(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7467432号
(P7467432)

(45)発行日　令和6年4月15日(2024.4.15)

(24)登録日　令和6年4月5日(2024.4.5)

(51)国際特許分類			FI		
H04L	*9/32*	*(2006.01)*	H04L	9/32	200D
H04L	*9/14*	*(2006.01)*	H04L	9/32	100E
G06F	*21/32*	*(2013.01)*	H04L	9/32	100D
G06F	*21/35*	*(2013.01)*	H04L	9/14	
G06Q	*20/34*	*(2012.01)*	G06F	21/32	

請求項の数　20　（全46頁）　最終頁に続く

(21)出願番号　特願2021-518080(P2021-518080)
(86)(22)出願日　令和1年10月1日(2019.10.1)
(65)公表番号　特表2022-504072(P2022-504072A)
(43)公表日　令和4年1月13日(2022.1.13)
(86)国際出願番号　PCT/US2019/053963
(87)国際公開番号　WO2020/072424
(87)国際公開日　令和2年4月9日(2020.4.9)
審査請求日　令和4年9月20日(2022.9.20)
(31)優先権主張番号　62/740,352
(32)優先日　平成30年10月2日(2018.10.2)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　16/351,365
(32)優先日　平成31年3月12日(2019.3.12)
最終頁に続く

(73)特許権者　519111877
キャピタル・ワン・サービシーズ・リミテッド・ライアビリティ・カンパニー
Ｃａｐｉｔａｌ Ｏｎｅ Ｓｅｒｖｉｃｅｓ，ＬＬＣ
アメリカ合衆国２２１０２バージニア州マクリーン、キャピタル・ワン・ドライブ１６８０番
(74)代理人　100145403
弁理士　山尾 憲人
(74)代理人　100132241
弁理士　岡部 博史
(74)代理人　100135703
弁理士　岡部 英隆
(72)発明者　ケビン・オズボーン
最終頁に続く

(54)【発明の名称】　非接触カードの暗号化認証のためのシステムおよび方法

(57)【特許請求の範囲】

【請求項１】

システムであって、前記システムは、

サーバを、備え、

前記サーバは、

アカウントと業者との間のトランザクションを識別し、

前記トランザクションと前記アカウントの過去のトランザクションパターンとの比較に基づいて、前記トランザクションを高リスクとして識別し、

中間デバイスに認証要求を送信し、

前記中間デバイスからの前記認証要求に応答して、非接触カードによって送信された暗号文を受信し、

暗号化アルゴリズムを使用してセッション鍵に基づいて前記暗号文を検証し、

前記検証された暗号文に基づいて前記トランザクションを承認するように構成される、システム。

【請求項２】

前記サーバは、マスター鍵および一意の識別子に基づいて認証多様化鍵を生成し、

前記認証多様化鍵に基づいて前記セッション鍵を生成するようにさらに構成される、

請求項１に記載のシステム。

【請求項３】

前記トランザクションは、前記過去のトランザクションパターンと矛盾する時期に実行

される、請求項１に記載のシステム。
【請求項４】
前記トランザクションは、前記過去のトランザクションパターンと矛盾する地理的地域で実施される、請求項１に記載のシステム。
【請求項５】
前記トランザクションを高リスクとして識別することはさらに、前記業者と不正なトランザクションとの関連付けに基づいている、請求項１に記載のシステム。
【請求項６】
前記トランザクションを高リスクとして識別することはさらに、前記業者の場所に基づいており、
前記業者の前記場所は、不正なトランザクションに関連付けられた地理的地域にある、
請求項１に記載のシステム。
【請求項７】
前記サーバは、生体認証情報およびパスワードのグループから選択された少なくとも１つに関する第２の認証要求を前記中間デバイスに送信するようにさらに構成され、
前記サーバは、前記認証要求を保留しているトランザクションを遅らせるようにさらに構成される、請求項１に記載のシステム。
【請求項８】
前記認証要求を送信する前に、前記トランザクションの値を閾値と比較し、
前記トランザクションの前記値が前記閾値を超えた場合に、前記認証要求を送信するようにさらに構成される、請求項１に記載のシステム。
【請求項９】
プロセッサが、アカウントと業者との間のトランザクションを識別することと、
前記プロセッサが、前記トランザクションと前記アカウントの過去のトランザクションパターンとの比較に基づいて、前記トランザクションを高リスクとして識別することと、
前記プロセッサが、中間デバイスに認証要求を送信することと、
前記プロセッサが、前記中間デバイスからの前記認証要求に応答して、非接触カードによって送信された暗号文を受信することと、
前記プロセッサが、暗号化アルゴリズムを使用してセッション鍵に基づいて前記暗号文を検証することと、
前記プロセッサが、前記検証された暗号文に基づいて前記トランザクションを承認することと、
を含む方法。
【請求項１０】
前記方法は、
前記プロセッサが、マスター鍵および一意の識別子に基づいて認証多様化鍵を生成することと、
前記プロセッサが、前記認証多様化鍵に基づいて前記セッション鍵を生成することと、
をさらに含む、請求項９に記載の方法。
【請求項１１】
前記方法は、
前記プロセッサが、生体認証情報およびパスワードのグループから選択された少なくとも１つに関する第２の認証要求を前記中間デバイスに送信することをさらに含む、請求項９に記載の方法。
【請求項１２】
前記方法は、
前記プロセッサが、前記認証要求を保留しているトランザクションを遅らせることをさらに含む、請求項９に記載の方法。
【請求項１３】
前記トランザクションを決定することは、前記過去のトランザクションパターンと矛盾す

る時期に実行されること、
を含む、請求項９に記載の方法。
【請求項１４】
前記トランザクションを決定することは、前記過去のトランザクションパターンと矛盾する地理的地域で実行されること、
を含む、請求項９に記載の方法。
【請求項１５】
サーバであって、前記サーバは、
プロセッサを、備え、
前記プロセッサは、
アカウントと業者との間のトランザクションを識別し、
前記トランザクションと前記アカウントの過去のトランザクションパターンとの比較に基づいて、前記トランザクションを高リスクとして識別し、
中間デバイスに認証要求を送信し、
前記中間デバイスからの前記認証要求に応答して、非接触カードによって送信された暗号文を受信し、
暗号化アルゴリズムを使用してセッション鍵に基づいて前記暗号文を検証し、
前記検証された暗号文に基づいて前記トランザクションを承認するように構成される、
サーバ。
【請求項１６】
前記プロセッサは、
マスター鍵および一意の識別子に基づいて認証多様化鍵を生成し、
前記認証多様化鍵に基づいて前記セッション鍵を生成するようにさらに構成される、
請求項１５に記載のサーバ。
【請求項１７】
前記トランザクションを高リスクとして識別することはさらに、前記業者と不正なトランザクションとの関連付けに基づいている、請求項１５に記載のサーバ。
【請求項１８】
前記トランザクションを高リスクとして識別することはさらに、前記業者の場所に基づいており、
前記業者の前記場所は、不正なトランザクションに関連付けられた地理的地域にある、
請求項１５に記載のサーバ。
【請求項１９】
前記トランザクションは複数のトランザクションを含み、
前記複数のトランザクションは、過去のトランザクションパターンと一致しない頻度で行われる、
請求項１記載のシステム。
【請求項２０】
前記トランザクションが複数のトランザクションを含み、
前記複数のトランザクションは、他の多数のトランザクションから所定の時間内に行われる、
請求項１記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
関連する出願への相互参照
この出願は、２０１９年３月１２日に出願された米国特許出願第１６／３５１，３６５号の優先権を主張する。これは、２０１８年１１月２９日に出願された米国特許出願第１６／２０５，１１９号の一部継続であり、優先権を主張し、２０１８年１０月２日に出願された米国仮特許出願第６２／７４０，３５２号から優先権を主張し、その開示は、参照

によりその全体が本明細書に援用される。

【０００２】

本開示は、暗号化、より具体的には、非接触カードの暗号化認証のためのシステムおよび方法に関する。

【背景技術】

【０００３】

データのセキュリティとトランザクションの整合性は、企業と消費者にとって非常に重要である。電子取引が商業活動のますます大きなシェアを構成するにつれて、この必要性は増大し続けている。

【０００４】

電子メールは、トランザクションを検証するためのツールとして使用できるが、電子メールは攻撃を受けやすく、ハッキングやその他の不正アクセスに対して脆弱である。ショートメッセージサービス（ＳＭＳ）メッセージも使用できるが、それも危殆化され得る。さらに、トリプルＤＥＳアルゴリズムなどのデータ暗号化アルゴリズムにも同様の脆弱性がある。

【０００５】

金融カード（例えば、クレジットカードやその他の支払いカード）を含む多くのカードをアクティブ化するには、カード所有者が電話番号に電話をかけたり、Ｗｅｂサイトにアクセスしたり、カード情報を入力したり提供したりするという時間のかかるプロセスが必要である。さらに、チップベースの金融カードの使用が増えると、対面購入のための以前の技術（例えば、磁気ストリップカード）よりも安全な機能が提供されるが、アカウントへのアクセスは、カード所有者の身元を確認するためにログイン資格情報（例えば、ユーザー名やパスワード）に依存し得る。しかしながら、ログイン資格情報が危殆化された場合、別の人がユーザのアカウントにアクセスし得る。

【０００６】

これらおよびその他の欠陥が存在する。したがって、非接触カードのデータセキュリティ、認証、および検証を提供するために、これらの欠陥を克服する適切な解決策をユーザに提供する必要がある。さらに、カードをアクティブ化するための改善された方法と、アカウントアクセスのための改善された認証の両方が必要である。

【発明の概要】

【０００７】

開示された技術の態様には、非接触カードの暗号認証のためのシステムおよび方法が含まれる。様々な実施形態は、非接触カードの暗号認証を実施および管理するためのシステムおよび方法を説明する。

【０００８】

本開示の実施形態は、認証システムであって、認証サーバと、認証サーバとのデータ通信においてクライアントデバイス上で実行するための命令を備えるクライアントアプリケーションと、プロセッサおよびメモリを含む非接触カードと、を備え、認証サーバは、トランザクション要求を受信し、トランザクション要求は、トランザクションの実行を要求するアカウントのアカウント情報およびトランザクションのトランザクション情報を含み、トランザクション要求の受信に応答して、トランザクションの値が所定の値を超える場合、少なくとも１つの認証要素を要求する認証要求をクライアントアプリケーションに送信し、少なくとも１つの認証要素は、非接触カードをクライアントデバイスの通信範囲に配置することによって生成された暗号文を含み、クライアントデバイスから認証信号を受信し、認証信号は、暗号文を含み、認証信号を受信したときにトランザクションを承認する、ように構成される、認証システムを提供する。

【０００９】

本開示の実施形態は、認証システムであって、ネットワークとのデータ通信における認証サーバと、ネットワークとのデータ通信においてクライアントデバイス上で実行するための命令を備えるクライアントアプリケーションと、プロセッサおよびメモリを含む非接

触カードであって、非接触カードは、アカウント情報を有するアカウントに関連付けられている、非接触カードと、を備え、認証サーバは、トランザクション要求を受信し、トランザクション要求は、非接触カードに関連付けられたアカウントのアカウント情報およびトランザクションのトランザクション情報を含み、トランザクション要求の受信に応答して、トランザクションの値が所定の値を超えたときに、少なくとも１つの認証要素を要求する認証要求をクライアントアプリケーションに送信し、少なくとも１つの認証要素を含む認証信号をクライアントアプリケーションから受信し、認証信号がクライアントアプリケーションから受信されたときに、トランザクションを承認する、ように構成される、認証システムを提供する。

【００１０】

本開示の実施形態は、トランザクションを認証する方法であって、認証サーバが、トランザクション検証要求を受信するステップであって、トランザクション検証要求は、トランザクションの実行を要求するアカウントのアカウント情報およびトランザクションのトランザクション情報を含む、ステップと、トランザクション要求の受信に応答して、認証サーバが、トランザクションの値が所定の値を超えたときにクライアントデバイス上で実行するための命令を備えるクライアントアプリケーションに認証要求を送信するステップであって、認証要求は、少なくとも１つの認証要素を要求し、少なくとも１つの認証要素は、クライアントデバイスの通信範囲に非接触カードを配置することによって生成される暗号文を含む、ステップと、クライアントアプリケーションが、センサおよび通信インターフェースの少なくとも１つを介して少なくとも１つの認証要素を検出するステップと、クライアントアプリケーションが、認証要素を含む認証信号を認証サーバに送信するステップと、クライアントアプリケーションからの認証信号の受信に応答して、認証サーバが、少なくとも１つの認証要素を検証するステップと、認証サーバが、認証要素の検証に応答してトランザクションを承認するステップと、を含むトランザクションを認証する方法を提供する。

【００１１】

開示された設計のさらなる特徴、およびそれによって提供される利点は、添付の図面に示される特定の例示的な実施形態を参照して、以下により詳細に説明される。

【図面の簡単な説明】

【００１２】

【図１Ａ】例示的な実施形態に係るデータ伝送システムの図である。

【図１Ｂ】例示的な実施形態に係る認証されたアクセスを提供するためのシーケンスを示す図である。

【図２】例示的な実施形態に係るデータ伝送システムの図である。

【図３】例示的な実施形態に係る非接触カードを使用するシステムの図である。

【図４】例示的な実施形態に係る鍵多様化の方法を示すフローチャートである。

【図５Ａ】例示的な実施形態に係る非接触カードの図である。

【図５Ｂ】例示的な実施形態に係る非接触カードの接触パッドの図である。

【図６】例示的な実施形態に係るデバイスと通信するためのメッセージを示す図である。

【図７】例示的な実施形態に係るメッセージおよびメッセージフォーマットを示す図である。

【図８】例示的な実施形態に係る鍵動作を示すフローチャートである。

【図９】例示的な実施形態に係る鍵システムの図である。

【図１０】例示的な実施形態に係る暗号を生成する方法のフローチャートである。

【図１１】例示的な実施形態に係る鍵多様化のプロセスを示すフローチャートである。

【図１２】例示的な実施形態に係るカードアクティブ化のための方法を示すフローチャートである。

【図１３】例示的な実施形態に係る認証システムの図である。

【図１４】例示的な実施形態に係るトランザクションを認証する方法を示すフローチャートである。

【発明を実施するための形態】
【００１３】
以下の実施形態の説明は、本発明の異なる態様の特徴および教示を特に説明するために数字を参照する非限定的な代表的な例を提供する。記載された実施形態は、実施形態の説明から他の実施形態と別個に、または組み合わせて実施できると認識されるべきである。実施形態の説明を検討する当業者は、本発明の異なる説明された態様を学習および理解できなければならない。実施形態の説明は、具体的にはカバーされていないが、実施形態の説明を読んだ当業者の知識の範囲内である他の実施形態が、本発明の出願と一致すると理解される程度まで、本発明の理解を容易にするはずである。
【００１４】
本開示のいくつかの実施形態の目的は、１つまたは複数の鍵を１つまたは複数の非接触カードに組み込むことである。これらの実施形態では、非接触カードは、認証および他の方法では非接触カードに加えて別個の物理的トークンを担持することをユーザに要求し得る他の多くの機能を実行できる。非接触インターフェースを採用することにより、非接触カードは、ユーザのデバイス（携帯電話など）とカード自体との間で相互作用および通信するための方法を提供され得る。例えば、多くのクレジットカードトランザクションの基礎となるＥＭＶプロトコルには、Ａｎｄｒｏｉｄ（登録商標）のオペレーティングシステムには十分な認証プロセスが含まれているが、読み取り専用でしか使用できないため、近距離無線通信（ＮＦＣ）の使用に関してより制限されているｉＯＳ（登録商標）には課題がある。本明細書に記載の非接触カードの例示的な実施形態は、ＮＦＣ技術を利用する。
【００１５】
図１Ａは、例示的な実施形態に係るデータ伝送システムを示している。以下でさらに説明するように、システム１００は、非接触カード１０５、クライアントデバイス１１０、ネットワーク１１５、およびサーバ１２０を含み得る。図１Ａは、コンポーネントの単一のインスタンスを示しているが、システム１００は、任意の数のコンポーネントを含み得る。
【００１６】
システム１００は、１つまたは複数の非接触カード１０５を含み得、これらは、図５Ａから図５Ｂを参照して以下でさらに説明される。いくつかの実施形態では、非接触カード１０５は、一例ではＮＦＣを利用して、クライアントデバイス１１０と無線通信できる。
【００１７】
システム１００は、ネットワーク対応コンピュータであり得るクライアントデバイス１１０を含み得る。本明細書で言及されるように、ネットワーク対応コンピュータは、コンピュータデバイス、または、例えば、サーバ、ネットワークアプライアンス、パーソナルコンピュータ、ワークステーション、電話、ハンドヘルドＰＣ、パーソナルデジタルアシスタント、シンクライアント、ファットクライアント、インターネットブラウザ、またはその他のデバイスを含む通信デバイスを含み得るが、これらに限定されない。クライアントデバイス１１０はまた、モバイルデバイスであり得る。例えば、モバイルデバイスには、Ａｐｐｌｅ（登録商標）のｉＰｈｏｎｅ（登録商標）、ｉＰｏｄ（登録商標）、ｉＰａｄ（登録商標）、またはＡｐｐｌｅのｉＯＳ（登録商標）オペレーティングシステムを実行するその他のモバイルデバイス、ＭｉｃｒｏｓｏｆｔのＷｉｎｄｏｗｓ（登録商標）Ｍｏｂｉｌｅオペレーティングシステムを実行するデバイス、ＧｏｏｇｌｅのＡｎｄｒｏｉｄ（登録商標）オペレーティングシステムを実行するデバイス、および／または他のスマートフォン、タブレット、または同様のウェアラブルモバイルデバイスが含まれ得る。
【００１８】
クライアントデバイス１１０デバイスは、プロセッサおよびメモリを含むことができ、処理回路は、本明細書に記載されている機能を実行するために必要に応じて、プロセッサ、メモリ、エラーおよびパリティ／ＣＲＣチェッカー、データエンコーダ、衝突防止アルゴリズム、コントローラ、コマンドデコーダ、セキュリティプリミティブおよび改ざん防止ハードウェアを含む追加のコンポーネントを含み得ることが理解される。クライアント

デバイス１１０は、ディスプレイおよび入力デバイスをさらに含み得る。ディスプレイは、コンピュータモニター、フラットパネルディスプレイ、および液晶ディスプレイ、発光ダイオードディスプレイ、プラズマパネル、およびブラウン管ディスプレイを含むモバイルデバイス画面などの視覚情報を提示するための任意のタイプのデバイスであり得る。入力デバイスは、タッチスクリーン、キーボード、マウス、カーソル制御デバイス、タッチスクリーン、マイク、デジタルカメラ、ビデオレコーダまたはカムコーダなど、ユーザのデバイスによって利用可能でサポートされている情報をユーザのデバイスに入力するための任意のデバイスを含み得る。これらのデバイスは、情報を入力し、本明細書に記載のソフトウェアおよび他のデバイスと相互作用するために使用できる。

【００１９】

いくつかの例では、システム１００のクライアントデバイス１１０は、例えば、システム１００の１つまたは複数のコンポーネントとのネットワーク通信を可能にし、データを送信および／または受信する、ソフトウェアアプリケーションなどの１つまたは複数のアプリケーションを実行できる。

【００２０】

クライアントデバイス１１０は、１つまたは複数のネットワーク１１５を介して１つまたは複数のサーバ１２０と通信でき、サーバ１２０とのそれぞれのフロントエンドからバックエンドへのペアとして動作できる。クライアントデバイス１１０は、例えば、クライアントデバイス１１０上で実行されるモバイルデバイスアプリケーションから、１つまたは複数の要求をサーバ１２０に送信できる。１つまたは複数の要求は、サーバ１２０からのデータの検索に関連付けられ得る。サーバ１２０は、クライアントデバイス１１０から１つまたは複数の要求を受信できる。クライアントデバイス１１０からの１つまたは複数の要求に基づいて、サーバ１２０は、１つまたは複数のデータベース（図示せず）から要求されたデータを検索するように構成され得る。１つまたは複数のデータベースからの要求されたデータの受信に基づいて、サーバ１２０は、受信されたデータをクライアントデバイス１１０に送信するように構成され得、受信されたデータは、１つまたは複数の要求に応答する。

【００２１】

システム１００は、１つまたは複数のネットワーク１１５を含み得る。いくつかの例では、ネットワーク１１５は、無線ネットワーク、有線ネットワーク、または無線ネットワークと有線ネットワークの任意の組み合わせのうちの１つまたは複数であり得、クライアントデバイス１１０をサーバ１２０に接続するように構成され得る。例えば、ネットワーク１１５は、光ファイバネットワーク、パッシブ光ネットワーク、ケーブルネットワーク、インターネットネットワーク、衛星ネットワーク、ワイヤレスローカルエリアネットワーク（ＬＡＮ）、移動体通信のためのグローバルシステム、パーソナルコミュニケーションサービス、パーソナルエリアネットワーク、ワイヤレスアプリケーションプロトコル、マルチメディアメッセージングサービス、拡張メッセージングサービス、ショートメッセージサービス、時間分割マルチプレックスベースのシステム、コード分割マルチアクセスベースのシステム、Ｄ－ＡＭＰＳ、Ｗｉ－Ｆｉ、固定ワイヤレスデータ、ＩＥＥＥ　８０２．１１ｂ、８０２．１５．１、８０２．１１ｎおよび８０２．１１ｇ、ブルートゥース（登録商標）、ＮＦＣ、無線周波数識別（ＲＦＩＤ）、Ｗｉ－Ｆｉなどのうちの１つまたは複数を含み得る。

【００２２】

さらに、ネットワーク１１５は、電話回線、光ファイバ、ＩＥＥＥイーサネット９０２．３、ワイドエリアネットワーク、ワイヤレスパーソナルエリアネットワーク、ＬＡＮ、またはインターネットなどのグローバルネットワークを含むがこれらに限定されない。さらに、ネットワーク１１５は、インターネットネットワーク、無線通信ネットワーク、セルラネットワークなど、またはそれらの任意の組み合わせをサポートできる。ネットワーク１１５は、スタンドアロンネットワークとして、または互いに協力して動作する、１つのネットワーク、または上記の任意の数の例示的なタイプのネットワークをさらに含み得

る。ネットワーク１１５は、それらが通信可能に結合されている１つまたは複数のネットワーク要素の１つまたは複数のプロトコルを利用できる。ネットワーク１１５は、他のプロトコルとの間でネットワークデバイスの１つまたは複数のプロトコルに変換できる。ネットワーク１１５は、単一のネットワークとして示されているが、１つまたは複数の例によれば、ネットワーク１１５は、例えば、インターネット、サービスプロバイダのネットワーク、ケーブルテレビネットワーク、クレジットカードアソシエーションネットワークなどの企業ネットワーク、およびホームネットワークなどの複数の相互接続されたネットワークを含み得ることを理解されたい。

【００２３】

システム１００は、１つまたは複数のサーバ１２０を含み得る。いくつかの例では、サーバ１２０は、メモリに結合された１つまたは複数のプロセッサを含み得る。サーバ１２０は、複数のワークフローアクションを実行するために異なる時間に様々なデータを制御および呼び出すための中央システム、サーバまたはプラットフォームとして構成され得る。サーバ１２０は、１つまたは複数のデータベースに接続するように構成できる。サーバ１２０は、少なくとも１つのクライアントデバイス１１０に接続され得る。

【００２４】

図１Ｂは、本開示の１つまたは複数の実施形態に係る認証されたアクセスを提供するための例示的なシーケンスを示すタイミング図である。システム１００は、非接触カード１０５およびクライアントデバイス１１０を備え得、これは、アプリケーション１２２およびプロセッサ１２４を含み得る。図１Ｂは、図１Ａに示されているのと同様のコンポーネントを参照できる。

【００２５】

ステップ１０２で、アプリケーション１２２は、非接触カード１０５と通信する（例えば、非接触カード１０５に近づけられた後）。アプリケーション１２２と非接触カード１０５との間の通信は、アプリケーション１２２と非接触カード１０５との間のＮＦＣデータ転送を可能にするために、クライアントデバイス１１０のカードリーダ（図示せず）に十分に近い非接触カード１０５を含み得る。

【００２６】

ステップ１０４で、クライアントデバイス１１０と非接触カード１０５との間で通信が確立された後、非接触カード１０５は、メッセージ認証コード（ＭＡＣ）暗号文を生成する。いくつかの例では、これは、非接触カード１０５がアプリケーション１２２によって読み取られるときに発生し得る。特に、これは、ＮＦＣデータ交換フォーマットに従って作成され得る近距離無線データ交換（ＮＤＥＦ）タグのＮＦＣ読み取りなどの読み取り時に発生し得る。例えば、アプリケーション１２２などのリーダは、ＮＤＥＦ生成アプレットのアプレットＩＤを用いて、アプレット選択メッセージなどのメッセージを送信できる。選択が確認されると、一連の選択ファイルメッセージとそれに続く読み取りファイルメッセージが送信され得る。例えば、シーケンスには、「機能ファイルの選択」、「機能ファイルの読み取り」、および「ＮＤＥＦファイルの選択」が含まれ得る。この時点で、非接触カード１０５によって維持されるカウンタ値は、更新またはインクリメントされ得、その後に「ＮＤＥＦファイルの読み取り」が続き得る。この時点で、ヘッダと共有秘密を含むメッセージが生成され得る。次に、セッション鍵を生成できる。ＭＡＣ暗号文は、メッセージから作成できる。メッセージには、ヘッダと共有秘密が含まれ得る。次に、ＭＡＣ暗号文をランダムデータの１つまたは複数のブロックと連結し、ＭＡＣ暗号文と乱数（ＲＮＤ）をセッション鍵で暗号化できる。その後、暗号文とヘッダを連結し、ＡＳＣＩＩ１６進数としてエンコードして、ＮＤＥＦメッセージ形式で返すことができる（「ＮＤＥＦファイルの読み取り」メッセージに応答）。

【００２７】

いくつかの例では、ＭＡＣ暗号文はＮＤＥＦタグとして送信され得、他の例では、ＭＡＣ暗号文はユニフォームリソースインジケータとともに（例えば、フォーマットされた文字列として）含まれ得る。

【００２８】
いくつかの例では、アプリケーション１２２は、非接触カード１０５に要求を送信するように構成され得、要求は、ＭＡＣ暗号文を生成するための命令を備える。
【００２９】
ステップ１０６で、非接触カード１０５は、ＭＡＣ暗号文をアプリケーション１２２に送信する。いくつかの例では、ＭＡＣ暗号文の送信は、ＮＦＣを介して行われるが、本開示はそれに限定されない。他の例では、この通信は、ブルートゥース（登録商標）、Ｗｉ－Ｆｉ、または他の無線データ通信手段を介して行われ得る。
【００３０】
ステップ１０８で、アプリケーション１２２は、ＭＡＣ暗号文をプロセッサ１２４に通信する。
【００３１】
ステップ１１２で、プロセッサ１２４は、アプリケーション１２２からの命令に従って、ＭＡＣ暗号文を検証する。例えば、以下で説明するように、ＭＡＣ暗号文を検証できる。
【００３２】
いくつかの例では、ＭＡＣ暗号文の検証は、クライアントデバイス１１０とデータ通信しているサーバ１２０など、クライアントデバイス１１０以外のデバイスによって実行され得る（図１Ａに示されているように）。例えば、プロセッサ１２４は、ＭＡＣ暗号文を検証できるサーバ１２０に送信するために、ＭＡＣ暗号文を出力できる。
【００３３】
いくつかの例では、ＭＡＣ暗号文は、検証の目的でデジタル署名として機能し得る。この検証を実行するために、公開鍵非対称アルゴリズム、例えば、デジタル署名アルゴリズムとＲＳＡアルゴリズム、またはゼロ知識プロトコルなどの他のデジタル署名アルゴリズムを使用できる。
【００３４】
図２は、例示的な実施形態に係るデータ伝送システムを示している。システム２００は、１つまたは複数のサーバ２２０と、例えば、ネットワーク２１５を介して通信している送信または送信デバイス２０５、受信または受信デバイス２１０を含み得る。送信または送信デバイス２０５は、図１Ａを参照して上で論じたクライアントデバイス１１０と同じまたは同様であり得る。受信または受信デバイス２１０は、図１Ａを参照して上で論じたクライアントデバイス１１０と同じまたは同様であり得る。ネットワーク２１５は、図１Ａを参照して上で論じたネットワーク１１５と同様であり得る。サーバ２２０は、図１Ａを参照して上で論じたサーバ１２０と同様であり得る。図２は、システム２００のコンポーネントの単一のインスタンスを示しているが、システム２００は、図示されたコンポーネントをいくつでも含み得る。
【００３５】
暗号化アルゴリズム、ハッシュベースのメッセージ認証コード（ＨＭＡＣ）アルゴリズム、暗号ベースのメッセージ認証コード（ＣＭＡＣ）アルゴリズムなどの対称暗号化アルゴリズムを使用する場合、対称アルゴリズムと鍵を使用して保護されたデータを最初に処理する当事者と、同じ暗号化アルゴリズムと同じ鍵を使用してデータを受信して処理する当事者との間で、鍵を秘密にしておくことが重要である。
【００３６】
同じ鍵を何度も使用しないことも重要である。鍵が頻繁に使用または再利用されると、その鍵が危殆化され得る。鍵が使用されるたびに、同じ鍵を使用して暗号化アルゴリズムによって処理されたデータの追加サンプルが攻撃者に提供される。攻撃者が持っている同じ鍵で処理されたデータが多いほど、攻撃者が鍵の値を発見する可能性が高くなる。頻繁に使用される鍵は、様々な攻撃に含まれ得る。
【００３７】
さらに、対称暗号化アルゴリズムが実行されるたびに、対称暗号化動作中に使用された鍵に関するサイドチャネルデータなどの情報が明らかになり得る。サイドチャネルデータ

には、鍵の使用中に暗号化アルゴリズムが実行されるときに発生するわずかな電力変動が含まれ得る。サイドチャネルデータを十分に測定して、攻撃者が鍵を回復できるようにするための鍵に関する十分な情報を明らかにできる。同じ鍵を使用してデータを交換すると、同じ鍵で処理されたデータが繰り返し明らかにされる。

【００３８】

しかしながら、特定の鍵が使用される回数を制限することにより、攻撃者が収集できるサイドチャネルデータの量が制限され、それによって、この攻撃や他の種類の攻撃への露出が減少する。本明細書でさらに説明するように、暗号情報の交換に関与する当事者（例えば、送信者および受信者）は、カウンタ値と組み合わせて最初の共有マスター対称鍵から独立して鍵を生成し、それによって、使用されている共有対称鍵を定期的に置き換え、当事者の同期を維持するために任意の形式の鍵交換に頼る必要がある。送信者と受信者が使用する共有秘密対称鍵を定期的に変更することで、上記の攻撃を不可能にする。

【００３９】

図２に戻ると、システム２００は、鍵の多様化を実施するように構成され得る。例えば、送信者および受信者は、それぞれのデバイス２０５および２１０を介してデータ（例えば、元の機密データ）を交換することを望むことができる。上で説明したように、送信デバイス２０５および受信デバイス２１０の単一のインスタンスが含まれ得るが、各当事者が同じ共有秘密対称鍵を共有する限り、１つまたは複数の送信デバイス２０５および１つまたは複数の受信デバイス２１０が関与し得ることが理解される。いくつかの例では、送信デバイス２０５および受信デバイス２１０は、同じマスター対称鍵でプロビジョニングされ得る。さらに、同じ秘密対称鍵を保持する任意の当事者またはデバイスは、送信デバイス２０５の機能を実行でき、同様に、同じ秘密対称鍵を保持する任意の当事者は、受信デバイス２１０の機能を実行できることが理解される。いくつかの例では、対称鍵は、安全なデータの交換に関与する送信デバイス２０５および受信デバイス２１０以外の全ての当事者から秘密に保たれる共有秘密対称鍵を備え得る。さらに、送信デバイス２０５と受信デバイス２１０の両方に同じマスター対称鍵を提供でき、さらに、送信デバイス２０５と受信デバイス２１０との間で交換されるデータの一部は、カウンタ値と呼ばれ得るデータの少なくとも一部分を備え得ることが理解される。カウンタ値は、送信デバイス２０５と受信デバイス２１０との間でデータが交換されるたびに変化する数を備え得る。

【００４０】

システム２００は、１つまたは複数のネットワーク２１５を含み得る。いくつかの例では、ネットワーク２１５は、無線ネットワーク、有線ネットワーク、または無線ネットワークと有線ネットワークの任意の組み合わせのうちの１つまたは複数であり得、１つまたは複数の送信デバイス２０５および１つまたは複数の受信デバイス２１０をサーバ２２０に接続するように構成され得る。例えば、ネットワーク２１５は、光ファイバネットワーク、パッシブ光ネットワーク、ケーブルネットワーク、インターネットネットワーク、衛星ネットワーク、ワイヤレスＬＡＮ、モバイル通信のためのグローバルシステム、パーソナル通信サービス、パーソナルエリアネットワーク、ワイヤレスアプリケーションプロトコル、マルチメディアメッセージングサービス、拡張メッセージングサービス、ショートメッセージサービス、時間分割マルチプレックスベースのシステム、コード分割マルチアクセスベースのシステム、Ｄ－ＡＭＰＳ、Ｗｉ－Ｆｉ、固定ワイヤレスデータ、ＩＥＥＥ８０２．１１ｂ、８０２．１５．１、８０２．１１ｎおよび８０２．１１ｇ、ブルートゥース（登録商標）、ＮＦＣ、ＲＦＩＤ、Ｗｉ－Ｆｉなどのうちの１つまたは複数を含み得る。

【００４１】

さらに、ネットワーク２１５は、これらに限定されないが、電話回線、光ファイバ、ＩＥＥＥイーサネット９０２．３、ワイドエリアネットワーク、ワイヤレスパーソナルエリアネットワーク、ＬＡＮ、またはインターネットなどのグローバルネットワークを含み得る。さらに、ネットワーク２１５は、インターネットネットワーク、無線通信ネットワーク、セルラネットワークなど、またはそれらの任意の組み合わせをサポートできる。ネッ

トワーク２１５は、スタンドアロンネットワークとして、または互いに協力して動作する、１つのネットワーク、または上記の任意の数の例示的なタイプのネットワークをさらに含み得る。ネットワーク２１５は、それらが通信可能に結合されている１つまたは複数のネットワーク要素の１つまたは複数のプロトコルを利用できる。ネットワーク２１５は、他のプロトコルとの間で、ネットワークデバイスの１つまたは複数のプロトコルに変換できる。ネットワーク２１５は、単一のネットワークとして示されているが、１つまたは複数の例によれば、ネットワーク２１５は、例えば、インターネット、サービスプロバイダのネットワーク、ケーブルテレビネットワーク、クレジットカードアソシエーションネットワークなどの企業ネットワーク、およびホームネットワークなどの複数の相互接続されたネットワークを備え得ることを理解されたい。

【００４２】

いくつかの例では、１つまたは複数の送信デバイス２０５および１つまたは複数の受信デバイス２１０は、ネットワーク２１５を通過することなく、相互に通信し、データを送受信するように構成され得る。例えば、１つまたは複数の送信デバイス２０５と１つまたは複数の受信デバイス２１０との間の通信は、ＮＦＣ、ブルートゥース（登録商標）、ＲＦＩＤ、Ｗｉ－Ｆｉなどのうちの少なくとも１つを介して発生し得る。

【００４３】

ブロック２２５で、送信デバイス２０５が対称暗号化動作で機密データを処理する準備をしているとき、送信者は、カウンタを更新できる。さらに、送信デバイス２０５は、適切な対称暗号法アルゴリズムを選択でき、これは、対称暗号化アルゴリズム、ＨＭＡＣアルゴリズム、およびＣＭＡＣアルゴリズムのうちの少なくとも１つを含み得る。いくつかの例では、多様化値を処理するために使用される対称アルゴリズムは、所望の長さの多様化された対称鍵を生成するために必要に応じて使用される任意の対称暗号化アルゴリズムを備え得る。対称アルゴリズムの非限定的な例には、３ＤＥＳまたはＡＥＳ１２８、ＨＭＡＣ－ＳＨＡ－２５６などの対称ＨＭＡＣアルゴリズム、ＡＥＳ－ＣＭＡＣなどの対称ＣＭＡＣアルゴリズムなどの対称暗号化アルゴリズムが含まれ得る。選択された対称アルゴリズムの出力が十分に長い鍵を生成しない場合、異なる入力データと同じマスター鍵で対称アルゴリズムの複数の反復を処理するなどの技術は、十分な長さの鍵を生成するために必要に応じて組み合わせることができる複数の出力を生成し得ることを理解されたい。

【００４４】

ブロック２３０で、送信デバイス２０５は、選択された暗号化アルゴリズムを採用し、マスター対称鍵を使用して、カウンタ値を処理できる。例えば、送信者は、対称暗号化アルゴリズムを選択し、送信デバイス２０５と受信デバイス２１０との間の全ての会話で更新するカウンタを使用できる。次に、送信デバイス２０５は、マスター対称鍵を使用して、選択された対称暗号化アルゴリズムでカウンタ値を暗号化し、多様化された対称鍵を作成できる。

【００４５】

いくつかの例では、カウンタ値は、暗号化されない場合がある。これらの例では、カウンタ値は、暗号化なしで、ブロック２３０で送信デバイス２０５と受信デバイス２１０との間で送信され得る。

【００４６】

ブロック２３５で、多様化された対称鍵を使用して、結果を受信デバイス２１０に送信する前に機密データを処理できる。例えば、送信デバイス２０５は、多様化された対称鍵を使用する対称暗号化アルゴリズムを使用して機密データを暗号化でき、出力は、保護された暗号化データを備える。次に、送信デバイス２０５は、保護された暗号化データを、カウンタ値とともに、処理のために受信デバイス２１０に送信できる。

【００４７】

ブロック２４０で、受信デバイス２１０は、最初にカウンタ値を取得し、次に、暗号化への入力としてカウンタ値を使用し、暗号化のための鍵としてマスター対称鍵を使用して、同じ対称暗号化を実行できる。暗号化の出力は、送信者によって作成されたものと同じ

多様な対称鍵値であり得る。

【００４８】

次に、ブロック２４５で、受信デバイス２１０は、保護された暗号化データを取得し、多様化された対称鍵とともに対称復号アルゴリズムを使用して、保護された暗号化データを復号できる。

【００４９】

ブロック２５０で、保護された暗号化されたデータを復号した結果として、元の機密データが明らかにされ得る。

【００５０】

次に機密データを送信者から受信者にそれぞれの送信デバイス２０５および受信デバイス２１０を介して送信する必要があるとき、異なるカウンタ値を選択して、異なる多様な対称鍵を生成できる。マスター対称鍵と同じ対称暗号法アルゴリズムを使用してカウンタ値を処理することにより、送信デバイス２０５と受信デバイス２１０の両方が、同じ多様な対称鍵を独立して生成できる。マスター対称鍵ではなく、この多様な対称鍵は、機密データを保護するために使用される。

【００５１】

上で説明したように、送信デバイス２０５と受信デバイス２１０の両方は、最初に、共有マスター対称鍵をそれぞれ所有している。共有マスター対称鍵は、元の機密データの暗号化には使用されない。多様化された対称鍵は、送信デバイス２０５と受信デバイス２１０の両方によって独立して作成されるため、両者の間で送信されることは決してない。したがって、攻撃者は、多様化された対称鍵を傍受することはできず、攻撃者は、マスター対称鍵で処理されたデータを見ることはない。機密データではなく、カウンタ値のみがマスター対称鍵で処理される。その結果、マスター対称鍵に関するサイドチャネルデータの削減が明らかになる。さらに、送信デバイス２０５および受信デバイス２１０の動作は、新しい多様化値、したがって、新しい多様化された対称鍵を作成する頻度に関する対称要件によって支配され得る。一実施形態では、新しい多様化値、したがって、新しい多様化された対称鍵は、送信デバイス２０５と受信デバイス２１０との間の全ての交換のために作成され得る。

【００５２】

いくつかの例では、鍵多様化値は、カウンタ値を構成し得る。鍵多様化値の他の非限定的な例には、新しい多様化鍵が必要とされるたびに生成されるランダムナンス、送信デバイス２０５から受信デバイス２１０に送信されるランダムナンス、送信デバイス２０５および受信デバイス２１０から送信されたカウンタ値の完全な値、送信デバイス２０５および受信デバイス２１０から送信されるカウンタ値の一部分、送信デバイス２０５および受信デバイス２１０によって独立して維持されるが、２つのデバイス間で送信されないカウンタ、送信デバイス２０５と受信デバイス２１０との間で交換されるワンタイムパスコード、機密データの暗号化ハッシュが含まれる。いくつかの例では、鍵多様化値の１つまたは複数の部分が、複数の多様化された鍵を作成するために当事者によって使用され得る。例えば、カウンタを鍵多様化値として使用できる。さらに、上記の例示的な鍵多様化値のうちの１つまたは複数の組み合わせを使用できる。

【００５３】

他の例では、カウンタの一部分を鍵多様化値として使用できる。複数のマスター鍵値が当事者間で共有される場合、複数の多様化された鍵値は、本明細書に記載のシステムおよびプロセスによって取得され得る。新しい多様化値、したがって、新しい多様化された対称鍵は、必要に応じて何度でも作成できる。最も安全な場合、送信デバイス２０５と受信デバイス２１０との間の機密データの交換ごとに、新しい多様化値が作成され得る。事実上、これにより、シングルユースセッション鍵などのワンタイム使用鍵が作成され得る。

【００５４】

図３は、非接触カードを使用するシステム３００を示している。システム３００は、非接触カード３０５、１つまたは複数のクライアントデバイス３１０、ネットワーク３１５

、サーバ３２０、３２５、１つまたは複数のハードウェアセキュリティモジュール３３０、およびデータベース３３５を含み得る。図３は、コンポーネントの単一のインスタンスを示しているが、システム３００は、任意の数のコンポーネントを含み得る。

【００５５】

システム３００は、１つまたは複数の非接触カード３０５を含み得、これは、図５Ａから図５Ｂに関して以下でさらに説明される。いくつかの例では、非接触カード３０５は、クライアントデバイス３１０との無線通信、例えば、ＮＦＣ通信であり得る。例えば、非接触カード３０５は、ＮＦＣまたは他の短距離プロトコルを介して通信するように構成された、無線周波数識別チップなどの１つまたは複数のチップを備え得る。他の実施形態では、非接触カード３０５は、ブルートゥース（登録商標）、衛星、Ｗｉ－Ｆｉ、有線通信、および／または無線接続と有線接続の任意の組み合わせを含むがこれらに限定されない他の手段を介してクライアントデバイス３１０と通信できる。いくつかの実施形態によれば、非接触カード３０５は、非接触カード３０５がカードリーダ３１３の範囲内にあるときに、ＮＦＣを介してクライアントデバイス３１０のカードリーダ３１３と通信するように構成され得る。他の例では、非接触カード３０５との通信は、物理的インターフェース、例えば、ユニバーサルシリアルバスインターフェースまたはカードスワイプインターフェースを介して達成され得る。

【００５６】

システム３００は、ネットワーク対応コンピュータであり得るクライアントデバイス３１０を含み得る。本明細書で言及されるように、ネットワーク対応コンピュータは、例えば、コンピュータデバイス、または、例えば、サーバ、ネットワークアプライアンス、パーソナルコンピュータ、ワークステーション、モバイルデバイス、電話、ハンドヘルドＰＣ、パーソナルデジタルアシスタント、シンクライアント、ファットクライアント、インターネットブラウザ、またはその他のデバイスを含む通信デバイスを含み得るが、これらに限定されない。１つまたは複数のクライアントデバイス３１０はまた、モバイルデバイスであり得る。例えば、モバイルデバイスには、Ａｐｐｌｅ（登録商標）のｉＰｈｏｎｅ（登録商標）、ｉＰｏｄ（登録商標）、ｉＰａｄ（登録商標）、またはＡｐｐｌｅのｉＯＳ（登録商標）オペレーティングシステムを実行するその他のモバイルデバイス、ＭｉｃｒｏｓｏｆｔのＷｉｎｄｏｗｓ（登録商標）Ｍｏｂｉｌｅオペレーティングシステムを実行するデバイス、ＧｏｏｇｌｅのＡｎｄｒｏｉｄ（登録商標）オペレーティングシステムを実行するデバイス、および／または他のスマートフォンまたは同様のウェアラブルモバイルデバイスを含み得る。いくつかの例では、クライアントデバイス３１０は、図１Ａまたは図１Ｂを参照して説明したように、クライアントデバイス１１０と同じまたは類似し得る。

【００５７】

クライアントデバイス３１０は、１つまたは複数のネットワーク３１５を介して１つまたは複数のサーバ３２０および３２５と通信できる。クライアントデバイス３１０は、例えば、クライアントデバイス３１０上で実行されているアプリケーション３１１から、１つまたは複数の要求を１つまたは複数のサーバ３２０および３２５に送信できる。１つまたは複数の要求は、１つまたは複数のサーバ３２０および３２５からのデータの検索に関連付けることができる。サーバ３２０および３２５は、クライアントデバイス３１０から１つまたは複数の要求を受信できる。クライアントデバイス３１０からの１つまたは複数の要求に基づいて、１つまたは複数のサーバ３２０および３２５は、１つまたは複数のデータベース３３５から要求されたデータを検索するように構成され得る。１つまたは複数のデータベース３３５からの要求されたデータの受信に基づいて、１つまたは複数のサーバ３２０および３２５は、受信されたデータをクライアントデバイス３１０に送信するように構成され得、受信されたデータは、１つまたは複数の要求に応答する。

【００５８】

システム３００は、１つまたは複数のハードウェアセキュリティモジュール（ＨＳＭ）３３０を含み得る。例えば、１つまたは複数のＨＳＭ３３０は、本明細書に開示されるよ

うに、１つまたは複数の暗号化動作を実行するように構成され得る。いくつかの例では、１つまたは複数のＨＳＭ３３０は、１つまたは複数の暗号化動作を実行するように構成された特別な目的のセキュリティデバイスとして構成され得る。ＨＳＭ３３０は、鍵がＨＳＭ３３０の外部に決して明らかにされないように構成され得、代わりに、ＨＳＭ３３０内で維持される。例えば、１つまたは複数のＨＳＭ３３０は、鍵導出、復号、およびＭＡＣ動作の少なくとも１つを実行するように構成できる。１つまたは複数のＨＳＭ３３０は、サーバ３２０および３２５内に含まれ得るか、またはサーバ３２０および３２５とデータ通信され得る。

【００５９】

システム３００は、１つまたは複数のネットワーク３１５を含み得る。いくつかの例では、ネットワーク３１５は、無線ネットワーク、有線ネットワーク、または無線ネットワークと有線ネットワークの任意の組み合わせのうちの１つまたは複数であり得、クライアントデバイス３１５をサーバ３２０および３２５に接続するように構成され得る。例えば、ネットワーク３１５は、光ファイバネットワーク、パッシブ光ネットワーク、ケーブルネットワーク、セルラネットワーク、インターネットネットワーク、衛星ネットワーク、ワイヤレスＬＡＮ、モバイル通信のためのグローバルシステム、パーソナル通信サービス、パーソナルエリアネットワーク、ワイヤレスアプリケーションプロトコル、マルチメディアメッセージングサービス、拡張メッセージングサービス、ショートメッセージサービス、時間分割マルチプレックスベースのシステム、コード分割マルチアクセスベースのシステム、Ｄ－ＡＭＰＳ、Ｗｉ－Ｆｉ、固定ワイヤレスデータ、ＩＥＥＥ ８０２．１１ｂ、８０２．１５．１、８０２．１１ｎおよび８０２．１１ｇ、ブルートゥース（登録商標）、ＮＦＣ、ＲＦＩＤ、Ｗｉ－Ｆｉ、および／またはそれらのネットワークの任意の組み合わせのうちの１つまたは複数を含み得る。非限定的な例として、非接触カード３０５およびクライアントデバイス３１０からの通信は、ＮＦＣ通信、クライアントデバイス３１０とキャリアとの間のセルラネットワーク、およびキャリアとバックエンドとの間のインターネットを備え得る。

【００６０】

さらに、ネットワーク３１５は、電話回線、光ファイバ、ＩＥＥＥイーサネット９０２．３、ワイドエリアネットワーク、ワイヤレスパーソナルエリアネットワーク、ローカルエリアネットワーク、またはインターネットなどのグローバルネットワークを含むがこれらに限定されない。さらに、ネットワーク３１５は、インターネットネットワーク、無線通信ネットワーク、セルラネットワークなど、またはそれらの任意の組み合わせをサポートできる。ネットワーク３１５は、スタンドアロンネットワークとして、または互いに協力して動作する、１つのネットワーク、または上記の任意の数の例示的なタイプのネットワークをさらに含み得る。ネットワーク３１５は、それらが通信可能に結合されている１つまたは複数のネットワーク要素の１つまたは複数のプロトコルを利用できる。ネットワーク３１５は、他のプロトコルとの間で、ネットワークデバイスの１つまたは複数のプロトコルに変換できる。ネットワーク３１５は、単一のネットワークとして示されているが、１つまたは複数の例によれば、ネットワーク３１５は、例えば、インターネット、サービスプロバイダのネットワーク、ケーブルテレビネットワーク、クレジットカードアソシエーションネットワークなどの企業ネットワーク、およびホームネットワークなどの複数の相互接続されたネットワークを備え得ることを理解されたい。

【００６１】

本開示による様々な例では、システム３００のクライアントデバイス３１０は、１つまたは複数のアプリケーション３１１を実行でき、１つまたは複数のプロセッサ３１２、および１つまたは複数のカードリーダ３１３を含む。例えば、ソフトウェアアプリケーションなどの１つまたは複数のアプリケーション３１１は、例えば、システム３００の１つまたは複数のコンポーネントとのネットワーク通信を可能にし、データを送信および／または受信するように構成され得る。図３には、クライアントデバイス３１０のコンポーネントの単一のインスタンスのみが示されているが、任意の数のデバイス３１０を使用できる

ことが理解される。カードリーダ３１３は、非接触カード３０５から読み取る、および／またはそれと通信するように構成され得る。１つまたは複数のアプリケーション３１１と併せて、カードリーダ３１３は、非接触カード３０５と通信できる。

【００６２】

クライアントデバイス３１０のいずれかのアプリケーション３１１は、短距離無線通信（例えば、ＮＦＣ）を使用して非接触カード３０５と通信できる。アプリケーション３１１は、非接触カード３０５と通信するように構成されたクライアントデバイス３１０のカードリーダ３１３とインターフェースするように構成され得る。注意すべきように、当業者は、２０センチメートル未満の距離がＮＦＣ範囲と一致していることを理解するであろう。

【００６３】

いくつかの実施形態では、アプリケーション３１１は、関連するリーダ（例えば、カードリーダ３１３）を介して非接触カード３０５と通信する。

【００６４】

いくつかの実施形態では、カードのアクティブ化は、ユーザ認証なしで発生し得る。例えば、非接触カード３０５は、ＮＦＣを介してクライアントデバイス３１０のカードリーダ３１３を介してアプリケーション３１１と通信できる。通信（例えば、クライアントデバイス３１０のカードリーダ３１３に近接するカードのタップ）は、アプリケーション３１１がカードに関連するデータを読み取り、アクティブ化を実行することを可能にする。場合によっては、タップは、アプリケーション３１１をアクティブ化または起動し、その後、１つまたは複数のアクションまたはアカウントサーバ３２５との通信を開始して、その後の使用のためにカードをアクティブ化できる。場合によっては、アプリケーション３１１がクライアントデバイス３１０にインストールされていない場合、カードリーダ３１３に対するカードのタップは、アプリケーション３１１のダウンロードを開始できる（例えば、アプリケーションダウンロードページへのナビゲーション）。インストールに続いて、カードをタップすると、アプリケーション３１１をアクティブ化または起動し、次に（例えば、アプリケーションまたは他のバックエンド通信を介して）カードのアクティブ化を開始できる。アクティブ化後、カードは商取引を含む様々なトランザクションで使用できる。

【００６５】

いくつかの実施形態によれば、非接触カード３０５は、仮想支払いカードを含み得る。それらの実施形態では、アプリケーション３１１は、クライアントデバイス３１０上に実施されたデジタルウォレットにアクセスすることによって、非接触カード３０５に関連する情報を検索でき、デジタルウォレットは、仮想支払いカードを含む。いくつかの例では、仮想支払いカードデータは、１つまたは複数の静的または動的に生成された仮想カード番号を含み得る。

【００６６】

サーバ３２０は、データベース３３５と通信するウェブサーバを備え得る。サーバ３２５は、アカウントサーバを備え得る。いくつかの例では、サーバ３２０は、データベース３３５内の１つまたは複数の資格情報と比較することによって、非接触カード３０５および／またはクライアントデバイス３１０からの１つまたは複数の資格情報を検証するように構成され得る。サーバ３２５は、非接触カード３０５および／またはクライアントデバイス３１０からの支払いおよびトランザクションなどの１つまたは複数の要求を許可するように構成され得る。

【００６７】

図４は、本開示の例による鍵多様化の方法４００を示している。方法４００は、図２で参照される送信デバイス２０５および受信デバイス２１０と同様の送信デバイスおよび受信デバイスを含み得る。

【００６８】

例えば、送信者と受信者は、送信デバイスと受信デバイスを介してデータ（例えば、元

の機密データ）を交換することを望み得る。上で説明したように、これらの２つの当事者が含まれ得るが、各当事者が同じ共有秘密対称鍵を共有する限り、１つまたは複数の送信デバイスおよび１つまたは複数の受信デバイスが関与し得ることが理解される。いくつかの例では、送信デバイスと受信デバイスは、同じマスター対称鍵でプロビジョニングされ得る。さらに、同じ秘密対称鍵を保持する任意の当事者またはデバイスが送信デバイスの機能を実行でき、同様に、同じ秘密対称鍵を保持する任意の当事者が受信デバイスの機能を実行できることが理解される。いくつかの例では、対称鍵は、安全なデータの交換に関与する送信デバイスおよび受信デバイス以外の全ての当事者から秘密に保たれる共有秘密対称鍵を備え得る。さらに、送信デバイスと受信デバイスの両方に同じマスター対称鍵を提供でき、さらに、送信デバイスと受信デバイスとの間で交換されるデータの一部は、カウンタ値と呼ばれ得るデータの少なくとも一部分を備えることが理解される。カウンタ値は、送信デバイスと受信デバイスとの間でデータが交換されるたびに変化する数を備え得る。

【００６９】

ブロック４１０で、送信デバイスおよび受信デバイスは、同じマスター対称鍵などの同じマスター鍵でプロビジョニングされ得る。送信デバイスが対称暗号化動作で機密データを処理する準備をしているとき、送信者は、カウンタを更新できる。さらに、送信デバイスは、適切な対称暗号法アルゴリズムを選択でき、これは、対称暗号化アルゴリズム、ＨＭＡＣアルゴリズム、およびＣＭＡＣアルゴリズムのうちの少なくとも１つを含み得る。いくつかの例では、多様化値を処理するために使用される対称アルゴリズムは、所望の長さの多様化された対称鍵を生成するために必要に応じて使用される任意の対称暗号法アルゴリズムを備え得る。対称アルゴリズムの非限定的な例には、３ＤＥＳまたはＡＥＳ１２８、ＨＭＡＣ－ＳＨＡ－２５６などの対称ＨＭＡＣアルゴリズム、ＡＥＳ－ＣＭＡＣなどの対称ＣＭＡＣアルゴリズムなどの対称暗号化アルゴリズムが含まれ得る。選択された対称アルゴリズムの出力が十分に長い鍵を生成しない場合、異なる入力データと同じマスター鍵で対称アルゴリズムの複数の反復を処理するなどの技術は、十分な長さの鍵を生成するために必要に応じて組み合わせることができる複数の出力を生成し得ることが理解される。

【００７０】

送信デバイスは、選択された暗号法アルゴリズムを使用し、マスター対称鍵を使用してカウンタ値を処理し得る。例えば、送信者は、対称暗号化アルゴリズムを選択し、送信デバイスと受信デバイス間の会話ごとに更新されるカウンタを使用できる。

【００７１】

次に、ブロック４２０で、送信デバイスは、マスター対称鍵を使用して、選択された対称暗号化アルゴリズムでカウンタ値を暗号化し、多様化された対称鍵を作成できる。多様化された対称鍵を使用して、結果を受信デバイスに送信する前に機密データを処理できる。例えば、送信デバイスは、多様化された対称鍵を使用する対称暗号化アルゴリズムを使用して機密データを暗号化し、出力は、保護された暗号化データを備えることができる。次に、送信デバイスは、保護された暗号化データを、カウンタ値とともに、処理のために受信デバイスに送信できる。いくつかの例では、暗号化以外の暗号化動作を実行でき、保護されたデータを送信する前に、多様化された対称鍵を使用して複数の暗号化動作を実行できる。

【００７２】

いくつかの例では、カウンタ値は、暗号化されない場合がある。これらの例では、カウンタ値は、暗号化なしで、ブロック４２０で送信デバイスと受信デバイスとの間で送信され得る。

【００７３】

ブロック４３０で、機密データは、１つまたは複数の暗号化アルゴリズムおよび多様化された鍵を使用して保護され得る。カウンタを使用する鍵の多様化によって作成される可能性のある多様化されたセッション鍵は、機密データを保護するために１つまたは複数の

暗号化アルゴリズムとともに使用され得る。例えば、データは、第１の多様化されたセッション鍵を使用してＭＡＣによって処理され得、結果の出力は、保護されたデータを生成する第２の多様化されたセッション鍵を使用して暗号化され得る。

【００７４】

ブロック４４０で、受信デバイスは、暗号化への入力としてカウンタ値を使用し、暗号化のための鍵としてマスター対称鍵を使用して、同じ対称暗号化を実行できる。暗号化の出力は、送信者によって作成されたものと同じ多様化された対称鍵値であり得る。例えば、受信デバイスは、カウンタを使用して、第１および第２の多様化されたセッション鍵の独自のコピーを独立して作成できる。次に、受信デバイスは、第２の多様化されたセッション鍵を使用して保護されたデータを復号し、送信デバイスによって作成されたＭＡＣの出力を明らかにできる。次に、受信デバイスは、第１の多様化されたセッション鍵を使用して、ＭＡＣ動作を通じて結果のデータを処理できる。

【００７５】

ブロック４５０で、受信デバイスは、保護されたデータを検証するために、１つまたは複数の暗号化アルゴリズムを備えた多様化された鍵を使用できる。

【００７６】

ブロック４６０で、元のデータを検証できる。ＭＡＣ動作の出力（第１の多様化されたセッション鍵を使用する受信デバイスを介して）が復号によって明らかにされたＭＡＣ出力と一致する場合、データは有効であると見なされ得る。

【００７７】

次に、機密データを送信デバイスから受信デバイスに送信する必要がある場合、異なるカウンタ値を選択でき、これにより、異なる多様化された対称鍵が生成される。マスター対称鍵と同じ対称暗号化アルゴリズムを使用してカウンタ値を処理することにより、送信デバイスと受信デバイスの両方が独立して同じ多様化された対称鍵を生成できる。マスター対称鍵ではなく、この多様化された対称鍵は、機密データを保護するために使用される。

【００７８】

上で説明したように、送信デバイスと受信デバイスの両方が、最初は共有マスター対称鍵をそれぞれ所有している。共有マスター対称鍵は、元の機密データの暗号化には使用されない。多様化された対称鍵は、送信デバイスと受信デバイスの両方によって独立して作成されるため、２者間で送信されることはない。したがって、攻撃者は、多様化された対称鍵を傍受することはできず、攻撃者は、マスター対称鍵で処理されたデータを見ることはない。機密データではなく、小さいカウンタ値のみがマスター対称鍵で処理される。その結果、マスター対称鍵に関するサイドチャネルデータの削減が明らかになる。さらに、送信者と受信者は、例えば、事前の取り決めまたは他の手段によって、新しい多様化値、したがって、新しい多様化された対称鍵を作成する頻度について合意できる。一実施形態では、新しい多様化値、したがって、新しい多様化された対称鍵は、送信デバイスと受信デバイスとの間の全ての交換のために作成され得る。

【００７９】

いくつかの例では、鍵多様化値はカウンタ値を構成し得る。鍵多様化値の他の非限定的な例には、新しい多様化された鍵が必要とされるたびに生成されるランダムナンス、送信デバイスから受信デバイスに送信されるランダムナンス、送信デバイスと受信デバイスから送信されたカウンタ値の完全な値、送信デバイスと受信デバイスから送信されたカウンタ値の一部、送信デバイスと受信デバイスによって独立して維持されるが、２つの間で送信されないカウンタ、送信デバイスと受信デバイスとの間で交換されるワンタイムパスコード、機密データの暗号化ハッシュが含まれる。いくつかの例では、鍵多様化値の１つまたは複数の部分が、複数の多様化された鍵を作成するために当事者によって使用され得る。例えば、カウンタを鍵多様化値として使用できる。

【００８０】

他の例では、カウンタの一部を鍵多様化値として使用できる。複数のマスター鍵値が当事者間で共有される場合、複数の多様化された鍵値は、本明細書に記載のシステムおよび

プロセスによって取得され得る。新しい多様化値、したがって、新しい多様化された対称鍵は、必要に応じて何度でも作成できる。最も安全なケースでは、送信デバイスと受信デバイスとの間で機密データを交換するたびに、新しい多様化値が作成され得る。事実上、これにより、単一のセッション鍵などのワンタイム使用鍵が作成され得る。

【００８１】

マスター対称鍵の使用回数を制限するなどの他の例では、送信デバイスの送信者と受信デバイスの受信者は、新しい多様化値、したがって、新しい多様化された対称鍵が定期的にのみ発生すること合意し得る。一例では、これは、送信デバイスと受信デバイスとの間の１０回の送信毎など、所定の回数の使用の後であり得る。他の例では、これは、特定の期間の後、送信後の特定の期間、または定期的に（例えば、指定された時間に毎日；指定された日の指定された時間に毎週）発生し得る。他の例では、これは、受信デバイスが、次の通信で鍵を変更することを望むことを送信デバイスに信号を送るたびであり得る。これは、ポリシーに基づいて制御でき、例えば、受信デバイスの受信者が認識している現在のリスクレベルによって異なり得る。

【００８２】

図５Ａは、１つまたは複数の非接触カード５００を示しており、カード５００の前面または背面に表示されたサービスプロバイダ５０５によって発行された、クレジットカード、デビットカード、またはギフトカードなどの支払いカードを備え得る。いくつかの例では、非接触カード５００は、支払いカードとは関係がなく、識別カードを備えることができるが、これに限定されない。いくつかの例では、支払いカードは、デュアルインターフェースの非接触支払いカードを備え得る。非接触カード５００は、プラスチック、金属、および他の材料から構成される単層または１つまたは複数の積層層を含み得る基板５１０を備え得る。例示的な基板材料には、ポリ塩化ビニル、ポリ塩化ビニルアセテート、アクリロニトリルブタジエンスチレン、ポリカーボネート、ポリエステル、陽極酸化チタン、パラジウム、金、カーボン、紙、および生分解性材料が含まれる。いくつかの例では、非接触カード５００は、ＩＳＯ／ＩＥＣ　７８１０規格のＩＤ－１フォーマットに準拠する物理的特性を有し得、そうでなければ、非接触カードは、ＩＳＯ／ＩＥＣ　１４４４３規格に準拠し得る。しかしながら、本開示に係る非接触カード５００は、異なる特性を有し得ることが理解され、本開示は、非接触カードが支払いカードに実施されることを必要としない。

【００８３】

非接触カード５００はまた、カードの前面および／または背面に表示される識別情報５１５、および接触パッド５２０を含み得る。接触パッド５２０は、ユーザデバイス、スマートフォン、ラップトップ、デスクトップ、またはタブレットコンピュータなどの他の通信デバイスとの接触を確立するように構成され得る。非接触カード５００はまた、図５Ａに示されていない処理回路、アンテナおよび他のコンポーネントを含み得る。これらのコンポーネントは、接触パッド５２０の後ろまたは基板５１０上の他の場所に配置し得る。非接触カード５００はまた、カードの背面に配置され得る磁気ストリップまたはテープを含み得る（図５Ａには示されていない）。

【００８４】

図５Ｂに示されるように、図５Ａの接触パッド５２０は、マイクロプロセッサ５３０およびメモリ５３５を含む、情報を格納および処理するための処理回路５２５を含み得る。処理回路５２５は、本明細書に記載の機能を実行するために必要に応じて、プロセッサ、メモリ、エラーおよびパリティ／ＣＲＣチェッカー、データエンコーダ、衝突防止アルゴリズム、コントローラ、コマンドデコーダ、セキュリティプリミティブおよび改ざん防止ハードウェアを含む追加のコンポーネントを含み得ることが理解される。

【００８５】

メモリ５３５は、読み取り専用メモリ、ライトワンスリードマルチプルメモリ、または読み取り／書き込みメモリ、例えば、ＲＡＭ、ＲＯＭ、およびＥＥＰＲＯＭであり得、非接触カード５００は、これらのメモリのうちの１つまたは複数を含み得る。読み取り専用

メモリは、工場で読み取り専用または１回限りのプログラム可能としてプログラム可能である。１回限りのプログラム可能性により、１回書き込みを行ってから、何度も読み取る機会を提供する。ライトワンス／リードマルチプルメモリは、メモリチップが工場から出荷された後のある時点でプログラムできる。一度メモリをプログラムすると、書き換えはできないが、何度も読み取ることができる。読み取り／書き込みメモリは、工場出荷後に何度もプログラムおよび再プログラムされ得る。何度も読み取ることもある。

【００８６】

メモリ５３５は、１つまたは複数のアプレット５４０、１つまたは複数のカウンタ５４５、および顧客識別子５５０を格納するように構成され得る。１つまたは複数のアプレット５４０は、Ｊａｖａ　Ｃａｒｄアプレットなどの１つまたは複数の非接触カード上で実行するように構成された１つまたは複数のソフトウェアアプリケーションを備え得る。しかしながら、アプレット５４０は、Ｊａｖａカードアプレットに限定されず、代わりに、非接触カードまたは限られたメモリを有する他のデバイス上で動作可能な任意のソフトウェアアプリケーションであり得ることが理解される。１つまたは複数のカウンタ５４５は、整数を格納するのに十分な数値カウンタを備え得る。顧客識別子５５０は、非接触カード５００のユーザに割り当てられた一意の英数字識別子を備え得、識別子は、非接触カードのユーザを他の非接触カードユーザから区別し得る。いくつかの例では、顧客識別子５５０は、顧客とその顧客に割り当てられたアカウントの両方を識別し得、さらに、顧客のアカウントに関連付けられた非接触カードを識別し得る。

【００８７】

前述の例示的な実施形態のプロセッサおよびメモリ要素は、接触パッドを参照して説明されているが、本開示はそれに限定されない。これらの要素は、パッド５２０の外側に実施されるか、パッド５２０から完全に分離されて、または接触パッド５２０内に配置されるプロセッサ５３０およびメモリ５３５要素に加えてさらなる要素として実施され得ることが理解される。

【００８８】

いくつかの例では、非接触カード５００は、１つまたは複数のアンテナ５５５を備え得る。１つまたは複数のアンテナ５５５は、非接触カード５００内で、接触パッド５２０の処理回路５２５の周りに配置し得る。例えば、１つまたは複数のアンテナ５５５は、処理回路５２５と一体であり得、１つまたは複数のアンテナ５５５は、外部ブースターコイルと共に使用され得る。他の例として、１つまたは複数のアンテナ５５５は、接触パッド５２０および処理回路５２５の外部にあり得る。

【００８９】

一実施形態では、非接触カード５００のコイルは、空芯変圧器の二次側として機能できる。端子は、電力または振幅変調を遮断することによって非接触カード５００と通信できる。非接触カード５００は、非接触カードの電源接続のギャップを使用して端子から送信されたデータを推測でき、これは、１つまたは複数のコンデンサを介して機能的に維持できる。非接触カード５００は、非接触カードのコイルの負荷を切り替えるか、または負荷変調することによって、通信を戻すことができる。負荷変調は、干渉によって端子のコイルで検出され得る。

【００９０】

上で説明したように、非接触カード５００は、スマートカードまたはＪａｖａ　Ｃａｒｄなどの限られたメモリを有する他のデバイス上で動作可能なソフトウェアプラットフォーム上に構築され得、１つまたは複数のアプリケーションまたはアプレットが安全に実行され得る。アプレットを非接触カードに追加して、様々なモバイルアプリケーションベースのユースケースで多要素認証（ＭＦＡ）用のワンタイムパスワード（ＯＴＰ）を提供できる。アプレットは、モバイルＮＦＣリーダなどのリーダからの近接場データ交換要求などの１つまたは複数の要求に応答し、ＮＤＥＦテキストタグとしてエンコードされた暗号的に安全なＯＴＰを備えるＮＤＥＦメッセージを生成するように構成できる。

【００９１】

図６は、例示的な実施形態に係る、ＮＤＥＦショートレコードレイアウト（ＳＲ＝１）６００を示している。１つまたは複数のアプレットは、ＯＴＰをＮＤＥＦタイプ４のよく知られたタイプのテキストタグとしてエンコードするように構成できる。いくつかの例では、ＮＤＥＦメッセージは、１つまたは複数のレコードを備え得る。アプレットは、ＯＴＰレコードに加えて１つまたは複数の静的タグレコードを追加するように構成できる。例示的なタグには、タグタイプ：よく知られているタイプ、テキスト、英語のエンコーディング（ｅｎ）；アプレットＩＤ：Ｄ２７６０００００８５０１０１；機能：読み取り専用アクセス；エンコーディング：認証メッセージは、ＡＳＣＩＩ１６進数としてエンコードできる；ｔｙｐｅ－ｌｅｎｇｔｈ－ｖａｌｕｅ（ＴＬＶ）データは、ＮＤＥＦメッセージを生成するために使用できる個人化パラメータとして提供され得る、が含まれるが、これらに限定されない。一実施形態では、認証テンプレートは、実際の動的認証データを提供するための既知のインデックスを備えた第１のレコードを備え得る。

【００９２】

図７は、例示的な実施形態に係るメッセージ７１０およびメッセージフォーマット７２０を示している。一例では、追加のタグが追加される場合、第１のバイトは、メッセージの開始を示すように変更されるが、終了は示さず、後続のレコードが追加され得る。ＩＤ長がゼロであるため、ＩＤ長フィールドとＩＤはレコードから省略される。メッセージの例には、ＵＤＫ　ＡＵＴ鍵；派生したＡＵＴセッション鍵（０ｘ００００００５０を使用）；バージョン１．０；ｐＡＴＣ＝０ｘ００００００５０；ＲＮＤ＝４８３８ＦＢ７ＤＣ１７１Ｂ８９Ｅ；ＭＡＣ＝＜計算された８バイト＞が含まれる。

【００９３】

いくつかの例では、データは、安全なチャネルプロトコル２の下でＳＴＯＲＥ　ＤＡＴＡ（Ｅ２）を実施することによって、個人化時に非接触カードに格納され得る。個人化ビューローは、ＥＭＢＯＳＳファイル（アプレットＩＤで指定されたセクション）から１つまたは複数の値を読み取り、認証と安全なチャネルの確立後に、１つまたは複数のストアデータコマンドを非接触カードに送信できる。

【００９４】

ｐＵＩＤは、１６桁のＢＣＤエンコード番号で構成される。いくつかの例では、ｐＵＩＤは１４桁で構成され得る。

【表１】

項目	長さ（バイト）	暗号化されている？	注
ｐＵＩＤ	８	いいえ	
ＡｕｔＫｅｙ	１６	はい	ＭＡＣセッション鍵を導出するための３ＤＥＳ鍵
ＡｕｔＫＣＶ	３	いいえ	鍵チェック値
ＤＥＫＫｅｙ	１６	はい	暗号化セッション鍵を導出するための３ＤＥＳ鍵
ＤＥＫＫＣＶ	３	いいえ	鍵チェック値
カード共有ランダム	４バイト	いいえ	４バイトの真の乱数（事前生成）
ＮＴＬＶ	Ｘバイト	いいえ	ＮＤＥＦメッセージのＴＬＶデータ

【００９５】
いくつかの例では、１つまたは複数のアプレットは、その個人化状態を維持するように構成されて、ロック解除および認証された場合にのみ個人化を許可できる。他の状態は、標準的な状態の事前個人化を備え得る。終了状態に入ると、１つまたは複数のアプレットは、個人化データを削除するように構成され得る。終了状態では、１つまたは複数のアプレットは、全てのアプリケーションプロトコルデータユニット（ＡＰＤＵ）要求への応答を停止するように構成され得る。
【００９６】
１つまたは複数のアプレットは、認証メッセージで使用できるアプレットバージョン（２バイト）を維持するように構成できる。いくつかの例では、これは最上位バイトのメジャーバージョン、最下位バイトのマイナーバージョンとして解釈され得る。各バージョンのルールは、認証メッセージを解釈するように構成されている。例えば、メジャーバージョンに関しては、これには、各メジャーバージョンが特定の認証メッセージレイアウトと特定のアルゴリズムを備えることが含まれ得る。マイナーバージョンの場合、これには、バグ修正、セキュリティ強化などに加えて、認証メッセージまたは暗号化アルゴリズムへの変更、静的タグコンテンツへの変更が含まれ得ない。
【００９７】
いくつかの例では、１つまたは複数のアプレットは、ＲＦＩＤタグをエミュレートするように構成され得る。ＲＦＩＤタグは、１つまたは複数の多型タグを含み得る。いくつかの例では、タグが読み取られるたびに、非接触カードの信頼性を示す可能性のある様々な暗号化データが提示される。１つまたは複数のアプリケーションに基づいて、タグのＮＦＣ読み取りが処理され得、トークンがバックエンドサーバなどのサーバに送信され得、そ

してトークンがサーバで検証され得る。

【００９８】

いくつかの例では、非接触カードおよびサーバは、カードが適切に識別され得るように特定のデータを含み得る。非接触カードは、１つまたは複数の一意の識別子を備え得る。読み取り動作が行われるたびに、カウンタを更新するように構成できる。いくつかの例では、カードが読み取られるたびに、検証のためにサーバに送信され、（検証の一部として）カウンタが等しいかどうかが判別される。

【００９９】

１つまたは複数のカウンタは、リプレイ攻撃を防ぐように構成できる。例えば、暗号文が取得されて再生された場合、カウンタが読み取られたり、使用されたり、その他の方法で渡されたりすると、その暗号文はすぐに拒否される。カウンタを使用していない場合は、再生され得る。いくつかの例では、カードで更新されるカウンタは、トランザクション用に更新されるカウンタとは異なる。いくつかの例では、非接触カードは、トランザクションアプレットであり得る第１のアプレット、および第２のアプレットを備え得る。各アプレットは、カウンタを備え得る。

【０１００】

いくつかの例では、カウンタが非接触カードと１つまたは複数のサーバとの間で同期しなくなり得る。例えば、非接触カードがアクティブ化されて、カウンタが更新され、非接触カードによって新しい通信が生成されても、通信は、１つまたは複数のサーバで処理するために送信され得ない。これにより、非接触カードのカウンタと１つまたは複数のサーバで維持されているカウンタが同期しなくなり得る。これは、例えば、カードがデバイスに隣接して格納されている場合（例えば、デバイスと一緒にポケットに入れて運ばれている場合）や、非接触カードが斜めに読み取られている場合、非接触カードがＮＦＣ範囲の電源が入っているが読み取り可能でないように、カードの位置がずれているか、配置されていない場合など、意図せずに発生し得る。非接触カードがデバイスに隣接して配置されている場合、デバイスのＮＦＣ範囲をオンにして非接触カードに電力を供給し、その中のカウンタを更新できるが、デバイス上のアプリケーションは、通信を受信しない。

【０１０１】

カウンタの同期を維持するために、モバイルデバイスがウェイクアップしたことを検出し、１つまたは複数のサーバと同期して、検出によって読み取りが発生したことを示し、カウンタを前方に移動するように構成された、バックグラウンドアプリケーションなどのアプリケーションを実行できる。非接触カードと１つまたは複数のサーバのカウンタが同期しなくなり得るため、１つまたは複数のサーバは、非接触カードのカウンタが、１つまたは複数のサーバによって読み取られ、依然として有効であると見なされる前に、閾値または所定の回数更新されることを可能にするように構成され得る。例えば、カウンタが非接触カードのアクティブ化を示す発生毎に１ずつインクリメント（またはデクリメント）するように構成されている場合、１つまたは複数のサーバは、非接触カードから読み取った任意のカウンタ値を有効として許可するか、または閾値範囲（例えば、１から１０）内の任意のカウンタ値を許可し得る。さらに、１つまたは複数のサーバは、１０を超えたが、別の閾値範囲値（１０００など）を下回ったカウンタ値を読み取る場合、ユーザタップなどの非接触カードに関連付けられたジェスチャを要求するように構成され得る。ユーザタップから、カウンタ値が目的の範囲または許容範囲内にある場合、認証は、成功する。

【０１０２】

図８は、例示的な実施形態に係る鍵動作８００を示すフローチャートである。図８に示されるように、ブロック８１０で、２つの銀行識別子番号（ＢＩＮ）レベルのマスター鍵を、アカウント識別子およびカードシーケンス番号と組み合わせて使用して、カード毎に２つの一意の派生鍵（ＵＤＫ）を生成できる。いくつかの例では、銀行識別子番号は、１つまたは複数のサーバによって提供される口座番号または予測不可能な番号などの１つの番号または１つまたは複数の番号の組み合わせを備え得、セッション鍵の生成および／または多様化に使用され得る。ＵＤＫ（ＡＵＴＫＥＹおよびＥＮＣＫＥＹ）は、個人化プロ

セス中にカードに格納され得る。

【０１０３】

ブロック８２０で、カウンタは、カード毎に鍵の１つの一意のセットが生成されるマスター鍵導出とは対照的に、使用毎に変化し、毎回異なるセッション鍵を提供するので、多様化データとして使用できる。いくつかの例では、両方の動作に４バイト方式を使用することが望ましい。したがって、ブロック８２０で、２つのセッション鍵が、ＵＤＫからのトランザクション毎に作成され得る。すなわち、ＡＵＴＫＥＹからの１つのセッション鍵と、ＥＮＣＫＥＹからの１つのセッション鍵である。カードでは、ＭＡＣ鍵（すなわち、ＡＵＴＫＥＹから作成されたセッション鍵）の場合、ＯＴＰカウンタの下位２バイトを多様化に使用できる。ＥＮＣ鍵（すなわち、ＥＮＣＫＥＹから作成されたセッション鍵）の場合、ＯＴＰカウンタの全長をＥＮＣ鍵に使用できる。

【０１０４】

ブロック８３０で、ＭＡＣ鍵は、ＭＡＣ暗号文を準備するために使用され得、ＥＮＣ鍵は、暗号文を暗号化するために使用され得る。例えば、ＭＡＣセッション鍵を使用して暗号文を準備し、その結果を１つまたは複数のサーバに送信する前にＥＮＣ鍵で暗号化し得る。

【０１０５】

ブロック８４０で、２バイトの多様化が支払いＨＳＭのＭＡＣ認証機能で直接サポートされるので、ＭＡＣの検証および処理が単純化される。暗号文の復号は、ＭＡＣの検証の前に実行される。セッション鍵は、１つまたは複数のサーバで独立して導出されるため、第１のセッション鍵（ＥＮＣセッション鍵）と第２のセッション鍵（ＭＡＣセッション鍵）が生成される。第２の派生鍵（すなわち、ＥＮＣセッション鍵）を使用してデータを復号でき、第１の派生鍵（すなわち、ＭＡＣセッション鍵）を使用して、復号されたデータを検証できる。

【０１０６】

非接触カードの場合、アプリケーションのプライマリアカウント番号（ＰＡＮ）とカードにエンコードされているＰＡＮシーケンス番号に関連する可能性のある別の一意の識別子が導出される。鍵の多様化は、非接触カード毎に１つまたは複数の鍵を作成できるように、マスター鍵の入力として識別子を受信するように構成できる。いくつかの例では、これらの多様化された鍵は、第１の鍵および第２の鍵を備え得る。第１の鍵には、認証マスター鍵（カード暗号文生成／認証鍵－Ｃａｒｄ－Ｋｅｙ－Ａｕｔｈ）が含まれ得、さらに多様化して、ＭＡＣ暗号文の生成および検証時に使用されるＭＡＣセッション鍵を作成し得る。第２の鍵は、暗号化マスター鍵（カードデータ暗号化鍵－Ｃａｒｄ－Ｋｅｙ－ＤＥＫ）を備え得、さらに多様化されて、暗号化されたデータを暗号化および復号するときに使用されるＥＮＣセッション鍵を作成し得る。いくつかの例では、第１および第２の鍵は、それらをカードの一意のＩＤ番号（ｐＵＩＤ）および支払いアプレットのＰＡＮシーケンス番号（ＰＳＮ）と組み合わせることによって発行者マスター鍵を多様化することによって作成され得る。ｐＵＩＤは、１６桁の数値を備え得る。上で説明したように、ｐＵＩＤは、１６桁のＢＣＤ符号化番号を備え得る。いくつかの例では、ｐＵＩＤは、１４桁の数値を備え得る。

【０１０７】

いくつかの例では、ＥＭＶセッション鍵導出方法が２＾１６の使用でラップし得るため、完全な３２ビットカウンタなどのカウンタを多様化方法の初期化配列に追加できる。

【０１０８】

クレジットカードなどの他の例では、口座番号などの番号、または１つまたは複数のサーバによって提供される予測不可能な番号を、セッション鍵の生成および／または多様化に使用できる。

【０１０９】

図９は、本開示の１つまたは複数の実施形態を実施するように構成されたシステム９００の図を示している。以下で説明するように、非接触カードの作成プロセス中に、２つの

暗号化鍵がカード毎に一意に割り当てられ得る。暗号化鍵は、データの暗号化と復号の両方で使用できる対称鍵を備え得る。Ｔｒｉｐｌｅ　ＤＥＳ（３ＤＥＳ）アルゴリズムは、ＥＭＶで使用でき、非接触カードのハードウェアによって実施される。鍵多様化プロセスを使用することにより、鍵を必要とする各エンティティの一意に識別可能な情報に基づいて、マスター鍵から１つまたは複数の鍵を導出し得る。

【０１１０】

マスター鍵管理に関しては、２つの発行者マスター鍵９０５、９１０が、１つまたは複数のアプレットが発行されるポートフォリオの各部分に対して必要とされ得る。例えば、第１のマスター鍵９０５は、発行者暗号文生成／認証鍵（Ｉｓｓ－Ｋｅｙ－Ａｕｔｈ）を備え得、第２のマスター鍵９１０は、発行者データ暗号化鍵（Ｉｓｓ－Ｋｅｙ－ＤＥＫ）を備え得る。本明細書でさらに説明されるように、２つの発行者マスター鍵９０５、９１０は、カード毎に一意であるカードマスター鍵９２５、９３０に多様化されている。いくつかの例では、バックオフィスデータとしてのネットワークプロファイルレコードＩＤ（ｐＮＰＲ）９１５および導出鍵インデックス（ｐＤＫＩ）９２０を使用して、認証のための暗号化プロセスで使用する発行者マスター鍵９０５、９１０を識別できる。認証を実行するシステムは、認証時に非接触カードのｐＮＰＲ９１５およびｐＤＫＩ９２０の値を検索するように構成できる。

【０１１１】

いくつかの例では、ソリューションのセキュリティを強化するために、セッション鍵（セッションごとの一意の鍵など）を取得できるが、上で説明したように、マスター鍵を使用する代わりに、カードから派生した一意の鍵とカウンタを多様化データとして使用できる。例えば、カードが動作中に使用されるたびに、メッセージ認証コード（ＭＡＣ）の作成と暗号化の実行に異なる鍵が使用され得る。セッション鍵の生成に関して、暗号文を生成し、１つまたは複数のアプレット内のデータを暗号化するために使用される鍵は、カードの一意の鍵（Ｃａｒｄ－Ｋｅｙ－Ａｕｔｈ９２５およびＣａｒｄ－Ｋｅｙ－Ｄｅｋ９３０）に基づくセッション鍵を備え得る。セッション鍵（Ａｕｔ－Ｓｅｓｓｉｏｎ－Ｋｅｙ９３５およびＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙ９４０）は、１つまたは複数のアプレットによって生成され、１つまたは複数のアルゴリズムでアプリケーショントランザクションカウンタ（ｐＡＴＣ）９４５を使用して導出される。データを１つまたは複数のアルゴリズムに適合させるために、４バイトのｐＡＴＣ９４５の下位２バイトのみが使用される。いくつかの例では、４バイトのセッション鍵導出方法は、：Ｆ１：＝ＰＡＴＣ（下位２バイト）｜｜’Ｆ０’｜｜’００’｜｜ＰＡＴＣ（４バイト）Ｆ１：＝ＰＡＴＣ（下位２バイト）｜｜’０Ｆ’｜｜’００’｜｜ＰＡＴＣ（４バイト）ＳＫ：＝｛（ＡＬＧ（ＭＫ）［Ｆ１］）｜｜ＡＬＧ（ＭＫ）［Ｆ２］｝、ここで、ＡＬＧには３ＤＥＳ　ＥＣＢが含まれ、ＭＫにはカード一意の派生マスター鍵が含まれ得る、を備え得る。

【０１１２】

本明細書で説明するように、１つまたは複数のＭＡＣセッション鍵は、ｐＡＴＣ９４５カウンタの下位２バイトを使用して導出できる。非接触カードをタップするたびに、ｐＡＴＣ９４５が更新されるように構成され、カードマスター鍵Ｃａｒｄ－Ｋｅｙ－ＡＵＴＨ９２５およびＣａｒｄ－Ｋｅｙ－ＤＥＫ９３０は、セッション鍵Ａｕｔ－Ｓｅｓｓｉｏｎ－Ｋｅｙ９３５およびＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙ９４０にさらに多様化される。ｐＡＴＣ９４５は、個人化時またはアプレットの初期化時にゼロに初期化できる。いくつかの例では、ｐＡＴＣカウンタ９４５は、個人化時または個人化の前に初期化され得、各ＮＤＥＦ読み取りで１ずつインクリメントするように構成され得る。

【０１１３】

さらに、各カードの更新は一意であり、個人化によって割り当てられるか、ｐＵＩＤまたはその他の識別情報によってアルゴリズムによって割り当てられる。例えば、奇数番号のカードは２ずつインクリメントまたはデクリメントでき、偶数番号のカードは５ずつインクリメントまたはデクリメントできる。いくつかの例では、更新は、シーケンシャルリードでも異なり得、１枚のカードが１、３、５、２、２、…の繰り返しで順番にインクリ

メントし得る。特定のシーケンスまたはアルゴリズムシーケンスは、個人化時に、または一意の識別子から派生した１つまたは複数のプロセスから定義され得る。これにより、リプレイ攻撃者が少数のカードインスタンスから一般化するのが難しくなり得る。

【０１１４】

認証メッセージは、１６進ＡＳＣＩＩ形式のテキストＮＤＥＦレコードのコンテンツとして配信され得る。いくつかの例では、認証データと、認証データのＭＡＣが後に続く８バイトの乱数のみが含まれ得る。いくつかの例では、乱数は暗号文Ａの前にあり、１ブロックの長さであり得る。他の例では、乱数の長さに制限があり得ない。さらなる例では、合計データ（すなわち、乱数と暗号文）は、ブロックサイズの倍数であり得る。これらの例では、ＭＡＣアルゴリズムによって生成されたブロックに一致するように、さらに８バイトのブロックを追加し得る。他の例として、採用されたアルゴリズムが１６バイトのブロックを使用した場合、そのブロックサイズの倍数を使用するか、出力をそのブロックサイズの倍数に自動的または手動でパディングし得る。

【０１１５】

ＭＡＣは、ファンクション鍵（ＡＵＴ－Ｓｅｓｓｉｏｎ－Ｋｅｙ）９３５によって実行され得る。暗号文で指定されたデータは、ｊａｖａｃａｒｄ．ｓｉｇｎａｔｕｒｅ方法：ＡＬＧ＿ＤＥＳ＿ＭＡＣ８＿ＩＳＯ９７９７＿１＿Ｍ２＿ＡＬＧ３で処理して、ＥＭＶＡＲＱＣ検証方法に関連付けることができる。この計算に使用される鍵は、上で説明したように、セッション鍵ＡＵＴ－Ｓｅｓｓｉｏｎ－Ｋｅｙ９３５を備え得る。上で説明したように、カウンタの下位２バイトを使用して、１つまたは複数のＭＡＣセッション鍵を多様化できる。以下で説明するように、ＡＵＴ－Ｓｅｓｓｉｏｎ－Ｋｅｙ９３５は、ＭＡＣデータ９５０に使用され得、結果として得られるデータまたは暗号文Ａ９５５および乱数ＲＮＤは、ＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙ９４０を使用して暗号化され、メッセージで送信される暗号文Ｂまたは出力９６０を作成できる。

【０１１６】

いくつかの例では、最後の１６（バイナリ、３２ｈｅｘ）バイトが乱数のゼロＩＶとそれに続くＭＡＣ認証データを伴うＣＢＣモードを使用する３ＤＥＳ対称暗号化を備えるように、１つまたは複数のＨＳＭコマンドが復号のために処理され得る。この暗号化に使用される鍵は、Ｃａｒｄ－Ｋｅｙ－ＤＥＫ９３０から派生したセッション鍵ＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙ９４０を備え得る。この場合、セッション鍵導出のＡＴＣ値は、カウンタｐＡＴＣ９４５の最下位バイトである。

【０１１７】

以下のフォーマットは、バイナリバージョンの例示的な実施形態を表す。さらに、いくつかの例では、第１のバイトはＡＳＣＩＩ「Ａ」に設定され得る。

【表２】

メッセージフォーマット				
１	２	４	８	８
０ｘ４３（メッセージタイプ「A」）	バージョン	ｐＡＴＣ	ＲＮＤ	暗号文A（ＭＡＣ）

暗号文A（ＭＡＣ）	８バイト
ＭＡＣ	

２	８	４	４	１８バイト入力データ
バージョン	ｐＵＩＤ	ｐＡＴＣ	共有秘密	

メッセージフォーマット			
１	２	４	１６
０ｘ４３（メッセージタイプ「A」）	バージョン	ｐＡＴＣ	暗号文B

暗号文A（ＭＡＣ）	８バイト
ＭＡＣ	

２	８	４	４	１８バイト入力データ
バージョン	ｐＵＩＤ	ｐＡＴＣ	共有秘密	

暗号文B	１６	
Ｓｙｍ暗号化		
８	８	
ＲＮＤ	暗号文A	

【０１１８】

他の例示的なフォーマットを以下に示す。この例では、タグは、１６進形式でエンコードできる。

【表３】

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

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

【０１１９】

受信されたメッセージのＵＩＤフィールドを抽出して、マスター鍵Ｉｓｓ－Ｋｅｙ－ＡＵＴＨ９０５およびＩｓｓ－Ｋｅｙ－ＤＥＫ９１０から、その特定のカードのカードマスター鍵（Ｃａｒｄ－Ｋｅｙ－Ａｕｔｈ９２５およびＣａｒｄ－Ｋｅｙ－ＤＥＫ９３０）を導出できる。カードマスター鍵（Ｃａｒｄ－Ｋｅｙ－Ａｕｔｈ９２５およびＣａｒｄ－Ｋｅｙ－ＤＥＫ９３０）を使用して、受信されたメッセージのカウンタ（ｐＡＴＣ）フィールドを使用して、その特定のカードのセッション鍵（Ａｕｔ－Ｓｅｓｓｉｏｎ－Ｋｅｙ９３５およびＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙ９４０）を導出できる。暗号文Ｂ９６０は、ＤＥＫ－Ｓｅｓｓｉｏｎ－ＫＥＹを使用して復号できる。これにより、暗号文Ａ９５５とＲＮＤが生成され、ＲＮＤは、破棄され得る。ＵＩＤフィールドは、非接触カードの共有秘密を検索するために使用できる。これは、メッセージのＶｅｒ、ＵＩＤ、およびｐＡＴＣフィールドとともに、再作成されたＡｕｔ－Ｓｅｓｓｉｏｎ－Ｋｅｙを使用して暗号化ＭＡＣを介して処理され、ＭＡＣ’などのＭＡＣ出力を作成できる。ＭＡＣ’が暗号文Ａ９５５と同じである場合、これは、メッセージの復号とＭＡＣチェックが全て合格したことを示す。次に、ｐＡＴＣを読み取って、それが有効かどうかを判断する。

【０１２０】

認証セッション中に、１つまたは複数の暗号文が１つまたは複数のアプリケーションによって生成され得る。例えば、１つまたは複数の暗号文は、ＩＳＯ９７９７－１アルゴリズム３とＡｕｔ－Ｓｅｓｓｉｏｎ－Ｋｅｙ９３５などの１つまたは複数のセッション鍵を介した方法２のパディングを使用して３ＤＥＳ　ＭＡＣとして生成できる。入力データ９

５０は、次の形式：バージョン（２）、ｐＵＩＤ（８）、ｐＡＴＣ（４）、共有秘密（４）をとることができる。いくつかの例では、括弧内の数字はバイト単位の長さを備え得る。いくつかの例では、共有秘密は、１つまたは複数の安全なプロセスを通じて、乱数が予測できないことを保証するように構成され得る１つまたは複数の乱数発生器によって生成され得る。いくつかの例では、共有秘密は、認証サービスによって知られている、個人化時にカードに注入されるランダムな４バイトの２進数を備え得る。認証セッション中に、共有秘密が１つまたは複数のアプレットからモバイルアプリケーションに提供され得ない。方法２のパディングには、入力データの最後に必須の０ｘ’８０’バイトを追加することと、８バイト境界までの結果データの最後に追加できる０ｘ’００’バイトを追加することが含まれ得る。結果として得られる暗号文は、８バイトの長さで構成され得る。

【０１２１】

いくつかの例では、ＭＡＣ暗号文を使用して第１のブロックとして非共有乱数を暗号化する利点の１つは、対称暗号化アルゴリズムのＣＢＣ（ブロックチェーン）モードを使用しながら、初期化ベクトルとして機能することである。これにより、固定または動的ＩＶを事前に確立しなくても、ブロック間で「スクランブル」を行うことができる。

【０１２２】

ＭＡＣ暗号文に含まれるデータの一部としてアプリケーショントランザクションカウンタ（ｐＡＴＣ）を含めることにより、認証サービスは、クリアデータで伝達される値が改ざんされているかどうかを判断するように構成できる。さらに、１つまたは複数の暗号文にバージョンを含めることにより、攻撃者が暗号化ソリューションの強度を低下させようとして、アプリケーションのバージョンを故意に偽って伝えることは困難である。いくつかの例では、ｐＡＴＣはゼロから始まり、１つまたは複数のアプリケーションが認証データを生成するたびに１ずつ更新され得る。認証サービスは、認証セッション中に使用されるｐＡＴＣを追跡するように構成できる。いくつかの例では、認証データが認証サービスによって受信された以前の値以下のｐＡＴＣを使用する場合、これは、古いメッセージを再生しようとする試みとして解釈され、認証されたものは拒否され得る。いくつかの例では、ｐＡＴＣが以前に受信した値よりも大きい場合、これを評価して許容範囲または閾値内にあるかどうかを判断し、範囲または閾値を超えているか範囲外にある場合、検証は失敗したか、信頼できないと見なされ得る。ＭＡＣ動作９３６では、データ９５０は、暗号化されたＭＡＣ出力（暗号文Ａ）９５５を生成するために、Ａｕｔ－Ｓｅｓｓｉｏｎ－Ｋｅｙ９３５を使用してＭＡＣを介して処理される。

【０１２３】

カード上の鍵を公開する総当たり（ブルートフォース）攻撃に対する追加の保護を提供するために、ＭＡＣ暗号文Ａ９５５が暗号化されることが望ましい。いくつかの例では、暗号化テキストに含まれるデータまたは暗号文Ａ９５５は、乱数（８）、暗号文（８）を備え得る。いくつかの例では、括弧内の数字はバイト単位の長さを備え得る。いくつかの例では、乱数は、１つまたは複数の安全なプロセスを通じて、乱数が予測不可能であることを保証するように構成され得る１つまたは複数の乱数発生器によって生成され得る。このデータを暗号化するために使用される鍵は、セッション鍵を備え得る。例えば、セッション鍵は、ＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙ９４０を備え得る。暗号化動作９４１において、データまたは暗号文Ａ９５５およびＲＮＤは、ＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙ９４０を使用して処理されて、暗号化されたデータ、暗号文Ｂ９６０を生成する。データ９５５は、暗号ブロックチェーンモードで３ＤＥＳを使用して暗号化され、攻撃者が全ての暗号化テキストに対して攻撃を実行する必要があることを確認できる。非限定的な例として、高度暗号化標準（ＡＥＳ）などの他のアルゴリズムを使用できる。いくつかの例では、０ｘ’０００００００００００００００’の初期化ベクトルを使用できる。正しく復号されたデータは、ランダムに表示されるため、誤って復号されたデータと区別がつかないため、このデータの暗号化に使用される鍵を総当たりで見つけようとする攻撃者は、正しい鍵がいつ使用されたかを判断できなくなる。

【０１２４】

認証サービスが１つまたは複数のアプレットによって提供される１つまたは複数の暗号文を検証するには、認証セッション中に次のデータを１つまたは複数のアプレットからモバイルデバイスに平文で伝達する必要がある：使用される暗号化アプローチを判断するためのバージョン番号と暗号化の検証のためのメッセージフォーマット、これにより、アプローチを将来変更できる；暗号資産を検索し、カード鍵を導出するためのｐＵＩＤ；暗号文に使用されるセッション鍵を導出するためのｐＡＴＣ。

【０１２５】

図１０は、暗号文を生成するための方法１０００を示している。例えば、ブロック１０１０で、ネットワークプロファイルレコードＩＤ（ｐＮＰＲ）および導出鍵インデックス（ｐＤＫＩ）を使用して、認証のための暗号化プロセスで使用する発行者マスター鍵を識別できる。いくつかの例では、この方法は、認証を実行して、認証時に非接触カードのｐＮＰＲおよびｐＤＫＩの値を検索することを含み得る。

【０１２６】

ブロック１０２０で、発行者マスター鍵は、それらをカードの一意のＩＤ番号（ｐＵＩＤ）および１つまたは複数のアプレット、例えば、支払いアプレットのＰＡＮシーケンス番号（ＰＳＮ）と組み合わせることによって多様化できる。

【０１２７】

ブロック１０３０で、Ｃａｒｄ－Ｋｅｙ－ＡｕｔｈおよびＣａｒｄ－Ｋｅｙ－ＤＥＫ（一意のカード鍵）は、発行者マスター鍵を多様化して、ＭＡＣ暗号文を生成するために使用され得るセッション鍵を生成することによって作成され得る。

【０１２８】

ブロック１０４０で、暗号文を生成し、１つまたは複数のアプレット内のデータを暗号化するために使用される鍵は、カード一意の鍵（Ｃａｒｄ－Ｋｅｙ－ＡｕｔｈおよびＣａｒｄ－Ｋｅｙ－ＤＥＫ）に基づくブロック１０３０のセッション鍵を備え得る。いくつかの例では、これらのセッション鍵は、１つまたは複数のアプレットによって生成され、ｐＡＴＣを使用して導出され、セッション鍵Ａｕｔ－Ｓｅｓｓｉｏｎ－ＫｅｙおよびＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙになる。

【０１２９】

図１１は、一例に係る鍵の多様化を示す例示的なプロセス１１００を示している。最初に、送信者と受信者に２つの異なるマスター鍵をプロビジョニングし得る。例えば、第１のマスター鍵は、データ暗号化マスター鍵を備え得、第２のマスター鍵は、データ完全性マスター鍵を備え得る。送信者は、ブロック１１１０で更新され得るカウンタ値、およびそれが受信者との共有を保証し得る保護されるべきデータなどの他のデータを有する。

【０１３０】

ブロック１１２０で、カウンタ値は、データ暗号化マスター鍵を使用して送信者によって暗号化されてデータ暗号化派生セッション鍵を生成し得、カウンタ値はまた、データ完全性マスター鍵を使用して送信者によって暗号化されてデータ完全性派生セッション鍵を生成し得る。いくつかの例では、カウンタ値全体またはカウンタ値の一部が両方の暗号化中に使用され得る。

【０１３１】

いくつかの例では、カウンタ値は、暗号化されない場合がある。これらの例では、カウンタは、送信者と受信者の間で平文で、すなわち、暗号化なしで送信できる。

【０１３２】

ブロック１１３０で、保護されるべきデータは、データ完全性セッション鍵および暗号化ＭＡＣアルゴリズムを使用して、送信者による暗号化ＭＡＣ動作で処理される。プレーンテキストと共有秘密を含む保護されたデータを使用して、セッション鍵（ＡＵＴ－Ｓｅｓｓｉｏｎ－Ｋｅｙ）の１つを使用してＭＡＣを生成できる。

【０１３３】

ブロック１１４０で、保護されるべきデータは、対称暗号化アルゴリズムと組み合わせてデータ暗号化派生セッション鍵を使用して送信者によって暗号化され得る。いくつかの

例では、ＭＡＣは、例えば、各８バイトの長さの等量のランダムデータと組み合わされ、第２のセッション鍵（ＤＥＫ－Ｓｅｓｓｉｏｎ－Ｋｅｙ）を使用して暗号化される。

【０１３４】

ブロック１１５０で、暗号化されたＭＡＣは、暗号文の検証のために、追加の秘密情報（共有秘密、マスター鍵など）を識別するのに十分な情報とともに、送信者から受信者に送信される。

【０１３５】

ブロック１１６０で、受信者は、受信したカウンタ値を使用して、上で説明したように、２つのマスター鍵から２つの派生セッション鍵を独立して導出する。

【０１３６】

ブロック１１７０において、データ暗号化派生セッション鍵は、保護されたデータを復号するために対称復号動作と組み合わせて使用される。その後、交換されたデータに対して追加の処理が行われる。いくつかの例では、ＭＡＣが抽出された後、ＭＡＣを再現して一致させることが望ましい。例えば、暗号文を検証するときに、適切に生成されたセッション鍵を使用して復号できる。保護されたデータは、検証のために再構築され得る。適切に生成されたセッション鍵を使用してＭＡＣ動作を実行し、復号されたＭＡＣと一致するかどうかを判断できる。ＭＡＣ動作は、不可逆プロセスであるため、検証する唯一の方法は、ソースデータから再作成を試みることである。

【０１３７】

ブロック１１８０で、データ完全性派生セッション鍵は、保護されたデータが変更されていないことを検証するために、暗号化ＭＡＣ動作と組み合わせて使用される。

【０１３８】

本明細書に記載の方法のいくつかの例は、以下の条件が満たされたときに成功した認証がいつ判断されるかを有利に確認できる。まず、ＭＡＣを検証する機能は、派生セッション鍵が適切であることを示している。ＭＡＣは、復号が成功し、適切なＭＡＣ値が得られた場合にのみ正しくなり得る。復号が成功した場合は、正しく導出された暗号化鍵が暗号化されたＭＡＣの復号に使用されたことを示し得る。派生セッション鍵は、送信者（例えば、送信デバイス）と受信者（例えば、受信デバイス）だけが知っているマスター鍵を使用して作成されるため、最初にＭＡＣを作成してＭＡＣを暗号化した非接触カードが実際に本物であると信頼し得る。さらに、第１および第２のセッション鍵を導出するために使用されるカウンタ値は、有効であることが示され得、認証動作を実行するために使用され得る。

【０１３９】

その後、２つの派生セッション鍵は破棄され得、データ交換の次の反復は、カウンタ値を更新し（ブロック１１１０に戻る）、セッション鍵の新しいセットが作成され得る（ブロック１１２０で）。いくつかの例では、組み合わされたランダムデータは破棄され得る。

【０１４０】

本明細書に記載のシステムおよび方法の例示的な実施形態は、セキュリティ要素認証を提供するように構成され得る。セキュリティ要素認証は、複数のプロセスを備え得る。セキュリティ要素認証の一部として、第１のプロセスは、ログインし、デバイス上で実行されている１つまたは複数のアプリケーションを介してユーザを検証することを備え得る。第２のプロセスとして、ユーザは、ログインの成功および１つまたは複数のアプリケーションを介した第１のプロセスの検証に応答して、１つまたは複数の非接触カードに関連する１つまたは複数の行動に従事できる。事実上、セキュリティ要素認証には、ユーザの身元を安全に証明することと、非接触カードに関連付けられた１つまたは複数のタップジェスチャを含むがこれに限定されない１つまたは複数のタイプの行動に従事することの両方が含まれ得る。いくつかの例では、１つまたは複数のタップジェスチャは、ユーザによるデバイスへの非接触カードのタップを備え得る。いくつかの例では、デバイスは、モバイルデバイス、キオスク、端末、タブレット、または受信したタップジェスチャを処理するように構成された任意の他のデバイスを備え得る。

【０１４１】
いくつかの例では、非接触カードを１つまたは複数のコンピュータキオスクまたは端末などのデバイスにタップして、コーヒーなどの購入に応答するトランザクションアイテムを受信するために本人確認を行うことができる。非接触カードを使用することにより、ロイヤルティプログラムでＩＤを証明する安全な方法を確立できる。例えば、報酬、クーポン、オファーなどを取得したり、特典を受け取ったりするためにＩＤを安全に証明することは、単にバーカードをスキャンするのとは異なる方法で確立される。例えば、非接触カードとデバイスとの間で暗号化されたトランザクションが発生し得る。これは、１つまたは複数のタップジェスチャを処理するように構成され得る。上で説明したように、１つまたは複数のアプリケーションは、ユーザのＩＤを検証し、次に、例えば、１つまたは複数のタップジェスチャを介して、ユーザにそれに行動または応答させるように構成され得る。いくつかの例では、例えば、ボーナスポイント、ロイヤルティポイント、報酬ポイント、ヘルスケア情報などのデータが、非接触カードに書き戻され得る。
【０１４２】
いくつかの例では、非接触カードは、モバイルデバイスなどのデバイスにタップされ得る。上で説明したように、ユーザのＩＤは、１つまたは複数のアプリケーションによって検証され得、次いで、それは、ＩＤの検証に基づいて、ユーザに所望の利益を与えるであろう。
【０１４３】
いくつかの例では、非接触カードは、モバイルデバイスなどのデバイスをタップすることによってアクティブ化され得る。例えば、非接触カードは、ＮＦＣ通信を介してデバイスのカードリーダを介してデバイスのアプリケーションと通信できる。カードのタップがデバイスのカードリーダに近接している通信では、デバイスのアプリケーションが非接触カードに関連付けられたデータを読み取り、カードをアクティブ化し得る。いくつかの例では、アクティブ化は、カードが他の機能、例えば、購入、アカウントまたは制限された情報へのアクセス、または他の機能を実行するために使用されることを許可し得る。いくつかの例では、タップは、デバイスのアプリケーションをアクティブ化または起動し、次に、１つまたは複数のアクションまたは１つまたは複数のサーバとの通信を開始して、非接触カードをアクティブ化できる。アプリケーションがデバイスにインストールされていない場合、カードリーダの近くにある非接触カードをタップすると、アプリケーションのダウンロードページへのナビゲーションなど、アプリケーションのダウンロードが開始され得る。インストールに続いて、非接触カードをタップすると、アプリケーションがアクティブ化または起動され、その後、例えば、アプリケーションまたは他のバックエンド通信を介して、非接触カードのアクティブ化が開始される。アクティブ化の後、非接触カードは、商取引を含むがこれに限定されない様々な活動で使用され得る。
【０１４４】
いくつかの実施形態では、非接触カードのアクティブ化を実行するためにクライアントデバイス上で実行するように専用のアプリケーションを構成し得る。他の実施形態では、ウェブポータル、ウェブベースのアプリ、アプレットなどがアクティブ化を実行できる。アクティブ化は、クライアントデバイスで実行することも、クライアントデバイスが非接触カードと外部デバイス（例えば、アカウントサーバ）の仲介役として機能することもある。いくつかの実施形態によれば、アクティブ化を提供する際に、アプリケーションは、アカウントサーバに、アクティブ化を実行するデバイスのタイプ（例えば、パーソナルコンピュータ、スマートフォン、タブレット、または販売時点情報管理（ＰＯＳ）デバイス）を示し得る。さらに、アプリケーションは、送信のために、関係するデバイスのタイプに応じて、異なるデータおよび／または追加のデータをアカウントサーバに出力し得る。例えば、そのようなデータは、マーチャントタイプ、マーチャントＩＤなどのマーチャントに関連する情報、およびＰＯＳデータおよびＰＯＳ　ＩＤなどのデバイスタイプ自体に関連する情報を備え得る。
【０１４５】

いくつかの実施形態では、例示的な認証通信プロトコルは、いくつかの変更を加えて、トランザクションカードと販売時点情報管理デバイスとの間で一般的に実行されるＥＭＶ標準のオフライン動的データ認証プロトコルを模倣できる。例えば、認証プロトコルの例は、カード発行者／支払い処理業者自体との支払いトランザクションを完了するために使用されないため、一部のデータ値は不要であり、カード発行者／支払い処理業者へのリアルタイムのオンライン接続を必要とせずに認証を実行し得る。当技術分野で知られているように、販売時点情報管理（ＰＯＳ）システムは、取引額を含むトランザクションをカード発行者に提出する。発行者がトランザクションを承認するか拒否するかは、カード発行者が取引額を認識しているかどうかに基づき得る。一方、本開示の特定の実施形態では、モバイルデバイスから発生するトランザクションは、ＰＯＳシステムに関連する取引額を欠いている。したがって、いくつかの実施形態では、ダミーの取引額（すなわち、カード発行者が認識可能であり、アクティブ化が発生するのに十分な値）を、例示的な認証通信プロトコルの一部として渡し得る。ＰＯＳベースのトランザクションは、トランザクションの試行回数に基づいてトランザクションを拒否する場合もある（例えば、トランザクションカウンタ）。バッファ値を超えて何度も試行すると、緩やかに減少し得る。緩やかな減少は、トランザクションを受け入れる前にさらなる検証を必要とする。いくつかの実施では、正当なトランザクションの減少を回避するために、トランザクションカウンタのバッファ値が変更され得る。

【０１４６】

いくつかの例では、非接触カードは、受信者のデバイスに応じて情報を選択的に通信できる。非接触カードは、タップされると、タップの対象となるデバイスを認識でき、この認識に基づいて、非接触カードは、そのデバイスに適切なデータを提供できる。これは、非接触カードが、支払いまたはカード認証などの即時のアクションまたはトランザクションを完了するために必要な情報のみを送信することを有利にする。データの送信を制限し、不要なデータの送信を回避することで、効率とデータセキュリティの両方を向上させることができる。情報の認識と選択的な通信は、カードのアクティブ化、残高の転送、アカウントアクセスの試行、商取引、ステップアップ詐欺の削減など、様々なシナリオに適用できる。

【０１４７】

非接触カードタップが、例えば、ｉＰｈｏｎｅ（登録商標）、ｉＰｏｄ（登録商標）、ｉＰａｄ（登録商標）などＡｐｐｌｅのｉＯＳ（登録商標）オペレーティングシステムを実行しているデバイスに向けられている場合、非接触カードはｉＯＳ（登録商標）オペレーティングシステムを認識し、このデバイスと通信するための適切なデータを送信できる。例えば、非接触カードは、例えばＮＦＣを介してＮＤＥＦタグを使用してカードを認証するために必要な暗号化されたＩＤ情報を提供できる。同様に、非接触カードのタップが、例えば、Ａｎｄｒｏｉｄ（登録商標）スマートフォンやタブレットなどＡｎｄｒｏｉｄ（登録商標）オペレーティングシステムを実行しているデバイスに向けられている場合、非接触カードは、Ａｎｄｒｏｉｄ（登録商標）オペレーティングシステムを認識し、このデバイスと通信するための適切なデータを送信できる（本明細書に記載の方法による認証に必要な暗号化されたＩＤ情報など）。

【０１４８】

他の例として、非接触カードタップは、キオスク、チェックアウトレジスタ、支払いステーション、または他の端末を含むがこれらに限定されないＰＯＳデバイスに向けることができる。タップを実行すると、非接触カードは、ＰＯＳデバイスを認識し、アクションまたはトランザクションに必要な情報のみを送信できる。例えば、商取引を完了するために使用されるＰＯＳデバイスを認識すると、非接触カードは、ＥＭＶ標準の下でトランザクションを完了するために必要な支払い情報を伝達できる。

【０１４９】

いくつかの例では、トランザクションに参加するＰＯＳデバイスは、非接触カードによって提供される追加情報、例えば、デバイス固有の情報、位置固有の情報、およびトラン

ザクション固有の情報を要求または指定できる。例えば、ＰＯＳデバイスが非接触カードからデータ通信を受信すると、ＰＯＳデバイスは、非接触カードを認識し、アクションまたはトランザクションを完了するために必要な追加情報を要求できる。

【０１５０】

いくつかの例では、ＰＯＳデバイスは、特定の非接触カードに精通している、または特定の非接触カード取引の実行に慣れている認定販売者または他のエンティティと提携できる。しかしながら、そのような提携は、記載された方法の実行のために必要とされないことが理解される。

【０１５１】

ショッピングストア、食料品店、コンビニエンスストアなどのいくつかの例では、非接触カードは、アプリケーションを開かなくてもモバイルデバイスにタップされて、１つまたは複数の購入をカバーするために１つまたは複数の報酬ポイント、ロイヤルティポイント、クーポン、オファーなどを利用したいという願望または意図を示すことができる。したがって、購入の背後にある意図が提供される。

【０１５２】

いくつかの例では、１つまたは複数のアプリケーションは、非接触カードの１つまたは複数のタップジェスチャを介して起動されたことを判断するように構成され得、その結果、ユーザのＩＤを検証するために、午後３時５１分に起動し、午後３時５６分にトランザクションが処理または実行された。

【０１５３】

いくつかの例では、１つまたは複数のアプリケーションは、１つまたは複数のタップジェスチャに応答する１つまたは複数のアクションを制御するように構成され得る。例えば、１つまたは複数のアクションは、報酬の収集、ポイントの収集、最も重要な購入の決定、最も費用のかからない購入の決定、および／またはリアルタイムで他のアクションへの再構成を備え得る。

【０１５４】

いくつかの例では、データは、生体認証／ジェスチャ認証としてタップ行動について収集され得る。例えば、暗号的に安全で傍受されにくい一意の識別子が１つまたは複数のバックエンドサービスに送信され得る。一意の識別子は、個人に関する二次情報を検索するように構成できる。二次情報は、ユーザに関する個人を特定できる情報を備え得る。いくつかの例では、二次情報は、非接触カード内に格納され得る。

【０１５５】

いくつかの例では、デバイスは、請求書を分割するか、または複数の個人の間で支払いをチェックするアプリケーションを含み得る。例えば、各個人が非接触カードを所有し、同じ発行金融機関の顧客であり得るが、必須ではない。これらの各個人は、購入を分割するために、アプリケーションを介してデバイス上でプッシュ通知を受信し得る。支払いを示すためにカードタップを１回だけ受け入れるのではなく、他の非接触カードを使用し得る。いくつかの例では、異なる金融機関を有する個人は、カードをタップする個人から１つまたは複数の支払い要求を開始するための情報を提供するための非接触カードを所有し得る。

【０１５６】

以下の使用例の例は、本開示の特定の実施の例を説明している。これらは説明のみを目的としており、限定を目的としたものではない。あるケースでは、第１の友人（支払人）が第２の友人（受取人）に金額を支払う義務がある。支払人は、ＡＴＭにアクセスしたり、ピアツーピアアプリケーションを介して交換を要求したりするのではなく、非接触カードを使用して受取人のスマートフォン（またはその他のデバイス）を介して支払いを行う。受取人は、スマートフォンで適切なアプリケーションにログオンし、支払い要求オプションを選択する。それに応じて、アプリケーションは、受取人の非接触カードを介して認証を要求する。例えば、アプリケーションは、受取人が非接触カードをタップするように要求する表示を出力する。アプリケーションが有効になっている状態で、受取人がスマー

トフォンの画面に対して非接触カードをタップすると、非接触カードが読み取られて検証される。次に、アプリケーションは、支払人が非接触カードをタップして支払いを送信するように求めるプロンプトを表示する。支払人が非接触カードをタップすると、アプリケーションは、カード情報を読み取り、関連するプロセッサを介して、支払人のカード発行会社に支払い要求を送信する。カード発行会社は、トランザクションを処理し、トランザクションのステータスインジケータをスマートフォンに送信する。次に、アプリケーションは、トランザクションのステータスインジケータを表示するために出力する。

【０１５７】

他の例では、クレジットカードの顧客は、新しいクレジットカード（またはデビットカード、他の支払いカード、またはアクティブ化が必要な他のカード）をメールで受け取り得る。カード発行会社に関連付けられた提供された電話番号に電話したり、Ｗｅｂサイトにアクセスしたりしてカードをアクティブ化するのではなく、顧客は、自分のデバイス（例えば、スマートフォンなどのモバイルデバイス）のアプリケーションを介してカードをアクティブ化することを決定できる。顧客は、デバイスのディスプレイに表示されるアプリケーションのメニューからカードアクティブ化機能を選択できる。アプリケーションは、画面に対してクレジットカードをタップするように顧客に促し得る。デバイスの画面に対してクレジットカードをタップすると、アプリケーションは、顧客のカードをアクティブ化するカード発行サーバなどのサーバと通信するように構成できる。次に、アプリケーションは、カードのアクティブ化が成功したことを示すメッセージを表示し得る。これでカードのアクティブ化が完了する。

【０１５８】

図１２は、例示的な実施形態に係るカードアクティブ化のための方法１２００を示している。例えば、カードのアクティブ化は、カード、デバイス、および１つまたは複数のサーバを含むシステムによって完了できる。非接触カード、デバイス、および１つまたは複数のサーバは、非接触カード１０５、クライアントデバイス１１０、サーバ１２０など、図１Ａ、図１Ｂ、図５Ａ、および図５Ｂを参照して前述したものと同じまたは類似のコンポーネントを参照できる。

【０１５９】

ブロック１２１０で、カードは、データを動的に生成するように構成され得る。いくつかの例では、このデータは、アカウント番号、カード識別子、カード検証値、または電話番号などの情報を含み得、これらは、カードからデバイスに送信され得る。いくつかの例では、データの１つまたは複数の部分は、本明細書に開示されるシステムおよび方法を介して暗号化され得る。

【０１６０】

ブロック１２２０で、動的に生成されたデータの１つまたは複数の部分は、ＮＦＣまたは他の無線通信を介してデバイスのアプリケーションに通信され得る。例えば、デバイスに近接するカードのタップは、デバイスのアプリケーションが非接触カードに関連するデータの１つまたは複数の部分を読み取ることを可能にし得る。いくつかの例では、デバイスがカードのアクティブ化を支援するアプリケーションを備えない場合、カードのタップは、デバイスを指示するか、またはカードをアクティブ化するための関連アプリケーションをダウンロードするように顧客にソフトウェアアプリケーションストアに促され得る。いくつかの例では、ユーザは、カードをデバイスの表面に向けて、デバイスの表面に斜めに、または平らに、近くに、または近接して配置するなど、十分にジェスチャ、配置、または方向付けるように促され得る。カードの十分なジェスチャ、配置、および／または向きに応答して、デバイスは、カードから受信したデータの１つまたは複数の暗号化された部分を１つまたは複数のサーバに送信し始め得る。

【０１６１】

ブロック１２３０で、データの１つまたは複数の部分は、カード発行者サーバなどの１つまたは複数のサーバに通信され得る。例えば、データの１つまたは複数の暗号化された部分は、カードのアクティブ化のためにデバイスからカード発行サーバに送信され得る。

【０１６２】
ブロック１２４０で、１つまたは複数のサーバは、本明細書に開示されるシステムおよび方法を介して、データの１つまたは複数の暗号化された部分を復号し得る。例えば、１つまたは複数のサーバは、デバイスから暗号化されたデータを受信し、受信したデータを比較して１つまたは複数のサーバにアクセス可能なデータを記録するためにそれを復号し得る。１つまたは複数のサーバによるデータの１つまたは複数の復号された部分の結果の比較が成功した一致をもたらす場合、カードは、アクティブ化され得る。１つまたは複数のサーバによるデータの１つまたは複数の復号された部分の結果の比較が失敗した一致をもたらす場合、１つまたは複数のプロセスが行われ得る。例えば、失敗した一致の判断に応答して、ユーザは、カードを再度タップ、スワイプ、または手を振るジェスチャをするように促され得る。この場合、ユーザがカードをアクティブ化することを許可される試行回数を備える所定の閾値があり得る。あるいは、ユーザは、カード検証の試みが失敗したことを示すメッセージなどの通知をデバイスで受信し、カードをアクティブ化するための支援のために関連するサービスに電話、電子メール、またはテキストメッセージを送信するか、カード検証の試みが失敗を示す電話などの他の通知をデバイスで受信し、カードをアクティブ化するための支援のために関連サービスに電話、電子メール、またはテキストメッセージを送信するか、またはカード検証の試みが失敗したことを示す電子メールなどの他の通知を受信し、カードをアクティブ化するための支援のために関連するサービスに電話、電子メール、またはテキストメッセージを送信し得る。
【０１６３】
ブロック１２５０で、１つまたは複数のサーバは、カードのアクティブ化の成功に基づいてリターンメッセージを送信し得る。例えば、デバイスは、１つまたは複数のサーバによるカードのアクティブ化が成功したことを示す１つまたは複数のサーバからの出力を受信するように構成され得る。デバイスは、カードのアクティブ化が成功したことを示すメッセージを表示するように構成され得る。カードがアクティブ化されると、不正使用を回避するために、データの動的生成を中止するようにカードを構成し得る。このようにして、カードは、その後アクティブ化されない場合があり、カードがすでにアクティブ化されていることが１つまたは複数のサーバに通知される。
【０１６４】
他の例のケースでは、顧客は、自分の携帯電話で自分の金融口座にアクセスしたいと考えている。顧客は、モバイルデバイスでアプリケーション（例えば、銀行アプリケーション）を起動し、ユーザ名とパスワードを入力する。この段階で、顧客は、第１レベルのアカウント情報（例えば、最近の購入）を確認し、第１レベルのアカウントオプション（例えば、クレジットカードの支払い）を実行し得る。しかしながら、ユーザが第２レベルのアカウント情報（例えば、支出制限）にアクセスしたり、第２レベルのアカウントオプション（例えば、外部システムへの転送）を実行したりする場合は、第２の要素認証が必要である。したがって、アプリケーションは、ユーザがアカウント検証のためにトランザクションカード（例えば、クレジットカード）を提供することを要求する。次に、ユーザは、自分のクレジットカードをモバイルデバイスにタップし、アプリケーションは、クレジットカードがユーザのアカウントに対応していることを検証する。その後、ユーザは、第２レベルのアカウントデータを表示し、および／または第２レベルのアカウント機能を実行し得る。
【０１６５】
本発明の特定の実施形態では、非接触カードの暗号化認証を使用して、支払いトランザクションを含むトランザクションにさらなる認証を提供し得る。さらなる認証は、トランザクションに関与する特定のアカウントの承認されたユーザの存在および認可を検証することを含むがこれらに限定されない、トランザクションにセキュリティの追加のレベルを提供し、その後のトランザクション調整のために承認されたユーザの存在の暗号化証明をオフラインで作成して、ユーザの不正の可能性を減らし得る（例えば、後で承認されたトランザクションが承認されていないと主張することによって）。さらに、さらなる認証は

、他のトランザクション参加者（例えば、ベンダ、業者など）がトランザクション処理機器および要件をアップグレードする必要性を減らす、最小限にする、または必要としない様々なインスタンスで提供され得る。

【０１６６】

そのような実施のための例示的なシステムは、非接触カードを使用するシステム１３００を示す図１３に示されている。図３に示されるシステムと同様に、システム１３００は、非接触カード１３０５、１つまたは複数のクライアントデバイス１３１０、ネットワーク１３１５、認証サーバ１３２０、業者サーバ１３２５、およびデータベース１３３０を含み得る。図１３は、コンポーネントの単一のインスタンスを示しているが、システム１３００は、任意の数のコンポーネントを含み得る。

【０１６７】

いくつかの例では、非接触カード１３０５は、クライアントデバイス１３１０と無線通信し得る。例えば、ＮＦＣまたは他の形態の無線通信である。非接触カード１３０５は、図５Ａおよび図５Ｂに示されている非接触カードの同じまたは類似のコンポーネントを参照し得る。非接触カード１３０５は、基板、ＥＭＶチップなどのプロセッサ、およびメモリを含み得る。いくつかの例では、非接触カード１３０５は、建物アクセスカード、クレジットカード、デビットカード、識別カード、ロイヤルティプログラムカード、および交通カードのうちの少なくとも１つを備え得る。

【０１６８】

非接触カード１３０５は、第１のアプレット１３０６および第２のアプレット１３０７をさらに含み得る。いくつかの例では、第１のアプレット１３０６は、第２のアプレット１３０７とは異なるアプレットであり得、第１のアプレット１３０６および第２のアプレット１３０７の両方は、それぞれ、１つまたは複数のアプレット識別子に関連付けられ得る。いくつかの例では、第１のアプレット１３０６は、支払いアプレット、例えば、Ｊａｖａカード支払いアプレットであり得、クライアントデバイス１３１０などの他のデバイスとの通信から排除され得る。いくつかの例では、第１のアプレット１３０６は、第２のアプレット１３０７とのみ通信でき、第２のアプレット１３０７は、クライアントデバイス１３１０または他のデバイスと通信するように構成され得る。これらの例では、第１のアプレット１３０６は、クライアントデバイス１３１０または他のデバイスとの通信のために第２のアプレット１３０７にデータを提供し得る。いくつかの例では、第２のアプレット１３０７は、支払いアプレット、例えば、Ｊａｖａカード支払いアプレットであり得るか、または第２のアプレット１３０７は、セキュリティアプレット、通信アプレット、認証アプレット、暗号化アプレット、前述のアプレット適応、または本明細書に記載の機能を実行することができる他のアプレットであり得る。さらに、図１３は、第１のアプレット１３０６および第２のアプレット１３０７を示しているが、システム１３００は、３つ以上のアプレットを含み得、第１のアプレット１３０６および第２のアプレット１３０７のそれぞれの特徴および機能は、複数のアプレット間で分割され、実行され得ることが理解される。追加の機能を提供するために、追加のアプレットが含まれ得ることも理解される。

【０１６９】

いくつかの例では、第２のアプレット１３０７は、第１のアプレット１３０６によって提供されるデータがクライアントデバイス１３１０または他のデバイスにいつ通信され得るかを制御し得る。例えば、第２のアプレット１３０７は、認証手順の完了時、または認証が完了したという通知または信号を認証サーバ１３２０から受信したときに、第１のアプレット１３０６によるデータの通信を許可するように構成され得る。例示的な認証手順は、限定されないが、クライアントデバイス１３１０の通信範囲内に非接触カード１３０５を持ち込み、アクセス資格情報または他の識別情報（例えば、パスワードまたはＰＩＮ）を提供し、本明細書に記載の方法によって暗号文を生成し、第２の要素認証を完了し、生体認証情報を提供し、本明細書に記載されている他の方法、またはそれらの組み合わせを含み得る。第２のアプレット１３０７は、認証手順を実行し、この手順をサポートする

情報を提供し得、または認証手順は、クライアントデバイス１３１０、認証サーバ１３２０、またはそれらの組み合わせによって実行され得る。いくつかの例では、非接触カード１３０５上の第２のアプレット１３０７の存在は、認証手順を開始させ得る。

【０１７０】

いくつかの例では、第１のアプレット１３０６は、データをクライアントデバイス１３１０または他のデバイスに直接通信するように構成され得る。この通信は、第２のアプレット１３０７によって制御され得、第２のアプレット１３０７は、認証手順の完了または認証通知または認証信号の受信まで、第１のアプレット１３０６による通信を排除し得る。

【０１７１】

いくつかの例では、クライアントデバイス１３１０は、コンピュータデバイス、または、例えば、サーバ、ネットワークアプライアンス、パーソナルコンピュータ（ＰＣ）、ワークステーション、モバイルデバイス、電話、ハンドヘルドＰＣ、パーソナルデジタルアシスタント（ＰＤＡ）、シンクライアント、ファットクライアント、インターネットブラウザ、またはその他のデバイスを含む通信デバイスであり得る。クライアントデバイス１３１０はまた、モバイルデバイスであり得る。例えば、モバイルデバイスには、Ａｐｐｌｅ（登録商標）のｉＰｈｏｎｅ（登録商標）、ｉＰｏｄ（登録商標）、ｉＰａｄ（登録商標）、またはＡｐｐｌｅ（登録商標）のｉＯＳ（登録商標）オペレーティングシステムを実行するその他のモバイルデバイス、Ｍｉｃｒｏｓｏｆｔ（登録商標）のＷｉｎｄｏｗｓ（登録商標）モバイルオペレーティングシステムを実行するデバイス、Ａｎｄｒｏｉｄ（登録商標）オペレーティングシステムを実行するデバイス、および／または他のスマートフォンまたは同様のウェアラブルモバイルデバイスが含まれ得る。クライアントデバイス１３１０は、１つまたは複数のネットワーク１３１５を介して、認証サーバ１３２０および業者サーバ１３２５などの１つまたは複数のサーバ、および支払い端末１３３５と通信し得、１つまたは複数のサーバとのそれぞれのフロントエンドツーバックエンドのペアとして動作し得る。クライアントデバイス１３１０は、例えば、デバイス１３１０上で実行されるモバイルデバイスアプリケーションから、１つまたは複数の要求を１つまたは複数のサーバに送信し得る。１つまたは複数の要求は、１つまたは複数のサーバからのデータの取得に関連付けられ得る。

【０１７２】

システム１３００は、１つまたは複数のネットワーク１３１５を含み得る。いくつかの例では、ネットワーク１３１５は、無線ネットワーク、有線ネットワーク、または無線ネットワークと有線ネットワークの任意の組み合わせのうちの１つまたは複数であり得、クライアントデバイス１３１０を１つまたは複数のサーバに接続するように構成され得る。例えば、ネットワーク１３１５は、光ファイバネットワーク、パッシブ光ネットワーク、ケーブルネットワーク、インターネットネットワーク、衛星ネットワーク、無線ＬＡＮ、モバイル通信のためのグローバルシステム（ＧＳＭ）、パーソナル通信サービス（ＰＣＳ）、パーソナルエリアネットワーク、ワイヤレスアプリケーションプロトコル（ＷＡＰ）、マルチメディアメッセージングサービス（ＭＭＳ）、拡張メッセージングサービス（ＥＭＳ）、ショートメッセージサービス（ＳＭＳ）、時分割多重（ＴＤＭ）ベースのシステム、コード分割多重アクセス（ＣＤＭＡ）ベースのシステム、Ｄ－ＡＭＰＳ、Ｗｉ－Ｆｉ、固定ワイヤレスデータ、ＩＥＥＥ　８０２．１１ｂ、８０２．１５．１、８０２．１１ｎおよび８０２．１１ｇ、ブルートゥース（登録商標）、近距離無線通信（ＮＦＣ）、無線周波数識別（ＲＦＩＤ）、Ｗｉ－Ｆｉなどのうちの１つまたは複数を含み得る。

【０１７３】

さらに、ネットワーク１３１５は、これらに限定されないが、電話回線、光ファイバ、ＩＥＥＥイーサネット９０２．３、広域ネットワーク（ＷＡＮ）、無線パーソナルエリアネットワーク、ローカルエリアネットワーク（ＬＡＮ）、またはインターネットなどのグローバルネットワークを含み得る。さらに、ネットワーク１３１５は、インターネットネットワーク、無線通信ネットワーク、セルラネットワークなど、またはそれらの任意の組み合わせをサポートし得る。ネットワーク１３１５は、スタンドアロンネットワークとし

て、または互いに協力して動作する、１つのネットワーク、または上記の任意の数の例示的なタイプのネットワークをさらに含み得る。ネットワーク１３１５は、それらが通信可能に結合されている１つまたは複数のネットワーク要素の１つまたは複数のプロトコルを利用し得る。ネットワーク１３１５は、他のプロトコルとの間で、ネットワークデバイスの１つまたは複数のプロトコルに変換し得る。ネットワーク１３１５は、単一のネットワークとして示されているが、１つまたは複数の例によれば、ネットワーク１３１５は、例えば、インターネット、サービスプロバイダのネットワーク、ケーブルテレビネットワーク、クレジットカードアソシエーションネットワークなどの企業ネットワーク、およびホームネットワークなどの複数の相互接続されたネットワークを備え得ることを理解されたい。

【０１７４】

システム１３００は、認証サーバ１３２０および業者サーバ１３２５などの１つまたは複数のサーバを含み得る。いくつかの例では、１つまたは複数のサーバは、メモリに結合された１つまたは複数のプロセッサを含み得る。１つまたは複数のサーバは、本明細書に記載の１つまたは複数の機能を実行するために複数のワークフローアクションを実行するために異なる時間に様々なデータを制御および呼び出すための中央システム、サーバまたはプラットフォームとして構成され得る。１つまたは複数のサーバは、１つまたは複数のデータベースを含み得るか、または１つまたは複数のデータベースとデータ通信し得る。１つまたは複数のサーバは、少なくとも１つのクライアントデバイス１３１０とデータ通信し得る。

【０１７５】

システム１３００は、支払い端末１３３５を含み得る。支払い端末１３３５は、認証サーバ１３２０または業者サーバ１３２５のようなサーバであり得るか、または異なる構成を有し得る。例示的な構成には、電子支払いキオスク、支払いリーダ、レジ、または取引に従事するのに適した他の任意のデバイスが含まれるが、これらに限定されない。支払い端末１３３５は、ネットワーク１３１５を介して、クライアントデバイス１３１０、認証サーバ１３２０、および業者サーバ１３２５を含む、システム１３００の他のコンポーネントとデータ通信し得る。

【０１７６】

システム１３００は、データベース１３３０を含み得る。データベース１３３０は、リレーショナルまたは非リレーショナルデータベースであり得、データベース１３３０に含まれるデータは、単一のデータベースまたは複数の別個のデータベースによって格納され得る。データベース１３３０は、これらに限定されないが、アカウントおよびトランザクション情報、識別情報、ユーザ情報、およびトランザクションをサポートし、本明細書に記載の機能を実行するために必要な他の情報を含み得る。

【０１７７】

図１４は、例示的な実施形態に係るトランザクションを認証する方法のフローチャートを示し、この方法は、例えば、システム１３００によって実施され得る。ステップ１４０２で、カードトランザクションが開始される。カードトランザクションの開始は、例えば、「カード提示」トランザクションである、商品またはサービスの支払いのために非接触カード１３０５が支払い端末１３３５に提示されるときに起こり得る。あるいは、カードに関連付けられた口座番号が商品またはサービスの支払いのためにウェブサイトに入力されたときなど、非接触カード１３０５が「カード非提示トランザクション」の支払いに使用されるときに、カードトランザクションの開始が起こり得る。

【０１７８】

ステップ１４０４で、トランザクション要求が認証サーバ１３２０に送信される。カード提示トランザクションの場合、トランザクション要求は、支払い端末１３３５で発信され得る。あるいは、カード非提示トランザクションの場合、トランザクション要求はクライアントデバイス１３１０で発信され得る。トランザクション要求は、最初に業者サーバ１３２５、すなわち、商品またはサービスが購入されている業者に属するサーバに送信さ

れ得る。次に、トランザクション要求は、業者サーバから、銀行サーバまたは支払い機関サーバなどの１つまたは複数の仲介者を介して、認証サーバ１３２０に送信され得る。

【０１７９】

ステップ１４０６で、トランザクション要求を受信すると、認証サーバ１３２０は、要求されたトランザクションが高リスクトランザクションであるかどうかを決定する。トランザクションは、例えば、不正なトランザクションに関連付けられている業者と実行される場合、高リスクトランザクションになり得る。他の例として、不正なトランザクションに関連する地理的地域に所在する業者と取引を行う場合、その取引は、高リスクトランザクションであり得る。さらに、トランザクションは、カード所有者の過去のトランザクションパターンに適合せず、例えば、カード所有者のトランザクション履歴に基づいて異常な時期または異常な地理的地域で行われる場合、高リスクトランザクションとして指定され得る。さらに、高リスクトランザクションは、異常な頻度で実行されるトランザクション、または他の多数のトランザクションの所定の期間内に発生するトランザクションであり得る。高リスクトランザクションはさらに、過去の不正行為または潜在的に不正な過去の活動があることが知られている、業者またはその他のアカウントで行われるトランザクションであり得る。認証サーバ１３２０は、決定を行うときに、データベース１３３０に格納されたカード所有者のトランザクション履歴を参照し得る。

【０１８０】

ステップ１４０６で、認証サーバ１３２０が、トランザクションが高リスクトランザクションではない（いいえ）と決定した場合、方法は、ステップ１４０８に進む。ステップ１４０８で、認証サーバ１３２０は、トランザクションの値が所定の閾値を超えるかどうかを決定する。例えば、認証サーバ１３２０は、要求されたトランザクションが特定の金額を超えているかどうかを決定し得る。所定の閾値は、カード所有者によって設定され得るか、または認証サーバ１３２０によって自動的に設定され得る。

【０１８１】

ステップ１４０８で、認証サーバ１３２０が、トランザクションの値が所定の閾値を超えないと決定した場合、方法は、ステップ１４１８に進み、トランザクションは、認証サーバ１３２０によって許可される。

【０１８２】

しかしながら、ステップ１４０６で、認証サーバ１３２０が、トランザクションが高リスクトランザクションである（はい）と決定した場合、方法は、ステップ１４１０に進む。同様に、ステップ１４０８で、認証サーバ１３２０が、トランザクションの値が所定の値を超える（はい）と決定した場合、方法は、ステップ１４１０に進む。方法がステップ１４１０に進むとき、要求されたトランザクションは、さらなる認証を待つ間、一時的に保留される。

【０１８３】

ステップ１４１０で、認証サーバ１３２０は、ネットワーク１３１５を介して、非接触カード認証のためにクライアントデバイス１３１０に要求を送信する。要求は、アプリケーション内通知、ポップアップ通知、ＳＭＳメッセージ、電子メール、またはその他の適切な通知の形式であり得る。要求は、要求されたトランザクションを進めるためにさらなる認証が必要であることを説明し得、さらに、カード所有者に、非接触カード１３０５をクライアントデバイス１３１０の通信範囲に持ち込むように促し得る。

【０１８４】

さらに安全を確保するために、認証サーバ１３２０は、非接触カード１３０５を通信範囲に持ち込むことに加えて、カード所有者が生体認証情報を提供し、ＰＩＮを提供し、パスワードを提供し、または他の識別情報をクライアントデバイス１３１０に提供することをさらに要求し得る。クライアントデバイス１３１０は、メモリに格納された参照生体認証情報に対して、提供された生体認証情報を検証し得る。生体認証情報は、例えば、指紋情報、光学データ、顔認識、および／または網膜情報を含み得る。

【０１８５】

ステップ１４１２で、カード所有者は、クライアントデバイス１３１０を介して非接触カード認証の要求を受信すると、非接触カード１３０５をクライアントデバイス１３１０の通信範囲に持ち込み得る。

【０１８６】

非接触カード１３０５がクライアントデバイス１３１０の通信範囲にあるとき、非接触カード１３０５は、認証される。非接触カード１３０５は、本明細書に記載のプロセスのいずれかによって認証され得る。いくつかの例では、クライアントデバイス１３１０のプロセッサ１３１１は、非接触カード１３０５によって生成されたＭＡＣ暗号文を検証し得る。次に、プロセッサ１３１１は、非接触カード１３０５が検証されたことを認証サーバ１３２０に通信し得る。あるいは、非接触カードによって生成されたＭＡＣ暗号文は、検証のために認証サーバ１３２０に送信され得る。

【０１８７】

ステップ１４１４で非接触カードが認証されない（いいえ）場合、認証サーバ１３２０は、ステップ１４１６で要求されたトランザクションを拒否し、それにより、トランザクションが実行されることを禁止する。トランザクションが拒否されると、認証サーバ１３２０は、トランザクションが拒否されたことをカード所有者に通知する通知をクライアントデバイス１３１０にさらに送信し得る。その後、方法は、終了する。

【０１８８】

ステップ１４１４で非接触カードが認証された（はい）場合、認証サーバ１３２０は、ステップ１４１８でのトランザクションを許可する。トランザクションが許可されると、認証サーバ１３２０は、トランザクションが承認されたことをカード所有者に通知する通知をクライアントデバイス１３１０にさらに送信し得る。その後、方法は、終了する。

【０１８９】

本明細書に記載のシステム１３００および方法１４００は、非接触カードを使用するトランザクションのセキュリティを改善する。具体的には、非接触カードとクライアントデバイスを使用した暗号化認証を要求することで、カード所有者が非接触カードを紛失したり、非接触カードが盗まれたり、非接触カードに印刷された情報が盗まれたりする状況を防ぐ。暗号化認証を要求することにより、トランザクションに従事しようとする人は、基本的に、非接触カードを提供することに加えて、非接触カードに関連付けられたクライアントデバイスも所有していることを証明し、さらにクライアントデバイスにアクセスできることを証明する必要がある（すなわち、ＰＩＮ、パスワード、または生体認証を使用してロックを解除できる）。これにより、非接触カードが不正使用される可能性が低くなる。さらに、暗号化認証の要求は、高リスクトランザクションであるか、または所定の値を超える金額の提案されたトランザクションに対してのみ必要となり得、カード所有者は、全てのトランザクションの追加の認証層を負担する必要がなくなる。システム１３００および方法１４００のさらなる利点は、非接触カードへのセキュリティ機能の組み込み、および非接触カード自体の使用により、システムの他のコンポーネントを変更する必要なしに、本明細書に記載のセキュリティ機能を提供し得る。

【０１９０】

さらに、暗号化認証を要求することは、非接触カードが商品またはサービスの支払いに使用されているトランザクションに限定される必要はない。本明細書に記載の方法１４００は、非接触カードのプロビジョニングに同様に適用し得る。例えば、カード所有者がＧｏｏｇｌｅ　Ｐａｙ（登録商標）やＡｐｐｌｅ　Ｐａｙ（登録商標）などのオンライン決済サービスで使用するために非接触カードをプロビジョニングしようとすると、同様に、非接触カードをプロビジョニングしようとしている人が、単にカードに印刷された情報を使用するのではなく、実際に非接触カードを所有していることを検証するために暗号認証が必要になり得る。これにより、カード番号、ＣＶＣ、および有効期限を違法な手段で取得したが、非接触カードを物理的に所有していない個人による非接触カードの使用に対するセキュリティが提供され得る。

【０１９１】

いくつかの例では、本開示は、非接触カードのタップに言及している。しかしながら、本開示は、タップに限定されず、本開示は、他のジェスチャ（例えば、カードのウェーブまたは他の動き）を含むことが理解される。

【０１９２】

明細書および請求の範囲を通じて、以下の用語は、文脈が明確に別段の指示をしない限り、少なくとも本明細書に明示的に関連付けられた意味をとる。「または」という用語は、包括的な「または」を意味することを意図している。さらに、「ａ」、「ａｎ」、および「ｔｈｅ」という用語は、別段の指定がない限り、または文脈から明確になって単数形に向けられない限り、１つまたは複数を意味することを意図している。

【０１９３】

この説明では、多くの具体的な詳細が説明されている。しかしながら、開示された技術の実施は、これらの特定の詳細なしで実施され得ることが理解されるべきである。他の例では、この説明の理解を曖昧にしないために、よく知られた方法、構造、および技術は、詳細に示されていない。「いくつかの例」、「他の例」、「一例」、「例」、「様々な例」、「一実施形態」、「実施形態」、「いくつかの実施形態」、「例示的な実施形態」、「様々な実施形態」、「１つの実施」、「実施」、「例示的な実施」、「様々な実施」、「いくつかの実施」などへの言及は、そのように説明された開示された技術の実施が特定の特徴、構造、または特性を含み得るが、全ての実施が必ずしも特定の特徴、構造、または特性を含むとは限らないことを示す。さらに、「一例では」、「一実施形態では」、または「一実施では」という句の繰り返し使用は、同じ例、実施形態、または実施を必ずしも指すとは限らないが、そうであってもよい。

【０１９４】

本明細書で使用される場合、特に明記されていない限り、共通の対象を説明するための序数形容詞「第１」、「第２」、「第３」などの使用は、同様の対象の異なるインスタンスが参照されていることを示すだけであり、そのように記述された対象は、時間的、空間的、ランク付け、またはその他の方法で、特定の順序である必要があることを意味するものではない。

【０１９５】

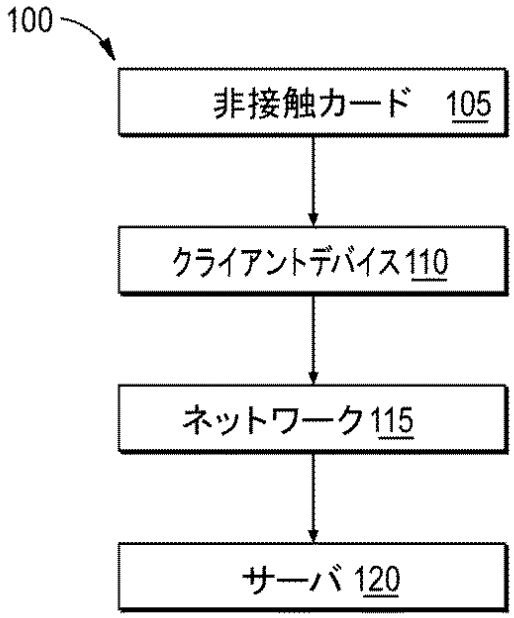
開示された技術の特定の実施は、現在最も実用的で様々な実施であると考えられているものに関連して説明されてきたが、開示された技術は、開示された実施に限定されるべきではなく、逆に、添付の請求の範囲内に含まれる様々な修正および同等の取り決めをカバーすることを意図していることを理解されたい。本明細書では特定の用語が使用されているが、それらは一般的かつ説明的な意味でのみ使用されており、限定の目的ではない。

【０１９６】

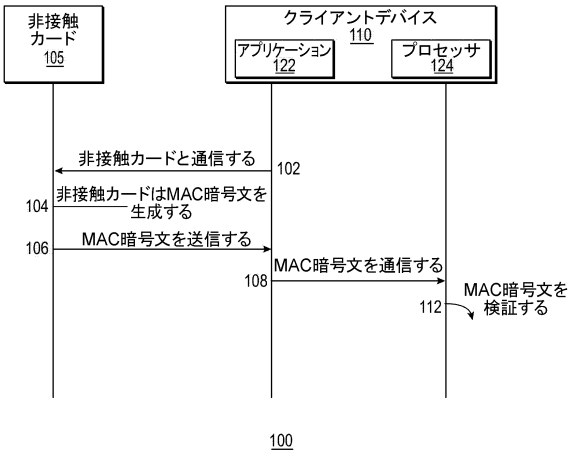
この書面による説明は、例を使用して、最良のモードを含む開示された技術の特定の実施を開示し、また、当業者が、任意のデバイスまたはシステムの作成および使用、並びに任意の組み込まれた方法の実行を含む、開示された技術の特定の実施を実践できるようにする。開示された技術の特定の実施の特許性のある範囲は、請求の範囲で定義され、当業者に発生する他の例を含み得る。そのような他の例は、請求の範囲の文字通りの言語と異ならない構造要素を有する場合、または請求の範囲の文字通りの言語と実質的に異なる同等の構造要素を含む場合、請求の範囲の範囲内にあることを意図している。

【図面】

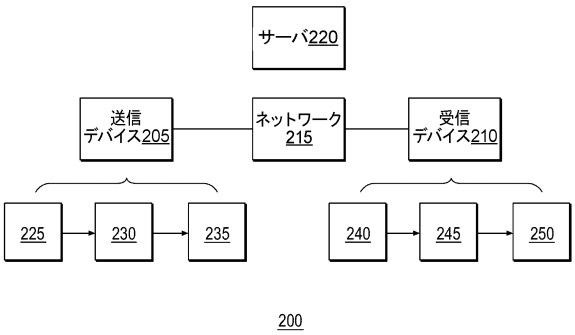
【図１Ａ】



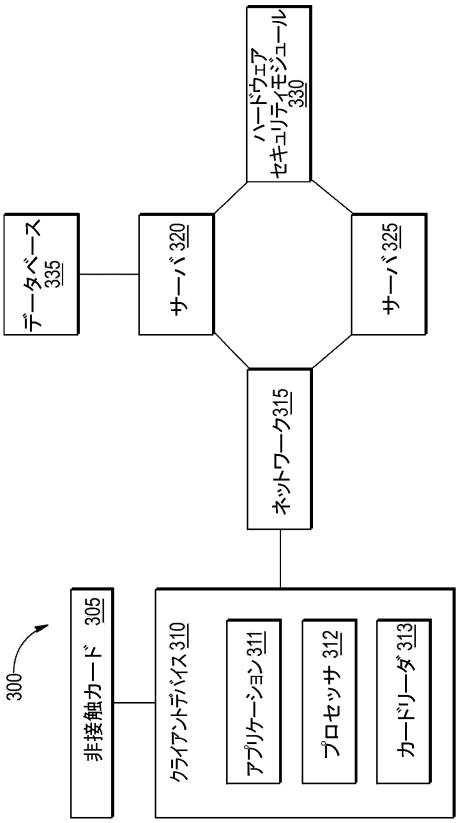
【図１Ｂ】



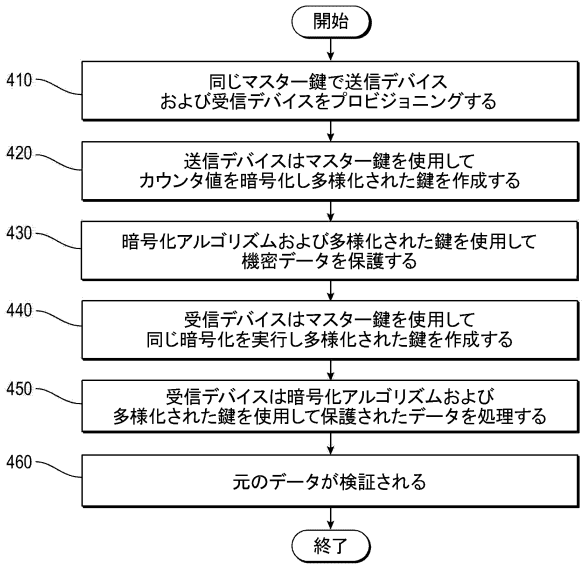
【図２】



【図３】

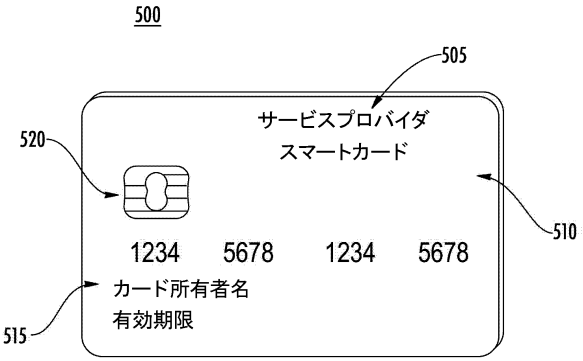


【図４】

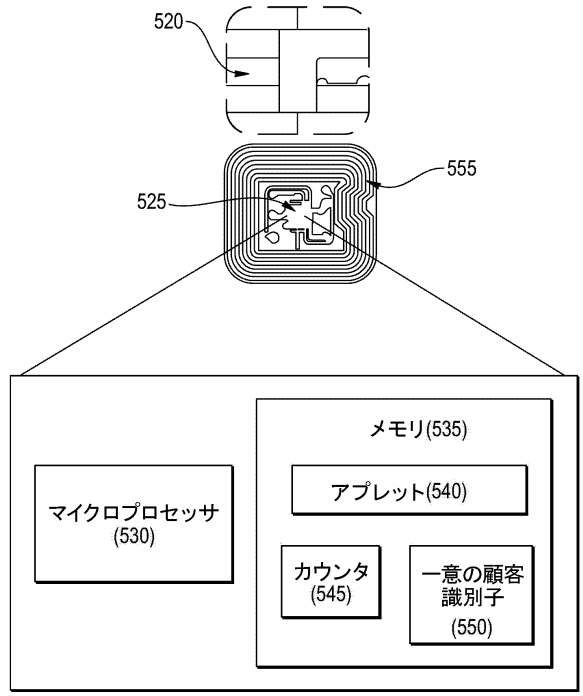


400

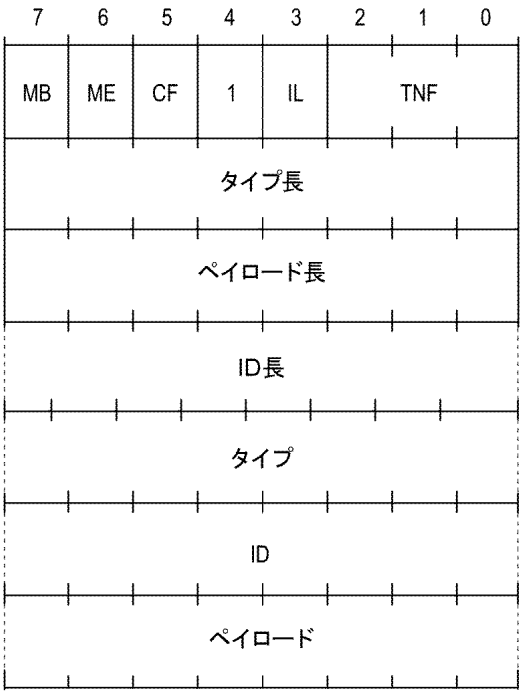
【図５Ａ】



【図５Ｂ】

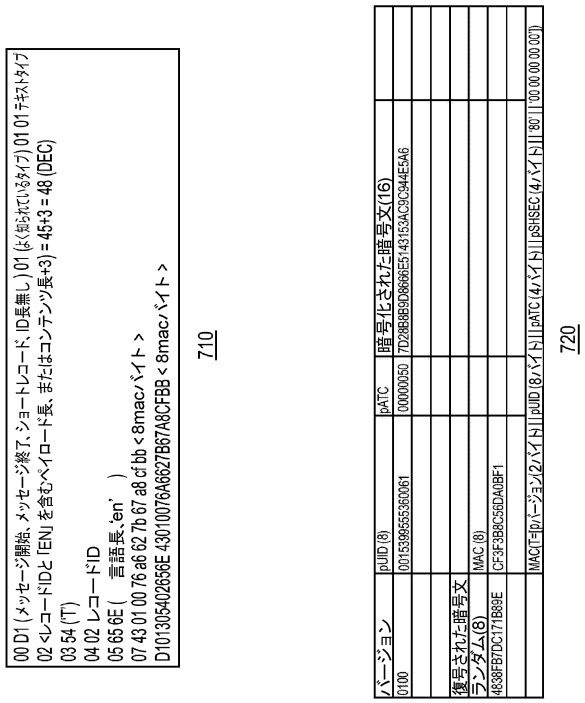


【図６】

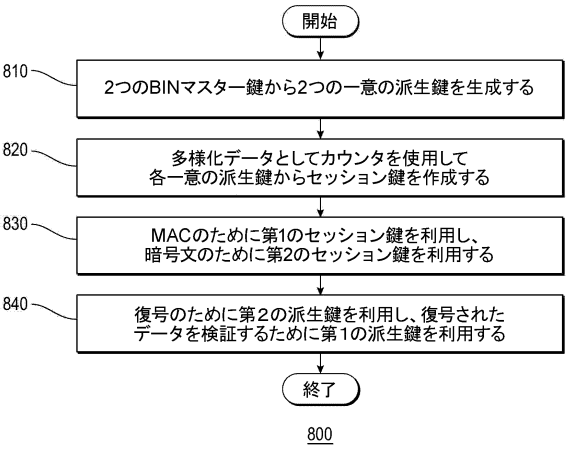


600

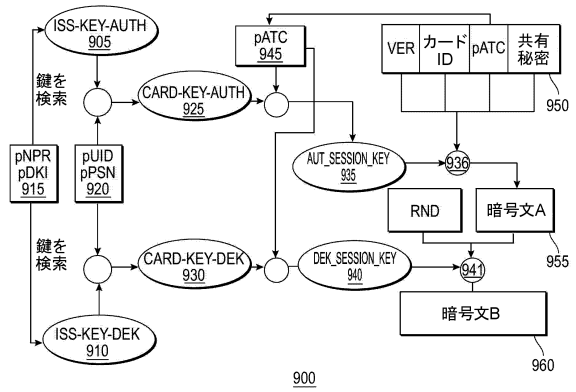
【図７】


00 D1 (メッセージ開始、メッセージ終了、ショートレコード、ID長無し) 01 (よく知られているタイプ) 01 01 テキストタイプ
02 <レコードIDと「EN」を含むペイロード長、またはコンテンツ長+3) = 45+3 = 48 (DEC)
03 54 ('T')
04 02 レコードID
05 65 6E (言語長、'en')
07 43 01 00 76 a6 62 7b 67 a8 cf bb < 8macバイト >
D1013054026 56E 43010076A6627B67A8CFBB < 8macバイト >
710
バージョン
0100
pUID (8)
0015398555360061
pATC
00000050
暗号化された暗号文(16)
7D28B8B9D8666E5143153AC9C944E5A6
復号された暗号文
ランダム(8)
4838FB7DC171B89E
MAC (8)
CF3F3B8C56DA0BF1
MAC(T=[pバージョン(2バイト)||pUID (8バイト)||pATC (4バイト)||pSHSEC (4バイト)||'80'||'00 00 00 00 00'])
720

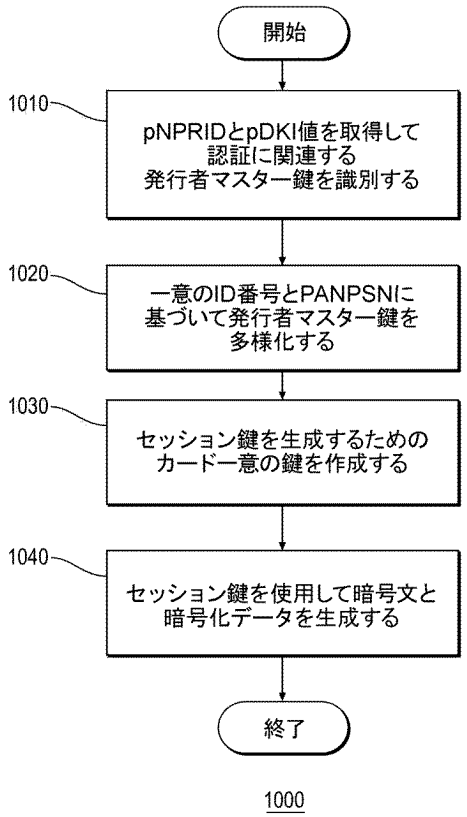
【図８】


開始
810
2つのBINマスター鍵から2つの一意の派生鍵を生成する
820
多様化データとしてカウンタを使用して
各一意の派生鍵からセッション鍵を作成する
830
MACのために第1のセッション鍵を利用し、
暗号文のために第2のセッション鍵を利用する
840
復号のために第２の派生鍵を利用し、復号された
データを検証するために第１の派生鍵を利用する
終了
800

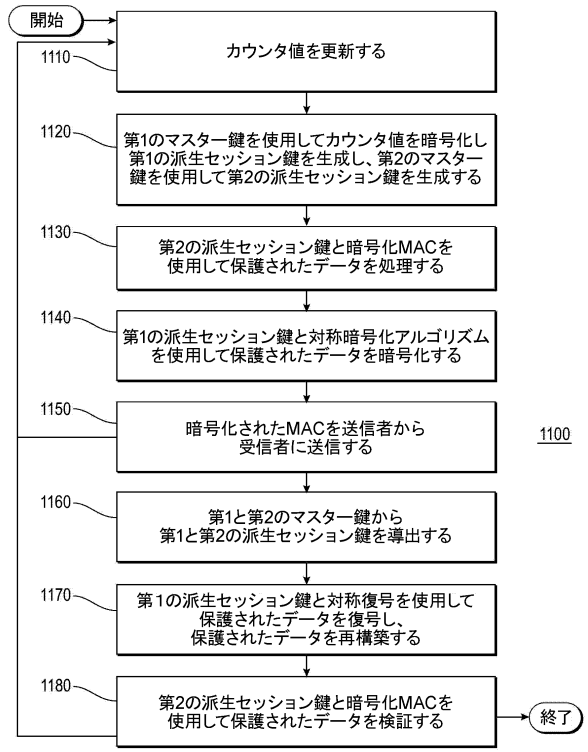
【図９】


ISS-KEY-AUTH
905
鍵を
検索
CARD-KEY-AUTH
925
pATC
945
VER
カード
ID
pATC
共有
秘密
950
pNPR
pDKI
915
pUID
pPSN
920
AUT_SESSION_KEY
935
936
RND
暗号文A
955
鍵を
検索
CARD-KEY-DEK
930
DEK_SESSION_KEY
940
941
暗号文B
960
ISS-KEY-DEK
910
900

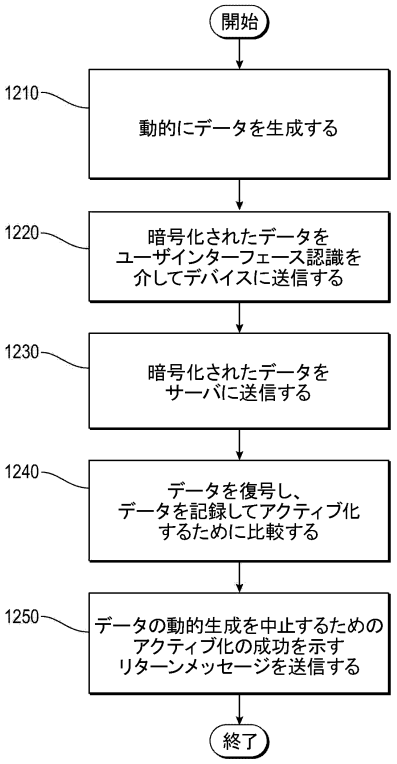
【図１０】


開始
1010
pNPRIDとpDKI値を取得して
認証に関連する
発行者マスター鍵を識別する
1020
一意のID番号とPANPSNに
基づいて発行者マスター鍵を
多様化する
1030
セッション鍵を生成するための
カード一意の鍵を作成する
1040
セッション鍵を使用して暗号文と
暗号化データを生成する
終了
1000

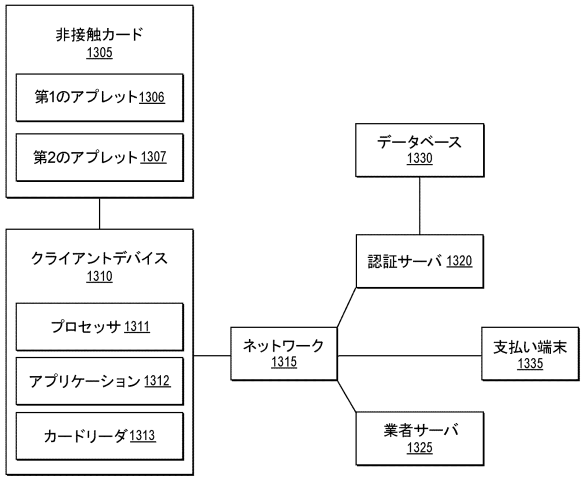
【図１１】



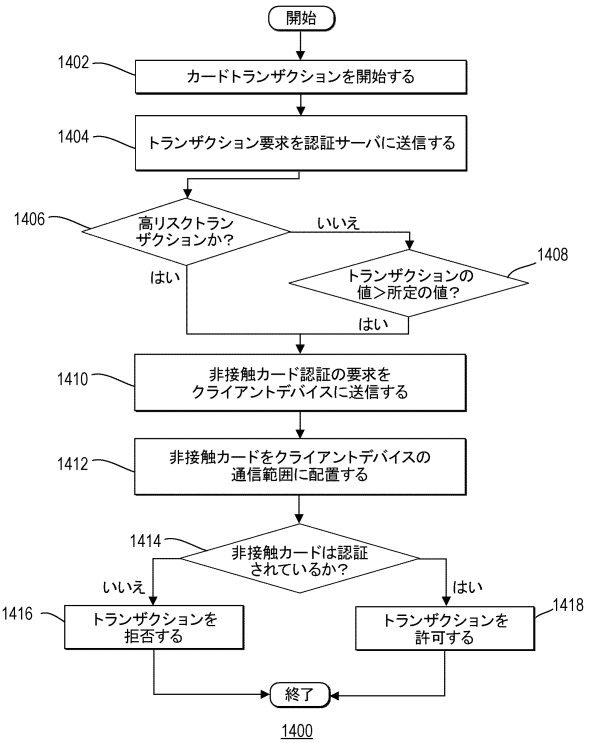
【図１２】



【図１３】



【図１４】



フロントページの続き

(51)国際特許分類　　ＦＩ
　Ｇ０６Ｆ　21/35
　Ｇ０６Ｑ　20/34

(33)優先権主張国・地域又は機関
　米国(US)
(31)優先権主張番号　16/205,119
(32)優先日　平成30年11月29日(2018.11.29)
(33)優先権主張国・地域又は機関
　米国(US)
アメリカ合衆国０２４６１マサチューセッツ州ニュートン・ハイランズ、ヒルサイド・ロード４９番
(72)発明者　ジェフリー・ルール
アメリカ合衆国２０８１５メリーランド州チェビー・チェイス、レアード・プレイス３９０６番
(72)発明者　ジェームズ・アッシュフィールド
アメリカ合衆国２３１１３バージニア州ミッドロージアン、オールド・フォート・ドライブ１４１０６番
(72)発明者　スリニバサ・チグルパティ
アメリカ合衆国６００４７イリノイ州ロング・グローブ、ティール・コート５８０４番
審査官　金沢 史明
(56)参考文献　特表２０１５－５３０６３７（ＪＰ，Ａ）
特表２００７－５１４３３３（ＪＰ，Ａ）
米国特許出願公開第２０１６／０２９４５５０（ＵＳ，Ａ１）
米国特許出願公開第２０１８／０２４０１１０（ＵＳ，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／００－ ９／４０