(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2024-537678
(P2024-537678A)
(43)公表日　令和6年10月16日(2024.10.16)

(51)国際特許分類			FI			テーマコード（参考）
Ｇ０６Ｆ	*21/35*	*(2013.01)*	Ｇ０６Ｆ	21/35		２Ｅ２５０
Ｅ０５Ｂ	*49/00*	*(2006.01)*	Ｅ０５Ｂ	49/00	Ｋ	

審査請求　未請求　予備審査請求　未請求　（全22頁）

(21)出願番号　特願2024-516980(P2024-516980)
(86)(22)出願日　令和4年9月16日(2022.9.16)
(85)翻訳文提出日　令和6年5月14日(2024.5.14)
(86)国際出願番号　PCT/US2022/043780
(87)国際公開番号　WO2023/043987
(87)国際公開日　令和5年3月23日(2023.3.23)
(31)優先権主張番号　17/477,244
(32)優先日　令和3年9月16日(2021.9.16)
(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　100161883
弁理士　北出 英敏
(72)発明者　メイマン，タイラー
最終頁に続く

(54)【発明の名称】　ロックを解除するための決済カードの使用

(57)【要約】
例示的な実施形態は、決済カード上で、ユーザルーム、セキュリティで保護された場所、従業員の場所のドア、トランク、クローゼット、またはその他のロックされた場所またはアイテムなどの場所へのアクセスのロックを解除するための鍵を提供できる。決済カードの例は、クレジットカード、デビットカード、スマートカード、従業員識別カードなどを含むが、これらに限定されない。デジタルキーとして機能するセキュアなトークンは、決済カードにアップロードされ得る。そして、決済カードは、ロックのワイヤレスリーダの近くに配置され得る。ワイヤレスリーダは、セキュアなトークンを取得し、その内容を抽出する。内容が正しければロックが解除される。それ以外の場合、ロックはロックされたままになる。

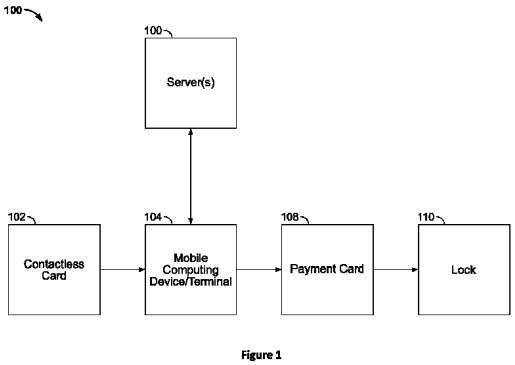


Figure 1

【特許請求の範囲】
【請求項１】
無線通信プロトコルを介して非接触カードから発信された識別情報及び資格情報を受信することと、
前記識別情報及び前記資格情報に基づいて、当事者の身元を確認することと、
前記身元を確認した後、決済カードについてのコードを送信することと、
を含み、前記コードは、ロックを解除するためのデジタルキーとして機能する、
方法。
【請求項２】
前記決済カードは、前記無線通信プロトコルの機能を有するスマートカード又はクレジットカードのいずれかである、請求項１に記載の方法。
【請求項３】
前記無線通信プロトコルは、近距離無線通信（ＮＦＣ）である、請求項１に記載の方法。
【請求項４】
前記ロックは、ホテルの部屋用である、請求項１に記載の方法。
【請求項５】
前記コードについての部屋番号を格納することと、前記決済カードに前記当事者の前記身元を格納することと、をさらに含む、請求項４に記載の方法。
【請求項６】
コンピューティングデバイスから前記コードを受信することをさらに含む、請求項１に記載の方法。
【請求項７】
前記識別情報及び前記資格情報は、暗号化されたパッケージで受信される、請求項１に記載の方法。
【請求項８】
無線通信プロトコルを介して非接触カードから携帯可能コンピューティングデバイスで当事者についての資格情報及び識別情報を受信することと、
前記資格情報及び前記識別情報を認証機関に送信することと、
前記当事者の前記身元の確認を受信することと、
前記当事者の前記身元を確認した後、前記無線通信プロトコルを介して決済カードにコードを送信することと、
を含み、前記コードは、ロックを解除するためのデジタルキーとして機能する、
方法。
【請求項９】
前記携帯可能コンピューティングデバイスは、スマートフォン、タブレットコンピューティングデバイス、スマートウォッチ又はウェアラブルデバイスのいずれかである、請求項８に記載の方法。
【請求項１０】
前記無線通信プロトコルは、近距離無線通信（ＮＦＣ）プロトコルである、請求項８に記載の方法。
【請求項１１】
前記ロックは、ホテルの部屋用である、請求項８に記載の方法。
【請求項１２】
前記識別情報及び資格情報は、暗号化されたパッケージで受信される、請求項８に記載の方法。
【請求項１３】
送信すること及び確認を受信することは、ネットワーク接続を介して行われる、請求項８に記載の方法。
【請求項１４】

前記ネットワーク接続は、無線ネットワーク接続、携帯ネットワーク接続または優先ネットワーク接続のいずれかである、請求項１３に記載の方法。
【請求項１５】
スマートカードであって、
メモリであって、
ユーザに関する識別情報と、
前記スマートカードでロックを解除するためのキーコードと、
前記キーコードで前記ロックを解除するためのコンピュータプログラム命令と、
無線決済を実行するためのコンピュータプログラム命令と、
を格納するメモリと、
前記メモリに格納された、前記ロックを解除するためのコンピュータプログラム命令及び無線決済を実行するためのコンピュータプログラム命令を実行するプロセッサと、
前記スマートカードが無線通信できるようにするハードウェアと、
を備える、スマートカード。
【請求項１６】
前記ハードウェアは、近距離無線通信（ＮＦＣ）無線通信が可能である、請求項１５に記載のスマートカード。
【請求項１７】
前記ロックは、ドアのロックである、請求項１５に記載のスマートカード。
【請求項１８】
前記ロックは、ホテルの部屋のロックである、請求項１７に記載のスマートカード。
【請求項１９】
前記メモリは、前記キーコードをデバイスからダウンロードするためのコンピュータプログラム命令をさらに格納する、請求項１５に記載のスマートカード。
【請求項２０】
前記デバイスは、スマートフォンである、請求項１９に記載のスマートカード。
【発明の詳細な説明】
【背景技術】
【０００１】
（関連出願への相互参照）
この出願は、２０２１年９月１６日に出願された「ロックを解除するための決済カードの使用（USE OF A PAYMENT CARD TO UNLOCK A LOCK）」という発明の名称の米国特許出願第１７／４７７，２４４号に対する優先権を主張する。前述の出願の内容は、その開示全体を本件明細書に援用される。
【０００２】
ホテルなどの宿泊施設では、客に客室にアクセスするための鍵を提供する。鍵は通常、磁気ストライプ付きのプラスチックカードキー、又は無線周波数識別（ＲＦＩＤ）タグ付きのプラスチックカードキーのいずれかである。磁気ストライプ付きのプラスチックカードキーの場合、ホテルの係員は、チェックイン時に、客にプラスチックカードキーを渡す前に、客に関する情報をカードの磁気ストライプにエンコードする。例えば、客の識別子、有効日時、有効期限日時、部屋番号が磁気ストライプにエンコードされ得る。客がプラスチックカードキーを使用するとき、磁気ストライプを有するプラスチックカードキーの端を、客室のドアに組み込まれた磁気カードリーダに通す。磁気カードリーダは磁気ストライプから情報を読み取り、その情報は錠によって分析される。情報がドアのロックを解除するための正しい情報である場合、ドアのロックが解除され、客は部屋に入ることができる。情報がドアのロック解除に適切でない場合、アクセスは拒否され、ドアはロックされたままになる。
【０００３】
ＲＦＩＤチップを備えるプラスチックカードキーの動作は多少異なる。ホテルの係員は、チェックイン時に、客にプラスチックカードキーを渡す前に、客の情報をプラスチック

カードキーのＲＦＩＤチップにエンコードする。客がプラスチックカードキーを使用するとき、客はプラスチックカードキーを客室のドアに組み込まれたＲＦＩＤリーダに当てる。ＲＦＩＤリーダは、プラスチックカードキー内のＲＦＩＤチップから情報をワイヤレスで読み取る。情報がドアのロックを解除するための正しい情報である場合、ドアのロックが解除され、客は部屋に入ることができる。情報がドアのロック解除に適切でない場合、アクセスは拒否され、ドアはロックされたままになる。

【０００４】

このようなプラスチックカードキーは、他の目的にも使用できる。例えば、雇用主は従業員に、雇用主の敷地内への入場やセキュアなエリアへの入場を許可するために、このようなプラスチックカードキーを渡すことがある。例えば、企業内のセキュアな研究室では、カードキーによるアクセスが求められる場合がある。プラスチックカードキーは、ロックが必要とみなされる他の場所にアクセスするために使用され得る。このようなプラスチックカードキーは、トランク、金庫などのロックされる物品にも使用され得る。

【０００５】

これらの種類のプラスチックカードキーの使用には欠点がある。例えば、これらの種類のプラスチックカードキーは特にセキュアではない。磁気ストライプまたはＲＦＩＤタグ上の情報は、磁気カードリーダまたはＲＦＩＤリーダを持つ当事者が容易にアクセスできる。さらに、このようなプラスチックカードキーは置き忘れやすい。その結果、プラスチックカードキーが悪意のある人の手に渡ったり、新しいカードを入手するまでユーザがロックされた場所や物品にアクセスできなくなったりする可能性がある。さらに、ユーザが追加のカードを管理しなければならないのは不便である。最後に、宿泊施設のオーナーにとって、プラスチックカードキーを購入するのは、紛失や破損が多いことを考えると、コストがかかる。

【発明の概要】

【０００６】

本発明の一態様によれば、方法は、無線通信プロトコルを介して非接触カードから発信された識別情報および資格情報を受信することを含む。識別情報及び資格情報に基づいて、当事者の身元が確認される。身元の確認後、決済カードのコードが送信される。コードは、ロックを解除するためのデジタルキーとして機能する。

【０００７】

決済カードは、無線通信プロトコルの機能を備えたスマートカード又はクレジットカードであってもよい。無線通信プロトコルは、近距離無線通信（ＮＦＣ）プロトコルであってもよい。ロックはホテルの部屋用であってもよい。方法は、決済カード上にコードについての部屋番号を格納し、当事者の身元を決済カードに格納することを含んでもよい。方法はまた、コンピューティングデバイスからコードを受信することを含んでもよい。識別情報及び資格情報は、暗号化されたパッケージで受信されてもよい。

【０００８】

本発明の別の態様によれば、方法は、無線通信プロトコルを介して非接触カードから携帯可能コンピューティングデバイスで当事者についての資格情報及び識別情報を受信することを含む。資格情報及び識別情報は認証機関に送信される。当事者の身元の確認が受信される。当事者の身元が確認されると、無線通信プロトコルを介してコードが決済カードに送信される。コードはロックを解除するためのデジタルキーとして機能する。

【０００９】

携帯可能コンピューティングデバイスは、スマートフォン、タブレットコンピューティングデバイス、スマートウォッチ、又はウェアラブルデバイスであってもよい。無線通信プロトコルは、近距離無線通信（ＮＦＣ）プロトコルであってもよい。鍵はホテルの部屋用であってもよい。識別情報及び資格情報は暗号化されたパッケージで受信されてもよい。送信すること及び確認を受信することは、ネットワーク接続を介して行われてもよい。ネットワーク接続は、無線ネットワーク接続、携帯ネットワーク接続、又は有線ネットワーク接続のいずれかであってもよい。

【００１０】
さらなる発明の態様によれば、スマートカードは、ユーザに関する識別情報と、スマートカードでロックを解除するためのキーコードと、キーコードでロックを解除するためのコンピュータプログラム命令、無線決済を実行するためのコンピュータプログラム命令と、を格納するメモリを含む。スマートカードはまた、メモリに格納された、ロックを解除するためのコンピュータプログラム命令及び無線決済を実行するためのコンピュータプログラム命令を実行するプロセッサを含む。スマートカードはさらに、スマートカードが無線通信できるようにするハードウェアを含む。
【００１１】
ハードウェアは、近距離無線通信（ＮＦＣ）無線通信が可能であってもよい。ロックはドアのロックであってもよい。ロックはホテルの部屋のロックであってもよい。メモリは、デバイスからキーコードをダウンロードするためのコンピュータプログラム命令をさらに格納してもよい。デバイスはスマートフォンであってもよい。
【図面の簡単な説明】
【００１２】
【図１】図１は、例示的な実施形態の例示的な環境を示す。
【図２】図２は、デジタルキーを決済カードに送信するために実行され得る例示的なステップのフローチャートを示す。
【図３】図３は、このような例示的な実施形態において実行され得る例示的なステップのフローチャートを示す。
【図４】図４は、例示的な実施形態に適し得る例示的なコンピューティング環境を示す。
【図５】図５は、このような対話を実行する際のさまざまな構成要素のアクティビティを示す。
【図６Ａ】図６Ａは、例示的な実施形態に適した例示的な非接触カードの前面を示す。
【図６Ｂ】図６Ｂは、図６Ａの非接触カードの構成要素を示す。
【図７】図７は、非接触カードとコンピューティングデバイスとの間の対話を示す構成要素の図を示す。
【図８Ａ】図８Ａは、例示的な実施形態において暗号化ハッシュ関数がどのように使用されるかを示すブロック図を示す。
【図８Ｂ】図８Ｂは、例示的な実施形態においてハッシュ化され得る入力の想定されるタイプの図を示す。
【図９】図９は、例示的な実施形態に従ったセキュアパッケージの暗号化を示すブロック図を示す。
【図１０】図１０は、例示的な実施形態において客の身元を認証する際に実行され得る例示的なステップのフローチャートを示す。
【図１１】図１１は、例示的な実施形態において認証サービスの一部として格納される特定の項目を示す。
【図１２】図１２は、例示的な実施形態において開始側当事者を認証するために実行されるステップのフローチャートを示す。
【図１３】図１３は、例示的な実施形態に適した決済カードのブロック図を示す。
【図１４】図１４は、例示的な実施形態において決済カードを使用して支払いを行うために実行され得る例示的なステップのフローチャートを示す。
【発明を実施するための形態】
【００１３】
例示的な実施形態は、ユーザの決済カードに場所または物品へのアクセスのロックを解除するための鍵を提供できる。決済カードの例は、限定されないが、クレジットカード、デビットカード、スマートカード、支払い機能付き従業員識別カードなどを含む。デジタルキーとして機能するセキュアなトークンは、ユーザの決済カードにアップロードされ得る。例えば、鍵が宿泊施設の部屋用である場合、客はウェブサイトにログインするか宿泊施設のアプリケーションにアクセスし、個人情報と決済情報を提供してチェックインでき

る。いくつかの場合、客は、デジタルキーとして機能するセキュアなトークンを使用して決済カードをエンコードするセルフサービス端末にアクセスできる。他の例では、ユーザは、スマートフォン、タブレット、スマートウォッチ又はウェアラブルデバイスなどのモバイルコンピューティングデバイスの機能を活用して、アプリケーションまたはＷｅｂサイトを使用してセキュアなトークンをダウンロードし、そのセキュアなトークンを決済カードに送信できる。その後、決済カードは、錠のワイヤレスリーダの近くに配置され得る。ワイヤレスリーダはセキュアなトークンを取得し、その内容を抽出する。ロックを解除するための内容が正しければ、錠は解除される。それ以外の場合、錠はロックされたままになる。

【００１４】

例示的な実施形態において使用するのに適した無線通信プロトコルは、近距離無線通信（ＮＦＣ）プロトコル又はその他の無線通信プロトコルである。したがって、モバイルコンピューティングデバイス又は端末及び決済カードはＮＦＣ対応であってもよい。セルフサービス端末が使用される場合、端末はＮＦＣを介してセキュアなトークンを決済カードに送信できる。同様に、モバイルコンピューティングデバイスは、ＮＦＣを介してセキュアなトークンを決済カードに送信できる。決済カードは同様に、ＮＦＣを介してセキュアなトークンを錠のワイヤレスリーダに送信できる。

【００１５】

例示的な実施形態には、ロックされた場所または物品にアクセスするために追加のプラスチックカードを必要としないという利点がある。これにより、ユーザは追加のプラスチックカードを管理する必要がなくなる。同様に、多くのユーザが自身の決済カードに鍵をエンコードすることを選択するため、プラスチックカードキーの発行者はそれほど多くのプラスチックカードキーを購入する必要がなくなり、費用が削減されるという利点もある。例示的な実施形態で使用される決済カード上のデジタルキーは、ユーザが決済カードに注意を払う傾向があるため、ユーザによって紛失される可能性が低くなり、一方、ユーザは、新しいプラスチックカードキーを簡単に入手できるため、従来のプラスチックカードキーにはあまり注意を払わない。例示的な実施形態で使用される鍵は、デジタルキーとして機能する各セキュアなトークンが暗号化されており、セキュアパッケージを復号するために必要な復号鍵がなければアクセスできないという点でセキュアである。

【００１６】

図１は、例示的な実施形態についての例示的な環境１００の一例を示す。例示的な環境１００は、非接触カード１０２を含む。非接触カード１０２はＮＦＣプロトコルをサポートし、ＮＦＣプロトコルを介して他のデバイスと通信できる。例えば、非接触カード１０２は、モバイルコンピューティングデバイスまたは端末１０４に十分に近い（例えば、１．５インチ以内）場合、モバイルコンピューティングデバイスまたは端末１０４と無線通信できる。例示的な非接触カード１０２の詳細は以下に示す。モバイルコンピューティングデバイス１０４は、例えば、スマートフォン、タブレットコンピューティングデバイス、スマートウォッチ、ウェアラブルコンピューティングデバイス、またはモバイルであり、本明細書で記載する必要な機能を備えたその他のコンピューティングデバイスであってもよい。端末１０４は、サーバ１０６とインターフェースされたＮＦＣ対応端末またはコンピュータシステムであってもよい。モバイルコンピューティングデバイス／端末１０４は、無線、有線、またはそれらの組み合わせのネットワーク接続を介してサーバ１０６と通信できる。サーバ１０６は、Ｗｅｂサーバであってもよく、クラウド上に配置されてもよく、またはローカルエリアネットワーク（ＬＡＮ）、インターネットなどのワイドエリアネットワーク（ＷＡＮ）、またはそれらの組み合わせを介してアクセス可能であってもよい。

【００１７】

モバイルコンピューティングデバイス／端末１０４は、ユーザの決済カード１０８と通信できる。例えば、前述のように、モバイルコンピューティングデバイス／端末１０４は、デジタルキーとして機能するセキュアパッケージを決済カード１０８に提供できる。決

済カード１０８は、以下に記載するように、錠１１０と対話してドアのロックを解除できる。

【００１８】

決済カードのデジタルキーの用途の１つは、モーテル、ホテル、旅館、レンタル物件などの宿泊施設のドアのロックを解除することである。宿泊部屋またはレンタル物件のロックを解除するためにユーザが決済カード上のデジタルキーを使用する場合に、決済カード１０８にデジタルキーを取得するために、例示的な実施形態で使用できるアプローチが少なくとも２つある。第１のアプローチでは、モバイルコンピューティングデバイス１０４がデジタルキーを決済カード１０８に送信する。図２は、デジタルキーを決済カード１０８に送信するために実行され得る例示的なステップのフローチャートを示す。まず、ユーザは、モバイルコンピューティングデバイス１０４を使用して、宿泊施設のアプリケーション（ホテルチェーンやレンタル代理店のアプリケーションなど）にアクセスするか、宿泊施設のＷｅｂサイトにアクセスしてチェックインする（２０２）。ウェブサイトはサーバ１０６上で実行されてもよく、又はアプリケーションはサーバ１０６と通信してもよい。ユーザは、チェックインするために、名前、住所、電話番号などの識別情報と、クレジットカード番号、デビットカード番号などの支払い情報の提供が求められ得る。いくつかの場合、以下に記載するように、ユーザは、身元（identity）を認証するために、非接触カード１０２をモバイルコンピューティングデバイス１０４にタップするように要求され得る。客が正常にチェックインすると、ユーザは、決済カード１０８に保存するためのデジタルキーを生成するオプションを求められ得る（２０４参照）。ユーザが決済カード１０８に保存するためのデジタルキーを生成するオプションを選択した場合、モバイルコンピューティングデバイス１０４は、デジタルキーとして機能するセキュアなトークンを決済カード１０８に送信する（２０６参照）。以下に記載するように、セキュアなトークンは、サーバ１０６からモバイルコンピューティングデバイス１０８にダウンロードされ、その後、決済カード１０８に送信されてもよい。

【００１９】

宿泊施設における使用についての別の方法としては、宿泊施設のフロントデスク又はキオスクのセルフサービス端末から鍵をダウンロードする方法がある。図３は、このような例示的な実施形態において実行され得る例示的なステップのフローチャート３００を示す。まず、ユーザは、上記のように、Ｗｅｂサイト又はアプリケーションを使用するか、従業員又はキオスクに必要な個人情報と支払い情報を提供することでチェックインする（３０２参照）。チェックインの一部として、ユーザは自身の身元を求められ得る（３０４参照）。これには、適切な身分証明書の提示、キオスクを介した個人情報の提供、又は非接触カード１０２を使用した身元の確認が含まれてもよい。ユーザの身元が確認されると、デジタルキーとして機能するセキュアなトークンは、端末１０４を介して決済カード１０８にアップロードされる（３０６参照）。端末１０４は、例えば、宿泊施設の受付に設置される。いくつかの例示的な実施形態では、端末１０４はＮＦＣ対応であり、ＮＦＣを使用して、同様にＮＦＣ対応であるユーザの決済カード１０８にセキュアなトークンを送信する。

【００２０】

図４は、例示的な実施形態に適し得る、図１よりも詳細に例示したコンピューティング環境４００を示す。客４１８は、モバイルコンピューティングデバイス／端末４０２にアクセスできる。モバイルコンピューティングデバイス／端末４０２は、中央処理装置（ＣＰＵ）、グラフィックス処理装置（ＧＰＵ）、特定用途向け集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、またはその他の処理装置などのプロセッサ４０８を含む。プロセッサ４０８は、アプリケーション４１４などのコンピュータプログラムにあるような命令を実行して、本明細書で記載する機能を実行できる。モバイルコンピューティングデバイス／端末４０２は、ランダムアクセスメモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）、ソリッドステートメモリ、光ディスクストレージ、磁気ディスクストレージ、またはデータ及び命令を格納するためのその他のさまざまなメモリ又は

ストレージを含むストレージ４１０を含み得る。ストレージ４１０は、プロセッサ実行可能命令を保持する非一時的なコンピュータ可読記憶媒体を含み得る。ストレージ４１０はアプリケーション４１４を格納し得る。アプリケーション４１４は、本明細書で記載するように、チェックインし、セキュアなトークンを決済カード１０８に送信する機能を提供できる。アプリケーション４１４は、非接触カード１０２を使用してユーザ４１８の身元を認証できるようにすることもできる。アプリケーション４１４は、いくつかの例示的な実施形態では、ウェブブラウザであってもよい。

【００２１】

モバイルコンピューティングデバイス／端末４０２は、ＮＦＣ機能４１６を提供するための集積回路（ＩＣ）を含んでもよい。ＮＦＣ　ＩＣ　４１６は、ＮＦＣ通信に参加するためのＮＦＣ送受信機とループアンテナを含んでもよい。非接触カード４２０は、非接触カードがモバイルコンピューティングデバイス／端末４０２にタップされたときなどに、ＮＦＣを介してモバイルコンピューティングデバイス／端末４０２と通信できる。非接触カード４２０は、セキュアな通信に使用されるカウンタ４１５を含んでもよい。決済カード４０３は、ＮＦＣまたは別の無線プロトコルを介してモバイルコンピューティングデバイス／端末と無線通信できる。

【００２２】

モバイルコンピューティングデバイス／端末４０２は、サーバ４０４及び／又はサーバ４３０と通信できる。いくつかの例示的な実施形態では、モバイルコンピューティングデバイス／端末４０３は、サーバ４３０とのみ直接通信する。これらのサーバ４０４及び４３０は、ネットワーク４０６を介してモバイルコンピューティングデバイス／端末４０２に接続され得る。ネットワーク４０６は、インターネット及び／又は携帯電話ネットワークなどのワイドネットワークのほか、企業ネットワーク、イーサネットネットワーク、ＷｉＦｉネットワークなどのローカルエリアネットワーク又はイントラネットを含み得る。サーバ４０４は、１つ以上のプロセッサ４２２を含み得る。プロセッサ４２２は、プロセッサ４０８について説明したものと同様のさまざまな形態をとることができる。サーバ４０４は、モバイルコンピューティングデバイス／端末４０２のストレージ４１０について上述したストレージまたはメモリの形態を含むストレージ４２４を含んでもよい。ストレージ４２４は、コンピュータプログラミング命令４４０を格納し得る。いくつかの例示的な実施形態では、これらのコンピュータプログラミング命令４４０は、ユーザ４１８が宿泊施設にチェックインし、上記のようにデジタルキーを取得するためにアクセスできるＷｅｂサイトについてである。コンピュータプログラミング命令はまた、チェックインおよびデジタルキーの取得を容易にするためにアプリケーション４１４と対話するサーバコードであってもよい。サーバ４３０は、ユーザの身元の認証が必要な場合に使用され、身元認証を提供するためにサーバ４０４によって呼び出されてもよい。サーバは、ユーザの身元を認証するための認証サービス４３２を実行するプロセッサ４３３を含んでもよい。サーバ４０４および４３０は、データベースなどのデータ４３４にアクセスできてもよい。

【００２３】

上述したように、宿泊部屋のデジタルキーとして決済カードを使用する１つのオプションは、ユーザが非接触カードを使用して身元を証明し、モバイルコンピューティングデバイスを介してデジタルキーを決済カードに送信することである。図５は、このような対話を実行する際のさまざまな構成要素のアクティビティを示す。図５は、図４の構成要素の描写を参照して説明される。まず、ユーザ４１８は、モバイルコンピューティングデバイス４０２上でアプリケーション４１４を開く（５０２参照）。アプリケーションは、宿泊施設のアプリケーションであってもよく、宿泊施設のウェブサイトにアクセスできるようにするウェブブラウザであってもよい。アプリケーション４１４を使用して、ユーザ４１８は、サーバ４４０上のコンピュータプログラム命令４４０を含むプログラムと通信し、チェックインを要求する（５０３参照）。チェックインプロセスの一部として、アプリケーション４１４は、ユーザ４１８に非接触カード４２０をモバイルコンピューティングデバイス４０２にタップするように指示する（５０４参照）。非接触カード４２０はタップ

され、ＮＦＣを介してセキュアパッケージで識別情報をモバイルコンピューティングデバイス４０２に送信する（５０６参照）。非接触カード４２０からのセキュアパッケージの構成と内容については、以下で詳しく説明する。モバイルコンピューティングデバイス４０２は、識別情報を含むセキュアパッケージをサーバ４０４に送信する（５０８参照）。サーバ４３０は、セキュアパッケージをサーバ４３０上の認証サービス４３２に転送できる。そして、サーバ４３０上の認証サービス４３２がユーザの身元を認証する（５１０参照）。ユーザが認証されると、サーバ４０４などによってユーザはチェックインされ得る。例示的な実施形態では、サーバ４０４は、サーバ４３０にユーザの身元の認証を実行してその結果をサーバ４０４に通知するように要求できる。認証が成功しなかった場合、拒否がサーバ４０４に送信され、モバイルコンピューティングデバイス４０２上のアプリケーション４１４に転送され得る。認証が成功すると、ユーザはチェックインされ、サーバ４０４によってモバイルコンピューティングデバイス４０２上のアプリケーション４１４にチェックインの成功が報告される（５１２参照）。

【００２４】

次に、モバイルコンピューティングデバイス４０２上のアプリケーション４１４は、ユーザに決済カードを鍵として使用するように指示し得る（５１４参照）。ユーザは、決済カードを鍵として使用したい旨を肯定的に応答し得る（５１６参照）。ユーザがこのオプションを選択しない場合、プロセスは停止する。それ以外の場合、アプリケーション４１４はサーバ４０４に鍵を要求できる（５１８参照）。サーバ上のコンピュータプログラム命令４４０は、デジタルキーであるセキュアパッケージを生成する。そして、セキュアパッケージのキーコード及びその他の情報は、サーバ４０４からモバイルコンピューティングデバイス４０２上のアプリケーション４１４に送信され得る（５２０参照）。アプリケーション４１４は、ユーザ４１８に決済カードをモバイルコンピューティングデバイス４０２にタップするように指示する。決済カードは、モバイルコンピューティングデバイス４０３にタップされる（５２４参照）。デジタルキーコードを保持するセキュアパッケージは、タップの結果として、モバイルコンピューティングデバイス上のアプリケーション４１４によってＮＦＣを介して決済カードに送信され得る。具体的には、モバイルコンピューティングデバイス４０２はキーコードを送信し（５２６参照）、キーコードは決済カードに保存される（５２８参照）。

【００２５】

非接触カードの使用の詳細に焦点を当てて説明する。図６Ａは、販売業者、金融機関などのサービスプロバイダ６０６によって発行され得る非接触カード６００の表面の例を示す。一部の例示的な実施形態では、非接触カード６００は識別カードを含んでもよい。いくつかの場合、カード６００はデュアルインタフェース非接触決済カードを含んでもよい。非接触カード６００は、プラスチック、金属、及びその他の材料で構成された単層または積層を含み得る基板６０８を含んでもよい。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６００は、ＩＳＯ／ＩＥＣ７８１０規格のＩＤ－１形式に準拠した物理的特性を有してもよく、または非接触カード６００は、ＩＳＯ／ＩＥＣ１４４４３規格に準拠してもよい。しかしながら、本開示による非接触カード６００は異なる特性を有してもよいことが理解される。

【００２６】

非接触カード６００はまた、カードの表面及び／又は裏面に表示される識別情報６０４、及び接触パッド６０２を含み得る。接触パッド６０２は、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、又はタブレットコンピュータなどの別の通信デバイスとの接続を確立するように構成され得る。非接触カード６００は、図６Ａに示されていない処理回路、アンテナ、及びその他の構成要素を含んでもよい。これらの構成要素は、接触パッド６０２の後ろ、又は基板６０８上の他の場所に配置され得る。非接触カード６００はまた、磁気ストライプ又はテープを含んでもよく、これらはカードの裏面に配置さ

れ得る（図６Ａには図示せず）。

【００２７】

図６Ｂに示すように、図５Ａの接触パッド６０２は、マイクロプロセッサ６１４及びメモリ６１６を含む、情報を格納及び処理する処理回路６１０を含んでもよい。処理回路６１０には、本明細書で説明する機能を実行するために必要な、プロセッサ、メモリ、エラーおよびパリティ／ＣＲＣチェッカー、データエンコーダ、衝突防止アルゴリズム、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などの追加の構成要素が含まれ得ることが理解される。

【００２８】

メモリ６１６は、読み取り専用メモリ、ライトワンスリードマルチプルメモリ又は読み取り／書き込み型メモリ、例えば、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭなどであってもよく、非接触カード６００は、これらのメモリの１つ以上を含み得る。読み取り専用メモリは、読み取り専用または１回限りのプログラム可能（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る。ワンタイムプログラマブルであることにより、一度書き込んでから何度も読み取る機会が提供される。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を出荷された後のある時点でプログラムされ得る。当該メモリは、一旦プログラムされると、書き換えることはできないが、何度も読み取られ得る。読み取り／書き込みメモリは、工場出荷後、何度もプログラムおよび再プログラムされ得る。また、当該メモリは、何度も読み取られ得る。

【００２９】

メモリ６１６は、１つ又は複数のアプレット６１８、１つ又は複数のカウンタ６２０、および一意の顧客識別子６２２を格納するように構成され得る。１つ又は複数のアプレット６１８は、ＪａｖａＣａｒｄアプレットなどの、１つ又は複数の非接触カード上で実行す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を含んでもよい。しかしながら、アプレット６１８はＪａｖａＣａｒｄアプレットに限定されず、非接触カードまたはメモリが制限されたその他のデバイス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つ又は複数のカウンタ６２０は、整数を格納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６２２は、非接触カード６００のユーザに割り当てられた一意の英数字識別子を含んでもよく、この識別子によって、非接触カードのユーザを他の非接触カードのユーザと区別できる。いくつかの例では、顧客識別子６２２は、顧客、及び当該顧客に割り当てられたアカウントの両方を識別でき、さらに当該顧客のアカウントに関連付けられた非接触カードを識別できる。

【００３０】

いくつかの例では、非接触カード６００は１つ又は複数のアンテナ６１２を備えていてもよい。１つ又は複数のアンテナ６１２は、非接触カード６００内及び接触パッド６０２の処理回路６１０の周囲に配置され得る。例えば、１つ又は複数のアンテナ６１２は処理回路６１０と一体化されてもよく、１つ又は複数のアンテナ６１２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６１２は、接触パッド６０２及び処理回路６１０の外部にあってもよい。

【００３１】

一実施形態では、非接触カード６００のコイルは、空芯変圧器の二次側として機能できる。端末は、電力を遮断するか、振幅変調することによって非接触カード６００と通信できる。非接触カード６００は、１つ又は複数のコンデンサを通じて機能的に維持され得る非接触カードの電源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できる。非接触カード６００は、非接触カードのコイルの負荷を切り替えるか、負荷変調を行うことによって通信を返信できる。負荷変調は、干渉により端末のコイルで検出され得る。

【００３２】

上記したように、非接触カード６００は、スマートカード又はＪａｖａＣａｒｄなどのメモリが制限された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され得、１つ又は複数のアプリケーション又はアプレットをセキュアに実行され得る。さ

まざまなモバイルアプリケーションベースのユースケースで多要素認証（ＭＦＡ）用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が追加され得る。アプレットは、モバイルＮＦＣリーダなどの読み取り機からの、近距離データ交換要求などの１つ又は複数の要求に応答し、ＮＤＥＦテキストタグとしてエンコードされた暗号化されたセキュアなＯＴＰを含むＮＤＥＦメッセージを生成するように構成され得る。

【００３３】

図７は、非接触カード７０２とコンピューティングデバイス７０６との間の対話を示す構成要素の図を示す。非接触カードはＮＦＣ機能を備えることができる。非接触カードがモバイルコンピューティングデバイス７０８上のＮＦＣリーダ７０８に近づくと、セキュアパッケージ７０４内の識別情報は、コンピューティングデバイスに送信される。

【００３４】

識別情報７０４を保持するセキュアパッケージの生成は、ＭＤ５又はＳＨＡ－１などの暗号化ハッシュ関数によって生成され得る。図８Ａは、例示的な実施形態において暗号化ハッシュ関数がどのように使用されるかを示すブロック図８００を示す。図８Ａに示す例では、３つの入力８０２、８０４、及び８０６がハッシュ関数８０８に一緒に渡される。３つの入力を示すという選択は、説明を目的としたものであり、制限を意図したものではない。いくつかの場合、他の入力数が使用されてもよい。ハッシュ関数８０８は出力ハッシュ値８１２を生成する。ハッシュ関数８０８の性質上、ハッシュ関数８０８で使用された鍵８１０を知らなければ、ハッシュ値８１２から入力８０２、８０４、及び８０６を導出することは計算上困難である。鍵８１０は秘密を維持される。鍵８１０は、セッションごとに動的に生成され、非接触カードに固有のものとなり得る。したがって、ハッシュ関数８０８は、セキュアパッケージに含まれる内容（例えば、入力８０２、８０４、及び８０６）についてのセキュリティの層を提供する。

【００３５】

例示的な実施形態では、入力８０２、８０４、及び８０６は、当事者（party）が交換したい情報、及び開始側当事者を認証するためのプロトコルに応じて異なってもよい。図８Ｂは、例示的な実施形態においてハッシュ化され得る入力８３２の想定されるタイプの図８３０を示す。これらの例示的な実施形態では、非接触カードによって生成されたワンタイムパスワード８３４は入力として含まれてもよい。開始側当事者のアカウント識別子８３６が提供されてもよい。これは、開始側当事者のアカウントを一意に識別するアカウント番号又はその他の識別子であってもよい。アカウント識別子８３６は、開始側当事者の電話番号であってもよい。いくつかの場合、開始側当事者の電話番号は、ハッシュ値８１２に含まれず、モバイルコンピューティングデバイスから送信されたメッセージから導出され得る。入力８３２は、カウンタ値８３８及び／又は開始側当事者の名前８４０を含んでもよい。

【００３６】

セキュリティの追加レイヤとして、ハッシュ値９０２は暗号化され得る。図９は、このような暗号化を示すブロック図９００を示す。上記のように生成されたハッシュ値９０２は、暗号化鍵９０６を使用してハッシュ値を暗号化する暗号化エンジン９０４に渡される。結果の出力はセキュアパッケージ９０８である。暗号化エンジン７０４は、ＤＥＳ、ＡＥＳ、ＲＳＡ、ＤＳＡなどのさまざまな暗号化アルゴリズムのいずれかを使用できる。これらは、ＤＥＳやＡＥＳなどの対称暗号化アルゴリズム、又はＲＳＡやＤＳＡなどの非対称暗号化アルゴリズムであってもよい。認証サービス４３２は、セキュアパッケージを復号するための適切な鍵を所有していると推定される。図９には示されていないが、ハッシュ値９０２と組み合わせて他の内容が暗号化されてもよい。

【００３７】

図１０は、ユーザの身元を認証する際に実行され得る例示的なステップのフローチャート１０００を示す。ユーザは、非接触カード７０２を、上記したようにＮＦＣリーダ７０８を備えたモバイルコンピューティングデバイス７０６にタップする（１００２参照）。

モバイルコンピューティングデバイス７０６は、非接触カード７０２から取得したセキュアパッケージを含むメッセージを、サーバ４３０上の認証サービス４３２に送信する（１００４参照）。セキュアパッケージ内のワンタイムパスワード（ＯＴＰ）及びその他の情報が抽出される（１００６参照）。認証サービス４３２は、抽出された情報を使用してユーザの身元を認証する（１００８参照）。

【００３８】

非接触カードから発信されたセキュアパッケージを受信する認証サービスについては、ここでは詳しく説明しない。図１１は、認証サービス１１００の一部として格納される特定の項目を示す。これらの項目には、復号／暗号化動作で使用され得る同期カウンタ１１０２が含まれる。認証サービス１１００は、セキュアパッケージに対して復号動作を実行するための復号コード１１０４を含む。認証サービス１１００は、多くの復号鍵および暗号化鍵１１０６を格納してもよい。

【００３９】

概して、サーバ４３０（又は他のコンピューティングデバイス）及び非接触カード４２０は、同じマスター鍵（マスター対称鍵とも呼ばれる）がプロビジョニングされ得る。より具体的には、各非接触カード４２０は、認証サービス４３２内に対応するペアを有する個別のマスター鍵がプログラムされ得る。例えば、非接触カード４２０が製造されるときに、固有のマスター鍵が非接触カード４２０のメモリにプログラムされ得る。同様に、固有のマスター鍵は、認証サービス４３２がアクセスできるアカウント情報内の非接触カード４２０に関連付けられた顧客の記録に保存（及び／又は別のセキュアな場所に保存）され得る。マスター鍵は、非接触カード４３２及び認証サービス４３２以外のすべての当事者から秘密を維持され得るため、システムのセキュリティが強化される。

【００４０】

マスター鍵をカウンタと組み合わせて使用することで、鍵の多様化によるセキュリティを強化できる。カウンタ４１５及び１１０２は、非接触カード４２０と認証サービス４３２との間で同期される値を含む。カウンタ値は、非接触カード４２０と認証サービス４３２との間でデータが交換されるたびに変化する数値を含んでもよい。

【００４１】

モバイルコンピューティングデバイス４０２と非接触カード４２０との間で通信が確立された後、非接触カード４２０はメッセージ認証コード（ＭＡＣ）暗号文を生成できる。いくつかの例では、非接触カード４２０が読み取られるときにこれが発生し得る。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る近距離データ交換（ＮＤＥＦ）タグの、ＮＦＣ読み取りなどの読み取り時に発生し得る。例えば、ＮＦＣリーダなどのリーダは、ＮＤＥＦ生成アプレットのアプレットＩＤを含む、アプレット選択メッセージなどのメッセージを送信できる。選択が確認されると、選択ファイルメッセージの後に読み取りファイルメッセージが続くシーケンスが送信され得る。例えば、シーケンスは、「Select Capabilities file」、「Read Capabilities file」、及び「Select NDEF file」を含んでもよい。この時点で、非接触カード４２０によって維持されるカウンタ値４１５が更新又はインクリメントされ、その後に「Read NDEF file」が続き得る。この時点で、ヘッダと共有秘密を含むメッセージが生成される場合がある。そして、セッション鍵が生成され得る。ＭＡＣ暗号文は、ヘッダと共有秘密を含むメッセージから作成され得る。そして、ＭＡＣ暗号文は１つ又は複数のランダムデータのブロックと連結され、ＭＡＣ暗号文及び乱数（ＲＮＤ）は、セッション鍵を用いて暗号化され得る。その後、暗号文とヘッダが連結され、ＡＳＣＩＩ１６進数としてエンコードされ、（「Read NDEF file」メッセージに応答して）ＮＤＥＦメッセージ形式で返される。いくつかの例では、ＭＡＣ暗号文はＮＤＥＦタグとして送信され、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（たとえば、フォーマットされた文字列）とともに含まれ得る。そして、非接触カード４２０は、ＭＡＣ暗号文をモバイルコンピューティングデバイス４０２に送信し、モバイルコンピューティングデバイス４０２は、以下に説明するように、検証のためにＭＡＣ暗号文を認証サービス４３２に転送する。しかしながら、一部の実施形

態では、モバイルコンピューティングデバイス４０２は、ＭＡＣ暗号文を検証し得る。

【００４２】

より一般的には、データを（例えば、サーバ４３０へ）送信する準備をするとき、非接触カード４２０はカウンタ４１５をインクリメントできる。そして、非接触カード４２０は、マスター鍵及びカウンタ値を暗号化アルゴリズムへの入力として提供し、暗号化アルゴリズムは多様化された鍵を出力として生成する。暗号化アルゴリズムには、暗号化アルゴリズム、ハッシュベースのメッセージ認証コード（ＨＭＡＣ）アルゴリズム、暗号ベースのメッセージ認証コード（ＣＭＡＣ）アルゴリズムなどが含まれ得る。暗号化アルゴリズムの非限定的な例としては、３ＤＥＳ又はＡＥＳ１２８などの対称暗号化アルゴリズム、ＨＭＡＣ－ＳＨＡ－２５６などの対称ＨＭＡＣアルゴリズム、ＡＥＳ－ＣＭＡＣなどの対称ＣＭＡＣアルゴリズムなどが挙げられる。

【００４３】

そして、非接触カード４２０は、多様化された鍵を使用してデータ（例えば顧客識別子及びその他のデータ）を暗号化できる。そして、非接触カード４２０は、暗号化されたデータをモバイルコンピューティングデバイス４０２に（例えば、ＮＦＣ接続、Ｂｌｕｅｔｏｏｔｈ接続などを介して）送信できる。そして、モバイルコンピューティングデバイス４０２は、暗号化されたデータをネットワーク４０６を介してサーバコンピューティングデバイス４３０上の認証サービス４３２に送信できる。少なくとも１つの実施形態では、非接触カード４２０は、暗号化されたデータとともにカウンタ値を送信する。このような実施形態では、非接触カード４２０は、暗号化されたカウンタ値、または暗号化されていないカウンタ値を送信できる。

【００４４】

カウンタが例として使用されているが、非接触カード４２０、モバイルコンピューティングデバイス４０２、及び／又は認証サービス４３２間の通信を保護するために他のデータが使用されてもよい。例えば、カウンタは、新しい多様化された鍵が必要になるたびに生成されるランダムなｎｏｎｃｅ、非接触カード４２０及び認証サービス４３２から送信されるカウンタ値の完全な値、非接触カード４２０及び認証サービス４３２から送信されるカウンタ値の一部、非接触カード４２０及び認証サービス４３２によって独立して維持されるが両者間では送信されないカウンタ、非接触カード４２０と認証サービス４３２との間で交換されるワンタイムパスコード、及びデータの暗号化ハッシュに置き換えられてもよい。いくつかの例では、多様化された鍵の１つ以上の部分が、複数の多様化された鍵を作成するために当事者によって使用されてもよい。

【００４５】

図１２は、セキュアパッケージを含む認証メッセージが受信側当事者である認証サービス４３２によって受信された後、開始側当事者を認証するために実行されるステップのフローチャート１２００を示す。まず、認証サービス４３２は復号鍵１１０６を使用してセキュアパッケージを復号する。さらに、復号鍵１１０６は、ハッシュを復号して、ハッシュ関数８０８によってハッシュされた入力を抽出するために使用される（１２０２参照）。抽出されたパスワード及びカウンタ値は、有効なパスワード及び有効なカウンタ値と比較され得る（１２０４参照）。パスワードが一致し、カウンタ値が一致するかどうか、又はパスワードの有効期限が切れていないことを抽出されたカウンタ値が示しているかどうかが判断される（１２０６参照）。パスワードが一致し、抽出されたカウンタ値に基づいて抽出されたパスワードが期限切れになっていない場合、他の抽出された情報が比較され得る（１２０８参照）。

【００４６】

その他の情報は、モバイルコンピューティングデバイス４０２の電話番号などの他の認証要素１００２であり、ユーザ４１８の記録上の電話番号と比較され得る。その他の認証要素は、ユーザの地理位置情報を含んでもよい。地理位置情報は、ユーザの居住地に関する情報と比較できるＧＰＳ情報や市外局番、交換局プレフィックス情報などの情報であってもよい。その他の認証要素はまた、ユーザと認証サービス４３２と間で共有される共有

秘密を含んでもよい。

【００４７】

図１２を再度参照すると、その他の情報が有効である場合（１２１０参照）、ユーザ４１８は認証される（１２１４参照）。そうでない場合、ユーザ４１８は認証されない（１２１２参照）。同様に、パスワードが一致しないか、抽出されたカウンタ値によって示されるようにパスワードの有効期限が切れている場合、ユーザは認証されない（１２１２参照）。

【００４８】

決済カードに焦点を当てて議論する。図１３は、例示的な実施形態で使用するのに適した決済カード１３００のブロック図を示す。決済カード１３００は、支払いに使用できるクレジットカード、デビットカード、またはその他の種類のカードである。いくつかの実施形態では、決済カード１３００は、多機能カード又は接触カードなどのスマートカードであってもよい。決済カード１３００は、上記したように、コンピュータプログラミング命令を実行するプロセッサ１３０２と、ＮＦＣ機能を提供するＮＦＣハードウェア１３１４を含み得る。決済カード１３００はまたメモリ１３０４を含み得る。メモリ１３０４は、決済カードを使用して電子決済を実行するための命令１３０６を格納し得る。メモリ１３０４は、上記したようにロックを解除するための命令１３０８を格納し得る。これらの命令１３０６および１３０８は、プロセッサ１３０２によって実行され、上記の決済カード１３００の機能を実行する。メモリ１３０４は、ドアのロック（錠）、エリアのロック、アイテムのロックなどのロックを解除するために使用されるキーコード１３１０を保持し得る。最後に、メモリはデータ１３１２を格納し得る。

【００４９】

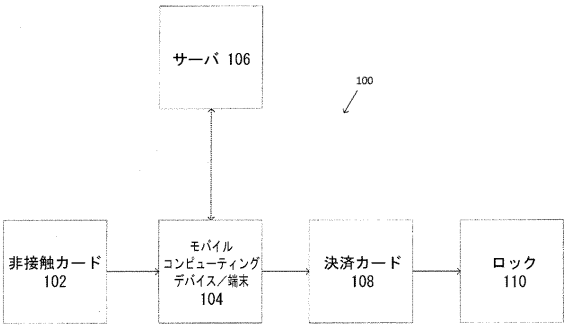
図１４は、宿泊施設、職場、店舗などでの支払いに決済カード１３００を使用するために実行され得る例示的なステップのフローチャート１４００を示す。まず、ユーザは、購入したいものを特定する（１４０２参照）。そして、ユーザは決済カードをリーダにタップして支払いを実行する（１４０４参照）。例えば、ユーザルームのユーザは、ユーザルーム内に設置されたリーダに決済カードをタップすることで、ミニバーの物品について支払ったり、映画について支払ったりできる。リーダは、支払いを実現するために決済カードとＮＦＣを介してワイヤレスで通信できるＮＦＣリーダであってもよい。別の例として、ＮＦＣ対応であり、職場のセキュリティ保護されたエリアのロックを解除するために使用され得る識別カードを従業員が有してもよい。従業員は、ランチルームのチェックアウト時にＮＦＣリーダに識別カードをタップして昼食代を支払うことができる。購入代金は、部屋アカウント、従業員アカウント、銀行口座などのユーザアカウントに請求される（１４０６参照）。

【００５０】

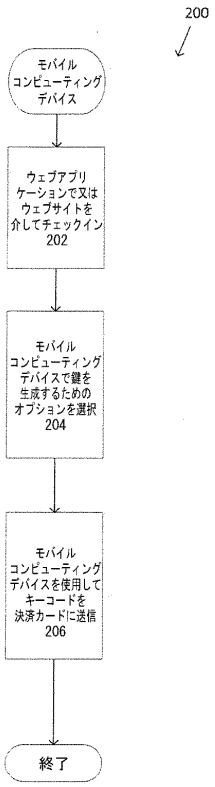
本出願は例示的な実施形態に焦点を当てているが、本明細書に添付されている特許請求の範囲から逸脱することなく、形式および詳細にさまざまな変更を加えることができることを理解されたい。

【図面】

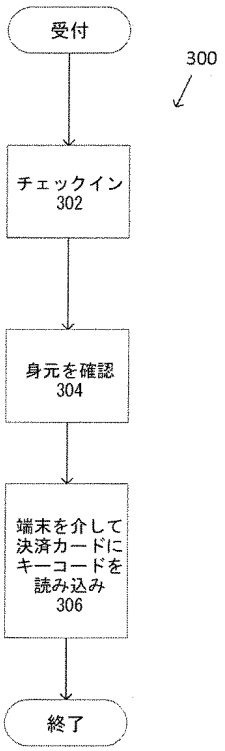
【図１】


サーバ 106
100
非接触カード
102
モバイル
コンピューティング
デバイス／端末
104
決済カード
108
ロック
110

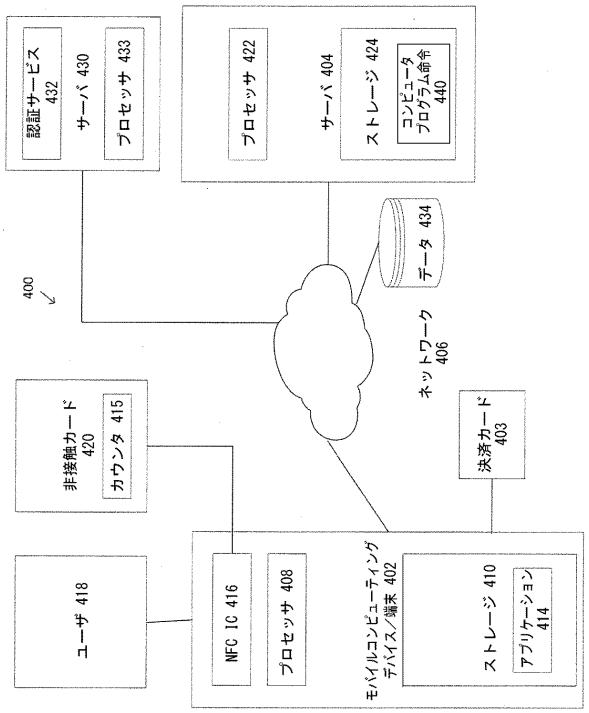
【図２】


200
モバイル
コンピューティング
デバイス
ウェブアプリ
ケーションで又は
ウェブサイトを
介してチェックイン
202
モバイル
コンピューティング
デバイスで鍵を
生成するための
オプションを選択
204
モバイル
コンピューティング
デバイスを使用して
キーコードを
決済カードに送信
206
終了

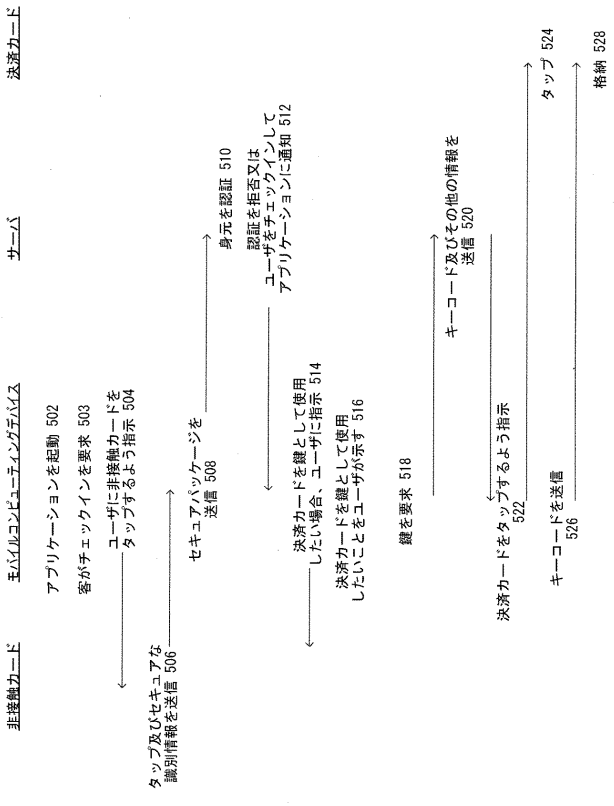
【図３】


受付
300
チェックイン
302
身元を確認
304
端末を介して
決済カードまたは
キーコードを
読み込み
306
終了

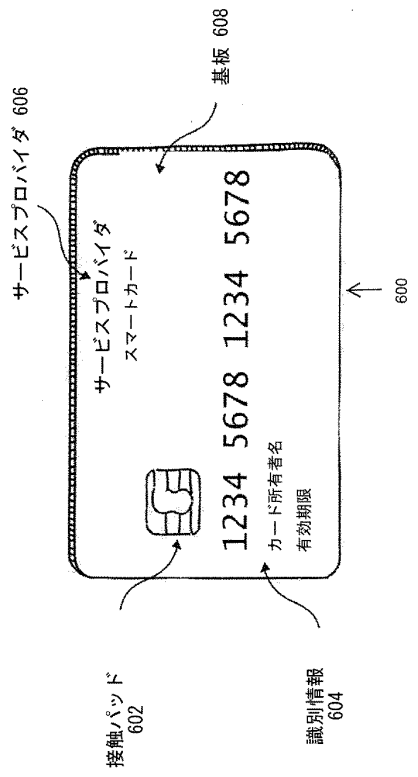
【図４】


認証サービス
432
サーバ 430
プロセッサ 433
プロセッサ 422
サーバ 404
ストレージ 424
コンピュータ
プログラム命令
440
400
データ 434
ネットワーク
406
非接触カード
420
カウンタ 415
決済カード
403
ユーザ 418
NFC IC 416
プロセッサ 408
モバイルコンピューティング
デバイス／端末 402
ストレージ 410
アプリケーション
414

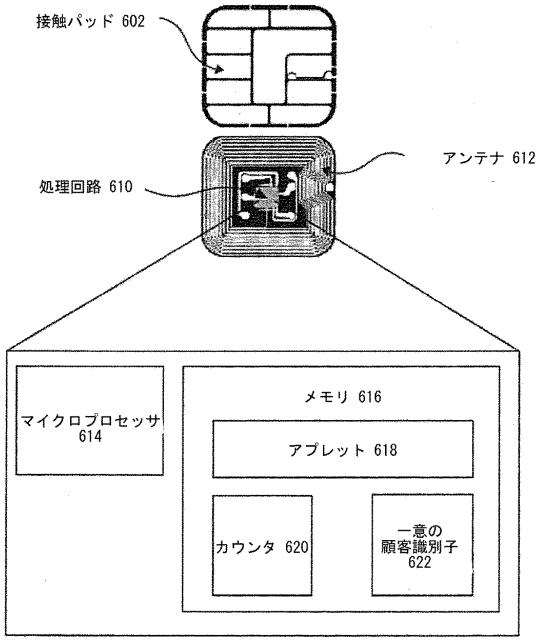
【図５】


非接触カード
モバイルコンピューティングデバイス
サーバ
決済カード
アプリケーションを起動 502
客がチェックインを要求 503
ユーザに非接触カードを
タップするよう指示 504
タップ及びセキュアな
識別情報を送信 506
セキュアパッケージを
送信 508
身元を認証 510
認証を指否又は
ユーザをチェックインして
アプリケーションに通知 512
決済カードを鍵として使用
したい場合、ユーザに指示 514
決済カードを鍵として使用
したいことをユーザが示す 516
鍵を要求 518
キーコード及びその他の情報を
送信 520
決済カードをタップするよう指示
522
タップ 524
キーコードを送信
526
格納 528

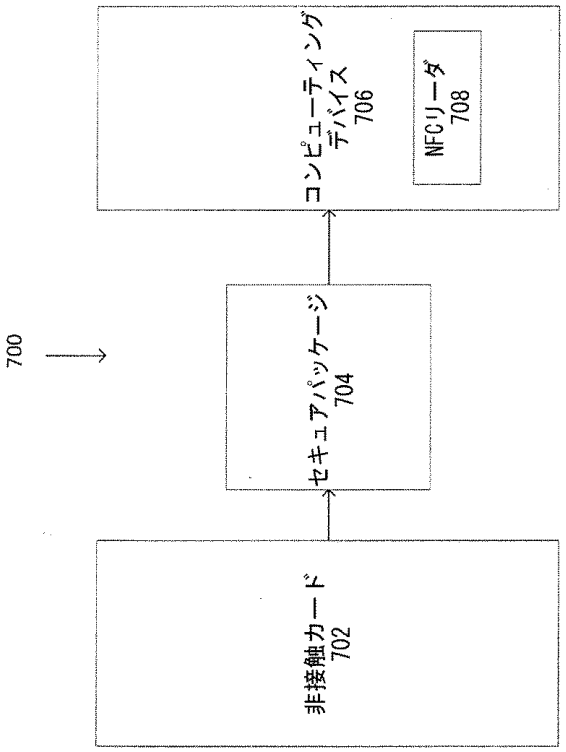
【図６Ａ】


サービスプロバイダ 606
基板 608
サービスプロバイダ
スマートカード
1234 5678 1234 5678
カード所有者名
有効期限
600
接触パッド
602
識別情報
604

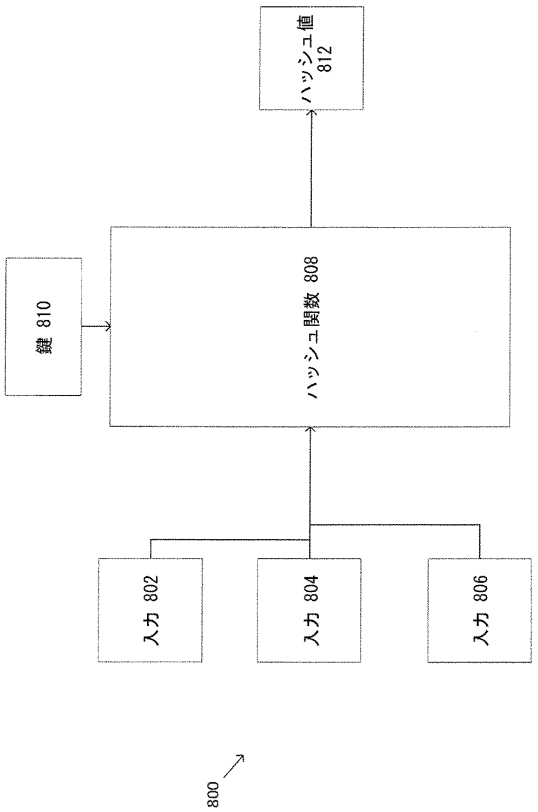
【図６Ｂ】



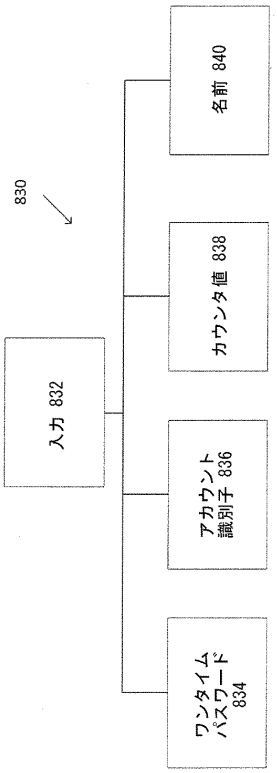
【図７】



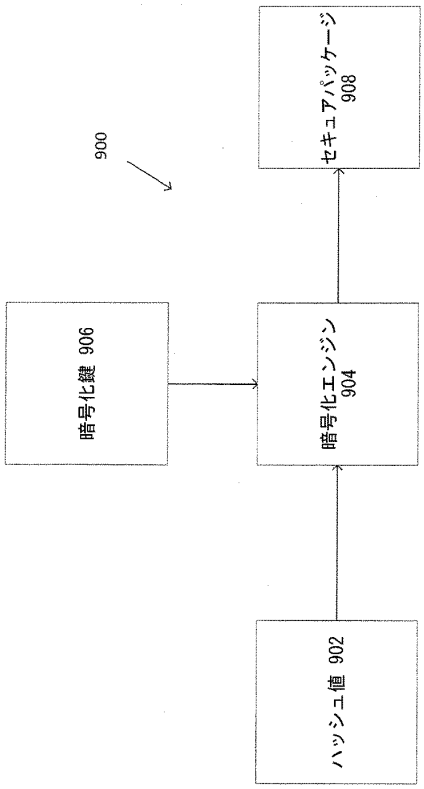
【図８Ａ】



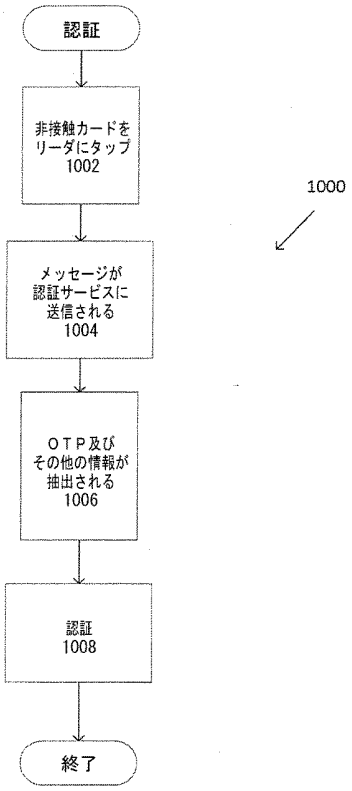
【図８Ｂ】



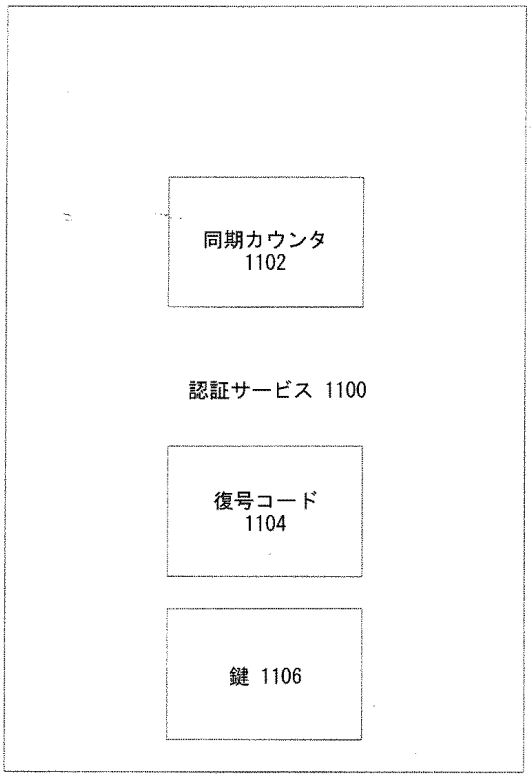
【図９】



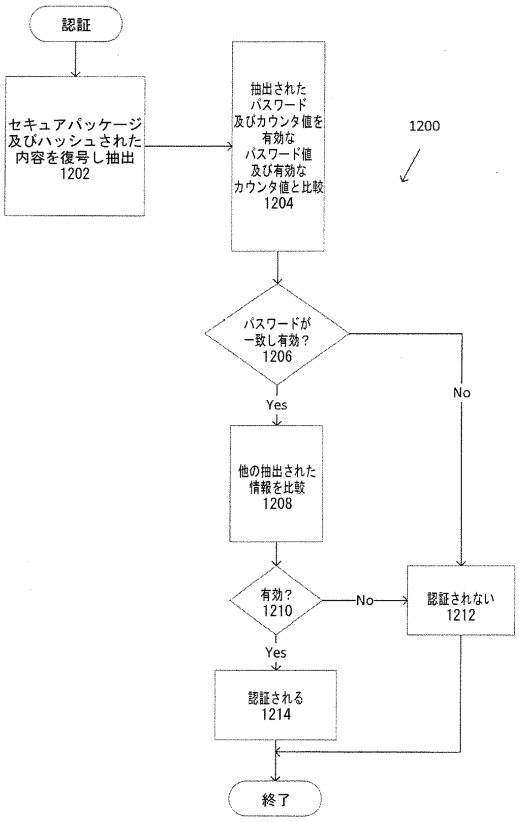
【図１０】



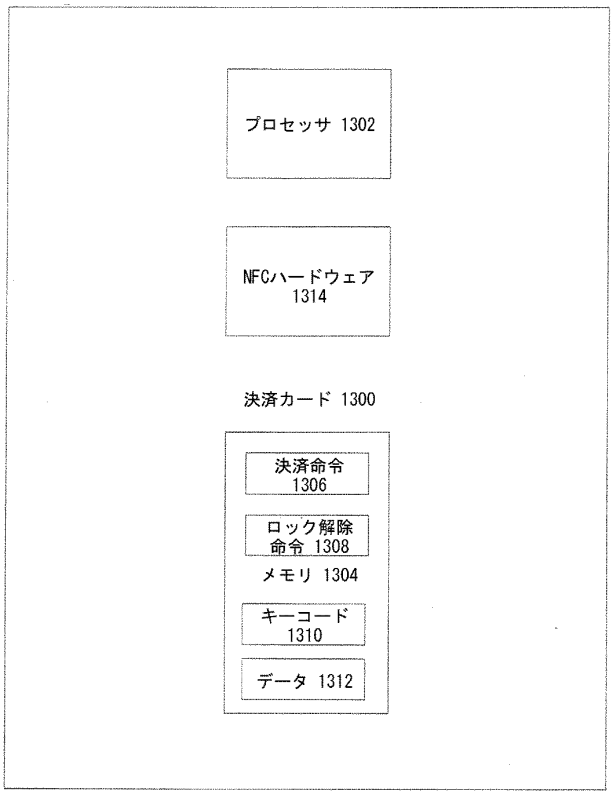
【図１１】



【図１２】



【図１３】


プロセッサ 1302
NFCハードウェア 1314
決済カード 1300
決済命令 1306
ロック解除命令 1308
メモリ 1304
キーコード 1310
データ 1312

【図１４】


決済
1400
ユーザが施設で購入したいものを特定 1402
ユーザが鍵決済カードをタップ 1404
ユーザのアカウントに請求される 1406
終了

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/043780

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C9/00 G07C9/27 G06Q20/34
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)
G07C G07G G06Q

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2020/175793 A1 (WISHNE JUSTIN [US]) 4 June 2020 (2020-06-04) abstract; figures 1,3,5 paragraph [0005] paragraphs [0023] - [0036] paragraphs [0043] - [0046] paragraphs [0049] - [0052]	1-20
A	CN 109 034 758 A (INDUSTRIAL & COMMERCIAL BANK OF CHINA CO LTD) 18 December 2018 (2018-12-18) paragraphs [0030] - [0040]	1-20
A	WO 2020/157823 A1 (FUJITSU FRONTECH LTD [JP]) 6 August 2020 (2020-08-06) abstract; figures 1,2 paragraphs [0011] - [0039]	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
1 December 2022	12/12/2022

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	Pfyffer, Gregor

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2022/043780

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2020175793 A1	04-06-2020	CA 3007504 A1	15-06-2017
		EP 3374740 A1	19-09-2018
		US 2017161978 A1	08-06-2017
		US 2018225900 A1	09-08-2018
		US 2019279451 A1	12-09-2019
		US 2020175793 A1	04-06-2020
		US 2022024410 A1	27-01-2022
		WO 2017100318 A1	15-06-2017
CN 109034758 A	18-12-2018	NONE	
WO 2020157823 A1	06-08-2020	CA 3125642 A1	06-08-2020
		JP 7096914 B2	06-07-2022
		JP WO2020157823 A1	09-09-2021
		US 2021295626 A1	23-09-2021
		WO 2020157823 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,CV,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．ＢＬＵＥＴＯＯＴＨ

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　カルバシ，ネガル
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　シャー，サリク
アメリカ合衆国２０００９ワシントン・ディストリクト・オブ・コロンビア、ベルモント・ストリート・ノースウエスト１６１６、ユニット・エイ

(72)発明者　ホートン，マシュー
アメリカ合衆国７４１４６オクラホマ州タルサ、サウス・ワンハンドレッドエイティーンス・イースト・アベニュー４０２１

(72)発明者　ベンクレイラ，アブデルカデル ムハメド
アメリカ合衆国２００１５ワシントン・ディストリクト・オブ・コロンビア、ハリソン・ストリート・ノースウエスト４４１３

(72)発明者　アトキンス，フィービー
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　ジョーハル，イムレン
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

Ｆターム（参考）　2E250　AA06 BB08 BB67 DD06 EE10 EE15 FF28 FF36 GG06