	06-08-2020
		WO 2020160065 A1	06-08-2020

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,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．ＺＩＧＢＥＥ

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、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・カンパニー内

(72)発明者　バージェロン，ジョージ

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、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・カンパニー内

(72)発明者　ニューマン，ケイトリン

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、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・カンパニー内

(72)発明者　ハート，コリン

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、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・カンパニー内