(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2022-508752
(P2022-508752A)
(43)公表日　令和4年1月19日(2022.1.19)

(51)国際特許分類　FI
H04L 9/32 (2006.01)　H04L 9/00　673C
G06F 21/60 (2013.01)　G06F 21/60　320
G06F 21/60　360

審査請求　有　予備審査請求　未請求　（全34頁）

(21)出願番号　特願2021-545350(P2021-545350)
(86)(22)出願日　平成30年10月15日(2018.10.15)
(85)翻訳文提出日　令和3年4月14日(2021.4.14)
(86)国際出願番号　PCT/US2018/055833
(87)国際公開番号　WO2020/081044
(87)国際公開日　令和2年4月23日(2020.4.23)
(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,B
最終頁に続く

(71)出願人　505468864
ビザ インターナショナル サービス アソシエーション
アメリカ合衆国、９４１２８－８９９９　カリフォルニア州、サン フランシスコ、ピー．オー． ボックス ８９９９
(74)代理人　110000855
特許業務法人浅村特許事務所
(72)発明者　オービエ、アンドレアス
アメリカ合衆国、カリフォルニア、サン マテオ、マリーナ コート １６３１、ユニット シー．
(72)発明者　オービエ、クリスチャン
アメリカ合衆国、カリフォルニア、レッドウッド シティー、クリーブランド ス
最終頁に続く

(54)【発明の名称】　異種データメッセージの機密データを安全に伝達するための技術

(57)【要約】
識別子などの機密を安全に通信するための、システムおよび方法を開示する。ユーザデバイスは、端末タイプ指標を含む第一のメッセージを受信してもよい。端末タイプ指標の特定の値について、ユーザデバイスは、第一の識別子および暗号化された識別子を含む、要求メッセージを送信するように構成され得る。端末タイプ指標の他の値については、ユーザデバイスは、第二の識別子の第一の部分および暗号化された識別子の第二の部分に少なくとも部分的に基づいて、難読化された識別子を生成するように構成され得る。その後、ユーザデバイスは、難読化された識別子および暗号化された識別子を含む、要求メッセージを送信し得る。

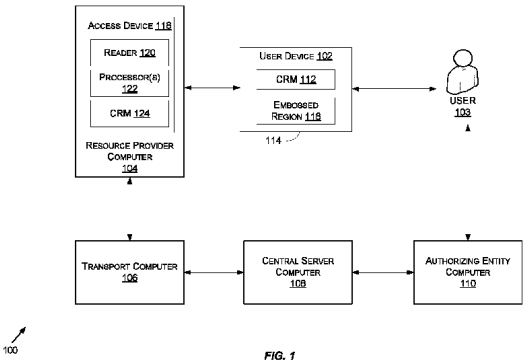


FIG. 1

【特許請求の範囲】
【請求項１】
ユーザデバイスによってアクセスデバイスから、端末タイプ指標を含む第一のメッセージを受信することと、
第一の端末タイプを示す、前記端末タイプ指標に応じて、
前記ユーザデバイスから前記アクセスデバイスへ、第一の識別子および暗号化された識別子を含む第二のメッセージを送信することと、
第二の端末タイプを示す、前記端末タイプ指標に応じて、
前記ユーザデバイスによって、第二の識別子の第一の部分および前記暗号化された識別子の第二の部分に少なくとも部分的に基づいて、難読化された識別子を生成することと、
前記ユーザデバイスから前記アクセスデバイスへ、前記難読化された識別子および前記暗号化された識別子を含む、前記第二のメッセージを送信することと、を含む、コンピュータ実装方法。
【請求項２】
前記ユーザデバイスによって、保存されたカウンタ値を取得することであって、前記暗号化された識別子が、前記保存されたカウンタ値をさらに利用して生成されることと、
前記要求メッセージの送信に応じて、修正されたカウンタ値を生成することと、
前記修正されたカウンタ値を前記ユーザデバイスに保存することと、をさらに含む、請求項１に記載のコンピュータ実装方法。
【請求項３】
前記暗号化された識別子を生成することが、前記ユーザデバイスに保存された一意の導出鍵で、前記第二の識別子および前記修正されたカウンタ値を暗号化することをさらに含む、請求項２に記載のコンピュータ実装方法。
【請求項４】
前記暗号化された識別子の前記第二の部分が、前記暗号化された識別子の右端の７ビットを含む、請求項１に記載のコンピュータ実装方法。
【請求項５】
前記第二の識別子の前記第一の部分が、前記第二の識別子の左端の８ビットを含む、請求項１に記載のコンピュータ実装方法。
【請求項６】
前記第二の識別子の前記部分が、アクワイアラと関連付けられた識別番号を含む、請求項１に記載のコンピュータ実装方法。
【請求項７】
前記第一の識別子および前記暗号化された識別子を含む前記要求メッセージを、前記アクセスデバイスに送信することによって、前記アクセスデバイスに、
前記第一の識別子を複数の保存された識別子と比較させ、
前記第一の識別子が、前記複数の保存された識別子に含まれるとき、前記要求メッセージを拒否させ、前記要求メッセージを拒否することによって、前記アクセスデバイスにより管理されるリソースへのアクセスを、前記ユーザデバイスには与えず、
前記第一の識別子が、前記複数の保存された識別子に含まれないとき、前記要求メッセージを承認させ、前記要求メッセージを承認することによって、前記アクセスデバイスによって管理される前記リソースへのアクセスが、前記ユーザデバイスに対して許可される、請求項１に記載のコンピュータ実装方法。
【請求項８】
前記第一の識別子および前記暗号化された識別子を含む前記要求メッセージを、前記アクセスデバイスに送信することによって、前記アクセスデバイスに、
前記第一の識別子および前記暗号化された識別子を含む、承認要求メッセージを生成させ、
前記承認要求メッセージを承認事業体コンピュータに送信させる、請求項１に記載のコンピュータ実装方法。

【請求項９】
前記承認事業体コンピュータが、
前記第一の識別子および前記暗号化された識別子を含む、前記承認要求メッセージを受信し、
前記第一の識別子と関連付けられた、保存された識別子を識別し、
前記暗号化された識別子から復号された識別子を生成し、
前記保存された識別子を前記復号された識別子と比較し、
前記保存された識別子と前記復号された識別子との比較に少なくとも部分的に基づいて、前記承認要求メッセージを処理するように構成される、請求項８に記載のコンピュータ実装方法。
【請求項１０】
前記難読化された識別子および前記暗号化された識別子を含む前記要求メッセージを、前記アクセスデバイスに送信することによって、前記アクセスデバイスに、
前記難読化された識別子および前記暗号化された識別子を含む、承認要求メッセージを生成させ、
前記承認要求メッセージを承認事業体コンピュータに送信させ、前記難読化された識別子および前記暗号化された識別子を含む、前記承認要求メッセージを送信することによって、前記承認事業体コンピュータに、前記難読化された識別子の一部分に少なくとも部分的に基づいて導出鍵を導き出させ、前記導出鍵を利用して、前記暗号化された識別子から復号された識別子を生成させ、前記復号された識別子を利用して、前記承認要求メッセージを処理させる、請求項１に記載のコンピュータ実装方法。
【請求項１１】
一つ以上のプロセッサと、
コンピュータ実行可能命令を保存する、一つ以上のメモリであって、前記一つ以上のプロセッサにより前記コンピュータ実行可能命令を実行することによって、前記ユーザデバイスに、
アクセスデバイスから、端末タイプ指標を含む第一のメッセージを受信させ、
第一の端末タイプを示す、前記端末タイプ指標に応じて、
前記アクセスデバイスへ、第一の識別子および暗号化された識別子を含む第二のメッセージを送信させ、
第二の端末タイプを示す、前記端末タイプ指標に応じて、
第二の識別子の第一の部分および前記暗号化された識別子の第二の部分に少なくとも部分的に基づいて、難読化された識別子を生成させ、
前記アクセスデバイスへ、前記難読化された識別子および前記暗号化された識別子を含む、前記第二のメッセージを送信させる、一つ以上のメモリとを備える、ユーザデバイス。
【請求項１２】
前記コンピュータ実行可能命令を、前記一つ以上のプロセッサにより実行することによってさらに、前記ユーザデバイスに、
保存されたカウンタ値を取得させ、前記暗号化された識別子が、前記保存されたカウンタ値をさらに利用して生成され、
前記要求メッセージの送信に応じて、修正されたカウンタ値を生成させ、
前記修正されたカウンタ値を前記ユーザデバイスに保存させる、請求項１１に記載のユーザデバイス。
【請求項１３】
前記暗号化された識別子を生成することが、前記ユーザデバイスに保存された一意の導出鍵で、前記第二の識別子および前記修正されたカウンタ値を暗号化することをさらに含む、請求項１２に記載のユーザデバイス。
【請求項１４】
前記暗号化された識別子の前記第二の部分が、前記暗号化された識別子の右端の７ビットを含む、請求項１１に記載のユーザデバイス。

【請求項１５】
前記第二の識別子の前記第一の部分が、前記第二の識別子の左端８ビットを含む、請求項１１に記載のユーザデバイス。
【請求項１６】
前記第二の識別子の前記部分が、アクワイアラと関連付けられた識別番号を含む、請求項１１に記載のユーザデバイス。
【請求項１７】
前記第一の識別子および前記暗号化された識別子を含む前記要求メッセージを、前記アクセスデバイスに送信することによって、前記アクセスデバイスに、
前記第一の識別子を複数の保存された識別子と比較させ、
前記第一の識別子が、前記複数の保存された識別子に含まれるとき、前記要求メッセージを拒否させ、前記要求メッセージを拒否することによって、前記アクセスデバイスにより管理されるリソースへのアクセスを、前記ユーザデバイスには与えず、
前記第一の識別子が、前記複数の保存された識別子に含まれないとき、前記要求メッセージを承認させ、前記要求メッセージを承認することによって、前記アクセスデバイスによって管理される前記リソースへのアクセスが、前記ユーザデバイスに対して許可される、請求項１１に記載のユーザデバイス。
【請求項１８】
前記第一の識別子および前記暗号化された識別子を含む前記要求メッセージを、前記アクセスデバイスに送信することによって、前記アクセスデバイスに、
前記第一の識別子および前記暗号化された識別子を含む、承認要求メッセージを生成させ、
前記承認要求メッセージを承認事業体コンピュータに送信させる、請求項１１に記載のユーザデバイス。
【請求項１９】
前記承認事業体コンピュータが、
前記第一の識別子および前記暗号化された識別子を含む、前記承認要求メッセージを受信し、
前記第一の識別子と関連付けられた、保存された識別子を識別し、
前記暗号化された識別子から復号された識別子を生成し、
前記保存された識別子を前記復号された識別子と比較し、
前記保存された識別子と前記復号された識別子との比較に少なくとも部分的に基づいて、前記承認要求メッセージを処理するように構成される、請求項１８に記載のユーザデバイス。
【請求項２０】
前記難読化された識別子および前記暗号化された識別子を含む前記要求メッセージを、前記アクセスデバイスに送信することによって、前記アクセスデバイスに、
前記難読化された識別子および前記暗号化された識別子を含む、承認要求メッセージを生成させ、
前記承認要求メッセージを承認事業体コンピュータに送信させ、前記難読化された識別子および前記暗号化された識別子を含む、前記承認要求メッセージを送信することによって、前記承認事業体コンピュータに、前記難読化された識別子の一部分に少なくとも部分的に基づいて導出鍵を導き出させ、前記導出鍵を利用して、前記暗号化された識別子から復号された識別子を生成させ、前記復号された識別子を利用して、前記承認要求メッセージを処理させる、請求項１１に記載のユーザデバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示の実施形態は、取引で利用されるメッセージ内の機密データを難読化することに関する。これらの技術は、接触および／または非接触スマートカード取引に適用することが

できる。概して、非接触スマートカードは、消費者に効率的な支払方法を提供するように設計されている。スマートカードは、例えば、無線周波数または赤外線信号を使用することによって、必要な情報を販売時点情報管理（ＰＯＳ）デバイスに提供して、取引を完了することができる。ＰＯＳデバイスは、提供された情報を受信し、取引を処理し得る。

【背景技術】

【０００２】

スマートカードによって送られる情報は、ユーザのアカウント識別子（例えば、個人アカウント番号）などの機密データを含むことができる。結果として、この情報を傍受し得る熟練した不正行為者から、ユーザを保護するために、セキュリティ対策が必要となる。アカウント識別子全体が暗号化されていないため、現在の技術は問題がある場合がある。他の従来の技術では、アカウント識別子は、暗号化され得るが、既知のデータフィールドを有する既知のプロトコルに従って、依然として送信および／または提供される。利口な不正行為者は、メッセージ内の暗号化されたデータフィールドを簡単に識別することができるため、その情報を自身の非道な行為に利用できる可能性が高い。加えて、従来の技術を使用すると、アカウント識別子は静的なままであり、不正行為者がユーザの取引を追跡できる可能性がある。

【０００３】

その上さらに、従来のシステムでは、機密情報の使用は制限されない。例えば、不正行為者は、一旦機密情報を取得したなら、様々な状況で機密情報を利用し得る。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

本発明の実施形態は、これらおよび他の問題に、個々にかつまとめて対処する。

【課題を解決するための手段】

【０００５】

本発明の実施形態は、非接触スマートカードなどのユーザデバイスと関連付けられたアカウント識別子（例えば、ＰＡＮ）を、安全に伝達するために使用できる方法、システム、デバイス、およびコンピュータ可読媒体を対象とする。一部の実施形態では、ユーザデバイスには、プライマリアカウント番号（ＰＡＮ）およびセカンダリアカウント番号（ＳＡＮ：ｓｅｃｏｎｄａｒｙ　ａｃｃｏｕｎｔ　ｎｕｍｂｅｒ）が保存されていてもよい。アカウント識別子（例えば、ＰＡＮ）は、プライバシーの保護のため、アカウント識別子を追跡することができないように伝達されてもよい。有利には、本発明の実施形態では、アカウント情報は、安全に、かつ既存の支払インフラを著しく更新する必要が全くないように伝達される。

【０００６】

追加のアカウント識別子（例えば、ＳＡＮ）は、静的識別子が必要とされる状況で、本明細書で論じる実施形態において利用され得る。例として、いくつかのタイプのアクセスデバイスは、ほぼリアルタイムで、ユーザによるリソースへのアクセスを許可または拒否することが期待される。したがって、こうしたアクセスデバイスは、スマートカードのユーザへのアクセスを迅速に許可もしくは拒否するために、許可リストおよび／またはブロックリストと照合するよう、静的識別子を利用してもよい。追加のアカウント識別子（例えば、ＳＡＮ）は、特定の状況においてのみ利用され得る。例えば、システムによって、ＳＡＮが、特定のタイプの端末および／もしくは小売業者、ならびに／または取引が関与する取引でのみ使用可能であることを保証し得る。非限定的な例として、システムは、ＳＡＮが、交通端末（例えば、公共交通機関の自動改札）が関与する取引でのみ利用され得ることを保証するように、構成されてもよい。

【０００７】

本発明の一実施形態は、ユーザデバイスによってアクセスデバイスから、端末タイプ指標を含む第一のメッセージを受信することを含む方法を対象とする。方法は、第一の端末タイプを示す端末タイプ指標に応じて、ユーザデバイスからアクセスデバイスへ、第一の識

別子（例えば、ＳＡＮ）および暗号化された識別子（例えば、ＰＡＮおよび取引カウンタから生成された暗号化された識別子）を含む、要求メッセージを送信することをさらに含み得る。方法は、第二の端末タイプを示す端末タイプ指標に応じて、ユーザデバイスによって、第二の識別子（例えば、プライマリＰＡＮ）の第一の部分および暗号化された識別子の第二の部分に少なくとも部分的に基づいて、難読化された識別子を生成することをさらに含み得る。方法は、ユーザデバイスからアクセスデバイスへ、送信することをさらに含み得る。一部の実施形態では、要求メッセージは、難読化された識別子および暗号化された識別子を含み得る。

【０００８】

本発明の別の実施形態は、一つ以上のプロセッサと、一つ以上のプロセッサによって実行されるとき、ユーザデバイスに動作を実施させるコンピュータ実行可能命令を含む、一つ以上のメモリとを備えるユーザデバイスを対象とする。動作は、ユーザデバイスによってアクセスデバイスから、端末タイプ指標を含む第一のメッセージを受信することを含み得る。動作は、第一の端末タイプを示す端末タイプ指標に応じて、ユーザデバイスからアクセスデバイスへ、第一の識別子（例えば、ＳＡＮ）および暗号化された識別子（例えば、プライマリＰＡＮおよび取引カウンタから生成された暗号化された識別子）を含む、要求メッセージを送信することをさらに含み得る。動作は、第二の端末タイプを示す端末タイプ指標に応じて、ユーザデバイスによって、第二の識別子（例えば、プライマリＰＡＮ）の第一の部分および暗号化された識別子の第二の部分に少なくとも部分的に基づいて、難読化された識別子を生成することをさらに含み得る。動作は、ユーザデバイスからアクセスデバイスへ、送信することをさらに含み得る。一部の実施形態では、要求メッセージは、難読化された識別子および暗号化された識別子を含み得る。

【０００９】

本発明の別の実施形態は、（非一時的）コンピュータ可読媒体を対象とする。コンピュータ可読媒体は、本明細書で論じる方法を実施するためのコードを含む。一部の実施形態では、スマートカードなどのユーザデバイスが、このコンピュータ可読媒体を備えてもよい。

【００１０】

本発明のこれらのおよび他の実施形態について、図面を参照して以下でさらに詳細に記載する。

【図面の簡単な説明】

【００１１】

【図１】図１は、一部の実施形態による、取引を処理するためのシステムのブロック図を示す。

【図２】図２は、一部の実施形態による、データを生成しユーザデバイスに保存する方法を示す。

【図３】図３は、一部の実施形態による、コンピューティングデバイス（例えば、スマートカード）上に常駐するデータから、一意に導出された鍵を生成するための方法を示す。

【図４】図４は、一部の実施形態による、オフライン認証を実施するための方法を示す。

【図５】図５は、一部の実施形態による、機密データを安全に伝達するための方法のフローチャートを示す。

【図６】図６は、一部の実施形態で使用するための例示的な記録形式を示す。

【図７】図７は、一部の実施形態で使用するための別の例示的な記録形式を示す。

【図８】図８は、一部の実施形態による、データ検証を実施するための方法のフローチャートを示す。

【図９】図９は、一部の実施形態による、データ検証を実施する別の方法のフローチャートを示す。

【発明を実施するための形態】

【００１２】

上記のように、慣例の支払取引では、アカウント識別子（例えば、プライマリＰＡＮとも

呼ばれる個人アカウント識別子）は、非接触スマートカードなどのユーザデバイスから、最終的に従来の支払処理ネットワークを通って、アクセスデバイス（例えば、ＰＯＳ端末、自動改札機リーダなど）を通過するとき、暗号化されていない。一部の従来の技術では、アカウント識別子は、暗号化および／または難読化される場合があるが、暗号化／難読化されたデータは、依然として、取引メッセージの従来のデータフィールドの中に提供されてもよく、データフィールドは、潜在的な不正行為者には容易に識別可能である。

【００１３】

アカウント識別子全体の暗号化は、可能であるものの、すべての状況下で実用的であるわけではない場合がある。アカウント識別子が暗号化されている場合、従来の取引処理システムでは、取引をうまく処理できない場合がある。例えば、代表的なアカウント識別子は銀行識別番号（ＢＩＮ）を含む。ＢＩＮは、承認要求メッセージを、適切な発行者または支払プロセッサにルーティングするように使用される。アカウント識別子が暗号化される場合、ＢＩＮは変更される。ＢＩＮが変わると、適切な承認要求メッセージを、正しい発行者にルーティングできない。

【００１４】

アカウント識別子全体の暗号化に関連付けられた別の制限は、アカウント識別子における数字の配列と関連付けられる、エラーチェックに関する。エラーチェックは、アカウント識別子の数字が適切な配列にあるかを判定する、チェックサムアルゴリズムを使用して達成され得る。チェックサムアルゴリズムの例は、ＭＯＤ－１０アルゴリズム（「Ｌｕｈｎチェック」としても知られる）である。

【００１５】

したがって、アカウント識別子全体の暗号化によって、少なくともＢＩＮ、チェックサムが損なわれ、レシートに印刷された数字によりアカウント識別子を識別する機能が毀損するであろう。

【００１６】

本明細書に記載されるプロセスは、開始するデバイス（例えば、スマートカード）にあるアカウント識別子を保護するために使用され得る。以下でさらに詳細に説明するように、本発明の実施形態では、アカウント識別子の一部分のみを難読化し、これにより、ＢＩＮにアカウントを与えて暗号化しないままとし、Ｌｕｈｎチェックの利用を続けることが可能になる。加えて、本発明の実施形態はまた、代表的な承認要求メッセージ内のアカウント識別子を難読化するだけでなく、暗号化されたアカウント識別子全体を、識別できる可能性を低くするために、メッセージの他の場所に提供することを保証するようにも使用できる。

【００１７】

また本明細書で論じる技術によって、取引の状況（例えば、どのタイプの端末が情報を要求しているか）に応じて、難読化された識別子またはＳＡＮを、ユーザデバイスが利用することも可能になる。したがって、取引タイプ、端末タイプなどの第一のセットに関連付けられている取引に対して、難読化されたＰＡＮを取引で利用してもよく、一方ＳＡＮは、取引タイプ、端末タイプなどの第二のセットと関連付けられる取引に利用してもよい。ＳＡＮは、許容可能な状況で利用されるとき、承認事業体によって処理のみされるように制限されてもよい。取引／端末タイプ取引の第一のセットに対して、ユーザの活動を追跡できないように、難読化されたＰＡＮを利用してもよい。これらの技術によって、オフライン取引（例えば、端末がその場でスマートカードを認証する取引）、およびオフライン取引から生じる後続のオンライン取引に、静的識別子を利用することが可能になり、一方、対応するオフライン認証が不要なオンライン認証取引には、動的識別子（例えば、動的値）を利用してもよい。

【００１８】

本発明の詳細な実施形態について論じる前に、特定の用語についてのいくつかの説明が有用であり得る。

【００１９】

「コンピューティングデバイス」（「ユーザデバイス」とも呼ばれる）は、計算を実施することができ、他のデバイスと通信できる、任意の好適なデバイスであってもよい。スマートカードなどの消費者用ポータブルデバイスは、コンピューティングデバイスの一例である。他のタイプのコンピューティングデバイスは、ポータブルではない場合がある。

【００２０】

「動的値」は、動的に変化する値を指すことを意図する。コンピューティングデバイスは、様々な動的値を維持できる。動的値の例は、アプリケーション取引カウンタ（ＡＴＣ：ａｐｐｌｉｃａｔｉｏｎ ｔｒａｎｓａｃｔｉｏｎ ｃｏｕｎｔｅｒ）である。ＡＴＣは最初に、コンピューティングデバイス（例えば、承認事業体）の発行者によって、所定の値に設定されてもよい。その後、ＡＴＣは各取引と共に値が増加してもよい。交互にＡＴＣは、各取引と共にその初期の所定値から減少し得る。ＡＴＣは、任意の長さの値であってもよい。加えて、発行者は、対応するＡＴＣを、発行者のコンピュータがアクセス可能なように維持してもよい。この対応するＡＴＣは、不正目的で再現された可能性のある支払サービスを識別するために使用され得る。代替の実施形態では、取引データに基づく暗号文、デジタル署名、またはハッシュ値が、コンピューティングデバイスに保存されたＡＴＣの代わりに、またはそれと併せて使用され得る。

【００２１】

他の動的値（例えば、データ要素）の例には、時刻、現在の取引額、および端末からランダムに生成された番号などが含まれ得る。データ要素は、取引ごとに、またはほぼ取引ごとに変更できるという意味で動的である。動的データ要素は、ユーザのコンピューティングデバイスに関係してもよく、および／または概してユーザに関係し得る。

【００２２】

「承認事業体」は、要求を承認する事業体とすることができる。承認事業体の例は、発行者、政府機関、文書保管所、アクセス管理者などであり得る。「発行者」は通常、ユーザのアカウントを保持するビジネス事業体（例えば、銀行）を指し得る。発行者はまた、消費者に対して携帯電話、スマートカード、タブレット、またはラップトップなどのユーザデバイスに保存される、支払証明書を発行することができる。「承認事業体コンピュータ」は、承認事業体によって、または承認事業体に代わって操作されてもよい。

【００２３】

「アクワイアラ」は通常、特定の小売業者または他の事業体とビジネス関係を有するビジネス事業体（例えば、商業銀行）とすることができる。一部の事業体は、発行者およびアクワイアラの両方の機能を果たすことができる。一部の実施形態は、こうした単一事業体の発行者－アクワイアラを含み得る。アクワイアラは、「転送コンピュータ」とも総称され得る、アクワイアラコンピュータを操作し得る。

【００２４】

「リソースプロバイダ」は、物品、サービス、情報、および／またはアクセスなど、リソースを提供できる事業体であり得る。リソースプロバイダの例には、小売業者、アクセスデバイス、安全なデータアクセスポイントなどを含む。「小売業者」は通常、取引に携わり、物品もしくはサービスを販売する、または物品もしくはサービスへのアクセスを提供することができる事業体であり得る。「リソースプロバイダコンピュータ」は、リソースプロバイダによって、またはリソースプロバイダに代わって操作され得る、任意の好適なコンピューティングデバイスであってもよい。

【００２５】

「処理ネットワークコンピュータ」（中央サーバコンピュータとも呼ばれる）は、ネットワークデータを処理するために使用される、サーバコンピュータを含み得る。一部の実施形態では、処理ネットワークコンピュータは、データベースに結合されてもよく、一つ以上のクライアントコンピュータからの要求にサービスを提供する、いずれのハードウェア、ソフトウェア、他のロジック、または前述の組み合わせを含んでもよい。処理ネットワークコンピュータは、一つ以上の計算装置を備えてもよく、一つ以上のクライアントコンピュータからの要求にサービスを提供する、様々なコンピュータ構造、配置、およびコン

パイルのうちのいずれを使用してもよい。一部の実施形態では、処理ネットワークコンピュータは、複数のサーバコンピュータを操作し得る。こうした実施形態では、各サーバコンピュータは、所与の領域に対する取引を処理するか、または取引データに基づいて特定タイプの取引に対処するように構成され得る。

【００２６】

処理ネットワークコンピュータは、承認サービスと、例外ファイルサービスと、清算および決済サービスとをサポートし配信するのに使用される、データ処理サブシステム、ネットワーク、ならびに動作を含んでいてもよい。例示的な処理ネットワークコンピュータは、ＶｉｓａＮｅｔ（商標）を含んでいてもよい。ＶｉｓａＮｅｔ（商標）を含むネットワークは、クレジットカード取引、デビットカード取引、および他のタイプの商取引を処理することができる。特にＶｉｓａＮｅｔ（商標）には、承認要求を処理する統合支払システム（Ｉｎｔｅｇｒａｔｅｄ　Ｐａｙｍｅｎｔｓシステム）と、清算および決済サービスを実施するＢａｓｅ　ＩＩシステムとが含まれる。処理ネットワークコンピュータは、インターネットを含む、任意の好適な有線または無線ネットワークを使用することができる。

【００２７】

「承認要求メッセージ」は、取引処理コンピュータおよび／または承認事業体コンピュータ（例えば、支払カードの発行者）へ送られて、取引に対する承認を要求する電子メッセージであってもよい。一部の実施形態による承認要求メッセージは、支払デバイスまたは支払アカウントを使用する消費者によりなされる支払いと関連付けられた、電子取引情報を交換するシステムの標準である、ＩＳＯ８５８３に準拠することができる。承認要求メッセージは、支払デバイスまたは支払アカウントと関連付けられてもよい、発行者アカウント識別子を含んでもよい。承認要求メッセージはまた、単に例として、サービスコード、ＣＶＶ（カード検証値）、ｄＣＶＶ（動的カード検証値）、有効期限などを含む、「識別情報」に対応する追加のデータ要素を含むことができる。承認要求メッセージはまた、取引を識別および／または承認するかの判定に利用されてもよい、いかなる他の情報だけでなく、取引額、小売業者識別子、小売業者所在地など、現在の取引と関連付けられた、任意の情報などの「取引情報」を含んでもよい。

【００２８】

「承認応答メッセージ」は、承認事業体コンピュータまたは取引処理コンピュータによって生成された、承認要求メッセージに応答する電子メッセージとすることができる。承認応答メッセージは、単に例として、次の状態指標のうちの一つ以上を含んでもよい。承認―取引が承認された。拒否―取引が承認されなかった。または、コールセンター―応答はより多くの情報を保留中で、小売業者は、フリーダイヤルの認証電話番号に電話する必要がある。承認応答メッセージはまた、承認事業体（例えば、発行者銀行）が、承認要求メッセージに応じて、取引の承認を示す、リソースプロバイダコンピュータへの電子メッセージ（直接または取引処理コンピュータを介してのいずれか）で返信するコードであり得る、承認コードを含むことができる。コードは、承認の証明として役割を果たし得る。一部の実施形態では、取引処理コンピュータは、承認応答メッセージを生成するか、またはそれをリソースプロバイダに転送し得る。

【００２９】

「プライマリアカウント番号」（ＰＡＮ：ｐｒｉｍａｒｙ　ａｃｃｏｕｎｔ　ｎｕｍｂｅｒ）は、支払アカウントに対する識別子であり得る。ＰＡＮは、一連の英数字（例えば、１６個）を含み得る。ＰＡＮ（またはＰＡＮの難読化もしくは暗号化されたバージョン）を使用して、支払取引を開始、承認、決済、または解決することができる。一部の実施形態では、ＰＡＮをいかなるタイプの取引に利用してもよい。

【００３０】

「‐アカウント番号」（ＳＡＮ）は、支払アカウントに対する別の識別子であり得る。ＳＡＮは、一連の英数字（例えば、１６個）を含み得る。ＳＡＮ（またはＰＡＮの難読化もしくは暗号化されたバージョン）を使用して、取引を開始、承認、決済、または解決する

ことができる。一部の実施形態では、ＳＡＮの使用を特定のタイプの取引に制限し得る。例えば、ＳＡＮは、取引が特定のタイプの小売業者（例えば、公共交通機関、交通機関の小売業者、競技場の小売業者など）を含むとき、取引が特定の端末タイプの端末（例えば、自動改札機など）によって開始されるとき、および／または取引が特定タイプの取引（例えば、交通機関の取引、料金の確認取引など）であるときに利用され得る。一部の実施形態では、ＳＡＮがＰＡＮと関連付けられてもよく、両方が特定のユーザのアカウント（例えば、ユーザに代わって発行者により維持される金融口座）と関連付けられてもよい。一部の実施形態では、ＰＡＮおよび関連付けられたＳＡＮ各々が、同じ左端の８桁（例えば、銀行識別番号（ＢＩＮ）に対応する）を含む場合がある。

【００３１】

「難読化された識別子」は、難読化されたバージョンの識別子（例えば、１６桁のＰＡＮ）である、識別子を含み得る。一部の実施形態では、難読化された識別子は、「形式保存」であってもよく、既存の取引処理ネットワークで使用されるアカウント識別子に準拠する数値形式（例えば、ＩＳＯ８５８３金融取引メッセージ形式）を有することができる。一部の実施形態では、難読化された識別子は、支払取引を開始、承認、決済、もしくは解決するように、または元の証明書が通常提供されるであろう他のシステムで、元の証明書を表すように、ＰＡＮの代わりに使用されてもよい。

【００３２】

「暗号化された識別子」は、任意の好適な暗号化された値を含み得る。暗号化された値は、例えば、対称および／または非対称の暗号化技術を利用して、任意の好適な暗号化技術を利用する、識別子（例えば、プライマリＰＡＮ）から生成され得る。一部の実施形態では、暗号化された識別子は、プライマリＰＡＮおよび動的値を利用して生成されてもよく、両方ともにユーザデバイスに保存されている。

【００３３】

本出願の目的のために、「支払データ」は、金融用途に関して、取引を実行するように支払サービスによって使用されるそれらのデータ要素、および非金融取引に関して、本発明を除いて必要ないかなるデータ要素も含むことができる。例えば、支払サービスが、磁気ストライプクレジットカード取引であるとき、「支払データ」は、プライマリアカウント番号、有効期限、サービスコード、および任意データなど、クレジットカード業界の当業者が理解するような、トラック１および／またはトラック２のデータを含むであろう。「支払データ」はまた、一意のカード識別番号、またはサービスプロバイダに対する一意の識別番号も含み得る。支払データは、ユーザデバイス（例えば、クレジットおよび／またはデビットカード、スマートカードなど）上に配置されるメモリの中に存在し得る。

【００３４】

「サーバコンピュータ」は通常、強力なコンピュータまたはコンピュータのクラスタである。例えば、サーバコンピュータは、大型メインフレーム、ミニコンピュータクラスタ、またはユニットとして機能するサーバ群であり得る。一例では、サーバコンピュータは、ウェブサーバに結合されるデータベースサーバであり得る。

【００３５】

「プロセッサ」は、任意の好適な単数または複数のデータ計算デバイスを指すことができる。プロセッサは、所望の機能を達成するために共に動作する、一つ以上のマイクロプロセッサを備えることができる。プロセッサは、ユーザおよび／またはシステム生成要求を実行するプログラム構成要素を実行するのに適切な、少なくとも一つの高速データプロセッサを備えるＣＰＵを含んでもよい。ＣＰＵは、ＡＭＤのアスロン、デュロン、および／もしくはオプテロン、ＩＢＭおよび／もしくはモトローラのＰｏｗｅｒＰＣ、ＩＢＭおよびソニーのセルプロセッサ、インテルのセレロン、アイテニウム、ペンティアム（登録商標）、ジーオン、および／もしくはＸＳｃａｌｅ、ならびに／または同様のプロセッサ（複数可）などのマイクロプロセッサであってもよい。

【００３６】

「メモリ」は、電子データを保存できる、任意の好適な単数または複数のデバイスであっ

てもよい。好適なメモリとして、所望の方法を実施するためにプロセッサによって実行できる命令を保存する、非一時的コンピュータ可読媒体が含まれ得る。メモリの例として、一つ以上のメモリチップ、ディスクドライブなどが含まれ得る。こうしたメモリは、任意の好適な電気的、光学的、および／または磁気的な動作モードを使用して動作することができる。

【００３７】

図１は、一部の実施形態による、取引を処理するためのシステム１００のブロック図を示す。システム１００は、認証、ならびに／または金融取引および非金融取引の承認のために、図１に示す様々なコンピュータ間のデータ通信を促進するように使用され得る。システム１００は、ユーザデバイス１０２、リソースプロバイダコンピュータ１０４、転送コンピュータ１０６、中央サーバコンピュータ１０８、および承認事業体コンピュータ１１０を含む。これらのシステムおよびコンピュータの各々が、互いと動作連通していてもよい。説明を簡単にするために、ある一定数の構成要素を図１に示している。しかしながら、本発明の実施形態は、各構成要素を一つより多く含んでもよいことは理解されるものとする。加えて、本発明の一部実施形態は、図１に示す構成要素のすべてより少ないまたは多い数を含んでもよい。加えて、図１の構成要素は、任意の好適な通信プロトコルを使用して、任意の好適な通信媒体（インターネットを含む）を介して通信してもよい。

【００３８】

リソースプロバイダコンピュータ１０４は、リソースプロバイダ（例えば、小売業者、交通システムなど）によって、またはリソースプロバイダに代わって操作されてもよく、転送コンピュータは、リソースプロバイダと関連付けられてもよい。例えば、転送コンピュータは、リソースプロバイダと関連付けられたアカウントを管理する責任を負う、アクワイアラ（例えば、金融機関）によって操作されてもよい。承認事業体コンピュータ１１０は、発行者（例えば、別の金融機関）によって操作されてもよい。一部の実施形態では、事業体はアクワイアラおよび発行者の両方であり、本発明の実施形態はこうした事業体を含む。

【００３９】

ユーザデバイス１０２は、いかなる好適な形態であってもよい。例えば、ユーザデバイス１０２は、財布および／またはポケットに収まることができるように、携帯型でかつコンパクトであり得る。ユーザデバイス１０２の例としては、スマートカード、クレジットカードおよび／またはデビットカード、キーチェーンデバイスなどを挙げることができる。ユーザデバイス１０２の他の例には、携帯電話、携帯情報端末（ＰＤＡ）、ポケットベル、支払カード、セキュリティカード、アクセスカード、スマートメディア、トランスポンダなどが含まれ得る。ユーザデバイス１０２はまた、小売店舗のポイントなどを保存するためのストアドバリューカードであってもよい。

【００４０】

ユーザデバイス１０２は、コンピュータ可読媒体（ＣＲＭ）１１２および本体１１４を備えてもよい。ＣＲＭ１１２は、プラスチック基材、ハウジング、または他の構造の形態であってもよい、本体１１４上にあり得る。ユーザデバイス１０２は、カードの形態である場合、個人アカウント番号（ＰＡＮ）が浮き出すエンボス領域１１６を有してもよい。一部の実施形態では、ＣＲＭ１１２は、ＰＡＮ、およびセカンダリアカウント番号（例えば、ＳＡＮ）、ならびに／またはカウンタを保存してもよい。

【００４１】

コンピュータ可読媒体１１２は、データを保存するメモリであってもよく、いかなる好適な形態であってもよい。例示のＣＲＭ１１２は、磁気ストライプ、メモリチップなどの形態であってもよい。コンピュータ可読媒体１１２は、プライマリＰＡＮ、ならびに／または暗号化されたおよび／もしくは難読化されたＰＡＮを、暗号化または難読化された形式で電子的に保存し得る。

【００４２】

中央サーバコンピュータ１０８は、承認サービスと、例外ファイルサービスと、清算およ

び決済サービスとをサポートし配信するのに使用される、データ処理サブシステム、ネットワーク、ならびに動作を含んでいてもよい。例示の支払処理ネットワークは、ＶｉｓａＮｅｔ（商標）を含んでいてもよい。ＶｉｓａＮｅｔ（商標）などの支払処理ネットワークは、クレジットカード取引、デビットカード取引、および他のタイプの商取引を処理することができる。特にＶｉｓａＮｅｔ（商標）には、承認要求を処理するＶＩＰシステム（Ｖｉｓａ　Ｉｎｔｅｇｒａｔｅｄ　Ｐａｙｍｅｎｔｓシステム）と、清算および決済サービスを実施するＢａｓｅ　１１システムが含まれる。

【００４３】

中央サーバコンピュータ１０８は、サーバコンピュータを含み得る。サーバコンピュータは通常、強力なコンピュータまたはコンピュータのクラスタである。例えば、サーバコンピュータは、大型メインフレーム、ミニコンピュータクラスタ、またはユニットとして機能するサーバ群であり得る。一例では、サーバコンピュータは、ウェブサーバに結合されるデータベースサーバであり得る。中央サーバコンピュータ１０８は、インターネットを含む、任意の好適な有線または無線ネットワークを使用することができる。

【００４４】

リソースプロバイダコンピュータ１０４は、ユーザデバイス１０２と相互作用できるアクセスデバイス１１８（例えば、自動改札機、ドア、販売時点情報管理端末など）も有してもよく、またはアクセスデバイス１１８からの通信を受信してもよい。図１では、アクセスデバイス１１８は、リソースプロバイダコンピュータ１０４の構成要素であってもよく、ならびに／またはアクセスデバイス１１８は、リソースプロバイダコンピュータによってアクセス可能であり、および／もしくはリソースプロバイダコンピュータ１０４と通信してもよい。一部の実施形態では、アクセスデバイス１１８は、本発明の他の実施形態では、いかなる他の好適な場所にも配置される可能性がある。リソースプロバイダコンピュータ１０４は、リソースプロバイダ（例えば、小売業者）によって操作される、任意の好適な計算装置を含み得る。一部の実施形態では、リソースプロバイダコンピュータ１０４は、リソースプロバイダ（例えば、小売業者）と関連付けられた、一つ以上のウェブサイトをホストし得る、一つ以上のサーバコンピュータを含んでもよい。一部の実施形態では、リソースプロバイダコンピュータ１０４は、ユーザ（例えば、消費者）とリソースプロバイダとの取引のため、支払検証および／または認証プロセスの一部として、転送コンピュータ１０６を介して中央サーバコンピュータ１０８にデータを送るように構成されてもよい。リソースプロバイダコンピュータ１０４はまた、リソースプロバイダとユーザ１０３との取引に対する承認要求メッセージを生成し、追加の取引処理のため、承認要求メッセージを承認事業体コンピュータ１１０に（例えば、転送コンピュータ１０６および／または中央サーバコンピュータ１０８を介して）ルーティングするように構成されてもよい。

【００４５】

本発明の実施形態によるアクセスデバイスは、任意の好適な形態であってもよい。アクセスデバイスの例として、販売時点情報管理（ＰＯＳ）デバイス、自動改札機、ドア、携帯電話、ＰＤＡ、パーソナルコンピュータ（ＰＣ）、タブレットＰＣ、ハンドヘルド専用リーダ、セットトップボックス、電子キャッシュレジスタ（ＥＣＲ）、現金自動預入支払機（ＡＴＭ）、仮想キャッシュレジスタ（ＶＣＲ）、キオスク、セキュリティシステム、アクセスシステムなどが挙げられる。

【００４６】

アクセスデバイス１１８は、リーダ１２０、プロセッサ１２２、およびコンピュータ可読媒体１２４を含み得る。リーダ１２０では、任意の好適な接触または非接触動作モードを使用することができる。例えば、例示のカードリーダには、ユーザデバイス１０２と相互作用するように、ＲＦ（無線周波数）アンテナ、磁気ストライプリーダなどを含むことができる。

【００４７】

少なくとも一実施形態では、ユーザ１０３は、ユーザデバイス１０２（例えば、クレジッ

トカード）を使用して、リソースプロバイダコンピュータ１０４で商品またはサービスの購入を開始し得る。ユーザデバイス１０２は、ＰＯＳ（販売時点情報管理）端末などのアクセスデバイス１１８と、相互作用することができる。例えば、ユーザ１０３は、クレジットカードを取り出してもよく、それをＰＯＳ端末の適切なスロットに通してもよい。あるいは、ＰＯＳ端末が非接触リーダであってもよく、ユーザデバイス１０２が、非接触カードなどの非接触型デバイスであってもよい。この相互作用の間に、ユーザデバイス１０２は、アクセスデバイス１１８が特定のタイプの端末（例えば、ＰＯＳデバイス）であると判定するように構成され得る。アクセスデバイス１１８が、この特定のタイプの端末であると仮定すると、ユーザデバイス１０２は、ユーザデバイス１０２に保存されたプライマリＰＡＮの難読化されたバージョンと、プライマリＰＡＮの暗号化されたバージョンとを、アクセスデバイス１１８に提供し得る。

【００４８】

承認要求メッセージはその後、転送コンピュータ１０６に転送されてもよい。転送コンピュータ１０６は通常、特定のリソースプロバイダ（例えば、小売業者）または他の事業体と取引関係があり、取引のプロセスに関与し得る、ビジネス事業体（例えば、商業銀行）と関連付けられる。転送コンピュータ１０６は、リソースプロバイダ用のアカウントを発行および管理し、リソースプロバイダに代わって、承認事業体コンピュータ１１０と資金を交換し得る。一部の事業体は、承認事業体コンピュータ１１０および転送コンピュータ１０６両方の機能を果たすことができる。本発明の実施形態は、こうした単一事業体の発行者－アクワイアラコンピュータを含む。承認要求メッセージを受信した後、転送コンピュータ１０６は、承認要求メッセージを中央サーバコンピュータ１０８に送り得る。中央サーバコンピュータ１０８はその後、承認要求メッセージを、ユーザデバイス１０２の承認事業体コンピュータ１１０、または承認事業体に代わって役割を果たす第三者事業体に転送し得る。

【００４９】

中央サーバコンピュータ１０８は、処理（例えば、支払処理）に使用される、少なくとも一つのサーバコンピュータを含むか、または操作する、ネットワークであってもよい。中央サーバコンピュータ１０８の中にあるサーバコンピュータは、プロセッサと、プロセッサに結合されたコンピュータ可読媒体とを含んでもよく、コンピュータ可読媒体は、本明細書に記載される機能を果たすために、プロセッサによって実行可能なコードを含む。一部の実施形態では、サーバコンピュータは、データベースに結合されてもよく、一つ以上のクライアントコンピュータからの要求にサービスを提供する、いずれのハードウェア、ソフトウェア、他のロジック、または前述の組み合わせを含んでもよい。サーバコンピュータは、一つ以上の計算装置を備えてもよく、一つ以上のクライアントコンピュータからの要求にサービスを提供する、様々なコンピュータ構造、配置、およびコンパイルのうちのいずれを使用してもよい。一部の実施形態では、中央サーバコンピュータ１０８は、複数のサーバコンピュータを操作し得る。こうした実施形態では、各サーバコンピュータは、所与の領域に対する取引を処理するか、または取引データに基づいて特定タイプの取引に対処するように構成され得る。

【００５０】

中央サーバコンピュータ１０８は、承認サービスと、例外ファイルサービスと、清算および決済サービスとをサポートし配信するのに使用される、データ処理サブシステム、ネットワーク、ならびに動作を含んでいてもよい。中央サーバコンピュータ１０８は、ＶｉｓａＮｅｔ（商標）を含んでもよい。ＶｉｓａＮｅｔ（商標）を含むネットワークは、クレジットカード取引、デビットカード取引、および他のタイプの商取引を処理することができる。特にＶｉｓａＮｅｔ（商標）には、承認要求を処理する統合支払システム（Ｉｎｔｅｇｒａｔｅｄ　Ｐａｙｍｅｎｔｓシステム）と、清算および決済サービスを実施するＢａｓｅ　ＩＩシステムとが含まれる。支払処理ネットワークは、インターネットを含む、任意の好適な有線または無線ネットワークを使用することができる。

【００５１】

中央サーバコンピュータ１０８は、取引要求メッセージを処理し、取引要求メッセージに対する適切な宛先（例えば、認証コンピュータ（複数可））を判定し得る。中央サーバコンピュータ１０８はまた、取引の清算および決済に対処し、ならびに／またはそれらを容易にし得る。

【００５２】

承認事業体コンピュータ１１０は通常、消費者（例えば、ユーザ１０３）用の消費者アカウントを発行および維持する、ビジネス事業体（例えば、銀行）と関連付けられる。承認事業体コンピュータ１１０は、クレジットカードおよびデビットカードなどを含む、消費者アカウント用の支払デバイスを発行してもよい。

【００５３】

承認事業体コンピュータ、または承認事業体に代わって役割を果たす第三者事業体が、承認要求メッセージを受信した後、承認事業体コンピュータ１１０、または発行者に代わって役割を果たす第三者事業体は、ＰＡＮを取引に利用するべきと判定してもよい。例えば、承認事業体コンピュータ１１０は、難読化されたＰＡＮが、承認要求メッセージの中で利用されている、承認要求メッセージの小売業者タイプが、ＰＡＮを含むことを示す、および／または承認要求メッセージの取引タイプが、ＰＡＮを含むことを示すと判定し得る。一部の実施形態では、承認要求メッセージに含まれるＰＡＮは、既知のセカンダリアカウント識別子（ＳＡＮ）のマッピングと照合されてもよく、識別された場合、承認要求メッセージは拒否され得る。一部の実施形態では、承認要求メッセージの中のＰＡＮが、既知のＳＡＮのマッピングに含まれていない（例えば、ＳＡＮではない）場合、メッセージをさらに処理してもよい。ＰＡＮが利用されていると判定されると、承認事業体コンピュータは、取引を許可または却下するように、承認要求メッセージを処理し得る。承認事業体コンピュータは、承認応答メッセージを中央サーバコンピュータ１０８に送り返して、現在の取引が承認されるか否か（または承認されないか）を示してもよい。中央サーバコンピュータ１０８はその後、承認応答メッセージを転送して転送コンピュータ１０６に戻す。次いで転送コンピュータ１０６は、応答メッセージをリソースプロバイダコンピュータ１０４に送り返す。

【００５４】

リソースプロバイダコンピュータ１０４が、承認応答メッセージを受信した後、リソースプロバイダコンピュータ１０４のところにあるアクセスデバイス１１８によって、その後、承認応答メッセージをユーザ１０３に提供し得る。応答メッセージは、アクセスデバイス１１８によって表示されてもよく、またはレシート上に印刷されてもよい。

【００５５】

一日の終わりに、通常の清算および決済プロセスを、システム１００によって行うことができる。清算プロセスは、アクワイアラと発行者との間で金銭的詳細を交換して、ユーザのアカウントへの転記およびユーザの決済状況の調整を容易にするプロセスである。

【００５６】

別の例示的実施形態では、ユーザ１０３は、ユーザデバイス１０２を利用して、オフライン取引を開始してもよい。例えば、ユーザ１０３は、特定の端末タイプを有する（例えば、交通システムへのアクセスを許可／制限する、交通機関の自動改札機および／または料金確認デバイスを示す）アクセスデバイス１１８のところで、ユーザデバイス１０２を提示してもよい。一部の実施形態では、アクセスデバイスが非接触リーダであってもよく、ユーザデバイス１０２が、非接触カードなどの非接触デバイスであってもよい。一部の実施形態では、ユーザデバイス１０２を提示すると、アクセスデバイス１１８は、ユーザデバイス１０２に認証データを要求し得る。アクセスデバイス１１８が特定の端末タイプであるため、ユーザデバイスは、ＣＲＭ１１２のユーザデバイス１０２に保存されたＳＡＮなどの情報を提供し得る。加えて、ユーザデバイスは、アクセスデバイス１１８に提供されるデータ内に、ＰＡＮの暗号化されたバージョンを提供し得る。

【００５７】

承認事業体コンピュータ、または承認事業体に代わって役割を果たす第三者事業体が、承

認要求メッセージを受信した後、承認事業体コンピュータ１１０、または発行者に代わって役割を果たす第三者事業体は、ＳＡＮが承認要求メッセージに含まれることを判定するように構成され得る。例として、承認事業体コンピュータ１１０は、メッセージに含まれるアカウント番号フィールドのデータが、７つのゼロで終わっていないという判定、要求する小売業者が、特定の小売業者タイプ（例えば、交通機関の小売業者タイプ）と関連付けられるという判定、ならびに／または承認要求メッセージが、取引のタイプ（例えば、交通機関の取引）および／もしくは承認要求メッセージが生成された端末のタイプ（例えば、交通端末）を示すという判定に、少なくとも部分的に基づいて、ＳＡＮが承認要求メッセージに含まれると判定してもよい。承認事業体コンピュータは、ＳＡＮの使用を許可しない取引において、ＳＡＮを含むいかなる承認要求メッセージも拒否するように構成され得る。ＳＡＮが許可される取引（例えば、交通機関の取引、料金の取引など）についてのメッセージに、ＳＡＮが含まれる場合、承認事業体コンピュータは、承認要求メッセージの処理を進めて、取引を承認または拒否することができる。承認事業体コンピュータは、承認応答メッセージを中央サーバコンピュータ１０８に送り返して、現在の取引が承認されるか否か（または承認されないか）を示してもよい。中央サーバコンピュータ１０８はその後、承認応答メッセージを転送して転送コンピュータ１０６に戻す。次いで転送コンピュータ１０６は、応答メッセージをリソースプロバイダコンピュータ１０４に送り返す。

【００５８】

少なくとも一実施形態では、承認事業体は、ユーザデバイス１０２に対してパーソナライゼーションプロセスを実施してもよい。このパーソナライゼーションプロセスの間、マスター導出鍵（ＭＤＫ：ｍａｓｔｅｒ　ｄｅｒｉｖａｔｉｏｎ　ｋｅｙ）、ＰＡＮ、およびＳＡＮは、ユーザデバイス１０２（例えば、ＣＲＭ１１２内）に保存され得る。ユーザデバイス１０２は、マスター鍵から一つ以上の一意の導出鍵を導き出す機能を果たすように構成され得る。一部の実施形態では、ユーザデバイス１０２が、マスター鍵および少なくともＰＡＮの一部分を使用して、ＵＤＫを導出してもよい。例えば、ＵＤＫは、マスター鍵およびＰＡＮの左端８桁を使用して導出されてもよい。一部の実施形態では、ＰＡＮの左端８桁は、銀行識別番号（ＢＩＮ）と関連付けられてもよい。

【００５９】

生成されると、ＵＤＫを任意の好適な時点に利用して、暗号化された識別子および／または難読化された識別子を生成してもよい。一部の実施形態では、ＵＤＫは、識別子全体（例えば、ＰＡＮ）だけでなく、カウンタ、日付、時間、および／または取引額などの動的値をも暗号化し得る。例として、ＰＡＮは、ユーザデバイス１０２上に保存された動的値（例えば、取引カウンタ）と連結され、ＵＤＫおよび暗号化アルゴリズムを使用して暗号化されてもよい。一部の実施形態では、暗号化された識別子の一部分（例えば、右端の７桁）は識別し、難読化された識別子を生成しするように使用され得る。一部の実施形態では、難読化された識別子は、ＰＡＮの元の８桁（ＢＩＮに対応する）、暗号化された識別子の一部分、およびチェックサム値（例えば、Ｌｕｈｎチェックサムに対応する）を含み得る。その上さらなる実施形態では、難読化された識別子は、ＰＡＮの元の８桁（ＢＩＮに対応する）、任意の好適な数のパディング値（例えば、７つのゼロ）、およびチェックサム値を含み得る。難読化された識別子および／または暗号化された識別子は、ユーザデバイス１０２に保存され得る。

【００６０】

取引の初期化時（例えば、非交通機関での取引）、または別の好適な時点に、ユーザデバイス１０２は、難読化された値および暗号化された識別子を、データトラックの形態で提供するように構成され得る。データトラックは、トラック１またはトラック２のデータトラックとしてフォーマットできる。トラック１（「国際航空運送協会」）は、トラック２よりも多くの情報を保存し、カード所有者の氏名だけでなく、アカウント番号および他の任意データも含む。このトラックは、クレジットカードで予約を確保するときに、航空会社が使用することがある。トラック２（「米国銀行協会」（ＡＢＡ））が現在最もよく使

用されている。トラック２は、ＡＴＭおよびクレジットカードチェッカーによって読み取られてもよい。ＡＢＡがトラック２の仕様を設計しており、全世界の銀行が従わなければならない。カード保有者のアカウント、暗号化されたＰＩＮ、および他の任意データが含まれる。

【００６１】

一部の実施形態では、難読化された値は、従来ユーザのアカウント番号（例えば、タグ５７）を含む、トラック２のデータトラックのデータフィールドに提供されてもよい。一部の実施形態では、暗号化された識別子は、トラック２のデータトラックの異なる部分（例えば、タグ９Ｆ１Ｆ（任意データタグ）に、タグ９Ｆ７Ｃ（顧客専用データタグ）に、タグ９Ｆ１０（発行者アプリケーションデータ）に、もしくはトラック２のデータの任意の好適な部分に、または上記のいかなる好適な組み合わせ）に提供されてもよい。

【００６２】

他の実施形態では、取引（例えば、交通機関の取引）の初期化時、または別の好適な時点に、ユーザデバイス１０２は、ＳＡＮおよび暗号化された識別子を、データトラックの形態で提供するように構成され得る。一部の実施形態では、ＳＡＮは、従来ユーザのアカウント番号（例えば、タグ５７）を含む、トラック２のデータトラックのデータフィールドに提供されてもよい。一部の実施形態では、暗号化された識別子は、トラック２のデータトラックの異なる部分（例えば、タグ９Ｆ１Ｆ（任意データタグ）に、タグ９Ｆ７Ｃ（顧客専用データタグ）に、タグ９Ｆ１０（発行者アプリケーションデータ）に、もしくはトラック２のデータの任意の好適な部分に、または上記のいかなる好適な組み合わせ）に提供されてもよい。

【００６３】

従来の取引処理によれば、アクセスデバイス１１８は、トラック２のデータトラックを受信し、データをリソースプロバイダコンピュータ１０４に提供してもよく、リソースプロバイダコンピュータ１０４は、その後、トラック２のデータの少なくとも一部分を、承認要求メッセージによって転送コンピュータ１０６に転送し得る。一部の実施形態では、アクセスデバイス１１８は、承認要求メッセージを生成し、トラック２のデータの少なくとも一部分を含み、承認要求メッセージを直接、転送コンピュータ１０６に転送し得る。

【００６４】

受信時、または別の好適な時点に、転送コンピュータ１０６は、承認要求メッセージを中央サーバコンピュータ１０８に転送し得る。中央サーバコンピュータ１０８は、暗号化された値が承認要求メッセージの中に存在すると判定し得る。中央サーバコンピュータ１０８は、マスター導出鍵および難読化された識別子の一部分（承認メッセージにも含まれる）を利用して、保存されたＵＤＫを読み出すか、ならびに／またはＵＤＫを導出し得る。ＵＤＫを中央サーバコンピュータ１０８が利用して、暗号化された値を復号して、暗号化されていないＰＡＮ全体を取得し得る。一部の実施形態では、中央サーバコンピュータ１０８は、承認要求メッセージを修正して、暗号化されていないＰＡＮを含め、さらなる処理のために、修正された承認要求メッセージを承認事業体コンピュータ１１０へ送信し得る。

【００６５】

他の実施形態では、中央サーバコンピュータ１０８および／または承認事業体コンピュータ１１０は、難読化された識別子の少なくとも一部分（例えば、ＢＩＮに対応する最初の８桁）を利用して、変更されていない承認要求メッセージを承認事業体コンピュータ１１０に転送し得る。承認事業体コンピュータ１１０は、マスター導出鍵、および難読化された識別子の一部分またはＳＡＮ（承認メッセージにも含まれる）を利用して、保存されたＵＤＫを読み出すか、ならびに／またはＵＤＫを導出し得る。ＵＤＫを承認事業体コンピュータ１１０が利用して、暗号化された識別子を復号して、暗号化されていないＰＡＮ全体を取得し得る。中央サーバコンピュータ１０８および／または承認事業体は、ＳＡＮを利用して、関連付けられたＰＡＮを読み出すために、既知のＰＡＮ／ＳＡＮの関連付けを示すマッピングを調べてもよい。関連付けられたＰＡＮを、暗号化されていないＰＡＮと

比較して、承認要求メッセージを検証することができる。
【００６６】
承認事業体コンピュータ１１０は、承認要求メッセージを処理し、承認応答メッセージを送信して中央サーバコンピュータ１０８に戻してもよい。一部の実施形態では、承認応答メッセージは、難読化された識別子および暗号化された値を含み、暗号化されていない識別子を除外してもよい。
【００６７】
中央サーバコンピュータ１０８は、承認応答メッセージを転送して、転送コンピュータ１０６を介してリソースプロバイダコンピュータ１０４に戻し得る。リソースプロバイダコンピュータ１０４が、承認応答メッセージを受信した後、リソースプロバイダコンピュータ１０４のところにあるアクセスデバイス１１８によって、その後、承認応答メッセージをユーザ１０３に提供し得る。応答メッセージは、アクセスデバイス１１８によって表示されてもよく、またはレシート上に印刷されてもよい。
【００６８】
一日の終わりに、通常の清算および決済プロセスを、システム１００によって行うことができる。
【００６９】
本明細書に記載される技術を利用することによって、機密データ（例えば、ＰＡＮ）を伝達するためのより安全な方法が可能になる。静的識別子が必要な取引（例えば、ブロックリストに基づいてアクセスを確認または拒否するために）については、ＳＡＮを利用して取引を実施し得る。ＳＡＮを利用し、ＳＡＮが特定のタイプ（複数可）の取引（例えば、交通機関の取引、料金の取引など）でのみ利用され得ることを保証することによって、ＳＡＮは不正行為者から保護される。たとえ不正行為者が盗聴して、ＳＡＮにアクセスすることができたとしても、システムによって、ＳＡＮが特定のタイプの取引にのみ利用され、他の取引には利用できないことが保証されるであろう。他の取引（例えば、非交通機関での取引）に対して、ＰＡＮは暗号化され、従来とは異なるデータフィールドに提供され、通常ＰＡＮを含むであろう、従来のデータフィールドには代わりに、ＰＡＮが判定される可能性の低い、難読化された値が含まれる。難読化された値には、依然として元のＢＩＮが含まれ、承認要求／応答メッセージに対する従来のルーティング技術は、変わらないままであることが保証され得る。本明細書に記載される技術によって、承認要求／応答メッセージからＰＡＮを識別することが、不可能でないにしても困難になる。加えて、一部の実施形態では、ＰＡＮは、常に変化している動的値を使用して暗号化される。したがって、暗号化された値および難読化された値は、承認要求ごとに変更することができ、特定のユーザに対する取引を経時的に追跡することが、不可能でないにしても困難になる。それゆえ、本明細書で論じる技術を利用することで、機密データを送信するためのプライバシーの保護およびセキュリティが向上する。
【００７０】
図２は、一部の実施形態による、データを生成しユーザデバイス（例えば、図１のユーザデバイス１０２）に保存する方法２００を示す。方法２００は、承認事業体コンピュータ（例えば、承認事業体コンピュータ１１０）がマスター導出鍵を取得し得る、２０２から始まってもよい。一部の実施形態では、マスター導出鍵（ＭＤＫ）を利用して、一つ以上の一意の導出鍵を導き出してもよい。承認事業体コンピュータ１１０は、一つのユーザデバイスに対するＭＤＫが、そのユーザデバイスに対して一意であることを保証し得る。したがって、承認事業体コンピュータ１１０は、様々なユーザデバイス（例えば、ユーザデバイス１０２）に対応し得る、多くのマスター導出鍵を管理してもよい。
【００７１】
２０４で、承認事業体コンピュータ１１０は、ユーザデバイスがパーソナライズされるユーザに対応する、個人アカウント番号（ＰＡＮ）を取得し得る。少なくとも一実施形態では、ＰＡＮは、ユーザに代わって承認事業体によって管理される、ユーザの金融口座と関連付けられ得る。

【００７２】
２０６で、承認事業体コンピュータ１１０は、セカンダリアカウント番号（ＳＡＮ）を取得および／または生成し得る。全体を通して論じるように、ＳＡＮが一つ以上の特定タイプの取引でのみ利用され得るように、ＳＡＮは、承認事業体のコンピュータ１１０によって制限されてもよい。例として、交通システムまたは料金の確認システムなどで、ユーザを迅速に（例えば、リアルタイムまたはほぼリアルタイムで）認証しなければならない場合があり得る。システムの状況を考えると、ほぼリアルタイムでリソース（例えば、交通リソース）へのアクセスを可能にするほど十分迅速に、ユーザのオンライン認証を実施することが可能ではない場合がある。したがって、一部の認証システムでは、アクセスデバイスでオフライン認証を実施し、その後、関係する取引を行うための承認要求メッセージでフォローアップする。このＳＡＮを生成して、こうしたオフライン認証シナリオで利用してもよい。
【００７３】
２０８で、承認事業体コンピュータ１１０は、ＰＡＮとＳＡＮとの関係を示す、アカウント番号マッピングを維持してもよい。承認事業体コンピュータ１１０は、図５に関してより詳細に論じるように、検証の目的でマッピングを利用するように構成されてもよい
【００７４】
２１０で、承認事業体コンピュータ１１０は、ユーザデバイス１０２にデータを送信し得る。例として、承認事業体コンピュータ１１０は、ＭＤＫ、ＰＡＮ、およびＳＡＮをユーザデバイス１０２に送信し得る。一部の実施形態では、承認事業体コンピュータ１１０が、データを中間デバイスに送信してもよく、その後、中間デバイスがデータをユーザデバイス１０２に転送し得る。
【００７５】
２１２で、データはＣＲＭ１１２内のユーザデバイス１０２に保存され得る。２１４で、ユーザデバイス１０２は、ＭＤＫを使用して、一つ以上の一意の導出鍵を生成してもよい。例として、一意の導出鍵（ＵＤＫ：ｕｎｉｑｕｅ　ｄｅｒｉｖａｔｉｏｎ　ｋｅｙ）は、図３に関係してより詳細に記載されるプロセスにより生成され得る。一つ以上のＵＤＫが生成されてもよく、各ＵＤＫは特定の目的のために利用されてもよいことは理解されるべきである。例えば、ＵＤＫはＭＡＣ用に、別のＵＤＫは暗号化用に、また別のＵＤＫは暗号文生成用に生成されてもよく、さらに別のＵＤＫは図３のプロセスによって生成され得る。ユーザデバイス１０２が、好適な数のＵＤＫを生成してもよく、またはこうしたＵＤＫが代わりに、２０２もしくは任意の好適な時点に、承認事業体コンピュータ１１０によって生成されてもよいことは理解されるべきである。
【００７６】
２１６で、ユーザデバイス１０２は、承認事業体コンピュータ１１０によって有効化されてもよい。有効化されると、ユーザデバイス１０２は、アクセスデバイスで、または様々な取引を実施するためにオンラインで利用され得る。
【００７７】
図３は、一部の実施形態による、ユーザデバイス（例えば、スマートカード）上に常駐するデータから、一意に導出された鍵を生成するための方法を示す。方法は、ユーザデバイス１０２の一つ以上のプロセッサを利用して、図１のユーザデバイス１０２によって実施されてもよい。
【００７８】
少なくとも一実施形態では、マスター導出鍵（ＭＤＫ）３０２および識別子３０４は、パーソナライゼーションプロセス（例えば、図２の方法２００）の実施中、ユーザデバイス１０２に保存されている。一部の実施形態では、識別子３０４は、個人アカウント番号の例であってもよい。ＵＤＫ３０６は、ユーザデバイス１０２上に存在するこうしたデータから導出されてもよい。
【００７９】
例として、ユーザデバイス１０２は、識別子３０８の一部分を識別するように構成されて

もよい。一部の実施形態では、その識別子３０８の一部分は、識別子３０４全体よりも少ない部分を含み得る。例えば、その識別子３０８の一部分は、識別子３０４の左端８桁を含み得る。一部の実施形態では、識別子３０４の左端８桁は、支払処理ネットワーク（例えば、システム１００）内のルーティングのために使用され得る、銀行識別番号（ＢＩＮ）に対応してもよい。

【００８０】

一部の実施形態では、その識別子３０８の一部分は、所定の固定長の文字列を作成するように、いくつかのパディングビット（例えば、パディング３１０）と連結されてもよい。一部の例では、連結された値は、パディングが６４ビットを含み、識別子３０８の一部分が、別の６４ビット（各々８ビットを含む８桁）を含む、長さ１２８ビットであってもよいが、連結された値は、この長さであることに限定されない。連結された値は、ＭＤＫ３０２と共に、データ暗号化アルゴリズム３１２への入力として提供されてもよい。

【００８１】

データ暗号化アルゴリズム３１２は、任意の好適な暗号化方法論を含み得る。例えば、データ暗号化アルゴリズム３１２には、トリプルＤＥＳ暗号化アルゴリズムを利用してもよい。一部の実施形態では、データ暗号化アルゴリズム３１２によって行われる暗号化から生じる値が、ＵＤＫ３０６である。

【００８２】

図４は、一部の実施形態による、オフライン認証を実施するための方法４００を示す。方法は、発見プロセスがアクセスデバイス１１８によって実行され得る、４０２から始まってもよい。例えば、図１のリーダ１２０は、リーダのＲＦフィールドに入ってきた可能性のある、非接触カードの存在に対してポーリングしてもよい。

【００８３】

４０４で、アクセスデバイス１１８は、ユーザデバイス１０２でアプリケーション選択プロセスを開始し得る。アプリケーション選択プロセスは、ユーザデバイス１０２の有効化後、直ちに実施されてもよく、ユーザデバイス１０２およびアクセスデバイス１１８（またはリーダ１２０）の両方がサポートするアプリケーションのうちの、どのアプリケーションを使用して、取引を行うかを判定するプロセスである。例として、アクセスデバイス１１８（例えば、アクセスデバイス１１８のリーダ１２０）は、相互にサポートするアプリケーションの候補リストを作成し得る。候補リストからの単一のアプリケーションを識別し選択して、取引を処理し得る。

【００８４】

４０６で、アプリケーション処理を開始してもよい。例えば、アクセスデバイス１１８（またはリーダ１２０）は、ユーザデバイス１０２に、取引処理が始まると信号を送ってもよい。一部の実施形態では、取引処理の開始では、アクセスデバイス１１８（リーダ１２０）からユーザデバイス１０２へ、ＧＥＴ　ＰＲＯＣＥＳＳＩＮＧ　ＯＰＴＩＯＮＳ（処理オプション取得）コマンドを送ることによって、信号を送ることができる。このコマンドを発行するとき、アクセスデバイス１１８は、任意の好適なデータ要素を提供し得る。一部の実施形態では、ユーザデバイス１０２およびアクセスデバイス１１８（リーダ１２０）によって、相互にサポートされる非接触経路（複数可）が判定され、非接触経路を選んで取引を処理してもよい。後続の取引処理は、選ばれた非接触経路に従って実施されてもよい。

【００８５】

４０８で、ユーザデバイス１０２は、アプリケーションデータを、アクセスデバイス１１８（リーダ１２０）に戻して提供してもよい。一部の実施形態では、ユーザデバイス１０２が最初に、ＧＥＴ　ＰＲＯＣＥＳＳＩＮＧ　ＯＰＴＩＯＮＳを受信してもよい。コマンドに応じて、ユーザデバイス１０２は、任意の好適なアプリケーションデータを生成し得る。例として、ユーザデバイス１０２に保存されたカウンタが、修正されてもよい（例えば、値の増加、減少など）。ユーザデバイス１０２は、保存されたＰＡＮと共にカウンタを利用して、ユーザデバイス１０２にも保存され得る、暗号化されたＰＡＮを生成し得る

。ＧＥＴ　ＰＲＯＣＥＳＳＩＮＧ　ＯＰＴＩＯＮＳコマンドによって、アクセスデバイス１１８が特定の端末タイプ（例えば、非交通端末タイプ、またはユーザデバイスに保存される端末タイプの第一のセットの端末タイプなど）であると示される場合に、ユーザデバイス１０２は、保存されたＰＡＮの一部分および暗号化された識別子の一部分から、難読化されたＰＡＮを生成し得る。難読化されたＰＡＮおよび暗号化された識別子は、この使用事例ではアプリケーションデータとして提供され得る。しかしながら、ＧＥＴ　ＰＲＯＣＥＳＳＩＮＧ　ＯＰＴＩＯＮＳコマンドによって、アクセスデバイス１１８が別の特定の端末タイプ（例えば、交通端末タイプ、またはユーザデバイスに保存される端末タイプの第二のセットの端末タイプなど）であると示される場合に、ユーザデバイス１０２は、保存されたＳＡＮおよび暗号化された識別子を、アプリケーションデータとして提供し得る。

【００８６】

４１０で、アクセスデバイス１１８（リーダ１２０）が、取引を処理するために必要なアプリケーションデータを読み取ると、アプリケーションデータの読み取りは完了とみなされ得る。読み取り時間中、アクセスデバイス１１８は、取引に必須の全データ要素が、カードによって返ってきたかを判定し得る。必須のデータ要素すべてが返ってきたわけではない場合、または冗長なデータが返ってきた（例えば、データ要素の発生が二回以上返された）場合、アクセスデバイス１１８（リーダ１２０）は取引を終了してもよい。

【００８７】

４１２で、アクセスデバイス１１８（リーダ１２０）は制限を処理してもよい。例として、アクセスデバイス１１８（リーダ１２０）は、アプリケーションの有効期限、アプリケーションの使用法、および／またはＳＡＮが端末例外ファイル（ＴＥＦ：Ｔｅｒｍｉｎａｌ　Ｅｘｃｅｐｔｉｏｎ　Ｆｉｌｅ）上にあるかを確認し得る。ＴＥＦは、リソースへのアクセスを与えるべきではないＳＡＮが保存されている、ブラックリストと見なされ得る。ＳＡＮが端末例外ファイルに登場する場合、アクセスデバイス１１８（リーダ１２０）は、ユーザデバイス１０２にアクセス（例えば、アクセスデバイス１１８によって管理される自動改札機への）を与えないように構成されてもよく、さらなる処理は行われなくてもよい。

【００８８】

しかしながら、ＳＡＮがＴＥＦに含まれない場合、方法４００は、オフラインデータ認証を実行し得る、４１４に進んでもよい。オフラインデータ認証は、オフライン取引をサポートするアクセスデバイス（リーダ）に対して実施されてもよく、オフライン取引が要求されるユーザデバイスに対して実施されてもよい。オフラインデータ認証中、アクセスデバイス１１８（リーダ１２０）は、ユーザデバイス１０２によって返される動的署名を検証してもよく、ユーザデバイス１０２からのデータを認証し得る。

【００８９】

一部の実施形態では、アクセスデバイス１１８（リーダ１２０）は、オンライン取引をサポートしてもよい。これらの実施形態では、アクセスデバイス１１８（リーダ１２０）は、４１６で承認要求メッセージを、承認事業体コンピュータ１１０に（例えば、図１の転送コンピュータ１０６および／または中央サーバコンピュータ１０８を介して）送ってもよい。承認要求メッセージは、ＳＡＮおよびユーザデバイス１０２に保存される暗号化された識別子を含み得る。

【００９０】

４１８で承認要求メッセージを受信すると、または任意の好適な時点に、承認事業体コンピュータ１１０は、所定のホストベースのリスク管理パラメータを使用して、取引を検討し、承認または拒否する。一部の実施形態では、承認事業体コンピュータ１１０は、取引がＳＡＮを含むことを判定するように構成されてもよい。一部の実施形態では、承認要求メッセージのアカウント識別子フィールドの値が読み出され、対応するＰＡＮにマッピングされる、既知の全ＳＡＮを含むマッピングと比較されてもよい。アカウント識別子フィールドの値が、既知のＳＡＮと等しい場合、取引はＳＡＮを利用していると判定され得る

。一部の実施形態では、承認事業体コンピュータ１１０は、取引を開始するアクセスデバイス（例えば、アクセスデバイス１１８）が特定のタイプであるか、もしくはアクセスデバイスと関連付けられた小売業者が、特定の小売業者タイプであるか、または承認要求メッセージの取引タイプが、許容可能な取引タイプを示す取引においてのみ、ＳＡＮを利用することが可能になるように構成されてもよい。非限定的な例として、承認事業体コンピュータ１１０は、非交通端末タイプと関連付けられるアクセスデバイス（例えば、非交通機関の小売業者によって操作されるアクセスデバイス）を伴う取引で、ＳＡＮを利用するオンライン処理を拒否し、一方で、交通端末タイプと関連付けられるアクセスデバイス（例えば、交通機関の小売業者によって操作されるアクセスデバイス１２０）を伴う取引のために、ＳＡＮを利用するオンライン処理を許可するように構成されてもよい。

【００９１】

一部の実施形態では、承認要求メッセージに含まれるＳＡＮは、暗号化された識別子に対応するＰＡＮと関連付けられてもよい。承認事業体コンピュータ１１０は、銀行識別番号（ＢＩＮ）に対応するＳＡＮの左端８桁を読み出すように構成され得る。承認事業体コンピュータ１１０は、ＢＩＮと、承認事業体コンピュータ１１０によって維持されるマッピングに保存されるような、ＳＡＮと関連付けられたＰＡＮとを利用して、ＵＤＫを導出し得る。導出されたＵＤＫを使用して、承認事業体コンピュータ１１０は、承認メッセージの暗号化された識別子を復号して、復号されたＰＡＮを判定し得る。復号されたＰＡＮは、マッピングに保存され、メッセージのＳＡＮと関連付けられたＰＡＮと比較されてもよい。復号されたＰＡＮが保存されたＰＡＮと一致する場合、メッセージは有効とみなされ、そうでない場合には、無効とみなされ得る。承認事業体コンピュータ１１０はさらに、従来のオンライン不正および信用調査を実施し、カード生成暗号文を利用して、オンラインカード認証を実施するなどを行い得る。

【００９２】

図５は、一部の実施形態による、機密データを安全に伝達するための方法５００のフローチャートを示す。方法５００は、コンピューティングデバイス（例えば、図１のユーザデバイス１０２、スマートカード）によって実施されてもよい。コンピューティングデバイスは、一つ以上のプロセッサと、コンピュータ実行可能命令を保存する一つ以上のメモリとを備えてもよく、一つ以上のプロセッサによりコンピュータ実行可能命令を実行することによって、コンピューティングデバイスに方法５００を実施させる。図５に示し以下に記載されるステップは、図１の取引処理の説明および対応する説明と併せて使用することができる。それらの説明は、参照により本明細書に組み込まれる。コンピューティングデバイスは、一つ以上のＵＤＫ、第一の識別子（例えば、セカンダリアカウント番号（ＳＡＮ））、第二の識別子（例えば、プライマリアカウント番号（ＰＡＮ））、動的値、またはコンピューティングデバイスのメモリ内にある任意の好適なデータを保存し得る。

【００９３】

暗号化された識別子は、任意の好適なタイプで（例えば、図４に関係して上で論じたように、アクセスデバイスからＧＥＴ　ＰＲＯＣＥＳＳＩＮＧ　ＯＰＴＩＯＮＳコマンドを受信した後）、生成されてもよい（例えば、コンピューティングデバイスによって）。コンピューティングデバイスは、一意の導出鍵（例えば、ＵＤＫ２０６）を使用して、第二の識別子（例えば、ＰＡＮ）および動的値（例えば、カウンタ、日付、時間など）を暗号化することによって、暗号化された識別子を生成し得る。一部の実施形態では、第二の識別子および動的値は、暗号化される前に、共に、および／または追加のパディング値で連結されてもよい。一部の実施形態では、暗号化された識別子は、コンピューティングデバイスに保存されてもよい（例えば、タグ９Ｆ７Ｃ（顧客専用データタグ）および／もしくはタグ９Ｆ１０（発行者アプリケーションデータ）など、トラック１ならびに／もしくはトラック２のデータの一部として、タグ９Ｆ１Ｆ（任意データタグ）の中に、もしくはトラック１および／もしくはトラック２のデータのいずれかの部分の中に、または上記のいかなる好適な組み合わせ。加えて、または代替で、暗号化された識別子は、上記のタグのいずれか、またはトラック１および／もしくはトラック２のデータの別の好適な部分で潜在

的に利用可能な、将来使用するため確保されているデータフィールドの一部として提供されてもよい。

【００９４】

方法５００は、要求メッセージが、コンピューティングデバイス（例えば、スマートカード）によって、アクセスデバイス（例えば、自動改札機）から受信され得る、ブロック５０２から始まってもよい。一部の実施形態では、要求メッセージは、上記のような図４のＧＥＴ　ＰＲＯＣＥＳＳＩＮＧ　ＯＰＴＩＯＮＳコマンドに対応し得る。アクセスデバイスは、ユーザデバイスにデータを要求するように構成された、任意の好適なデバイスであってもよい。

【００９５】

５０４で、コンピューティングデバイスは、要求メッセージに少なくとも部分的に基づいて、要求するアクセスデバイスのタイプ指標を判定し得る。例として、要求メッセージは、要求が特定のタイプの端末／アクセスデバイスによって開始されたことを示す、タイプ指標を含み得る。非限定的な例として、要求メッセージは、要求するデバイスが、地下鉄システムなどの交通システム内にある自動改札機であることを示していてもよい。コンピューティングデバイスは、タイプ指標が第一のタイプセット（例えば、交通タイプを含む第一のタイプセット）に属するか否かを判定してもよい。

【００９６】

５０６で、タイプ指標が第一のタイプセットに含まれると判定された場合、または要求メッセージが特定のタイプの端末／アクセスデバイスによって開始されたと判定される場合、コンピューティングデバイスは、少なくとも第一の識別子（例えば、ＳＡＮ）、およびＰＡＮから生成／導出された暗号化された識別子を含む、第二のメッセージを（例えば、アクセスデバイスへ）送信し得る。一部の実施形態によれば、メッセージは、アクセスデバイスに提供されてもよく、アクセスデバイスによって、コンピューティングデバイスのユーザが、リソースへのアクセスを許可または拒否される。非限定的な例として、交通機関の駅にある自動改札機などのアクセスデバイスでは、第一の識別子（例えば、ＳＡＮ）に基づいて、ユーザへのアクセスが許可または拒否され得る。図４に関係して上に記載されるように、一部の実施形態では、アクセスデバイス（または関連付けられたリソースプロバイダコンピュータ）は続いて、承認要求メッセージを生成し得る。承認要求メッセージは、とりわけ、第一の識別子（ＳＡＮ）を含む第一のデータフィールドと、暗号化された識別子を含む第二のデータフィールドとを含み得る。一部の実施形態では、承認要求メッセージは、さらなる承認処理のために、中央サーバコンピュータ（例えば、図１の中央サーバコンピュータ１０８）に送信される。

【００９７】

５０８で、タイプ指標が、第一のタイプセットに含まれないと判定された場合、または特定タイプの端末／アクセスデバイスではないと判定された場合、難読化された識別子が生成され得る（例えば、ユーザデバイス１０２によって）。一部の実施形態では、難読化された識別子は、第二の識別子（ＰＡＮ）の最初の８桁、７つのゼロ、およびＬｕｈｎチェックサム値を含み得る。他の実施形態では、難読化された識別子は、第二の識別子（例えば、ＰＡＮ）のその一部分および暗号化された識別子の一部分に、少なくとも部分的に基づいて生成されてもよい。例として、難読化された識別子は、識別子の最初の８桁および暗号化された識別子の最後の７桁（または任意の好適な数のゼロ）を含むように生成されてもよい。これは単に一例であり、識別子のより少ないまたは多い桁、および暗号化された識別子のより少ないまたは多い桁が利用され得る。同様に、難読化されたものは、１６桁または任意の好適な数の桁を含み得る。一部の実施形態では、Ｌｕｈｎチェックサム値は、難読化された識別子から計算され、難読化された識別子の一部として含まれてもよい（例えば、進行中の例では最後の桁、桁１６）。

【００９８】

５１０で、第二のメッセージ（例えば、トラック２のメッセージ）が提供されてもよい（例えば、ユーザデバイス１０２によって）。一部の実施形態では、メッセージは、少なく

とも難読化された識別子および暗号化された識別子を含んでもよい。一部の実施形態によれば、メッセージは、アクセスデバイス（例えば、アクセスデバイス１１８）に提供されてもよく、アクセスデバイスによって、承認要求メッセージを生成させる（例えば、図１のアクセスデバイス１１８および／またはリソースプロバイダコンピュータ１０４によって）。承認要求メッセージは、とりわけ、難読化された識別子を含む第一のデータフィールドと、暗号化された識別子を含む第二のデータフィールドとを含み得る。一部の実施形態では、承認要求メッセージは、さらなる承認処理のために、中央サーバコンピュータ（例えば、図１の中央サーバコンピュータ１０８）に送信される。

【００９９】

図６は、一部の実施形態で使用する、例示的な記録形式６００を示す。例えば、記録形式６００は、ＳＡＮおよび暗号化された識別子を含む、トラック２のデータ（例えば、認証データ）を含み得る。記録形式６００は、図５の５０６に関係して記載される、第二のメッセージの例であってもよい。非限定的な一例では、ＰＡＮ６０１は、ユーザと関連付けられ、ユーザのデバイス（例えば、スマートカード）上に保存されてもよい。一部の実施形態では、ＳＡＮ６０２は、ユーザと関連付けられ、ユーザのデバイス上に保存されてもよい。図６に説明するように、ＰＡＮ６０１およびＳＡＮ６０２は各々１６桁を含んでもよい。一部の実施形態では、ＰＡＮ６０１は、トラック２のデータによって定義されるように、トラック２のデータのタグ５７に保存される。一部の実施形態では、ＳＡＮ６０２は、トラック２のデータによって定義されるように、トラック２のデータのタグ５Ａに保存される。

【０１００】

記録形式６００の最初の１６桁（例えば、識別子データフィールド６０３）（例えば、桁１～１６）は従来、ＳＡＮ６０２に確保され得る。次に、区切り文字データフィールド６０４が、アカウント識別子と有効期限データフィールド６０６との間に緩衝を提供する。サービスコードデータフィールド６０８が、有効期限データフィールド６０６に続いてもよい。個人識別番号検証指標（ＰＶＫＩ）データフィールド６１０およびＰＩＮ検証情報データフィールド６１４が後に続く。次に、ｄＣＶＶデータフィールド６１４、取引カウンタデータフィールド６１６、および非接触指標データフィールド６１８が含まれる。最後に、任意データフィールド６２０が後に続く。任意データフィールドは、暗号化値データフィールド６２１および暗号文バージョン番号データフィールド６２３を含み得る。暗号化値データフィールド６２１および暗号文バージョン番号データフィールド６２３は、必ずしも図６に示される数ではなく、任意の好適な桁数を含んでもよい。

【０１０１】

一部の実施形態によれば、ＰＡＮ６０１を最初に利用して、暗号化された値（例えば、暗号化された識別子）を生成してもよい。例として、図１のユーザデバイス１０２は、図３のＰＡＮ６０１およびＵＤＫ３０６を、記憶装置から読み出すように構成されてもよい。一部の実施形態では、取引カウンタ（または他の動的値）もまた読み出されてもよい。ＰＡＮおよび取引カウンタ（または他の動的値）は、暗号化アルゴリズムへの入力として、ＵＤＫ３０６と共に利用されて、暗号化された値を生成し得る。一部の実施形態では、ＰＡＮおよび取引カウンタ（または他の動的値）は、入力の前に連結されてもよい。結果として得られた暗号化された値は、記録形式６００で保存され得る。例として、結果として得られた暗号化された値は、任意データフィールド６２０の暗号化値データフィールド６２１内に示されるように保存されてもよい。一部の実施形態では、任意データフィールド６２０は、トラック２標準によって定義される、特定のタグに対応する（例えば、タグ９Ｆ１Ｆ（任意データタグ）、タグ９Ｆ７Ｃ（顧客専用データタグ）、タグ９Ｆ１０（発行者アプリケーションデータ）、トラック２のデータの任意の好適な部分、または上記の任意の好適な組み合わせで）。

【０１０２】

一部の実施形態では、暗号文バージョン番号データフィールド６２３は、任意データフィールド６２０が、暗号化値データフィールド６２１内に暗号化された値を含むことを示す

、番号を保存してもよい。
【０１０３】
一部の実施形態によれば、ユーザデバイス１０２は、識別子データフィールド６０３にＳＡＮ６０２を提供するように構成され得る。識別子データフィールド６０３の桁１６は、識別子データフィールド６０３が、変更されていないことを検証するために利用され得る（例えば、受信時に）、チェックサム値（例えば、Ｌｕｈｎチェックサム／値）を含み得る。一部の実施形態では、ユーザデバイス１０２によって、トラック２のデータの要求者が、特定の端末タイプ（例えば、交通端末タイプ、オフライン認証に関連付けられた端末タイプなど）と関連付けられていると判定されたとき、ＳＡＮ６０２が、識別子データフィールド６０３内に提供されてもよい。
【０１０４】
取引が開始されると、識別子データフィールド６０３内に含まれるＳＡＮ６０２、および任意データフィールド６２０内の（例えば、暗号化値データフィールド６２１の）暗号化された値が、提供されてもよい（例えば、上記のようにアクセスデバイスに）。一部の実施形態では、取引カウンタの値を増加（または減少）することができ、および／または新しい動的値を、取引カウンタデータフィールド７１６の中に生成し保存してもよい。別の取引がユーザデバイス１０２によって開始される場合、本明細書で論じるプロセスは、新しい取引カウンタ／動的値およびＰＡＮ７０１を利用して繰り返されて、その後、後続の取引で提供され得る、新しい暗号化された値および新しい難読化された識別子を生成してもよい。
【０１０５】
図７は、一部の実施形態で使用する、別の例示的な記録形式７００を示す。例えば、記録形式７００は、難読化された識別子および暗号化された識別子を含む、トラック２のデータ（例えば、支払データ）を含み得る。記録形式６００は、図５の５１０に関係して記載される、第二のメッセージの例であってもよい。非限定的な一例では、ＰＡＮ７０１は、ユーザと関連付けられ、ユーザのデバイス（例えば、スマートカード）上に保存されてもよい。一部の実施形態では、ＳＡＮ７０２もまた、ユーザと関連付けられ、ユーザのデバイス上に保存されてもよい。図７に説明するように、ＰＡＮ７０１およびＳＡＮ７０２は各々１６桁を含んでもよい。一部の実施形態では、ＰＡＮ７０１は、トラック２のデータによって定義されるように、トラック２のデータのタグ５７に保存される。一部の実施形態では、ＳＡＮ７０２は、トラック２のデータによって定義されるように、トラック２のデータのタグ５Ａに保存されてもよい。
【０１０６】
記録形式７００の最初の１６桁（例えば、識別子データフィールド７０３）（例えば、桁１～１６）は、アカウント識別子の難読化されたバージョン（例えば、難読化されたＰＡＮ７０３、ＰＡＮ７０１の難読化されたバージョン）に確保され得る。次に、区切り文字データフィールド７０４が、アカウント識別子と有効期限データフィールド７０６との間に緩衝を提供する。サービスコードデータフィールド７０８が、有効期限データフィールド７０６に続いてもよい。個人識別番号検証指標（ＰＶＫＩ）データフィールド７１０およびＰＩＮ検証情報データフィールド７１２が後に続く。次に、ｄＣＶＶデータフィールド７１４、取引カウンタデータフィールド７１６、および非接触指標データフィールド７１８が含まれ得る。最後に、任意データフィールド７２０が後に続き得る。任意データフィールドは、暗号化値データフィールド７２１および暗号文バージョン番号データフィールド７２３を含み得る。暗号化値データフィールド７２１および暗号文バージョン番号データフィールド７２３は、必ずしも図７に示される数ではなく、任意の好適な桁数を含んでもよい。
【０１０７】
一部の実施形態によれば、ＰＡＮ７０１を最初に利用して、暗号化された値（例えば、暗号化された識別子）を生成してもよい。例として、図１のユーザデバイス１０２は、図３のＰＡＮ７０１およびＵＤＫ３０６を、記憶装置から読み出すように構成されてもよい。

一部の実施形態では、取引カウンタ（または他の動的値）もまた読み出されてもよい。ＰＡＮ７０１および取引カウンタ（または他の動的値）は、暗号化アルゴリズムへの入力として、ＵＤＫ３０６と共に利用されて、暗号化された値を生成し得る。一部の実施形態では、ＰＡＮ７０１および取引カウンタ（または他の動的値）は、入力の前に連結されてもよい。結果として得られた暗号化された値は、記録形式７００で保存され得る。例として、結果として得られた暗号化された値は、任意データフィールド７２０の暗号化値データフィールド７２１内に示されるように保存されてもよい。一部の実施形態では、任意データフィールド７２０は、トラック２標準によって定義される、特定のタグに対応する（例えば、タグ９Ｆ１Ｆ（任意データタグ）、タグ９Ｆ７Ｃ（顧客専用データタグ）、タグ９Ｆ１０（発行者アプリケーションデータ）、トラック２のデータの任意の好適な部分、または上記の任意の好適な組み合わせで）。

【０１０８】

一部の実施形態では、暗号文バージョン番号データフィールド７２３は、任意データフィールド７２０が、暗号化値データフィールド７２１内に暗号化された値を含むことを示す、番号を保存してもよい。

【０１０９】

一部の実施形態によれば、ユーザデバイス１０２は、難読化されたＰＡＮ７０３を生成するように構成されてもよい。例として、ユーザデバイス１０２は、ＰＡＮ７０１の最初の８桁を取得し、識別子データフィールド７０３の桁１～８にこの情報を保存してもよい。一部の実施形態では、識別子データフィールド７０３の桁９～１５は、ゼロなどのパディング値を含み得る。あるいは、ユーザデバイス１０２は、暗号化された値の何らかの部分を取得し、記録形式７００内にその部分を保存するように構成されてもよい。例えば、暗号化された値の最後の７桁を取得し、識別子データフィールド７０３の桁９～１５として保存してもよい。識別子データフィールド７０３の桁１６は、識別子データフィールド７０３が、変更されていないことを検証するために利用され得る（例えば、受信時に）、チェックサム値（例えば、Ｌｕｈｎチェックサム／値）を含み得る。

【０１１０】

取引が開始されると、難読化されたＰＡＮ７０３、および任意データフィールド７２０内の（例えば、暗号化値データフィールド７２１の）暗号化された値が、提供されてもよい（例えば、上記のようにアクセスデバイスに）。取引カウンタの値を増加（または減少）することができ、および／または新しい動的値を、取引カウンタデータフィールド７１６の中に生成し保存してもよい。別の取引がユーザデバイス１０２によって開始される場合、本明細書で論じるプロセスは、新しい取引カウンタ／動的値およびＰＡＮ７０１を利用して繰り返されて、その後、後続の取引で提供され得る、新しい暗号化された値および新しい難読化された識別子を生成してもよい。

【０１１１】

図８は、一部の実施形態による、データ検証を実施するための方法のフローチャートを示す。方法８００は、コンピューティングデバイス（例えば、図１の中央サーバコンピュータ１０８および／または承認事業体コンピュータ１１０）によって実施され得る。コンピューティングデバイスは、一つ以上のプロセッサと、コンピュータ実行可能命令を保存する一つ以上のメモリとを備えてもよく、一つ以上のプロセッサによりコンピュータ実行可能命令を実行することによって、コンピューティングデバイスに方法８００を実施させる。

【０１１２】

方法８００は、メッセージ（例えば、承認要求メッセージ）を受信し得る、ブロック８０２から始まってもよい。一部の実施形態では、メッセージは、第一の識別子（例えば、ＳＡＮ）および暗号化された識別子を含んでもよい。図８に示し以下に記載されるステップは、図１の取引処理の説明および対応する説明と併せて使用することができる。それらの説明は、参照により本明細書に組み込まれる。

【０１１３】

ブロック８０４で、コンピューティングデバイスは、承認要求メッセージを開始した、要求するデバイスと関連付けられたタイプを検証し得る。一部の実施形態では、コンピューティングデバイスは、承認要求メッセージに含まれる値（例えば、小売業者の名前、住所、タイプ指標、端末タイプなど）を、コンピューティングデバイスに保存されるか、またはコンピューティングデバイスがアクセス可能なデータ（例えば、ＳＡＮの利用が許される値）と比較してもよい。承認要求メッセージに含まれる値が、保存されたデータに含まれる場合、コンピューティングデバイスによって、承認要求メッセージをさらに処理することが可能になり得る。値が承認要求メッセージに含まれていない場合、コンピューティングデバイスは、承認要求メッセージを拒否し、それを示す承認応答メッセージを要求者に送信し得る。

【０１１４】

８０６で、第一の識別子（例えば、ＳＡＮ）を利用して、予想される識別子（例えば、プライマリＰＡＮ）を取得してもよい。一部の実施形態では、コンピューティングデバイスは、ＰＡＮとＳＡＮとの既知の関連を示すマッピングを調べてもよい。

【０１１５】

８０８で、コンピューティングデバイスは、暗号化された識別子および一意の導出鍵を利用して、復号された識別子を生成し得る。一部の実施形態では、コンピューティングデバイスが、第一の識別子（例えば、ＳＡＮ）の一部分から、一意の導出鍵（ＵＤＫ）を導き出してもよい。一部の実施形態では、ＵＤＫは、事前に導出され、記憶装置から読み出されてもよい。例として、コンピューティングデバイスは、第一の識別子の左端８桁を読み出し、それらの数字を所定の暗号化アルゴリズムへの入力として使用して、ＵＤＫを生成し得る。左端の８桁は、銀行識別番号（ＢＩＮ）に対応してもよい。ＵＤＫは、生成されると、暗号化された識別子を復号するために利用され得る。

【０１１６】

８１０で、コンピューティングデバイスは、復号された識別子が予想される識別子５１０と一致することを、検証するように構成され得る。すなわち、復号された識別子は、コンピューティングデバイスによって維持されるマッピング内に定義されるような、第一の識別子（例えば、ＳＡＮ）と関連付けられたプライマリＰＡＮに対応する。

【０１１７】

８１２で、メッセージは、復号された識別子を利用して、コンピューティングデバイスによって処理されてもよい。例として、コンピューティングデバイスは、中央サーバコンピュータ（例えば、図１の中央サーバコンピュータ１０８）であってもよい。このシナリオでは、メッセージ（例えば、承認要求メッセージ）を処理することは、復号された識別子を含むようにメッセージを修正することと、さらなる処理のために承認事業体コンピュータ（例えば、承認事業体コンピュータ１１０）にメッセージを送信することとを含み得る。一部の実施形態では、コンピューティングデバイスは、承認事業体コンピュータ１１０であってもよい。このシナリオでは、メッセージを処理することは、復号された識別子を含むメッセージデータによる、取引の承認を含み得る。処理は、取引が承認または拒否されたことを示す、承認応答メッセージの生成をさらに含んでもよい。承認応答メッセージは、暗号化された識別子を含み、例えば、図１に関係する上記のプロセスによって、中央サーバコンピュータ１０８に送信されてもよい。

【０１１８】

図９は、一部の実施形態による、データ検証を実施する別の方法のフローチャートを示す。方法９００は、コンピューティングデバイス（例えば、図１の中央サーバコンピュータ１０８および／または承認事業体コンピュータ１１０）によって実施され得る。コンピューティングデバイスは、一つ以上のプロセッサと、コンピュータ実行可能命令を保存する一つ以上のメモリとを備えてもよく、一つ以上のプロセッサによりコンピュータ実行可能命令を実行することによって、コンピューティングデバイスに方法９００を実施させる。

【０１１９】

方法９００は、メッセージ（例えば、承認要求メッセージ）を受信し得る、ブロック９０

２から始まってもよい。一部の実施形態では、メッセージは、難読化された識別子および暗号化された識別子を含んでもよい。図９に示し以下に記載されるステップは、図１の取引処理の説明および対応する説明と併せて使用することができる。それらの説明は、参照により本明細書に組み込まれる。

【０１２０】

ブロック９０４で、コンピューティングデバイスは、メッセージが識別された暗号化されたものを含むことを識別し得る。一部の実施形態では、メッセージが暗号化された識別子を含むことを識別することは、特定のデータフィールド（例えば、図３の任意データフィールド３２０）を、ゼロでない値について確認することを含み得る。データフィールドが、ゼロでない値を含む場合、コンピューティングデバイスによって、暗号化された値がメッセージの中に存在すると結論を出し得る。一部の実施形態では、メッセージが暗号化された識別子を含むことを識別することは、特定のデータフィールド（例えば、図３の暗号文バージョン番号データフィールド３２３）を、ゼロでない値（または特定の値）について確認することを含み得る。

【０１２１】

ブロック９０６で、コンピューティングデバイスは、暗号化された識別子および一意の導出鍵を利用して、復号された識別子を生成し得る。一部の実施形態では、コンピューティングデバイスが、難読化された識別子の一部分から、一意の導出鍵（ＵＤＫ）を導き出してもよい。一部の実施形態では、ＵＤＫは、事前に導出され、記憶装置から読み出されてもよい。例として、コンピューティングデバイスは、難読化された識別子の左端８桁を読み出し、それらの数字を所定の暗号化アルゴリズムへの入力として使用して、ＵＤＫを生成し得る。ＵＤＫは、生成されると、暗号化された識別子を復号するために利用され得る。

【０１２２】

ブロック９０８で、メッセージは、復号された識別子を利用して、コンピューティングデバイスによって処理されてもよい。例として、コンピューティングデバイスは、中央サーバコンピュータ（例えば、図１の中央サーバコンピュータ１０８）であってもよい。このシナリオでは、メッセージ（例えば、承認要求メッセージ）を処理することは、復号された識別子を含むようにメッセージを修正することと、さらなる処理のために承認事業体コンピュータ（例えば、承認事業体コンピュータ１１０）にメッセージを送信することとを含み得る。一部の実施形態では、コンピューティングデバイスは、承認事業体コンピュータ１１０であってもよい。このシナリオでは、メッセージを処理することは、復号された識別子を含むメッセージデータによる、取引の承認を含み得る。処理は、取引が承認または拒否されたことを示す、承認応答メッセージの生成をさらに含んでもよい。承認応答メッセージは、暗号化された識別子を含み、例えば、図１に関係する上記のプロセスによって、中央サーバコンピュータ１０８に送信されてもよい。

【０１２３】

技術面の改善

本明細書に記載される技術を利用することによって、機密データ（例えば、ＰＡＮ）を伝達するためのより安全な方法が可能になる。ＰＡＮは、暗号化され、非従来型のデータフィールドだけでなく、通常はＰＡＮを含むであろうが、代わりにＰＡＮが判定される可能性が低い難読化された値を含む、従来のデータフィールドにも提供される。難読化された値には、依然として元のＢＩＮが含まれ、承認要求／応答メッセージに対する従来のルーティング技術は、変わらないままであることが保証され得る。本明細書に記載される技術によって、承認要求／応答メッセージからＰＡＮを識別することが、不可能でないにしても困難になる。加えて、一部の実施形態では、ＰＡＮは、常に変化している動的値を使用して暗号化される。したがって、暗号化された値は、各承認要求に対して変更することができ、特定のユーザに対する取引を経時的に追跡することが、不可能でないにしても困難になる。その結果、これらの方法によって、特定のユーザおよび／またはアカウントが、承認要求／応答メッセージから識別できないことを保証することによって、個人データの

プライバシーに関して改善をもたらす。

【０１２４】

本明細書に記載されるコンピューティングデバイスのいずれもが、上記の事業体または構成要素のいずれかを実装するために使用され得る、コンピュータシステムの例であってもよい。こうしたコンピュータシステムのサブシステムは、システムバスを介して相互接続してもよい。追加のサブシステムには、プリンタ、キーボード、記憶デバイス、およびディスプレイアダプタに結合されるモニタが含まれる。入出力（Ｉ／Ｏ）コントローラに結合する、周辺デバイスおよびＩ／Ｏデバイスは、シリアルポートなどの当技術分野で既知の任意の数の手段によって、コンピュータシステムに接続することができる。例えば、Ｉ／Ｏポートまたは外部インターフェースを使用して、インターネットなどの広域ネットワーク、マウス入力デバイス、またはスキャナに、コンピュータ装置を接続できる。システムバスを介した相互接続により、中央プロセッサが、各サブシステムと通信し、サブシステム間の情報の交換だけでなく、システムメモリまたは記憶デバイスからの命令の実行を制御することが可能になり得る。システムメモリおよび／または記憶デバイスは、コンピュータ可読媒体を具現化してもよい。

【０１２５】

記載のように、本発明のサービスは、一つ以上の機能、プロセス、動作、または方法ステップを実装することを伴い得る。一部の実施形態では、機能、プロセス、動作、または方法ステップは、好適にプログラムされたコンピューティングデバイス、マイクロプロセッサ、データプロセッサなどによる一組の命令またはソフトウェアコードの実行の結果として実装されてもよい。命令またはソフトウェアコードのセットは、コンピューティングデバイス、マイクロプロセッサなどによってアクセスされるメモリ、または他の形態のデータ記憶要素に保存されてもよい。他の実施形態では、機能、プロセス、動作、または方法ステップは、ファームウェアまたは専用のプロセッサ、集積回路によって実装されてもよい。

【０１２６】

本出願に記載のソフトウェアコンポーネントまたは機能のいずれかは、例えば、従来の技術もしくはオブジェクト指向の技術を使った、例えば、Ｊａｖａ、Ｃ＋＋、またはＰｅｒｌなどの任意の好適なコンピュータ言語を使用する、プロセッサによって実行されるソフトウェアコードとして実施されてもよい。ソフトウェアコードは、ランダムアクセスメモリ（ＲＡＭ）、読み出し専用メモリ（ＲＯＭ）、ハードドライブもしくはフロッピーディスクなどの磁気媒体、またはＣＤ－ＲＯＭのような光媒体などの、コンピュータ可読媒体上の一連の命令またはコマンドとして保存されてもよい。そのようなコンピュータ可読媒体は、単一の計算装置上またはその内部にあってもよく、システムまたはネットワーク内の異なる計算装置上もしくはその内部に存在し得る。

【０１２７】

上の記載は例示であり、限定するものではない。本開示を検討すると、本発明の多くの変形が、当業者に対して明らかとなるであろう。そのため、本発明の範囲は、上の記載を参照して判定されるべきではなく、代わりに、係属中の特許請求の範囲を参照して、それらの全範囲または同等物と併せて判定されるべきである。

【０１２８】

いずれの実施形態の一つ以上の特徴は、本発明の範囲から逸脱することなく、いずれの他の実施形態の一つ以上の特徴と組み合わせてもよい。

【０１２９】

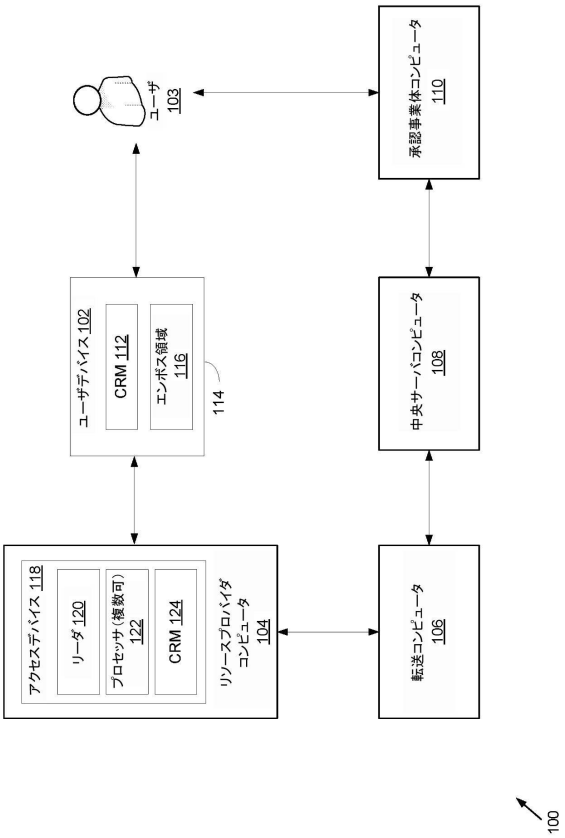
「一つの（ａ）」、「一つの（ａｎ）」、または「その（ｔｈｅ）」の列挙は、特に反対の指示がない限り、「一つ以上」を意味することを意図している。

【０１３０】

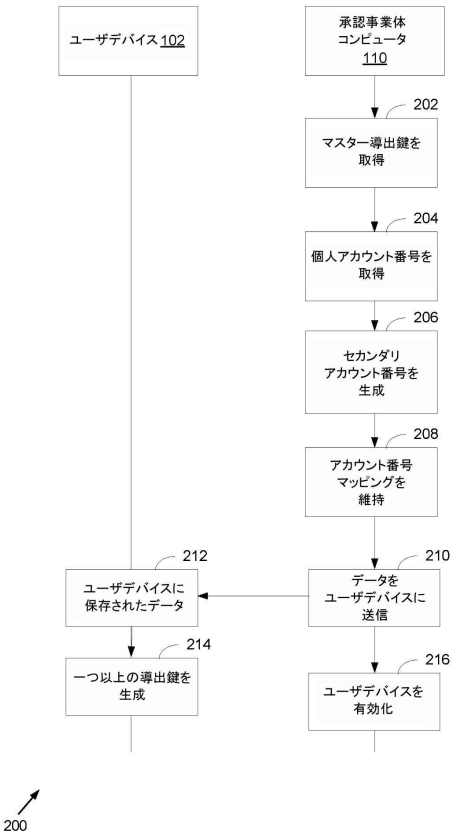
上で言及したすべての特許、特許出願、刊行物、および記載は、あらゆる目的のためにその全体が参照により本明細書に援用される。いずれも先行技術と認められない。

【図面】

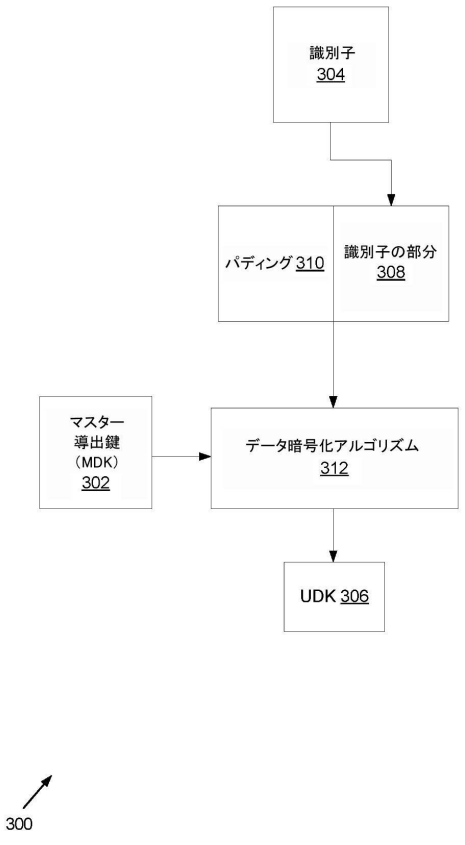
【図１】


ユーザ 103
承認事業体コンピュータ 110
ユーザデバイス 102
CRM 112
エンボス領域 116
114
中央サーバコンピュータ 108
アクセスデバイス 118
リーダ 120
プロセッサ（複数可） 122
CRM 124
リソースプロバイダコンピュータ 104
転送コンピュータ 106
100

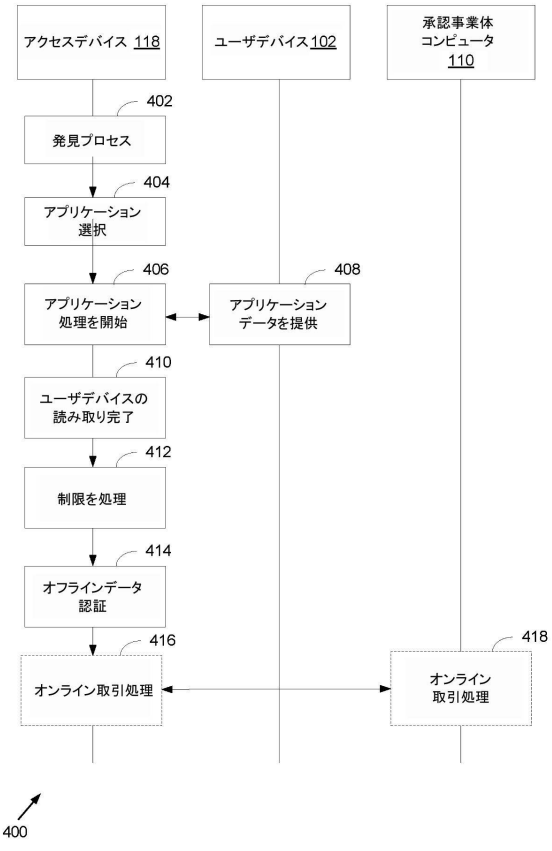
【図２】


ユーザデバイス 102
承認事業体コンピュータ 110
202
マスター導出鍵を取得
204
個人アカウント番号を取得
206
セカンダリアカウント番号を生成
208
アカウント番号マッピングを維持
210
データをユーザデバイスに送信
212
ユーザデバイスに保存されたデータ
214
一つ以上の導出鍵を生成
216
ユーザデバイスを有効化
200

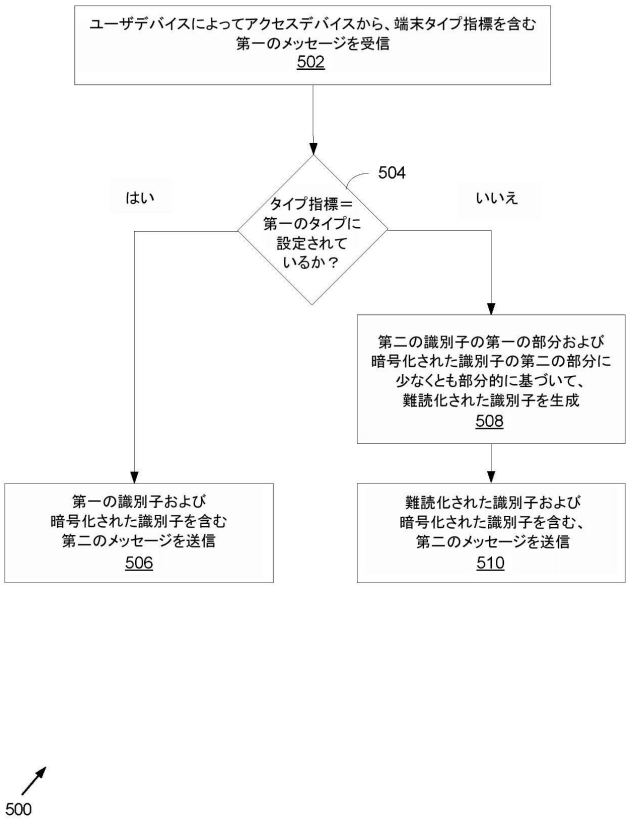
【図３】


識別子 304
パディング 310
識別子の部分 308
マスター導出鍵（MDK） 302
データ暗号化アルゴリズム 312
UDK 306
300

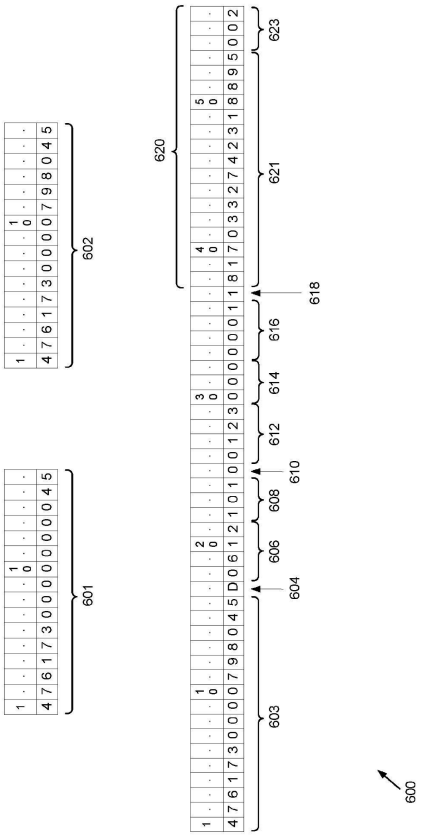
【図４】


アクセスデバイス 118
ユーザデバイス 102
承認事業体コンピュータ 110
402
発見プロセス
404
アプリケーション選択
406
アプリケーション処理を開始
408
アプリケーションデータを提供
410
ユーザデバイスの読み取り完了
412
制限を処理
414
オフラインデータ認証
416
オンライン取引処理
418
オンライン取引処理
400

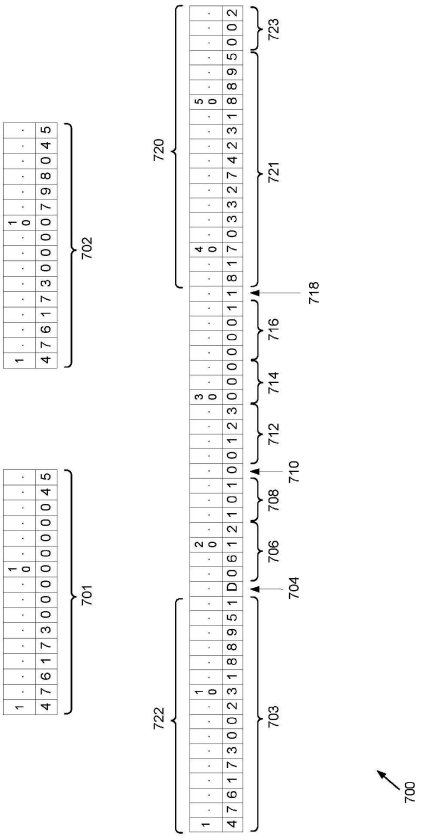
【図５】


ユーザデバイスによってアクセスデバイスから、端末タイプ指標を含む第一のメッセージを受信
502
504
タイプ指標＝第一のタイプに設定されているか？
はい
いいえ
第一の識別子および暗号化された識別子を含む第二のメッセージを送信
506
第二の識別子の第一の部分および暗号化された識別子の第二の部分に少なくとも部分的に基づいて、難読化された識別子を生成
508
難読化された識別子および暗号化された識別子を含む、第二のメッセージを送信
510
500

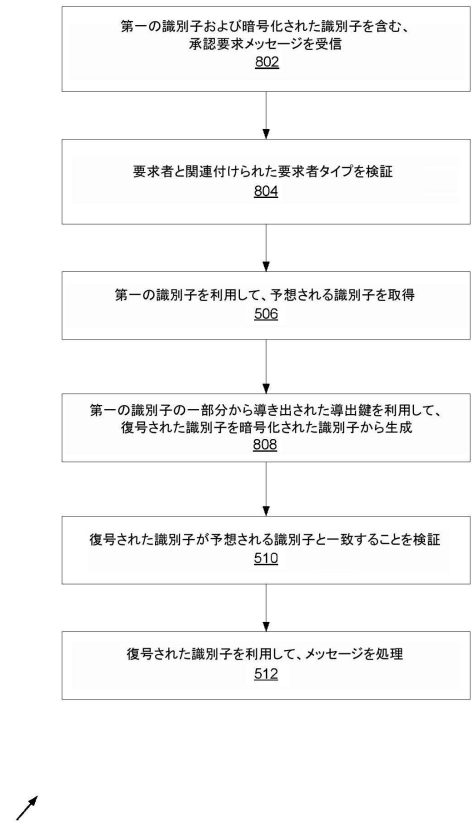
【図６】


602
601
620
621
623
618
616
614
612
610
608
606
604
603
600

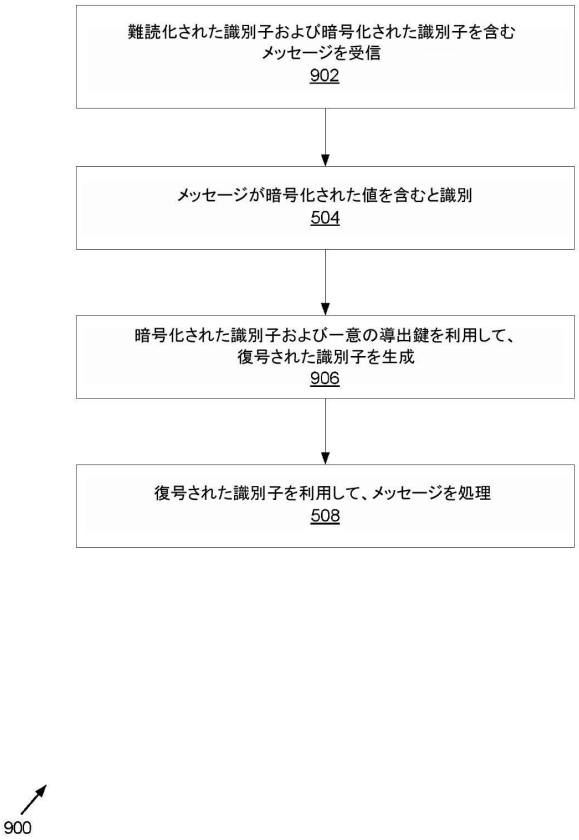
【図７】


702
701
720
721
723
718
716
714
712
710
708
706
704
703
722
700

【図８】


第一の識別子および暗号化された識別子を含む、承認要求メッセージを受信
802
要求者と関連付けられた要求者タイプを検証
804
第一の識別子を利用して、予想される識別子を取得
506
第一の識別子の一部分から導き出された導出鍵を利用して、復号された識別子を暗号化された識別子から生成
808
復号された識別子が予想される識別子と一致することを検証
510
復号された識別子を利用して、メッセージを処理
512
800

【図９】


難読化された識別子および暗号化された識別子を含む
メッセージを受信
902
メッセージが暗号化された値を含むと識別
504
暗号化された識別子および一意の導出鍵を利用して、
復号された識別子を生成
906
復号された識別子を利用して、メッセージを処理
508
900

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2018/055833

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i

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)
H04L 9/08; G06K 1/00; G06K 19/00; G06Q 20/20; G06Q 20/36; G06Q 20/38; G06Q 20/40

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & keywords: terminal, type indicator, encrypt, obfuscated identifier, counter

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2017-0228728 A1 (VISA EUROPE LIMITED) 10 August 2017 See paragraphs [0064], [0071]-[0075], [0086]-[0088], [0095], [0108], [0110]; and figures 2-4.	1-20
Y	US 2015-0220917 A1 (CHRISTIAN AABYE et al.) 06 August 2015 See paragraphs [0069], [0084], [0119]; and figures 4-9.	1-20
A	US 2015-0235211 A1 (SIMON HURRY et al.) 20 August 2015 See paragraphs [0035], [0064]; and figures 2-8.	1-20
A	US 2014-0019276 A1 (VISA EUROPE LIMITED) 16 January 2014 See paragraphs [0059]-[0092]; and figures 1-6.	1-20
A	US 2009-0184163 A1 (AYMAN HAMMAD et al.) 23 July 2009 See paragraphs [0034]-[0076]; and figures 1-5.	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
22 May 2019 (22.05.2019)	**01 July 2019 (01.07.2019)**

Name and mailing address of the ISA/KR	Authorized officer
International Application Division Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea	KIM, Seong Woo
Facsimile No. +82-42-481-8578	Telephone No. +82-42-481-3348

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2018/055833

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2017-0228728 A1	10/08/2017	AU 2015-334634 A1	27/04/2017
		CA 2965445 A1	28/04/2016
		CN 107077670 A	18/08/2017
		EP 3210177 A1	30/08/2017
		KR 10-2017-0077170 A	05/07/2017
		MX 2017005313 A	21/06/2017
		WO 2016-063089 A1	28/04/2016
US 2015-0220917 A1	06/08/2015	AU 2015-214271 A1	21/07/2016
		CA 2936985 A1	13/08/2015
		CN 105960776 A	21/09/2016
		EP 3103084 A1	14/12/2016
		WO 2015-120082 A1	13/08/2015
US 2015-0235211 A1	20/08/2015	AU 2004-267784 A1	03/03/2005
		BR PI0813326 A2	23/12/2014
		CA 2655465 C	07/03/2017
		CN 107067246 A	18/08/2017
		EP 1656600 B1	28/06/2017
		JP 2016-170801 A	23/09/2016
		KR 10-1762389 B1	04/08/2017
		US 9940621 B2	10/04/2018
		WO 2009-003080 A1	31/12/2008
US 2014-0019276 A1	16/01/2014	CN 102754113 A	24/10/2012
		EP 2513848 B1	02/08/2017
		GB 2476233 B	23/05/2018
		US 2013-0066776 A1	14/03/2013
		WO 2011-073216 A1	23/06/2011
US 2009-0184163 A1	23/07/2009	AU 2007-300163 B2	17/10/2013
		BR PI0821707 A2	16/06/2015
		CA 2664593 A1	03/04/2008
		EP 2076889 B1	04/07/2018
		JP 5657895 B2	21/01/2015
		KR 10-1531476 B1	25/06/2015
		US 10210508 B2	19/02/2019
		WO 2009-085415 A1	09/07/2009
		ZA 201004606 B	28/09/2011

フロントページの続き

G,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,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．ＪＡＶＡ
トリート １０１２