

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6438989号  
(P6438989)

(45) 発行日 平成30年12月19日 (2018. 12. 19)

(24) 登録日 平成30年11月22日 (2018. 11. 22)

(51) Int. Cl. F I  
**G06Q 20/38 (2012.01)** G O 6 Q 20/38 3 1 0  
**G06Q 20/34 (2012.01)** G O 6 Q 20/34 3 7 0

請求項の数 20 外国語出願 (全 31 頁)

(21) 出願番号	特願2017-35054 (P2017-35054)	(73) 特許権者	503260918
(22) 出願日	平成29年2月27日 (2017. 2. 27)		アップル インコーポレイテッド
(62) 分割の表示	特願2015-557060 (P2015-557060) の分割		Apple Inc.
原出願日	平成26年2月6日 (2014. 2. 6)		アメリカ合衆国 95014 カリフォル ニア州 クパチーノ アップル パーク ウェイ ワン One Apple Park Way, Cupertino, Californ ia 95014, U. S. A.
(65) 公開番号	特開2017-134848 (P2017-134848A)	(74) 代理人	100076428
(43) 公開日	平成29年8月3日 (2017. 8. 3)		弁理士 大塚 康徳
審査請求日	平成29年3月23日 (2017. 3. 23)	(74) 代理人	100115071
(31) 優先権主張番号	61/761, 654		弁理士 大塚 康弘
(32) 優先日	平成25年2月6日 (2013. 2. 6)	(74) 代理人	100112508
(33) 優先権主張国	米国 (US)		弁理士 高柳 司郎

最終頁に続く

(54) 【発明の名称】 セキュアエレメントのトランザクション及びアセットの管理のための装置及び方法

(57) 【特許請求の範囲】

【請求項 1】

セキュアエレメントを含むクライアント装置において、  
前記クライアント装置または前記セキュアエレメントを一意に特定する特定情報を前記セキュアエレメントから取得することと、

仮想化交換媒体 (VME) を前記クライアント装置に提供するための提供要求をリモートサーバに送信することとであって、前記提供要求が前記セキュアエレメントから取得された前記特定情報を含む、送信することと、

前記VMEに関連付けられたアセット識別子を、前記提供要求に応じて前記リモートサーバから受信することと、

前記VMEの配信のための配信要求を前記リモートサーバに送信することとであって、前記配信要求は前記アセット識別子を含むことと、

前記VMEを、前記配信要求に応じて前記リモートサーバから受信することと、

前記VMEを前記セキュアエレメントに提供することと、を含む方法。

【請求項 2】

小売商装置とトランザクションを実行し、前記VMEに関連付けられたユーザアカウントに課金することをさらに含む請求項 1 に記載の方法。

【請求項 3】

前記VMEはバーチャルクレジットカードである請求項 1 または 2 に記載の方法。

【請求項 4】

前記特定情報は、前記セキュアエレメントが前記VMEに対応するアカウントに関連付けられていることを証明する請求項1から3のいずれか一項に記載の方法。

【請求項5】

前記VMEは前記セキュアエレメントについて一意のキーを用いて暗号化される請求項1から4のいずれか一項に記載の方法。

【請求項6】

前記特定情報は装置識別子を含む請求項1から5のいずれか一項に記載の方法。

【請求項7】

前記VMEを受信することの前に、

前記セキュアエレメントに事前にロードされた一回使用の値を含むチャレンジ値を前記セキュアエレメントから取得することと、

前記チャレンジ値を前記リモートサーバに送信することと、をさらに含む請求項1から6のいずれか一項に記載の方法。

【請求項8】

メモリとプロセッサとを備えるクライアント装置であって、

前記メモリは、前記プロセッサによって実行された場合に前記クライアント装置に動作を実行させる命令を含み、

前記動作は、

前記クライアント装置のセキュアエレメントから、前記クライアント装置または前記セキュアエレメントを一意に特定する特定情報を取得することと、

仮想化交換媒体(VME)を前記クライアント装置に提供するための提供要求をリモートサーバに送信することであって、前記提供要求が前記セキュアエレメントから取得された前記特定情報を含む、送信することと、

前記VMEに関連付けられたアセット識別子を、前記提供要求に応じて前記リモートサーバから受信することと、

前記VMEの配信のための配信要求を前記リモートサーバに送信することであって、前記配信要求は前記アセット識別子を含むことと、

前記VMEを、前記配信要求に応じて前記リモートサーバから受信することと、

前記VMEを前記セキュアエレメントに提供することと、を含むクライアント装置。

【請求項9】

前記動作は、小売商装置とトランザクションを実行し、前記VMEに関連付けられたユーザアカウントに課金することをさらに含む請求項8に記載のクライアント装置。

【請求項10】

前記VMEはバーチャルクレジットカードである請求項8または9に記載のクライアント装置。

【請求項11】

前記特定情報は、前記セキュアエレメントが前記VMEに対応するアカウントに関連付けられていることを証明する請求項8から10のいずれか一項に記載のクライアント装置

。

【請求項12】

前記VMEは前記セキュアエレメントについて一意のキーを用いて暗号化される請求項8から11のいずれか一項に記載のクライアント装置。

【請求項13】

前記特定情報は装置識別子を含む請求項8から12のいずれか一項に記載のクライアント装置。

【請求項14】

前記動作は、

前記VMEを受信することの前に、

前記セキュアエレメントに事前にロードされた一回使用の値を含むチャレンジ値を前記セキュアエレメントから取得することと、

10

20

30

40

50

前記チャレンジ値を前記リモートサーバに送信することと、をさらに含む請求項 8 から 13 のいずれか一項に記載のクライアント装置。

【請求項 15】

命令を含むコンピュータプログラムであって、  
前記命令は、クライアント装置のプロセッサによって実行された場合に前記クライアント装置に動作を行わせ、

前記動作は、

前記クライアント装置のセキュアエレメントから、前記クライアント装置または前記セキュアエレメントを一意に特定する特定情報を取得することと、

仮想化交換媒体（VME）を前記クライアント装置に提供するための提供要求をリモートサーバに送信することであって、前記提供要求が前記セキュアエレメントから取得された前記特定情報を含む、送信することと、

前記VMEに関連付けられたアセット識別子を、前記提供要求に応じて前記リモートサーバから受信することと、

前記VMEの配信のための配信要求を前記リモートサーバに送信することであって、前記配信要求は前記アセット識別子を含むことと、

前記VMEを、前記配信要求に応じて前記リモートサーバから受信することと、

前記VMEを前記セキュアエレメントに提供することと、を含むコンピュータプログラム。

【請求項 16】

前記動作は、小売商装置とトランザクションを実行し、前記VMEに関連付けられたユーザアカウントに課金することをさらに含む請求項 15 に記載のコンピュータプログラム。

【請求項 17】

前記VMEはバーチャルクレジットカードである請求項 15 または 16 に記載のコンピュータプログラム。

【請求項 18】

前記特定情報は、前記セキュアエレメントが前記VMEに対応するアカウントに関連付けられていることを証明する請求項 15 から 17 のいずれか一項に記載のコンピュータプログラム。

【請求項 19】

前記VMEは前記セキュアエレメントについて一意のキーを用いて暗号化される請求項 15 から 18 のいずれか一項に記載のコンピュータプログラム。

【請求項 20】

前記動作は、

前記VMEを受信することの前に、

前記セキュアエレメントに事前にロードされた一回使用の値を含むチャレンジ値を前記セキュアエレメントから取得することと、

前記チャレンジ値を前記リモートサーバに送信することと、をさらに含む請求項 15 から 19 のいずれか一項に記載のコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は全般的にセキュア機器のトランザクションの分野に関し、より詳細には、例示的な一実施形態における、金融商品及び他のアセットの展開に関する。

【背景技術】

【0002】

顧客及び小売商は一般に、金融及び他の関連するトランザクションを行うための便利でセキュアな手段を望む。クレジットカード、デビットカード、プリペイドカード、ギフトカード、クーポン、等、といったアセットはすべて、大きく「仮想化」された性質の通貨

10

20

30

40

50

の例である。具体的には、商品及び／又はサービスに対して物理的な通貨又は物理的なクーポンを実際に交換するのではなく、トランザクションは、例えば、口座番号又は「プロキシ」口座番号（例えば、店頭でのトランザクションの処理を目的に作成されたものであり、実際の貸方（credit）口座番号でも借方（debit）口座番号でもない）とともに行われており、資金は電子的に貸方記入／借方記入されている。

#### 【0003】

残念ながら、本明細書に詳述する理由により、それらのアセットを分配するための既存のソリューションは非効率であり、上手くいかない傾向にある。例えば、バーチャルウォレットパラダイムは、先存するアカウントに基づくことができ、金融取引を行うため、クライアント装置のユーザは、ウォレットサービスを伴う先存するアカウントを有する必要がある、（例えば、ウォレットに関連付けられているアカウントデータベースを提供する信頼されたエンティティ）、又はウォレットサービスに先払いしておく必要がある。加えて、既存のアセットは「代替可能」でなく、作成されると特定の用途専用となる。

10

#### 【0004】

顧客及び小売商は、トランザクション上の複雑さ及び／又は利便性（更に広がるモバイルデバイスの使用を含む）において着実に進化しているため、アセットを分配するための新規及び改善されたスキームが必要となっている。理想的には、そのようなソリューションは、顧客、小売商、及び振り出しエンティティに対して、アセットのフレキシビリティを損なうことなく、合理的で便利な管理機能を提示すべきである。

#### 【発明の概要】

20

#### 【0005】

本開示は、特に、セキュアエレメントのトランザクション及びアセットの管理のための装置及び方法を提供することで、先のニーズに対処する。

#### 【0006】

一実施形態では、アセットをクライアント装置へ分配するための方法が開示されている。この方法は、アセットをアカウントへ提供する要求をクライアント装置から受信することにより実行され得る。アセットを提供する要求は、クライアント装置を一意的に識別する装置識別子が伴われ得る。次に、アセットを提供する要求は認証される。ある場合には、アセットを提供する要求は、装置識別子を使用して、クライアント装置がアカウントに関連付けられているか検証することにて認証されている。要求を認証すると、アセットはアカウントに提供され、このアセットはクライアント装置に割り当てられる。次に、割り当てられたアセットを一意的に識別するアセット識別子が、アセットロッカーなどのリモート装置から受信される。アセット識別子は続いて、クライアント装置に送信される。その後、クライアント装置は、アセット識別子を使用して、割り当てられたアセットを要求し得る。割り当てられたアセット及びアセット識別子に対する要求をクライアント装置から受信すると、割り当てられたアセットは、クライアント装置に配信される。

30

#### 【0007】

別の実施形態では、アセットをクライアント装置へ分配するための方法が開示されている。クライアント装置は、クライアント装置を一意的に識別する装置識別子に関連付けられている。この方法は、クライアント装置に対するアセットを予め構成することにより実行されている。予め構成するプロセスは、（i）装置識別子に基づいてユニークキーとともにアセットを暗号化すること、（ii）アセットにチャレンジデータを埋め込むこと、及び／又は（iii）アセットをユーザアカウントと関連付けること、を含み得る。それに応じて、アセットは、クライアント装置に対して構成される又は「パーソナライズ」される。次に、予め構成されたアセットが、アセット識別子に関連付けられる。実施形態の一態様では、アセット識別子は、アセットを予め構成することの前に、クライアント装置に提供されている。クライアント装置は続いて、予め構成されたアセットを要求し得る。この要求は、アセット識別子を含み得る。要求を受信すると、予め構成されたアセットは、クライアント装置に配信され得る。

40

#### 【0008】

50

更に別の実施形態では、コンピュータ可読記憶媒体が開示されている。コンピュータ可読記憶媒体は、クライアント装置のプロセッサにより実行されると、クライアント装置に、アセットをアカウントへ提供する要求を送らせる命令を記憶する。要求は、リモート装置へ送信され得る。アカウントは、クライアント装置のユーザに関連付けられ得る。要求と併せて、クライアント装置は、クライアント装置を一意的に識別する装置識別子を送り得る。実施形態の一態様では、装置識別子は、クライアント装置内に配設されたセキュアエレメント上に記憶されている。更に、1つ以上のチャレンジも、セキュアエレメント上に記憶され得る。命令は更に、クライアント装置に、チャレンジをリモート装置へ送信させる。クライアント装置は続いて、リモート装置からアセットを受信し得る。受信したアセットは、受信したアセットが有効であるか検証するためにセキュアエレメントが使用し得るチャレンジデータを含み得る。チャレンジデータは、送信されたチャレンジに基づくことができる。

10

【0009】

この説明される実施形態の概要は、本明細書で説明する主題のいくつかの態様の基本的理解を提供するように、いくつかの例示的实施形態を要約することを目的として提供されるものにすぎない。したがって、上述した特徴が例にすぎず、いかなる方法でも本明細書で説明する主題の範囲又は趣旨を狭めるように解釈すべきではないことが了解されよう。本明細書で説明する主題の他の特徴、態様及び利点は、後続の詳細な説明、図及び請求の範囲から明らかになるであろう。

【0010】

20

本発明の他の態様及び利点は、例として、説明される実施形態の原理を例示する添付図とともに考慮される、下記の「発明を実施するための形態」から明らかとなるであろう。

【図面の簡単な説明】

【0011】

記載の実施形態は、以下の記載及び添付の図面を参照することによって一層良好に理解することができる。加えて、以下の記載及び添付の図面を参照することにより、記載の実施形態の利点を一層良好に理解することができる。

【0012】

【図1】本開示による、トランザクショナルネットワークの1つの例示的な構成の図形表現である。

30

【0013】

【図2】本開示による、プロビジョニングシステムの1つの例示的な構成の図形表現である。

【0014】

【図3A】本開示による、クライアント装置の例示的な一実施形態の論理ブロック図である。

【0015】

【図3B】本開示による、小売商装置の例示的な一実施形態の論理ブロック図である。

【0016】

【図4】本開示による、アセットエージェントの例示的な一実施形態の論理ブロック図である。

40

【0017】

【図5】本開示による、アセットブローカのアカウントサーバの例示的な一実施形態の論理ブロック図である。

【0018】

【図6】本開示による、アセットロッカーの例示的な一実施形態の論理ブロック図である。

【0019】

【図7】本開示による、アセットを分配するための一般化された方法の一実施形態の論理フローダイアグラムである。

50

【 0 0 2 0 】

【図 8】本開示による、例示的なプロビジョニングトランザクションを表す論理ラダーダイアグラムである。

【 0 0 2 1 】

【図 9 A】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。

【図 9 B】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。

【 0 0 2 2 】

【図 1 0 A】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。

10

【図 1 0 B】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。

【 0 0 2 3 】

【図 1 1】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。

【 0 0 2 4 】

【図 1 2】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。

【 0 0 2 5 】

20

【図 1 3 A】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。

【図 1 3 B】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。

【図 1 3 C】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。

【発明を実施するための形態】

【 0 0 2 6 】

本出願による方法及び装置の代表的な適用を、本セクションで説明する。これらの実施例は、説明する実施形態を理解する上での文脈と手助けを加えることのみを目的として提供される。それゆえ、説明される実施形態は、これらの具体的な詳細の一部又はすべてを伴わずに実践することができる点が、当業者には明白となるであろう。他の場合、説明される実施形態を不必要に不明瞭化することを回避するために、周知のプロセスステップは、詳細には説明されていない。他の適用が可能であり、以下の例は限定的なものと解釈されるべきでない。

30

【 0 0 2 7 】

以下の発明を実施するための形態では、その説明の一部を形成し、説明される実施形態による具体的な実施形態が実例として示される、添付図面が参照される。これらの実施形態は、当業者が説明される実施形態を実施できるように十分詳細に説明されるが、これらの例は限定的なものでなく、他の実施形態が使用されてもよく、説明される実施形態の趣旨又は範囲から逸脱せずに変更が行われてもよいということが理解されよう。

40

【 0 0 2 8 】

仮想化された「ウォレット」は、顧客、小売商、及び金融機関に対して大きな利点を提供し得る。仮想化されたウォレットのバーチャル「コンテンツ」は、1つ以上のアセットを含み得る。いずれのエンティティ（例えば、ユーザ、小売商、金融機関、等）も、適切に有効にされたセキュア機器との間でそれらのアセットを自由に転送し得、そのうえ、それらのアセットはフレキシブルに記憶、バックアップ、等、され得る。既存のソリューションは、例えば、分配、アップデート、パッチング、等、特定の基本トランザクションを、インターネットプロトコル（IP）ネットワークを介して提供する。しかし、金融トランザクション及び情報の機密性により、窃盗、悪用、悪意のある行為、等を防止するために

50

有意のセキュリティ対策が必要である。

【 0 0 2 9 】

本説明の文脈について、本開示を通しての実施形態は、仮想化交換媒体（VME）の形式をとるアセットを説明することに注意すべきである。仮想化交換媒体の一般例は、クレジット「カード」番号、デビット「カード」番号、プリペイド「カード」番号、アカウント情報、及び仮想通貨、等、を含むがこれらに限定しない。より一般的には、仮想化交換媒体はまた、例えば、電子クーポン、電子商品券、電子チケット、電子パス、等、実際の価値を伴わない手段も包含する。この説明は限定するものでなく、説明された実施形態は、有用なものと及び/又は価値のあるものすべての分配に使用されることが理解されるべきである。更に、VMEは、複雑さにおいて多岐に渡る、多種多様なデータ構造（例えば、10 スtring、アレイ、オブジェクト、暗号エレメント、等）内に実装され得、例えば、シンプルな実装は、シンプルな口座番号とされ得、より複雑な実装は、アカウント情報、及び/又はチェック値を組み込み得る。いくつかの場合では、VMEは、例えば、暗号保護、アカウントビリティ（つまり、トランザクション履歴）、匿名性、不正検知、等、といった、更なる機能を提供し得る。

【 0 0 3 0 】

説明された実施形態は、セキュアトランザクション及びVMEの管理のための方法及び装置に関する。一実施形態では、プロビジョニングシステムは、VMEをクライアント装置へ分配する。プロビジョニングシステムは、L1、L2、及びL3として参照され得る、20 3つのレベルを有するセキュリティプロトコルにしたがってVMEを管理し、クライアント装置へ分配する1つ以上のエンティティを含む。L1では、VMEは安全に生成され、記憶され、及び暗号化されている。L1は、1つ以上のアセットロッカーにより促進され得る。L2は、VMEの有効なコピー数を制御及び管理する。L2は、VMEの不注意な複製及び/又は悪意のある複製を防ぎ得る。実施形態の一態様では、L2は、1つ以上のチャレンジを使用し得、VMEの第1のコピーが分配された後での、VMEの二重のコピーを無効にする。L2は、1つ以上のアセットエージェントにより促進され得る。L3は、意図されたクライアント装置へのアセットの分配を認証及び認可する。実施形態の一態様では、L3は、認証プロセス中に、クライアント装置内に配設されたセキュアエレメントから取得した識別子を使用し得る。L3はまた、認証プロセス中に、ユーザのアカウントに関連付けられている情報を使用し得る。L3は、1つ以上のアセットブローカにより促進され得る。30

【 0 0 3 1 】

一実施形態では、クライアント装置とプロビジョニングシステムとの間のプロビジョニングトランザクションが開示されている。プロビジョニングシステムは、アセットブローカと、アセットエージェントと、アセットロッカーと、を含む。クライアント装置は、クライアント装置に関連付けられている装置識別子を含む。識別子は、クライアント装置内に配設されたセキュアエレメント内に記憶され、暗号化され得る。ユーザアカウントは、クライアント装置がユーザ（つまり、顧客）により購入されると作成され得る。あるいは、ユーザアカウントは、クライアント装置が購入されると、ユーザにより識別される、先存するアカウントとされ得る。クライアント装置は、アセットブローカからVMEを要求し、例えば、装置識別子などの識別情報を提供する。アセットブローカは、識別情報を認証し、SE/クライアント装置がユーザアカウントに関連付けられていることを判定する。40 認証されると、アセットブローカは、SEの署名をアセットエージェントに転送し得る。アセットエージェントは、セキュアエレメントの識別を検証し、セキュアエレメントに対するVMEを識別する。次に、セキュアエレメントは、チャレンジをプロビジョニングシステムへ提供する。提供されたチャレンジに基づくチャレンジデータは、アセットエージェントにより、VME内に埋め込まれ得る。それに応じて、チャレンジデータは、VMEのコピーが二重に発行されることの防止に使用され得る。アセットロッカーは続いて、クライアント装置のセキュアエレメントに対して、VMEに関連付けられている識別子、例えば、VME識別子を提供し得る。VME識別子を受信すると、クライアント装置はそ50

の後、VME 識別子を使用して、アセットブローカからVME の配信を要求し得る。

【0032】

別の実施形態では、VME の構成及び配信は、セキュアエレメントを有するクライアント装置をユーザが購入するまで延期され得る。このようにして、クライアント装置は、VME を伴って製造又は予めプログラムされない。むしろ、クライアント装置は、クライアント装置をユーザへ配信することの前に、VME に予め割り当てられているよう、「予めパーソナライズ」されている。「予めのパーソナライゼーション」プロセスは、プロビジョニングシステム内に記憶されたVME を、クライアント装置に関連付けられている識別子と関連付けることを含み得る。購入時には、認証情報がユーザにより提供される。移送期間中（例えば、ユーザがクライアント装置を購入した時と、ユーザがVME を要求した時との間の時間、及び/又は、クライアント装置をユーザへ出荷するために要する時間との間）は、VME は、クライアント装置に対して予め構成され得る。VME を予め構成することは、(i) セキュアエレメントに特有のキーを伴ってVME を暗号化することと、(ii) VME 内にチャレンジデータを埋め込むことと、(iii) VME を認証情報と関連付けること、を含み得る。VME は続いて、VME 識別子に関連付けられる。次に、クライアント装置は、VME 識別子を使用してVME を要求し得る。同様に、プロビジョニングシステムは、予め構成されたクライアント装置へVME を配信し得る。このようにして、VME は、リアルタイムでのトラフィックを必要とすることなく、VME が要求されると、クライアント装置に途切れなくロードされ得る。

10

【0033】

更に別の実施形態では、VME のプールからのVME は、VME に対する要求をクライアント装置から受信する前に、クライアント装置に対して割り当てられている（例えば、VME のプール内のそれぞれのVME は、最初は、特定のクライアント装置に関連付けられていない）。クライアント装置が購入されると、認証情報がユーザにより提供される。クライアント装置はユーザへ提供され得る。クライアント装置に加えて、クライアント装置を認証するために使用され得る識別情報、例えば、クライアント装置を一意的に識別する装置識別子も、ユーザへ提供される。例えば、装置識別子は、クライアント装置が梱包されている箱上に配設されたステッカから収集され得る。クライアント装置は続いて、ユーザの命令にて、VME のアクティベーションを要求する際に、装置識別子をプロビジョニングシステムへ提供し得る。

20

30

【0034】

それら及び他の実施形態が、図1～図13Cを参照して以下に説明されている。しかしながら、これらの図に関して本明細書に記載される「発明を実施するための形態」は、説明を目的とするものにすぎず、限定するものとして解釈するべきではないことが、当業者には容易に理解されるであろう。

【0035】

ここで図1を参照すると、1つの例示的トランザクショナルネットワーク100が示される。例示的トランザクショナルネットワーク100は、1つ以上のクライアント装置102と、1つ以上の小売商装置（「販売時点情報管理システム」（POS）とも呼ばれる）104と、1つ以上のバックエンドサーバ106と、を含む。先のトランザクショナルネットワーク100は、広範に可能なネットワークトポロジ及び機能を単に示していることが、当業者には容易に理解されるであろう。そのうえ、様々な実装は、図1に示す様々なエンティティを組み合わせてもよく、及び/又は更に分割してもよいことが認識されるべきである。

40

【0036】

トランザクションは、クライアント装置102がトランザクション情報を暗号により符号化し、小売商装置104へ送信すると行われる。一例では、クライアント装置102は、例えば、（近距離無線通信（NFC）、等といった）適切なリーダー上でスワイプすること、グラフィカルユーザインタフェース（GUI）からトランザクション識別子（例えば、バーコード、数字、等）を目視確認することに、等により、トランザクションを小売

50

商装置 104 とともに実行するよう構成されたバーチャル「ウォレット」を含み得る。別の例では、クライアント装置 102 は、クライアント装置 102 の存在を小売商装置 104 (例えば、レジスター、モバイルタブレット、等) にアラートするために使用されている、全地球測位システム (GPS) 受信機又は他の位置情報 (例えば、Wi-Fi (登録商標) の存在、等) を含み得、既知のユーザアカウントの課金を認可するため、それに続くクライアント装置 102 のユーザの妥当性検証 (例えば、顔写真などの生体認証) が行われる。トランザクション情報は、(i) エイリアス、(ii) 増分カウンタ、(iii) 乱数、(iv) 小売商識別子、(v) 他のトランザクションエラーラ (例えば、取引金額、タイムスタンプ、ロケーションスタンプ、等)、の組み合わせを含み得る。

**【0037】**

小売商装置 104 は、保護されたトランザクション情報をバックエンドサーバ 106 へ提供する。その後は、バックエンドサーバ 106 は、保護されたトランザクション情報を復号し、トランザクションを検証し、トランザクションを適切に処理し得る。例えば、エイリアス値がクレジットカード番号にマップされており、暗号化された情報が正しいと、続いてバックエンドサーバ 106 が、エイリアス値にマップされているクレジットカード番号とともにトランザクションを処理する。あるいは、トランザクション情報が破損している、又は不正であることが判明すると、トランザクションは拒否される。

**【0038】**

例示的トランザクショナルネットワーク 100 内では、トランザクション情報に適用された暗号保護は、ユーザの価値のある情報をいずれの悪意のある他者及び/又は小売商から保護する。具体的には、悪意のある他者がトランザクション情報を奪おうとしても、又は、小売商装置 104 が (例えば、ウイルス、等に) 感染していても、暗号保護は、トランザクションが後に不正に再生されることを防止するよう援助し得る。それに応じて、ユーザ保護を最大化するため、暗号エレメントは、セキュアプロセッサ、セキュアファイルシステム、及びオペレーショナルメモリを含んでもよい、クライアント装置 102 内に配設されたセキュアエレメント内に物理的に保護されている。しかし、クライアントの機器内に記憶された暗号マテリアルのセキュリティを保つことが難しいことを当業者は認識するであろう。例えば、1つのそのような問題は、初期構成、展開、及び保守である。クライアント装置は、(信頼されていない場合もある) 機器製造業者により製造されている。また、特定のビジネスモデルは、(信頼されていない場合もある) 第三者としての参加者の市場に依存することもある。

**【0039】**

理想的には、暗号マテリアルを分配するためのソリューションは、大規模分配ネットワークに渡ってスケラブルであるべきである。そのうえ、分配スキームは、暗号マテリアル (証明書) を、いずれの仲介エンティティ (例えば、機器製造業者、第三者ブローカ、等) から保護しなければならない。いくつかの実施形態では、暗号マテリアルは固有であるべきである (つまり、単一のアセットインスタンスが単一のセキュアエレメントのみの内で一度に使用可能である)。最後に、ソリューションは、リアルタイムでの双方向作用に対する要件を最小化すべきである。

**【0040】**

ここで図 2 を参照すると、1つの例示的プロビジョニングシステム 200 が示される。示すように、プロビジョニングシステム 200 は、クライアント装置 300 と、アセットエージェント 400 と、アセットブローカ 500 と、アセットロッカー 600 と、を含む。前述するように、VME 動作の文脈内では、VME セキュリティは更に、レベル 1 (L1)、レベル 2 (L2)、及びレベル 3 (L3) を含むレベルに下位分割され得る。それぞれのレベルは、プロビジョニングシステム 200 のエレメントにより促進され得る。

**【0041】**

アセットロッカー 600 は、レベル 1 (L1) のセキュリティにしたがって VME セキュリティを行うために使用され得る。本明細書にて使用されるように、レベル 1 のセキュリティは一般的に、VME 内に含まれる秘密及び/又は暗号マテリアル (例えば、セキュ

10

20

30

40

50

アキー、暗号マテリアル、ユーザ履歴、等)を保護するよう構成されたセキュリティメカニズムを指すが、これらに限定しない。更に、用語「セキュリティ」とは、概して、データ及び/又はソフトウェアの保護を指す。例えば、暗号セキュリティは、VMEに関連付けられたデータ及び/又はソフトウェアを、無認可のアクティビティ及び/又は悪意の第三者による、窃盗、悪用、破壊、公開、及び/又は改竄から保護する。

【0042】

アセットエージェント400は、レベル2(L2)のセキュリティにしたがってVMEセキュリティを行うために使用され得る。本明細書にて使用されるように、レベル2のセキュリティは一般的に、VMEの予期しない複製及び/又は悪意のある複製を防止するためのセキュリティメカニズムを指すが、これらに限定しない(保存エンフォースメント)。更に、用語「保存性」、「保存する」、及び「保存された」とは、本明細書で使用する時、簡単に増加又は減少させることができない、(物理的又は仮想的のいずれかの)要素を指す。例えば、保存されたVMEは、通常動作の間にコピー又は複製することができない。更には、本明細書で使用する時、(物理的又は仮想的のいずれかの)要素に適用される用語「固有性」とは、その要素が、特定の特性及び/又は特質を有する唯一無二の要素であるという特性を指す。例えば、固有のVMEは、複製のVMEを有し得ない。

10

【0043】

アセットブローカ500は、レベル3(L3)のセキュリティにしたがってVMEセキュリティを行うために使用され得る。本明細書にて使用されるように、レベル3のセキュリティは一般的に、意図されたユーザ(例えば、個人、企業、マシンクライアント、等)に関連付けられている機器(例えば、クライアント装置、POS、等)へVMEを安全に配信するセキュリティメカニズムと呼ばれるが、これらに限定しない。その上に、本明細書で使用するように、用語「ユーザ認可」とは、概して、リソースに対するユーザのアクセスを指定することを指す。一般的な交換媒体(クレジットカード、デビットカード、現金)では、トランザクションは、媒体の物理的な所有を要求し得、物理的なカードは、ユーザにより保護されている。例えば、物理的なクレジットカードが使用される場合、カードはユーザの所有にある(及び、ユーザにより暗黙に認可されている)ことが想定されている。VME動作の文脈の範囲内では、VME移動のユーザ認可に対する類似の機能が必要である。特に、VMEの「所有者」(及び、プロビジョニングシステム200も)は、VMEが1つ以上の正当な機器にのみ移されたことを保証する必要がある。

20

30

【0044】

以降に明確にされる理由として、セキュリティのそれぞれのレベルは、限定された機能/責任一式に関連付けられており、したがって、レベル2のセキュリティを提供する機器は、レベル2に関連付けられているアクションを自由に行い得るが、VMEのレベル1の要素に影響を与えることが可能なレベル1のセキュリティでもある必要がある。例えば、(以下に詳述される)アセットエージェントは、VMEが複製されることを防止するが、しかし、このアセットエージェントは、VME内に含まれる暗号マテリアルを変更する機能を有する必要はなく、破損した暗号マテリアルを検出する義務を負うアセットエージェントである必要もない。

【0045】

VMEセキュリティレベルの先の定義は純粋に例示的なものであり、本明細書の説明を限定する意図はない。事実、先の専門用語は当業者の間での「業界用語」とみなされるべきであり、関連産業及び/又は技術の初期の進化の点から変更されるであろうことが理解されよう。

40

【0046】

ソフトウェアは一般的に、ハードウェアよりも柔軟であり、例えば、ソフトウェアは、コピー、修正、及び配布が容易であることが理解されよう。更には、ソフトウェアは、多くの場合、ハードウェアの均等物よりも安価に、電力効率的に、物理的に小さく作製することができる。しかし、VMEデータの機密性(例えば、顧客財務情報、アセットブローカの暗号の秘密、等)は特別な配慮が必要とされる。ユーザ保護のために、VMEの意図

50

されない複製、及び/又は破損が防止されなければならないことが予期される。それに応じて、VME動作は、(i)セキュリティ、(ii)固有性、及び(iii)保存の特性を満たすべきである。

【0047】

例示的な一実施形態では、セキュアエレメントへのVMEの配信を有効にする分配インフラストラクチャが開示されている。セキュアエレメントは、クライアント装置及び/又は小売商装置内に配設され得る。そのうえ、開示されているインフラストラクチャの様々な機能は、個人(例えば、機器製造業者、第三者小売商、顧客、等)が、インフラストラクチャの各部をホストし得るよう、フレキシブルに仕切られ得及び/又は適合され得、そのような断片的なソリューションは、それぞれ個々の当事者のニーズに最適化され得る。依然として更に、例示的な実施形態は、動作における冗長性を提供し得る。

10

【0048】

ここで図3Aを参照すると、1つの例示的なクライアント装置300が提示されている。例示的なクライアント装置300は、クライアントと小売商との間のインタフェース302と、プロセッササブシステム304と、非一時的コンピュータ可読媒体(メモリサブシステム)306と、セキュアエレメント308と、を含む。いくつかの変形例では、セキュアエレメント308は、セキュアプロセッサ308Aと、セキュアな非一時的コンピュータ可読媒体(セキュアメモリ)308Bと、を更に含む。本明細書にて使用されるように、用語「クライアント装置」は、ユーザのVMEのうちの1つ以上と取引及び/又は管理するよう構成されている機器を含むがこれに限定しない。クライアント装置の一般例は、特に、無線対応セルラー電話、(例えば、iPhone(登録商標)などの)スマートホン、無線対応パーソナルコンピュータ(PC)、ハンドヘルドコンピュータなどのモバイルデバイス、携帯情報端末(PDA)、パーソナルメディア機器(PMD)、(例えば、iPad(登録商標)などの)ワイヤレスタブレット、いわゆる「ファブレット」、又は先のいずれの組み合わせである。

20

【0049】

プロセッササブシステム304は、デジタル信号プロセッサ、マイクロプロセッサ、フィールドプログラマブルゲートアレイ、又は、1つ以上の基板上に実装された複数の処理構成要素のうちの1つ以上を含み得る。プロセッササブシステム304はまた、内部キャッシュメモリも含み得る。プロセッササブシステム304は、メモリサブシステム306と通信し、後者は、例えば、スタティックランダムアクセスメモリ(SRAM)、フラッシュ、及び/又はシンクロナスダイナミックランダムアクセスメモリ(SDRAM)構成要素を含み得るメモリを含む。メモリサブシステム306は、当該技術分野において周知であるように、データアクセスを容易にするために、ダイレクトメモリアccess(DMA)タイプのハードウェアのうちの1つ以上を実装し得る。例示的な実施形態のメモリサブシステム306は、プロセッササブシステム304により実行可能なコンピュータ実行可能命令を含む。

30

【0050】

例示的な一実施形態では、クライアント装置300は、1つ以上のインタフェース、例えば、小売商装置へ接続するよう適合された、クライアントと小売商との間のインタフェース302を含む。クライアントと小売商との間のインタフェース302は、無線インタフェース又は代替的に物理的インタフェース(有線)とすることができる。無線インタフェースは、最大で数センチメートルの操作範囲を有する(例えば、国際標準化機構(ISO)規格14443A/Bに準拠し、その全体において参照により本明細書に組み込まれているそれらなどの、例えば、無線周波数識別(RFID)、NFC、等)「タッチ」又は「パンプ」タイプのインタフェースから、例えば、移動通信用のグローバルシステム(GSM)(登録商標)、符号分割多元接続(CDMA)、ユニバーサル移動体通信システム(UMTS)、ロングタームエボリューション(LTE)/LTEアドバンスド、ワールドワイドインターオペラビリティフォーマイクロウェーブアクセス(WiMAX)(登録商標)、Wi-Fi(登録商標)、Bluetooth(登録商標)、ワイヤレスユニ

40

50

バーサルシリアルバス（USB）（登録商標）、等といった、より強力な無線インタフェースを含み得る。物理的インタフェースの一般例は、例えば、USB（登録商標）（例えば、USB 2.0、USB 3.0）、FireWire（登録商標）、Thunderbolt（登録商標）、等、を含む。そのうえ、特定の機器が、例えば、加入者識別モジュール（SIM）カード又はクレジットカード、等、といった、「カード」タイプのフォームファクターを有し得ることが更に理解されよう。それら「カード」機器は、支払いリーダーの既存のエコシステムとの後方互換性を提供し得、一方で本明細書に説明する向上機能を依然としてサポートする。

#### 【0051】

いくつかの実施形態では、クライアント装置300は、例えば、キーパッド、タッチスクリーン（例えば、マルチタッチインタフェース）、液晶ディスプレイ（LCD）、バックライト、スピーカ、及び/又はマイクロホンが挙げられるがこれらに限定されない任意の数の周知のI/Oを含むユーザインタフェースサブシステムなどの、他の構成要素を更に含み得る。特定のアプリケーションでは、ユーザインタフェースは不要とされてもよいことが認識される。例えば、カードタイプクライアントの実施形態は、ユーザインタフェースを欠くことができる。

10

#### 【0052】

図示した実施形態では、クライアント装置300は、セキュアエレメント308を含む。セキュアエレメント308は、この実施形態では、セキュアメモリ308B内に記憶されたソフトウェアを実行する、セキュアプロセッサ308Aを含む。セキュアメモリ308Bは、他の構成要素（セキュアプロセッサ308A以外）に対してはアクセス不可である。更には、セキュアエレメント308は、改竄を防止するために、更に硬質にする（例えば、樹脂内に包み込む）ことができる。

20

#### 【0053】

セキュアエレメント308は、1つ以上のVMEを受信し、転送し、そして記憶することが可能である。一実施形態では、セキュアエレメント308は、ユーザに関連付けられているVMEの単一のアレイ又は複数のVMEを記憶する（例えば、クレジット「カード」、デビット「カード」、プリペイドアカウント又はカード番号、バスの定期券、映画チケットの商品券、クーポン、「ロイヤリティ」プログラムエレメント、等）。いくつかの変形例では、それぞれのVMEは、コンピュータ可読命令、及び関連データ（例えば、暗号キー、完全性キー、等）を含む、小型ファイルシステムに更に関連付けられ得る。

30

#### 【0054】

ファイルシステムは、更なる機能をサポートし得る。例えば、ファイルシステムは、例えば、セキュリティ（例えば、他のエンティティとの通信を保護するための認証プログラム、認可プログラム、及び暗号マテリアル）、ユーザ管理（例えば、勘定残高情報、最新のトランザクション履歴、等）、等のためのプログラム及びデータを含み得る。その関連ファイルシステムを伴うVMEは、固有であり、保存されたデータアセットであることが、当業者には容易に理解されるであろう。

#### 【0055】

そのうえ、一実施形態では、セキュアエレメント308は、記憶されたVME及びそれらの関連ファイルシステムのリスト又はマニフェストを維持する。マニフェストは、記憶されたVMEの現在の状態についての情報を含み得、そのような情報は、例えば、可用性、妥当性、アカウント情報（例えば、経常勘定、等）、及び/又は以前に発生したエラーを含み得る。マニフェストは、利用可能なVMEのユーザセレクションを有効にするよう、ユーザインタフェースに更にリンク又は連結され得る。いくつかの場合では、ユーザは、例えば、すべてのトランザクション、小売商とのすべてのトランザクション、期間内のすべてのトランザクション、等に対して、1つのVMEをデフォルト（例えば、デフォルトクレジットカード）として選択し得る。

40

#### 【0056】

いくつかの変形例では、セキュアエレメント308は、1つ以上の関連機器の暗号キー

50

を有し得る。それらの機器キーは、交換をセキュア化するために使用される。1つのそのような変形例では、暗号キーは、メッセージトランザクションを暗号化するための一組の非対称パブリックキー/プライベートキーである。パブリックキーは、プライベートキーの完全性を損なうことなく自由に分配され得る。例えば、クライアント装置300は、リバースト、シャミル及びアドルマン(RSA)アルゴリズムに基づいて、パブリックキー/プライベートキーが割り当て(又は、内部生成)されてもよく、パブリックキーは、クライアント装置300と安全に通信しようとするいずれの機器にも利用可能となる。クライアント装置300のパブリックキーを用いて暗号化されたメッセージは、(クライアント装置300内に安全に記憶された)クライアント装置自身のプライベートキーのみにより復号され得る。他の変形例では、暗号キーは対称である(つまり、暗号装置及び復号装置は同じキーを有する)。対称の変形例は、暗号論的に低減した複雑性を提供してもよいが、暗号装置及び復号装置の双方は、共用キーを強固に保護することを必要とする。

10

**【0057】**

他の変形例では、セキュアエレメント308は、デジタル証明書を検証及び/又は発行するための暗号キーを有し得る。デジタル証明書は、例えば、(証明書の)発行者の識別の検証に使用され得る。例えば、セキュアエレメント308は、小売商装置が後に、(クライアント装置の署名付き証明書を回収することで)トランザクションが発生したことを証明できるよう、デジタル証明書を小売商装置へ発行し得る。同様に、セキュアエレメント308は、小売商装置が信頼され得ることを証明する、小売商装置から提供されたデジタル証明書を検証し得る。

20

**【0058】**

クライアントと小売商との間のトランザクション(又は、クライアント/第三者の仲介トランザクション)中、セキュアエレメント308は、関連する1つ以上のVMEとトランザクションを行う。簡易的な実施形態は、口座番号、「プロキシ」番号、又はそれらのサブセットの送信とされ得る。より複雑な変形例では、送信は、例えば、取引金額、暗号保護、証明情報(例えば、トランザクションの時刻/日付及び場所)、小売商ID情報、等、を組み込み得る。

**【0059】**

本明細書に説明する多くの実施形態が、金融トランザクションの文脈において説明されている一方で、非金融トランザクションも等しく適している。例えば、商品券、チケット、等は、使用にしたがって、クレジット数を増分及び/又は減分され得る。他の例では、トランザクションは、妥当性チェック、例えば、バスの定期券が一定期間に有効であり(例えば、日数、週数、月数、年数、等)、したがって、その一定期間の任意の回数の使用は有効である、とされ得る。同様に、特定の種類のパスは、パスがそのブラックアウト期間に無効である、例えば、「ブラックアウト」日の対象とされてもよい。

30

**【0060】**

いくつかの実施形態では、クライアントと小売商(又は、他)との間のトランザクションは、クライアント装置300と小売商装置との間で共通の時間に行われ(つまり、クライアント装置300及び小売商装置の双方に、同時にトランザクションが生じる)、例えば、NFCトランザクションでは、クライアント装置のNFCインタフェースは、クライアント装置300上の少なくとも一部のパッシブなNFC ICに信号を送信するインターゲータなどの、小売商装置のNFCインタフェースに近接して(「バンプして」)配設される。

40

**【0061】**

しかし、代替のシナリオでは、クライアントと小売商との間のトランザクションは、時間シフト方式で行われ得ることが理解されよう。例えば、クライアント装置又は小売商装置が、トランザクションを最初に開始し、対応する機器が、後にトランザクションを認めてもよい。双方の機器がトランザクションを認めると、続いてトランザクションが完了され得る(例えば、適切な資金を送金すること、等)。例えば、クライアント及び小売商は、例えば、接続性のない農産物市場にて、トランザクションを行う。後に小売商装置がア

50

セットブローカに接続すると、トランザクションが開始される。続いてその後は、クライアント装置がそのトランザクション記録と同期し、トランザクションが完了する。いくつかの場合では、アセットブローカは、未決済の課金が発生している場合に、クライアント装置に更に通知し得る。

#### 【0062】

ここで図3Bを参照すると、1つの例示的な小売商装置350が提示されている。例示的な小売商装置350は、小売商とクライアントとの間のインタフェース352と、プロセッササブシステム354と、非一時的コンピュータ可読媒体（メモリサブシステム）356と、ネットワークインタフェース358と、を含む。本明細書にて使用されるように、用語「小売商装置」は、VMEに対応するサーバ（例えば、バックエンドサーバ106）と取引する、及び/又は、（例えば、トランザクションを許可すべきか判定するため、等）サーバにクエリするよう構成されている機器を含むがこれに限定しない。用語「小売商」の使用は決して、何かを買う又は売るエンティティにより所有又は操作される機器に対するこの定義を制限することを意図するものではないことが理解されよう。むしろ、この用語は、トランザクションが商品、サービス、仮定の報酬、であってもトランザクション処理すること、資金又はクレジット、クーポンの償還を取得すること又は預金すること、等、のために構成された又は有効にされた装置を含むがこれらに限定しない装置のためにより広範に意図されている。小売商装置の一般例は、キオスク、自動預金受け払い機（例えば、ATM）、「キャッシュ」レジスター、（例えば、RFID又はバーコードベースの）モバイルチェックアウトリーダー、モバイルワイヤレスタブレット、及びスマートホンまでも含むがこれらに限定しない。そのうえ、小売商装置は歴史的に特殊用途タイプの機器である一方で、顧客向け電子機器の現在での急速な増加により、例えば、第三者、又は機器ユーザ自身による、製作時、又は以降の提供時であっても、スモールビジネス事業が促進できることが理解されよう（例えば、無線対応携帯電話、スマートホン、パーソナルコンピュータ（PC）、ハンドヘルドコンピュータ、PDA、パーソナルメディア機器（PMD）、ワイヤレスタブレット、「ファブレット」、等）。

#### 【0063】

プロセッササブシステム354は、デジタル信号プロセッサ、マイクロプロセッサ、フィールドプログラマブルゲートアレイ、又は、1つ以上の基板上に実装された複数の処理構成要素のうちの1つ以上を含み得る。プロセッササブシステム354はまた、内部キャッシュメモリも含み得る。プロセッササブシステム354は、メモリサブシステム356と通信し、後者は、例えば、SRAM、フラッシュ、及び/又はSDRAM構成要素を含み得るメモリを含む。メモリサブシステム356は、当該技術分野において周知のようにデータアクセスを円滑にするために、DMAタイプのハードウェアのうちの1つ以上を実装し得る。例示的な実施形態のメモリサブシステム356は、プロセッササブシステム354により実行可能なコンピュータ実行可能命令を含む。

#### 【0064】

例示的な一実施形態では、小売商装置350は、1つ以上のインタフェース、例えば、クライアント装置へ接続するよう適合された、小売商とクライアントとの間のインタフェース352、を含む。小売商とクライアントとの間のインタフェース352は、無線インタフェース又は代替的に物理的インタフェース（有線）とすることができる。無線インタフェースは、最大で数センチメートルの操作範囲を有する（例えば、RFID、NFC、等）「タッチ」タイプのインタフェースから、例えば、GSM（登録商標）、CDMA、UMTS、LTE/LTE-A、WiMAX（登録商標）、Wi-Fi（登録商標）、Bluetooth（登録商標）、ワイヤレスUSB（登録商標）、等、又は先のいずれの組み合わせなどのより強力な無線インタフェースを含み得る。例えば、小売商装置350は、近距離NFCインタフェース、同様に長距離Wi-Fi（登録商標）インタフェース、更にはWiMAX（登録商標）インタフェース、衛星インタフェース、又はセルラーインタフェースを含み得る。物理的インタフェースの一般例は、例えば、USB（登録商標）、FireWire（登録商標）、Thunderbolt（登録商標）、等、を含む

10

20

30

40

50

。いくつかの変形例では、小売商とクライアントとの間のインタフェース 352 は、（例えば、既存のレガシーカードとの適合性を維持するため、等）カードリーダー又はスマートカードレセプタクルとして実装され得る。

【0065】

いくつかの実施形態では、小売商装置 350 はまた、例えば、キーパッド、タッチスクリーン（例えば、マルチタッチインタフェース）、LCD、バックライト、スピーカ、及び/又はマイクロホンが挙げられるがこれらに限定されない任意の数の周知の I/O を含むユーザインタフェースサブシステムなどの、他の構成要素も含み得る。特定のアプリケーションでは、ユーザインタフェースは不要とされてもよいことが認識される。例えば、簡易的なカードリーダー式の小売商装置は、ユーザインタフェースを欠いてもよい。

10

【0066】

図示した実施形態では、小売商装置 350 は、1つ以上の VME とのトランザクションを、アセットプロカーへ安全に報告するよう構成されたネットワークインタフェース 358 を含む。いくつかの変形例では、それぞれのトランザクションは、将来の参照/簿記のために、セキュアファイルシステム内に更に記憶されてもよい。ネットワークインタフェースの一般例は、Ethernet（登録商標）、デジタル加入者回線（DSL）、ケーブル、ハイブリッドファイバーコアキシャル（Hybrid Fiber Coaxial）、無線ローカルエリアネットワーク（WLAN）、セルラーデータ接続、等、を含むがこれらに限定しない。

【0067】

いくつかの実施形態では、小売商装置 350 は、高度暗号化標準（AES）/データ暗号化標準（DES）での暗号化、インターネットプロトコルセキュリティ（IPSec）、マルチメディアインターネットキーイング（MIKEY）、セキュアソケットレイヤー（SSL）/トランスポートレイヤーセキュリティ（TLS）、などの、関連機器の暗号キー又は他の暗号機能を有し得るがこれらに限定しない。それらの機器キー（及び/又は他の機能）は、交換をセキュア化するために使用され得る。1つのそのような変形例では、暗号キーは、一組の非対称パブリックキー/プライベートキーである。更に他の変形例では、暗号キーは、一組の対称キーである。他の変形例では、小売商装置 350 は、デジタル証明書を検証及び/又は発行するための暗号キーを有し得る。そのうえ、NFC インタフェース（使用されている場合）は、機密のユーザ情報又は支払い情報を送信中に暗号化するためなどの、適用された暗号を有し得る。

20

30

【0068】

例示的なクライアントと小売商との間のトランザクション中、小売商装置 350 は、関連する 1つ以上の VME とトランザクションを行う。例えば、小売商装置 350 は、商品/サービスとの引き換えに、クライアント装置のバーチャルクレジットカードを受信（又は、要求）し得る。受信した情報は、例えば、取引される金額、妥当性チェック情報、暗号保護、証明情報（例えば、トランザクションの時刻/日付及び場所）、小売商 ID、等、を更に組み込むことができる。他の実施形態では、小売商装置 350 は、例えば、トランザクションが正常に行われた場合に取引された金額、使用された支払いソース、小売商 ID、等の報告を、クライアント装置へ報告を返し得る。

40

【0069】

例示的な小売商装置とアセットプロカーとの間のトランザクション中、小売商装置 350 は、トランザクションをアセットプロカーへ報告する。これは、クライアント装置の VME、貸方記入/借方記入対象の小売商アカウント、等、及び取引金額に関連付けられている情報を報告することを含み得る。これに応じて、アセットプロカーは、クライアント装置の対応するアカウントから小売商装置のアカウントへ金額が正常に送金されたこと（又は、送金が失敗したこと）を認める。

【0070】

ここで図 4 を参照すると、1つの例示的なアセットエージェント 400 が提示されている。例示的なアセットエージェント 400 は、クライアント装置インタフェース 402 と

50

、プロセッササブシステム404と、非一時的コンピュータ可読媒体（メモリサブシステム）406と、ネットワークインタフェース408と、を含む。本明細書にて使用されるように、用語「アセットエージェント」は、VMEを分配するよう構成されているエンティティを含むがこれに限定しない。VMEの一般例は、機器製造業者、第三者の再販業者、等、を含むがこれらに限定しない。

#### 【0071】

プロセッササブシステム404は、デジタル信号プロセッサ、マイクロプロセッサ、フィールドプログラマブルゲートアレイ、又は、1つ以上の基板上に実装された複数の処理構成要素のうちの1つ以上を含み得る。プロセッササブシステム404はまた、内部キャッシュメモリも含み得る。プロセッササブシステム404は、メモリサブシステム406と通信し、後者は、例えば、SRAM、フラッシュ、及び/又はSDRAM構成要素を含み得るメモリを含む。メモリサブシステム406は、当該技術分野において周知のようにデータアクセスを円滑にするために、DMAタイプのハードウェアのうちの1つ以上を実装し得る。例示的な実施形態のメモリサブシステム406は、プロセッササブシステム404により実行可能なコンピュータ実行可能命令を含む。

10

#### 【0072】

例示的な一実施形態では、アセットエージェント400は、1つ以上のインタフェース、例えば、クライアント装置へ接続するよう適合されたクライアント装置インタフェース402を含む。クライアント装置インタフェース402は、無線インタフェース又は代替的に物理的インタフェース（有線）とされ得る。無線インタフェースは、例えば、GSM（登録商標）、CDMA、UMTS、LTE/LTE-A、WiMAX（登録商標）、Wi-Fi（登録商標）、Bluetooth（登録商標）、ワイヤレスUSB（登録商標）、等、を含み得る。物理的インタフェースの一般例は、例えば、USB（登録商標）、FireWire（登録商標）、Thunderbolt（登録商標）、等、を含む。

20

#### 【0073】

図示した実施形態では、アセットエージェント400は、1つ以上のVMEの分配を、アセットブローカへ安全に報告するよう構成されたネットワークインタフェース408を含む。ネットワークインタフェースの一般例は、Ethernet（登録商標）、DSL、ケーブル、ハイブリッドファイバーコアキシャル（Hybrid Fiber Coaxial）、WLAN、セルラーデータ接続、等、を含むがこれらに限定しない。

30

#### 【0074】

いくつかの実施形態では、アセットエージェント400は、関連機器の暗号キーを有し得る。それらの機器キーは、交換をセキュア化するために使用され得る。1つのそのような変形例では、暗号キーは、一組の非対称パブリックキー/プライベートキーである。更に他の変形例では、暗号キーは、一組の対称キーである。他の変形例では、アセットエージェント400は、デジタル証明書を検証及び/又は発行するための暗号キーを有し得る。

#### 【0075】

例示的な一実施形態では、アセットエージェント400は、先天的にはセキュアエレメントに関連付けられていない（つまり、セキュアエレメントを有するクライアント装置に関連していない）VMEのデータベース、等、を有する。以降に詳述されるように、VMEは、L2セキュリティレイヤーにしたがって、アセットエージェントにより、セキュアエレメントに関連付けられ得る。L2セキュリティレイヤーは、VMEが配信された際に「複製」されることを防ぐ。

40

#### 【0076】

例えば、1つの実装では、クライアント装置は、数々の「チャレンジ」を要求し、予めロードされており、それぞれのチャレンジは、要求が有効であり、現在のものである（例えば、以前の要求により再生されていない）か、検証するために使用されている。より具体的には、それぞれのチャレンジは、クライアント装置のセキュアエレメントに対して唯一有効なチャレンジである、一回限りのチャレンジであり、つまり、チャレンジが一度使

50

用されると、次のチャレンジのみがセキュアエレメントに対して有効である。ユーザが様々なアカウントにサインアップするにしたいが、アセットエージェント400によりVMEが提供される。クライアント装置がチャレンジの残りを使い果たすと、ユーザは、新たなチャレンジを要求するようクライアント装置に指示し得る。いくつかの変形例では、VMEの転送は、例えば、サービスキオスクを介して、バーチャルプライベートネットワーク(VPN)接続上のパーソナルコンピュータ(PC)を介して、等、セキュアリンクを介して行われている。

**【0077】**

ここで図5を参照すると、アセットブローカ500の1つの例示的なアカウントサーバ501が提示されている。例示的なアカウントサーバ501は、ネットワークインタフェース502と、プロセッササブシステム504と、非一時的コンピュータ可読媒体(メモリサブシステム)506と、アカウントデータベース508と、を含む。本明細書にて使用されるように、用語「アセットブローカ」は、VMEに関連付けられているアカウントへ適切に借方記入する、貸方記入する、及び/又はVMEに関連付けられているアカウントを有効にするよう構成されているシステム及びネットワークを含むがこれらに限定しない。そのようなシステムは、1つ以上のアカウントサーバ、例えば、アカウントサーバ501を含み得る。したがって、「アセットブローカ」への参照はまた、アセットブローカの1つ以上のアカウントサーバ及びその逆も呼べることで理解される。

10

**【0078】**

プロセッササブシステム504は、デジタル信号プロセッサ、マイクロプロセッサ、フィールドプログラマブルゲートアレイ、又は、1つ以上の基板上に実装された複数の処理構成要素のうちの1つ以上を含み得る。プロセッササブシステム504はまた、内部キャッシュメモリも含み得る。プロセッササブシステム504は、メモリサブシステム506と通信し、後者は、例えば、SRAM、フラッシュ、及び/又はSDRAM構成要素を含み得るメモリを含む。メモリサブシステム506は、当該技術分野において周知のようにデータアクセスを円滑にするために、DMAタイプのハードウェアのうちの1つ以上を実装し得る。例示的な実施形態のメモリサブシステム506は、プロセッササブシステム504により実行可能なコンピュータ実行可能命令を含む。

20

**【0079】**

例示的な一実施形態では、アカウントサーバ501は、クライアント装置及び小売商装置へのネットワーク接続を確立するよう適合されたネットワークインタフェース502を含む。ネットワークインタフェースの一般例は、Ethernet(登録商標)、DSL、ケーブル/ハイブリッドファイバーコアキシャル(Hybrid Fiber Coaxial)、WLAN、ワイヤレス大都市圏ネットワーク(WMAN)、セルラーデータ接続、ミリ波、等、を含むがこれらに限定しない。

30

**【0080】**

いくつかの実施形態では、アカウントサーバ501は、関連する暗号キーを有し得る。それらのキーは、メッセージ交換をセキュア化するために使用され得る。1つのそのような変形例では、暗号キーは、一組の非対称パブリックキー/プライベートキーである。更に他の変形例では、暗号キーは、一組の対称キーである。他の変形例では、アカウントサーバ501は、例えば、デジタル証明書を検証及び/又は発行するための暗号キーを有し得る。

40

**【0081】**

例示的な一実施形態では、アカウントサーバ501は、顧客アカウントに対してVMEを認証及び認可するよう構成されている。VMEは、L3セキュリティレイヤーにしたがって、アカウントサーバ501により関連付けられている。L3セキュリティレイヤーは、顧客アカウントのVMEの組み合わせが信頼でき、認可されている(つまり、不正でも悪用でもない)か、検証する。

**【0082】**

ここで図6を参照すると、1つの例示的なアセットロッカー600が提示されている。

50

例示的なアセットロッカーは、ネットワークインタフェース602と、プロセッササブシステム604と、非一時的コンピュータ可読媒体（メモリサブシステム）606と、セキュアデータベース608と、を含み得る。本明細書にて使用されるように、用語「アセットロッカー」は、VMEを記憶し、暗号化し、及び生成するよう構成されている機器を含むがこれに限定しない。例えば、アセットロッカー600は、信頼されたセキュリティモジュール（TSM）とされ得る。

【0083】

プロセッササブシステム604は、デジタル信号プロセッサ、マイクロプロセッサ、フィールドプログラマブルゲートアレイ、又は、1つ以上の基板上に実装された複数の処理構成要素のうちの1つ以上を含み得る。プロセッササブシステム604はまた、内部キャッシュメモリも含み得る。プロセッササブシステム604は、メモリサブシステム606と通信し、後者は、例えば、SRAM、フラッシュ、及び/又はSDRAM構成要素を含み得るメモリを含む。メモリサブシステム606は、当該技術分野において周知のようにデータアクセスを円滑にするために、DMAタイプのハードウェアのうちの1つ以上を実装し得る。メモリサブシステム606は、プロセッササブシステム604により実行可能であるコンピュータ実行可能命令を含むが、他の種類のコンピュータ化されたロジック（例えば、ハードウェア及びソフトウェア/ファームウェアの組み合わせ）が同様に使用されてもよい。

【0084】

例示的な一実施形態では、アセットロッカー600は、1つ以上のアカウントサーバへのネットワーク接続を確立するよう適合されたネットワークインタフェース602を含む。ネットワークインタフェースの一般例は、Ethernet（登録商標）、DSL、ケーブル、ハイブリッドファイバーコアキシャル（Hybrid Fiber Coaxial）、WLAN、セルラーデータ接続、等、を含むがこれらに限定しない。

【0085】

いくつかの実施形態では、アセットロッカー600は、関連する暗号キーを有し得る。それらのキーは、メッセージ交換をセキュア化するために使用され得る。1つのそのような変形例では、暗号キーは、一組の非対称パブリックキー/プライベートキーである。更に他の変形例では、暗号キーは、一組の対称キーである。他の変形例では、アセットロッカー600は、デジタル証明書を検証及び/又は発行するための暗号キーを有し得る。

【0086】

アセットロッカー600は、1つ以上のVMEを提供及び/又は生成するよう更に構成されている。例示的な一実施形態では、VMEは、特定の規格（例えば、米国規格協会（ANSI）の規格X4.13-1983（その全体において参照により本明細書に組み込まれている））にしたがって生成され、セキュアデータベース608内に記憶されている。代替的に、VMEは、例えば、専用フォーマット又は特定使用フォーマットにしたがって構築され得る。本開示の内容を所与として、非常に多くの可能なフォーマットが、関連の当業者に容易に理解されるであろう。

【0087】

例示的な一実施形態では、アセットロッカー600は、クライアント装置のセキュアエレメントに対してVMEを暗号化するよう構成されている。アセットロッカー600は、それぞれのアセットが、L1セキュリティレイヤーにしたがって、暗号化されている間のみ転送されることを促進する。L1セキュリティレイヤーは、VMEが、アセットロッカー600又はクライアント装置のセキュアエレメントのいずれかの内の、（暗号化されていない）プレーンテキスト内にのみ存在することを促進する。

【0088】

ここで図7を参照すると、VMEをシステム内に分配するための一般化された方法700の一実施形態が開示されている。ステップ702では、1つ以上のVMEのコンテンツは、第1の標準的な、信頼された関係にしたがって保護されている。例示的な一実施形態では、第1の信頼された関係は、VME内に含まれる秘密及び/又は暗号マテリアル（例

10

20

30

40

50

えば、セキュアキー、暗号マテリアル、ユーザ履歴、等)を保護するよう構成されている。例えば、第1の信頼された関係は、VMEを、固有の機器キー及び承認証明書にしたがって、暗号化する又は復号するよう構成されている、(ハードウェア又はソフトウェア内に実装された)セキュリティモジュールに基づいている。特に、セキュリティモジュールは、第1の信頼された関係にしたがっている、所望する行先装置(例えば、クライアント装置又は小売商装置)へ配信するために、VMEを暗号化するよう、又は第1の信頼された関係にしたがっているソース機器から受信したアクセス制御クライアントを復号するよう構成されている。例示的な一実施形態では、すべてのVMEは、各機器との間に転送されている際には、暗号化されなければならない(つまり、VMEは、暗号化されていない形態では、いずれの他の機器へ転送され得ない)。第1の信頼された関係レベルにあるそれぞれの機器には、VMEを安全に転送するために使用され得る固有の機器キー及び承認証明書が所与される。

10

**【0089】**

第1の標準的な、信頼された関係の様々な実装はまた、物理的及び/又は論理的に保護もされ得る。例えば、第1の標準的な、信頼された関係は、強制的に開放される/アクセスされると自身を破壊するよう構成されたハードウェアセキュリティモジュール(HSM)内の保護を含み得る。より一般的には、第1の標準的な、信頼された関係の例示的な実施形態は、信頼された境界を最小限保護する。信頼された境界の一般例は、物理的境界(例えば、物理的隔離、等)、及び/又は論理的境界(例えば、暗号化された通信、等)の双方を含む。

20

**【0090】**

ステップ704では、VMEのコピー数は、第2の標準的な、信頼された関係にしたがって制御されている。例示的な一実施形態では、第2の信頼された関係は、VMEの予期しない複製及び/又は悪意のある複製を防ぐよう構成されている(保存エンフォースメント)。例えば、第2の標準的な、信頼された関係は、それ自体又は別の機器に対してVMEを暗号化するよう構成されたセキュリティモジュールにより管理され得る。同様に、セキュリティモジュールは、(例えば、非対称暗号キーに基づいて)別の特定の機器によってのみ復号されてもよいVMEを暗号化し得る。いくつかの実施形態では、セキュリティモジュールの暗号化スキームは、一組の非対称キーに基づくことができるか、又は、代替的に、セキュリティモジュールの暗号化スキームは、一組の対称キーを使用し得る。

30

**【0091】**

先に説明するように、一組のパブリックキー/プライベートキーは、秘密のプライベートキー、及び公表可能なパブリックキーに基づいている。パブリックキー/プライベートキースキームは、暗号化及び復号に使用されるキーが異なり、したがって、エンクリプタ及びデクリプタは、同じキーを共有しないため、「非対称」とみなされる。対照的に、「対称」キースキームは、暗号化及び復号の両方に同じキー(又は、自明に変換したキー)を使用する。RSAアルゴリズムは、関連技術の範囲内で広く使用されている公開/秘密キーペア暗号法の種類の1つだが、本明細書に説明する実施形態は、RSAアルゴリズムに(又は、一組の非対称キー又は対称キーが重要であることに対して)全く制限されないものと認識されよう。

40

**【0092】**

パブリック/プライベート暗号化方式は、メッセージを暗号化し、及び/又は署名を生成する目的で使用することができる。具体的には、メッセージを、秘密キーで暗号化し、パブリックキーで復号することができる、それによって、そのメッセージが送信中に変更されていないことを保証する。同様に、秘密キーで生成された署名は、パブリックキーで検証することができ、その署名を生成したエンティティが正当なものであることを保証する。どちらの用途においても、秘密キーは秘匿されており、自由に配布される。

**【0093】**

ステップ706では、VMEは、第3の信頼された関係にしたがって、行先装置へ使用のために分配されている。第3の信頼された関係は、エンティティ認証及び認可を必要と

50

する。より直接的には、第3の信頼された関係は、VMEが、それらの識別を認証し得るエンティティ、及びVMEに対して認可されているエンティティのみに送信されることを保証する。

【0094】

分配モデルのフレキシビリティにより、多くの異なるスキームが想定されており、及び、本開示の提供により当業者は認識するであろう。本発明の様々な態様にしたがう動作に適した幅広いスキームを例示する、種々のVME分配スキームが以降に詳しく開示されている。

【0095】

ここで図8を参照すると、プロビジョニングトランザクションの例示的な一実施形態を表す論理ラダーダイアグラムが示されている。プロビジョニングトランザクションは、クライアント装置、アセットブローカ、アセットエージェント、及びアセットロッカーにより実行され得る。クライアント装置は、セキュアエレメント(SE)と、アプリケーションプロセッサ(AP)(例えば、プロセッササブシステム304)と、を含む。SEは、本開示にしたがうトランザクションを促進する、ソフトウェアレイヤーのいわゆる「スタック」を含むソフトウェアを記憶し得る。それぞれのソフトウェアレイヤーは、その対応するピアソフトウェアレイヤーとネゴシエートされる階層的な機能一式に対して責任を負う。いくつかの場合では、APは、危険(例えば、「脱獄」、等)にさらされ得ることが更に理解され、その結果、信頼関係は、SEと、対応する論理的レイヤーエンティティとの間にのみある、つまり、APは信頼されていない。

【0096】

セキュリティソフトウェアプロトコルは、L1レイヤーと、L2レイヤーと、L3レイヤーと、を含む。L1セキュリティは、VMEデータの暗号化及び復号を行う。L1の動作は、セキュアな実行環境(例えば、SE又はTSM)に限定されている。L1内では、VMEデータは、論理的L1境界内のプレーンテキスト(つまり、暗号化されていない)にて記憶され得、論理的L1境界外では、VMEデータは安全に暗号化されている。L2セキュリティは、VMEデータが複製されることを防ぐ。L2境界は、VMEのコピーが1つのみ、L2境界外に存在することを保証する。L2境界内では複数のコピーが存在し得る。そのうえ、L2セキュリティは、暗号化されたVMEデータ内にチャレンジを更に埋め込み得る。VMEをインストールする前に、クライアント装置は、VME内に埋め込まれたチャレンジを、クライアント装置上に記憶されたチャレンジと比較し得、VMEが古くなっていないか検証する(つまり、VMEは、現在の唯一のVMEである)。L3セキュリティは、VMEを所有する顧客の信用、所有権、及び証明を確立する責任を負う。それぞれのVMEについて、SEは情報を記憶し得、VMEに関連付けられている所有権を示す。

【0097】

例示的な一実施形態では、アセットロッカーは、VMEのデータ構成要素を生成し、バルクロットにてVMEを記憶するよう構成されているTSMである。アセットロッカーは、L1セキュリティにしたがってVME動作を行い、暗号化されたVMEのみが送信されることを保証する(つまり、VMEは、暗号化されていない形態では、アセットロッカー外に送信されない)。VMEを顧客に提供するため、アセットエージェントは、暗号化されたVMEをアセットロッカーから受信し、VMEを記憶し、クライアント装置へ必要に応じて提供する。アセットエージェントは、L2セキュリティにしたがってVME動作を行い、暗号化されたVMEのコピーが1つのみクライアント装置へ提供されることを保証する。最後に、アセットブローカの例示的な実施形態は、L3セキュリティにしたがってVME動作を行い、暗号化されたVMEの送信が、認証され、認可されているSEを伴うクライアント装置へのみ生じることを促進する。VMEがクライアント装置へ配信されると、アセットブローカは、VMEを、クライアント装置と関連付けられているアカウントと、及び/又は、クライアント装置のユーザと関連付けられているアカウントと関連付け得る。

10

20

30

40

50

## 【 0 0 9 8 】

－実施形態では、クライアント装置内に記憶されたソフトウェアアプリケーションは、新たなバーチャルクレジットカード（VCC）が、ユーザのアカウントへ使用のために提供されることを要求する。ソフトウェアアプリケーションは、APとともに実行されている。802では、APは、クライアント装置又はSEを一意的に識別するSEからの情報を要求する。例えば、情報は、装置識別子を含み得る。APは、装置識別子を、新たなVCCに対する要求にて、804にてアセットブローカへ送信する。アセットブローカは要求を認証し、VCCをユーザのアカウントへ提供する。認証は、装置識別子に基づいている。実施形態の一態様では、アセットブローカは、SE/クライアント装置がユーザアカウントに関連付けられていることを判定することで、要求を認証する。

10

## 【 0 0 9 9 】

SEは、装置識別子が、クライアント装置からアセットブローカへ安全に送信されるよう、装置識別子を電子署名とともに暗号化し得る。アセットブローカが新たなVCCを認証/認可すると、アセットブローカは、SEの電子署名をアセットエージェントへ転送する。アセットエージェントはSEの電子署名を検証し、したがって、VCCに対する行先のSEを806にて一意的に識別する。807では、いずれの更なるVCCオプションが、クライアント装置へ提供されている。

## 【 0 1 0 0 】

余談として、いわゆる「チャレンジ」は、特定のVMEをSEと関連付けるために使用される重要なリソースである。具体的には、それぞれのSEは、特定数のチャレンジを保持し、L2セキュリティを維持する。チャレンジが有効であることを検証することで、SEは、VMEが「古い」VME（つまり、無効、又は、さもなければ使用できない複製）でないか確かめ得る。SEは、照合チャレンジデータを伴うVMEを受信すると、チャレンジを削除する。以下の実装を考慮すると、SEは、アセットエージェントと共有される数多くのチャレンジを作成する（又は、与えられる）。続いてその後は、アセットエージェントは、SEに対して提供されているVME内に現在のチャレンジを埋め込み得る。SEがVMEを受信すると、SEは、受信したVMEが適切なチャレンジを含み、古いものでないか検証し得る。

20

## 【 0 1 0 1 】

先のスキームの1つの潜在的な欠点は、固定数のチャレンジは、サービスの妨害（DOS）攻撃とともに容易に危険にさらされ得ることである。DOS攻撃では、SEは、すべてのそのチャレンジリソースを使い尽くすまでチャレンジを生成するよう、継続してトリガされる。それらの最後まで、SEの例示的な実施形態は、チャレンジを消費するようSEをトリガするであろう要求を処理する前に、アセットブローカ/アセットエージェントとのセッションハンドシェイクを更に行う。加えて、リソースが使い果たされ、SEが新たなチャレンジを作成できない、思いもよらない場合は、SEは、別の一式のチャレンジを活用するために特別に割り当てられた、個別の一式の保存されたチャレンジを記憶し得る。いくつかの場合では、SEはまた、相手先商標製造会社（OEM）クレデンシャルを含み得、これは、OEMがチャレンジ動作を更に制御するために使用し得る。

30

## 【 0 1 0 2 】

808では、APは、VCCと関連付けるためのチャレンジをSEが提供することを要求する。SEにより提供されると、チャレンジがアセットブローカへ810にて送信され、続いて、アセットエージェントへ812にて転送される。アセットエージェントはチャレンジを検証し、続いて、パーソナライゼーション情報をアセットロッカーへ814にて提供する。アセットロッカーは、SEに対する新たなVCCをパーソナライズし、関連付けられたVCC識別子をアセットブローカへ816にて提供する。次に、アセットブローカは、VCC識別子をAPへ817にて提供する。APがVCC識別子を受信すると、APは、VCCの配信を818にて要求し得る。その後は、アセットブローカは、クライアント装置のSEへ820にてVCCを提供し得る。

40

## 【 0 1 0 3 】

50

大規模分配ネットワークの動作中は、複数の現実的な問題が生じることを、関連ネットワークの当業者は認識するであろう。具体的には、大規模分配ネットワークは、大型のトラフィックバーストを扱うよう、スケラブルでなければならない(クライアント装置のいわゆる「開設日」に生じ得るなどの)。ネットワークトラフィック全体を削減するための1つのスキームは、VMEの配信の延期を必要とする(可能な場合)。

#### 【0104】

図9A及び図9Bを参照すると、VMEをシステム内に分配するための一般化された方法900の一実施形態が開示されている。予めパーソナライズされた動作中、SEを有するいわゆる「予めパーソナライズされた」クライアント装置は、出荷前にVMEが予め割り当てられている(つまり、ユーザが店頭にて機器を購入する際、オンラインで機器を発売する際、等)。902では、クライアント装置がユーザへ配送される前に、クライアント装置に関連付けられている箱上に配設されたステッカ、ラベル、又は他の証印がスキャンされる。例えば、箱は、クライアント装置が包まれている小売梱包とすることができる。このステッカは、クライアント装置を一意的に識別し、VMEに関連付けられ得る情報(例えば、装置識別子)を含む。VMEは、クライアント装置に対して、例えば、(i) VMEを、(ステッカから判定された)SE(L1)に特有のキーとともに904にて暗号化し、(ii)割り当てられた初期チャレンジをVME(L2)内に906にて埋め込み、及び、(iii) VMEを、(購入時に判定された)ユーザの認証/認可情報(L3)と908にて関連付けることにより、予め構成され得る。VMEは続いて、VMEを一意的に識別する識別子、例えば、VME識別子に、910にて割り当てられる。その後は、クライアント装置は、VME識別子を使用して、912にてVMEを要求し得る。914では、要求及びVME識別子を受信すると、VMEは、クライアント装置へ、その完全に構成された状態にて配信され得る。

#### 【0105】

先のスキームは、クライアント装置(及び/又は、クライアント装置に関連付けられている箱)から収集した情報、及び購入時のユーザからの情報に基づいて、VMEを効率的に予め構成する。VMEは、機器が移送(例えば、出荷時、自宅へ持ち帰る際、等)にある間に、ベストエフォートベースにしたがって構成されている(つまり、構成は、リソースが利用可能となると生じる)。その後は、VMEは、キャッシュされた位置から、リアルタイムでのトラフィックを必要とすることなく、クライアント装置内に途切れなくロードされ得る。システムの信頼性を最大にするため、予め構成されたVMEはまた、複数の地理的位置にて冗長にキャッシュされ得る、つまり、異なる地理的位置に渡る複数のデータセンターが、VMEの複製を有する(VMEの第1のコピーが回収されると複製は古くなるよう、L2セキュリティが初期チャレンジスキームを提供する)。

#### 【0106】

より直接的には、従来の製造スキームとは異なり、クライアント装置の例示的な実施形態は、VMEを伴って製造されておらず、予めプログラムされてもいない。VMEの構成及び配信は、クライアント装置が製造及び/又は展開されるまで「延期」され得る。例えば、複数のVMEがクライアント装置によりサポートされ得ると、続いて、クライアント装置は、ユーザがアカウントを有効にする際に、選択されたVMEとともに後に構成され得る、包括的なソフトウェアを有し得る。いくつかの実装では、包括的なソフトウェアは、包括的なVME、又はデフォルトのVMEを含み得る。この実装では、ユーザがクライアント装置を購入すると、ユーザは、デフォルトのVMEとともに使用するためのクレジットカードアカウント(又は同様のもの)の提供を許可されてもよい(又は必要とされてもよい)。その後は、クライアント装置が有効にされると、アクティベーションシーケンスの一部として、デフォルトのVMEが自動でロードされる。

#### 【0107】

図10A及び図10Bを参照すると、VMEをシステム内に分配するための一般化された方法1000の別の実施形態が開示されている。この変形例では、SEを有するクライアント装置は、出荷時(つまり、ユーザが店頭にて機器を購入する際、オンラインで機器

10

20

30

40

50

を発注する際、等)に、VMEのプールから1002にてVMEが割り当てられており、つまり、特定のVMEはクライアント装置に関連付けられていない。この時、ユーザは、認証/認可情報を1004にて提供し得る。クライアント装置がユーザへ1006にて配信されると、クライアント装置を一意的に識別する情報が、例えば、小売商の販売時点情報管理システム、自宅にいるユーザ、等、により入力される。情報は、クライアント装置に関連付けられている箱上に配設されたステッカ、ラベル、又は他の証印から収集される。情報はまた、VMEがクライアント装置に対して割り当てられるべきであるが、まだ割り当てられていないことも示し得る。情報を1008にて受信したことに応じて、アセットブローカ、アセットエージェント、及びアセットブローカは協調し、(ステッカから判定される)SE(L1)に特有のキーとともにVMEを1010にて暗号化し、チャレンジデータをVME(L2)内に1012にて埋め込み、及び、VMEを(購入時に判定される)ユーザの認証/認可情報(L3)と1014にて関連付けることにより、利用可能なVMEを割り当てる。1016では、新規に作成され、暗号化されたVMEが、クライアント装置へ、その完全に構成された状態にて配信される。

10

#### 【0108】

先のスキームは、必要に応じて効率的にVMEを構成する。そのような実装は、アセットブローカ及び/又はアセットエージェントが、VMEのプールを知的に管理可能にする。VMEのプール内のそれぞれのVMEは特定のクライアント装置(つまり、特定の用途専用)に割り当てられておらず、必要に応じて割り当てられているため、アセットブローカ及び/又はアセットエージェントは、まだ有効でない在庫を追跡する必要はない(例えば、機器によっては購入されて、有効にされる前に返却されてもよく、これは不要なVMEの「攪拌」を削減する)。これは、VMEが有限リソースである場合に有効となり得る。口座番号は有限リソース(及び、したがって、その不足において貴重)であることが、当業者には容易に理解されるであろう。例えば、ANSI規格X4.13-1983(その全体において参照により本明細書に以前に組み込まれている)は、多くの国内クレジットカードシステムにより使用されるアカウントナンバリングシステムである。ANSI規格X4.13-1983の16桁のクレジットカード番号によると、それらのサブセットのみが実際の口座番号を表し(例えば、最大で1000万の固有の口座番号を表すためには8桁のみ使用され得)、他の桁は他の用途に与えられている(例えば、カード発行者の識別、「チェック」値の提供、カード番号の識別、等)。

20

30

#### 【0109】

ここで図11を参照すると、VMEをシステム内に分配するための一般化された方法1100の別の実施形態が開示されている。この実施形態では、VMEの構成は、最初のトランザクションが発生するまで完全に延期され得る。この実施形態は、システムとクライアント装置との間に複数のトランザクション(例えば、定期トランザクション)が発生する場合に有用とされ得る。例えば、ユーザは、例えば、複数の映画パス、月間バス定期券、等を購入するよう選択してもよい。1102では、ユーザは、支払い情報、例えば、クレジットカード情報をシステムへ提供する。1104では、クライアント装置を識別する情報、例えば、装置識別子がシステムへ提供される。装置識別子は、いずれの前述の実施形態にしたがって提供され得る(例えば、「予めのパーソナライゼーション」プロセス、ユーザによる入力、APによる提供、等)。最初のトランザクションは、1106にて正常に行われ得る。その間、VMEが装置識別子を使用してクライアント装置に対して構成され、支払い情報及び/又はチャレンジデータが提供され、VMEが1108にて構成されると、以降の使用のために1110にてクライアント装置へ配信される。いくつかの場合では、配信は、準備完了時のプッシュ通知、自動ダウンロード、又は手動ダウンロードに基づくことができる。

40

#### 【0110】

ここで図12を参照すると、VMEをシステム内に分配するための一般化された方法1200の別の実施形態が開示されている。方法1200は、アセットブローカとともに、SEを有するクライアント装置、アセットエージェント、及びアセットロッカーと通信し

50

て実行され得る。1202では、アセットブローカは、VMEをユーザのアカウントへ使用のために提供する要求をクライアント装置から受信する。アカウントは、クライアント装置のユーザと関連付けられ得る（つまり、アカウントはユーザにより所有されている）。要求は、クライアント装置、例えば、装置識別子に一意的に関連付けられている識別情報を含み得る。実施形態の一態様では、要求はまた、アカウントを識別する情報を送信することを含み得る。次に、アセットブローカは、1204にて要求を認証する。アセットブローカは、装置識別子により識別されたクライアント装置がアカウントに関連付けられていることを検証することで、要求を認証し得る。アセットブローカは続いて、アセットエージェント及びアセットロッカーと協調し、本明細書に説明する実施形態にしたがって、アカウントに対してVMEを提供し、クライアント装置に対してVMEを構成する。1206では、アセットブローカは、アセットロッカーからVME識別子を受信する。VME識別子は、クライアント装置に対して構成されているVMEを識別する。アセットブローカは続いて、VME識別子をクライアント装置へ1208にて送信し得る。クライアント装置は、VME識別子を記憶し得、その後、構成されたVMEをアセットブローカから要求する際にVME識別子を使用する。VMEに対する要求をクライアント装置から1210にて受信すると、アセットブローカは、構成されたVMEをクライアント装置へ1212にて送信し得る。

#### 【0111】

ここで図13A～図13Cを参照すると、VMEをシステム内に分配するための一般化された方法1300の別の実施形態が開示されている。方法1300は、アセットエージェント、アセットブローカ、及び/又はアセットロッカーを含み得るプロビジョニングシステムと通信するクライアント装置により実行され得る。クライアント装置は、SE及びAPを含み得る。明確化及び簡略化を目的として、クライアント装置とアセットブローカとの間で実行される方法1300が以下に説明されることに注意すべきである。方法1300の各ステップはまた、クライアント装置と、プロビジョニングシステムの1つ以上のエンティティ（例えば、アセットエージェント、アセットブローカ）との間で実行され得ることが理解されるべきである。

#### 【0112】

1302では、クライアント装置は、使用のためにVMEのユーザのアカウントへの提供を希望することを示す入力を受信する。入力は、クライアント装置でのI/Oインタフェース（例えば、ボタン、キーパッド、タッチスクリーン、音声コマンド、等）を使用してユーザにより入力され得る。1304では、クライアント装置は、識別情報をSEから要求し得る。識別情報は、クライアント装置、例えば、装置識別子に一意的に関連付けられている。識別情報は、SEから取得され得る。代替の実施形態では、識別情報は、クライアント装置外部のソースから取得され得る。例えば、ユーザは、クライアント装置の箱上のステッカから識別情報を取得し得、クライアント装置のI/O機器を使用して識別情報を入力し得る。

#### 【0113】

SEから装置識別子を受信すると、クライアント装置は、VMEを提供する要求をアセットブローカへ1306にて送信し得る。要求に加えて、クライアント装置はまた、装置識別子もアセットブローカへ1308にて送信する。1310では、クライアント装置は、チャレンジに対する要求をアセットブローカから受信する。チャレンジは、本明細書に説明するように、L2セキュリティにしたがって、VMEの検証に使用され得る。アセットブローカから要求を受信したことに応じて、APは、チャレンジをSEから1312にて要求し得る。チャレンジをSEから受信すると、クライアント装置は、チャレンジをアセットブローカへ1314にて送信する。プロビジョニングシステムは、要求を認証し、クライアント装置に対してVMEを構成し得る。次に、クライアント装置は、VME識別子をアセットブローカから1316にて受信し得る。VME識別子は、クライアント装置に対して構成されているVMEを一意的に識別し得る。その後、クライアント装置は、構成されたVMEに対する要求をアセットブローカへ1318にて送信し得る。要求に加え

10

20

30

40

50

て、クライアント装置は、VME識別子を1320にて送信する。要求及びVME識別子を受信したことに応じて、アセットブローカは、構成されたVMEをクライアント装置へ1322にて配信し得る。SEは、受信したVMEが、有効なチャレンジデータとともに埋め込まれていることを検証することで、受信したVMEが有効である（つまり、受信したVMEが古くない）か、1324にて検証し得る。

【0114】

特定の機構が、特定の方法の具体的なステップのシーケンスの観点から説明されているが、これらの説明は、本明細書で開示される、より広範な方法の例示にすぎないものであり、具体的な適用によって、必要に応じて修正することができる点が、認識されるであろう。あるステップは、ある状況下では、不必要又は任意選択とすることができる。更には、特定のステップ又は機能性を、開示される実施形態に追加してもよく、あるいは2つ以上のステップの実行の順序を、置き換えることもできる。すべてのこのような変更形態は、本開示の範囲内に包含され、本明細書において特許請求されるとみなされる。

10

【0115】

更に、説明される実施形態の様々な態様、実施形態、実装、又は特徴は、個別に若しくは任意の組み合わせで使用できる。記載される実施形態の様々な態様は、ソフトウェア、ハードウェア、又はハードウェアとソフトウェアとの組み合わせによって実施できる。更に、説明した実施形態は、コンピュータ可読媒体上のコンピュータ可読コードとして実施できる。コンピュータ可読媒体は、後にコンピュータシステムによって読み出すことが可能なデータを記憶することができる、任意のデータ記憶装置である。コンピュータ可読媒体の例としては、読み出し専用メモリ、ランダムアクセスメモリ、CD-ROM、HDD、DVD、磁気テープ、及び光学的データ記憶装置が挙げられる。コンピュータ可読媒体はまた、ネットワーク結合されたコンピュータシステム上に分散させることもでき、コンピュータ可読コードが分散方式で記憶及び実行される。

20

【0116】

上述の説明は、説明の目的上、説明される実施形態の完全な理解を提供するために、具体的な専門用語を使用した。しかしながら、それらの具体的詳細は、記載される実施形態を實踐するために必須のものではないことが、当業者には明らかとなるであろう。それゆえ、上述の具体的な実施形態の説明は、例示及び説明の目的のために提示される。それらの説明は、網羅的であることも、又は説明される実施形態を開示される厳密な形態に限定することも意図してはいない。上記の教示を考慮して、多くの修正形態及び変更形態が可能であることが、当業者には明らかとなるであろう。

30

【図1】

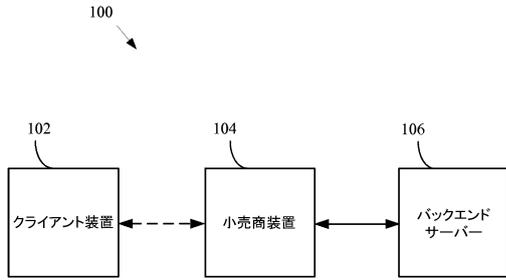


FIG. 1

【図2】

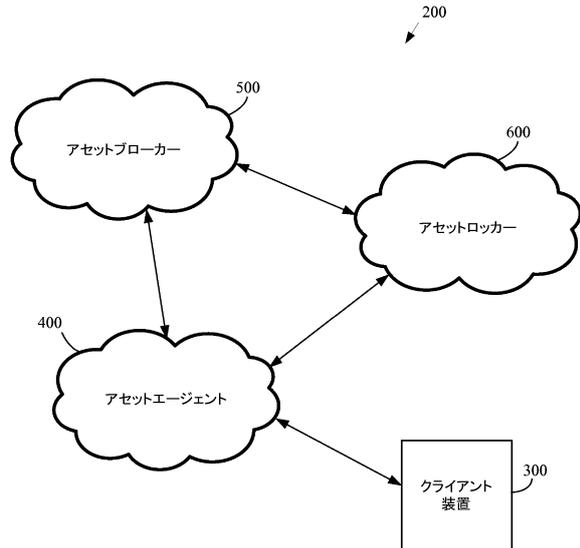


FIG. 2

【図3A】

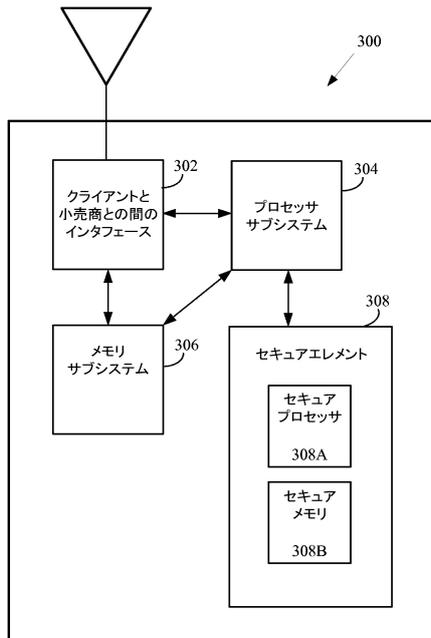


FIG. 3A

【図3B】

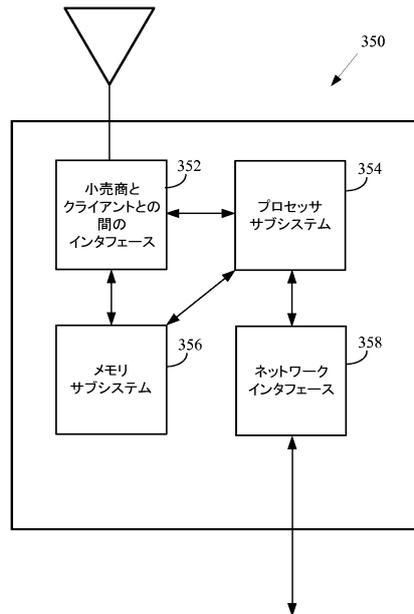


FIG. 3B

【図4】

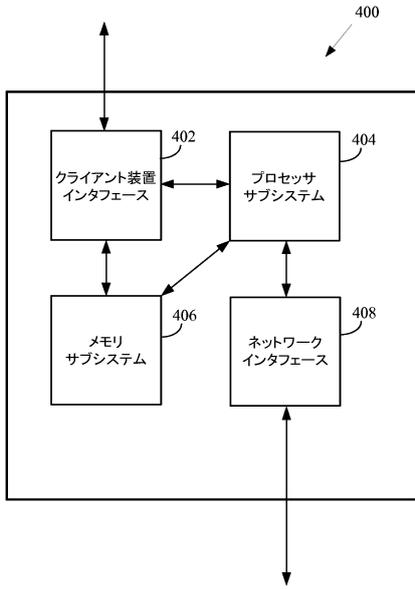


FIG. 4

【図5】

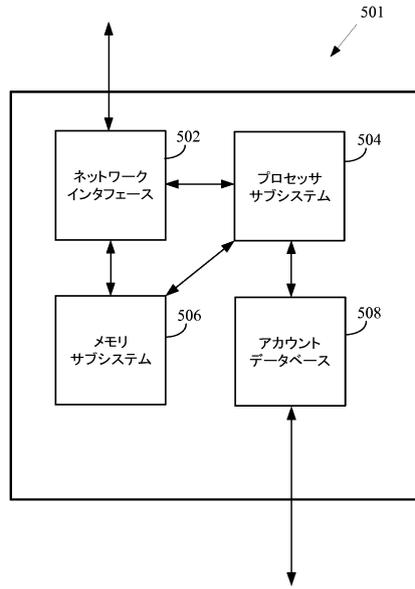


FIG. 5

【図6】

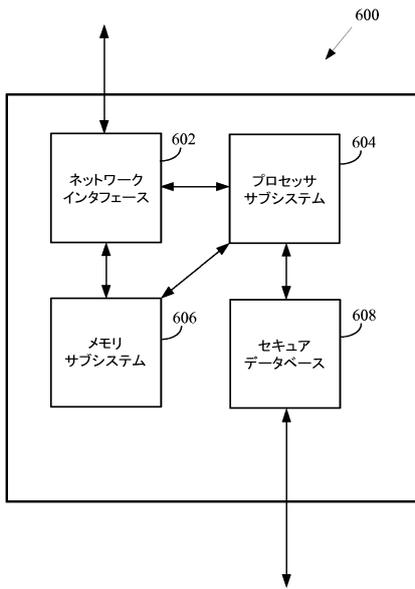


FIG. 6

【図7】

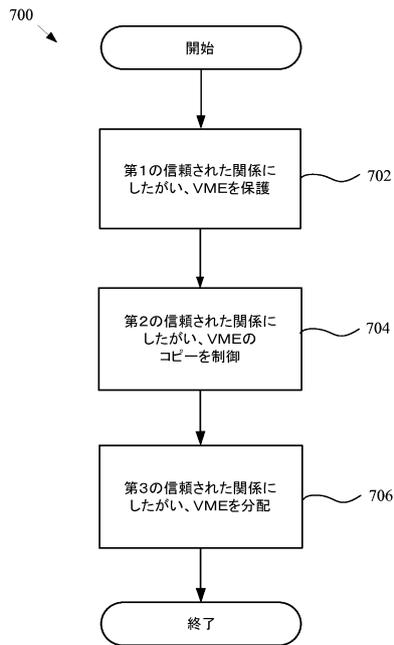


FIG. 7

【図8】

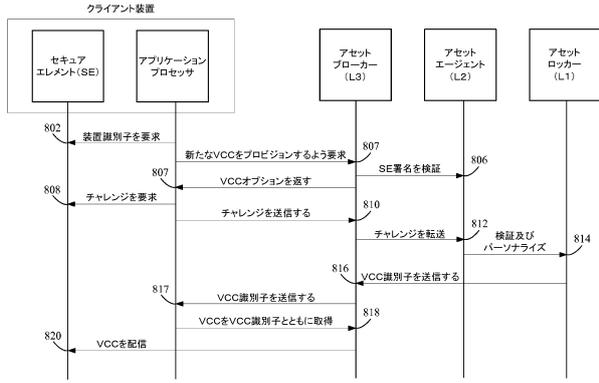


FIG. 8

【図9A】

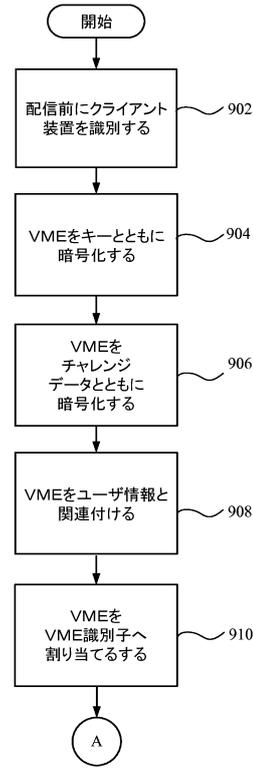


FIG. 9A

【図9B】

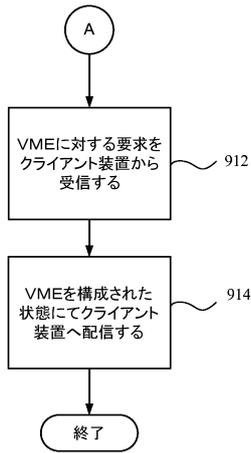


FIG. 9B

【図10A】

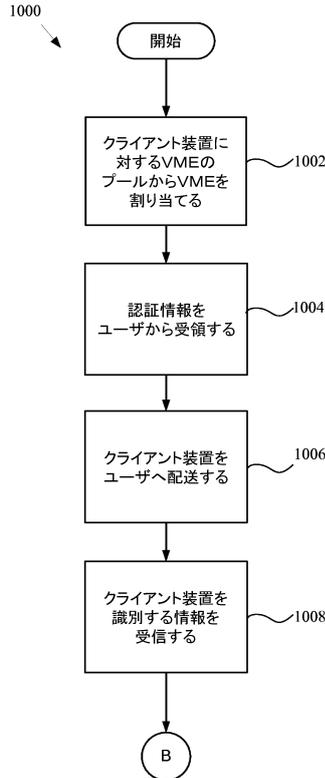


FIG. 10A

【図10B】

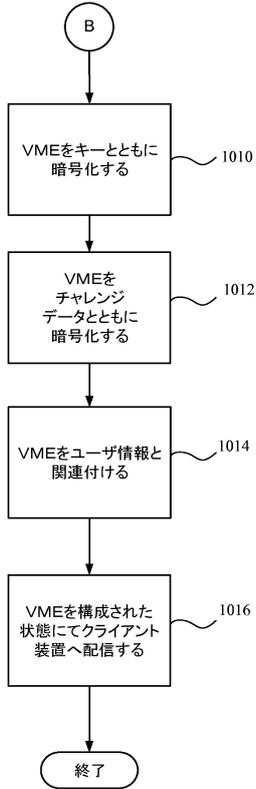


FIG. 10B

【図11】

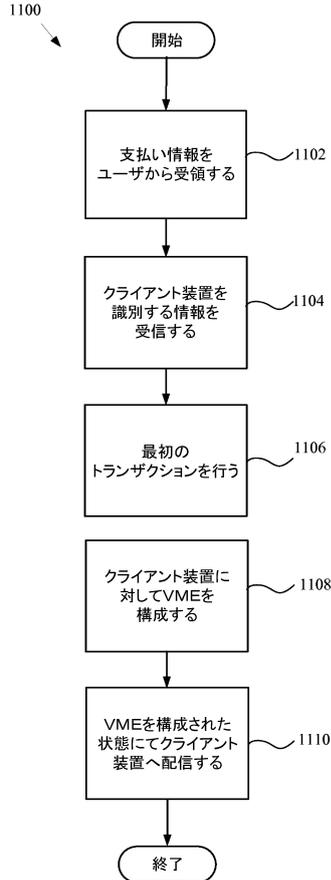


FIG. 11

【図12】

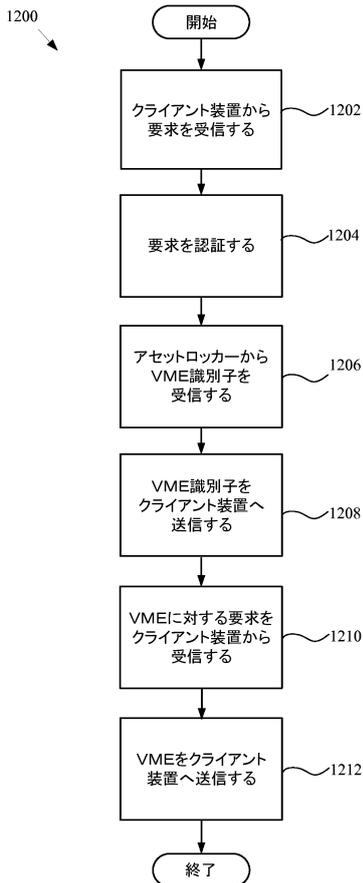


FIG. 12

【図13A】

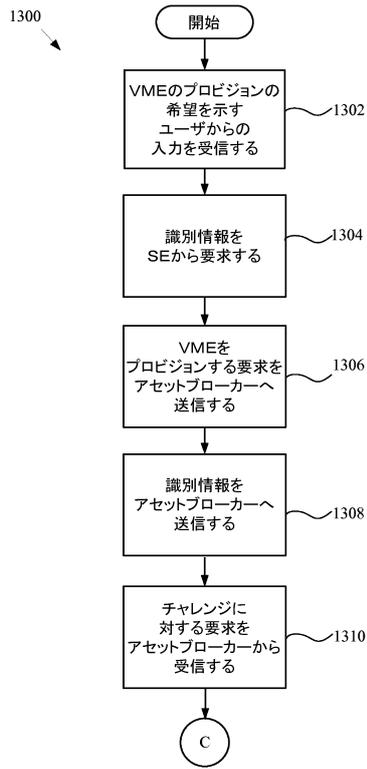


FIG. 13A

【図13B】

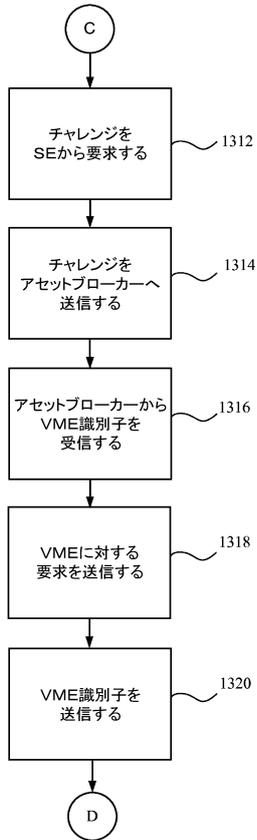


FIG. 13B

【図13C】

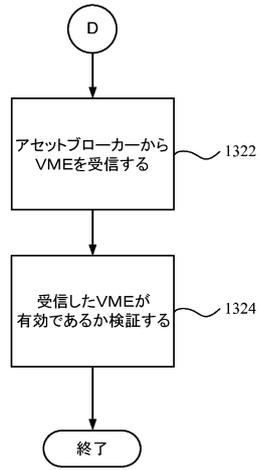


FIG. 13C

## フロントページの続き

- (74)代理人 100116894  
弁理士 木村 秀二
- (74)代理人 100130409  
弁理士 下山 治
- (74)代理人 100134175  
弁理士 永川 行光
- (72)発明者 ハガティ, デイビット ティー.  
アメリカ合衆国 カリフォルニア州 9 5 0 1 4 , クパチーノ, インフィニット ループ 1
- (72)発明者 カーン, アーメル エー.  
アメリカ合衆国 カリフォルニア州 9 5 0 1 4 , クパチーノ, インフィニット ループ 1
- (72)発明者 シャープ, クリストファー  
アメリカ合衆国 カリフォルニア州 9 5 0 1 4 , クパチーノ, インフィニット ループ 1
- (72)発明者 ホーク, ジェラルド ファン  
アメリカ合衆国 カリフォルニア州 9 5 0 1 4 , クパチーノ, インフィニット ループ 1
- (72)発明者 リンデ, ヨアキム  
アメリカ合衆国 カリフォルニア州 9 5 0 1 4 , クパチーノ, インフィニット ループ 1
- (72)発明者 マクラウリン, ケヴィン ピー.  
アメリカ合衆国 カリフォルニア州 9 5 0 1 4 , クパチーノ, インフィニット ループ 1
- (72)発明者 ジアト, メヘディ  
アメリカ合衆国 カリフォルニア州 9 5 0 1 4 , クパチーノ, インフィニット ループ 1
- (72)発明者 ヴァイド, ユーセフ エイチ.  
アメリカ合衆国 カリフォルニア州 9 5 0 1 4 , クパチーノ, インフィニット ループ 1

審査官 山下 剛史

- (56)参考文献 特表2012-505475(JP,A)  
特開2003-70067(JP,A)  
国際公開第2012/168940(WO,A1)  
米国特許第8196131(US,B1)  
中道理, NFCは“おサイフ”を超えて 第2部<海外動向>セキュア・エレメントの争奪へApple, Google, 日経エレクトロニクス, 日経BP社, 2011年 3月21日, 第1052号, p.66-71

- (58)調査した分野(Int.Cl., DB名)  
G06Q 10/00-99/00  
G06F 21/00