

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2020-529089
(P2020-529089A)

(43) 公表日 令和2年10月1日(2020.10.1)

(51) Int.Cl. F I テーマコード(参考)
G06Q 20/32 (2012.01) G06Q 20/32 320 5L055

審査請求 未請求 予備審査請求 有 (全 34 頁)

(21) 出願番号 特願2020-522273 (P2020-522273)
(86) (22) 出願日 平成30年7月2日(2018.7.2)
(85) 翻訳文提出日 令和2年2月13日(2020.2.13)
(86) 国際出願番号 PCT/SG2018/050321
(87) 国際公開番号 W02019/009803
(87) 国際公開日 平成31年1月10日(2019.1.10)
(31) 優先権主張番号 201741023345
(32) 優先日 平成29年7月3日(2017.7.3)
(33) 優先権主張国・地域又は機関
インド(IN)

(71) 出願人 520000456
ジーピー ネットワーク アジア プーテ
イーイー. リミテッド
GP NETWORK ASIA PTE
. LTD.
シンガポール 068809, #38-
01 オウ ダウンタウン, シェントン
ウェイ, 6
6, Shenton Way, #38
-01 OUE Downtown, O
68809 Singapore
(74) 代理人 100137095
弁理士 江部 武史
(74) 代理人 100091627
弁理士 朝比 一夫

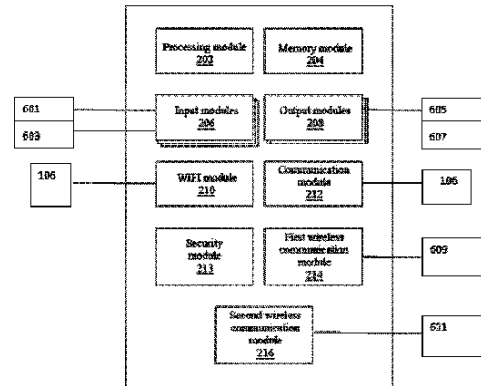
最終頁に続く

(54) 【発明の名称】 支払処理

(57) 【要約】

支払端末を操作する方法は、アクティブ化入力を受信する工程と、アクティブ化入力にตอบสนองして、第1のタイプの外部支払デバイスと通信するための第1の無線信号および第2のタイプの外部支払デバイスと通信するための第2の無線信号を出力する工程と、を含む。第1の無線信号および第2の無線信号は、互いに異なる第1のプロトコルおよび第2のプロトコルにそれぞれ対応するフォーマットにされている。方法は、第1の無線信号および第2の無線信号の一方に対する返信を受信する工程と、返信にตอบสนองして、第1の無線信号および第2の無線信号の他方の出力を終了する工程とを、さらに含む。

【選択図】 図6



162

FIG 6

【特許請求の範囲】**【請求項 1】**

支払端末を操作する方法であって、
アクティブ化入力を受信する工程と、

前記アクティブ化入力に应答して、第 1 のタイプの外部支払デバイスと通信するための第 1 の無線信号および第 2 のタイプの外部支払デバイスと通信するための第 2 の無線信号を出力する工程であって、

前記第 1 の無線信号および前記第 2 の無線信号は、互いに異なる第 1 のプロトコルおよび第 2 のプロトコルにそれぞれ対応するフォーマットにされている、前記出力する工程と、

前記第 1 の無線信号および前記第 2 の無線信号の一方に対する返信を受信する工程と、
前記返信に应答して、前記第 1 の無線信号および前記第 2 の無線信号の他方の出力を終了する工程と、を含むことを特徴とする方法。

【請求項 2】

前記外部支払デバイスを認証するために前記返信を処理し、これにより、通信チャンネルを確立する工程をさらに含む請求項 1 に記載の方法。

【請求項 3】

前記外部支払デバイスを認証するために前記返信を処理する工程をさらに含み、
前記処理する工程の後に、前記終了する工程が実行される請求項 1 に記載の方法。

【請求項 4】

前記第 1 の無線信号および前記第 2 の無線信号は、NFC 信号およびブルートゥース信号を含む請求項 1 に記載の方法。

【請求項 5】

前記外部支払デバイスを認証するために前記返信を処理し、これにより、通信チャンネルを確立する工程と、

前記通信チャンネルから、ユーザーを示すデータを受信する工程と、
入力として、取引額を示すデータを受信する工程と、

前記ユーザーを示す前記データおよび前記取引額を示す前記データを、サーバーに送信する工程と、をさらに含む請求項 1 に記載の方法。

【請求項 6】

前記外部支払デバイスを認証するために前記返信を処理し、これにより、通信チャンネルを確立する工程と、

前記通信チャンネルから、ユーザーを示すデータおよび現在の取引を特定するためのワンタイム検証子を受信する工程と、

入力として、取引額を示すデータを受信する工程と、

前記ユーザーを示す前記データ、前記ワンタイム検証子を示すデータ、および取引額を示すデータを、サーバーに送信する工程と、をさらに含む請求項 1 に記載の方法。

【請求項 7】

前記通信チャンネルを介して、新たなワンタイム検証子を出力する工程をさらに含む請求項 6 に記載の方法。

【請求項 8】

应答された前記第 1 の無線信号および前記第 2 の無線信号のいずれかを示す情報をサーバーに通信する工程をさらに含む請求項 1 に記載の方法。

【請求項 9】

処理デバイスおよび命令を保持している記憶手段を有し、外部デバイスと無線通信するための支払端末であって、

前記命令は、前記処理デバイスを制御し、前記支払端末に、

アクティブ化入力に应答して、第 1 のタイプの外部支払デバイスと通信するための第 1 の無線信号および第 2 のタイプの外部支払デバイスと通信するための第 2 の無線信号を出力させ、

10

20

30

40

50

前記第 1 の無線信号および前記第 2 の無線信号の一方に対する返信の受信に応答して、前記第 1 の無線信号および前記第 2 の無線信号の他方の出力を終了させ、

前記第 1 の無線信号および前記第 2 の無線信号は、互いに異なる第 1 のプロトコルおよび第 2 のプロトコルにそれぞれ対応するフォーマットにされていることを特徴とする支払端末。

【請求項 10】

前記アクティブ化入力を提供するためのキーパッドと、前記処理デバイスの制御下において情報を表示するディスプレイと、サーバーと通信するための出力デバイスと、をさらに有する請求項 9 に記載の支払端末。

【請求項 11】

前記第 1 の無線信号を出力するよう構成された第 1 の無線デバイスと、前記第 2 の無線信号を出力するよう構成された第 2 の無線デバイスと、をさらに有し、

前記第 1 の無線デバイスおよび前記第 2 の無線デバイスの双方は、前記処理デバイスの制御下にある請求項 9 に記載の支払端末。

【請求項 12】

セキュリティ鍵用の記憶手段を含むセキュリティデバイスをさらに有し、

前記セキュリティデバイスは、前記支払端末による使用のために、前記セキュリティ鍵を用いて、データを暗号化または復号化するよう構成されている請求項 9 に記載の支払端末。

【請求項 13】

前記第 1 の無線信号を出力するよう構成されたパーソナルエリアネットワークデバイスを有している請求項 9 に記載の支払端末。

【請求項 14】

前記第 2 の無線信号を出力するよう構成された近距離通信デバイスを有している請求項 9 に記載の支払端末。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、支払技術の分野に属する。

【背景技術】

【0002】

キャッシュレス支払いが、利便性のため、広く多用されるようになってきている。そのような支払いは、カードや携帯電話を含み得る。インターネット接続性は、携帯電話を用いてキャッシュレス電子取引を実行する際の制限である。

【0003】

インターネットの勢力範囲が拡大していようとも、携帯電話を使用しているユーザーが常にインターネットに接続されているかどうかは確実ではない。また、インターネットの使用は、世界の一部の社会の大規模な部分において、安価なものではないであろう。このような状況においては、携帯電話を介した電子取引を完了させることは、実現可能なものではないであろう。

【0004】

さらに、従来、商業者 (merchant) は、異なる複数のタイプのデジタル支払いを可能とするため、複数の異なるタイプの支払端末を配置する必要があった。1つの例として、商業者は、カードを用いた支払いを受け付けるための支払端末を配備しなくてはならない。さらに、商業者は、携帯電話を介した支払いをサポートするために、更に別の端末を配備しなければならない。そのような追加的な端末が配備されたとしても、該端末は、特定のタイプの通信技術 (例えば、NFC) を用いた携帯電話しかサポートしないであろう。

【0005】

このような状況を改善するニーズが存在している。

【発明の概要】

10

20

30

40

50

【発明が解決しようとする課題】**【0006】**

第1の態様において、2つの通信プロトコルまたは通信方法の一方に対応可能なデバイスが、支払端末に近づけられた際に、通信が発生し得るよう、2つの通信プロトコルまたは通信方法に対応する信号を出力するために支払端末が用いられる。

【0007】

第2の態様において、支払端末が提供され、さらに、支払端末は、2つの異なる通信方法を用いて通信を実行可能である。使用の際、支払端末は、2つの方法の一方を用いた携帯電話や支払カードのような支払デバイスとの通信を開始するよう、双方の方法に関連する信号を出力する。2つの方法の一方によって通信が確立されると、他方の方法が終了される。

10

【0008】

第3の態様において、支払端末を操作する方法が提供される。該方法は、アクティブ化入力(activation input)を受信する工程と、それに応答して、第1のタイプの外部支払デバイスと通信を行うための第1の無線信号および第2のタイプの外部支払デバイスと通信を行うための第2の無線信号を出力する工程と、を含む。ここで、第1の無線信号および第2の無線信号は、互いに異なる第1のプロトコルおよび第2のプロトコルにそれぞれ対応するフォーマットにされている。該方法は、第1の無線信号および第2の無線信号の一方に対する返信を受信する工程と、返信に応答して、第1の無線信号および第2の無線信号の他方の出力を終了する工程と、をさらに含む。

20

【0009】

該方法は、外部支払デバイスを認証するために、返信を処理し、これにより、通信チャンネルを確立する工程をさらに含んでもよい。

【0010】

該方法は、外部支払デバイスを認証するために、返信を処理する工程をさらに含み、処理する工程の後に、終了する工程を実行する。

【0011】

第1の無線信号および第2の無線信号は、NFC信号およびブルートゥース(登録商標)信号を含んでもよい。

【0012】

該方法は、外部支払デバイスを認証するために、返信を処理し、これにより、通信チャンネルを確立する工程と、ユーザーを示すデータを通信チャンネルから受信する工程と、入力として、取引額を示すデータを受信する工程と、ユーザーを示すデータおよび取引額を示すデータを、サーバーに送信する工程と、を含んでもよい。

30

【0013】

該方法は、外部支払デバイスを認証するために、返信を処理し、これにより、通信チャンネルを確立する工程と、通信チャンネルから、ユーザーを示すデータおよび現在の取引を特定するためのワンタイム検証子(one-time verifier)を受信する工程と、入力として、取引額を示すデータを受信する工程と、ユーザーを示すデータ、ワンタイム検証子を示すデータ、および取引額を示すデータを、サーバーに送信する工程と、をさらに含んでもよい。

40

【0014】

該方法は、通信チャンネルを介して新たなワンタイム検証子を出力する工程をさらに含んでもよい。

【0015】

該方法は、応答された第1の無線信号および第2の無線信号のいずれかを示す情報をサーバーに通信する工程をさらに含んでもよい。

【0016】

第4の態様において、処理デバイスおよび命令を保存している記憶手段を有し、外部デバイスと無線通信を行うための支払端末が開示される。命令は、処理デバイスを制御し、

50

支払端末に、アクティブ化入力に応答して、第1のタイプの外部支払端末と通信を行うための第1の無線信号および第2のタイプの外部支払端末と通信を行うための第2の無線信号を出力させ、ここで、第1の無線信号および第2の無線信号は、互いに異なる第1のプロトコルおよび第2のプロトコルにそれぞれ対応したフォーマットにされており、第1の無線信号および第2の無線信号の一方に対する返信の受信に応答して、第1の無線信号および第2の無線信号の他方の出力を終了させる。

【0017】

該支払端末は、アクティブ化信号を提供するためのキーパッドと、処理デバイスの制御下において情報を表示するためのディスプレイと、サーバーと通信を行うための出力デバイスと、をさらに含んでいてもよい。

10

【0018】

支払端末は、第1の無線信号を出力するよう構成された第1の無線デバイスと、第2の無線信号を出力するよう構成された第2の無線デバイスと、をさらに含んでいてもよく、第1の無線デバイスおよび第2の無線デバイスの双方は、処理デバイスの制御下にある。

【0019】

支払端末は、セキュリティ鍵用の記憶手段を含むセキュリティデバイスをさらに含んでいてもよく、セキュリティデバイスは、支払端末による使用のために、セキュリティ鍵を用いて、データを暗号化または復号化するよう構成されている。

【0020】

パーソナルエリアネットワークデバイスは、第1の無線信号を出力するよう構成されて

20

【0021】

近距離通信デバイスは、第2の無線信号を出力するよう構成されていてもよい。

【0022】

第5の態様において、支払いを処理するためにシステムが提供される。該システムは、第1の無線通信モジュールおよび第2の無線通信モジュールを含む支払端末を含む。第1の無線通信モジュールは、第2の通信方法とは異なる第1の通信方法を用いて、近距離通信を開始および確立することができる。第2の無線通信モジュールは、第2の通信方法を用いて、近距離通信を開始および確立することができる。支払端末は、取引を開始するための入力を受信し、さらに、第1の無線通信モジュールおよび第2の無線通信モジュールに、それぞれの方法を用いて、通信を開始するよう試みさせるよう構成されている。第1の通信方法および第2の通信方法の一方によって通信可能な外部エンティティ（external entity）は、支払端末に近づけられ得、これにより、第1の無線通信モジュールと第2の無線通信モジュールのいずれが通信に成功したかに応じて、支払端末と外部エンティティとの間で通信が開始され得る。

30

【0023】

第1の無線通信モジュールは、パーソナルエリアネットワークモジュールであってもよい。第2の無線通信モジュールは、近距離通信モジュールであってもよい。支払端末は、取引が完了するまでに、第1の無線通信モジュールおよび第2の無線通信モジュールを用いた任意の他の外部エンティティとの通信チャンネルを確立する試みを終了するよう、さらに構成されていてもよい。外部エンティティは、カードおよび携帯通信デバイスの1つであってもよい。ここで、支払端末は、確立された通信が、カードの近距離通信タグ、携帯通信デバイスの近距離通信モジュール、または携帯通信デバイスのパーソナルエリアネットワークモジュールのいずれによるものであるかを特定するよう、さらに構成されていてもよい。支払端末は、確立された通信が、カードの近距離通信タグ、携帯通信デバイスの近距離通信モジュール、または携帯通信デバイスのパーソナルエリアネットワークモジュールのいずれによるものかを、サーバーに通信するよう、さらに構成されていてもよい。外部エンティティは、携帯通信デバイスであってもよい。ここで、支払端末は、携帯通信デバイスとの通信を確立する際に、少なくとも、取引に結び付けられた支払いを実行しようと試みているユーザーを特定するデータを受信し、さらに、取引を処理するた

40

50

めに、少なくとも、ユーザーを特定するデータ、商業者を特定するデータ、および支払額を特定するデータをサーバーに通信し、これにより、携帯通信デバイスが、インターネットを用いずに支払いを実行することを可能とするよう、構成されていてもよい。支払端末は、外部エンティティから、位置検証データ (location validation data) を受信し、位置検証データに基づいて、支払端末を用いた支払いが受付可能か否かを検証し、支払が受け付けられないと検証された場合には取引を拒絶し、支払が受付可能と検証された場合には、取引を処理するよう、さらに構成されていてもよい。外部エンティティは、近距離通信を確立可能なカードであってもよく、支払端末は、カードから、ユーザーを特定するデータおよびワンタイム検証子として利用されるデータを読み込み、カードに、新たなワンタイム検証子を書き込み、ユーザーを特定するデータおよびワンタイム検証子として使用されるデータをサーバーに通信するよう、さらに構成されていてもよい。ここで、ワンタイム検証子は、取引を拒絶または取引を処理するために、ワンタイム検証子が、現在の取引のために支払端末から期待されているものであるかを検証するために用いされてもよい。支払端末は、取引の度に、ユニークなワンタイム識別子をサーバーに通信するよう、さらに構成されていてもよい。外部エンティティは、携帯通信デバイスであってもよく、支払端末は、携帯通信デバイスから、ユーザーを特定するデータおよびワンタイム検証子として使用されるデータを受信し、携帯通信デバイス内の新たなワンタイム検証子を更新し、ユーザーを特定するデータおよびワンタイム検証子として利用されるデータを、サーバーに通信するよう、構成されていてもよい。ここで、ワンタイム検証子は、取引を拒絶または取引を処理するために、ワンタイム検証子が、現在の取引のために携帯通信デバイスから期待されているものであるかを検証するために用いられる。

10

20

30

40

50

【0024】

他の態様において、方法が、支払いを処理するために提供される。該方法は、支払端末において、取引を開始するための入力を受信する工程を含む。その後、支払端末内に設けられた、第1の無線通信モジュールおよび第2の無線通信モジュールは、外部エンティティとの通信チャネルを確立するよう試みる。第1の無線通信モジュールは、第2の通信チャネルと異なる第1の通信チャネルを用いて、近距離通信を確立することができる。第2の無線通信モジュールは、第2の無線通信チャネルを用いて通信を確立することができる。さらに、該方法は、第1の無線通信モジュールおよび第2の無線通信モジュールのいずれが外部エンティティとの通信チャネルの確立に成功したかに基づいて、第1の無線通信モジュールおよび第2の無線通信モジュールの一方を用いて、外部エンティティとの通信チャネルを確立する工程を、さらに含む。

【0025】

さらに別の態様において、システムが、支払いを処理するために提供される。該システムは、パーソナルエリアネットワーク (PAN) モジュールを含む支払端末を含んでいる。支払端末は、PANモジュールに、識別子 (identifier) をブロードキャストさせるよう構成されている。システムは、携帯通信デバイスをさらに含む。デバイスは、支払端末によってブロードキャストされた識別子を受信し、ブロードキャストされた識別子の信号強度が第1のしきい値を超える場合に、支払端末のPANモジュールとの通信チャネルを確立するためのリクエストを自動的に送信し、さらに、通信チャネルが確立されると、デバイスと支払端末のPANモジュールとの間の信号強度が第1のしきい値を下回ったとしても、取引が完了するまで、支払端末のPANモジュールとの通信を維持し続けるよう、構成されている。

【0026】

さらに別の態様において、方法が、支払いを処理するために提供される。該方法は、支払端末のパーソナルエリアネットワークモジュールによって、識別子をブロードキャストする工程と、携帯通信デバイスによって、支払端末によってブロードキャストされた識別子を受信する工程と、携帯通信デバイスによって、ブロードキャストされた識別子の信号強度が第1のしきい値を超える場合、支払端末のパーソナルエリアネットワークモジュールとの通信チャネルを確立するためのリクエストを自動的に送信する工程と、を含む。

該方法は、通信チャンネルが確立されると、携帯通信デバイスと支払端末のパーソナルエリアネットワークモジュールとの間の信号強度が第1のしきい値を下回ったとしても、取引が完了するまで、携帯通信デバイスと支払端末のパーソナルエリアネットワークモジュールとの間の通信を維持する工程を、さらに含む。

【0027】

また、支払いを処理するためのシステムが開示される。該システムは、パーソナルエリアネットワークモジュールを含む支払端末を含む。ここで、支払端末は、パーソナルエリアネットワークモジュールに、識別子をブロードキャストさせるよう構成されている。携帯通信デバイスは、支払端末によってブロードキャストされた識別子を受信し、ブロードキャストされた識別子の信号強度が第1のしきい値を超える場合、支払端末のパーソナル

10

【0028】

第1のしきい値は、携帯通信デバイスおよび支払端末が、互いに20センチメートル以内に位置している際に、通信チャンネルを確立するよう設定されていてもよい。第1のしきい値は、携帯通信デバイスおよび支払端末が、互いに10センチメートル以内に位置している際に、通信チャンネルを確立するよう設定されていてもよい。

20

【0029】

第1のしきい値は、互いに事前設定された距離以内に位置している場合に、通信チャンネルを確立するよう構成されていてもよい。

【0030】

支払端末および携帯通信デバイスの少なくとも1つは、携帯通信デバイスと支払端末のパーソナルエリアネットワークモジュールとの間の信号強度が第2のしきい値を下回った場合、確立された通信チャンネルを終了させるよう、さらに構成されていてもよい。

【0031】

第2のしきい値は、遠隔で、再設定可能であってもよい。

【0032】

支払端末は、通信チャンネルを確立する際に、少なくとも、取引に結び付けられた支払いを実行しようと試みるユーザーを特定するデータを受信し、取引を処理するために、少なくとも、ユーザーを特定するデータ、商業者を特定するデータ、および支払額を特定するデータを、サーバーに通信することにより、携帯通信デバイスがインターネットを用いない支払いを実行することを可能とするよう、構成されていてもよい。

30

【0033】

支払端末は、サーバーから、携帯通信デバイスを用いて支払いを実行するユーザーの口座残高に対応するデータを受信し、さらに、通信チャンネルを介して、口座残高に対応するデータを、携帯通信デバイスへ通信するよう、さらに構成されていてもよい。

【0034】

支払端末は、サーバーから、取引情報に対応するデータを受信し、さらに、通信チャンネルを介して、少なくとも、取引情報に対応するデータの一部を、携帯通信デバイスに通信するよう、さらに構成されていてもよい。

40

【0035】

支払端末は、ユーザーの口座残高を表示することができなくともよく、さらに、携帯通信デバイスは、取引の後に、ユーザーの口座残高を表示するよう構成されていてもよい。

【0036】

識別子は、互換性 (compatibility) を特定するデータを含んでいてもよい。ここで、携帯通信デバイスは、携帯通信デバイスによって受信された識別子が互換性を特定するデータを含んでいる場合、通信チャンネルを確立することを自動的にリクエストするために

50

、支払端末を考慮 (consider) するよう構成されている。

【0037】

支払端末は、転送される額を示す入力を受信し、額を示す入力を受信された後に、識別子のブロードキャストを開始するための入力を受信し、さらに、通信チャンネルが確立されると、支払端末に接続された商業者および額に対応するデータを、携帯通信デバイスへ通信するよう、構成されていてもよい。ここで、額および商業者に対応する情報は、携帯通信デバイス上に表示される。

【0038】

第1のしきい値は、遠隔で、再設定可能であってもよい。

【0039】

パーソナルエリアネットワークモジュールは、ブルートゥース (登録商標) ローエナジーモジュールまたはブルートゥースモジュールのいずれであってもよい。

【0040】

また、支払いを処理するための方法が開示される。該方法は、支払端末のパーソナルエリアネットワークモジュールによって、識別子をブロードキャストする工程と、携帯通信デバイスによって、支払端末によってブロードキャストされた識別子を受信する工程と、携帯通信デバイスによって、ブロードキャストされた識別子の信号強度が第1のしきい値を超える場合、支払端末のパーソナルエリアネットワークモジュールとの通信チャンネルを確立するためのリクエストを自動的に送信する工程と、通信チャンネルが確立されると、携帯通信デバイスと支払端末のパーソナルエリアネットワークモジュールとの間の信号強度が第1のしきい値を下回ったとしても、取引が完了するまで、携帯通信デバイスと支払端末のパーソナルエリアネットワークモジュールとの間の通信を維持する工程と、を含む。

【図面の簡単な説明】

【0041】

添付の各種図面において、各図は以下の通りである。

【図1】図1は、支払いを処理するためのシステム100を示している。

【図2】図2は、システム100の支払端末102のブロック図である。

【図3A】図3Aは、システム100による支払いを処理する例示的な方法のフローチャートである。

【図3B】図3Bは、システム100による支払いを処理する例示的な方法のフローチャートである。

【図3C】図3Cは、システム100による支払いを処理する例示的な方法のフローチャートである。

【図3D】図3Dは、システム100による支払いを処理する例示的な方法のフローチャートである。

【図3E】図3Eは、システム100による支払いを処理する例示的な方法のフローチャートである。

【図3F】図3Fは、システム100による支払いを処理する例示的な方法のフローチャートである。

【図4A】図4Aは、支払端末102に入力された額を示している。

【図4B】図4Bは、支払を実行するために、ユーザーによって開かれるスマートフォン104bのアプリケーションのユーザーインターフェースを示している。

【図4C】図4Cは、支払端末102をサーチするスマートフォン104bのアプリケーションのユーザーインターフェースを示している。

【図4D】図4Dは、スマートフォン104bが支払端末102に近づけられた後、BLEチャンネルを介して、支払端末102とペアリングされたスマートフォン104bを示している。

【図4E】図4Eは、ユーザーが支払いを承認するための入力を提供しているスマートフォン104bのアプリケーションのインターフェースを示している。

10

20

30

40

50

【図 4 F】図 4 F は、取引が処理されていることを示す、スマートフォン 1 0 4 b のアプリケーションのユーザーインターフェースを示している。

【図 4 G】図 4 G は、取引が成功した後に取引情報が表示される、スマートフォン 1 0 4 b のアプリケーションのユーザーインターフェースを示している。

【図 5 A】図 5 A は、例示的な取引パケットの高次概略図を示している。

【図 5 B】図 5 B は、別の取引パケットを示している。

【図 6】図 6 は、支払端末へのいくつかの接続がどのようにして実行されるかを示す、支払端末の実施形態のブロック概略図である。

【発明を実施するための形態】

【0042】

以下の説明において、電話またはスマートフォンに対する参照は、特定のタイプの携帯通信デバイスに対する参照に限定する意図はなく、該用語は、利便性のために用いられるものであって、本発明は、任意のタイプの携帯通信デバイスをカバーするものである。

【0043】

支払を実行するユーザーが、インターネットの使用を必要とせずに、支払を処理することができるシステムが開示される。支払いは、例えば、近距離通信（NFC）対応カード、または、NFC若しくはブルートゥースローエナジー（BLE）技術を用いるスマートフォンを用いて実行され得る。

【0044】

支払いは、商業者の位置（merchant location）に配備されている支払端末によって容易とされる。支払端末は、パーソナルエリアネットワークモジュール（BLEモジュール）と、NFCモジュールと、を備えていてもよい。1つの実施形態において、取引開始の際、支払端末は、BLEおよびNFCの双方を同時に使用して、支払を実行する消費者/ユーザーによって提供される外部エンティティーとの通信を開始することを試みるよう構成されている。外部エンティティーは、NFC対応カード、または、支払端末と取引するためのアプリケーションがインストールされているNFC若しくはブルートゥースローエナジー（BLE）技術を用いるスマートフォンであり得る。

【0045】

別の実施形態において、取引端末は、所定の時間の間、BLEおよびNFCの一方を試し、その後、成功しなかった場合には、BLEおよびNFCの他方を試し、さらに、必要であれば、BLEおよびNFCの双方の試みを交互に繰り返すよう構成されている。

【0046】

実施形態の1つにおいて、支払端末が、BLEおよびNFCの一方を介して、外部エンティティーとの通信チャンネルを確立することに成功すると、支払端末は、開始された取引が完了するまで、他方の技術（任意の他の外部エンティティーとの通信を確立する試みを）を無効化するよう構成されている。

【0047】

別の実施形態において、支払端末は、2つの出力の他方に返信する信号を検出するとすぐに、2つの出力の一方の発信を中止する。これにより、端末を駆動するバッテリーのバッテリーパワーを節約することができる。

【0048】

実施形態の1つにおいて、支払端末との通信チャンネルは、NFCを介して確立される。ここで、ユーザーは、カードまたはNFC対応スマートフォンを、支払端末に近づける。支払端末は、電話のカード/NFCモジュールからデータを読み出し、開始された支払取引を処理するために、それを、バックエンドサーバーに通信する。ここで、商業者は、使用される通信手段がどのようなものであるかについて、支払端末に指示を出さず、むしろ、支払端末が自動的に、自身で判断することに留意されたい。

【0049】

実施形態の1つにおいて、支払端末との通信チャンネルは、BLEを介して確立される。ここで、ユーザーは、BLE対応スマートフォンを、支払端末に近づける。支払端末は

10

20

30

40

50

、電話のBLEモジュールからデータを受信し、開始された支払取引を処理するために、それを、バックエンドサーバーに通信する。このケースにおいても、商業者は、使用される通信手段がどのようなものであるかについて、支払端末に指示を出さず、むしろ、支払端末が自動的に、自身で判断することに留意されたい。

【0050】

BLEの場合、支払端末は、ユーザーの口座内の差し引き額や残高のような、(バックエンドサーバーから受信される)取引情報を、BLEを介して確立された通信チャンネルを介して、ユーザーのスマートフォンに通信する。よって、ユーザーは、インターネットを用いることなく、または、SMS若しくは類似の代替物に依存することなく、支払を実行することが可能というだけでなく、取引および口座についての更新を入手することができる。

10

【0051】

図1を参照し、支払いを処理するためのシステム100は、NFC対応カード104aや携帯通信デバイス104bのような外部エンティティを介して支払いを受信可能な支払端末102を有している。支払端末102は、使用の際に、通信ネットワーク108を介して、サーバー106と通信を行う。

【0052】

支払端末102は、演算デバイスの中でも特に、例えば、カードリーダー、スマートフォン、POSシステム、タブレット、ファブレット、コンピューター、ラップトップコンピューターであってもよい。

20

【0053】

ここで、図2を参照し、支払端末102の実施形態は、処理モジュール202と、メモリーモジュール204と、入力モジュール206と、出力モジュール208と、WiFiモジュール210と、通信モジュール212と、セキュリティモジュール213と、第1の無線通信モジュール214と、第2の無線通信モジュール216と、を備えている。メモリーモジュール204は、バスに接続されており、バスは、メモリーモジュール204を処理モジュール202に接続している。処理モジュール202は、バス123によって他の全てのモジュールに接続されている。処理モジュール202は、メモリー204内に保存されている実行可能命令の制御下において動作し、支払端末102の機能を実行し、さらに、一般的に、デバイスの他のモジュールを呼び出し(コールし)、他のモジュールの機能を実行する。

30

【0054】

ここで、図6を参照し、本実施形態において、入力モジュール206は、キーパッド601およびスタイラスペン603に接続されている。出力モジュール208は、ディスプレイスクリーン605およびプリンター607に接続されている。WiFiモジュールは、無線接続を介して、サーバー106に接続されているよう示されており、通信モジュール212は、有線接続を介して、サーバー106に接続されるよう示されている。使用の際、おそらく、サーバー106に対する複数の接続の1つのみが採用されることになるであろうことは、理解されるであろう。第1の無線通信モジュール214は、NFCアンテナに接続されており、第2の無線通信モジュールは、Bluetoothアンテナ611に接続されている。いくつかの実施形態において、アンテナは、それぞれの無線通信モジュールに組み込まれている。

40

【0055】

図2に戻り、処理モジュール202は、1つ以上のプロセッサの形態で実施されており、さらに、ハードウェア、コンピューター実行可能命令、ファームウェア、またはこれらの組み合わせで、適切に実施されていてもよい。処理モジュール202のコンピューター実行可能命令またはファームウェア実施は、様々な記述される機能を実行するために、任意の好適なプログラム言語によって記載されたコンピューター実行可能またはマシーン実行可能命令を含んでいてもよい。

【0056】

50

実施形態の1つにおいて、メモリーモジュール204は、ハードディスクドライブ、eMMC、SSD、またはEEPROMのような永続メモリー(permanent memory)を含む。メモリーモジュールは、プロセッサ202によって実行される実行可能プログラム命令およびデータを保存するよう構成されていてもよい。メモリーモジュール204は、一次および二次メモリーの形態で実施されていてもよく、一次メモリーはハードワイヤードメモリーであり、二次メモリーは、SDカードのような取り外し可能メモリーである。メモリーモジュール204は、プロセッサ202がロード可能および実行可能な、追加的なデータおよびプログラム命令と、これらプログラムの実行中に生成されるデータを保存していてもよい。さらに、メモリーモジュール204は、ランダムアクセスメモリーおよび/またはディスクドライブのような揮発性メモリー、または、非揮発性メモリーであつてもよい。メモリーモジュール204は、コンパクトフラッシュ(登録商標)カード、メモリースティック、スマートメディア、マルチメディアカード、セキュアデジタルメモリー、または任意の他のメモリーストレージのような取り外し可能メモリーを含んでいてもよい。

10

【0057】

現在説明されている実施形態において、入力モジュール206は、入力デバイスの中でも特に、キーボード、タッチスクリーン、マウス、マイク、およびスタイラスペンのような入力デバイスのためのインターフェースを提供する。出力モジュール208は、特に、ディスプレイスクリーン、スピーカー、プリンター、触覚フィードバックデバイスのような出力デバイスのためのインターフェースを提供する。

20

【0058】

現在説明されている実施形態において、入力モジュール206および出力モジュール208は、支払端末102との間でデータを交換するためにも用いられ、さらに、NFC対応カード104a、携帯通信デバイス104bから端末によって導出されたデータを、サーバー106と交換するためにも用いられる。

【0059】

実施形態の1つにおいて、WiFiモジュールは、通信ネットワーク108を介して、サーバー106と通信を行うために、支払端末102によって用いられる。

【0060】

実施形態の1つにおいて、通信モジュール212は、通信ネットワーク108を介して、サーバー106と通信を行うために、支払端末102によって用いられる。実施形態の1つにおいて、通信モジュール212は、GPRSモジュールである。他の実施形態において、電気通信を可能とする他のモジュールが採用される。

30

【0061】

複数の実施形態において、通信モジュール212は、特に、モデム、ネットワークインターフェースカード(イーサネット(登録商標)カード等)、通信ポート、またはPCメモリーカード国際協会(PCMCIA)スロットを備えている。実施形態の1つにおいて、通信モジュール212は、有線プロトコルおよび無線プロトコルの双方をサポートするデバイスを備えている。実施形態の1つにおいて、電気信号の形態のデータは、通信モジュール212を介して、送信される。他の実施例において、信号の中でも特に、1つ以上の電磁気的信号、光学的信号が用いられる。

40

【0062】

実施形態の1つにおいて、支払端末は、デジタル鍵を用いて、端末102と外部エンティティ104との間で交換されるデータを、暗号化、復号化および認証する。本実施形態における鍵は、セキュリティモジュール213に保持されている。このセキュリティモジュールは、デバイスによって使用される全ての鍵を収納しており、ワンタイムライトオンリーデバイス(one-time write only device)である。鍵は、セキュアな環境において、セキュリティモジュール213内に書き込まれる。セキュリティモジュール213は、モジュールから鍵を直接読み出すことができないように、設計されている。暗号化が要求されている場合、データがセキュリティモジュール213内に送り出され、次に、鍵を用

50

いて処理した後に、暗号化されたデータが返される。セキュリティモジュール213の鍵に直接アクセスする方法は存在せず、これにより、鍵の安全性が保証される。同様に、データを復号化する際、データがセキュリティモジュール213内に送り出され、鍵を用いてデータを処理し、復号化されたデータが返される。

【0063】

セキュリティモジュール213は、ソフトウェア、ファームウェア、ハードウェア、またはこれらの組み合わせの形態で配備されていてもよい。

【0064】

実施形態の1つにおいて、第1の無線通信モジュール214は、パーソナルエリアネットワークモジュール（以下、PANモジュールと称する）である。現在説明されている実施形態において、PANモジュールは、ブルートゥースローエネルギー（BLE）モジュールである。他の実施形態において、現在の文脈におけるBLEと同様の技術が用いられてもよい。

10

【0065】

実施形態の1つにおいて、第2の無線通信モジュール216は、近距離通信モジュール（以下、NFCモジュールと称する）である。他の実施例において、現在の文脈におけるNFCと同様の技術が用いられてもよい。

【0066】

したがって、支払端末102は、第2の通信チャンネルまたはプロトコル（例えば、NFC）と異なる第1の通信チャンネルまたはプロトコル（例えば、BLE）を用いて、外部エンティティ104と近距離通信を確立することができる第1の無線通信モジュール214と、第2の通信チャンネルまたはプロトコルを用いて通信を確立可能な第2の無線通信モジュール216と、を有していることに、留意されたい。

20

【0067】

以下、図2から6を参照して、動作中における支払端末の実施形態の高いレベルの説明がなされる。

【0068】

最初に、処理モジュール202のプロセッサが、待機状態にあり、さらに、本実施形態では、2つの無線通信モジュール214、216もまた待機している。端末は、キートン601から入力モジュール206への入力によって「立ち上げ」られ、バス123を介して、処理モジュール202の待機プロセスを中断する。処理モジュールは、バス123を介して、メモリーモジュール204から命令を取り出し、これを処理し、バス123を介して、第1および第2の無線通信モジュール214、216に出力を提供し、これにより、第1および第2の無線通信モジュール214、216が、自身のそれぞれの問い合わせ信号、すなわち、BLEおよびNFC信号をそれぞれ発信することを開始し、外部デバイス104を探し出す。問い合わせ信号は、それぞれのアンテナ609、611を介して、外部に送信される。

30

【0069】

2つのアンテナ609、611の一方によって、2つの問い合わせ信号の一方に対する応答が受信されると、対応する無線通信モジュールは、バス123を介して、処理モジュール202を呼び出し、処理モジュール202は、メモリーモジュール204内に保存されている命令に基づいて、他方の無線通信モジュールに、自身の問い合わせ信号の発信を停止するよう、命令する。簡潔性のため、第1の無線通信モジュールを想定し、BLEモジュール214は、応答を受信し、よって、第2の無線通信モジュール216は、待機状態に入るよう、命令される。

40

【0070】

アンテナ609を介して外部デバイス104から受信されたデータは、バス123に沿って、セキュリティモジュール213へ送られる。本明細書において別の箇所でも述べたように、セキュリティモジュール213は、内部に保存されたデジタル鍵を用いて、処理モジュール202の制御下において該データを復号化する。これにより、支払端末が、外部

50

デバイス104（例えば、電話のアプリケーションまたはカード）を認証することが可能となる。適切であれば、認証が実行された後、いくつかの情報がスクリーン605に送信され、例えば、ユーザー/商業者に、「額を入力して下さい」、「pinを入力して下さい」等の動作を実行する指示を表示する。

【0071】

そのような任意の指示に対する応答、例えば、キーパッド601に対してなされた入力が、入力モジュール206によって受信される。その後、この応答が処理モジュール202によって処理され、処理の結果に応じて、より多くの情報がスクリーン605に表示され、さらなる指示および応答を促す、または、取引情報が、サーバー106に送信するのに十分となる。

【0072】

その後、処理モジュール202は、Wi-Fiモジュール210および通信モジュール212の一方に、端末102によって受信および処理されたデータに基づいて、サーバー106と相互通信するよう、指示する。

【0073】

端末102から受信されたデータに回答して、サーバー106は、Wi-Fiモジュール210および通信モジュール212の一方を介して、データを返す。このデータは、バス123を介して、処理モジュール202によって処理され、データから導出された情報が適切であれば、出力モジュール208を介して、ディスプレイスクリーン605および/またはプリンター607に表示される。

【0074】

取引の終了時に、処理モジュールは、自身の待機状態に戻る。

【0075】

取引の処理の間のいくつかの時点で、端末102は、外部デバイス104に、データ、典型的には、セキュリティモジュール213内に保存されている鍵によって暗号化されたデータを送信してもよい。別の箇所で述べたように、外部デバイスに送信されるデータは、例えば、セキュリティ目的のためのワンタイムコードを含んでいてもよい。

【0076】

図3A～3Fにおいて、サーバー106、外部エンティティ104（外部エンティティ104a、104bのタイプは、本明細書のより容易な読解を助けるため、いくつかの例において、外部エンティティ104と称される）、および支払端末102の1つの実施形態によって実行されるタスクが述べられる。

【0077】

工程302において、支払端末102は、請求されるべき額を示す入力を受信する。1つの例として、商業者は、支払端末102に設けられた、物理またはデジタルキーパッドを用いて、請求されるべき額を示す入力を受信する。1つの例として、図4Aを参照し、商業者は、ユーザー/顧客から受け取ろうとしている350Rs（ルピー）の額を入力する。

【0078】

工程304において、支払端末102は、外部エンティティ104との取引を開始するための入力を受信する。1つの例として、再度図4Aを参照し、額を入力した後、支払端末102のユーザーは、リターンキーを押し、即時入力（インスタント入力）を提供する。リターンキーの押下は、前の工程において述べられた額、および、現在の工程において述べられている入力の確認（承認）として解釈され得ることに留意すべきである。

【0079】

工程306において、開始入力に回答して、支払端末102（例えば、支払端末102の処理モジュール202）は、第1の無線通信モジュール214（以下、本明細書のより容易な読解を助けるため、BLEモジュール214と称される）および第2の無線通信モジュール216（以下、本明細書のより容易な読解を助けるため、NFCモジュール216と称される）に、外部エンティティ104との通信を確立するよう試みさせる。1つ

10

20

30

40

50

の例として、モジュール 2 1 4、2 1 6 の双方は、開始入力に応答して切り替えられてもよく、その後、通信チャンネルを確立するよう試みる。代替的に、モジュール 2 1 4、2 1 6 の双方が、既にオン（オンであるが、スリープ」または「省エネ」モード）であってもよく、この場合、起動および外部エンティティ 1 0 4 との通信チャンネルの確立を試みる。

【 0 0 8 0 】

工程 3 0 8 において、BLE モジュール 2 1 4 および NFC モジュール 2 1 6 の双方は、通信チャンネルを確立するよう試みる。1 つの例として、BLE モジュール 2 1 4 の場合、BLE モジュール 2 1 4 は、自身の識別子のブロードキャストを開始してもよい。一方、NFC モジュール 2 1 6 の場合、NFC モジュール 2 1 6 は、電磁場を生成する。商業者は、モジュール 2 1 4、2 1 6 のいずれが使用されるべきであるかを指定することはなく、むしろ、支払端末 1 0 2 がモジュール 2 1 4、2 1 6 の双方を用いて、通信チャンネルの確立を試み、その後、認証の後、モジュール 2 1 4、2 1 6 の適切な一方を用いて通信チャンネルを確立するよう構成されていることに、留意されたい。

10

【 0 0 8 1 】

図 3 B 中の工程 3 1 0 を参照し、留意すべきことは、外部エンティティ 1 0 4 が NFC または BLE 対応であるかを、外部エンティティ 1 0 4 が判断していると思われる場合であっても、工程 3 1 0 は、説明の目的のためだけで提供されていることは、よく理解されるであろう。上述のように、外部エンティティ 1 0 4 が、BLE または NFC 能力の 1 つ以上を有する NFC 対応カード 1 0 4 a（クレジットカード、デビットカード、アクセスカード、コーポレートカード、フードカード）または携帯通信デバイス 1 0 4 b（例えば、スマートフォン）であってもよいことは適切に理解されるであろう。以下、BLE 対応携帯通信デバイス 1 0 4 b の場合の取引フローを説明する。ここで、外部エンティティ 1 0 4 が NFC 対応カード 1 0 4 a または NFC 対応携帯通信デバイス 1 0 4 b である状況について説明する。NFC および BLE 能力を有する携帯通信デバイス 1 0 4 b の場合、これらの一方が初期アプリケーション設定、アプリケーションのユーザー規定設定、または、モジュールの可用性（availability）として規定および用いられてもよいことに、留意されたい。

20

【 0 0 8 2 】

工程 3 1 2 を参照すると、外部エンティティ 1 0 4 は、検出のために、支払端末 1 0 2 に近接する。1 つの例として、商業者が、支払受付の準備が出来ている支払端末 1 0 2 を有していると、ユーザー/顧客は、NFC カード 1 0 4 a または NFC デバイス 1 0 4 b を、（NFC が要求する範囲まで）支払端末 1 0 2 に近づける。

30

【 0 0 8 3 】

説明の目的のため、いくつかの実施形態において、NFC カード/デバイス 1 0 4 a、1 0 4 b は、実施形態の支払端末 1 0 2 のみが、実施形態の NFC カード/デバイスと正確に相互通信可能なように、暗号化されたデータを送信する。これは、カード/デバイスの「ロック（locking）」として知られる現象を生じさせる。

【 0 0 8 4 】

工程 3 1 4 を参照し、支払端末 1 0 2 は、外部エンティティ 1 0 4 を検出し、外部エンティティ 1 0 4 を認証することによって、外部エンティティ 1 0 4 のロックを解除することを試みる。認証が成功すると、通信チャンネルが確立される。すなわち、認証が成功した後にのみ、取引データが送信されることになる。

40

【 0 0 8 5 】

その後、NFC カード 1 0 4 a または NFC デバイス 1 0 4 b を検出した後、支払端末 1 0 2 は、通信モジュール 2 1 4、2 1 6 のいずれが外部エンティティ 1 0 4 との通信チャンネルの起動に成功したかに基づいて、第 1 の無線通信モジュール 2 1 4 および第 2 の無線通信モジュール 2 1 6 の一方を用いて、外部エンティティ 1 0 4 との通信チャンネルを確立する。このケースでは、支払端末 1 0 2 は、第 2 の無線通信モジュール 2 1 6（NFC モジュール 2 1 6）を用いて、外部エンティティ 1 0 4 との通信チャンネルを

50

確立している。よって、確立された通信チャンネルは、NFCチャンネルと称されてもよい。

【0086】

本実施形態において、BLEおよびNFC信号の一方に対する応答が受信されると、支払端末102は、該取引が完了するまで、第1の無線通信モジュール214および第2の無線通信モジュール216を用いた任意の他の外部エンティティーとの通信チャンネルを確立する任意の試みを終了する。

【0087】

別の実施形態において、通信チャンネルを確立する際に、支払端末からの出力信号に対する応答を受信するだけでなく、外部デバイスを認証した際に、データ通信を開始してもよく、支払端末は、現在の取引が完了するまで、他方のモジュール、すなわち、応答がない通信モジュールの更なる出力を終了する。

10

【0088】

確立されたNFCチャンネルを用いて、支払端末102は、外部エンティティー104と連携して、外部エンティティー104のロックを解除する。カード/デバイスレベルおよび支払端末102において配備される既知の（または、将来において開発されるであろう）セキュリティ技術が、NFCカード104aまたはNFCデバイス104bのロックを解除するため用いられてもよい。支払端末102がロックを解除することに失敗した場合、その後、本実施形態では、取引が終了される（取引が完了する）。

【0089】

工程316を参照し、ロック解除が成功すると、支払端末102は、カードメモリからユーザトークンを読み出す。ユーザトークンは、クレジットカードのカード番号と同様に、取引に結び付けられた支払いを実行しようとするユーザーを特定するデータである。

20

【0090】

実施形態の1つにおいて、ユーザトークンの読み出しに加えて、外部エンティティー104は、ワンタイム検証子として使用されるデータを保存している。この実施形態において、保存されているワンタイム検証子もまた、セキュリティを向上させるために、支払端末102によって読み出される。

【0091】

ワンタイム検証子は、試みられている各取引にユニークなデータとして理解可能である。NFCカード104aの場合、取引を処理するために支払端末102によって既存のワンタイム検証子が読み出される度に、新たなワンタイム検証子が、カード104aに書き込まれてもよいことに、留意されたい。さらに、いくつかのスマートフォンは、このデータをNFCモジュールに書き込むことを許可しておらず、この場合、前述の例において実施されているようには、ワンタイム検証子の提供が行われないうちに、留意されたい。

30

【0092】

説明のため、図5Aを参照し、取引データパケット500は、典型的には、顧客トークン501と、顧客識別子(customer identifier)503と、取引額505と、商業者ID507と、を含む。ユーザーが端末において請求を支払うまたは支払おうと試みた際に、ハッカーがデータを傍受することができる場合、ハッカーは、同じ端末で、同じ額を何回も支払いを実行することが可能である。これは、「リプレイアタック」と称されることもある。そのため、本物の取引とリプレイアタックとを区別可能なものとするのが望ましい。

40

【0093】

本実施形態において、「リプレイアタック」を検知するためにセーフティー機構が所定の位置に存在している。リプレイアタックにおいて、ハッカーは、2つのデバイス間で交換されているデータを傍受し、同じものを何回もリプレイする。システムが、そのようなアタックを検知および警告を出すことを可能とするために、毎回、何か新しいものをデータパケットに導入する必要がある。本実施形態において、図5Bに示されているように、

50

(a) 各取引後にカードのカウンターを保持およびインクリメントすること、および (b) データパケットの一部として、支払デバイスにタイムスタンプを送信すること、の一方または双方によって達成される。

【 0 0 9 4 】

よって、本実施形態のパケット 5 2 0 は、顧客トークン 5 0 1、顧客識別子 5 0 3、取引額 5 0 5、および商業者 ID 5 0 7 だけでなく、カード/デバイスに保存されたカウンター数 5 0 9 および取引のタイムスタンプ 5 1 1 を含んでいる。

【 0 0 9 5 】

実施形態の 1 つにおいて、NFC カード 1 0 4 a または携帯デバイス 1 0 4 b の NFC モジュールから読み出されたデータ (または、BLE を介して通信されたデータ) は、支払端末 1 0 2 が、データが NFC カード 1 0 4 a または携帯デバイス 1 0 4 b の NFC モジュール (または、携帯デバイスの BLE を介して) のいずれから収集されたのかを特定することを可能とするデータを含んでいる。したがって、支払端末 1 0 2 (または、サーバー 1 0 6、または双方) は、確立された通信が、カード 1 0 4 a の近距離通信タグ、携帯通信デバイス 1 0 4 b の近距離通信モジュール、または携帯通信デバイス 1 0 4 b のパーソナルエリアネットワークモジュール 2 1 4 のいずれによって確立されたかを特定することができる。このような提供は、サーバー 1 0 6 が取引を処理するのに必要なデータセットを確立することを可能とすることに、留意されたい。1 つの例として、NFC カード 1 0 4 a の場合、ワンタイム検証子が必要とされる一方、携帯デバイス 1 0 4 b の NFC モジュールの場合、ワンタイム検証子は、取引を処理するために、(上述の制約のために) 必要とされなくともよい。

【 0 0 9 6 】

実施形態の 1 つにおいて、NFC カード/デバイス 1 0 4 a から読み出された、または、BLE を介して受信されたデータは、位置検証データを含んでいる。換言すれば、支払端末 1 0 2 は、外部エンティティ 1 0 4 から位置検証データを受信する。位置検証データは、支払端末 1 0 2 を用いた支払いが受付可能かを検証するために用いられる。

【 0 0 9 7 】

実施形態の 1 つにおいて、データは、外部エンティティ 1 0 4 (例えば、カード 1 0 4 a) に書き込まれ、端末は、端末が関心の場所にある場合を除いて、該コードを送信するカードを拒絶するよう設定されている。支払デバイスが唯一つの企業からの支払いを受け付けることを期待されている、会社内の社員食堂のような完全にクローズドな一括 (グループ) 支払環境において、請求は、支払デバイスレベルにおいてローカルに実行される。デバイスが、特定の識別子 (企業を特定するもの) が付されている顧客カードを発見できない場合には、取引は直ちに拒絶される。サーバー呼び出しは、必要とされない。

【 0 0 9 8 】

支払いが受け付けられないと判断された場合、その後、取引が拒絶される。他方、支払いが受け付け可能であると検証された場合、その後、取引が処理される。説明されている検証は、支払端末 1 0 2 によって実行されてもよい。

【 0 0 9 9 】

代替的に、検証は、サーバー 1 0 6、または双方によって実行されてもよい。

【 0 1 0 0 】

支払デバイスが一般的な小売店に位置している別のケースにおいて、請求は、サーバー 1 0 6 において生じる。また、顧客識別子は、サーバーに送信されるデータパケットの一部である。バックエンドにおいて、特定の顧客識別子を有する顧客が、特定の場所 (例えば、リコールされる商業者 ID 5 0 7 (取引データパケットの一部でもある) によって特定された場所) において支払いを行うことを禁止する規則が設定されている。

【 0 1 0 1 】

実施例の 1 つとして、企業は、自身の敷地内に配備されたフードコート内で使用するための NFC カード 1 0 4 a を、自身の従業員に発行していてもよい。敷地外の支払端末 1 0 2 において、支払いを実行するためにカード 1 0 4 a が用いられた場合、支払端末 1 0

10

20

30

40

50

2 (または、サーバー 106) は、位置検証データを読み込んだ際、取引を拒絶してもよい。

【0102】

ここで、工程 318 を参照し、支払端末 102 は、新たなワンタイム検証子を、外部エンティティ 104 に書き込む。1つの例として、新たなワンタイム検証子は、NFCカード 104a に書き込まれる。実施形態の1つにおいて、携帯デバイス 104b のNFCモジュールがそのような書き込みを許可している場合には、携帯デバイス 104b のNFCモジュールの場合であっても、新たなワンタイム検証子が、携帯デバイス 104b のNFCモジュールに書き込まれる。新たなワンタイム検証子は、次の取引に用いられる。新たなワンタイム検証子は、既存のワンタイム検証子と比較して、事前設定されたようにインクリメント/デクリメントされたものであってもよい。代替的に、ワンタイム検証子は、既存のロジックに基づいて、ランダムに生成されたコードであってもよい。実施形態の1つにおいて、新たなワンタイム検証子は、支払端末 102 によって生成される。工程 320 において、新たなワンタイム検証子は、(そのような提供がなされている場合) NFCカード 104a または携帯デバイス 104b のNFCモジュールに記録される。

10

【0103】

ワンタイム検証子は、各取引の度に、外部エンティティ 104 から収集されたデータに新しさ (freshness) を追加することに、留意するべきである。1つの例として、(従来行われているように) 一定であるユーザートークンのみが収集される場合、ユーザートークンへアクセスする不正システムは、取引を実行するためのユーザートークンを悪用することができる。

20

【0104】

工程 322 を参照すると、支払端末 102 は、ユーザートークンと、ワンタイム検証子と(存在するのであれば)、商業者IDと、端末IDと、支払端末 102 のワンタイム検証子と、ユーザーデータおよび取引情報入手のために用いられたソース(NFCカード/携帯またはBLE)と、をひとまとめにする。実施形態の1つにおいて、支払端末 102 は、同様に、新たなワンタイム検証子をひとまとめにしてもよい。外部エンティティ 104 に対応するワンタイム検証子とは別に、支払端末 102 用のワンタイム検証子が同様に存在し得ることに留意されたい。よって、支払端末 102 についての情報(例えば、商業者IDまたは端末ID)を有する不正システムは、それでも、悪用に備えた抵抗性(resistance)と共に提供され得る。実施形態の1つにおいて、ユーザーは、PINを支払端末 102 に通信し、取引を認証する必要がある。いくつかの実施形態において、PINは、特定の事前設定された額を超えた取引のためにのみ、要求されてもよい。

30

【0105】

さらに、支払端末 102 は、セキュリティ特徴を強化するために、認証およびセキュリティデータを、他のデータと共にひとまとめにしてもよい。

【0106】

工程 324 を参照し、支払端末 102 は、ひとまとめにされた情報を、サーバー 106 に送信する。支払端末 102 は、WiFiモジュール 210 を用いて、情報をサーバー 106 に送信してもよい。代替的に、支払端末 102 は、GPRSモジュールを用いて、情報をサーバー 106 に送信してもよい。代替的に、支払端末は、サーバー 106 にデータを通信する前に、セキュリティ目的のために、セキュリティモジュール 213 を用いて、ひとまとめにされたデータを暗号化してもよい。

40

【0107】

工程 326 を参照し、サーバー 106 は、支払端末 102 から、ひとまとめにされた情報を受信する。

【0108】

工程 328 を参照し、サーバー 106 は、取引を処理する。従来と異なる工程についての注目が不明確となるのを防止するため、取引の処理に含まれる従来工程については、議論しない。外部エンティティ 104 のワンタイム検証子および支払端末 102 のワン

50

タイム検証子は、支払リクエストが拒絶されるべきか、さらに処理されるべきかを判断するために用いられる。(支払端末102に対応する)ワンタイム検証子は、取引を拒絶または取引を処理するために、ワンタイム検証子が、現在の取引のために支払端末102から期待されているものであるかを検証するために用いられる。同様に、(外部エンティティ104に対応する)ワンタイム検証子は、取引を拒絶または取引を処理するために、ワンタイム検証子が、現在の取引のために外部エンティティ104から期待されているものであるかを検証するために用いられる。

【0109】

実施形態の1つにおいて、支払端末102は、外部エンティティ104に対応する新たなワンタイム検証子を、サーバー106に通信してもよく、これにより、サーバー106は、次の取引において外部エンティティ104から期待されているものを知る。

10

【0110】

実施形態の1つにおいて、外部エンティティ104または支払端末102の新たなワンタイム検証子は、前のワンタイム検証子に既知の変化が加わったものである。よって、サーバー106は、取引を拒絶または処理するために、前のワンタイム検証子を用いることにより、ワンタイム検証子を検証する必要がある。

【0111】

実施形態の1つにおいて、サーバー106は、次の取引で用いるために、新たなワンタイム検証子を支払端末102に通信する。

【0112】

期待されている外部エンティティ104からのワンタイム検証子が存在しない、または、間違っただワンタイム検証子の場合、サーバー106は、この問題が解決するまで、外部エンティティ104が、取引を実行することを阻止する。支払端末102についても同様である。

20

【0113】

工程330を参照し、サーバー106は、取引情報を支払端末102に送信する。取引情報は、成功した支払いまたは拒絶されている支払いに対応する情報を含んでもよい。また、取引情報は、他の情報の中でも特に、商業者の口座に入金されている額に対応する情報、および/または、支払いを実行したユーザー/顧客についての選択された情報を含んでもよい。

30

【0114】

工程332を参照し、支払端末102は、サーバー106から、取引情報を受信する。受信される情報のいくつかは、支払端末102によって出力(例えば、表示)されてもよい。いくつかの実施形態において、取引情報のいくつかは、支払端末102によって出力されないように防止されていてもよく、一方、そのような情報は、外部デバイス104(例えば、電話)に出力されてもよい。

【0115】

工程334を参照し、取引が完了すると、支払端末102は、次の取引(例えば、工程302から開始する)のための準備を行ってもよい。

【0116】

ここで、ブロック310を参照し、思い出してもらいたいが、ユーザー/顧客がNFCカード104aまたはNFC対応スマートフォン104bを用いて、支払いを実行することについての説明を、既に提供している。ここで、ユーザーが、BLE能力を有する携帯通信デバイス104b(例えば、スマートフォン)を用いて、支払いを実行する状況を参照する。

40

【0117】

BLEは、本発明の本質的部分ではなく、他のプロトコル、例えば、「通常の」BluetoothまたはWiFiもまた機能することは、理解されるべきである。

【0118】

ここで、図3中の一連の他の図面と併せて図3Eを参照する。上述のように、工程30

50

8を参照し、支払端末のNFCモジュール216およびBLEモジュール214の双方は、通信チャンネルを確立するよう試みてもよい。上述のように、BLEモジュール214の場合、BLEモジュール214は、自身の識別子のブロードキャストを開始してもよい。識別子は、互換性(compatibility)を特定するデータを含んでいてもよい。

【0119】

1つの例として、図3Eおよび図4Bを参照し、ユーザーは、携帯通信デバイス104b内の支払アプリケーションを開き、「今支払う(pay now)」アイコンをアクティブ化する。アプリケーションは、BLE対応スマートフォン104bのBLEモジュールに、支払端末102をサーチさせる(図4C参照)。

【0120】

複数の支払端末が存在する実施形態において、複数の支払端末は、典型的には、同じ強度で信号を発信するが、もちろん、2つの端末が、任意の特定の携帯通信デバイス(スマートフォン)から等距離にあることはあまり可能性が高くない。接続(ペアリング)の準備(readiness)を示す信号の発信は、本分野において「アドタイジング」と称されることがあり、典型的には、データの複数のパケットの発信から構成されている。用語「ペアリング」は、限定を意図するものではない。

【0121】

携帯通信デバイス(スマートフォン)において受信された信号強度は、スマートフォン、例えば、スマートフォン上において実行されているアプリケーションによって測定され、さらに、周辺において利用可能な複数の支払端末のそれぞれに対するスマートフォンの位置を判別するために用いられる。

【0122】

ペアリングの最初の工程として、図3Eの工程30において、アプリケーションは、周辺をスキャンし、自身と接続を確立可能な「適格候補(eligible candidates)」のリストを作成する。アプリケーションは、携帯通信デバイス(スマートフォン)が意図された支払端末とのペアリングのみをするよう保証するよう構成されている。例えば、商業者は、顧客に対し、アプリケーションを開き、電話を支払端末Aに近づけ、支払いを開始するよう依頼する。その後、アプリケーションが引き継ぎ、(すべての適格な支払端末のうち)どの支払端末が近くに位置しているのかを判別する。商業者は、顧客に対し、電話を支払端末Aに近づけるよう依頼しているので、アプリケーションは、支払端末Aのみが数インチしか離れておらず、一方、他のデバイスが数メートル離れていることを確認することができ、これにより、支払端末Aとのペアリングをリクエストすることができる。

【0123】

(最近接している利用可能な支払端末との接続を確立する)信号強度ロジックは、接続を確立するためだけのために用いられる。

【0124】

電話が支払端末とペアリングされ、それにより、接続を確立すると、接続は、アプリケーションが接続を切断すると決定する時点まで、アクティブ(有効)であり続ける。接続は、電話が端末から離れるように移動されたとしてもアクティブであり続け、アプリケーションは、端末とトークし続け、取引を完了させる。アプリケーションが、取引が完了したと判別すると、アプリケーションは接続を解除し、端末を解放する。

【0125】

端末は、2つの電話と同時にペアリングできないように構成されている。1つの電話が端末とペアリングまたは接続されると、該電話と端末との間の通信チャンネルが排他的なものとなる。すなわち、それ以外の電話は、端末とペアリングまたは通信することができない。端末は、該電話に対して効果的にロックされ、アプリケーションによるか、または、支払端末を物理的にリセットするかのいずれかによってのみロック解除(電話からの接続が解除)され得る。

【0126】

実施形態の1つにおいて、この「ロック」は、ペアリングが実施された際にアドタイ

10

20

30

40

50

ジングを停止するよう構成された端末によって実行される。1つの例において、スマートフォン上のアプリケーションは、アダプタイジングを停止するための命令を端末に発信する。別の実施例において、端末は、ペアリングが実行されるとすぐに、スマートフォンからの入力なしに、アダプタイジングを停止するよう構成されている。

【0127】

支払端末のプロセッサは、この命令を受信し、保存されている命令に応答して、処理を行い、自身の機能のアダプタイズを一時的に停止し、ペアリングを提供する。

【0128】

実施形態の1つにおいて、スマートフォン104bのアプリケーションは、識別子内に存在する互換性を示すデータを参照することによって、互換性のある支払端末102を探す。例えば、アダプタイジングしているいくつかのBLEまたはブルートゥースデバイスが存在し得るが、アプリケーションは、支払いを実行するために検討されている（したがって、ペアリングのためのリクエストを送信するために検討されている）支払端末102を特定することにのみ興味がある。

【0129】

ユーザーは、信号強度が第1のしきい値を超えるように、携帯電話を支払端末の近くに移動させ、図3Eの工程31において、スマートフォン104bは、ペアリングのために、リクエストを支払端末102に送信する。

【0130】

実施形態の1つにおいて、支払端末102からの信号の強度が第1のしきい値を超える場合、ペアリングのためのリクエストのみが外部に送信される。

【0131】

別の実施形態において、ユーザーが「今支払う」アイコンをアクティブ化するとすぐに、ペアリングのためのリクエストが外部に送信され、または、同様に、スマートフォンが取引を開始するよう指示される。

【0132】

さらに別の実施形態において、アプリケーションは、ペアリングが可能な1つ以上の端末の表示（指標、印）を、例えば、自身のディスプレイスクリーン上に表示し、ユーザーは、これらの1つを選択する。この選択が、ペアリングシーケンスを開始するためのリクエストを発生させる。

【0133】

1つの例として、複数の互換性のある支払端末102が商業者位置にあるものとする。スマートフォン104bのアプリケーションは、これらの支払端末102の全てを特定および候補リスト化するであろうが、ペアリングのためのリクエストを、これらのうちのどの1つに送信するかを決定しなければならない。

【0134】

実施形態の1つにおいて、単一の支払端末102が特定された状況であっても、ペアリングのためのリクエストは、信号強度が第1のしきい値を超えていないと送信されない。実際、支払いを実行するためのチャンネルとしてBLEを用いた場合であっても、ユーザー体験は、「タップおよび支払い（tap-and-pay）」に近いものとなるだろう。ユーザーは、スマートフォン104bを支払端末102に近づけ（図4D参照）、信号強度を増加させ、これにより、アプリケーションに、支払端末102とのペアリングをリクエストさせる。よって、スマートフォン104bは、ブロードキャストされた識別子の信号強度が第1のしきい値を超える場合、支払端末102のパーソナルエリアネットワークモジュール214との通信チャンネルを確立するためのリクエストを自動的に送信することは、理解されるであろう。

【0135】

第1のしきい値は、携帯通信デバイス104aおよび支払端末102が、互いに所定の距離内にあった際に、通信チャンネルを確立するよう、設定される。第1のしきい値は、ソフトウェア更新を介して遠隔に再設定可能であってもよく、または、支払い端末102

10

20

30

40

50

において設定可能であってもよい。

【0136】

実施形態の1つにおいて、第1のしきい値は、携帯通信デバイス104bおよび支払端末102が、互いに約20センチメートルの距離にあった際に、通信チャンネルを確立するよう設定されている。

【0137】

実施形態の1つにおいて、第1のしきい値は、携帯通信デバイス104bおよび支払端末102が、互いに約10センチメートルの距離にあった際に、通信チャンネルを確立するよう設定されている。

【0138】

第1のしきい値の設定に関し、ペアリングを処理するために、携帯通信デバイス104bと支払端末102との間の適切な距離を設定することができることは、理解されるであろう。

【0139】

図3Eの工程32において、支払端末102は、ペアリングのためのリクエストを受信する。支払端末102は、リクエストを受信すると、既知のプロトコルを用いて、スマートフォン104bと連携(co-ordinate)し、ペアリングを成功させるか、リクエストを拒絶するかする。ペアリングが成功した場合、支払端末102は、第1の無線通信モジュール214(BLEモジュール214)を用いて、外部エンティティー104との通信チャンネル(BLEチャンネル)を確立する。よって、確立された通信チャンネルは、BLEチャンネルと称することができる。

【0140】

通信チャンネルが確立される(ペアリングが実行される)と、スマートフォンは、スマートフォン104bと支払端末102のパーソナルエリアネットワークモジュール214との間の信号強度が第1のしきい値を下回ったとしても、支払端末102のパーソナルエリアネットワーク102との通信を維持し続ける。実際、ユーザーは、スマートフォン104bを支払端末102に近づけ、スマートフォン104bに、支払端末102とのペアリングを実行させるであろう。その後、ユーザーは、スマートフォン104bを引き戻すであろうが、通信チャンネルは維持されることとなるため、ユーザー体験を向上させ、取引処理をより信頼性の高いものとすることができる。

【0141】

実施形態の1つにおいて、支払端末102またはスマートフォン104bの少なくとも1つは、スマートフォン104bと支払端末102のパーソナルエリアネットワークモジュール214との間のチャンネル内の信号強度が第2のしきい値を下回った場合に、確立された通信チャンネルを終了するよう構成されている。第2のしきい値は制御可能であってもよい。第2のしきい値は、遠隔に再設定可能またはデバイスで再設定可能であってもよい。

【0142】

図3Eの工程33において、支払端末102は、取引情報をスマートフォン104bに送信する。情報は、BLEチャンネルを介して送信される。そのような情報は、特に、送金されるべき額および商業者情報を含んでいてもよい。

【0143】

図3Eの工程34、並びに、図4Dおよび4Eにおいて、スマートフォン104bは、支払端末102によって送信された取引情報を受信する。

【0144】

図3Eの工程3および図4Eにおいて、ユーザーは、アイコンをアクティブ化し、これにより、スマートフォン104bが、支払いの承認を送信し、さらに、取引を容易にするためのデータを通信する。なお、(NFCの文脈において述べられた関連データに加えて)通信されるデータは、リアルタイムデータを含んでいてもよい。リアルタイムデータは、時間に対応するデータを含んでいてもよい。ワンタイム検証子は、スマートフォン10

10

20

30

40

50

4 bによって生成されてもよい。また、実施形態の1つにおいて、ユーザーは、取引を許可するために、PINを通信しなければならない。いくつかの実施形態において、PINは、特定の事前設定された額を超える取引の場合のみ、要求されてもよい。

【0145】

図3Fの工程36において、支払端末102は、承認およびデータを受信し、工程32と関連して上で説明された複数の工程および後続の複数の工程が実行されてもよく、これらの工程は、このモードの取引のために適応されたものであってもよい。

【0146】

ここで、特に、工程332(図3D)、37および38(図3F)を参照し、支払端末102は、サーバー106から取引情報を受信する。上述のように、サーバー106は、受信したデータに基づいて、データがBLEチャンネルを介して支払端末102によって受信されたことを知ることに、留意されたい。よって、BLEチャンネルは、取引に対応する更新をユーザーに提供するために用いられ得る。したがって、サーバー106によって送信される典型的なデータとは別に、サーバー106は、送信を行い、支払端末102は、スマートフォン104bを用いて支払いを実行するユーザーの口座残高に対応するデータを受信する。支払端末102は、BLEチャンネルを介して、口座残高に対応するデータを、スマートフォン104bに通信する(図4G参照)。したがって、ユーザーは、インターネットを用いずに支払いを実行できるだけでなく、インターネットを用いずに取引についての更新を入手することができる。

【0147】

工程38が完了すると、スマートフォン104上で実行されているアプリケーションは、支払端末102との通信チャンネルを介してコマンドを送信する。このコマンドは、端末に、他のスマートフォンとの取引を可能とするよう、アダプタイジングを開始するよう、指示する。コマンドは、支払端末によって受信され、アダプタイジングが再開されるように、端末のメモリー内に保存されている命令に従って、支払端末の処理回路によって処理される。

【0148】

また、実施形態の1つにおいて、必要に応じて、商業者がアダプタイジングを再度可能とすることができるように、端末102は、物理リセットデバイス(例えば、リセット鍵)と共に提供されている。別の実施形態において、リセットは、遠隔に実行されてもよいが、いくつかのケースにおいて、物理リセットデバイスを用いるよりも安全性が低くなるであろう。

【0149】

リセットキーは、操作されたときに、支払端末を、アダプタイジングを開始可能な静止状態(quiescent state)で再起動させてもよいし、単純に、「アダプタイジング停止」コマンドを無効化(オーバーライド)し、処理回路に、「アダプタイジング再開」コマンドを送信してもよい。

【0150】

実施形態の1つにおいて、支払端末102は、サーバー106から、取引情報に対応するデータを受信し、さらに、通信チャンネルを介して、少なくとも、取引情報に対応するデータの一部を、スマートフォン104bに通信するよう、さらに構成されている。

【0151】

実施形態の1つにおいて、支払端末102は、ユーザーの口座残高を表示することができない。しかしながら、携帯通信デバイス104bは、取引の後、ユーザーの口座残高を表示するよう構成されている。口座残高に対応するデータは、ユーザーのスマートフォン104bのみが該データを復号化できるよう、暗号化されていてもよい。

【0152】

実施形態の態様を不必要に不明確としないために、典型的には、異なる工程で用いられる暗号化、復号化、認証、およびセキュリティ技術のいくつかは、詳述されていないことに、留意すべきである。

10

20

30

40

50

【0153】

上述の処理は、一連の工程として説明され、これは、単に説明のためのものである。したがって、いくつかの工程が追加されてもよく、いくつかの工程が省略されてもよいことは適切に理解されるであろうし、工程の順番は、変更可能であり、または、いくつかの工程は、同時に実行されてもよい。

【0154】

本明細書において開示された例示的な実施形態は、コンピューター、ハードウェア、またはソフトウェアとハードウェアの組み合わせにインストールされたソフトウェアを含む動作環境において実施され得る。

【0155】

特定の例示的な実施形態を参照して本発明の実施形態が記述されたが、本明細書において記述されたシステムおよび方法のより広い原理および範囲から逸脱することなく、これら実施形態に対する様々な変形および変更がなされ得ることは明らかである。したがって、明細書および図面は、限定目的というよりは、説明目的のものであることに留意されるべきである。

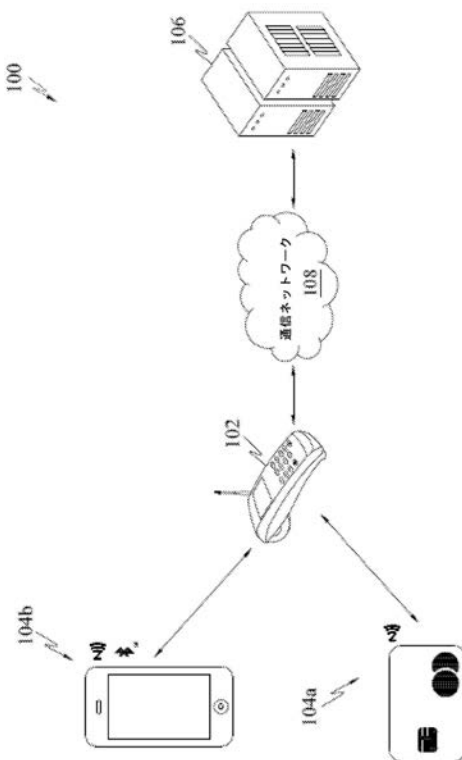
【0156】

本発明は、例示の目的でのみ記述されていることは、適切に理解されるであろう。添付の特許請求の範囲の原理および範囲から逸脱することなく、様々な変形が、本明細書において記述された技術に対してなされるであろう。開示の技術は、スタンドアロンな方法で提供されてもよいし、互いに組み合わされて提供されてもよい。したがって、該技術に対して記述された特徴も、別の技術と組み合わせて提供されていてもよい。

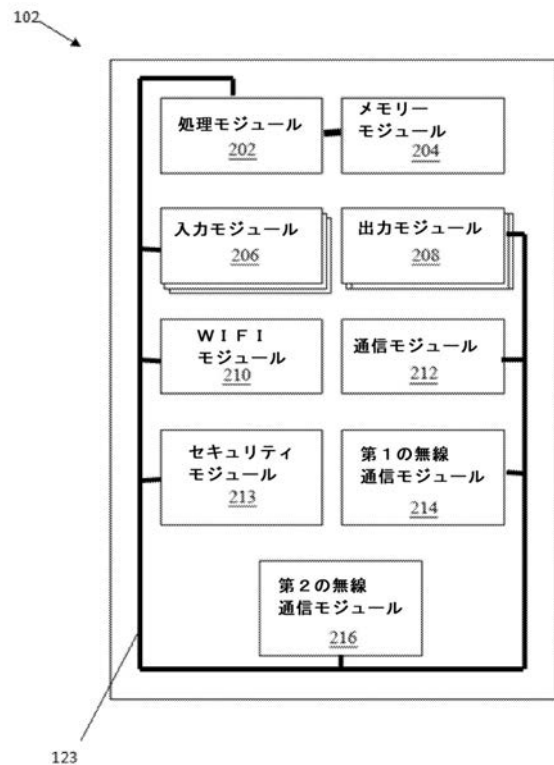
10

20

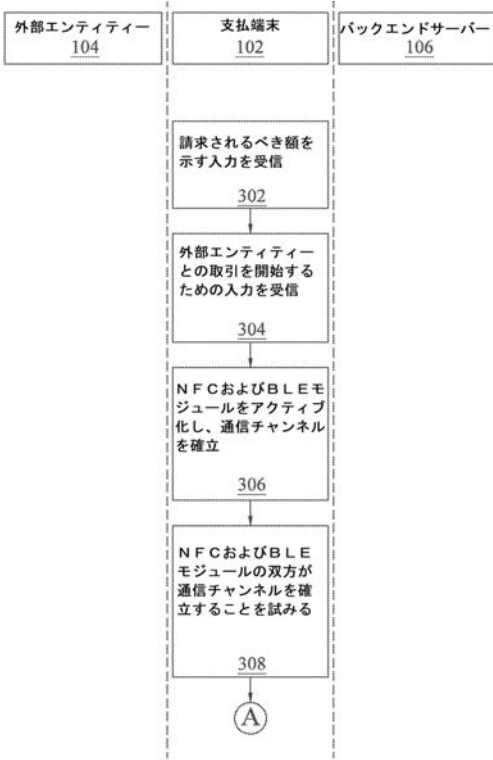
【図1】



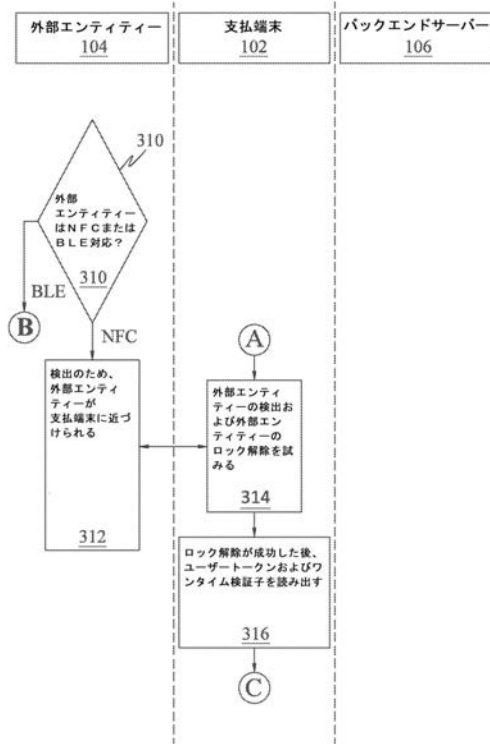
【図2】



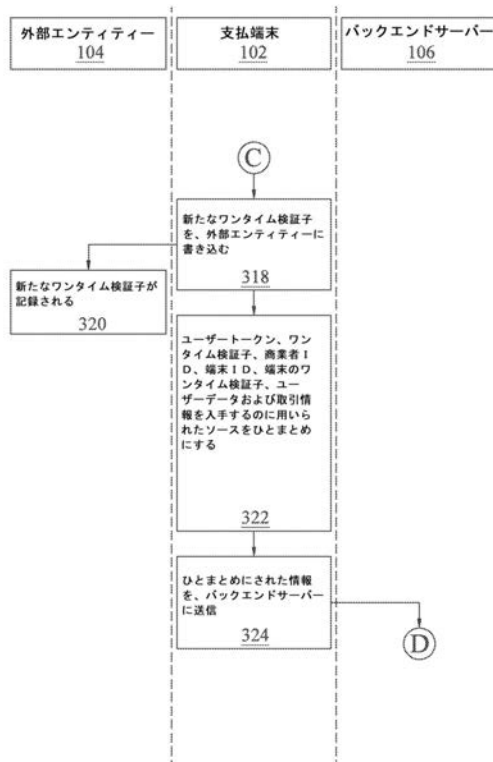
【図 3 A】



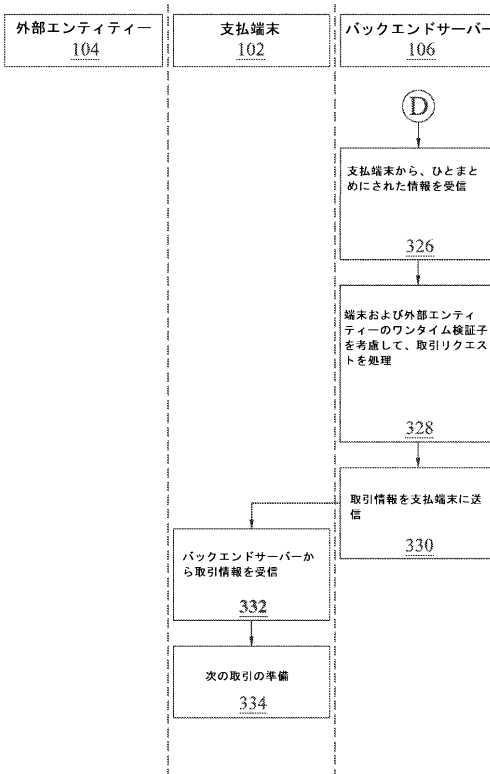
【図 3 B】



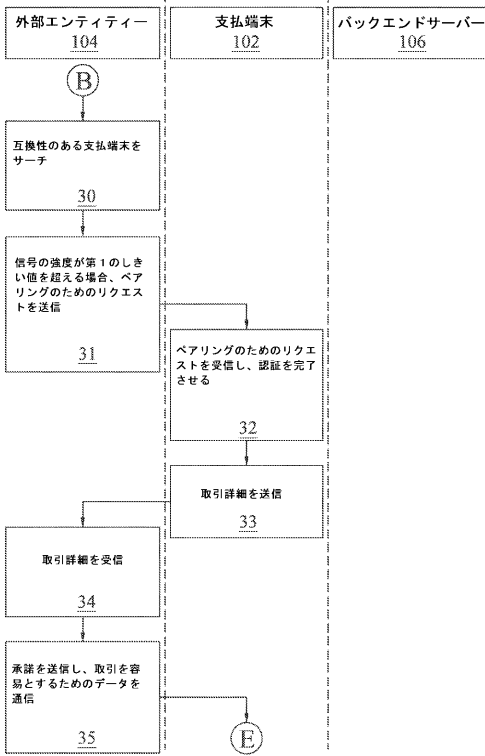
【図 3 C】



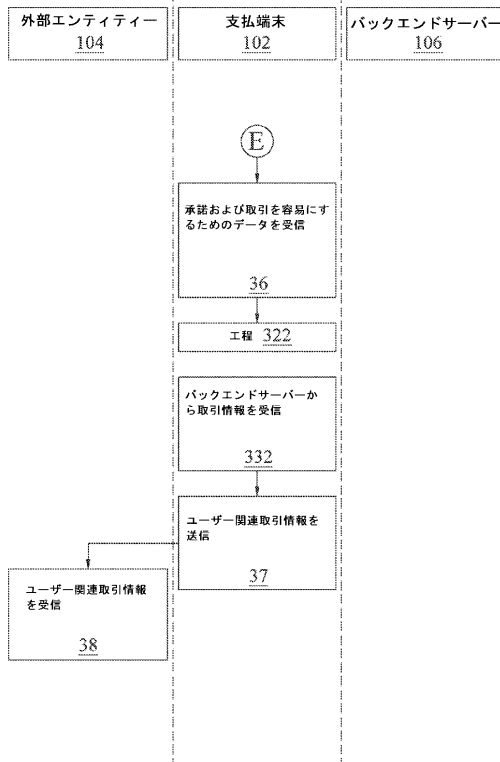
【図 3 D】



【図 3 E】



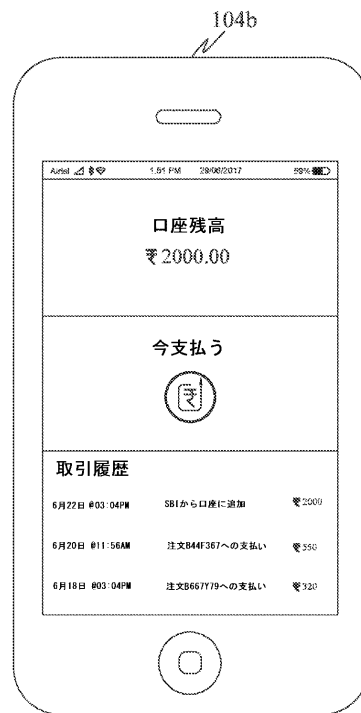
【図 3 F】



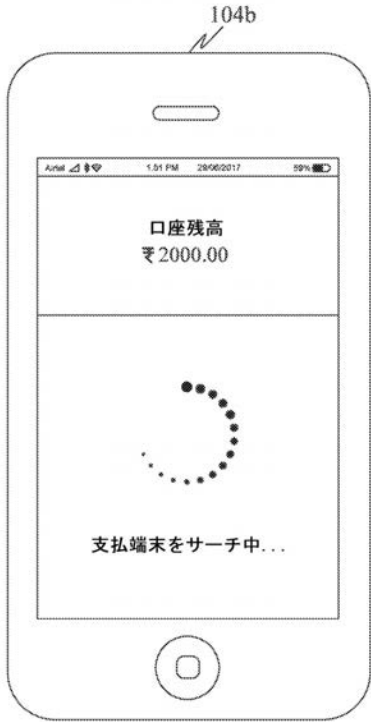
【図 4 A】



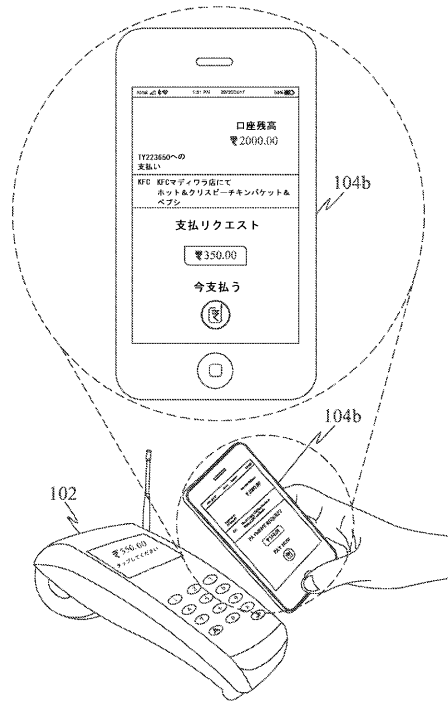
【図 4 B】



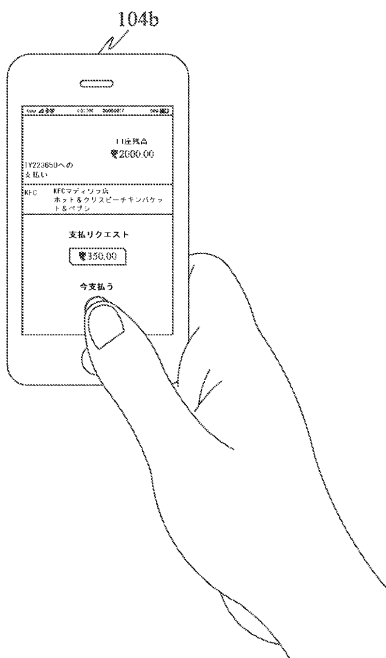
【図 4 C】



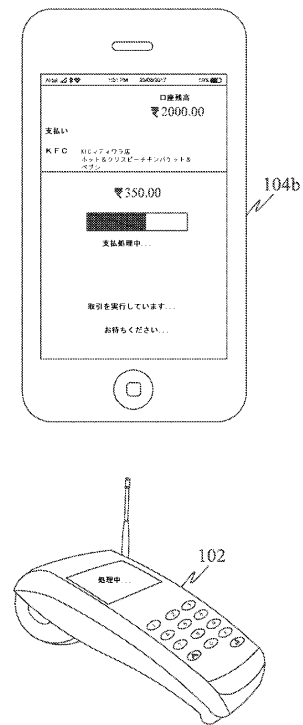
【図 4 D】



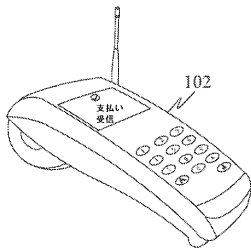
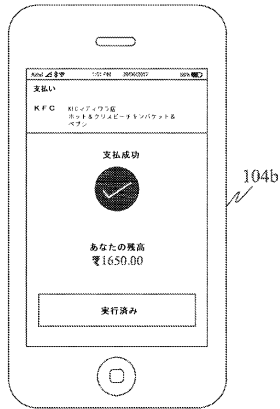
【図 4 E】



【図 4 F】



【図 4 G】



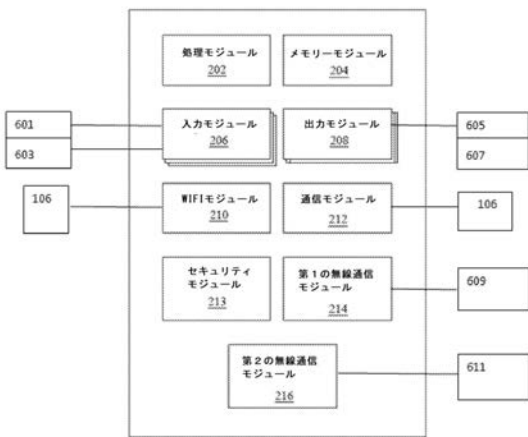
【図 5 A】



【図 5 B】



【図 6】



【手続補正書】

【提出日】令和1年5月2日(2019.5.2)

【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

支払端末を操作する方法であって、
アクティブ化入力を受信する工程と、
前記アクティブ化入力に応答して、第1の無線信号および第2の無線信号を同時に出力する工程であって、

前記第1の無線信号は、第1のタイプの外部支払デバイスと通信するためのものであり、前記第2の無線信号は、第2のタイプの外部支払デバイスと通信するためのものであり、

前記第1の無線信号および前記第2の無線信号は、互いに異なる第1のプロトコルおよび第2のプロトコルにそれぞれ対応するフォーマットにされている、前記出力する工程と、

前記第1の無線信号および前記第2の無線信号のいずれか一方に対する返信を受信する工程と、

前記返信に応答して、前記第1の無線信号および前記第2の無線信号の他方の出力を終了する工程と、を含むことを特徴とする方法。

【請求項2】

前記外部支払デバイスを認証するために前記返信を処理し、これにより、通信チャンネルを確立する工程をさらに含む請求項1に記載の方法。

【請求項3】

前記外部支払デバイスを認証するために前記返信を処理する工程をさらに含み、
前記処理する工程の後に、前記終了する工程が実行される請求項1に記載の方法。

【請求項4】

前記第1の無線信号および前記第2の無線信号は、NFC信号およびブルートゥース信号を含む請求項1に記載の方法。

【請求項5】

前記外部支払デバイスを認証するために前記返信を処理し、これにより、通信チャンネルを確立する工程と、

前記通信チャンネルから、ユーザーを示すデータを受信する工程と、

入力として、取引額を示すデータを受信する工程と、

前記ユーザーを示す前記データおよび前記取引額を示す前記データを、サーバーに送信する工程と、をさらに含む請求項1に記載の方法。

【請求項6】

前記外部支払デバイスを認証するために前記返信を処理し、これにより、通信チャンネルを確立する工程と、

前記通信チャンネルから、ユーザーを示すデータおよび現在の取引を特定するためのワンタイム検証子を受信する工程と、

入力として、取引額を示すデータを受信する工程と、

前記ユーザーを示す前記データ、前記ワンタイム検証子を示すデータ、および取引額を示すデータを、サーバーに送信する工程と、をさらに含む請求項1に記載の方法。

【請求項7】

前記通信チャンネルを介して、新たなワンタイム検証子を出力する工程をさらに含む請求項6に記載の方法。

【請求項 8】

応答された前記第 1 の無線信号および前記第 2 の無線信号のいずれかを示す情報をサーバーに通信する工程をさらに含む請求項 1 に記載の方法。

【請求項 9】

処理デバイスおよび命令を保持している記憶手段を有し、外部デバイスと無線通信するための支払端末であって、

前記命令は、前記処理デバイスを制御し、前記支払端末に、

アクティブ化入力にตอบสนองして、第 1 のタイプの外部支払デバイスと通信するための第 1 の無線信号および第 2 のタイプの外部支払デバイスと通信するための第 2 の無線信号を同時に出力させ、

前記第 1 の無線信号および前記第 2 の無線信号のいずれか一方に対する返信の受信にตอบสนองして、前記第 1 の無線信号および前記第 2 の無線信号の他方の出力を終了させ、

前記第 1 の無線信号および前記第 2 の無線信号は、互いに異なる第 1 のプロトコルおよび第 2 のプロトコルにそれぞれ対応するフォーマットにされていることを特徴とする支払端末。

【請求項 10】

前記アクティブ化入力を提供するためのキーパッドと、前記処理デバイスの制御下において情報を表示するディスプレイと、サーバーと通信するための出力デバイスと、をさらに有する請求項 9 に記載の支払端末。

【請求項 11】

前記第 1 の無線信号を出力するよう構成された第 1 の無線デバイスと、前記第 2 の無線信号を出力するよう構成された第 2 の無線デバイスと、をさらに有し、

前記第 1 の無線デバイスおよび前記第 2 の無線デバイスの双方は、前記処理デバイスの制御下にある請求項 9 に記載の支払端末。

【請求項 12】

セキュリティ鍵用の記憶手段を含むセキュリティデバイスをさらに有し、

前記セキュリティデバイスは、前記支払端末による使用のために、前記セキュリティ鍵を用いて、データを暗号化または復号化するよう構成されている請求項 9 に記載の支払端末。


【請求項 13】

前記第 1 の無線信号を出力するよう構成されたパーソナルエリアネットワークデバイスを有している請求項 9 に記載の支払端末。

【請求項 14】

前記第 2 の無線信号を出力するよう構成された近距離通信デバイスを有している請求項 9 に記載の支払端末。

【 国际调查报告 】

INTERNATIONAL SEARCH REPORT		International application No. PCT/SG2018/050321
A. CLASSIFICATION OF SUBJECT MATTER		
See Supplemental Box		
According to International Patent Classification (IPC)		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) G06Q; H04W		
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) FamPat, Incopat and CNKI: multi-mode, dual-mode, multiple, plural, more, two, second, wireless, interface, module, respond, reply, acknowledge, terminate, stop, cease, disable, payment, transaction, merchant, Bluetooth, BLE, NFC, RFID, short-range, mid-range, UWB, Zigbee, 双模, 多模, 两种, 两类, 多种, 多类, 第二种, 第二类, 无线, 近场, 蓝牙, 超宽带, 射频识别, 短距离, 近距离, 直连, 支付, 付款, 交易, 商户, 商家, 停止, 终止, 暂停, 禁用, 响应, 答复, 应答, 确认 and the related terms		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/0095761 A1 (CHU E. ET AL.) 18 April 2013 Paras. [0018]-[0020]	1-14
X	US 2012/0278192 A1 (SHIRRON E. ET AL.) 1 November 2012 Figs. 1-2 and Paras. [0010], [0017], [0024]-[0026], [0043]-[0044], [0050], [0065]	1-14
A	CN 205541169 U (SHENZHEN YUECHUANG HIGH TECHNOLOGY) 31 August 2016 Para. [0007] of the original non-English language document (a machine translation is enclosed only for your reference)	
A	US 2009/0047991 A1 (ELG J.) 19 February 2009 Para. [0094]	
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> 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		"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
"E" earlier application or patent but published on or after the international filing date		"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
"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)		"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
"O" document referring to an oral disclosure, use, exhibition or other means		"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed		
Date of the actual completion of the international search 13/09/2018 (day/month/year)		Date of mailing of the international search report 26/09/2018 (day/month/year)
Name and mailing address of the ISA/SG  Intellectual Property Office of Singapore 51 Bras Basah Road #01-01 Manulife Centre Singapore 189554 Email: pct@ipos.gov.sg		Authorized officer Yu Yang (Dr) IPPOS Customer Service Tel. No.: (+65) 6339 8616

INTERNATIONAL SEARCH REPORT		International application No. PCT/SG2018/050321
C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2017/0004475 A1 (WHITE M. W. ET AL.) 5 January 2017 Fig. 1 and Para. [0063]	
A	US 2016/0353233 A1 (YONG S. K. ET AL.) 1 December 2016 The Whole Document	

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SG2018/050321

Note: This Annex lists known patent family members relating to the patent documents cited in this International Search Report. This Authority is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013/0095761 A1	18/04/2013	DE 102012106254 A1 TW 201316797 A CN 103052126 A	18/04/2013 16/04/2013 17/04/2013
US 2012/0278192 A1	01/11/2012	EP 2702806 A1 CN 102768783 A WO 2012/148590 A1 JP 2012235447 A KR 20130136561 A	05/03/2014 07/11/2012 01/11/2012 29/11/2012 12/12/2013
CN 205541169 U	31/08/2016	NONE	
US 2009/0047991 A1	19/02/2009	WO 2009/022201 A1	19/02/2009
US 2017/0004475 A1	05/01/2017	EP 3295401 A1 WO 2017/004070 A1 CA 2990199 A1	21/03/2018 05/01/2017 05/01/2017
US 2016/0353233 A1	01/12/2016	CN 106211029 A EP 3101874 A1	07/12/2016 07/12/2016

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SG2018/050321**Supplemental Box**
(Classification of Subject Matter)

Int. Cl.

G06Q 20/32 (2012.01)**H04W 76/10 (2018.01)****H04W 88/06 (2009.01)****H04W 84/18 (2009.01)****H04W 48/16 (2009.01)**

フロントページの続き

(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, 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, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT

(72)発明者 ソマサンダラム , マニカバサガム

インド 560 037 バンガロール , シュリラム スパンドハナ , チャラガッタ ロード
, #304 , ビー6

Fターム(参考) 5L055 AA64