

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号
特表2025-519121
(P2025-519121A)

(43)公表日 令和7年6月24日(2025.6.24)

(51)国際特許分類
G 0 6 F 21/34 (2013.01)
G 0 6 F 8/65 (2018.01)

F I
G 0 6 F 21/34
G 0 6 F 8/65

テーマコード (参考)
5 B 3 7 6

審査請求 未請求 予備審査請求 未請求 (全36頁)

(21)出願番号	特願2024-569354(P2024-569354)	(71)出願人	519111877 キャピタル・ワン・サービシーズ・リミ テッド・ライアビリティ・カンパニー Capital One Service s, L L C 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
(86)(22)出願日	令和5年4月24日(2023.4.24)	(74)代理人	100145403 弁理士 山尾 憲人
(85)翻訳文提出日	令和7年1月21日(2025.1.21)	(74)代理人	100135703 弁理士 岡部 英隆
(86)国際出願番号	PCT/US2023/019567	(74)代理人	100163902 弁理士 市川 奈月
(87)国際公開番号	WO2023/229768	(72)発明者	ルッツ, ウェイン
(87)国際公開日	令和5年11月30日(2023.11.30)		
(31)優先権主張番号	17/664,460		
(32)優先日	令和4年5月23日(2022.5.23)		
(33)優先権主張国・地域又は機関	米国(US)		
(81)指定国・地域	AP(BW,CV,GH,GM,KE,LR,LS,MW,MZ ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW), EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES, FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV 最終頁に続く		最終頁に続く

(54)【発明の名称】 非接触カードを使用する装置のアプリケーションの設定

(57)【要約】

非接触カードを使用して装置上のアプリケーションを設定するシステム、方法、装置、およびコンピュータ可読媒体。装置で実行されるアプリケーションは、アカウントに関連付けられた非接触カードから暗号を受信し得る。アプリケーションは暗号をサーバに送信し得る。アプリケーションは、暗号に基づいて、アカウントに関連付けられた複数のアプリケーションの設定情報を受信し得る。アプリケーションは、設定情報に基づいて、装置上の各アプリケーションのそれぞれの設定を変更し得る。

【選択図】 図 1 A

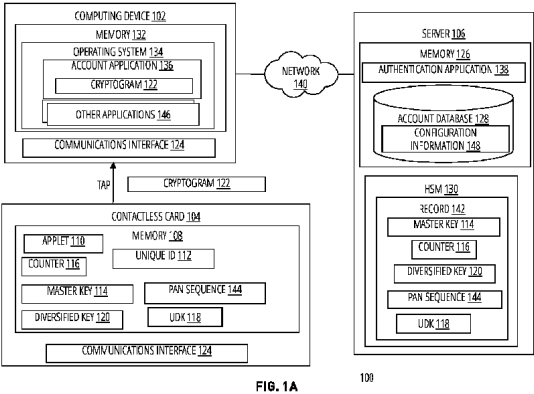


FIG. 1A

109

【特許請求の範囲】**【請求項 1】**

装置で実行されるアプリケーションによって、アカウントに関連付けられる非接触カードから暗号化されたデータを受信することと、

前記アプリケーションによって、前記暗号化されたデータをサーバに送信することと、

前記アプリケーションによって、前記暗号化されたデータに基づいて、前記アカウントに関連付けられる複数のアプリケーションの設定情報を受信することと、

前記設定情報に基づいて、前記装置の各アプリケーションの各設定を変更することと、を含む方法。

【請求項 2】

各アプリケーションを変更する前に、

前記アプリケーションによって、前記複数のアプリケーションのうちの第 1 アプリケーションが前記装置にインストールされていないことを決定することと、

前記アプリケーションによって、前記第 1 アプリケーションを前記装置にダウンロードすることと、

前記装置のオペレーティングシステム（OS）によって、前記第 1 アプリケーションを前記装置にインストールすることと、

をさらに含む、請求項 1 に記載の方法。

【請求項 3】

前記装置に前記第 1 アプリケーションをインストールした後に、

前記第 1 アプリケーションの設定情報に基づいて、前記第 1 アプリケーションの設定を変更すること

をさらに含む、請求項 2 に記載の方法。

【請求項 4】

前記設定情報を受信することは、前記サーバから複数の設定ファイルを受信することを含む、請求項 1 に記載の方法。

【請求項 5】

前記設定情報を受信することは、

各アプリケーションによって、前記サーバから各プッシュ通知を受信することを含み、

前記各プッシュ通知は、前記各アプリケーションの前記各設定情報を含み、

前記プッシュ通知は、バックグラウンド通知を含む、請求項 1 に記載の方法。

【請求項 6】

前記設定情報を受信することは、

各アプリケーションによって、前記サーバから各プッシュ通知を受信することであって、前記各プッシュ通知は、各トークンを含み、前記プッシュ通知は、バックグラウンド通知を含む、受信することと、

前記各アプリケーションによって、前記各トークンを前記サーバに送信することと、

前記各アプリケーションによって、前記各トークンに基づいて、前記各設定情報を受信することと、

を含む請求項 1 に記載の方法。

【請求項 7】

前記設定情報は、（i）1 つ以上のサーバに接続するための情報、（ii）アカウント情報、（iii）メッセージ、（iv）嗜好（preferences）、および（v）設定（settings）を含む、

請求項 1 に記載の方法。

【請求項 8】

非一過性のコンピュータ可読記憶媒体であって、装置のプロセッサによって実行されると、前記プロセッサに、

アプリケーションによって、アカウントに関連付けられる非接触カードから暗号化されたデータを受信することと、

10

20

30

40

50

前記アプリケーションによって、前記暗号化されたデータをサーバに送信することと、
前記アプリケーションによって、前記暗号化されたデータに基づいて、前記アカウント
に関連付けられる複数のアプリケーションの設定情報を受信することと、
前記設定情報に基づいて、前記装置の各アプリケーションの各設定を変更することと、
を実行させる命令を含む、非一過性のコンピュータ可読記憶媒体。

【請求項 9】

前記命令は、前記各アプリケーションの前記設定を変更する前に、前記プロセッサに、
前記アプリケーションによって、前記複数のアプリケーションのうちの第 1 アプリケー
ションが前記装置にインストールされていないことを決定することと、
前記アプリケーションによって、前記第 1 アプリケーションを前記装置にダウンロード
することと、

10

前記装置のオペレーティングシステム（OS）によって、前記第 1 アプリケーションを
前記装置にインストールすることと、
をさらに実行させる請求項 8 に記載のコンピュータ可読記憶媒体。

【請求項 10】

前記命令は、前記装置に前記第 1 アプリケーションをインストールした後に、
前記プロセッサに、前記第 1 アプリケーションの設定情報に基づいて、前記第 1 アプリ
ケーションの設定を変更すること
をさらに実行させる請求項 9 に記載のコンピュータ可読記憶媒体。

【請求項 11】

20

前記設定情報を受信することは、前記サーバから複数の設定ファイルを受信すること
を含む、請求項 9 に記載のコンピュータ可読記憶媒体。

【請求項 12】

前記設定情報を受信することは、各アプリケーションによって、前記サーバから各プッ
シュ通知を受信することを含み、前記各プッシュ通知は、前記各アプリケーションに対す
る前記各設定情報を含み、プッシュ通知は、バックグラウンド通知を含む、
請求項 8 に記載のコンピュータ可読記憶媒体。

【請求項 13】

前記設定情報を受信することは、
各アプリケーションによって、前記サーバから各プッシュ通知を受信することであって
、前記各プッシュ通知は、各トークンを含み、前記プッシュ通知は、バックグラウンド通
知を含む、受信することと、
前記各アプリケーションによって、前記各トークンを前記サーバに送信することと、
前記各アプリケーションによって、前記各トークンに基づいて、前記各設定情報を受信
することと、を含む、
請求項 8 に記載のコンピュータ可読記憶媒体。

30

【請求項 14】

前記設定情報は、(i) 1 つ以上のサーバに接続するための情報、(ii) アカウント情
報、(iii) メッセージ、(iv) 嗜好、および (v) 設定を含む、
請求項 8 に記載のコンピュータ可読記憶媒体。

40

【請求項 15】

プロセッサと、メモリとを備えるコンピュータ装置であって、
前記メモリは、前記プロセッサによって実行されると、前記プロセッサに、
アプリケーションによって、アカウントに関連付けられる非接触カードから暗号化さ
れたデータを受信することと、
前記アプリケーションによって、前記暗号化されたデータをサーバに送信しすること
と、

前記アプリケーションによって、前記暗号化されたデータに基づいて、前記アカウン
トに関連付けられる複数のアプリケーションの設定情報を受信することと、
前記設定情報に基づいて、前記コンピュータ装置の各アプリケーションの各設定を変

50

更することと、

を実行させる命令を格納する、
コンピュータ装置。

【請求項 16】

前記命令は、前記各アプリケーションの前記設定を変更する前に、前記プロセッサに、
さらに、

前記アプリケーションによって、前記複数のアプリケーションのうちの第1アプリケーションが前記装置にインストールされていないことを決定することと、

前記アプリケーションによって、前記第1アプリケーションを前記装置にダウンロード
することと、

前記装置のオペレーティングシステム（OS）によって、前記第1アプリケーションを
前記装置にインストールすることと、

を実行させる、請求項15に記載のコンピュータ装置。

【請求項 17】

前記命令は、さらに、前記第1アプリケーションをインストールした後に、

前記第1アプリケーションの設定情報に基づいて、前記第1アプリケーションの設定を
変更するように前記装置を実行する、請求項16に記載のコンピュータ装置。

【請求項 18】

前記設定情報を受信することは、前記サーバから複数の設定ファイルを受信することを含
む、請求項15に記載のコンピュータ装置。

【請求項 19】

前記設定情報を受信することは、各アプリケーションによって、前記サーバから各プッ
シュ通知を受信することを含み、前記各プッシュ通知は、前記各アプリケーションに対す
る前記各設定情報を含み、プッシュ通知は、バックグラウンド通知を含む、

請求項15に記載のコンピュータ装置。

【請求項 20】

前記設定情報を受信することは、

各アプリケーションによって、前記サーバから各プッシュ通知を受信することであって
、前記各プッシュ通知は、各トークンを含み、前記プッシュ通知は、バックグラウンド通
知を含む、受信することと、

前記各アプリケーションによって、前記各トークンを前記サーバに送信することと、

前記各アプリケーションによって、前記各トークンに基づいて、前記各設定情報を受信
することと、を含む、

請求項15に記載のコンピュータ装置。

【発明の詳細な説明】

【技術分野】

【0001】

本出願は、2022年5月23日に提出された「非接触カードを使用する装置のアプリケー
ションの設定」と題する米国特許出願番号17/664,460の優先権を主張する。前記出願
の内容は、参照によりその全体が本明細書に援用される。

【背景技術】

【0002】

新しい装置や追加の装置を設定は、面倒で時間がかかり、エラーが発生しやすい。例え
ば、ユーザは、他の装置を置き換えるために、新しい装置を購入するかもしれない。しか
し、新しい装置には、他の装置のアプリケーションや構成を含まない。

【発明の概要】

【0003】

非接触カードを使用して装置上のアプリケーションを設定するシステム、方法、装置、
およびコンピュータ可読媒体である。一態様では、方法は、装置上で実行されるアプリケ
ーションによって、アカウントに関連付けられた非接触カードから暗号を受信することと

10

20

30

40

50

、アプリケーションによって、暗号をサーバに送信することと、暗号に基づいて、アプリケーションによって、アカウントに関連付けられた複数のアプリケーションの設定情報を受信することと、設定情報に基づいて、装置上の各アプリケーションの各設定を変更することを含む。

【図面の簡単な説明】

【0004】

【図1A】図1Aは、一実施形態による主題の態様を示す図である。

【図1B】図1Bは、一実施形態による主題の態様を示す図である。

【図1C】図1Cは、一実施形態による主題の態様を示す図である。

【図1D】図1Dは、一実施形態による主題の態様を示す図である。

10

【図2A】図2Aは、一実施形態による主題の態様を示す図である。

【図2B】図2Bは、一実施形態による主題の態様を示す図である。

【図2C】図2Cは、一実施形態による主題の態様を示す図である。

【図2D】図2Dは、一実施形態による主題の態様を示す図である。

【図3】図3は、一実施形態によるルーチン300を示す図である。

【図4】図4は、一実施形態によるルーチン400を示す図である。

【図5】図5は、一実施形態によるルーチン500を示す図である。

【図6A】図6Aは、一実施形態による非接触カード104を示す。

【図6B】図6Bは、一実施形態による非接触カード104を示す。

【図7】図7は、一実施形態によるデータ構造700を示す図である。

20

【図8】図8は、一実施形態によるコンピュータアーキテクチャ800を示す。

【発明を実施するための形態】

【0005】

特定の要素や行為に関する議論を容易に識別するため、参照番号の最上位桁または数字は、その要素が最初に登場する図番号を指す。

【0006】

本明細書に開示される実施形態は、非接触カードを使用して、スマートフォン、タブレット、またはその他のコンピュータ装置などの装置を自動的に設定する安全な技術を提供する。装置を構成する例としては、装置にアプリケーションをインストールすること、装置からアプリケーションをアンインストールすること、および／または装置にアプリケーションを設定すること（例えば、アプリケーション設定、アプリケーションパラメータなどを変更すること）を含む。最初に、ユーザは、1つ以上のアプリケーションおよび／または1つ以上のアプリケーションの設定情報を登録できる。そうすることは、所定の装置および／またはアカウントの情報をアカウントデータベースに格納することを含む場合がある。登録は、アプリケーションおよび／または設定情報を非接触カードに関連付けてもよい。

30

【0007】

その後、ユーザは、以前に登録された装置、新しい装置、既存の装置などを含み得る任意の装置に対して、非接触カードをタップできる。一部の実施形態では、装置にカードをタップすると、カードが暗号を生成する場合がある。いくつかの実施形態では、暗号は、ユニフォームリソースロケータ（URL）のパラメータである。装置がURLおよび／または暗号を受信すると、装置はアプリケーションを起動し、検証のために暗号をサーバに送信できる。サーバは、暗号の解読に少なくとも部分的に基づいて暗号を検証する。

40

【0008】

他の実施形態では、装置にカードをタップすることにより、装置がURLに基づいてウェブブラウザを起動する場合がある。このような実施形態では、ウェブブラウザは、URLに関連付けられたページにアクセスできる。サーバは、ウェブブラウザがアクセスしたURLのパラメータとして暗号を識別する。サーバは、少なくとも部分的に暗号の解読に基づいて暗号を検証できる。

【0009】

50

装置へのカードのタップに応答して起動されるアプリケーションに関係なく、暗号を検証した後、サーバは暗号（および／または暗号のパラメータ）を使用して、アカウントデータベース内の関連アプリケーションおよび／またはアプリケーションの設定情報を識別できる。いくつかの実施形態では、サーバは、1つ以上のプッシュ通知を介して設定情報を装置に送信する。設定情報が閾値を超えるサイズを有する場合など、いくつかの実施形態では、サーバは、1つ以上のトークンを装置に送信してもよい。

【0010】

一度受信されると、装置は、受信された設定情報を各アプリケーションに適用できる。例えば、設定情報は、アカウントのログイン認証情報、1つ以上のサーバへの接続を確認するためのサーバ情報、ユーザの嗜好、設定などを含むことができる。一部の実施形態では、設定情報は、装置にインストールされていない1つ以上のアプリケーションの情報を含む場合がある。このような実施形態では、これらのアプリケーションは、設定情報の受信に基づいて装置にダウンロードおよびインストールされる場合がある。同様に、設定情報は、既存のアプリケーションを無効化またはアンインストールするための情報を含んでもよい。このような実施形態では、装置は、設定情報に基づいて、これらのアプリケーションを無効化および／またはアンインストールしてもよい。

【0011】

有利なことに、本明細書で開示される実施形態は、非接触カードを使用して装置を自動的に設定する安全な技術を提供する。設定を開始するために暗号検証を要求することにより、ユーザのアカウント、アプリケーション、装置、およびデータのセキュリティが向上する。さらに、このようにすることで、ユーザがサーバとの暗号検証を容易にする非接触カードにアクセスできる場合にのみ、装置の自動設定が実行されることが保証される。さらに、開示された自動設定機能を提供することにより、すべてのアプリケーション、オペレーティングシステム、および／または装置への統合を必要とすることなく、多くの異なるアプリケーション、オペレーティングシステム、および／または装置を自動的に設定できる。

【0012】

本明細書で使用される表記および命名法を一般的に参照すると、本明細書の詳細な説明は、コンピュータまたはコンピュータのネットワーク上で実行されるプログラム手順の観点から提示される場合がある。

【0013】

手順とは、ここでは、そして一般的には、所望の結果を導く自己整合的な一連の操作であると考えられる。これらの操作は、物理量の物理的操作を必要とする。必ずしも必要ではないが、通常、これらの量は、記憶、転送、結合、比較、その他の操作が可能な電気信号、磁気信号、光学信号の形をとる。このような信号をビット、値、要素、記号、文字、用語、数字などと呼ぶのは、主に一般的な用法から便利な場合がある。

【0014】

さらに、実行される操作は、しばしば、人間のオペレータによって実行される精神的操作に一般的に関連付けられる、加算または比較などの用語で言及される。1つ以上の実施形態の一部を形成する、本明細書に記載される操作のいずれにおいても、人間のオペレータのそのような能力は必要ではなく、ほとんどの場合において望ましいものでもない。むしろ、操作は機械操作である。様々な実施形態の操作を実行するのに有用な機械は、デジタルコンピュータまたは同様の装置を含む。

【0015】

いくつかの実施形態は、「結合」および「連結」という表現、ならびにそれらの派生語を用いて説明され得る。これらの用語は、必ずしも互いの同義語として意図されているわけではない。例えば、いくつかの実施形態は、2つ以上の要素が互いに直接物理的または電氣的に接触していることを示すために、「連結」および／または「結合」という用語を用いて説明される場合がある。しかし、「結合」という用語は、2つ以上の要素が互いに直接接触していないが、それでもなお互いに協力または相互作用することを意味する場合

10

20

30

40

50

もある。

【0016】

様々な実施形態はまた、これらの動作を実行するための装置またはシステムに関する。この装置は、必要な目的のために特別に構築されてもよいし、コンピュータに格納されたコンピュータプログラムによって選択的に起動または再設定されるように、コンピュータを含んでもよい。本明細書に示した手順は、特定のコンピュータや他の装置と本質的に関連するものではない。様々な機械が、本明細書の教示に従って書かれたプログラムと共に使用されてもよいし、必要な方法ステップを実行するために、より特殊な装置を構築することが便利であることが判明してもよい。これらの様々な機械に必要な構造は、与えられた説明から分かるであろう。

10

【0017】

次に、図面を参照するが、ここでは、全体を通して同様の要素を参照するために同様の参照数字が使用されている。以下の説明では、説明のために、その徹底的な理解を提供するために、多数の具体的な詳細を記載する。しかしながら、新規な実施形態は、これらの具体的な詳細なしに実施できる。他の例では、構造および装置は、その説明を容易にするためにブロック図の形態で示されている。

【0018】

図および添付の説明において、「a」および「b」および「c」（および同様の指定子）という指定は、任意の正の整数を表す変数であることを意図している。したがって、たとえば、実装が $a = 5$ の値を設定する場合、構成要素 $123-1 \sim 123-a$ （または $123a$ ）として図示される構成要素 123 の完全なセットは、構成要素 $123-1$ 、 $123-2$ 、 $123-3$ 、 $123-4$ および $123-5$ を含み得る。

20

【0019】

図1Aは、開示された実施形態と一致する、システムとも呼ばれる例示的なコンピューティングアーキテクチャ100を示す。図1Aないし1Cに示されるコンピューティングアーキテクチャ100は、特定のトポロジにおいて限定された数の要素を有するが、コンピューティングアーキテクチャ100は、所与の実装のために所望されるように、代替のトポロジにおいてより多くのまたはより少ない要素を含み得ることが理解され得る。

【0020】

コンピューティングアーキテクチャ100は、1つ以上のコンピュータ装置102、1つ以上のサーバ106、および1つ以上の非接触カード104を含む。非接触カード104は、クレジットカード、デビットカード、ATMカード、ギフトカード、支払いカード、スマートカードなど、任意のタイプのカードの代表である。非接触カード104は、NFC、EMV規格、または無線通信における他の短距離プロトコルを介して、装置102の通信インタフェース124（本明細書では、「カードリーダー」、「無線カードリーダー」、および／または「無線通信インタフェース」とも呼ばれる）と通信する、無線周波数識別（RFID）チップなどの1つ以上の通信インタフェース124を含むことができる。本明細書では、通信プロトコルの例としてNFCを使用するが、本開示は、EMV規格、ブルートゥース、および／またはWi-Fiなどの他のタイプの無線通信にも同様に適用可能である。

30

40

【0021】

コンピュータ装置102は、スマートフォン、タブレットコンピュータ、ウェアラブル装置、ラップトップ、ポータブルゲーム装置、仮想化コンピューティングシステム、マッシュアップ端末、POSシステム、サーバ、デスクトップコンピュータなど、任意の数およびタイプのコンピュータ装置を代表する。モバイル装置は、コンピュータ装置102の例として使用できるが、本開示を限定するものと考えられるべきではない。サーバ106は、サーバ、ワークステーション、計算クラスター、クラウドコンピューティングプラットフォーム、仮想化コンピューティングシステムなど、任意のタイプのコンピュータ装置を代表する。明確にするために描かれていないが、コンピュータ装置102、非接触カード104、およびサーバ106はそれぞれ、例えば、プログラム、コード、および／または命

50

令を実行するための１つ以上のプロセッサ回路を含む。

【００２２】

図示するように、非接触カード１０４のメモリ１０８は、アプレット１１０、カウンタ１１６、１つ以上のマスターキー１１４、１つ以上の多様化キー１２０、固有ID１１２、一次アカウント番号（PAN）シーケンス番号１４４、および１つ以上の固有派生キー（UDK）１１８を含む。固有ID１１２は、他の非接触カード１０４と比較して非接触カード１０４を一意に識別する任意の識別子であってよい。PANシーケンス１４４は、非接触カード１０４によって記憶されたカウンタ値を含んでもよい。アプレット１１０は、本明細書で説明する操作の一部または全部を実行する実行可能コードである。カウンタ１１６は、非接触カード１０４とサーバ１０６との間で同期される値である。カウンタ１１６は、非接触カード１０４とサーバ１０６（および／または非接触カード１０４とコンピュータ装置１０２）との間でデータが交換されるたびに变化する数値を含んでもよい。カウンタ１１６、マスターキー１１４、多様化キー１２０、UDK１１８、PANシーケンス１４４、および／または固有ID１１２は、以下でさらに詳細に説明するように、システム１００におけるセキュリティを提供するために使用される。

10

【００２３】

図示するように、装置１０２のメモリ１３２は、オペレーティングシステム１３４のインスタンスを含む。オペレーティングシステムの例は、Android（登録商標）OS、iOS（登録商標）、macOS（登録商標）、Linux（登録商標）、およびWindows（登録商標）オペレーティングシステムを含む。図示されているように、オペレーティングシステム１３４は、アカウントアプリケーション１３６と、１つ以上の他のアプリケーション１４６とを含む。アカウントアプリケーション１３６は、ユーザが、サーバ１０６によって記憶された設定情報１４８に基づいて装置１０２を構成するなどの様々な操作を実行することを可能にする。いくつかの実施形態では、アカウントアプリケーション１３６はさらに、支払いカードの有効化、アカウント残高の閲覧、アイテムの購入、支払いの処理などのような、他のアカウント関連操作を実行できる。いくつかの実施形態では、ユーザは、アカウントアプリケーション１３６の特定の機能にアクセスするために、認証クレデンシャルを使用して認証できる。例えば、認証資格情報は、ユーザ名（またはログイン）およびパスワード、生体認証情報（指紋、フェイスIDなど）などを含む。他のアプリケーション１４６は、ウェブブラウザ、電子メールクライアント、メッセージングクライアント、ソーシャルメディアアプリケーションなど、あらゆるタイプのアプリケーションの代表である。

20

30

【００２４】

図示するように、サーバ１０６のメモリ１２６は、認証アプリケーション１３８およびアカウントデータベース１２８を含む。アカウントデータベース１２８は、一般に、アカウント保持者（例えば、１つ以上のユーザ）、アカウント保持者の１つ以上のアカウント、およびアカウントの１つ以上の非接触カード１０４に関連する情報を含む。例えば、図示のように、アカウントデータベース１２８は、複数のアカウントの設定情報１４８を含むことができる。設定情報１４８は、コンピュータ装置１０２、オペレーティングシステム１３４、アカウントアプリケーション１３６、他のアプリケーション１４６、および／またはそれらの任意のコンポーネントを構成する任意のデータを含み得る。例えば、設定情報１４８は、１つ以上のサーバに接続するための情報（例えば、インターネットプロトコル（IP）アドレス、ポートなど）、アカウント情報（例えば、ログイン／パスワード）、受信トレイの内容（例えば、メッセージ、電子メールなど）、嗜好、変数値、および／または設定を含み得る。設定情報１４８は、設定情報１４８の１つ以上の部分を所定のコンピュータ装置１０２にインストールおよび／または構成する実行可能ファイル、スクリプトなどをさらに含み得る。設定情報１４８は、コンピュータ装置１０２および／またはその任意のソフトウェア部品の任意の属性および／または機能を変更するために使用され得るので、実施形態は、この文脈において限定されない。

40

【００２５】

50

前述のように、設定情報 148 は、コンピュータ装置 102 を自動的に設定するために使用され得る。換言すると、設定情報 148 は、所定の装置および／またはアカウント（任意のアプリケーション、オペレーティングシステム、および／またはパラメータを含む）の少なくとも一部の「バックアップ」を表すことができ、任意の装置がバックアップと同様の状態に復元し得る。例えば、ユーザが新しいスマートフォンを購入する場合、以前のスマートフォンからの設定情報 148 を使用して、新しいスマートフォンを自動的に設定できる。例えば、設定情報 148 を使用して、新しいスマートフォンにアプリケーションをインストールしたり（例えば、購入時にはスマートフォンに付属していなかったが、以前のスマートフォンにインストールされ、設定情報 148 の一部として登録されたアプリケーションなどである）、前のスマートフォンにインストールされていなかったアプリケーションを新しいスマートフォンから削除したり（設定情報 148 に基づき、制限されたアプリケーションを削除する）、古いスマートフォンから新しいスマートフォンに設定および／またはパラメータを適用する等する。

10

【0026】

様々な実施形態において、ユーザは、最初に設定情報 148 をサーバ 106 に登録できる。例えば、ユーザは、任意の装置および／またはアカウントのための設定情報 148 を登録するために、アカウントアプリケーション 136 の機能にアクセスするか、ウェブページにアクセスするか、または任意の他のリソースにアクセスできる。設定情報 148 は、アカウントに関連付けられた全ての装置および／またはアカウントに関連付けられた装置のサブセットに固有であってもよい。加えておよび／または代替的に、設定情報 148 は、アカウントに関連付けられた全てのアプリケーションおよび／またはアカウントに関連付けられたアプリケーションのサブセットに固有であってもよい。いくつかの実施形態では、アカウントアプリケーション 136 は、コンピュータ装置 102 を記述する情報、例えば、インストールされたアプリケーション、設定ファイルなどを収集してもよく、それは設定情報 148 として記憶されてもよい。他の実施形態では、ユーザは、所定の装置の異なるアプリケーション、設定、機能などを指定する入力を提供してもよい。いくつかの実施形態では、設定情報 148 は、登録される各アプリケーションのパッケージ名、登録されるオペレーティングシステム 134 を記述するメタデータ（例えば、装置の識別子、装置のバージョン、嗜好、設定など）、登録される各アプリケーションを記述するメタデータ、嗜好、ログイン情報、アプリケーション ID、または装置、アプリケーション、オペレーティングシステム 134、および／またはそれらのコンポーネントの他の属性を含む。さらに、設定情報 148 をアカウントデータベース 128 内のアカウントに関連付けることができ、これにより、サーバ 106 は、設定情報 148 をアカウントに関連付けられた 1 つ以上の非接触カード 104 にさらに関連付けることができる。

20

30

【0027】

例えば、ユーザは、ソーシャルメディアアプリケーション及び電子メールクライアントをサーバ 106 に登録できる。したがって、ユーザのための設定情報 148 は、ソーシャルメディアアプリケーションおよび電子メールクライアントの各パッケージ名、メディアアプリケーションおよび電子メールクライアントが各サーバに接続するための接続情報、ソーシャルメディアアプリケーションおよび電子メールアプリケーションにおけるユーザのアイデンティティ、電子メールクライアントの電子メール受信箱（またはフォルダ）、ソーシャルメディアアプリケーションにおけるソーシャルメディアプロフィール、ソーシャルメディアアプリケーションにおけるソーシャルメディアメッセージ、ソーシャルメディアアプリケーションおよび電子メールクライアントの各バージョン、表示設定（例えば、いずれかのアプリケーションでダークモードを有効にする）、いずれかのアプリケーションでプッシュ通知を有効にする、オペレーティングシステム 134 内の各アプリケーションのアクセス許可など。実施形態は、本文脈に限定されない。したがって、このような情報の表示は、アカウントの設定情報 148 として保存されてもよい。

40

【0028】

その後、ユーザは、設定情報 148 を使用して、コンピュータ装置 102 を設定するこ

50

とを望むことができる。例えば、コンピュータ装置 102 は、新しいスマートフォンである可能性があり、ユーザは、ソーシャルメディアアプリケーション及び電子メールクライアントを設定することを望み得る（例えば、電子メールクライアントのすべての電子メールを復元すること、ソーシャルメディアアプリケーションのソーシャルメディアプロフィール／設定をロードすることなど）。いくつかの実施形態では、これらのアプリケーションは新しいスマートフォンにインストールされていない可能性があるため、設定情報 148 はさらに、コンピュータ装置 102 にインストールするために、ソーシャルメディアアプリケーションおよび／または電子メールクライアントをダウンロードするために使用され得る。設定情報 148 に基づいて装置の設定を開始するために、ユーザは、非接触カード 104 をコンピュータ装置 102 にタップしてもよい。

10

【0029】

図 1A に描かれた実施形態では、ユーザは、非接触カード 104 をコンピュータ装置 102 にタップできる（または非接触カード 104 を装置 102 の通信インタフェース 124 の通信範囲内に入れる）。その後、アプレット 110 は、暗号 122 を生成してもよい。暗号 122 は、任意の適切な暗号技術に基づいて生成されてもよい。いくつかの実施形態では、暗号 122 は、非接触カード 104 の固有 ID 112 に基づいてもよい。いくつかの実施形態において、アプレット 110 は、暗号 122 を含むデータパッケージの一部として、暗号 122 および暗号化されていない識別子（例えば、カウンタ 116、PAN シーケンス 144、固有 ID 112、および／またはその他の固有識別子）を含むことができる。少なくとも 1 つの実施形態では、データパッケージは NDEF ファイルである。

20

【0030】

前述のように、コンピューティングアーキテクチャ 100 は、データを保護するためにキーの多様化を実行し、本明細書ではキーの多様化技法と呼ばれることがある。一般に、サーバ 106（または他のコンピュータ装置）および非接触カード 104 は、同じマスターキー 114（マスター対称キーとも呼ばれる）で提供されてもよい。より具体的には、各非接触カード 104 は、サーバ 106 のハードウェアセキュリティモジュール（HSM）130 に対応するペアを有する別個のマスターキー 114 でプログラムされる。例えば、非接触カード 104 が製造されるとき、一意のマスターキー 114 が非接触カード 104 のメモリ 108 にプログラムされてもよい。同様に、一意のマスターキー 114 は、HSM 130 内のレコード 142 に格納されてもよい。

30

【0031】

さらに、所定のカード 104 が製造されるとき、UDK 118 は、入力としてダイバースhing 係数と HSM 130 内のマスターキー 114 インデックスへの参照（例えば、レコード 142 へのインデックス）とを取る HSM 機能を介して、マスターキー 114 から多様化されてもよい。一部の実施形態では、多様化要因は、非接触カード 104 の固有 ID 112 および／または PAN シーケンス 144 であってもよい。UDK 118 は、非接触カード 104 および HSM 130 のレコード 142 に格納されてもよい。マスターキー 114 および UDK 118 は、非接触カード 104 およびサーバ 106 以外のすべての関係者から秘匿でき、それによりシステム 100 のセキュリティが強化される。記録部（record）142 に格納されるように描かれているが、いくつかの実施形態では、カウンタ 116 および／または PAN シーケンス 144 は、HSM 130 に格納されない。例えば、固有 ID 112、カウンタ 116、および PAN シーケンス 144 は、アカウントデータベース 128 に格納されてもよい。

40

【0032】

いくつかの実施形態では、暗号 122 を生成するために、アプレット 110 は、暗号アルゴリズムへの入力として、UDK 118、固有 ID 112、および多様化係数を提供し、それによって多様化キー 120 を生成できる。いくつかの実施形態では、多様化要因はカウンタ 116 である。他の実施形態では、PAN シーケンス 144 が多様化要因である。多様化キー 120 は、その後、多様化要因（例えば、カウンタ 116 および／または PAN シーケンス 144）または他の機密データなどのいくつかのデータを暗号化するために

50

使用され得る。アプレット 110 およびサーバ 106 は、暗号の復号化および／または検証処理を容易にするために、同じタイプのデータを暗号化してもよい。

【0033】

前述のように、非接触カード 104 およびサーバ 106 の UDK 118 は、キーの多様化を用いてセキュリティを強化するために、カウンタ 116 と組み合わせて使用できる。前述のように、カウンタ 116 は、非接触カード 104 とサーバ 106 の間で同期される値を含む。カウンタ 116 は、非接触カード 104 とサーバ 106 との間でデータが交換されるたびに变化する数値を含んでもよい（および／または非接触カード 104 と、装置 102）。データを送信する準備をするとき（例えば、サーバ 106 および／または装置 102 へ）、非接触カード 104 のアプレット 110 は、カウンタ 116 をインクリメントしてもよい。その後、非接触カード 104 のアプレット 110 は、UDK 118、固有 ID 112、およびカウンタ 116 を入力として暗号アルゴリズムに提供し、暗号アルゴリズムは出力として多様化キー 120 を生成する。暗号化アルゴリズムは、暗号化アルゴリズム、ハッシュベースのメッセージ認証コード（HMAC）アルゴリズム、暗号ベースのメッセージ認証コード（CMAC）アルゴリズムなどを含む。暗号アルゴリズムの非限定的な例には、3DES や AES107 などの対称暗号化アルゴリズム、HMAC-SHA-256 などの対称 HMAC アルゴリズム、AES-CMAC などの対称 CMAC アルゴリズムなどがある。キー多様化技術の例は、2018 年 11 月 29 日に出願された米国特許出願 16 / 205, 119 に詳細に記載されている。前述の特許出願は、参照によりその全体が本明細書に引用される。一部の実施形態では、PAN シーケンス 144 が、カウンタ 116 の代わりに暗号アルゴリズムへの入力として使用され、例えば、UDK 118、固有 ID 112 および PAN シーケンス 144 を暗号化することによって、多様化キー 120 を生成する。

【0034】

アプレット 110 は次に、多様化キー 120 と暗号アルゴリズムへの入力としてのデータを使用して、いくつかのデータ（例えば、固有 ID 112、カウンタ 116、PAN シーケンス 144、コマンド、および／または任意の他のデータ）を暗号化できる。例えば、多様化キー 120 で固有 ID 112 を暗号化することは、暗号化された固有 ID 112（例えば、暗号 122）をもたらす得る。前述のように、アプレット 110 とサーバ 106 は同じデータを暗号化してもよい。

【0035】

一部の実施形態では、2つの多様化キー 120 が、例えば暗号化機能への入力の 1つ以上の部分に基づいて生成されてもよい。一部の実施形態では、2つの多様化キー 120 は、2つの異なるマスターキー 114、2つの異なる UDK 118、固有 ID 112、およびカウンタ 116（または PAN シーケンス 144）に基づいて生成される。このような実施形態では、多様化キー 120 の一方を使用してメッセージ認証コード（MAC）が生成され、多様化キー 120 の他方を使用して MAC が暗号化されることがある。MAC は、機密データ、固有 ID 112、カウンタ 116、および／または PAN シーケンス 144 など、MAC アルゴリズムへの任意の適切なデータ入力に基づいて生成されてもよい。より一般的には、アプレット 110 およびサーバ 106 は、同じデータに基づいて MAC を生成してもよい。いくつかの実施形態では、暗号 122 は、NDEF ファイルなどのデータパッケージに含まれる。そして、アカウントアプリケーション 136 は、コンピュータ装置 102 の通信インタフェース 124 を介して、暗号 122 を含むデータパッケージを読み取ることができる。

【0036】

いくつかの実施形態では、アプレットは URL のパラメータとして暗号 122 を含む。たとえば、URL は「http://www.example.com/appconfig?param=ABC123&custID=123」である。このような例では、暗号 122 はパラメータ「ABC123」に対応し、固有 ID 112 はパラメータ「custID」に対応してもよい。オペレーティングシステム 134 によって受信されると、オペレーティングシステム 134 は、URL を処理するためのアプリケーションを開くことができる。いくつかの実施形態では、URL は、アカウ

ントアプリケーション 136 に登録されてもよく、これにより、オペレーティングシステム 134 は、アカウントアプリケーション 136 を起動し、アカウントアプリケーション 136 に入力として URL 120 を提供する。しかし、他の例では、オペレーティングシステム 134 は、ウェブブラウザを起動し、ウェブブラウザへの入力として URL を提供してもよい。他の実施形態では、暗号 122 は URL のパラメータではなく、NDEF ファイルなどのデータパッケージで URL とともに送信される。このような実施形態では、オペレーティングシステム 134 は、コンピュータ装置 102 の通信インタフェース 124 を介して、URL および暗号 122 を含むデータパッケージを読み取ることができる。

【0037】

図 1A に示す例では、オペレーティングシステム 134 は、暗号 122 の読み取りに基づいて、アカウントアプリケーション 136 を起動できる。前述のように、暗号 122 は URL のパラメータであってもよい。このような例では、URL はアカウントアプリケーション 136 に関連付けられていてもよい。これにより、オペレーティングシステム 134 がアカウントアプリケーション 136 を起動する。次に、アカウントアプリケーション 136 は、暗号 122 を抽出し、検証のために暗号 122 をサーバ 106 に送信できる。

【0038】

暗号 122 が URL のパラメータではない実施形態では、オペレーティングシステム 134 は、暗号 122 および／または暗号 122 を含む NDEF ファイルの読み取りに基づいて、アカウントアプリケーション 136 を起動できる。オペレーティングシステム 134 は、暗号 122 をアカウントアプリケーション 136 に提供してもよい。次に、アカウントアプリケーション 136 は、暗号 122 を抽出し、検証のために暗号 122 をサーバ 106 に送信できる。

【0039】

いくつかの実施形態では、アカウントアプリケーション 136（または他のアプリケーションを使用して、設定情報 148 に基づいてコンピュータ装置 102 を設定する）は、装置にインストールされない場合がある。いくつかのそのような実施形態では、オペレーティングシステム 134 は、URL および／または暗号 122 に基づいて、アカウントアプリケーション 136 をコンピュータ装置 102 にダウンロードおよびインストールさせてもよい。他のそのような実施形態では、アカウントアプリケーション 136 の開示された機能を含むアプリケーションクリップ（例えば、Apple（登録商標）App Clip）、インスタントアプリケーション（例えば、Android（登録商標）インスタントアプリケーション）、またはプログレッシブウェブアプリケーション（例えば、Android プログレッシブ Web アプリケーション）が、設定情報 148 に基づいてコンピュータ装置 102 を設定するためにコンピュータ装置 102 上にダウンロードおよびインストールされてもよい。そのような実施形態において、アプリケーションクリップ、インスタントアプリケーション、および／またはプログレッシブウェブアプリケーションは、設定情報 148 がコンピュータ装置 102 を設定するために使用された後、コンピュータ装置 102 から自動的に削除されてもよい。

【0040】

図 1B は、アカウントアプリケーション 136 が暗号 122 をサーバ 106 に送信する実施形態を示す。サーバ 106 は、サーバ 106 が保管するマスターキー 114 および／または UDK 118 のインスタンスに少なくとも部分的に基づく検証のために、暗号 122 を認証アプリケーション 138 および／または HSM 130 に提供できる。一部の実施形態では、認証アプリケーション 138 および／または HSM 130 は、サーバ 106 に提供された暗号化されていない一意の ID 112 を使用して、UDK 118（またはマスターキー 114）およびカウンタ 116 を識別してもよい。PAN シーケンス 144 が暗号 122 の生成に使用される例では、サーバ 106 は、暗号化されていない一意の ID 112 を使用して、アカウントデータベース 128 および／または HSM 130 内の PAN シーケンス 144 を識別してもよい。一部の例では、認証アプリケーション 138 は、入力として UDK 118、固有 ID 112、およびカウンタ 116 を HSM 130 の暗号化機能に提

10

20

30

40

50

供でき、HSM 130は出力として1つ以上の多様化キー120を生成する。他の実施形態では、サーバはUDK118、一意のID112、およびPANシーケンス144を暗号化して、多様化キー120を生成する。結果として得られる多様化キー120は、非接触カード104の多様化キー120に対応し、暗号122の復号化および／または一度復号化された後のMACの検証に使用できる。例えば、サーバ106は、アプレット110と同じデータ、例えば、機密データ、固有ID112、カウンタ116、および／またはPANシーケンス144に基づいてMACを生成してもよい。サーバ106が生成したMACが暗号122の復号化されたMACと一致する場合、サーバ106は暗号122を検証または認証できる。

【0041】

使用される復号化技法にかかわらず、認証アプリケーション138および／またはHSM130は、暗号122の復号化に成功し、MACを検証することにより、暗号122を検証および／または認証できる。復号化および／またはMACの検証に成功した場合、認証アプリケーション138は、アカウントデータベース128を参照して、アカウントの設定情報148を識別できる。一部の実施形態では、認証アプリケーション138は、サーバ106に提供された暗号化されていない一意のID112に基づいて設定情報148にアクセスできる。任意の適切な識別子を使用してアカウントの設定情報148にアクセスできるため、実施形態はこの文脈で限定されない。サーバ106は、さらに、サーバ106が暗号122を検証し、設定情報148を使用してコンピュータ装置102を設定してもよいことを示す応答を、コンピュータ装置102に（例えば、アカウントアプリケーション136および／またはオペレーティングシステム134に）送信してもよい。

【0042】

次に、認証アプリケーション138は、設定情報148を解析して、そこに登録されている各アプリケーション、オペレーティングシステム、および／または設定を識別できる。前の例に引き続き、設定情報148は、ソーシャルメディアアプリケーションおよび電子メールクライアントの指示を含むことができる。以下により詳細に説明するように、サーバ106は、その後、設定情報148（および／またはその一部）をコンピュータ装置102に送信できる。

【0043】

復号化に戻ると、認証アプリケーション138が暗号122を復号化できない場合（および／またはMACを検証できない場合）、認証アプリケーション138は暗号122を検証しない。このような例では、認証アプリケーション138は、コンピュータ装置102を自動的に設定するために設定情報148にアクセスすることを控えることを決定する。認証アプリケーション138は、失敗した復号化および／または検証の表示と、設定情報148がコンピュータ装置102を設定するために使用できないことの表示とを含む応答を、コンピュータ装置102に送信できる。

【0044】

図1Cは、認証アプリケーション138が、アカウントデータベース128内の設定情報148内の識別されたアプリケーションまたは他のソフトウェア部品ごとに、設定情報148を含むプッシュ通知150をアカウントアプリケーション136に送信する実施形態を示す。いくつかの実施形態では、プッシュ通知150は、サーバ106が暗号122を検証したこと、および設定情報148を使用してコンピュータ装置102を設定してもよいことの表示を含む。単一のプッシュ通知で送信されるように描かれているが、いくつかの実施形態では、サーバ106は、コンピュータ装置102に複数のプッシュ通知を送信してもよく、各プッシュ通知は、設定情報148の少なくとも一部を含む。いくつかの実施形態では、所定のプッシュ通知は、オペレーティングシステム134のバックグラウンドで受信され得る（例えば、コンピュータ装置102に表示するために出力されるのではなく、対応するアプリケーションおよび／またはオペレーティングシステム134に直接送信されるバックグラウンドプッシュ通知などである）。いくつかの実施形態では、プッシュ通知はフォアグラウンドプッシュ通知である（例えば、装置102に表示される通

10

20

30

40

50

知)。いくつかの実施形態において、設定情報 148 は、1 つ以上の設定ファイルを含む。

【0045】

さらに、いくつかの実施形態では、設定情報 148（および／またはその一部）のサイズは、サイズ閾値（例えば、1 メガバイト、10 メガバイトなど）を超えてもよい。そのような実施形態では、サーバ 106 は、1 つ以上のトークンを生成し、各トークンを設定情報 148 の 1 つ以上の部分に関連付け、1 つ以上のトークンをコンピュータ装置 102 に送信してもよい。次に、コンピュータ装置 102 は、関連する設定情報 148（および／またはその一部）をサーバ 106 から引き出すために、トークンをサーバ 106 に送信してもよい。例えば、トークンを設定情報 148 と関連付けることによって、サーバ 106 は、アカウントアプリケーション 136、オペレーティングシステム 134、および／または他のアプリケーション 146 からのトークンの受信に基づいて、関連する設定情報 148 を提供できる。

10

【0046】

いくつかの実施形態では、装置 102 は、設定情報 148 および／またはトークンを非接触カード 104 に送信してもよい。その後、非接触カード 104 は、設定情報 148 および／またはトークンをメモリ 108 に記憶してもよい。その後、コンピュータ装置 102 は、本明細書で説明されるようにコンピュータ装置 102 およびその任意の構成要素を設定するために、（例えば、コンピュータ装置 102 への非接触カード 104 のタップに応答する NFC を介して）非接触カード 104 から設定情報 148 を受信してもよい。

20

【0047】

さらに、示されるように、図 1C は、コンピュータ装置 102 が、アカウントアプリケーション 136 に加えて 3 つの異なるアプリケーション、例えば、他のアプリケーション 146-1、他のアプリケーション 146-2、および他のアプリケーション 146-N を含む実施形態を示す。有利には、アカウントアプリケーション 136 は、設定情報 148 を使用して、コンピュータ装置 102 上でこれらのアプリケーションを設定できる。

【0048】

図 1D は、アカウントアプリケーション 136 が、コンピュータ装置 102 を設定するために、サーバ 106 から受信した設定情報 148 の 1 つ以上の部分を使用する実施形態を示す。前述のように、アカウントアプリケーション 136 は、サーバ 106 が暗号 122 を検証し、設定情報 148 を使用してコンピュータ装置 102 を設定してもよいことを示すサーバ 106 からの応答に基づいて、設定情報 148 の使用を条件付けることができる。示されるように、アカウントアプリケーション 136 は、他のアプリケーション 146-1 を設定するために設定情報 148-1 を使用し、他のアプリケーション 146-N を設定するために設定情報 148-N を使用する。いくつかの実施形態では、アカウントアプリケーション 136 は、設定情報 148-1 ~ 148-N を生成するために設定情報 148 を解析してもよい。他の実施形態では、サーバ 106 は、コンピュータ装置 102 上で設定される各アプリケーションまたは他のエンティティに対して 1 つのファイルである、複数のファイルを含むように設定情報 148 を生成する。したがって、そのような実施形態では、設定情報 148-1 ~ 148-N は、サーバ 106 によって生成される。いくつかの実施形態では、設定情報 148 の少なくとも一部は、アカウントアプリケーション 136 に関連付けられ、したがって、アカウントアプリケーション 136 を設定（例えば、ユーザプロファイルをロード、設定など）するために使用される。

30

40

【0049】

いくつかの実施形態では、アカウントアプリケーション 136 は、設定情報 148 を各設定ファイルとして、各アプリケーションおよび／またはオペレーティングシステム 134 に関連付けられた場所に保存する（または書き込む）。例えば、アカウントアプリケーション 136 は、設定情報 148-1 を他のアプリケーション 146-1（例えば、アプリケーション 146-1）の設定情報を格納するファイルに関連するファイル名および／またはファイルロケーションで）用の設定ファイルとして保存してもよい。別の例として

50

、アカウントアプリケーション 136 は、設定情報 148 の一部を使用して、オペレーティングシステム 134 の 1 つ以上のファイル、レジストリ設定、または他のパラメータを格納および／または変更できる。いくつかのそのような例では、アカウントアプリケーション 136 は、設定情報 148 をオペレーティングシステム 134 に提供してもよく、オペレーティングシステム 134 は、設定情報 148 を使用してオペレーティングシステム 134 を修正してもよい。いくつかの実施形態において、設定情報 148 を使用することは、新しい設定情報をコンピュータ装置 102 に書き込むことを生じ得、コンピュータ装置 102 のいくつかの既存の設定情報を修正させ得（例えば、値や設定などを変更することによって）、および／またはコンピュータ装置 102 の他の既存の設定情報を変更しないままにし得る。

10

【0050】

さらに、アカウントアプリケーション 136 は、設定情報 148-3 を使用して、アプリケーション 146-3 がコンピュータ装置 102 にインストールされていないと判定する。そのような実施形態において、アカウントアプリケーション 136 は、設定情報 148-3（例えば、アプリケーション 146-3 のパッケージ名）を使用して、インターネットからアプリケーション 146-3 をダウンロードする。その後、アカウントアプリケーション 136 は、設定情報 148-3 を使用して、本明細書で説明するようにアプリケーション 146-3 を設定できる。

【0051】

同様に、アカウントアプリケーション 136 は、設定情報 148 を使用して、他のアプリケーション 146-2 が設定情報 148 に登録されていないと判定する。いくつかの実施形態では、アカウントアプリケーション 136 は、設定情報 148 に基づいて、他のアプリケーション 146-2 が制限されたアプリケーションであると判定する。たとえば、企業は、装置におけるソーシャルメディアアプリケーションの使用を制限できる。したがって、設定情報 148 に基づいて、アカウントアプリケーション 136 は、コンピュータ装置 102 に、他のアプリケーション 146-2 をアンインストールするか、または他の方法で無効にさせる。いくつかの実施形態では、アカウントアプリケーション 136 は、ユーザが他のアプリケーション 146-2 を再インストールまたは他の方法で有効にすることを恒久的に制限してもよい（例えば、他のアプリケーション 146-2 がコンピュータ装置 102 にインストールおよび／または有効にされることを制限するようにオペレーティングシステム 134 を設定することによって）。

20

30

【0052】

いくつかの実施形態において、アカウントアプリケーション 136 は、コンピュータ装置 102 を設定するために追加の許可を必要とし得る。例えば、アカウントアプリケーション 136 は、コンピュータ装置 102 の記憶媒体（例えば、不揮発性メモリおよび／または揮発性メモリ、明瞭化のために図示せず）へのアクセス、例えば、記憶装置の読み取り、書き込み、またはその他のアクセスを必要とする場合がある。そのような実施形態では、アカウントアプリケーション 136 および／またはオペレーティングシステム 134 は、アカウントアプリケーション 136 にストレージへのアクセスを許可するよう要求でき、これは、ユーザによって、ひいてはオペレーティングシステム 134 によって許可されることができる。

40

【0053】

したがって、設定情報 148 を使用してコンピュータ装置 102 を設定することによって、コンピュータ装置 102 は、すべての関連するアプリケーション、設定、および／または機能を含むように自動的に設定され得る。例えば、設定情報 148 を用いて電子メールクライアントを設定することにより、ユーザは、電子メールを閲覧し、新しい電子メールを受信し、電子メールサーバに接続し、新しい電子メールを送信できる。実施形態は、この文脈において限定されない。さらに、設定情報 148 を用いてコンピュータ装置 102 を設定する前であれば、ユーザは、電子メールクライアントを用いて（電子メールクライアントを手動で設定することなく）、電子メールを閲覧、電子メールを受信、電子メー

50

ルサーバに接続、または電子メールを送信することはできない。

【0054】

図2Aは、コンピュータ装置102の自動設定の少なくとも一部を実行するためにウェブブラウザ206を使用する実施形態を示す概略図200である。図2Aに描かれた例では、非接触カード104は、非接触カード104をコンピュータ装置102にタップすることに応答して、暗号204付きURLを生成する。暗号204付きURLは、他の関連情報（例えば、暗号化されていない識別子など）とともに、暗号122を参照して上述したように生成された暗号を含むことができる。より一般的には、暗号204付きURLは、図1Aないし1Dを参照して上述したように生成できる。

【0055】

オペレーティングシステム134（わかりやすくするために写真には写っていない）によって読み取られると、オペレーティングシステム134は、ウェブブラウザ206（たとえば、他のアプリケーション146の1つ）を起動し、ウェブブラウザ206に暗号204付きURLを提供できる。そうすることで、ウェブブラウザ206は、暗号204付きURL（またはその一部）にアクセスできる。いくつかの実施形態では、暗号204付きURLは、コンピュータ装置102を自動的に設定するための設定ページに向けられている。実施形態は、この文脈で限定されない。

【0056】

図2Bは、ウェブブラウザ206が、たとえば、暗号204付きURLを含むハイパーテキスト転送プロトコル（HTTP）要求に基づいて、暗号204付きURLにアクセスする実施形態を示す。図示されているように、認証アプリケーション138は、HTTPリクエストに基づいて、暗号204付きURLを受信できる。認証アプリケーション138は、検証のために、暗号204付きURLから暗号を抽出できる。たとえば、サーバ106は、暗号を検証するために、上述したように暗号を復号化し、および／またはその中に含まれるMACを検証できる。

【0057】

サーバ106が暗号を検証することに基づいて（たとえば、URL内の暗号を暗号204で復号化する、および／またはMACを検証する）、サーバ106は、アカウントデータベース128を参照して、関連する設定情報148を特定できる。サーバ106はさらに、検証に基づいて、サーバ106が暗号122を検証したこと、および設定情報148を使用してコンピュータ装置102を設定してもよいことを示す応答を、コンピュータ装置102に送信してもよい（例えば、ウェブブラウザ206および／またはオペレーティングシステム134に）。いくつかの実施形態では、認証アプリケーション138は、暗号204付きURLでサーバ106に提供された暗号化されていない固有ID112に基づいて、設定情報148にアクセスできる。任意の適切な識別子が、アカウントの設定情報148にアクセスするために使用され得るので、実施形態は、この文脈において限定されない。

【0058】

一方、サーバ106が暗号を復号できず、および／またはMACを検証できない場合、サーバ106は暗号を検証しない。このような例では、認証アプリケーション138は、コンピュータ装置102を自動的に設定するための設定情報148へのアクセスを控えることを決定する。

【0059】

図2Cは、サーバ106がURLの暗号部分を暗号204で検証する実施形態を示す。前述のように、サーバ106が暗号を検証すると、サーバ106は、非接触カード104に関連付けられたアカウントの設定情報148にアクセスする。次に、サーバ106は、設定情報148に表される複数の異なるアプリケーションを識別できる。特定されたアプリケーションごとに、サーバ106は、関連する設定情報148および／またはその一部を含む各プッシュ通知を生成してもよい。

【0060】

10

20

30

40

50

図示するように、サーバ 106 は、プッシュ通知 208、プッシュ通知 210、およびプッシュ通知 212 をコンピュータ装置 102 に送信する。示されるように、プッシュ通知 208 は設定情報 148-1 を含み、プッシュ通知 210 は設定情報 148-2 を含み、プッシュ通知 212 は設定情報 148-N を含む。そのような例では、各々のプッシュ通知およびその中の設定情報の各インスタンスは、装置上で実行される各アプリケーションに関連付けられてもよい。いくつかの実施形態では、プッシュ通知はまた、オペレーティングシステム 134 に送信されるプッシュ通知を含んでもよく、そのプッシュ通知は、オペレーティングシステム 134 に適用可能な設定情報 148（例えば、ブルーライトフィルタ、妨害禁止機能などを有効にする）を含んでもよい。いくつかの実施形態では、プッシュ通知 208、210、および／または 212 は、サーバ 106 が暗号 122 を検証したこと、および設定情報 148 を使用してコンピュータ装置 102 を設定してもよいことの各表示を含む。

10

【0061】

いくつかの実施形態では、プッシュ通知 208、210、および／または 212 は、オペレーティングシステム 134 のバックグラウンドで受信され得る（例えば、コンピュータ装置 102 に表示するために出力されるのではなく、対応するアプリケーションおよび／またはオペレーティングシステム 134 に直接送信されるバックグラウンドプッシュ通知などである）。いくつかの実施形態では、プッシュ通知 208、210、および／または 212 は、フォアグラウンドプッシュ通知である（例えば、装置 102 に表示される通知）。いくつかの実施形態において、設定情報 148 は、1 つ以上の設定ファイルを含む。さらに、いくつかの実施形態では、設定情報 148-1 ~ 148-N のサイズがサイズ閾値を超えることがある。このような実施形態では、サーバ 106 は、1 つ以上のトークンを生成し、各トークンをプッシュ通知 208、210、および 212 の各々に含めることができる。一度受信されると、各アプリケーションは、関連する設定情報 148（および／またはその一部）をサーバ 106 から引き出すために、受信されたトークンをサーバ 106 に提供できる。

20

【0062】

図 2D は、プッシュ通知 208、210、および 212 が、それぞれ、他のアプリケーション 146-1、146-2、および 146-N によって受信される実施形態を示す。一般に、一度受信されると、他のアプリケーション 146-1、146-2、および 146-N は、設定のために、それぞれ、設定情報 148-1、148-2、および 148-N を使用できる。例えば、他のアプリケーション 146-1 は設定情報 148-1 に基づいて設定されてもよく、他のアプリケーション 146-2 は設定情報 148-2 に基づいて設定されてもよく、他のアプリケーション 146-N は設定情報 148-N に基づいて設定されてもよい。いくつかの実施形態では、他のアプリケーション 146-1、146-2、および 146-N、ならびに／またはオペレーティングシステム 134 は、サーバ 106 が暗号 122 を検証し、設定情報 148 がコンピュータ装置 102 を設定するために使用可能であるという指示をサーバ 106 から受信することに基づいて、設定情報 148 の使用を条件付ける。

30

【0063】

いくつかの実施形態では、設定情報 148 は、各アプリケーションおよび／またはオペレーティングシステム 134 に関連する場所に各設定ファイルとして保存される。例えば、他のアプリケーション 146-1 は、設定情報 148-1 を、他のアプリケーション 146-1 のための設定ファイルとして（例えば、アプリケーション 146-1 のための設定情報を保存するファイルと関連付けられたファイル名および／またはファイルロケーションで）保存してもよい。別の例として、他のアプリケーション 146-1 は、設定情報 148-1 の一部を使用して、1 つ以上のファイル、レジストリ設定、または他のアプリケーション 146-1 を設定するオペレーティングシステム 134 の他のパラメータを格納および／または変更できる。いくつかのそのような例では、他のアプリケーション 146-1 は、設定情報 148-1 をオペレーティングシステム 134 に提供してもよく、オ

40

50

オペレーティングシステム 134 は、設定情報 148 を使用してオペレーティングシステム 134 を修正してもよい。同様に、アプリケーション 146-2 は、設定情報 148-2 を他のアプリケーション 146-2 のための設定ファイルとして記憶してもよく、アプリケーション 146-N は、設定情報 148-N を他のアプリケーション 146-N のための設定ファイルとして記憶してもよい。

【0064】

いくつかの実施形態では、設定情報 148-1 ~ 148-N を使用することは、新しい設定情報をコンピュータ装置 102 に書き込ませる可能性があり、コンピュータ装置 102 のいくつかの既存の設定情報を（例えば、値、設定などを変更することによって）変更させる可能性があり、および／またはコンピュータ装置 102 の他の既存の設定情報を変更されないままにさせる可能性がある。

10

【0065】

図 1 A ないし 1 D に描かれた実施形態と同様に、設定情報 148 は、コンピュータ装置 102 からアプリケーションをインストールおよび／またはアンインストールするために使用されてもよい。たとえば、オペレーティングシステム 134 は、プッシュ通知 210 を受信し、アプリケーション 146-2 がコンピュータ装置 102 にインストールされていないと判断できる。そのような例では、オペレーティングシステム 134 は、例えば、アプリケーションストア、インターネットなどから、アプリケーション 146-2 をダウンロードし、コンピュータ装置 102 にインストールしてもよい。同様に、設定情報 148-N が、アプリケーション 146-N が装置にインストールされることが許可されていないこと、および／または設定情報 148 に登録されていなかったことを指定する場合、設定情報 148-N は、アプリケーション 146-N に、コンピュータ装置 102 からのアプリケーション 146-N の除去（および／または無効化）を開始させることができる。

20

【0066】

有利なことに、設定情報 148 は、コンピュータ装置 102 を自動的に設定および／または復元するために使用される。暗号の検証を要求することにより、コンピュータ装置 102 の設定は安全な方法で完了する。より一般的には、ユーザは、バックアップを迅速に復元し、新しい装置を設定し、および／または設定情報 148 をある装置から別の装置に適用できる。

30

【0067】

開示された実施形態の動作は、以下の図を参照してさらに説明され得る。図には論理フローを含むものもある。本明細書で提示されるそのような図は特定の論理フローを含む場合があるが、論理フローは、本明細書で説明されるような一般的な機能がどのように実装され得るかの例を提供するに過ぎないことが理解され得る。さらに、所定の論理フローは、特に指示がない限り、必ずしも提示された順序で実行される必要はない。さらに、一部の実施形態では、論理フローに図示されたすべての行為が必要であるとは限らない。さらに、所定の論理フローは、ハードウェア要素、プロセッサによって実行されるソフトウェア要素、またはそれらの任意の組み合わせによって実装されてもよい。実施形態は、この文脈において限定されない。

40

【0068】

図 3 は、論理フロー（ルーチン）300 の一実施形態を示す。論理フロー 300 は、本明細書で説明する 1 つ以上の実施形態によって実行される操作の一部または全部を代表するものであってもよい。例えば、論理フロー 300 は、設定情報及び非接触カードを使用して装置を自動的に設定する動作の一部又は全部を含むことができる。実施形態は、この文脈において限定されない。

【0069】

ブロック 302 において、ルーチン 300 は、コンピュータ装置 102 上で実行されるアカウントアプリケーション 136 によって、アカウントに関連付けられた非接触カード 104 から暗号（例えば、暗号 122 および／または暗号 204 付き URL の暗号）を受

50

信する。ブロック304において、ルーチン300は、アカウントアプリケーション136によって、暗号をサーバ106に送信する。ブロック306において、ルーチン300は、サーバが暗号を検証することに基づいて、アカウントアプリケーション136によって、アカウントに関連付けられた複数のアプリケーションの設定情報148を受信する。サーバ106は、設定情報148とともに、サーバ106が暗号122を検証したこと、および設定情報148を使用してコンピュータ装置102を設定してもよいことを指定する表示を含むことができる。アプリケーションは、他のアプリケーション146、オペレーティングシステム134、および／またはアカウントアプリケーション136を含んでもよい。ブロック308において、ルーチン300は、設定情報148に基づいて、コンピュータ装置102上の各アプリケーションのそれぞれの設定を修正する。

10

【0070】

図4は、論理フロー（ルーチン）400の一実施形態を示す。論理フロー400は、本明細書で説明する1つ以上の実施形態によって実行される操作の一部または全部を代表するものであってもよい。例えば、論理フロー400は、設定情報及び非接触カードを使用して装置を自動的に設定する動作の一部又は全部を含むことができる。実施形態は、この文脈において限定されない。

【0071】

ブロック402において、ルーチン400は、サーバ106に、アカウントおよび／またはコンピュータ装置102に関連付けられた複数のアプリケーションおよび各アプリケーションの設定情報を登録する。そうすることによって、設定情報148が、アカウントデータベース128内のアカウントに関連付けられた少なくとも1つのエントリに記憶され得る。ブロック404において、ルーチン400は、コンピュータ装置102によって、アカウントに関連付けられた非接触カード104から暗号（例えば、暗号122および／または暗号204付きURLの暗号）を受信する。ブロック406において、ルーチン400は、コンピュータ装置102によって、暗号をサーバ106に送信する。ブロック408において、ルーチン400は、サーバ106から受信した応答に基づいて、コンピュータ装置102によって、サーバ106が暗号を検証し、設定情報148がコンピュータ装置102を設定するために使用できることを決定する。ブロック410において、ルーチン400は、サーバ106による暗号の検証に基づいて、コンピュータ装置102によって、アカウントに関連付けられた複数のアプリケーションのための設定情報148を受信する。アプリケーションは、他のアプリケーション146、オペレーティングシステム134、および／またはアカウントアプリケーション136を含み得る。

20

30

【0072】

ブロック412において、ルーチン400は、第1アプリケーションがコンピュータ装置102にインストールされていないという決定に基づいて、コンピュータ装置102によって、第1アプリケーション（例えば、他のアプリケーション146の一つ）をコンピュータ装置にダウンロードする。ブロック414において、ルーチン400は、コンピュータ装置102によって、第1アプリケーションを装置にインストールする。ブロック416において、ルーチン400は、設定情報148に基づいて、コンピュータ装置102から第2アプリケーション（例えば、他のアプリケーション146の他の一つ）をアンインストールする。例えば、設定情報148は、第2アプリケーションをアンインストールまたは無効にするように指定できる。ブロック418において、ルーチン400は、設定情報148に基づいて、コンピュータ装置102によって、各アプリケーションの各々の設定を修正する。

40

【0073】

図5は、論理フローまたはルーチン500の実施形態を示す。論理フロー500は、本明細書で説明する1つ以上の実施形態によって実行される動作の一部または全部を代表できる。例えば、論理フロー500は、設定情報及び非接触カードを使用して装置を自動的に設定する動作の一部又は全部を含むことができる。実施形態は、この文脈において限定されない。

50

【0074】

ブロック502において、ルーチン500は、サーバによって、複数のアプリケーションおよびアカウントを持つ各アプリケーションの設定情報を登録する。そうすることにより、設定情報148が、アカウントデータベース128内のアカウントに関連付けられたエントリに記憶される場合がある。ブロック504において、ルーチン500は、コンピュータ装置102によって、アカウントに関連付けられた非接触カード104から、暗号204付きURLを受信する。ブロック506において、ルーチン500は、コンピュータ装置102によって、暗号204付きURLに基づいてウェブブラウザを起動する。ブロック508において、ルーチン500は、ウェブブラウザ206によって、少なくとも暗号を、例えば、暗号204付きURLに関連付けられたウェブページにアクセスすることによって、サーバ106に送信する。ブロック510において、ルーチン500は、ウェブブラウザ206によって、サーバから受信した応答に基づいて、サーバが暗号204付きURLから暗号を検証したこと、および設定情報148がコンピュータ装置102を設定するために使用できることを決定する。

10

【0075】

ブロック512において、ルーチン500は、コンピュータ装置102によって、サーバによる暗号の検証に基づいて、アカウントに関連付けられた複数のアプリケーションの設定情報148を受信する。アプリケーションは、他のアプリケーション146、オペレーティングシステム134、および／またはアカウントアプリケーション136を含み得る。ブロック514において、ルーチン500は、装置によって、第1アプリケーションがコンピュータ装置102にインストールされていないという決定に基づいて、コンピュータ装置102に第1アプリケーションをダウンロードする。ブロック516において、ルーチン500は、コンピュータ装置102によって、コンピュータ装置102に第1アプリケーションをインストールする。ブロック518において、ルーチン500は、設定情報148に基づいて、コンピュータ装置102から第2アプリケーション（例えば、他のアプリケーション146の他の1つ）をアンインストールする。例えば、設定情報148は、第2アプリケーションをアンインストールまたは無効にするように指定できる。ブロック520において、ルーチン500は、コンピュータ装置102によって、設定情報148に基づいて、各アプリケーションの各々の設定を変更する。

20

【0076】

図6Aは、非接触カード104の構成例を示す概略図600であり、非接触カード104の前面または背面にサービスプロバイダ情報602として表示される、サービスプロバイダによって発行されるクレジットカード、デビットカード、またはギフトカードなどの支払カードを含むことができる。いくつかの例では、非接触カード104は決済カードとは無関係であり、限定するものではないが、身分証明書を含んでもよい。いくつかの例では、取引カードは、デュアルインタフェース非接触支払カード、ポイントカードなどを含んでもよい。非接触カード104は、基材604を含み得、この基材は、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つ以上の積層層を含み得る。例示的な基材は、ポリ塩化ビニル、ポリ塩化ビニルアセテート、アクリロニトリルブタジエンスチレン、ポリカーボネート、ポリエステル、陽極酸化チタン、パラジウム、金、炭素、紙、および生分解性材料を含む。いくつかの例では、非接触カード104はISO/IEC 7816標準のID-1フォーマットに準拠した物理的特性を有し、トランザクションカードはISO/IEC 14443標準に準拠している。しかし、本開示による非接触カード104は異なる特性を有してもよく、本開示は、決済カードにトランザクションカードを実装することを要求しないことが理解される。

30

40

【0077】

非接触カード104はまた、カードの前面および／または背面に表示された識別情報606と、接触パッド608とを含むことができる。接触パッド608は、1つ以上のパッドを含み、ATM、装置、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別のクライアント装置と、トランザクションカードを介して接触

50

を確立してもよい。接触パッドは、ISO/IEC 7816規格などの1つ以上の規格に従って設計され、EMVプロトコルに従って通信を可能にできる。非接触カード104は、図6Bでさらに説明するように、処理回路、アンテナ、その他の構成要素も含むことができる。これらの構成要素は、接触パッド608の後方または基板604上の他の場所、例えば基板604の異なる層内に配置されてもよく、接触パッド608と電気的および物理的に結合されてもよい。非接触カード104は、磁気ストリップまたはテープも含んでよく、この磁気ストリップまたはテープは、カードの裏面に配置されてよい（図6Aには示されていない）。非接触カード104は、NFCプロトコルを介して通信可能なアンテナと結合された近距離無線通信（NFC）装置を含むこともできる。実施形態はこのように限定されない。

10

【0078】

図6Bに示されるように、非接触カード104の接触パッド608は、プロセッサ612、メモリ108、および1つ以上の通信インタフェース124を含む、情報を記憶、処理、および通信するための処理回路610を含み得る。処理回路610は、本明細書で説明す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、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んでもよいことが理解される。

【0079】

メモリ108は、読み出し専用メモリ、書き込み一回読み出し多重メモリ、または読み出し/書き込みメモリ、例えば、RAM、ROM、およびEEPROMであってよく、非接触カード104は、これらのメモリのうちの1つ以上を含んでよい。読み出し専用メモリは、工場出荷時に読み出し専用としてプログラム可能であってもよいし、ワンタイムプログラム可能であってもよい。ワンタイムプログラマブルは、一度書き込んだら何度でも読み出す機会を提供する。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時点でプログラムできる。一度プログラムされたメモリは、書き直すことはできないが、何度でも読み出すことができる。読み出し/書き込みメモリは、工場出荷後に何度もプログラムされ、再プログラムされる可能性がある。読み出し/書き込みメモリは、工場出荷後に何度も読み出されることもある。ある実施態様では、メモリ108は、データを暗号化するためにプロセッサ612によって実行される暗号化アルゴリズムを利用する暗号化メモリであってもよい。

20

30

【0080】

メモリ108は、1つ以上のアプレット110、1つ以上のカウンタ116、固有ID112、マスターキー114、UDK118、多様化キー120、PANシーケンス144、および設定情報148を記憶し得る。設定情報148は、サーバ106によって生成された1つ以上のトークンを含むことができる。1つ以上のアプレット110は、Java（登録商標）カードアプレットなど、1つ以上の非接触カード104上で実行する1つ以上のソフトウェアアプリケーションを含み得る。しかし、アプレット110はJavaカードアプレットに限定されるものではなく、非接触カードまたは限られたメモリを有する他の装置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ってもよいことが理解される。1つ以上のカウンタ116は、整数を記憶するのに十分な数値カウンタを含んでもよい。一意のID112は、非接触カード104に割り当てられた一意の英数字識別子を含んでもよく、識別子は、非接触カード104を他の非接触カード104から区別してもよい。いくつかの例では、固有ID112は、顧客とその顧客に割り当てられた口座の両方を識別できる。

40

【0081】

前述の例示的な実施形態のプロセッサ612およびメモリ要素は、接触パッド608を参照して説明されているが、本開示はこれに限定されない。これらの要素は、接触パッド608の外部に実装されてもよいし、接触パッド608から完全に分離されてもよいし、接触パッド608内に配置されたプロセッサ612およびメモリ108要素に加えて、さ

50

らなる要素として実装されてもよいことが理解される。

【0082】

いくつかの例では、非接触カード104は、1つ以上のアンテナ614を含み得る。1つ以上のアンテナ614は、非接触カード104内で、接触パッド608の処理回路610の周囲に配置されてもよい。例えば、1つ以上のアンテナ614は、処理回路610と一体であってもよく、1つ以上のアンテナ614は、外部ブースターコイルと共に使用されてもよい。別の例として、1つ以上のアンテナ614は、接触パッド608および処理回路610の外部にあってもよい。

【0083】

一実施形態では、非接触カード104のコイルは、空芯変圧器の二次側として機能してもよい。端末は、電力または振幅変調を切断することによって非接触カード104と通信できる。非接触カード104は、非接触カード104の電力接続のギャップを使用して、端末から送信されたデータを推測してもよく、このデータは、1つ以上のコンデンサを介して機能的に維持されてもよい。非接触カード104は、非接触カード104のコイル上の負荷をスイッチングすることによって、または負荷変調によって、通信を送り返してもよい。負荷変調は、干渉によって端末のコイルで検出されることがある。より一般的には、アンテナ614、プロセッサ612、および／またはメモリ108を使用して、非接触カード104は、NFC、ブルートゥース、および／またはWi-Fi通信を介して通信するための通信インタフェースを提供する。

【0084】

上記で説明したように、非接触カード104は、Javaカードのような限られたメモリを有するスマートカードまたは他の装置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てもよく、1つ以上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てもよい。アプレット110は、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において多要素認証(MFA)のためのワンタイムパスワード(OTP)を提供するために非接触カードに追加されてもよい。アプレット110は、(例えば、モバイルコンピュータ装置102またはPOS端末の)モバイルNFCリーダなどのリーダからの近距離データ交換要求などの1つ以上の要求に応答し、NDEFテキストタグとして符号化された暗号的に安全なOTPからなるNDEFメッセージを生成してもよい。NDEFメッセージは、暗号122または暗号204付きURLなどの暗号、およびその他のデータを含むことができる。

【0085】

NDEF OTPの一例は、NDEFショートレコードレイアウト(SR=1)である。このような例では、1つ以上のアプレット110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し得る。いくつかの例では、NDEFメッセージは1つ以上のレコードを含み得る。

【0086】

いくつかの例では、1つ以上のアプレット110は、RFIDタグをエミュレートしてもよい。RFIDタグは、1つ以上の多形タグを含むことができる。いくつかの例では、タグが読み取られるたびに、非接触カードの真正性を示す可能性のある異なる暗号データが提示される。1つ以上のアプレット110に基づいて、タグのNFC読み取りが処理され、データがバンキングシステムのサーバなどのサーバに送信され、データがサーバで検証され得る。

【0087】

いくつかの例では、非接触カード104およびサーバは、カードが適切に識別されるように、特定のデータを含むことができる。非接触カード104は、1つ以上の固有の識別子(図示せず)を含むことができる。読み取り操作が行われるたびに、カウンタ116はインクリメントし得ることがある。いくつかの例では、非接触カード104からのデータが(例えば、装置によって)読み取られるたびに、カウンタ116は検証のためにサーバに送信され、カウンタ116が(検証の一部として)サーバのカウンタと等しいかどうかを判定する。

【0088】

1つ以上のカウンタ116は、リプレイ攻撃を防止してもよい。たとえば、暗号が取得され、リプレイされた場合、カウンタ116が読み取られたか、使用されたか、または他の方法で引き渡された場合、その暗号は直ちに拒否される。カウンタ116が使用されていない場合は、リプレイされ得る。いくつかの例では、非接触カード104でインクリメントされるカウンタは、トランザクションのためにインクリメントされるカウンタとは異なる。非接触カード104上ではアプレット110間の通信がないため、非接触カード104はアプリケーショントランザクションカウンタ116を決定できない。いくつかの例では、非接触カード104は、トランザクションアプレットである可能性のある第1アプレット440-1と、第2アプレット440-2を含み得る。各アプレット440-1、440-2は各々のカウンタ116を含んでもよい。

10

【0089】

いくつかの例では、カウンタ116は同期しない場合がある。いくつかの例では、斜めに読み取るなど、トランザクションを開始する偶発的な読み取りを考慮するために、カウンタ116はインクリメントしてもよいが、アプリケーションはカウンタ116を処理しない場合がある。

【0090】

カウンタ116を同期状態に保つために、コンピュータ装置102が起動したことを検出し、検出によって発生した読み取りがカウンタ116を進めることを示す銀行システムのサーバと同期する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が実行されてもよい。他の例では、ハッシュ化されたワンタイムパスワードは、誤同期のウィンドウが受け入れられるように利用されることがある。例えば、閾値10以内であれば、カウンタ116は進めてもよい。しかし、異なる閾値内、例えば10または1000内であれば、ユーザの装置を介して、ユーザがタップ、ジェスチャー、またはその他の方法で1回または複数回指示することを1つ以上のアプリケーションを介して要求する、再同期を実行するための要求が処理されてもよく、カウンタ116が適切な順序で増加すれば、ユーザがそうしたことを知ることができる。

20

【0091】

カウンタ116、マスターキー114、UDK118、および多様化キー120を参照して本明細書で説明するキーの多様化技法は、キーの多様化技法による暗号化および／または復号化の一例である。

30

【0092】

非接触カード104の作成プロセスにおいて、2つの暗号キーがカードごとに一意に割り当てられてもよい。暗号キーは、データの暗号化と復号化の両方で使用される対称キーを含み得る。トリプルDES(3DES)アルゴリズムは、EMVで使用されることがあり、非接触カード104のハードウェアで実装される。キー多様化プロセスを使用することにより、キー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、1つ以上のキーをマスターキーから導出できる。

【0093】

いくつかの例では、脆弱性の影響を受けやすい3DESアルゴリズムの欠陥を克服するために、セッションキーが導出されてもよいが(セッションごとに一意のキーなど)、マスターキーを使用するのではなく、固有のカード導出キー(例えば、UDK118)およびカウンタがダイビングデータとして使用されてもよい。例えば、非接触カード104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キーが使用されてもよい。この結果、暗号の三重化が実現する。セッションキーは、1つ以上のアプレットによって生成され、1つ以上のアルゴリズム(EMV 4.3 Book 2 A1.3.1 Common Session Key Derivationで定義される)でアプリケーショントランザクションカウンタを使用することによって導出されてもよい。

40

【0094】

さらに、各カードのインクリメントは一意であってもよく、個人化によって割り当てら

50

れるか、または何らかの識別情報によってアルゴリズム的に割り当てられる。例えば、奇数番号のカードは2ずつインクリメントし、偶数番号のカードは5ずつインクリメントできる。いくつかの例では、インクリメントはまた、1つのカードが1、3、5、2、2、...を繰り返して順番にインクリメントするように、順次読み取りで変化できる。特定のシーケンスまたはアルゴリズムシーケンスは、個人化時に定義されてもよいし、一意の識別子から派生する1つ以上のプロセスから定義されてもよい。これにより、リプレイ攻撃者が少数のカード例から一般化することを困難にできる。

【0095】

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。

【0096】

図7は、例示的な実施形態によるNDEFショートレコードレイアウト（SR=1）データ構造700を示す。1つ以上のアプレット110は、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OTPをエンコードし得る。いくつかの例では、NDEFメッセージは1つ以上のレコードを含む。アプレットは、OTPレコードに加えて、1つ以上の静的タグレコードを追加し得る。例示的なタグは、限定されないが、タグタイプ：周知のタイプ、テキスト、英語のエンコード（en）；アプレットID：D2760000850101；性能：読み込み専用アクセス；エンコード：認証メッセージはASCII16進数としてエンコードされ得る可能性があるタイプ長値（TLV）データは、NDEFメッセージの生成に使用されるパーソナライゼーションパラメータとして提供される。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周知のインデックスを持つ、最初のレコードを含み得る。データ構造700は、暗号122または暗号204付きURLなどの暗号、およびアプレット110によって提供される任意の他のデータを含み得る。

【0097】

図8は、先に説明したような様々な実施形態を実装するのに適した例示的なコンピュータアーキテクチャ800の一実施形態を示す。一実施形態では、コンピュータアーキテクチャ800は、コンピューティングアーキテクチャ100および／または200の一部を含むか、または一部として実装されてもよい。幾つかの実施形態では、コンピューティングシステム800は、例えば、非接触カード104、コンピュータ装置102、および／またはサーバ106を代表するものであってもよい。実施形態は、この文脈において限定されない。より一般的には、コンピューティングアーキテクチャ800は、図1Aないし7を参照して本明細書に記載されるすべての論理、アプリケーション、システム、方法、装置、および機能を実装する。

【0098】

本出願で使用される場合、「システム」および「構成要素」という用語は、ハードウェア、ハードウェアとソフトウェアとの組み合わせ、ソフトウェア、または実行中のソフトウェアのいずれかであるコンピュータ関連エンティティを指すことを意図しており、その例は、例示的なコンピューティングコンピュータアーキテクチャ800によって提供される。例えば、コンポーネントは、プロセッサ上で実行されるプロセス、プロセッサ、ハードディスクドライブ、（光学的および／または磁氣的記憶媒体の）複数の記憶ドライブ、オブジェクト、実行可能ファイル、実行スレッド、プログラム、および／またはコンピュータであり得るが、これらに限定されない。例示として、サーバ上で実行されるアプリケーションとサーバの両方がコンポーネントであり得る。1つ以上のコンポーネントは、プロセスおよび／または実行のスレッド内に存在でき、コンポーネントは、1つのコンピュータ上に局在でき、および／または2つ以上のコンピュータ間に分散できる。さらに、コンポーネントは、様々な種類の通信媒体によって互いに通信可能に結合され、動作を調整できる。この調整には、単方向または双方向の情報交換が関わる。例えば、構成部分は、通信媒体を介して通信される信号の形で情報を通信できる。情報は、様々な信号線に割り当てられた信号として実装できる。このような割り当てでは、各メッセージは信号である

10

20

30

40

50

。しかしながら、さらなる実施形態では、代替的にデータメッセージを採用できる。そのようなデータメッセージは、様々な接続を介して送信できる。例示的な接続は、パラレルインタフェース、シリアルインタフェース、およびバスインタフェースを含む。

【0099】

コンピュータアーキテクチャ800は、1つ以上のプロセッサ、マルチコアプロセッサ、コプロセッサ、メモリユニット、チップセット、コントローラ、周辺機器、インタフェース、発振器、タイミング装置、ビデオカード、オーディオカード、マルチメディア入出力（I/O）構成要素、電源などのさまざまな共通のコンピューティング要素を含む。しかし、実施形態は、コンピューティングコンピュータアーキテクチャ800による実装に限定されない。

【0100】

図8に示すように、コンピュータアーキテクチャ800は、プロセッサ802、システムメモリ804、およびシステムバス806からなるコンピュータ812を含む。プロセッサ802は、様々な市販のプロセッサのいずれでもよい。コンピュータ812は、コンピュータ装置102および／またはサーバ106を代表できる。

【0101】

システムバス806は、システムメモリ804を含むがこれに限定されないシステムコンポーネントのプロセッサ802へのインタフェースを提供する。システムバス806は、市販されている様々なバスアーキテクチャのいずれかを使用して、メモリバス（メモリコントローラの有無にかかわらず）、周辺バス、およびローカルバスにさらに相互接続できる、いくつかのタイプのバス構造のいずれかとできる。インタフェースアダプタは、スロットアーキテクチャを介してシステムバス806に接続できる。例示的なスロットアーキテクチャは、限定されないが、アクセラレーテッドグラフィックスポート（AGP）、カードバス、（拡張）業界標準アーキテクチャ（（E）ISA）、マイクロチャネルアーキテクチャ（MCA）、NuBus、ペリフェラルコンポーネントインターコネクト（拡張）（PCI（X））、ピーシーアイエクスプレス、PCメモ리카ード国際協会（PCMCIA）などを含む。

【0102】

コンピュータアーキテクチャ800は、様々な製造品を含むか、または実装できる。製造品は、ロジックを記憶するコンピュータ可読記憶媒体を含むことができる。コンピュータ可読記憶媒体の例は、揮発性メモリまたは不揮発性メモリ、取外し可能メモリまたは取外し不可能メモリ、消去可能メモリまたは消去不可能メモリ、書込み可能メモリまたは再書込み可能メモリなどを含む、電子データを記憶できる任意の有形媒体を含むことができる。ロジックの例は、ソースコード、コンパイルコード、インタプリタコード、実行可能コード、静的コード、動的コード、オブジェクト指向コード、ビジュアルコードなど、任意の適切なタイプのコードを使用して実装される実行可能なコンピュータプログラム命令を含み得る。実施形態はまた、少なくとも部分的に、非一過性のコンピュータ可読媒体に含まれ得、または、非一過性のコンピュータ可読媒体に含まれる命令として実装され得、命令は、本明細書で説明される動作の実行を可能にするために、1つ以上のプロセッサによって読み取られ、実行され得る。

【0103】

システムメモリ804は、読み出し専用メモリ（ROM）、ランダムアクセスメモリ（RAM）、ダイナミックRAM（DRAM）、ダブルデータレートDRAM（DDRAM）、シンクロナスDRAM（SDRAM）、スタティックRAM（SRAM）、プログラマブルROM（PROM）、消去可能プログラマブルROM（EPROM）、電氣的に消去可能なプログラマブルROM（EEPROM）、フラッシュメモリ、強誘電体ポリマーメモリなどのポリマーメモリ、オボニックメモリ、相変化メモリまたは強誘電体メモリ、シリコン-酸化物-窒化物-酸化物-シリコン（SONOS）メモリ、磁気カードまたは光カード、レイド（RAID：Redundant Array of Independent Disks）ドライブなどの装置のアレイ、ソリッドステートメモリ装置（例えば、USBメモリ、ソリッドステートドライブ（SSD））、およ

10

20

30

40

50

び情報を記憶するのに適した他のあらゆるタイプの記憶媒体などの1つ以上の高速メモリユニットの形態の様々なタイプのコンピュータ可読記憶媒体を含むことができる。図8に示す図示の実施形態では、システムメモリ804は、不揮発性808および／または揮発性810を含むことができる。基本入出力システム（BIOS）は、不揮発性808に格納できる。

【0104】

コンピュータ812は、内蔵（または外付け）ハードディスクドライブ814、リムーバブル磁気ディスク818から読み出しまたはリムーバブル磁気ディスク818に書き込むための磁気ディスクドライブ816、およびリムーバブル光ディスク822（例えば、CD-ROMまたはDVD）から読み出しまたはリムーバブル光ディスク822に書き込む光ディスクドライブ820を含む、1つ以上の低速メモリユニットの形態の様々なタイプのコンピュータ可読記憶媒体を含むことができる。ハードディスクドライブ814、磁気ディスクドライブ816、および光ディスクドライブ820は、それぞれ、HDDインタフェース824、およびFDDインタフェース826、および光ディスクドライブインタフェース828によってシステムバス806に接続され得る。外部ドライブ実装用のHDDインタフェース824は、ユニバーサルシリアルバス（USB）およびIEEE 1394インタフェース技術の少なくとも1つまたは両方を含むことができる。

【0105】

ドライブおよび関連するコンピュータ可読媒体は、データ、データ構造、コンピュータ実行可能命令などの揮発性および／または不揮発性ストレージを提供する。たとえば、オペレーティングシステム830、1つ以上のアプリケーション832、他のプログラムモジュール834、およびプログラムデータ836を含む、多数のプログラムモジュールをドライブおよび不揮発性808、および揮発性810に格納できる。一実施形態では、1つ以上のアプリケーション832、他のプログラムモジュール834、およびプログラムデータ836は、例えば、システム100の様々なアプリケーションおよび／またはコンポーネントを含み得る。

【0106】

ユーザは、例えばキーボード838やマウス840などのポインティング装置のような1つ以上の有線／無線入力装置を介して、コマンドや情報をコンピュータ812に入力できる。他の入力装置は、マイクロフォン、赤外線（IR）リモートコントロール、無線周波数（RF）リモートコントロール、ゲームパッド、スタイラスペン、カードリーダー、ドングル、指紋リーダー、手袋、グラフィックタブレット、ジョイスティック、キーボード、網膜リーダー、タッチスクリーン（例えば、静電容量式、抵抗式など）、トラックボール、トラックパッド、センサ、スタイラスなどを含み得る。これらおよび他の入力装置は、システムバス806に結合される入力装置インタフェース842を介してプロセッサ802に接続されることが多いが、パラレルポート、IEEE1394シリアルポート、ゲームポート、USBポート、IRインタフェースなどの他のインタフェースによって接続することもできる。

【0107】

モニター844または他のタイプのディスプレイ装置も、ビデオアダプタ846などのインタフェースを介してシステムバス806に接続される。モニター844は、コンピュータ812の内部であっても外部であってもよい。モニター844に加えて、コンピュータは通常、スピーカ、プリンタなどの他の周辺出力装置を含む。

【0108】

コンピュータ812は、リモートコンピュータ848などの1つ以上のリモートコンピュータへの有線および／または無線通信を介した論理接続を使用して、ネットワーク環境で動作できる。リモートコンピュータ848は、ワークステーション、サーバコンピュータ、ルータ、パーソナルコンピュータ、ポータブルコンピュータ、マイクロプロセッサベースの娯楽用電化製品、ピア装置、または他の一般的なネットワークノードとでき、典型的には、コンピュータ812に関連して説明した多くの要素またはすべての要素を含むが

10

20

30

40

50

、簡潔にするために、メモリおよび／または記憶装置 850 のみが図示される。描かれている論理接続は、ローカルエリアネットワーク 852 および／またはより大規模なネットワーク、例えばワイドエリアネットワーク 854 への有線／無線接続を含む。このような LAN および WAN ネットワーキング環境は、オフィスおよび会社において一般的であり、イントラネットのような企業全体のコンピュータネットワークを容易にし、そのすべてが、例えばインターネットのようなグローバル通信ネットワークに接続できる。

【0109】

ローカルエリアネットワーク 852 ネットワーキング環境で使用される場合、コンピュータ 812 は、有線および／または無線通信ネットワークインタフェースまたはネットワークアダプタ 856 を介してローカルエリアネットワーク 852 に接続される。ネットワークアダプタ 856 は、ローカルエリアネットワーク 852 への有線および／または無線通信を容易にでき、ネットワークアダプタ 856 の無線機能と通信するためにその上に配置された無線アクセスポイントを含むこともできる。

10

【0110】

広域ネットワーク 854 のネットワーキング環境で使用される場合、コンピュータ 812 はモデム 858 を含むことができ、あるいは広域ネットワーク 854 上の通信サーバに接続され、あるいはインターネットによるなど、広域ネットワーク 854 を介して通信を確立するための他の手段を有する。モデム 858 は、内部または外部、および有線および／または無線の装置とでき、入力装置インタフェース 842 を介してシステムバス 806 に接続する。ネットワーク環境では、コンピュータ 812 に関連して描かれたプログラムモジュール、またはその一部を、リモートメモリおよび／または記憶装置 850 に格納できる。図示したネットワーク接続は例示的なものであり、コンピュータ間の通信リンクを確立する他の手段を使用できることが理解されるであろう。

20

【0111】

コンピュータ 812 は、有線および無線装置または IEEE 802 ファミリーの規格を使用するエンティティ、例えば無線通信（例えば、IEEE 802.11 無線変調技術）で動作可能に配置された無線装置と通信するように動作可能である。これには、少なくとも Wi-Fi（または Wireless Fidelity）、WiMax、およびブルートゥース（登録商標）無線技術などが含まれる。Wi-Fi ネットワークは、IEEE 802.11（a、b、g、n、ac、ax など）と呼ばれる無線技術を使用し、安全で信頼性が高く、高速な無線接続を提供する。Wi-Fi ネットワークは、コンピュータ同士、インターネット、有線ネットワーク（IEEE 802.3 関連のメディアと機能を使用）への接続に使用できる。

30

【0112】

図 1 A ないし 12 を参照して先に説明したような装置の様々な要素は、様々なハードウェア要素、ソフトウェア要素、またはその両方の組み合わせを含み得る。ハードウェア要素の例としては、装置、論理装置、構成部分、プロセッサ、マイクロプロセッサ、回路、プロセッサ、回路素子（例えば、トランジスタ、抵抗器、コンデンサ、インダクタなど）、集積回路、特定用途向け集積回路（ASIC）、プログラマブル論理装置（PLD）、デジタル信号プロセッサ（DSP）、フィールドプログラマブルゲートアレイ（FPGA）、メモリユニット、論理ゲート、レジスタ、半導体装置、チップ、マイクロチップ、チップセットなどを挙げることができる。ソフトウェア要素の例には、ソフトウェア部品、プログラム、アプリケーション、コンピュータプログラム、アプリケーションプログラム、システムプログラム、ソフトウェア開発プログラム、マシンプログラム、オペレーティングシステムソフトウェア、ミドルウェア、ファームウェア、ソフトウェアモジュール、ルーチン、サブルーチン、機能、方法、手順、ソフトウェアインタフェース、アプリケーションプログラムインタフェース（API）、命令セット、コンピューティングコード、コンピュータコード、コードセグメント、コンピュータコードセグメント、単語、値、記号、またはそれらの任意の組み合わせが含まれ得る。しかしながら、実施形態がハードウェア要素および／またはソフトウェア要素を使用して実装されるかどうかを決定することは、所与の実装に対して所望される計算速度、電力レベル、熱許容範囲、処理サイクルバジェット、

40

50

入力データ速度、出力データ速度、メモリリソース、データバス速度、および他の設計または性能制約など、任意の数の要因に従って変化し得る。

【0113】

少なくとも1つの実施形態の1つ以上の態様は、プロセッサ内の様々なロジックを表す、機械可読媒体に格納された代表的な命令によって実装されてもよく、この命令が機械によって読み取られると、機械は、本明細書で説明する技術を実行するロジックを生成する。「IPコア」として知られるこのような表現は、有形の機械可読媒体に格納され、論理またはプロセッサを製造する製造機械にロードするために、様々な顧客または製造施設に供給され得る。いくつかの実施形態は、例えば、機械によって実行されると、実施形態に従った方法および／または動作を機械に実行させ得る命令または命令のセットを記憶し得る機械可読媒体または物品を使用して実施され得る。そのような機械は、例えば、任意の適切な処理プラットフォーム、コンピューティングプラットフォーム、コンピュータ装置、処理装置、コンピューティングシステム、処理システム、コンピュータ、プロセッサなどを含むことができ、任意の適切なハードウェアおよび／またはソフトウェアの組み合わせを使用して実装され得る。機械可読媒体または物品は、例えば、メモリ、取り外し可能または取り外し不可能な媒体、消去可能または消去不可能な媒体、書き込み可能または再書き込み可能な媒体を含むことができる、デジタルまたはアナログ媒体、ハードディスク、フロッピーディスク、読み出し専用コンパクトディスク（CD-ROM）、書き込み可能コンパクトディスク（CD-R）、書き替え可能コンパクトディスク（CD-RW）、光ディスク、磁気媒体、光磁気媒体、取り外し可能なメモリカードまたはディスク、様々なタイプのデジタル多用途ディスク（DVD）、テープ、カセットなど、任意の適切なタイプのメモリユニット、メモリ装置、メモリ物品、メモリ媒体、記憶装置、記憶物品、記憶媒体および／または記憶ユニットを含み得る。命令は、ソースコード、コンパイルされたコード、解釈されたコード、実行可能なコード、静的コード、動的コード、暗号化されたコードなど、任意の適切なタイプのコードを含むことができ、任意の適切な高レベル、低レベル、オブジェクト指向、視覚的、コンパイルされたおよび／または解釈されたプログラミング言語を使用して実装される。

10

20

【0114】

上述した装置の構成要素および機能は、ディスクリート回路、特定用途向け集積回路（ASIC）、論理ゲートおよび／またはシングルチップアーキテクチャの任意の組み合わせを使用して実装できる。さらに、装置の特徴は、マイクロコントローラ、プログラマブルロジックアレイおよび／またはマイクロプロセッサ、又は好適には前述の任意の組合せを用いて実装できる。ハードウェア、ファームウェアおよび／またはソフトウェア要素は、本明細書において、集合的にまたは個々に、「論理」または「回路」と呼ばれ得ることに留意されたい。

30

【0115】

上述したブロック図に示された例示的な装置は、多くの潜在的な実装の機能的に説明的な一例を表すことがあることが理解されるであろう。したがって、添付の図に描かれるブロック機能の分割、省略、または包含は、これらの機能を実装するハードウェア構成要素、回路、ソフトウェア、および／または要素が、実施形態において必ずしも分割、省略、または包含されることを推論しない。

40

【0116】

少なくとも1つのコンピュータ可読記憶媒体は、実行されたときに、本明細書で説明するコンピュータ実装方法のいずれかをシステムに実行させる命令を含むことができる。

【0117】

いくつかの実施形態は、「一実施形態（one embodiment）」または「一実施形態（an embodiment）」という表現を、それらの派生語とともに用いて説明されることがある。これらの用語は、実施形態に関連して説明される特定の特徵、構造、または特性が、少なくとも1つの実施形態に含まれることを意味する。本明細書の様々な箇所で「一実施形態において」という表現が現れるが、必ずしもすべてが同じ実施形態を指すわけでは

50

ない。さらに、特に断らない限り、上述した特徴は、任意の組み合わせで一緒に使用可能であると認識される。従って、別々に説明した特徴は、その特徴が互いに互換性がないと指摘されない限り、互いに組み合わせて採用できる。

【0118】

本開示の要約は、読者が技術開示の性質を迅速に把握できるように提供されるものであることを強調する。本開示の要約は、特許請求の範囲の範囲または意味を解釈または制限するために使用されないことを理解した上で提出される。さらに、前述の詳細な説明では、開示を合理化する目的で、様々な特徴が単一の実施形態にまとめられていることが分かる。この開示方法は、特許請求される実施形態が、各請求項に明示的に記載されている以上の特徴を必要とするという意図を反映していると解釈されるべきではない。むしろ、以下の請求項が反映するように、発明的主題は、単一の開示された実施形態の全ての特徴よりも少ない特徴にある。従って、以下の特許請求の範囲は、各請求項を別個の実施形態として独立させた状態で、本明細書に組み込まれる。添付の特許請求の範囲において、用語「を含む (including)」および「において (in which)」は、それぞれ、各用語「構成される (comprising)」および「において (wherein)」の平易な英語での等価物として使用される。さらに、「第1」、「第2」、「第3」などの用語は、単にラベルとして使用されており、その対象に数値要件を課すことを意図していない。

10

【0119】

上述したことは、開示された構造の例を含む。もちろん、構成要素および／または方法論の考え得るすべての組み合わせを説明することは不可能であるが、当業者であれば、さらに多くの組み合わせおよび順列が可能であることを認識し得る。したがって、新規なアーキテクチャは、添付の特許請求の範囲の精神および範囲内に入る、そのような変更、修正および変形をすべて包含することが意図される。

20

【0120】

例示的な実施形態の前述の説明は、例示および説明の目的で提示されたものである。これは、網羅的であること、または本開示を開示された正確な形態に限定することを意図するものではない。本開示に照らして、多くの修正および変形が可能である。本開示の範囲は、この詳細な説明によってではなく、むしろ本明細書に添付された特許請求の範囲によって限定されることが意図される。本出願の優先権を主張する将来の出願は、異なる態様で開示された主題を請求でき、一般に、本明細書において様々に開示されるかまたは他の方法で示されるような1つ以上の制限の任意のセットを含むことができる。

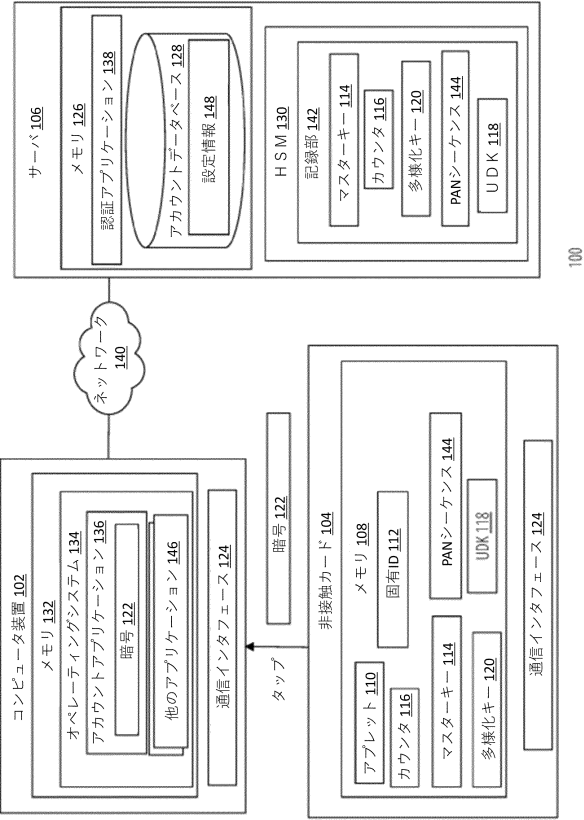
30

40

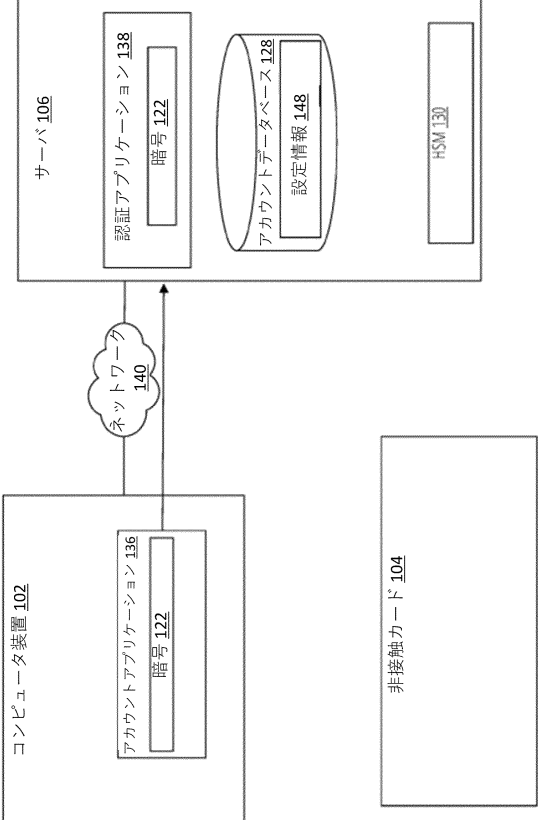
50

【図面】

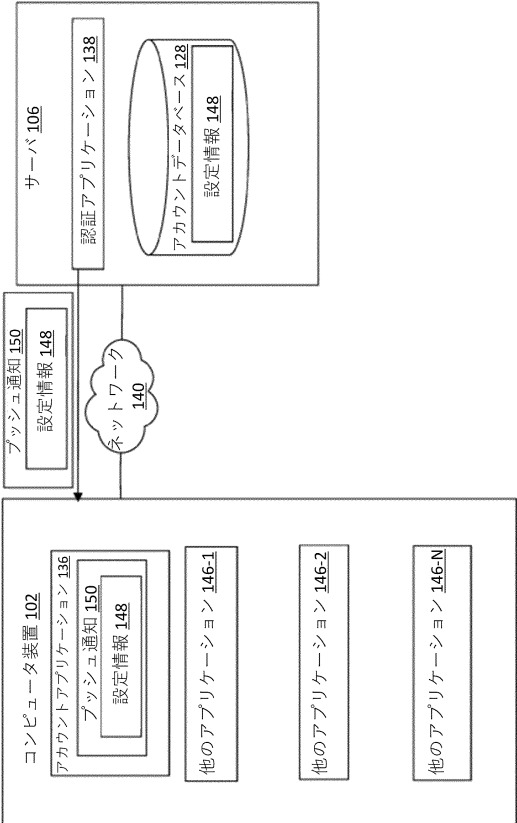
【図 1 A】



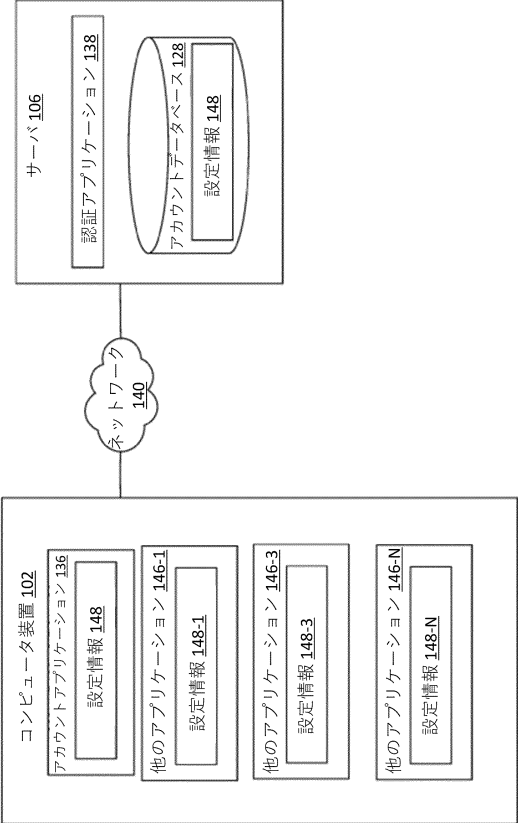
【図 1 B】



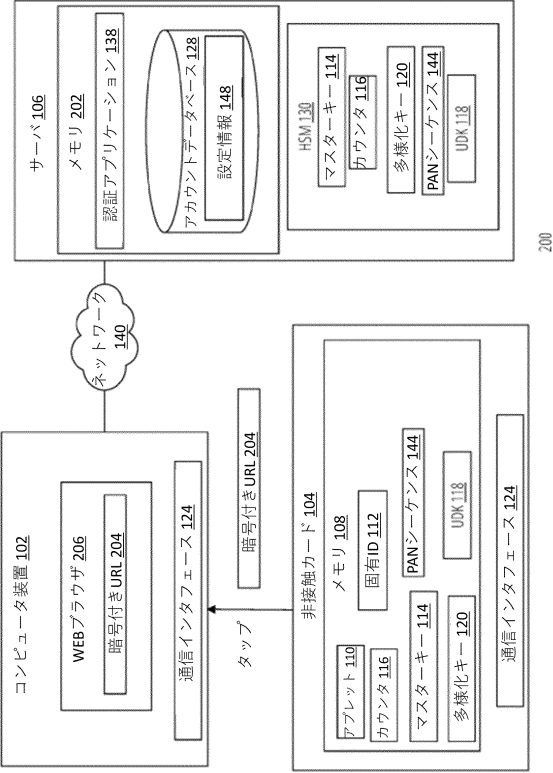
【図 1 C】



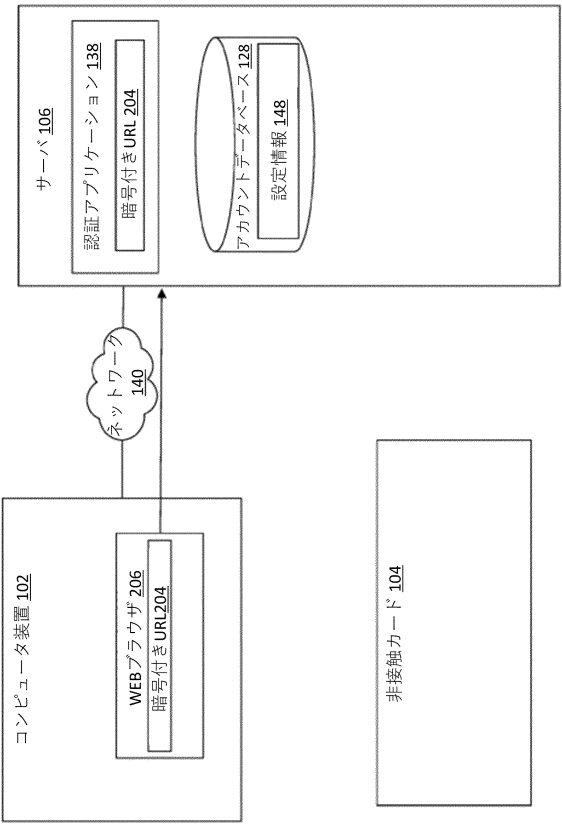
【図 1 D】



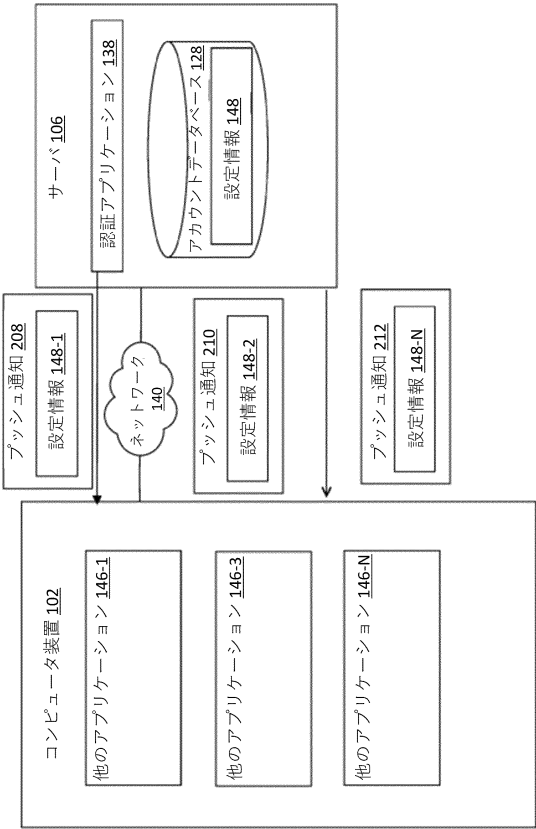
【図 2 A】



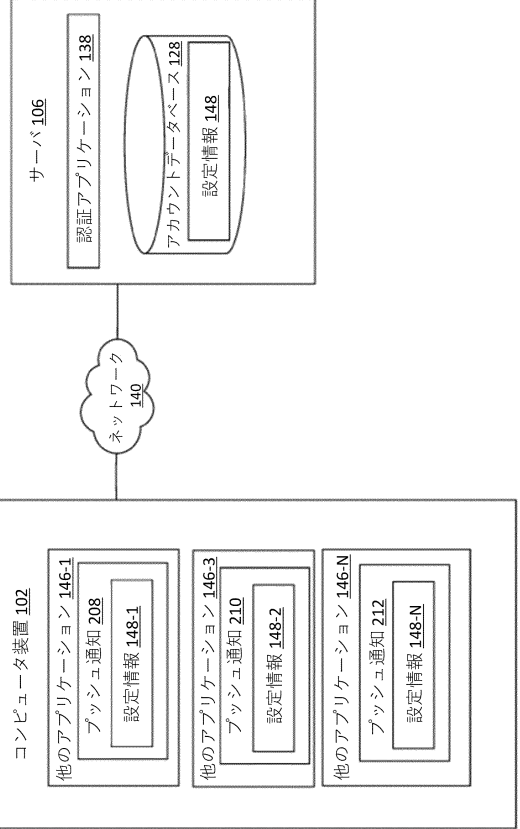
【図 2 B】



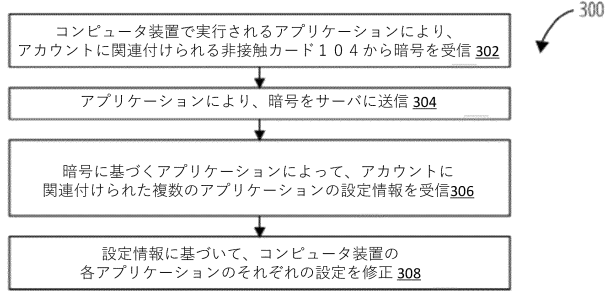
【図 2 C】



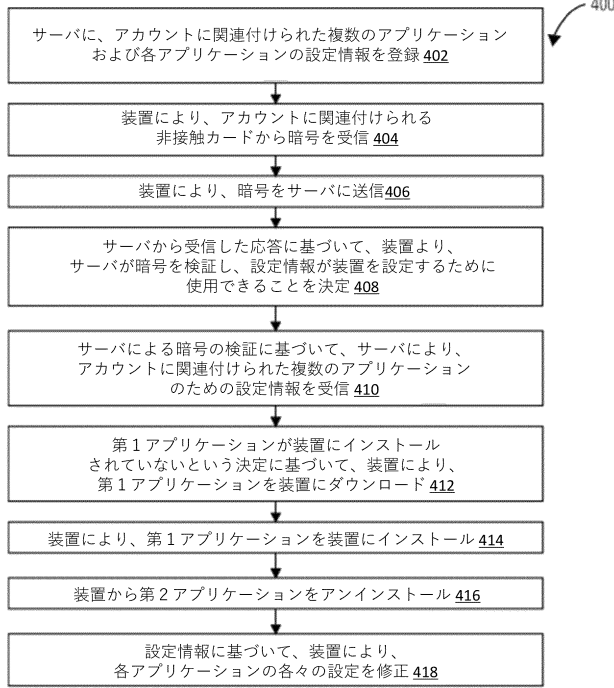
【図 2 D】



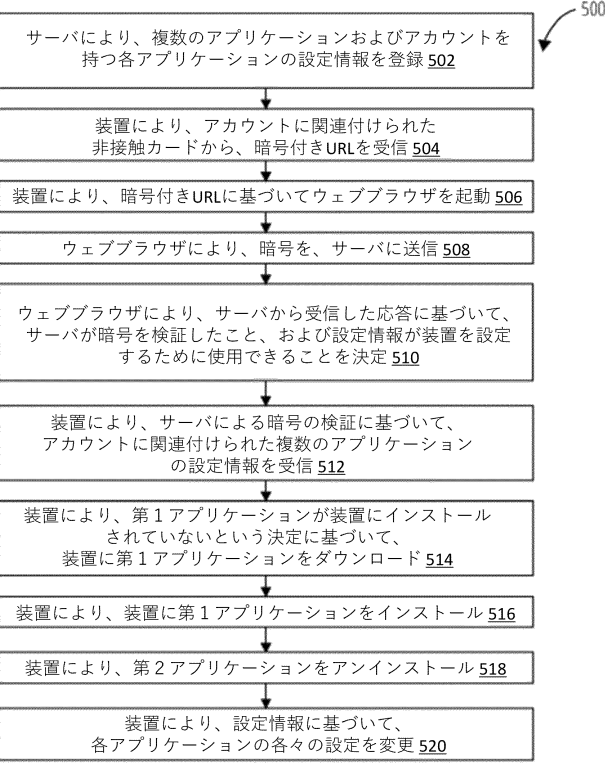
【図 3】



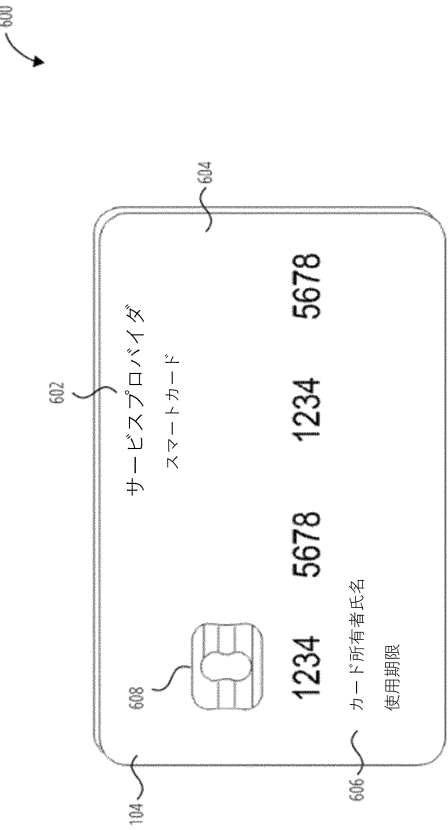
【図 4】



【図 5】



【図 6 A】



10

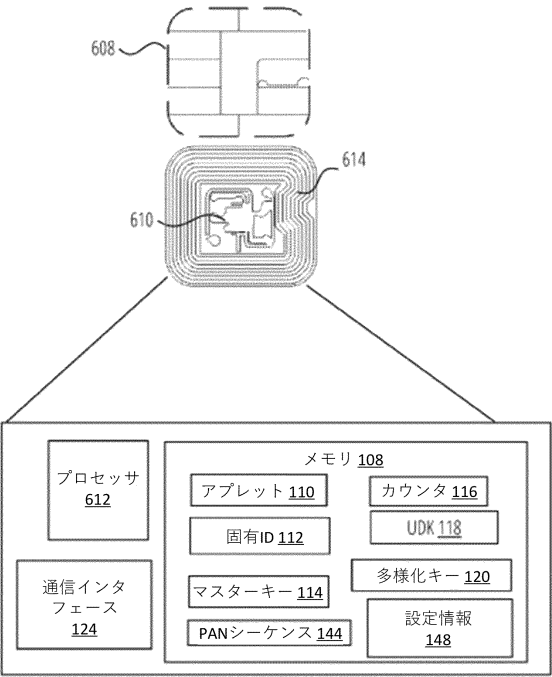
20

30

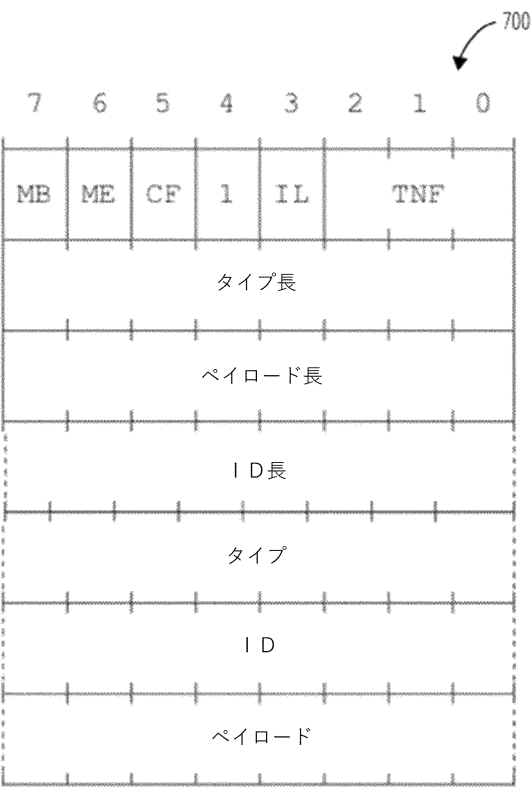
40

50

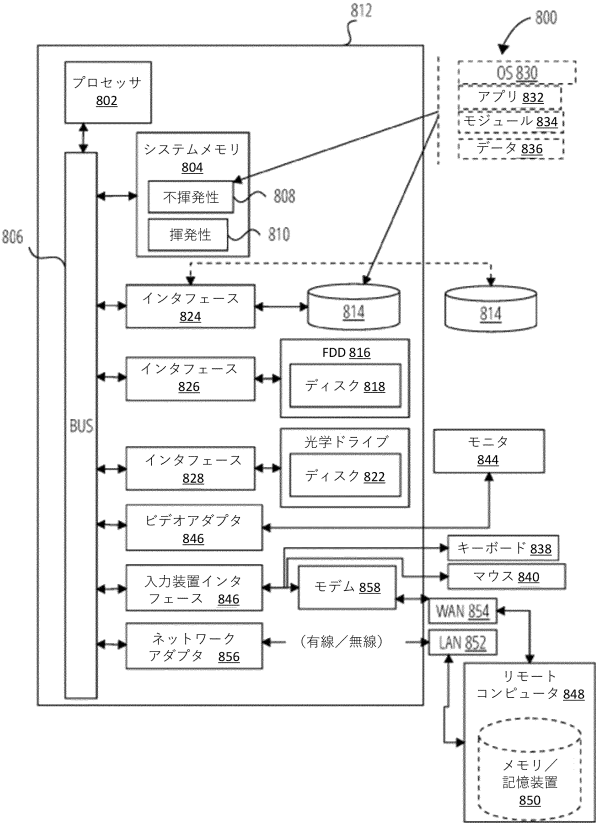
【図 6 B】



【図 7】



【図 8】



10

20

30

40

50

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2023/019567

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04W12/30 H04W12/47 H04W12/106 H04W12/069
ADD. H04L9/40

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W H04L G06Q G06F

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

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

EPO-Internal, WPI Data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2020/250659 A1 (RULE JEFFREY [US] ET AL) 6 August 2020 (2020-08-06) paragraph [0018] - paragraph [0062] figures 1A-7 -----	1-20
X	US 2021/201296 A1 (RULE JEFFREY [US] ET AL) 1 July 2021 (2021-07-01) paragraph [0020] - paragraph [0071] figures 1A-10 -----	1-20
A	US 2020/184462 A1 (RULE JEFFREY [US] ET AL) 11 June 2020 (2020-06-11) paragraph [0021] - paragraph [0148] figures 1A-8 -----	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

18 July 2023

Date of mailing of the international search report

26/07/2023

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Ghomrasseni, Z

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2023/019567

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2020250659 A1	06-08-2020	AU 2020215026 A1	20-05-2021
		CA 3118911 A1	06-08-2020
		CN 113302954 A	24-08-2021
		EP 3918820 A1	08-12-2021
		JP 7225413 B2	20-02-2023
		JP 2022524269 A	02-05-2022
		JP 2023058595 A	25-04-2023
		KR 20210120978 A	07-10-2021
		SG 11202104525X A	28-05-2021
		US 10467622 B1	05-11-2019
		US 2020250659 A1	06-08-2020
		US 2022318790 A1	06-10-2022
		US 2023222485 A1	13-07-2023
		WO 2020160065 A1	06-08-2020
US 2021201296 A1	01-07-2021	AU 2020418476 A1	19-05-2022
		CA 3155736 A1	08-07-2021
		CN 114902220 A	12-08-2022
		EP 4085360 A1	09-11-2022
		JP 2023510172 A	13-03-2023
		KR 20220120555 A	30-08-2022
		US 2021201296 A1	01-07-2021
		US 2022398566 A1	15-12-2022
US 2020184462 A1	11-06-2020	US 2020184462 A1	11-06-2020
		US 2021117957 A1	22-04-2021
		US 2022188807 A1	16-06-2022
		US 2023004953 A1	05-01-2023

フロントページの続き

,MC,ME,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,
ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,C
O,CR,CU,CV,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,I
R,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,MG,MK,MN,MU,MW
,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL
,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW
アメリカ合衆国 2 2 1 0 2 バージニア州マククリーン、キャピタル・ワン・ドライブ 1 6 8 0、キャ
ピタル・ワン・サービスーズ・リミテッド・ライアビリティ・カンパニー内
(72)発明者 オズボーン、ケビン
アメリカ合衆国 2 2 1 0 2 バージニア州マククリーン、キャピタル・ワン・ドライブ 1 6 8 0、キャ
ピタル・ワン・サービスーズ・リミテッド・ライアビリティ・カンパニー内
(72)発明者 ルール、ジェフリー
アメリカ合衆国 2 2 1 0 2 バージニア州マククリーン、キャピタル・ワン・ドライブ 1 6 8 0、キャ
ピタル・ワン・サービスーズ・リミテッド・ライアビリティ・カンパニー内

F ターム (参考) 5B376 CA29 CA47