

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7668209号
(P7668209)

(45)発行日 令和7年4月24日(2025.4.24)

(24)登録日 令和7年4月16日(2025.4.16)

(51)国際特許分類		F I	
H 0 4 L	9/32 (2006.01)	H 0 4 L	9/32 2 0 0 A
H 0 4 L	9/14 (2006.01)	H 0 4 L	9/14
G 0 6 F	21/32 (2013.01)	H 0 4 L	9/32 1 0 0 D
		G 0 6 F	21/32
請求項の数 17 (全46頁)			
(21)出願番号	特願2021-507677(P2021-507677)	(73)特許権者	519111877
(86)(22)出願日	令和1年10月2日(2019.10.2)		キャピタル・ワン・サービシーズ・リミ
(65)公表番号	特表2022-508010(P2022-508010 A)		テッド・ライアビリティ・カンパニー
(43)公表日	令和4年1月19日(2022.1.19)		Capital One Service
(86)国際出願番号	PCT/US2019/054186		s, L L C
(87)国際公開番号	WO2020/072575		アメリカ合衆国22102バージニア州
(87)国際公開日	令和2年4月9日(2020.4.9)		マククリーン、キャピタル・ワン・ドライ
審査請求日	令和4年9月29日(2022.9.29)		ブ1680番
(31)優先権主張番号	16/590,429	(74)代理人	100145403
(32)優先日	令和1年10月2日(2019.10.2)		弁理士 山尾 憲人
(33)優先権主張国・地域又は機関	米国(US)	(74)代理人	100132241
(31)優先権主張番号	16/205,119		弁理士 岡部 博史
(32)優先日	平成30年11月29日(2018.11.29)	(74)代理人	100135703
	最終頁に続く		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】

クライアントアプリケーションおよび多様化された鍵を格納する非一時的なメモリであって、

前記クライアントアプリケーションは、プロセッサ、メモリ、および通信インターフェースを備えるクライアントデバイスで実行するための命令を含み、

前記クライアントアプリケーションは、

サーバからチャレンジを受信し、
認証要求信号を非接触カードに送信し、

前記非接触カードから受信された認証データであって、前記多様化された鍵を用いて暗号化された認証データをサーバに送信し、

前記非接触カードから検索された前記認証データの検証であって、FIDO秘密鍵の使用を許可する検証を、前記サーバから受信し、

前記FIDO秘密鍵を使用して前記チャレンジに署名し、

前記署名されたチャレンジを前記サーバに送信するように構成される、
非一時的なメモリ。

【請求項2】

前記クライアントアプリケーションは、FIDO公開鍵を前記サーバに送信するように構成される、請求項1に記載の非一時的なメモリ。

【請求項3】

前記クライアントアプリケーションは、前記 F I D O 秘密鍵を前記クライアントデバイスの前記メモリに格納する、請求項 1 に記載の非一時的なメモリ。

【請求項 4】

前記クライアントアプリケーションは、前記サーバから前記チャレンジを受信する前に、前記チャレンジの要求を前記サーバに送信するように構成される、請求項 1 に記載の非一時的なメモリ。

【請求項 5】

前記認証データは、前記通信インターフェースによって生成された近距離無線通信範囲を介して前記非接触カードから受信される、請求項 1 に記載の非一時的なメモリ。

【請求項 6】

前記クライアントアプリケーションは、前記 F I D O 秘密鍵を使用して前記チャレンジに署名する前に、検証入力を受信するように構成される、請求項 1 に記載の非一時的なメモリ。

【請求項 7】

前記非一時的なメモリは、識別情報およびマスター鍵をさらに格納し、
前記クライアントアプリケーションは、前記マスター鍵とともに前記識別情報を使用して、前記多様化された鍵を生成するように構成される、請求項 1 に記載の非一時的なメモリ。

【請求項 8】

前記識別情報は、ウェブサイトのサイト識別子を含む、請求項 7 に記載の非一時的なメモリ。

【請求項 9】

前記サーバは、前記ウェブサイトに関連付けられている、請求項 8 に記載の非一時的なメモリ。

【請求項 10】

前記非一時的なメモリは、カウンタおよびマスター鍵を格納し、
前記クライアントアプリケーションは、前記マスター鍵および前記カウンタを使用して前記多様化された鍵を生成するように構成される、請求項 1 に記載の非一時的なメモリ。

【請求項 11】

前記クライアントアプリケーションは、前記サーバから前記カウンタを受信するように構成される、請求項 10 に記載の非一時的なメモリ。

【請求項 12】

前記 F I D O 秘密鍵は、前記非接触カードに格納され、前記多様化された鍵を用いて暗号化され、前記非接触カードの N F C 読み取りを介して前記前記クライアントアプリケーションに送信される、請求項 1 に記載の非一時的なメモリ。

【請求項 13】

前記チャレンジは、乱数またはランダムな文字の文字列の 1 つを含む、請求項 1 に記載の非一時的なメモリ。

【請求項 14】

プロセッサと、F I D O 秘密鍵および F I D O 公開鍵を格納するメモリと、通信インターフェースとを備えるクライアントデバイスで実行するための命令を含むクライアントアプリケーションが、サーバからのチャレンジを受信することと、

前記クライアントアプリケーションが、認証要求を非接触カードに送信することと、
前記クライアントアプリケーションが、前記非接触カードから受信された認証データをサーバに送信することと、

前記クライアントアプリケーションが、前記非接触カードから検索された前記認証データの検証であって、F I D O 秘密鍵の使用を許可する検証を、前記サーバから受信することと、

前記クライアントアプリケーションが、前記 F I D O 秘密鍵を使用して前記チャレンジに署名することと、

10

20

30

40

50

前記クライアントアプリケーションが、前記署名されたチャレンジを前記サーバに送信することと、

を含む方法。

【請求項 15】

前記方法は、

前記クライアントアプリケーションが、前記 F I D O 公開鍵を前記サーバに送信することを含む、請求項 14 に記載の方法。

【請求項 16】

前記クライアントアプリケーションは、前記 F I D O 秘密鍵を前記クライアントデバイスの前記メモリに格納する、請求項 14 に記載の方法。

【請求項 17】

前記方法は、

前記クライアントアプリケーションが、前記 F I D O 秘密鍵を使用して前記チャレンジに署名する前に、検証入力を受信することを含む、請求項 14 に記載の方法。

【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、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、2018年10月2日に出願された米国仮特許出願第62／740,352号および2019年10月2日に出願された米国特許出願第16／590,429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】

セキュリティへの懸念にもかかわらず、アカウントアクセスと重要な情報を保護するためのログイン資格情報パスワードの広範な使用が続いている。この問題に対する潜在的な解決策は、FIDO認証標準を作成するためのFIDO2プロジェクトの形でFIDOアライアンスによって提案されている。FIDO2プロジェクトには、W3Cのウェブ認証

10

20

30

40

50

仕様と F I D O クライアント認証プロトコルが組み込まれており、一般的なデバイスを使用してオンラインサービスを認証し、アカウントアクセスを制御できる。F I D O 2 プロジェクトは、秘密鍵を使用して認証器デバイスによって応答される暗号化チャレンジを開始することにより、デバイスの認証を提供する。しかしながら、デバイス認証プロセスの最初に承認されたユーザが存在することを証明するのが難しいなど、セキュリティの問題が残っている。

【 0 0 0 7 】

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】

【 0 0 0 8 】

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。

【 0 0 0 9 】

本開示の実施形態は、クライアントデバイスであって、プロセッサと、F I D O 公開鍵、F I D O 秘密鍵、およびアカウント情報を含むメモリと、非接触カードおよびサーバとのデータ通信における通信インターフェースであって、通信インターフェースは、通信範囲を有する、通信インターフェースと、を備え、トランザクションを開始するための命令を受信すると、プロセッサは、トランザクション要求を第1のサーバに送信し、トランザクション要求は、アカウント情報およびトランザクションに関連するトランザクション情報を含み、第2のサーバからチャレンジを受信し、非接触カードからトランザクション検証を要求し、通信インターフェースを介して、非接触カードが通信範囲に入ったときに、非接触カードからトランザクション検証を受信し、トランザクション検証は、チャレンジに関連してF I D O 秘密鍵の使用を許可し、秘密鍵を使用してチャレンジに署名し、署名されたチャレンジを第2のサーバに送信する、ように構成される、クライアントデバイスを提供する。

【 0 0 1 0 】

本開示の実施形態は、承認方法であって、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が、第1のサーバとのトランザクションを開始するステップと、クライアントアプリケーションが、トランザクション情報を第1の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が、第2のサーバによって送信されたチャレンジを受信するステップと、クライアントアプリケーションが、トランザクション検証を要求するステップと、クライアントアプリケーションが、トランザクション検証を受信するステップであって、トランザクション検証は、クライアントアプリケーションがクライアントデバイスのメモリに格納されたF I D O 秘密鍵を利用してチャレンジに署名することを承認する、ステップと、クライアントアプリケーションが、F I D O 秘密鍵を使用してチャレンジに署名するステップと、クライアントアプリケーションが、署名されたチャレンジを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が、トランザクションが承認されたというサーバからの指示を受信するステップと、を含む承認方法を提供する。

【 0 0 1 1 】

本開示の実施形態は、非接触カードであって、基板を、備え、基板は、アプレット、カウンタ値、マスター鍵、多様化された鍵、F I D O 公開鍵、およびF I D O 秘密鍵を含むメモリと、通信インターフェースと、メモリおよび通信インターフェースと通信するプロセッサと、を含み、プロセッサは、通信インターフェースがクライアントデバイスの通信範囲の範囲内にあるときに、カウンタ値を更新し、多様化された鍵およびカウンタ値を使用して暗号文を作成し、暗号文は、F I D O 公開鍵を格納し、通信インターフェースを介

10

20

30

40

50

して暗号文を送信する、ように構成されている、非接触カードを提供する。

【0012】

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】

【0013】

【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。

10

【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。

20

【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データ伝送システムを使用するFIDOシステムを示している。

【図14】例示的な実施形態に係るオンライン支払を処理するためのフローチャートを示している。

【図15】例示的な実施形態に係るオンライン支払を処理するためのクライアントデバイスのためのユーザインターフェースを示している。

【図16】例示的な実施形態に係るオンライン支払を処理するためのクライアントデバイスのためのユーザインターフェースを示している。

30

【発明を実施するための形態】

【0014】

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。

40

【0015】

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

50

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。

【0016】

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。

【0017】

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。

【0018】

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。

【0019】

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。

【0020】

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。

【0021】

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

10

20

30

40

50

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。

【0022】

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スペースのシステム、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。

【0023】

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。

【0024】

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。

【0025】

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

10

20

30

40

50

びプロセッサ 124 を含み得る。図 1 B は、図 1 A 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。

【0026】

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 のカードリーダー（図示せず）に十分に近い非接触カード 105 を含み得る。

【0027】

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 などのリーダーは、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「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、ASCII 16 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）。

【0028】

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。

【0029】

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。

【0030】

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。

【0031】

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。

【0032】

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。

【0033】

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 1 A 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。

10

20

30

40

50

【0034】

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。

【0035】

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。

10

【0036】

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。

20

【0037】

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。

【0038】

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。

30

【0039】

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。

40

【0040】

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

50

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变化する数を備え得る。

10

【0041】

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スペースのシステム、コード分割マルチアクセススペースのシステム、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 などのうちの 1 つまたは複数を含み得る。

20

【0042】

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。

30

40

【0043】

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。

【0044】

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

50

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。

10

【0045】

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。

【0046】

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。

20

【0047】

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。

【0048】

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。

30

【0049】

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。

【0050】

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。

【0051】

40

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。

【0052】

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21

50

0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。

【0053】

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。

【0054】

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。

【0055】

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。

【0056】

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がカードリーダー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のカードリーダー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。

【0057】

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3

10

20

30

40

50

10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。

【0058】

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。

【0059】

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。

【0060】

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

システム、D-A-M-P-S、W-i-F-i、固定ワイヤレスデータ、I-E-E-E 802.11b、802.15.1、802.11nおよび802.11g、ブルートゥース（登録商標）、N-F-C、R-F-I-D、W-i-F-i、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、N-F-C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。

【0061】

さらに、ネットワーク315は、電話回線、光ファイバ、I-E-E-E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。

【0062】

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ー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。カードリーダー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、カードリーダー313は、非接触カード305と通信できる。

【0063】

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、N-F-C）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のカードリーダー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N-F-C範囲と一致していることを理解するであろう。

【0064】

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

【0065】

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、N-F-Cを介してクライアントデバイス310のカードリーダー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のカードリーダー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 3 1 1 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 3 2 5 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 3 1 1 がクライアントデバイス 3 1 0 にインストールされていない場合、カードリーダー 3 1 3 に対するカードのタップは、アプリケーション 3 1 1 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 3 1 1 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する。

10

【0066】

いくつかの実施形態によれば、非接触カード 3 0 5 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 3 1 1 は、クライアントデバイス 3 1 0 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 3 0 5 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。

【0067】

サーバ 3 2 0 は、データベース 3 3 5 と通信するウェブサーバを備え得る。サーバ 3 2 5 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 3 2 0 は、データベース 3 3 5 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 3 0 5 および／またはクライアントデバイス 3 1 0 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 3 2 5 は、非接触カード 3 0 5 および／またはクライアントデバイス 3 1 0 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。

20

【0068】

図 4 は、本開示の例による鍵多様化の方法 4 0 0 を示している。方法 4 0 0 は、図 2 で参照される送信デバイス 2 0 5 および受信デバイス 2 1 0 と同様の送信デバイスおよび受信デバイスを含み得る。

【0069】

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变化する数を備え得る。

30

40

【0070】

ブロック 4 1 0 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。

50

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。

【0071】

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。

【0072】

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。

【0073】

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。

【0074】

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。

【0075】

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。

【0076】

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。

【0077】

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。

10

20

30

40

50

【0078】

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。

【0079】

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。

【0080】

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。

【0081】

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。

【0082】

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も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。

【0083】

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

10

20

30

40

50

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。

10

【0084】

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）。

20

【0085】

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。

【0086】

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。

30

【0087】

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。

40

50

【0088】

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。

【0089】

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。

【0090】

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。

【0091】

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。

【0092】

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：D2760000850101；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。

【0093】

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=4838FB7DC

10

20

30

40

50

1 7 1 B 8 9 E ; M A C = < 計算された 8 バイト > が含まれる。

【 0 0 9 4 】

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 S T O R E D A T A (E 2) 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、E M B O S S ファイル (アプレット I D 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。

【 0 0 9 5 】

p U I D は、1 6 桁の B C D エンコード番号で構成される。いくつかの例では、p U I D は 1 4 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

【 0 0 9 6 】

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 (A P D U) 要求への応答を停止するように構成され得る。

【 0 0 9 7 】

1 つまたは複数のアプレットは、認証メッセージで使え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。

【0098】

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。

10

【0099】

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を判別される。

【0100】

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。

20

【0101】

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。

30

【0102】

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

40

50

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。

【0103】

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（AUTHKEYおよびENCKEY）は、個人化プロセス中にカードに格納され得る。

10

【0104】

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、AUTHKEY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、AUTHKEY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。

20

【0105】

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。

【0106】

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。

30

【0107】

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。

40

【0108】

50

いくつかの例では、E M V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。

【0109】

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。

【0110】

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、E M V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。

【0111】

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pNPR 915およびpDKI 920の値を検索するように構成できる。

【0112】

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-Auth 925およびCard-Key-DEK 930) に基づくセッション鍵を備え得る。セッション鍵 (Aut-Session-Key 935およびDEK-Session-Key 940) 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pATC 945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。

【0113】

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、pATC 945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、pATC 945が更新されるように構成され、カードマスター鍵Card-Key-AUTH 925およびCard-Key-DEK 930は、セッション鍵Aut-Session-Key 935およびDEK-Session-Key 940にさらに多様化される。p

10

20

30

40

50

A T C 9 4 5 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、p A T C カウンタ 9 4 5 は、個人化時または個人化の前に初期化され得、各 N D E F 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。

【0114】

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、p U I D 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、…の繰り返して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。

10

【0115】

認証メッセージは、16 進 A S C I I 形式のテキスト N D E F 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 M A C 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、M A C 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。

20

【0116】

M A C は、ファンクション鍵 (A U T - S e s s i o n - K e y) 9 3 5 によって実行され得る。暗号文で指定されたデータは、j a v a c a r d . s i g n a t u r e 方法：A L G _ D E S _ M A C 8 _ I S O 9 7 9 7 _ 1 _ M 2 _ A L G 3 で処理して、E M V A R Q C 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 A U T - S e s s i o n - K e y 9 3 5 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 M A C セッション鍵を多様化できる。以下で説明するように、A U T - S e s s i o n - K e y 9 3 5 は、M A C データ 9 5 0 に使用され得、結果として得られるデータまたは暗号文 A 9 5 5 および乱数 R N D は、D E K - S e s s i o n - K e y 9 4 0 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 9 6 0 を作成できる。

30

【0117】

いくつかの例では、最後の 16 (バイナリ、32 h e x) バイトが乱数のゼロ I V とそれに続く M A C 認証データを伴う C B C モードを使用する 3 D E S 対称暗号化を備えるように、1 つまたは複数の H S M 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、C a r d - K e y - D E K 9 3 0 から派生したセッション鍵 D E K - S e s s i o n - K e y 9 4 0 を備え得る。この場合、セッション鍵導出の A T C 値は、カウンタ p A T C 9 4 5 の最下位バイトである。

40

【0118】

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 A S C I I 「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
0 x 4 3 (メッセージ タイプ「A」)	バージョン	p A T C	R N D	暗号文 A (MAC)
暗号文 A (MAC)	8 バイト			
MAC				
2	8	4	4	1 8 バイト入力データ
バージョン	p U I D	p A T C	共有秘密	

10

メッセージ フォーマット				
1	2	4		1 6
0 x 4 3 (メッセージ タイプ「A」)	バージョン	p A T C		暗号文 B
暗号文 A (MAC)	8 バイト			
MAC				
2	8	4	4	1 8 バイト入力データ
バージョン	p U I D	p A T C	共有秘密	
暗号文 B	1 6			
S y m 暗号化				
8	8			
R N D	暗号文 A			

20

30

40

【 0 1 1 9 】

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、1 6 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	

10

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			

20

30

【0120】

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。

40

【0121】

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

50

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950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。

【0122】

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。

【0123】

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。

【0124】

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'0000000000000000'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。

【0125】

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。

【0126】

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。

10

【0127】

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。

【0128】

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。

20

【0129】

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Auth-Session-KeyおよびDEK-Session-Keyになる。

【0130】

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。

30

【0131】

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。

40

【0132】

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。

【0133】

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（Auth-Session-Key）の1つを使用してMACを生成できる。

【0134】

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

50

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せられ、第2のセッション鍵（DEK-Session-Key）を使用して暗号化される。

【0135】

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。

【0136】

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。

【0137】

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。

【0138】

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。

【0139】

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。

【0140】

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、組み合わせられたランダムデータは破棄され得る。

【0141】

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チ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チジェスチャは、ユーザによるデバイスへの非接触カードのタッチを備え得る。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チジェスチャを処理する

10

20

30

40

50

ように構成された任意の他のデバイスを備え得る。

【0142】

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iosk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。

10

【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。

【0144】

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。

20

30

【0145】

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。

40

50

【0146】

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。

10

【0147】

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。

20

【0148】

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）。

30

40

【0149】

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。

【0150】

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

50

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。

【0151】

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。

【0152】

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。

【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、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。

【0154】

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。

【0155】

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。

【0156】

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。

【0157】

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

10

20

30

40

50

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。

【0158】

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。

【0159】

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一または類似のコンポーネントを参照できる。

【0160】

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。

【0161】

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。

【0162】

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

10

20

30

40

50

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。

【0163】

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
10 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
20 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。

【0164】

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。

【0165】

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。

【0166】

いくつかの例では、本明細書に記載のシステムおよび方法は、例えば、FIDO2認証を開始するユーザの身元を検証することによって、FIDO2フレームワークを補足するために適用され得る。FIDO2フレームワークの脆弱性は、FIDO2認証プロセスを実行しようとしているユーザの身元である。資格情報の登録とFIDO2フレームワークを介した認証を試みるユーザが、認証を受けることを主張し、認証を受けることを承認されているユーザであることを確認することにより、FIDO2フレームワークのセキュリ
50

ティが向上し、承認されていないユーザが除外され得る。他の例では、本明細書で説明されるシステムおよび方法は、ウェブ認証、CTAP FIDO、または他の認証実施を補足するために適用され得る。本開示は、任意の認証実施に適用でき、本開示は、FIDO 2フレームワークに限定されないことが理解される。

【0167】

本明細書に記載されるように、本開示の実施形態は、非接触カードとクライアントデバイスとの間のデータ送信のためのシステムおよび方法を提供する。一実施形態では、非接触カードおよびクライアントデバイスのそれぞれは、マスター鍵を含み得る。非接触カードは、マスター鍵を使用して多様化された鍵を生成し、カウンタ値をクライアントデバイスに送信する前にカウンタ値を保護し得る。クライアントデバイスは、マスター鍵とカウンタ値に基づいて多様化された鍵を生成し得る。FIDO秘密鍵は、対応するFIDO公開鍵を含む、クライアントデバイスとサーバとの間のFIDOTランザクションを容易にし得る。さらなる例として、クライアントデバイスは、一意の公開鍵と秘密鍵のペアをランダムに生成し得、またはクライアントデバイスは、マスター鍵と利用可能な識別情報（例えば、サービスプロバイダに関連付けられたウェブサイトのサイト識別子）を使用して1つまたは複数の多様化された鍵を生成し得る。

【0168】

例示的な実施形態では、本明細書に開示されるデータ伝送システムは、FIDOシステムに実施され得る。FIDOシステムには、クライアントデバイスとサービスプロバイダに関連付けられたサーバが含まれ得る。クライアントデバイスは、FIDO秘密鍵を格納し得、サーバは、FIDO秘密鍵に関連付けられたFIDO公開鍵を格納し得る。例えば、ユーザがサービスプロバイダにアカウントを登録すると、クライアントデバイスは、FIDO公開鍵と秘密鍵のペアを生成し得る。クライアントデバイスは、FIDO秘密鍵を格納し得、FIDO公開鍵をサービスプロバイダのサーバに送信し得る。その後、ユーザは、例えば、FIDO秘密鍵を使用してチャレンジに署名することにより、アカウントにサインインし得る。サーバは、クライアントデバイスに署名するためのチャレンジを提供し得る。例えば、サーバは、長い乱数またはランダムな文字の長い文字列をユーザに提供し得る。クライアントデバイスは、乱数またはランダムな文字を受信し、FIDO秘密鍵を使用して署名し得る。次に、クライアントデバイスは、署名された乱数をサーバに送信し得る。

【0169】

サーバは、FIDO公開鍵を使用して署名されたチャレンジを確認し、署名されたチャレンジが元のチャレンジと一致する場合にのみ、ユーザがアカウントにアクセスできるようにし得る。例えば、サーバは、チャレンジの暗号化ハッシュを実行し、FIDO公開鍵を使用してハッシュを確認し得る。サーバがサーバに格納されているFIDO公開鍵を使用して長い乱数を確認し、乱数または文字がクライアントデバイスに送信されたものと同じになると、サーバは、ユーザにアクセスを許可し得る。そうでなければ、クライアントデバイス（またはユーザ）へのアクセスが拒否され得る。

【0170】

一例の実施形態では、FIDO秘密鍵は、この例ではFIDO認証器として機能し得るクライアントデバイスでロックされている。FIDO秘密鍵は、クライアントデバイスの安全な要素に格納し得、FIDO秘密鍵は、ユーザがクライアントデバイスでFIDO秘密鍵のロックを解除した後にのみ使用し得る。クライアントデバイスは、ユーザアクションによってFIDO秘密鍵のロックを解除し得る。例えば、ユーザアクションには、指のスワイプ、PINの入力、マイクへの話しかけ、第2の要素デバイスの挿入、ボタンの押下などがあり得る。第2の要素のデバイスは、非接触カードであり得る。いくつかの例では、サーバは、秘密鍵を完成させるために必要な情報を提供できるため、承認されていない方法でアクセスまたは生成された場合でも、秘密鍵を使用することはできない。この情報には、例えば、秘密鍵自体の一部、秘密鍵の生成に使用される母鍵の一部、またはサーバで使用可能なその他のデータが含まれ得る。いくつかの例では、秘密鍵は、サーバによ

って提供された情報に基づいて繰り返し生成され得る。他の例では、第2の要素デバイスからの入力が必要とする、または第2の要素デバイスの使用時にのみ（例えば、第2の要素デバイスを含むユーザアクションによって）ロック解除される情報が提供され得る。

【0171】

他の例示的な実施形態では、サーバは、カウンタ値をクライアントデバイスに送信し得る。例えば、サーバは、非接触カードのトランザクションを追跡し得る。非接触カードがトランザクションを実行するたびに、サーバは、カウンタ値を所定の数だけインクリメントし得る。非接触カードは、非接触カードがサーバに関連してトランザクションを実行するたびに、カウンタ値をインクリメントすることもし得る。FIDOトランザクション中、例えば、クライアントデバイスがチャレンジに署名する場合、サーバは、カウンタ値をクライアントデバイスに送信し得る。このように、非接触カードとクライアントデバイスは、暗号化されたFIDO秘密鍵を送受信するときに同じカウンタ値を有し得る。

【0172】

図13は、例示的な実施形態に係るデータ伝送システムを使用するFIDOシステム1300を示している。この例示的な実施形態では、FIDOシステム1300は、サーバ1310、クライアントデバイス1320、および非接触カード1330を含み得る。サーバ1310は、システムの様々なユーザのアカウント情報を格納するためのデータベースを含み得る。クライアントデバイス1320は、クライアントデバイス1320上で実行するための命令を備える1つまたは複数の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含み、実行し得る。これらは、システム1300の1つまたは複数のコンポーネントとの通信を可能にし、データを送信および／または受信し、本明細書に記載のクライアントデバイス機能を実行するように構成される。クライアントデバイス1320は、様々なネットワークに接続され、NFC技術を使用して通信を送受信できるスマートフォンであり得、本明細書に記載の機能を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含み得る。他の例では、クライアントデバイス1320は、ドングルであり得、さらなる例では、クライアントデバイス1320は、ネットワーク対応コンピュータであり得る。非接触カード1330は、プロセッサ、メモリ、および送信機を含み得、本明細書に記載の非接触カードの機能を実行し得る。サーバ1310は、例えば、インターネットなどのネットワークを介して、クライアントデバイス1320と通信し得る。クライアントデバイス1320は、NFC技術を使用して、非接触カード1330から信号を送受信し得る。非接触カード1330は、非接触カードに限定されず、いくつかの例では、クライアントデバイス1320と同じまたは類似のデバイスであり得ることが理解される。

【0173】

一例の実施形態では、ユーザは、クライアントデバイス1320のユーザインターフェース上のアプリケーションまたはウェブサイトにアクセスし得る。アプリケーションは、サインインページ1321を表示し得、これは、サインインボタン1322およびセットアップデバイス1323を含み得る。ユーザがボタン1322をタップすると、クライアントデバイス1320は、FIDO技術を使用してユーザにサインインし得る。ユーザがボタン1323をタップすると、クライアントデバイス1320は、ユーザアカウントをサービスプロバイダに登録するか、またはユーザアカウントに関連してクライアントデバイス1320に登録し得る。

【0174】

例示的な実施形態では、ユーザは、ボタン1323をタップし得る。それに応答して、クライアントデバイス1320は、FIDO鍵ペア、すなわち、FIDO秘密鍵とFIDO公開鍵を生成し得るFIDO認証器アプリケーションをアクティブ化し得る。例えば、FIDO鍵ペアをランダムに生成し得、マスター鍵とサービスプロバイダに関連付けられたIDを使用して1つまたは複数の多様化された鍵を生成し得る。他の例として、多様化された鍵は、マスター鍵とカウンタ値を使用して生成され得る。クライアントデバイス1320は、FIDO秘密鍵を格納し、インターネットなどのネットワークを使用して、F

10

20

30

40

50

FIDO公開鍵をサーバ1310に送信し得る。サーバ1310がFIDO公開鍵を受信すると、サーバ1310は、ユーザのアカウントに関連付けられて、FIDO公開鍵をデータベースに格納し得る。

【0175】

例示的な実施形態では、ユーザは、ボタン1322をタップし得る。それに応答して、クライアントデバイス1320は、署名のためのチャレンジを要求するためにサーバ1310に信号を送信し得る。サーバ1310は、チャレンジをクライアントデバイス1320に送信し得る。チャレンジは、例えば、乱数の文字列であり得る。クライアントデバイス1320はまた、非接触カード1330に信号を送信して、非接触カード1330からの認証を要求し得、認証を受信すると、クライアントデバイス1320は、認証をサーバ1310に中継し得る。クライアントデバイス1320によってサーバ1310から応答を受信すると、クライアントデバイス1320に格納されたFIDO秘密鍵は、ロック解除され得る。

10

【0176】

いくつかの例では、プロキシ認証器をクライアントデバイス1320上に作成し得る。例えば、プロキシ認証器は、認証プロセスを開始し、サーバ1310との通信を確立するために、非接触カード1330をクライアントデバイス1320にタップするようにユーザに促し得る。次に、サーバ1310は、必要な任意の認証プロセスを実行し、認証プロセスの結果をクライアントデバイス1320に送信し得る。クライアントデバイス1320は、サーバ1310との相互作用なしにクライアントデバイス1320によって生成されたかのように結果を提示し得、それにより、プロキシ認証器として機能し得る。このプロセスは、サーバ1310に格納された1つまたは複数のFIDO秘密鍵のロックを解除するために使用し得る。チャレンジが受信された場合、クライアントデバイス1320は、チャレンジをサーバ1310に渡して秘密鍵を見つけ、適切な公開鍵／秘密鍵のペアまたはチャレンジに必要な公開鍵を生成し得る。

20

【0177】

クライアントデバイス1320が、FIDO秘密鍵を使用してチャレンジを受信すると、クライアントデバイス1320は、例えば、乱数の文字列を暗号化するなど、チャレンジに署名し得る。クライアントデバイス1320は、署名されたチャレンジをサーバ1310に送信し得る。サーバ1310は、FIDO公開鍵を使用して署名されたチャレンジを確認し得る。確認されたチャレンジがクライアントデバイス1320に送信されたチャレンジと同じである場合、サーバ1310は、クライアントデバイス1320（またはクライアントデバイス1320のユーザ）を認証し得る。確認されたチャレンジがクライアントデバイス1320に送信されたチャレンジと同じでない場合、サーバ1310は、クライアントデバイス1320がサーバ1310（または他のデバイス）にアクセスすることを妨げ得る。

30

【0178】

例示的な実施形態では、データ送信システムは、銀行によって使用されて、ユーザのオンライン支払いを処理し得る。銀行は、サーバを操作でき、ユーザは、ユーザのタブレットでオンライン支払いを要求し得る。また、ユーザは、銀行が発行した非接触カードを所有し得る。銀行が非接触カードを発行すると、サーバは、ユーザにFIDO鍵のペアを発行する。鍵のペアには、FIDO秘密鍵とFIDO公開鍵が含まれる。サーバは、FIDO公開鍵を保存するが、サーバは、非接触カードにFIDO秘密鍵を格納する。タブレットは、1つまたは複数のソフトウェアアプリケーションを含み得、インターネットを介してサーバと通信し得る。タブレットは、NFCプロトコルを使用して非接触カードと信号を送受信することもし得る。オンライン取引のセキュリティを強化するために、銀行は、特定の取引、例えば、所定の支払い額を超える支払いを必要とする取引について、顧客に顧客の身元を検証するように要求し得る。検証は、FIDO技術を使用して行い得る。いくつかの例では、FIDO公開鍵が非接触カードに関連付けられ得る。これらの例では、母秘密鍵、または固定秘密鍵を、例えば、サーバやタブレットなどFIDO認証器を実装

40

50

するデバイスに格納し得る。

【0179】

図14は、オンライン支払いを処理するための例示的なフローチャート1400を示している。ステップ1410で、トランザクションは、ユーザのタブレットで開始され得る。例えば、ユーザが第3者のウェブサイトにアクセスして、ダイヤモンドネックレスを注文し得る。ステップ1420で、タブレットは、ユーザの非接触カード情報（例えば、口座番号、口座所有者名、口座所有者住所、セキュリティコード、一意のカード識別子）および／またはトランザクション情報（例えば、金額、商人名、商人の場所、購入した商品またはサービスの日付、時刻）を第3者に送信し得、トランザクションの支払いを処理し得る。第3者は、支払いの承認のために銀行に連絡し得る。この例示的な実施形態では、ダイヤモンドネックレスの価格は、ユーザによるオンライン支払いのために規定された閾値を超え、銀行は、銀行が支払いを処理する前に、ユーザにユーザの身元を検証することを要求し得る。この閾値は、銀行またはユーザが規定し得る。

10

【0180】

ステップ1430で、タブレットは、銀行のサーバから、ユーザの身元を検証するためのチャレンジを受信し得る。それに応答して、ステップ1440で、タブレットに格納されたアプリケーション（例えば、タブレットにインストールされた銀行のアプリケーション）は、ウィンドウをポップアップし、ユーザに非接触カードをタップするように要求し得る。ステップ1450で、ユーザは、非接触カードをタブレットにタップし得、そうすることで、タブレットは、FIDO秘密鍵を使用する許可を与えられ得る。ステップ1460で、タブレットは、FIDO秘密鍵を使用してチャレンジに署名し得、ステップ1470で、タブレットは、署名されたチャレンジをサーバに送信し得る。署名されたチャレンジを受信することに応答して、サーバは、ステップ1480で、ユーザの身元を確認し、支払いを承認し得る。支払いが承認されると、サーバは、第3者にメッセージを送信し得る。ステップ1490で、タブレットは、トランザクションが処理されたことを示すメッセージを第3者から受信し得る。

20

【0181】

図15は、オンライン支払いを処理するためのクライアントデバイス1320の例示的なユーザインターフェースを示している。この例示的な実施形態では、クライアントデバイス1320は、チェックアウトページ1510を表示するタブレットである。このページには、ユーザが選択したダイヤモンドネックレスと商品の価格が表示され得る。ページ1510は、ユーザのクレジットカード情報を入力するためのフィールド1520を含み得る。ページ1510はまた、トランザクションを処理するためのボタン1530を含み得る。ユーザがボタン1530をタップすると、タブレットは、クレジットカード情報を第3者ベンダーに送信し得る。この例では、取引金額が閾値を超えているため、銀行は、ユーザに取引の検証を要求し得る。

30

【0182】

図16は、オンライン支払いを検証するためのクライアントデバイス1320の例示的なユーザインターフェースを示している。この例示的な実施形態では、第3者が支払いを処理するために銀行に連絡した後、銀行のサーバは、トランザクションを検証するためにクライアントデバイスまたはタブレット1320にメッセージまたは通信を送信し得る。メッセージまたは通信は、チャレンジを含み得、タブレット1320上でユーザの非接触カード1330をタップするようにユーザに求めるプロンプト1610を表示するようにタブレット1320に促し得る。続いて、ユーザは、タブレット1320上で非接触カード1330をタップし得、前述のように、非接触カード1330は、暗号化されたFIDO秘密鍵をタブレット1320に送信し得る。タブレット1320は、多様化された鍵を生成し得、多様化された鍵を使用することは、暗号化されたFIDO秘密鍵を復号し得る。タブレット1320がFIDO秘密鍵を所有すると、タブレット1320は、チャレンジに署名し、銀行のサーバに送信し得る。

40

【0183】

50

一例の実施形態では、タブレット1320は、銀行に関連するアプリケーションを含み得る。アプリケーションは、様々な銀行口座情報をユーザに表示し得る。例えば、アプリケーションは、ユーザが銀行で保持している各口座の口座残高を表示し得る。アプリケーションは、銀行サーバから通信またはメッセージを受信し、タブレット上でユーザにプロンプトを表示することもし得る。通信には、タブレットに表示されるチャレンジとメッセージが含まれ得る。アプリケーションが銀行サーバから通信を受信すると、アプリケーションは、タブレット1320の画面上にプロンプトまたはウィンドウを表示し得る。プロンプトまたはウィンドウは、タブレット1320に表示されている他のウィンドウまたはページに重ね合わせ得る。

【0184】

本開示は、FIDOフレームワークへの厳密な準拠に限定されず、この開示は、このフレームワークの変形を包含することが理解される。いくつかの例示的な実施形態では、FIDO公開鍵秘密鍵ペアがFIDO認証器上で生成され得るが、他の組み合わせも可能である。例えば、サーバがFIDO公開鍵秘密鍵ペアを生成することが可能であり、サーバは、例えば、ユーザがクライアントデバイスを登録したり、アカウントを開設したりする場合などに、FIDO秘密鍵を認証器に送信し得る。他の例として、FIDO公開鍵秘密鍵ペアを非接触カードに格納し得る。必要に応じて、FIDO認証器は、FIDO公開鍵またはFIDO秘密鍵を取得し得る。例えば、クライアントデバイスは、FIDO公開鍵をサーバに送信してクライアントデバイスを登録し得、サーバがクライアントデバイスにチャレンジを送信するときに、クライアントデバイスは、FIDO秘密鍵を取得し得る。他の例として、非接触カードから認証承認を受け取ると、FIDO認証器自体が署名チャレンジを続行しおよび／またはFIDO登録の完了に必要な公開鍵を提供し得る。

【0185】

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。

【0186】

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つまたは複数を含むことを意図している。

【0187】

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。

【0188】

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。

10

20

30

40

50

【0189】

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に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。

【0190】

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る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。

10

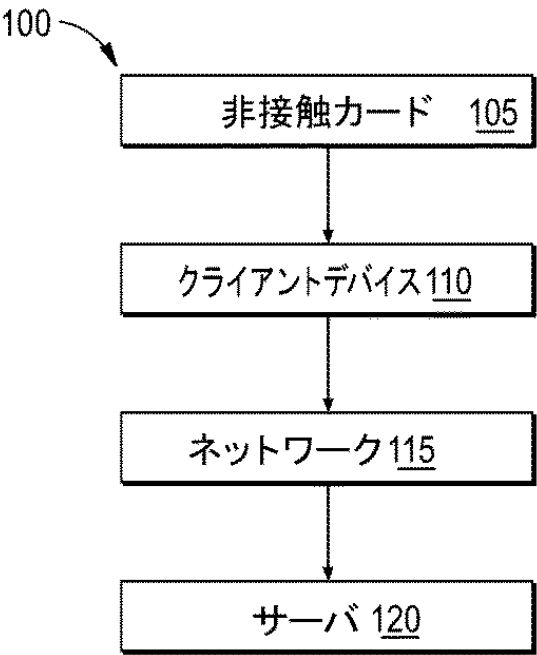
20

30

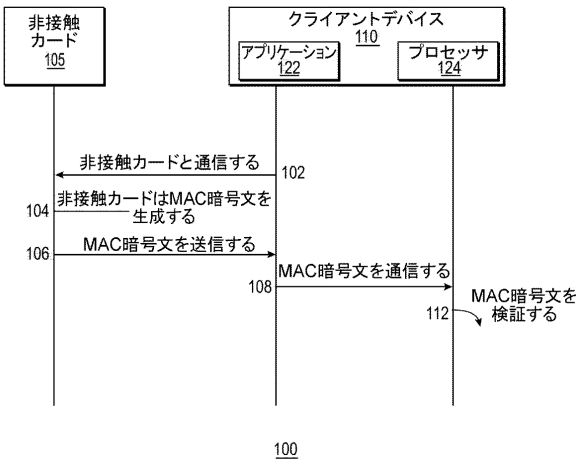
40

50

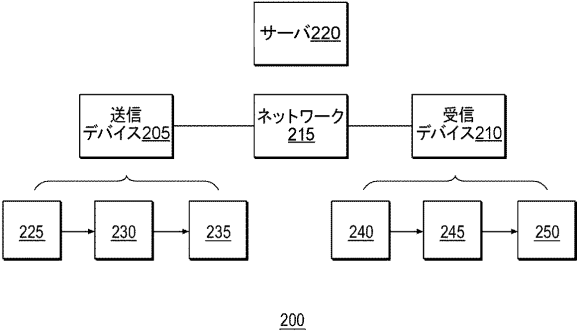
【図面】
【図 1 A】



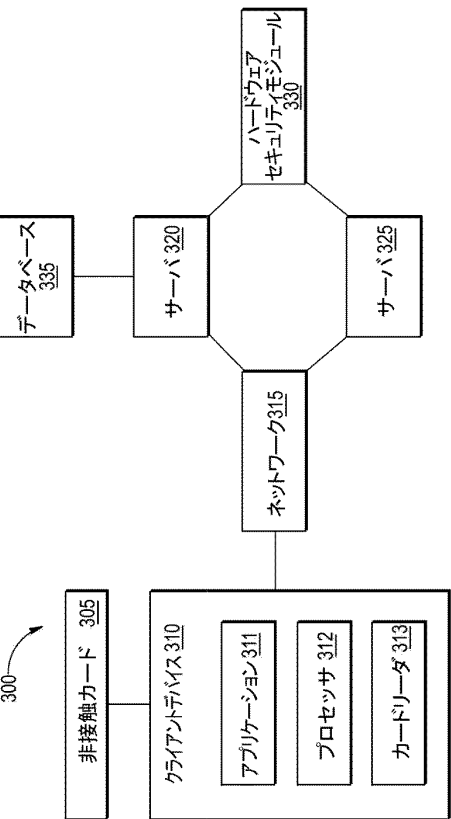
【図 1 B】



【図 2】



【図 3】



10

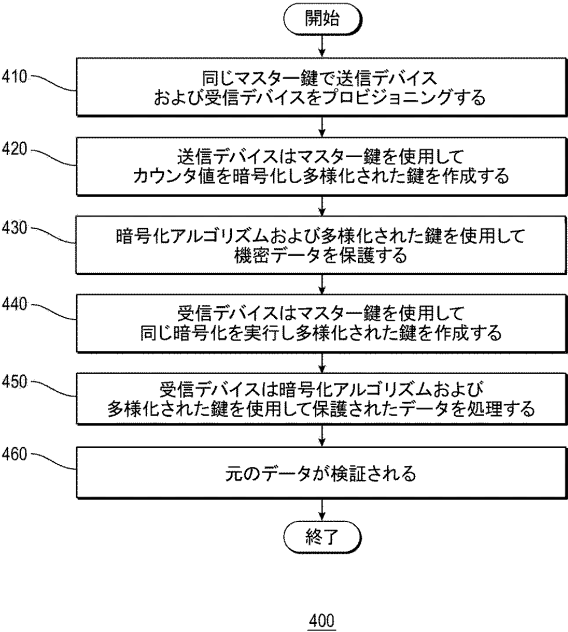
20

30

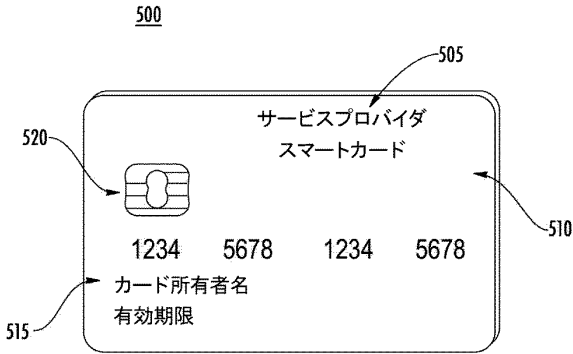
40

50

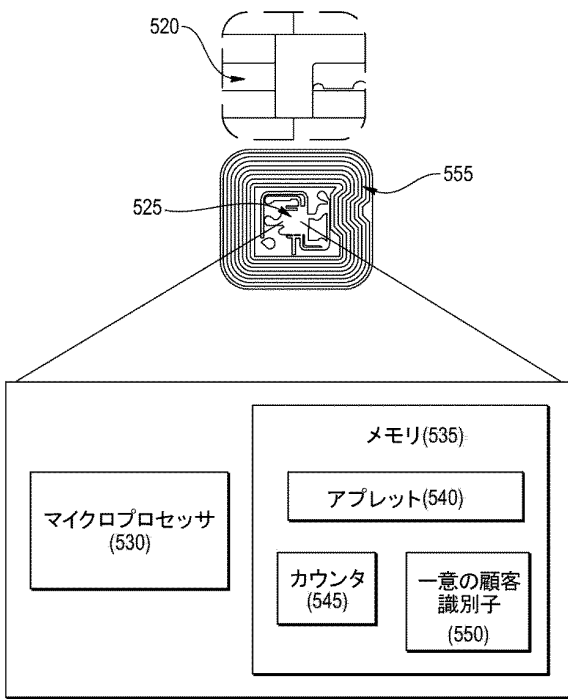
【図 4】



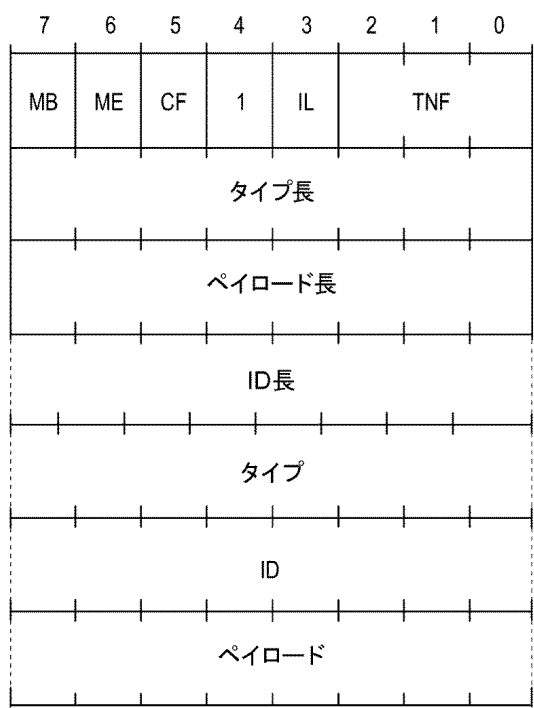
【図 5 A】



【図 5 B】



【図 6】



【図 7】

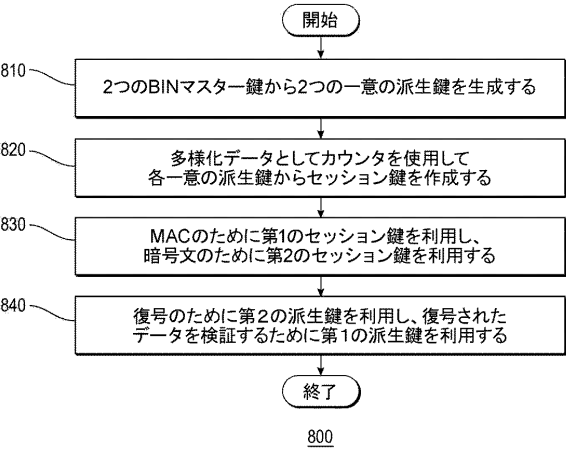
00 D1 (メッセージ開始、メッセージ終了、ショートコード、ID無し) 01 (拡張されているタイプ) 01 01 (ランダムタイプ)
02 <ランダムIDと ENU を含むペイロード長、またはコンテナ長+3> = 45+3 = 48 (DEC)
03 54 (T)
04 02 (ランダムID)
05 65 6E (言語長、en)
07 43 01 00 76 a6 62 7b 67 a8 cf bb <8mac>バイト>
D101305402656E 43010076A6627B67A8CFBB <8mac>バイト>

710

バージョン	pUID (8)	pATC	暗号化された暗号文 (16)
0100	001538655536061	00000050	7D28B8B9D868E5143153AC3C84E5A6
復号された暗号文 ランダム (8)			
4636F70C71B88E			
MAC (8)			
C3F3F398C56DA0BF1			
MAC (4) = pUID (2) + pATC (2) + pUID (8) + pATC (4) + pUID (8) + pATC (4) + pUID (8) + pATC (4)			

720

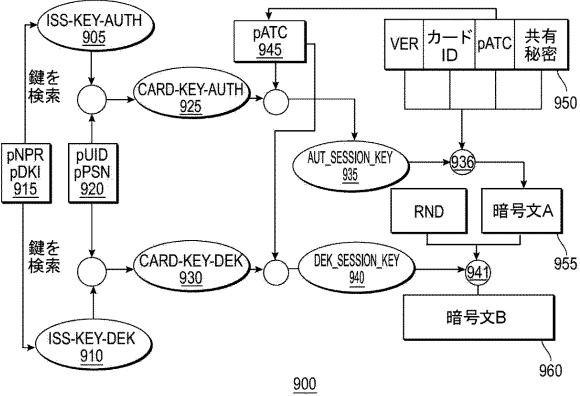
【図 8】



10

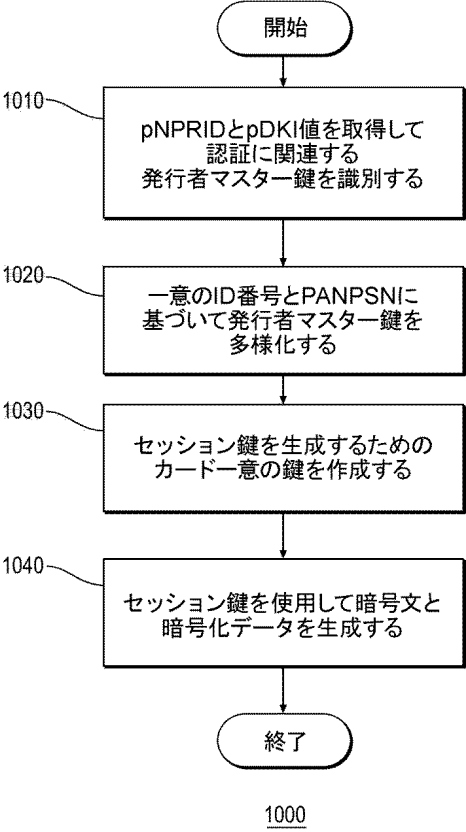
20

【図 9】



900

【図 10】

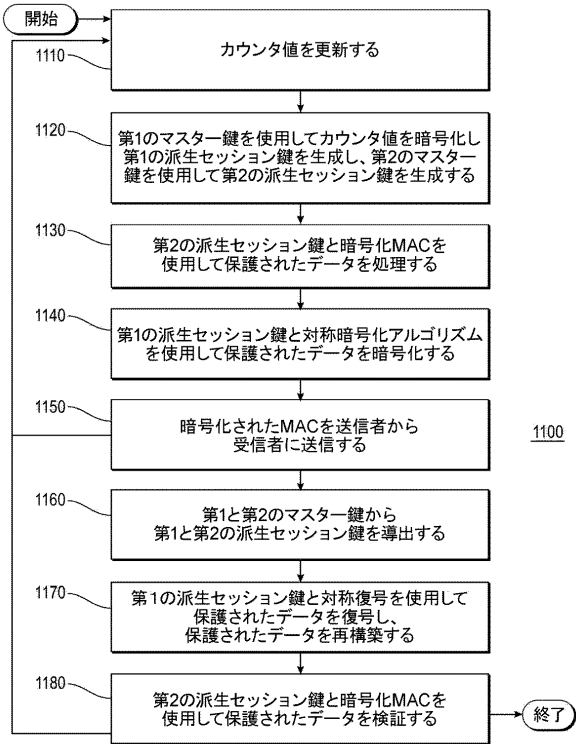


1000

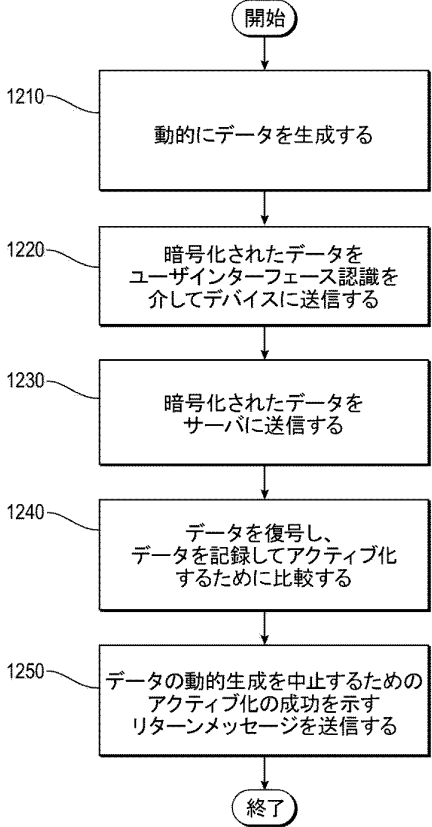
40

50

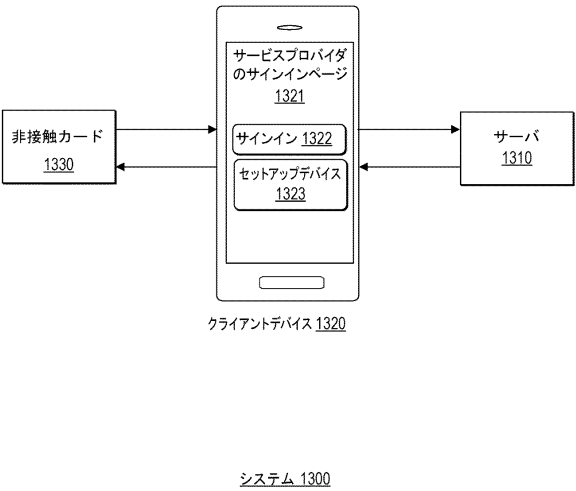
【図 1 1】



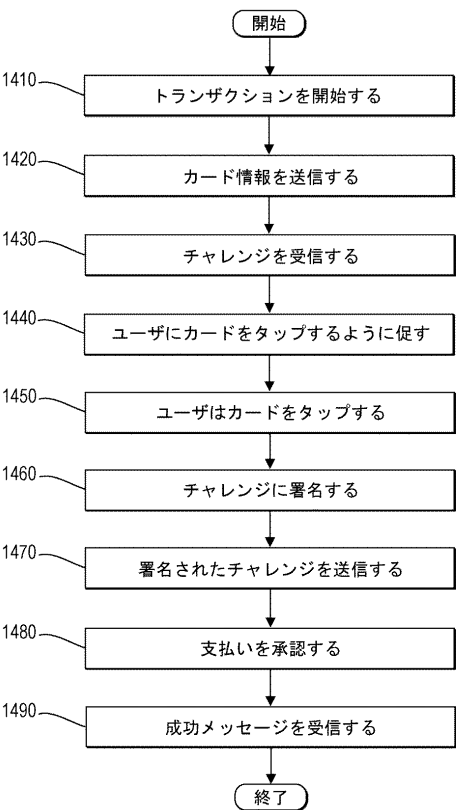
【図 1 2】



【図 1 3】

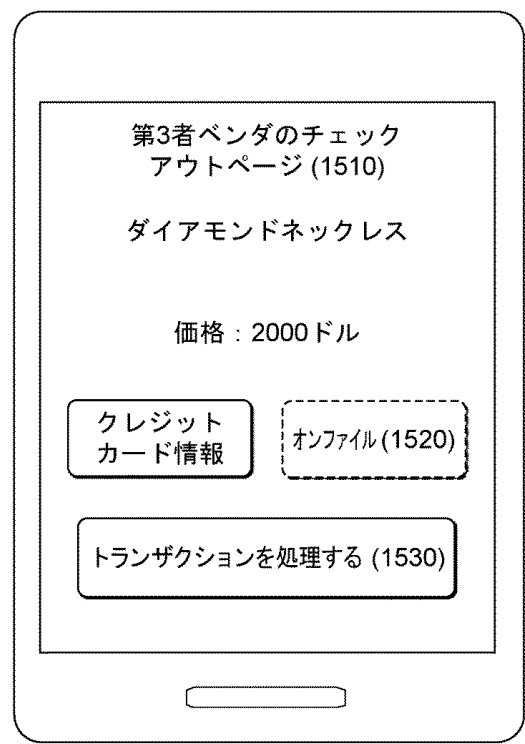


【図 1 4】



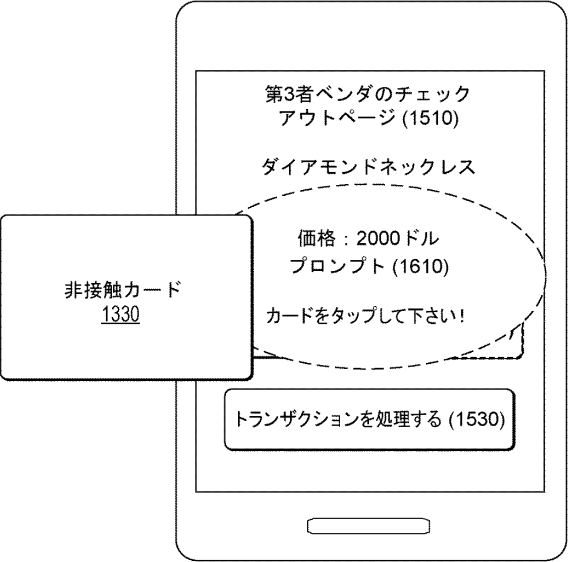
1400

【図 1 5】



クライアントデバイス 1320

【図 1 6】



クライアントデバイス 1320

10

20

30

40

50

フロントページの続き

(33)優先権主張国・地域又は機関

米国(US)

(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)

前置審査

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

(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

審査官 中里 裕正

(56)参考文献 特開2003-242149(JP, A)

特表2009-514262(JP, A)

特開2011-155495(JP, A)

特開2016-186687(JP, A)

特開2018-137587(JP, A)

米国特許出願公開第2015/0348026(US, A1)

米国特許第09935953(US, B1)

(58)調査した分野 (Int.Cl., DB名)

H04L 9/32

H04L 9/14

G06F 21/32