

(19) 日本国特許庁 (JP)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2010-509683

(P2010-509683A)

(43) 公表日 平成22年3月25日 (2010.3.25)

(51) Int.Cl.		F I			テーマコード (参考)
G06F 21/24	(2006.01)	G06F 12/14	540B		3E142
H04L 9/10	(2006.01)	H04L 9/00	621A		5B017
G07G 1/14	(2006.01)	G07G 1/14			5J104

審査請求 未請求 予備審査請求 未請求 (全 28 頁)

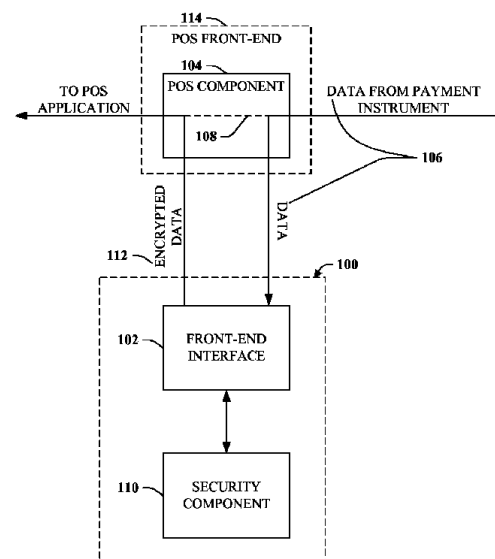
(21) 出願番号	特願2009-536406 (P2009-536406)	(71) 出願人	500046438
(86) (22) 出願日	平成19年11月3日 (2007.11.3)		マイクロソフト コーポレーション
(85) 翻訳文提出日	平成21年5月7日 (2009.5.7)		アメリカ合衆国 ワシントン州 9805
(86) 国際出願番号	PCT/US2007/083551		2-6399 レッドモンド ワン マイ
(87) 国際公開番号	W02008/058040		クロソフト ウェイ
(87) 国際公開日	平成20年5月15日 (2008.5.15)	(74) 代理人	100077481
(31) 優先権主張番号	11/556,317		弁理士 谷 義一
(32) 優先日	平成18年11月3日 (2006.11.3)	(74) 代理人	100088915
(33) 優先権主張国	米国 (US)		弁理士 阿部 和夫
		(72) 発明者	セルゲイ ブイコフ
			アメリカ合衆国 98052 ワシントン
			州 レッドモンド ワン マイクロソフト
			ウェイ マイクロソフト コーポレーシ
			ョン インターナショナル パテンツ内

最終頁に続く

(54) 【発明の名称】 支払データの保護

(57) 【要約】

本発明は、重要度の高い情報へのアクセスを暗号化手段によって制限することができるアーキテクチャもしくはアレンジメントに関する。特に、例えば、店頭において支払手段 (202) から得られたデータ (106) が初期段階で暗号化されるので、POS (もしくは別の) アプリケーション (204) が非暗号化形式のデータ (112) にアクセスできなくなる。さらに/または、POSアプリケーション (204) はデータ復号化手段にもアクセスできない。例えば、公開鍵基盤 (PKI) は、バックエンド支払プロセッサ (504i) が暗号化アルゴリズム (5122) を決定し、バックエンド支払プロセッサ自身を公開鍵 (502i) に関連させ、復号化用の秘密鍵 (602) を保持することができるように、利用されてもよい。公開鍵はPOS装置に転送することができ、データの復号化の際に使用される。また、公開鍵基盤 (PKI) を、より信頼度の高い者によって管理するようにしてもよい。



【特許請求の範囲】**【請求項 1】**

よりセキュアな P O S トランザクション環境を促進するためのフロントエンドシステムであって、

P O S コンポーネント（104）に取り付けるように構成され、支払手段（202）から得られたデータ（106）をインターセプトするフロントエンドインターフェース（102）と、

前記データを暗号化するセキュリティコンポーネント（110）と、を含み、

前記フロントエンドインターフェースは暗号化データ（112）を出力することを特徴とするフロントエンドシステム。

10

【請求項 2】

前記 P O S コンポーネントは、P O S 入力装置であることを特徴とする請求項 1 記載のシステム。

【請求項 3】

前記 P O S 入力装置は、磁気ストライプ読取装置（M S R）、磁気インク文字認識（M I C R）装置、P I N パッド、R F I D トランシーバ、または光源ベーススキャナの少なくとも 1 つであることを特徴とする請求項 2 記載のシステム。

【請求項 4】

前記 P O S コンポーネントは、P O S サービスオブジェクトであることを特徴とする請求項 1 記載のシステム。

20

【請求項 5】

前記 P O S コンポーネントは、P O S ミドルウェア、または P O S サービスオブジェクトと P O S ミドルウェアの組み合わせであることを特徴とする請求項 1 記載のシステム。

【請求項 6】

前記セキュリティコンポーネントは、前記データを暗号化するために公開鍵を使用することを特徴とする請求項 1 記載のシステム。

【請求項 7】

前記公開鍵は、バックエンド支払コンポーネントに関連付けられていることを特徴とする請求項 6 記載のシステム。

【請求項 8】

前記公開鍵及び暗号化アルゴリズムの少なくとも一方が、金融団体、金融協会、または支払プロセッサにより規定されていることを特徴とする請求項 6 記載のシステム。

30

【請求項 9】

前記セキュリティコンポーネントが公開鍵基盤（P K I）を使用して前記データを暗号化することを特徴とする請求項 1 記載のシステム。

【請求項 10】

前記支払手段は、クレジットカード、デビットカード、チャージカード、小切手、非接触型カード、または換金可能手段の少なくとも 1 つであることを特徴とする請求項 1 記載のシステム。

【請求項 11】

よりセキュアなトランザクション処理環境を促進するためのバックエンドシステムであって、

支払コンポーネント（504）に取り付けるように構成され、暗号情報（512）をフロントエンド P O S コンポーネントに送信するバックエンドインターフェース（502）と、

前記暗号情報に関連付けられたデータを復号化する復号化コンポーネントと、を含むことを特徴とするバックエンドシステム。

40

【請求項 12】

前記支払コンポーネントは、支払ミドルウェアであることを特徴とする請求項 11 記載のシステム。

50

【請求項 1 3】

前記支払コンポーネントは、支払オブジェクト、または支払オブジェクトと支払ミドルウェアの組み合わせであることを特徴とする請求項 1 1 記載のシステム。

【請求項 1 4】

前記支払コンポーネントは、支払プロセッサであることを特徴とする請求項 1 1 記載のシステム。

【請求項 1 5】

前記暗号情報は、公開鍵または暗号アルゴリズムの少なくとも一方であることを特徴とする請求項 1 1 記載のシステム。

【請求項 1 6】

前記復号化コンポーネントが秘密鍵を使用して前記データを復号化することを特徴とする請求項 1 1 記載のシステム。

【請求項 1 7】

前記バックエンドインターフェースが暗号化されたデータをインターセプトし、支払手段に関連付けられた復号化されたデータを出力することを特徴とする請求項 1 1 記載のシステム。

【請求項 1 8】

暗号化されていない支払手段情報へのアクセスを制限する方法であって、

購入手段（202）に関連した情報を含む P O S トランザクションデータ（106）を受信するステップ（902）と、

前記購入手段に関連付けられた金融団体に対応する公開鍵（512₁）を検索するステップ（904）と、

前記公開鍵を使用して前記 P O S トランザクションデータを暗号化するステップ（906）と、

暗号化した P O S トランザクションデータを P O S アプリケーション（204）に送信するステップ（908）と、

を含むことを特徴とする方法。

【請求項 1 9】

前記暗号化された P O S トランザクションデータを前記 P O S アプリケーションから受信するステップと、

秘密鍵を使用して、前記暗号化された P O S トランザクションデータを復号化するステップと、

をさらに含むことを特徴とする請求項 1 8 記載の方法。

【請求項 2 0】

P O S コンポーネントと相互対話するための第 1 のインターフェースを設けるステップ、及び

支払コンポーネントと相互対話するための第 2 のインターフェースを設けるステップ、の少なくとも一方をさらに含むことを特徴とする請求項 1 9 記載の方法。

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は、支払いデータの保護に関する。

【背景技術】**【0002】**

近年において非現金決済（トランザクション、商取引）が広く用いられるようになったのに伴い、消費者は益々色々な種類の非現金支払い手段（例えば、クレジットカード、デビットカード、非接触型カード）やその他の支払いカード／決済カード、並びに店頭（point-of-sale locations）で取引を完了させるための従前型のチェック（小切手）やその他の換金可能な手段に依存することが増えてきている。上記支払手段の使用が増えたので、これに付随する不正行為（例えば、詐欺やいわゆる I D 窃盗（

10

20

30

40

50

identity theft))が以前にも増して顕著になってきた。最近では、ID窃盗が多く、国において最も急速に増加している犯罪であるという見解が出ている。

【0003】

ID窃盗その他の詐欺的行為の主たる入口の1つはPOSアプリケーションに関連して発生する。なぜなら、これらのアプリケーションはバックエンド支払いプロセッサ (back-end payment processor) ヘトランザクションリクエストを送信する責任をしばしば持っているからである。そのため、POSアプリケーションは通常、クレジットカード番号/デビットカード番号等の個人情報及び/またはその他の重要な情報 (機密性の高い情報・要注意情報) ヘアクセスすることができる。従って、例えば、今日の小売産業・業界における最も大きな問題の1つは、POSアプリケーションはセ

10

【発明の概要】

【発明が解決しようとする課題】

【0004】

典型的なPOSアプリケーションは、磁気ストライプ (テープ) 読取機 (Magnetic Stripe Reader: MSR) により支払カード磁気トラック (磁気テープ部) からデータを読み取る。このデータはしばしば、カード番号、有効期限、カード所有者名等のかなり重要な情報を含んでいる。POSアプリケーションはこのようなデータを支払いサービスプロバイダに送り、料金を請求するか支払権限を与える。典型的には、POSアプリケーションはこのデータについてのフルコントロールを持つ。つまり、POSアプリケーションは上記データをデータベースに保存することもできるし、上記データを他の用途に使用することもできる。従って、多くのクレジットカードネットワーク (例えば、VisaやMasterCard) はカード情報の保存を禁止している。しかしながら、従来において、このポリシー・方針を強制する手段はなかった。今日、重要なデータの漏えいのほとんどは、意図的にデータを暴くことでPOSアプリケーションから起きるのではなく、単にデータの取り扱いを間違えたり、意図せずにデータをハッカー等に露呈することでPOSアプリケーションから発生している。その理由は、多くの場合、アプリケーション作成者側にセキュアプログラミングの専門知識が欠けているからである。重要データを高セキュリティで取り扱うことは、しばしば、当該分野で訓練されたプログラマーにとっても難しい。

20

30

【課題を解決するための手段】

【0005】

下記の説明は、特許請求の範囲に記載された発明の概要であり、本発明の幾つかの態様の基本的な理解を提供するものである。この発明の概要は、特許請求の範囲に記載された本発明の内容の全てを説明するものではない。また、発明の概要は、特許請求の範囲に記載された本発明の内容の重要な要素または必須の要素を特定するものではないし、本発明の範囲・外延を画定するものでもない。その唯一の目的は、後に記載されるより詳細な説明の前説明として、特許請求の範囲に記載された発明の内容の幾つかのコンセプトを簡単な形で示すことである。

40

【0006】

本明細書に開示され特許請求の範囲に記載された発明の主題は、その一態様において、支払手段から得られたデータをPOS (Point-Of-Sale) アプリケーション、並びにPOSフロントエンド (front-end) の他のアプリケーションから隔離することを容易にするアーキテクチャを備える。従って、上記アーキテクチャは、例えば、POS入力装置、POSサービスオブジェクト、POSミドルウェアなどの1つ以上のPOSコンポーネントに取り付けられ、または埋め込まれるように構成されたフロントエンドインターフェースを含むことができる。フロントエンドインターフェースは、支払手

50

段から得られたデータを取り込み、当該データを暗号化するセキュリティコンポーネントに当該データを転送する。

【0007】

本発明の1つの態様によれば、セキュリティコンポーネントは公開鍵基盤（PKI：Public Key Infrastructure）の取決めにより当該データを暗号化することができる。例えば、データは支払プロセッサ（または別の金融機関、取次店、特約店）に関連付けられた公開鍵の方法により、またはその他の手段により暗号化することができる。上記に基づき、支払手段から得られた重要度の高いデータは安全に暗号化することができる。この暗号化は、トランザクションの開始から直ちに行うことができる。また、当該データのセキュリティは、当該データが支払バックエンド（payment back-end）に到達するまで、維持される。

10

【0008】

本発明の1つの態様によれば、支払バックエンドは、支払コンポーネント（例えば、支払ミドルウェア、支払プロセッサ）に取り付けられるか埋め込まれるように構成されたバックエンドインターフェースを有してもよい。バックエンドインターフェースは復号化コンポーネントに動作可能なように接続することができる。この復号化コンポーネントは、バックエンドインターフェースによりインターセプトされた（捕らわれた）データを復号化する。復号化コンポーネントは、例えば、公開鍵を保持することができると共にフロントエンドへの公開鍵の送信を容易にすることができる。復号化コンポーネントはまた、データを復号化するために、前記公開鍵に関係付けられたプライベート鍵（秘密鍵）を保持することもできる。従って、PKIのキー及びその他の側面の規制（regulation）は、所定のトランザクションのより信頼された（そしてよりセキュアな）パーティー（parties）によって行うことができる。

20

【0009】

以下の記載及び添付図面は本発明の主題の幾つかの代表的な態様を詳細に説明するものである。しかし、当該態様は、本発明の原理・思想を適用することができる数個の形態だけしか示していない。本発明は、当該態様・形態の全てを包含するとともにその均等物も包含する。本発明の他の利点や新規な特徴は、添付図面を参照して下記の発明の詳細な説明を理解することにより明らかになるであろう。

【図面の簡単な説明】

30

【0010】

【図1】高セキュリティのPOSトランザクション環境を実現することができるフロントエンドシステムのブロック図である。

【図2】高セキュリティのPOSトランザクション環境を実現することができる例示的POSコンポーネントを含むフロントエンドを具備する典型的なシステムの図である。

【図3】POSフロントエンドにおける例示的POS入力装置のブロック図である。

【図4】POSフロントエンドで通常使用される例示的支払手段のブロック図である。

【図5】高セキュリティのトランザクション処理環境を実現することができるバックエンドシステムのブロック図である。

【図6】高セキュリティのトランザクション処理環境を実現することができる例示的支払コンポーネントを含むバックエンドを具備するシステムのブロック図である。

40

【図7】POSトランザクション情報のエンドツーエンド暗号化（end-to-end encryption）を実現することができるシステム700のブロック図である。

【図8】インターフェースを設定する方法を示す手順の例示的フローチャートである。

【図9】支払手段に付随した情報がPOSアプリケーションに送信される前に、当該情報をインターセプトして暗号化する方法を示す手順の例示的フローチャートである。

【図10】トランザクションデータがPOSアプリケーションを通過した後に、当該トランザクションデータをインターセプトして復号化する方法を示す手順の例示的フローチャートである。

【図11A】POSトランザクションのエンドツーエンド処理のための種々の構成を示す

50

図である。

【図 1 1 B】 P O S トランザクションのエンドツーエンド処理のための種々の構成を示す図である。

【図 1 1 C】 P O S トランザクションのエンドツーエンド処理のための種々の構成を示す図である。

【図 1 1 D】 P O S トランザクションのエンドツーエンド処理のための種々の構成を示す図である。

【図 1 1 E】 P O S トランザクションのエンドツーエンド処理のための種々の構成を示す図である。

【図 1 2】 開示されたアーキテクチャを実行するように動作できるコンピュータのブロック図である。

【図 1 3】 例示的なコンピューティング環境の概略ブロック図を示している。

【発明を実施するための形態】

【0 0 1 1】

以下に、図面を参照して本発明を説明する。同じ様な要素には同じような参照符号をつけている。以下の記載において、説明を簡単にするために、多くの詳細な事項が明記されて、本発明の内容が完全に理解できるようにしている。しかしながら、本発明はそのような詳細な事項が無くても実施可能である場合もある。また、別の場合にあっては、本発明の説明を容易にするために、周知の構造や装置がブロック図で示されている。

【0 0 1 2】

本明細書において使用される「コンポーネント」、「モジュール」、「システム」、「インターフェース」等の用語は、概して、コンピュータ関連エンティティ（つまり、ハードウェア、ハードウェアとソフトウェアの組み合わせ、ソフトウェアそのもの、または実行中のソフトウェア）を示す。例えば、コンポーネントは、プロセッサ上で実行するプロセス、プロセッサ、オブジェクト、エグゼキュタブル（`executable`）、実行のスレッド、プログラム、及び／またはコンピュータのことであるが、これらに限定されない。例えば、コントローラ上で実行されているアプリケーションと当該コントローラはコンポーネントと呼ぶことができる。1つ以上のコンポーネントはプロセス及び／またはスレッド内に存在することもあり、コンポーネントは1つのコンピュータに集中して（局所的に）設けられること、及び／または、2つ以上のコンピュータに分散して設けられることもある。

【0 0 1 3】

さらに、本発明は、コンピュータを制御して本発明の内容を実施すべく、ソフトウェア、ファームウェア、ハードウェアもしくはこれらの任意の組み合わせを作成する標準的なプログラミング及び／または工学技術を用いる方法、装置もしくは製造物として実施することもできる。ここで用語「製造物」は、任意のコンピュータ可読装置、キャリアもしくは媒体からアクセス可能なコンピュータプログラムを含む。例えば、コンピュータ可読媒体は、磁気記憶装置（例えば、ハードディスク、フロッピー（登録商標）ディスク、磁気ストライプ（磁気テープ））、光学ディスク（例えば、コンパクトディスク（`CD`）、デジタル多用途ディスク（`DVD`））、スマートカード、フラッシュメモリ装置（例えば、カード、スティック、キードライブ）を含む（尚、これらに限定されない）。また、搬送波（キャリア波）を用いてコンピュータ可読電子データを搬送することができる。搬送波は、例えば、電子メールを送受信するときに使用する搬送波や、インターネットもしくはローカルエリアネットワーク（`LAN`）等のネットワークにアクセスするときに使用する搬送波である。勿論、当業者であれば、本発明の範囲及び精神・思想から離れることなく、上記した装置等に多くの変更・変形等をなすことができるであろう。

【0 0 1 4】

また、本明細書において使用される「例示的な」の用語は、例を示す場合に用いる用語である。「例示的な」ものとして本明細書に示された態様・特徴や構造・構成・設計は、他の態様・特徴や構造に比べて好ましいもしくは優れているという意味に必ずしも解釈す

10

20

30

40

50

べきではない。用語「例示的な」は、技術思想を具体的な形で示すために使用されているのである。本明細書において「もしくは」、「または」等の用語は、当該用語の前後のものの中からいずれかを選択するという意味ではなく、両者を含んでもよいという意味で用いている。つまり、特に明記されていない限り、あるいは、文脈や前後関係から明らかな場合を除き、「XがAもしくは（または）Bを使用する」という文は、自然循環的に全てを包含することを意味している。よって、XがAを使用する場合と、XがBを使用する場合と、XがAとBの双方を使用する場合があるとき、「XはAもしくは（または）Bを使用する」という文は、上記3つの場合をすべて含む。

【0015】

ここで、図面を参照し、まず図1を参照して高セキュリティのPOSトランザクション環境のためのフロントエンドシステム100を説明する。概要を説明すると、システム100は、POSコンポーネント104に取り付け可能な（及び／または埋め込み可能な）フロントエンドインターフェース102を有することができる。フロントエンドインターフェース102は、支払手段（図示せず）から得られたデータ106がPOSコンポーネント104に受信されると、当該データ106をインターセプトする（奪う）ことができる。例えば、データ106はフロントエンドインターフェース102によりインターセプトされる（データ106は、インターセプトされないなら、符号108の破線で示すようにPOSコンポーネント104を横切る）。その後、データ106はセキュリティコンポーネント110に移動される。セキュリティコンポーネント110はデータ106を暗号化し、暗号化データ112を生成する。暗号化データ112はPOSフロントエンド114内の他のPOSコンポーネント（図示せず）に出力され、及び／または、POSアプリケーション（図示せず）に出力される。

【0016】

図示されるように、POSフロントエンド114は1つのPOSコンポーネント104を含むことができる。しかし、当然のことながら、POSフロントエンド114は、それぞれ異なる特性を有する多くのPOSコンポーネント104を含んでもよい。例示されたPOSコンポーネント104は以下において図2及び図3を参照して詳細に説明される。POSコンポーネント104は、例えば、店頭においてデータ106を獲得し及び／または処理するように実装される、ハードウェア、ソフトウェア、またはこれらの組み合わせのいずれでもよい。従って、説明の都合上、そしてこれに限定するわけではないが、POSフロントエンド114及び／または幾つかのもしくは全てのPOSコンポーネント104は、小売店・店舗の支払レジに設けられても良いし、小売店・店舗のコンピュータもしくはサーバに設けられてもよい。上記の場所に加えて、あるいは、上記の場所ではなく、POSコンポーネント104は自動販売機、公衆電話、乗継駅（例えば、自動改札装置）、キオスク、駅売店、通交料金徴収所等に設けることができる。つまり、POSコンポーネント104は、支払手段からのデータ106を受信することができる装置であれば、実質的に任意の装置に設けることができる。

【0017】

本発明の1つの態様によれば、本発明の1つの特徴の本質は、POSアプリケーションへの及び／またはその他の安全でない可能のあるアプリケーションやコンポーネントへの、データ106のセキュアではない露出を抑制することである。特に上記アプリケーションは通常、重要度の高いデータの誤った取扱いの主な源となり、さらに／または、ハッカーの主たるターゲットとなったり、詐欺、ID窃盗等に用いられる悪意・悪質コード（malicious code）となる。したがって、フロントエンドインターフェース102はデータ106がPOSアプリケーションに転送される（渡される）前にデータ106をインターセプトすることができる。その後、セキュリティコンポーネント110はデータ106を暗号化することができ、POSアプリケーション（もしくはその他のアプリケーション）はデータ106を受信する必要はなく、その代わりに、暗号化されたデータ112を受信する。暗号化されたデータ（暗号化データ）112は、POSアプリケーションの制御から外れる（離れる）と、復号化可能となる（典型的な場合、支払バックエン

ド（図示せず）において復号化可能となる）。これについては、図 5 及び図 6 を参照して以下において詳細に説明する。上記事項によれば、POS アプリケーション（もしくは別のアプリケーション）が高重要データ（例えば、データ 106）の取り扱いを誤る可能性が大幅に低減される。

【0018】

一般的に POS アプリケーションは、POS フロントエンド 114 及び／または（複数の）POS コンポーネント 104 に密接に関連づけられているので、セキュリティコンポーネント 110 が POS フロントエンド 114 において知られ、保存され、及び／または作成されたパスワード／コード／キーもしくは暗号化方式に従ってデータ 106 を暗号化することは望ましくない場合が多い。もし暗号化してしまうと、パスワードその他の手段が知られた場合に、POS アプリケーションによって処理される（取り扱われる）暗号化データ 112 が復号化される可能性が生ずる。その結果、高セキュリティ POS 支払トランザクション環境の効率・有効性のいくつかが損なわれてしまう。また、暗号化データ 112 は、最終的には、POS アプリケーションを通過した後のある時点で復号化しなければならない（当該復号化も、典型的には、支払バックエンドにおいてなされる）。従って、暗号化データ 112 を復号化する能力は、支払バックエンドが利用可能でなければならない能力であり、その他の意図していないアプリケーションやコンポーネントにより利用可能（またはアクセス可能）であってはならない。

【0019】

従って、本発明の 1 つの態様によれば、PKI（公開鍵基盤）を使用して、上記問題点を抑制することができる。一般に、PKI は周知の仕組みであり、利用者はユーザ ID を点検して認証することができる。PKI はまた、公開鍵を特定の複数のユーザに結び付けることを可能にし、これは通常、中央（中枢）にあるソフトウェアが分散配置された他のソフトウェアと協調しながら実施する。公開鍵は典型的には証明書に含まれている。PKI により、例えば、ユーザ同士を互いに認証することができる。さらに、ID 証明書に含まれる情報（例えば、複数の公開鍵のうちの 1 つ）を使用して、ユーザ間で送信されるメッセージを暗号化し認証することができる。

【0020】

一般に、PKI は、クライアントソフトウェア、サーバソフトウェア（例えば、認証機関）、ハードウェア（例えば、スマートカード）及び処理手順から成る。最初のユーザは秘密鍵を用いてメッセージにデジタル署名することができ、次のユーザは当該署名をチェックすることができる（例えば、PKI 内の認証機関によって発行された最初のユーザの証明書に含まれている公開鍵を使用して）。これにより、2 つ（もしくは 3 つ以上）の通信者（communicating parties）は、事前に秘密情報を交換することなく、機密性（秘匿性）、メッセージ完全性（message integrity）及びユーザ認証を確立することができる。

【0021】

上記説明によれば、POS コンポーネント 104 は、例えば、金融協会、金融団体、支払プロセッサ等により規定された PKI を用いて、支払バックエンドコンポーネントに係付けられた公開鍵を受信することができる。公開鍵はセキュリティコンポーネント 110 に与えることができ、暗号化データ 112 を生成するのに使用することができる。この場合、信頼できるバックエンドコンポーネントだけが暗号化データ 112 を復号化できるようにする（例えば、秘密鍵を使用して）。よって、支払手段に付随した高重要度データ 106 または当該情報を復号化するツールが、POS アプリケーションもしくは他の危険なコンポーネントや第三者によりアクセス可能である必要はない。また、暗号化手法の多くの関連する特徴は、最も信頼性の高い関与者（例えば、金融協会や金融団体）によって決めることができる。

【0022】

次に図 2 を参照すると、フロントエンドを備えたシステム 200 が示されており、このフロントエンドはよりセキュアな POS トランザクション環境を促進することができる複

数の例示的POSコンポーネントを有している。上述したように、フロントエンド114は例えば小売店（もしくはその他の施設・設備等）に設けられたPOSカウンタであり、種々のPOSコンポーネント104を含むことができる。これらPOSコンポーネント104は下記において個々にもしくは全体を一まとめにして、POSコンポーネント104として参照され、または、それぞれの特性に応じて、例えば、POS入力装置104₁、POSサービスオブジェクト104₂、POSミドルウェア104_Nなど、特定の参照符号を付けて称されることもある。当然のことながら、例示的POSコンポーネント104のすべてが存在する必要はなく、また、他のPOSコンポーネント104が追加的にまたは選択的に図2に示したPOSコンポーネント104に存在してもよい。さらに、POSコンポーネント104は図示された構成とは異なる構成で存在してもよい。

10

【0023】

例として（これに限定されるわけではないが）、従来のPOSフロントエンド（例えば、小売店のチェックアウトカウンタ／キオスク・レジ）は、例えば、支払手段202からデータ106を物理的に読み取り、または他の方法で獲得するPOS入力装置104₁を含む。本発明の1つの態様によれば、支払手段202はクレジットカードであり、POS入力装置104₁は磁気ストライプ（テープ）読取機（MSR：Magnetic Stripe Reader）である。しかしながら、他の態様でもよく、それらの多くは図3及び図4において示されており、後述される。本発明の説明のために従来のPOSフロントエンドの説明に戻ると、MSR装置（例えば、POS入力装置104₁）は、磁気トラックデータ（磁気テープ部のデータ：例えば、データ106）を付随MSRサービスオブジェクト（例えば、POSサービスオブジェクト104₂）に転送することができる。このMSRサービスオブジェクト（POSサービスオブジェクト104₂）は、処理前の（生の）磁気トラックデータを復号化すること及び／または所定フォーマットにすることができ、復号化されたデータをPOSアプリケーション204に送信することができる。典型的には、POSアプリケーション204は、その後、支払リクエストをクレジットカード情報とともに支払バックエンドに送ることができる。

20

【0024】

しかしながら、本発明の1つの目的がPOSアプリケーション204からデータ106へのアクセスを制限することであるので、システム200はフロントエンドインターフェース102を有している。フロントエンドインターフェース102は1つ以上のPOSコンポーネント104に組み込まれるか取り付けられる。従って、フロントエンドインターフェース102支払手段202から得られたデータ106をインターセプトすることができる。また、セキュリティコンポーネント110はデータ106を暗号化して暗号化データ112を生成することができる。理想的には、フロントエンドインターフェース102はPOS入力装置104₁（例えば、MSR）に取り付けられる。なぜなら、典型的な場合、このPOS入力装置が、支払手段202から得られたデータ106に（最初に）アクセスできる最初の（第1の）POSコンポーネント104であるからである。この場合、データ106は、支払手段202から受信されると直ちに暗号化することができる（それにより暗号化データ112が生成される）。

30

【0025】

本発明の別の目的は本明細書で説明される多くの特徴を、既存のハードウェアを用いて提供できるようにすることである。例えば、データ106の暗号化をする場合、既存のPOSフロントエンドのハードウェアもしくはソフトウェアに最小限の変更をするだけで当該暗号化を行うことができるようにする。つまり、いくつかの場合、既存のPOS入力装置104₁はフロントエンドインターフェース102及び／またはセキュリティコンポーネント110をサポートすることができない。そのような場合、フロントエンドインターフェース102を他のPOSコンポーネント104（例えば、POSサービスオブジェクト104₂）に設けることができる。

40

【0026】

典型的には、POSサービスオブジェクト104₂はプロセッサもしくはコントローラ

50

で実行されるソフトウェアコードにより構成されているので、POSサービスオブジェクト104₂にフロントエンドインターフェース102を実装することは、POSアプリケーション204がデータ106ではなく暗号化データ112に関与するようにするためには、かなりコスト面で有利である。しかし、フロントエンドインターフェース102（及び／もしくはこれに付随しているセキュリティコンポーネント110）をPOS入力装置104₁もしくはPOSサービスオブジェクト104₂のいずれかに実装することができない場合、POSミドルウェア104_Nを使用することができる。即ち、フロントエンドインターフェース102がPOSミドルウェア104_Nに用いられ、データ106がPOSアプリケーション204に到達する前にデータ106を暗号化する。

【0027】

ミドルウェアはコンピュータ技術分野においては周知のものであり、アプリケーション及び／もしくはコンポーネントが本質的に異なるハードウェアとネットワーク環境を介して相互通信（対話・相互作用）できるようにするコミュニケーションレイヤであると言える。よって、POSミドルウェア104_Nは通常の中継ミドルウェアコンポーネントであってもよいし、POS装置、コンポーネント及び／もしくはトランザクション（支払処理・決済処理）に適した構成・機能を有するミドルウェアであってもよい。

【0028】

図3及び図4は例示的POS入力装置及び例示的支払手段に関連している。例えば、図3は例示的POS入力装置104₁のブロック図であり、図4は例示的支払手段202のブロック図である。尚、図2及び図3は理解を助けるための図であり、限定的な意味を持つ図ではない。ここで特に示したもの以外のPOS入力装置104₁及び／または支払手段202を用いてもよい。それらPOS入力装置104₁及び支払手段202も、本明細書の開示及び本発明の範囲及び精神の中に含まれる。例えば図2に基づいて既に説明したように、POS入力装置104₁はMSR装置302であってよい。MSR装置302はトランザクションを行うために口座情報（アカウント情報）を読み取ることができる装置である。口座情報は例えば、クレジットカード402、デビットカード、チャージカード（もしくはその他の支払手段202）の例えば磁気テープから読み取る。MSR装置302はPOSレジ（図示せず）に一体化されてもよいし、別個のコンポーネントとして付設されてもよい。あるいは、MSR装置302はクレジットカード402（もしくはギフト認証カード等の磁気ストライプを含む支払手段202）の処理のための専用端末の一部として設けられてもよい。

【0029】

さらにPOS入力装置104₁は磁気インク文字認識（MICR：Magnetic Ink Character Recognition）装置304または他のタイプの光学装置306であってもよい。光学装置（例えば、上記装置304または306）は文字認識アプリケーションにおいて使用して、特定の情報（例えば、口座番号、支店コード（Routing Number））を判断・判定することができる。この特定の情報は、チェック404もしくはその他の換金可能な手段406等の支払手段202に付随している情報である。MICR装置（例えば、MICR装置304）の場合、当該装置は特別な文字（この特別な文字は、しばしば、銀行業界によって採用された基準に基づいた特別なインクで印字されている）を読めるように構成されている。このような特別な文字は典型的には、チェック404またはその他の換金可能手段406の下部に特別なフォントで印刷されている（例えば、E-13B、CMC-7等）。従って、MICR装置304は通常的光学装置306によりも高い効率且つ低いエラー率でチェック404を処理することができる。

【0030】

POS入力装置104₁の他の例としては、発光ダイオード（LED）装置308が挙げられる。発光ダイオード装置308は例えば、バーコードタイプ等の光学読取装置（例えば、レーザスキャナ）である。LED装置308を使用して特典クーポン408等（例えば、口座名義人に電子的に提供される割引券：この電子的割引券は口座名義人によって

10

20

30

40

50

印刷されることもある)を読み取ることができる。さらにPOS入力装置104₁はPIN(Personal Identification Number)パッド310であってもよい。PINパッド310により、口座名義人のPIN(コード)等の追加ID情報を認証することができる。PINパッド310は例えば、クレジットカード/チャージデビットカード402もしくはその他の支払手段202とともに使用することができる。

【0031】

POS入力装置104₁はRFID(Radio Frequency Identification)トランシーバ312であってもよい。RFIDトランシーバ312は非接触型カードもしくは非接触型装置410(またはRFIDタグを備える装置、つまり、RFIDトランスポンダ412)とともに使用することができる。RFIDトランシーバ312はスマートカードからデータ(例えば、口座情報・アカウント情報)を受信することができる。RFIDトランシーバ312は特に大量トランジットシステムにおいて広範に利用されており、高速でトランザクション(支払処理・決済処理)をすることができる。

【0032】

図5を簡単に見ると、よりセキュアなトランザクション処理環境を実現できるバックエンドシステム500が示されている。一般的にシステム500はバックエンドインターフェース502を含む。バックエンドインターフェース502は例えば支払バックエンド506に設けられた支払コンポーネント504に取り付けられる(あるいは組み込まれる)ようになっている。支払バックエンド506は、例えば、支払手段に付随しているクレジットカード発行会社、銀行、その他の金融団体・機関等に対応したコンピュータもしくはサーバを有することができる。説明の都合上、従来の支払バックエンドシステムはデータをPOSアプリケーションから受信するように構成されている(例えば、図2を用いてPOSアプリケーション204に関連して詳述されたように)。従って、データ(このデータは従来にあっては暗号化されていない)は支払バックエンド506に入り、1つ以上の支払コンポーネント504によって処理される(符号508の破線で示したように)。しかしながら、支払バックエンド506が暗号化データ112(例えば、図1及び図2のPOSフロントエンド114の出力)を受信するならば、支払バックエンド506は暗号化データ112を処理する能力及び/もしくは復号化する能力を備えていなければならない。

【0033】

よって、バックエンドインターフェース502は暗号化データ112をインターセプトすることができ、復号化コンポーネント510は暗号化データ112を復号化することができる。その結果、暗号化されていないデータ106は支払コンポーネント504もしくは支払バックエンド506内の他の支払コンポーネント(図示せず)に送られる。このようにすることで、採用されている暗号化スキーム(例えば、図1及び図2のPOSフロントエンド114において採用されているもの)は、支払バックエンド506において、及び/またはシステム500によって、決定することができる。従って、暗号(方法)情報512を事前にPOSフロントエンドに提供することができるし、または、例えば、POSにおいてトランザクションをする直前、もしくはトランザクションをしている間に、POSフロントエンドからの要求に応じてPOSフロントエンドに提供することもできる。

【0034】

次に図6を参照すると、バックエンドを備えるシステム600が示されており、このバックエンドは例示的支払コンポーネントを含んでいる。この支払コンポーネントにより、よりセキュアなトランザクション処理環境を促進することができる。一般に、支払バックエンド506は暗号情報512をインターネットなどのWAN(Wide Area Network)により、離れたところにいる第三者に送信することができる。暗号情報512は復号化コンポーネント510(及び/または1つ以上の支払コンポーネント504₁〜504_M)に安全に保存され、図1に基づいて上述したPKIに関連づけられる。例え

ば、暗号情報 5 1 2 は公開鍵 5 1 2₁や暗号化アルゴリズム 5 1 2₂を含んでいる。

【0035】

暗号情報 5 1 2 は支払バックエンド 5 0 4（もしくはそのコンポーネント）または別の金融団体によって、及び／または、暗号情報 5 1 2 は制度委員会（regulatory committee）もしくは基準委員会もしくは他の金融団体・協会によって決められる。よって、PKI（及び暗号情報 5 1 2）は、POS 販売者・納入業者もしくは他の者（トランザクションが行われる可能性が高いところ）よりも信頼性の高いもしくはより確実な者によって形成される。また、フロントエンドもしくはバックエンドのいずれかで使用されるツール・手段は、上記金融団体・協会により認証・承認・証明されるので、支払プロセッサ、（カード）発行銀行、加盟店銀行及びカード団体・協会にとって、支払データのセキュリティ及び信頼度はより高いレベルになる可能性がある。さらに、フロントエンドもしくはバックエンドで使用されるツール・手段は、POS アプリケーション及びソリューションのデータセキュリティコンプライアンス認証を簡略化することができる。なぜなら、当該アプリケーション及びソリューションの 1 つの態様をプラットフォームにより保証することができるからである。

【0036】

上記の説明によれば、支払バックエンド 5 0 6 は暗号化データ 1 1 を POS アプリケーション 2 0 4 から受信することができる。典型的な場合、上述したように、暗号化データ 1 1 2 は支払手段から得られた目立つデータ及び／もしくは重要なデータである。この暗号化データ 1 1 2 は暗号情報 5 1 2 を用いて暗号化される。暗号化データ 1 1 2 は例示した支払コンポーネント 5 0 4₁－5 0 4_Mの 1 つに転送される。支払コンポーネント 5 0 4₁－5 0 4_Mの幾つかもしくは全ては支払バックエンド 5 0 6 に設けることができる。バックエンドインターフェース 5 0 2 は支払コンポーネント 5 0 4₁－5 0 4_Mの 1 つ以上に付設されるか内臓され、暗号化データ 1 1 2 をインターセプトすることができる。

【0037】

例えば、バックエンドインターフェース 5 0 2（及び復号化コンポーネント 5 1 0）は支払コンポーネント 5 0 4₁に接続することができる。この場合、復号化コンポーネント 5 1 0 は例えば、公開鍵 5 1 2 に付随している（公開鍵とペアになっている）秘密鍵 6 0 2 を用いて暗号化データ 1 1 2 を復号化することができる。なぜなら、進行中のトランザクションは支払手段に付随した主要金融機関によってなされるからである。支払プロセッサ 5 0 4₁が暗号化データ 1 1 2 の復号化をサポートすることはできない、及び／または、復号化のために支払プロセッサ 5 0 4₁がバックエンドシステムに対して非常に多くの変更を要求する場合、復号化は支払オブジェクト 5 0 4₂で実行される。さらに、図 2 に基づいて詳細に説明した POS ミドルウェア 1 0 4_Nの場合と同じように、支払バックエンド 5 0 6 はミドルウェア（例えば、支払ミドルウェア 5 0 4_M）を使用して、例えば、暗号化データ 1 1 2 を復号化することができる。

【0038】

図 7 は、POS トランザクション情報のエンドツーエンド（end-to-end）暗号化を可能にするシステム 7 0 0 のブロック図を示している。システム 7 0 0 は、本発明の特徴・態様の多くが同時に示され且つ協調して（協働して）相互通信できる 1 つの例示的实施形態を図示するために提示されている。図示されているように、1 つ以上の支払コンポーネント 5 0 4 を含むことができる支払バックエンド 5 0 6 は、暗号情報 5 1 2（例えば、公開鍵等）を POS フロントエンド 1 1 4（もしくは POS フロントエンド 1 1 4 内のコンポーネント）に送信することができる。支払コンポーネント 5 0 4 には、バックエンドインターフェース 5 0 2 及び復号化コンポーネント 5 1 0 が付設されている。POS フロントエンド 1 1 4 は、支払手段 2 0 2 から得られたデータ 1 0 6 を受信することができる。

【0039】

例えば、POS コンポーネント 1 0 4 は MSR 装置であり、支払手段 2 0 2（例えば、クレジットカード）の磁気ストライプ・テープをスキャン（走査）する。フロントエンド

インターフェース102はMSR装置（もしくは別のPOSコンポーネント104）に取り付けることができ、データ106をインターセプトすることができる。セキュリティコンポーネント110は暗号化されていないデータ106から暗号化データ112を生成することができる。この暗号化の際に、例えば、公開鍵もしくはその他の暗号情報512を利用する。幾つかの場合、最終的には、まず他のPOSコンポーネント104（例えば、POSサービスオブジェクト）を通過した後、暗号化データ112をPOSアプリケーション204に送信することができる。その後、暗号化データ112は支払バックエンド506に転送することができる。

【0040】

POSアプリケーション204（及びその他の安全性の低い可能性があるアプリケーション）は、非暗号化データ106にアクセスする必要が全く無い。暗号化データ112は、複数の支払コンポーネント504のうちの1つに受信されたなら、復号化コンポーネント510によって復号化される。また、所定範囲の実施オプションもある。一例として、データ106は読取ハードウェア（例えば、POS入力装置）において暗号化することができる。別の例では、データ106の暗号化の全てがソフトウェアにより行われる（例えば、POSサービスオブジェクト、POSミドルウェアもしくは別のPOSコンポーネント104において行われる）。暗号化機能がハードウェア（MSR装置や他のPOS入力装置）に組み込まれており、復号化が支払プロセッサによって行われる場合は、暗号化データだけがPOSフロントエンド114のソフトウェアスタック（software stack）を通過する場合もあり得る。

【0041】

説明の一貫性と理解のために、セキュリティコンポーネント110によって実行される暗号化は、非対称PKI公開鍵もしくは認証により行われると本明細書に記載したが、他の手法を上記手法に加えてもいいし、他の手法を上記手法の代わりに使用してもよい。例えば、1つの例では、使い捨て（1回しか使えない）対称鍵によりデータ106を暗号化し、非対称鍵により暗号化された対称鍵をデータと共に転送する。暗号化アルゴリズム、鍵の長さ（キー長）、及び／または暗号情報512の他のパラメータは、ソリューションにより予め規定するか、支払プロセッサ、支払オブジェクトもしくは他の支払コンポーネント504により特定するか、第三者機関もしくは第三者団体により特定することができる。

【0042】

既に説明したように、本発明の1つの目的はPOSアプリケーション204を未暗号化データ（暗号化されていないデータ）106から隔離することである。上記の説明において、POSフロントエンド114と支払バックエンド506はほとんどPOSアプリケーション204専用のもので説明されてきた。例えば、データ106はPOSフロントエンド114で暗号化することができ、暗号化データ112としてPOSアプリケーション204を通過することができ、その後、支払バックエンド506で復号化されている。しかしながら、幾つかの場合、POSフロントエンド114と支払バックエンド506の一方または双方がPOSアプリケーション204の特徴・性質・機能を有してもよい。例えば、幾つかの供給者（vendors）がPOSサービスオブジェクト及び／もしくはPOSミドルウェアを実装してもよい（例えば、POSアプリケーション204によりロードされた外部ライブラリ及び／または外部モジュールとして実装する）。同様に、支払オブジェクト及び／もしくは支払ミドルウェアは同じような手法でPOSアプリケーション204により実装することができる。従って、このような場合、より包括的な理解のために、フロントエンドインターフェース102及び／もしくはセキュリティコンポーネント110がPOSアプリケーション204の外部モジュール等（もしくは外部モジュール等の一部）として存在することができる。同様に、バックエンドインターフェース502及び／もしくは復号化コンポーネント510についても同じ様に考えることができる。

【0043】

図8、図9及び図10はコンピュータ実装方法のプロセスフロー図を示している。説明

10

20

30

40

50

を簡単にするために、ここに示された方法（例えば、フローチャートとして示されている）の1つもしくは複数は、一連の動作（a c t）として図示され説明されるが、本発明は記載された動作順に限定されない。つまり、本発明によれば、いくつかの動作は異なる順序で実施することができ、且つ／または、図示された（もしくは説明された）他の動作と同時に実施することができる。例えば、当事者であれば、本発明の方法は、一連の相互関連状態または事象として記載すること（例えば、状態図のように）ができることが理解できるであろう。さらに、本発明に基づいて方法を実施するのに、図示された（説明された）動作の全てが必要というわけではない。

【0044】

図8を参照すると、インターフェースを設定するための方法800を示す手順の例示的フローチャートが示されている。符号802において、第1のインターフェースが設定される。このインターフェースはPOSコンポーネントと相互通信するためのインターフェースである。POSコンポーネントは例えば、POS入力装置（例えば、MSR装置、MICR装置、PINパッド、RFIDトランシーバ）である。また、POSコンポーネントはPOS入力装置に付随しているPOSオブジェクトであってもよい。あるいは、POSコンポーネントはPOSミドルウェアであってもよい。POSコンポーネントのタイプに拘わらず、第1のインターフェースはPOSコンポーネントと相互通信できるように設定することができ、例えば、動作可能に（o p e r a t i v e l y）POSコンポーネントに接続される。

【0045】

符号804において、第2のインターフェースが設定される。このインターフェースは支払コンポーネントと相互通信するためのインターフェースである。支払コンポーネントは例えば、支払プロセッサ、または支払プロセッサに付随している支払オブジェクトである。さらに、支払コンポーネントは支払ミドルウェアであってもよい。よって、手元にある（用意された）支払コンポーネントの種類・タイプに拘わらず、第2のインターフェースは支払コンポーネントと相互通信・相互作用することができる。

【0046】

次に図9を参照すると、支払手段に付随した情報がPOSアプリケーションに送信される前に、当該情報をインターセプトして暗号化するための方法を示す手順の例示的フローチャートが示されている。概要を説明すると、符号902において購入手段に関連した情報とともに支払処理データ（トランザクションデータ）が受信される。購入手段は例えば、クレジットカード、デビットカード、チェックもしくは他の換金可能な手段、非接触型カードもしくはRFIDトランスポンダを備えたその他の手段である。トランザクションデータは実質的に任意のPOSコンポーネント（図8で説明したもの）において第1のインターフェース（図8で説明したもの）により受信することができる。

【0047】

符号904において、金融団体に対応する公開鍵を検索して入手する。公開鍵はデータ記憶部に存在し、購入手段に付随している情報に基づいてアクセスすることができる。これに加え、あるいは、これに代えて、トランザクションの間に公開鍵を金融団体から入手することができる（例えば、もし公開鍵が上記データ記憶部になれば、公開鍵を更新する必要がある）。符号906において、公開鍵を使用して、支払手段から得られたPOSTランザクションデータが暗号化される（例えば、PKIシステムに基づいて）。符号908において、暗号化されたPOSTランザクションデータはPOSアプリケーション（もしくは別のアプリケーション）に転送される。

【0048】

次に図10を参照すると、トランザクションデータがPOSアプリケーションを通過した後、トランザクションデータをインターセプトして復号化するための方法を示す手順の例示的フローチャートが示されている。符号1002において、暗号化（された）POSTランザクションデータがPOSアプリケーションから受信される。例えば、POSTランザクションデータは、POSフロントエンドのアプリケーションに行く前に受信されて

暗号化することができる。符号1004において、秘密鍵を用いて暗号化POSTランザクションデータを復号化することができる。秘密鍵は例えば、PKIシステムに基づいてPOSフロントエンドにおいて暗号化に使用された公開鍵（一对の鍵）とペアになっている。

【0049】

図11A-図11EはPOSTランザクションのエンドツーエンド処理のための様々な構成を示しており、同時に参照され得る。当該コンポーネントは少なくとも1つの態様を表すが、他の構成も可能であり、それらも本発明の範囲及び精神に含まれる。例えば、図11A-図11Eは理解を容易にするために、MSR装置102を主（第1の）入力装置として示しているが、他の入力装置を使用してもよい。さらに、残りのコンポーネントは、他の様々な実施形態においても存在してよい。

10

【0050】

図11Aは従来のPOSTランザクションの態様を示している。MSR装置1102（例えば、店頭にある）はデータ1104を得る（例えば、クレジットカードの磁気ストライプ（テープ）を読むことによってデータを得る）。MSR装置1102は磁気ストライプから読み取ったデータ1104を、付随しているサービスオブジェクト1106に送信する。サービスオブジェクト1106は生データ1104を復号化し、当該データ1104をPOSアプリケーション1108に転送することができる。POSアプリケーション1108は支払いリクエストを上記データ1104とともに支払オブジェクト1110に送ることができる（あるいは、幾つかの場合、はっきりと図示してしてはいないが、支払プロセッサ1114に直接送ることができる）。POSアプリケーション1108から情報を受け取ると、支払オブジェクト1110はリクエストを支払プロセッサ1114に送ることができる、且つ／または、データ1112を支払プロセッサ1114に転送することもできる。データ1112はデータ1104とほぼ同じであるが、データ1112は例えば、支払プロセッサ1114バックエンドの構成・機能によっては、暗号化されたりされなかったりする。

20

【0051】

図11Bは本発明の1つの態様に基づく構成を示している。特に、図11Aに示された従来の構成は本明細書において説明するように改良することができ、公開鍵1118を支払プロセッサ1114からPOSフロントエンドへ（例えば、MSR装置1102自身へ）送ることができる。よって、支払手段から得られたデータ等の重要度の高いランザクションデータを、可能な限り早く暗号化することができる。特に、POSアプリケーション1108（もしくはフロントエンドハードウェア等で動作している別のアプリケーション）は上記情報（暗号化されていない状態の情報）にアクセスすることができなくなる。図示したように、暗号化されたデータ1116だけが、残りのコンポーネント（例えば、符号1106、1108、1110、…）を通過して支払プロセッサ1114に至る。

30

【0052】

図11Cは本発明の1つの態様を示している。この態様では、ランザクションデータの暗号化がMSRサービスオブジェクト1106（MSR装置1102ではない）においてなされる。例えば、この態様は、MSR装置1102が暗号化機能を容易に備えることができない場合に採用される。公開鍵1118は支払プロセッサ1114からMSRサービスオブジェクト1106に送信することができ、MSRサービスオブジェクト1106においてデータ1104が暗号化される。よって、暗号化データ1116をPOSアプリケーション1108に送ることができ、その後、支払オブジェクト1110に送り、最後に、支払プロセッサ1114に送ることができる。

40

【0053】

図11Dは本発明の1つの態様を示している。この態様では、復号化が支払オブジェクト1110（支払プロセッサ1114ではない）においてなされる。尚、暗号化はMSRサービスオブジェクト1106においてなされると説明したが、暗号化は図11Bに基づいて上述したようにMSR装置1102においてなされてもよい。従って、図示していな

50

いが、公開鍵 1 1 1 8 は M S R 装置 1 1 0 2 に送信することができる。この場合、M S R サービスオブジェクト 1 1 0 6 へ送られるように図示されているデータ 1 1 0 4 は、暗号化データ 1 1 1 6 になる。いずれにせよ、P O S アプリケーション 1 1 0 8 は暗号化データ 1 1 1 6 しか受信せず、このデータ 1 1 1 6 は支払オブジェクト 1 1 1 0 に送られ、そこで暗号化データ 1 1 1 6 は本明細書で説明したように復号化される。よって、データ 1 1 1 2 (このデータは例えば、支払バックエンドで採用された構成・設定に基づいて復号化されるか、あるいは、復号化されない) は支払プロセッサ 1 1 1 4 に送信することができる。

【0054】

図 1 1 E は本発明の 1 つの態様を示している。この態様は、フロントエンドもしくはバックエンドの少なくとも一方が容易に暗号化機能／復号化機能を備えることができない態様である。特に、ハードウェア (例えば、M S R 装置 1 1 0 2) もソフトウェア (例えば、M S R サービスオブジェクト 1 1 0 6) も、暗号化をすることができない場合、または、暗号化機能を備えるように変更することがフロントエンドにとって都合良くない場合 (ミドルウェアを使用する方が都合が良い場合)、P O S ミドルウェア 1 1 2 0 を使用して公開鍵 1 1 1 8 を受信すること、及び／もしくは、データ 1 1 0 4 を暗号化することができる。同様に、もしバックエンドがハードウェアレベル及びソフトウェアレベルのいずれにおいても適切な復号化を行うように設定されないならば、または、単にミドルウェアの使用がより好ましいバックエンドソリューションであるならば、支払ミドルウェア 1 1 2 2 を使用してデータ 1 1 1 6 を復号化してもよい。一旦復号化されると、データ 1 1 0 4 は支払オブジェクト 1 1 1 0 に送信することができ、当該データはその後、データ 1 1 1 2 として支払プロセッサ 1 1 1 4 に送信される。データ 1 1 1 2 は別のプロトコルに基づいて暗号化される場合もあるし暗号化されない場合もある。次のことが理解されるべきである。

【0055】

ここで、符号 1 1 0 6、1 1 1 0、1 1 2 0 及び 1 1 2 2 が符号 1 1 0 8 の外部モジュールとして P O S システム上で動作していることを強調すべきか？

【0056】

次に図 1 2 を参照すると、開示されたアーキテクチャを実行するように動作できる代表的なコンピュータシステムのブロック図が示されている。本発明の色々な態様に追加的な内容を加えるために、図 1 2 及び下記の記載において、本発明の当該色々な態様を実施することができる適切なコンピューティング環境 1 2 0 0 の簡単な且つ全体的な (全般的な) 説明をする。例えば、システムの種々のコンポーネント及び／もしくは上述した態様はシステム 1 2 0 0 によって実装することができる。また、本発明は本明細書において 1 つ以上のコンピュータで実行されるコンピュータ実行可能命令の一般的な説明の範疇で記載されてきたが、当事者であれば、本発明は他のプログラムモジュールとともに実装すること、及び／もしくは、ハードウェアとソフトウェアの組み合わせとして実装することができることが理解できるであろう。

【0057】

一般的に、プログラムモジュールはルーチン、プログラム、コンポーネント、データ構造等を含み、これらにより特定のタスクを実施したり、特定の抽象データ型を実行する。さらに、当事者であれば、本発明の方法は他のコンピュータシステム構造でも実施することができることが理解できるであろう。他のコンピュータシステム構造とは、単一プロセッサコンピュータシステム、マルチプロセッサコンピュータシステム、ミニコンピュータ、メインフレームコンピュータ、パーソナルコンピュータ、携帯型コンピューティング装置・デバイス、マイクロプロセッサを使用した家庭用電子機器、プログラム可能な家庭用電子機器等である。これらは 1 つ以上の付随デバイスに接続可能である。

【0058】

本発明の図示された態様は、分散型コンピュータ環境で実施することもできる。分散型コンピュータ環境では、通信ネットワークを介して接続された遠隔処理装置によって所定

のタスクが実行される。分散型コンピュータ環境では、プログラムモジュールはローカルメモリストレージ及びリモートメモリストレージに設けることができる。

【0059】

典型的にコンピュータは種々のコンピュータ可読媒体を含んでいる。コンピュータ可読媒体は、コンピュータによってアクセスできる任意の媒体であり、揮発性媒体及び不揮発性媒体を含み、取外し可能媒体及び取外し不可能媒体を含む。例えば（次のものに限定されないが）、コンピュータ可読媒体は、コンピュータストレージ媒体及び通信媒体を含む。コンピュータストレージ媒体は揮発性及び不揮発性の取外し可能媒体及び取外し不可能媒体を含む。これら媒体は、情報（コンピュータ可読命令、データ構造、プログラムモジュールその他のデータ等）の記憶・保存のためのすべての方法及び技術・手段において実装することができるものである。コンピュータストレージ媒体は（次のものに限定されないが）、RAM、ROM、EEPROM、フラッシュメモリ、その他のメモリ手段、CD-ROM、DVD、その他の光学ディスク記憶手段（ストレージ）、磁気カセット、磁気テープ、磁気ディスク記憶手段（ストレージ）、その他の磁気記憶手段・デバイスを含み、所望の情報を記憶するのに使用でき且つコンピュータによりアクセス可能な前記以外の任意の媒体も含む。

10

【0060】

通信媒体は、典型的には、コンピュータ可読命令、データ構造、プログラムモジュールもしくはその他のデータを変調データ信号（例えば、搬送波やその他の移送手段）に保持しており、任意の情報移送媒体を含む。「変調データ信号」という用語は、信号内の情報を暗号化するように設定もしくは変更された1つ以上の特性を有する信号を意味する。例えば（次のものに限定されないが）、通信媒体は、有線媒体（例えば、有線ネットワーク（wired network）や直接配線接続（direct-wired connection））及び無線媒体（例えば、音響、RF、赤外線、その他の無線媒体）を含む。上記したものの任意の組み合わせもコンピュータ可読媒体の範疇に入る。

20

【0061】

図12を再び参照すると、本発明の種々の態様・特徴を実装するための代表的な環境1200は、コンピュータ1202を含んでいる。コンピュータ1202は処理ユニット1204とシステムメモリ1206とシステムバス1208を含む。システムバス1208はシステムコンポーネント（例えば、システムメモリ1206：尚、システムメモリに限定されない）を処理ユニット1204に接続している。処理ユニット1204は市場入手可能な任意のプロセッサであってよい。デュアルマイクロプロセッサ及び他のマルチプロセッサアーキテクチャも、処理ユニット1204として用いることができる。

30

【0062】

システムバス1208は幾つかのタイプのバス構造のいずれでもよい。このシステムバスは、色々な市場入手可能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が付設されている場合もあるしされていない場合もある）、周辺バス、ローカルバスにさらに接続できる。システムメモリ1206はROM1210及びRAM1212を含む。BIOS（basic input/output system：ベーシックインプット／アウトプットシステム）が非揮発性メモリ1210（例えば、ROM、EPROM、EEPROM）に記憶されている。BIOSは、例えば起動の際に、コンピュータ1202内の要素同士間で情報を転送するのに役立つ基本ルーチンを含む。RAM1212は高速RAM（例えば、データをキャッシュするためのスタティックRAM）を含む。

40

【0063】

コンピュータ1202は内臓（内部）ハードディスクドライブ（HDD）1214を更に含む（内蔵HDD1214は例えば、EIDEやSATAである）。内臓HDD1214は適切な支持構造・ハウジング（図示せず）で外部（外付け）使用できるように構成されてもよい。コンピュータ1202はまた、磁気フロッピー（登録商標）ディスクドライブ（FDD）1216（例えば、取外し可能なディスク1218に読み書きするため

50

のドライブ)と光学ディスクドライブ1220(例えば、CD-ROMディスク1222を読んだり、その他の大容量光学媒体(例えば、DVD)に読み書きするためのドライブ)を含む。ハードディスクドライブ1214、磁気ディスクドライブ1216及び光学ディスクドライブ1220はハードディスクドライブインターフェース1224、磁気ディスクドライブインターフェース1226及び光学ドライブインターフェース1228により、それぞれシステムバス1208に接続することができる。外部(外付け)ドライブ用のインターフェース1224は、USB(Universal Serial Bus)及びIEEE1394インターフェース手段の少なくとも一方を含む。その他の外部ドライブ(駆動装置)接続手段も本発明の範囲に属する。

【0064】

上記ドライブ(駆動装置)及びこれらに取付けられるコンピュータ可読媒体により、データ、データ構造、コンピュータ実行可能命令等の不揮発的(nonvolatile)記憶が可能になる。コンピュータ1202については、上記ドライブ(駆動装置)及び媒体が適切なデジタルフォーマットで任意のデータを記憶する。上記コンピュータ可読媒体の説明はHDD、取外し可能磁気ディスク及び取外し可能光学媒体(例えば、CDやDVD)についてなされたが、当事者であれば、コンピュータにより読み取ることができる他のタイプの媒体(例えば、zipドライブ、磁気カセット、フラッシュメモリカード、カートリッジ)も上記した例示的な動作環境において使用できることは理解できるであろう。また、当事者であれば、上記のような媒体は本発明の方法を実施するためのコンピュータ実行可能命令を含むことができることも理解できるであろう。

【0065】

多数のプログラムモジュールが上記ドライブ(駆動装置)及びRAM1212に記憶可能である。プログラムモジュールは、オペレーティングシステム(OS)1230、1つ以上のアプリケーションプログラム1232、その他のプログラムモジュール1234及びプログラムデータ1236を含む。上記オペレーティングシステム、アプリケーション、モジュール及び/もしくはデータの全てもしくは一部はRAM1212にキャッシュすることができる。尚、本発明は種々の市場入手可能なオペレーティングシステムまたはオペレーティングシステムの組み合わせにより実施・実装することができる。

【0066】

ユーザはコマンド及び情報を1つ以上の有線入力装置/無線入力装置(例えば、キーボード1238及びポインティング装置(例えば、マウス1240))によりコンピュータ1202に入力することができる。他の入力装置(図示せず)としては、マイク、赤外線リモートコントローラ、ジョイスティック、ゲームパッド、スタイラスペン、タッチスクリーン等がある。上記及びその他の入力装置・デバイスはしばしば、処理ユニット1204に入力装置インターフェース1242を介して接続される。入力装置インターフェース1242はシステムバス1208に接続されている。尚、入力装置・デバイスは他のインターフェース(例えば、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インターフェース)により処理ユニットに接続されてもよい。

【0067】

モニタ1244またはその他のタイプの表示装置も、インターフェース(例えば、ビデオアダプタ1246)を介してシステムバス1208に接続することができる。モニタ1244に加え、典型的なコンピュータは他の周辺出力装置(図示せず;例えば、スピーカやプリンタ)を含んでいる。

【0068】

コンピュータ1202は論理接続手段を使用してネットワーク環境で動作することができる。論理接続手段は有線通信手段及び/もしくは無線通信手段を介して1つ以上のリモートコンピュータ(例えば、リモートコンピュータ1248)に接続されている。リモートコンピュータ1248は、例えば、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(携帯型)コンピュータ、マイクロプロセッサベースの娯楽用機器(エンターテインメントアプライアンス)、ピアデバイス及びその他の

一般的なネットワークノードである。リモートコンピュータ1248は典型的には、コンピュータ1202に関連して説明された要素の多くもしくは全てを含む。但し、説明を簡単にするために、メモリ／ストレージ装置1250しか図示されていない。図示した論理接続手段は、LAN1252及び／もしくはより大きなネットワーク（例えば、WAN1254）につながる有線接続手段／無線接続手段を含んでいる。LAN及びWANのネットワーク環境は大抵のオフィスや企業に存在しており、会社内のコンピュータネットワーク化（例えば、イントラネット）を可能にしている。上記ネットワークの全ては、インターネット等のグローバルな（国際的な）通信ネットワークに接続することができる。

【0069】

LANネットワーク環境で使用される場合、コンピュータ1202はローカルネットワーク1252に有線通信ネットワークインターフェース及び／もしくは無線通信ネットワークインターフェース（つまりアダプタ1256）を介して接続される。アダプタ1256はLAN1252への有線通信もしくは無線通信を可能にしている。LAN1252は、ワイヤレスアダプタ1256と通信するためのワイヤレスアクセスポイントを有している。

【0070】

WANネットワーク環境で使用される場合、コンピュータ1202はモデム1258を有するか、WAN1254上の通信サーバに接続されるか、WAN1254を介して通信を確立するためのその他の手段を有する（例えば、インターネットを利用して）。モデム1258は内部に設けられることもあるし外部に設けられることもあり、且つ、有線装置であっても無線装置でもよい。モデム1258はシステムバス1208にシリアルポートインターフェース1242を介して接続される。ネットワーク環境では、コンピュータ1202に関連して図示（説明）されたプログラムモジュールまたはその一部はリモートメモリ／ストレージ装置1250に記憶しておくことができる。図示されたネットワーク接続は例示であり、コンピュータ同士間で通信を確立する他の手段を使用してもよい。

【0071】

コンピュータ1202は、ワイヤレス環境内に設けられた任意のワイヤレス装置もしくはワイヤレスエンティティ（例えば、プリンタ、スキャナ、デスクトップコンピュータ及び／もしくはポータブルコンピュータ、PDA、通信衛星、ワイヤレスで検知可能なタグを備えた機器、ワイヤレスで検知可能なタグを備えた設備（例えば、キオスク、売店、露店、トイレ）及び電話）と通信することができる。これは少なくともWiFi及びBluetooth（登録商標）ワイヤレス手段・装置・技術を含む。よって、通信は従来のネットワークのように予め規定された構造を持つものでもよい。あるいは、通信は少なくとも2つの装置の間で為される純粋にアドホックな通信でもよい。

【0072】

WiFi（ワイヤレスフィデリティ）を用いると、自宅のソファ、ホテルの部屋のベッドまたは会社の会議室から配線無しでインターネットへ接続することができる。WiFiは携帯電話において使用されているのと同じようなワイヤレス技術（無線技術）である。この技術によれば、所定の装置（例えば、コンピュータ）はデータを室内及び室外に送受信することができる。送受信は基地局の通信範囲内であれば可能である。WiFiネットワークはIEEE802.11（a、b、g、その他）と呼ばれる無線技術を利用して、高セキュリティで（安全で）高信頼性で高速度のワイヤレス接続を提供する。WiFiネットワークを用いて、コンピュータ同士を接続することができるし、コンピュータをインターネットに接続することもできるし、コンピュータを有線ネットワーク（IEEE802.3であるイーサネット（登録商標）を使用するもの）に接続することもできる。WiFiネットワークは免許不要の2.4GHz及び5GHz無線帯域で、例えば、11Mbps（802.11a）もしくは54Mbps（802.11b）データレートで動作するか、上記帯域の両方を含む（デュアルバンド）製品とともに動作する。よって、WiFiネットワークは、多くのオフィスで使用されている基本的な12BaseT有線イーサネット（登録商標）ネットワークと同じような実世界（における）性能を提

10

20

30

40

50

供することができる。

【0073】

次に図13を参照すると、本願において開示されたアーキテクチャを実行することができる例示的コンピュータコンパイルション (compilation) システムの概略ブロック図が示されている。システム1300は1つ以上のクライアント1302を含む。クライアント1302はハードウェア (例えば、コンピュータインターフェースサポート付きのデジタルカメラ) 及び／もしくはソフトウェアである (例えば、スレッド、プロセス、コンピューティング装置)。クライアント1302は、例えば、本発明を使用することにより、クッキー及び／もしくは関連コンテクチュアルインフォメーション (associated contextual information) を有することができる。

10

【0074】

システム1300はさらに、1つ以上のサーバ1304を含む。サーバ1304もまた、ハードウェア及び／もしくはソフトウェアである (例えば、スレッド、プロセス、コンピューティング装置)。サーバ1304はスレッドを有することができ、例えば、本発明を使用することにより、変換 (transformations) を行うことができる。クライアント1302とサーバ1304との間で行うことができる1つの通信は、2つ以上のコンピュータプロセスの間で送信できるデータパケットを用いて行われる。データパケットは、例えば、クッキー及び／もしくは関連コンテクチュアルインフォメーションを含むことができる。システム1300は通信フレームワーク1306 (例えば、インターネット等のグローバル通信ネットワーク) を含む。通信フレームネットワーク1306を利用することにより、クライアント1302とサーバ1304との間の通信を容易に行うことができる。

20

【0075】

通信は有線 (光ファイバを含む) 技術・手段及び／もしくは無線技術・手段を利用すると容易に行うことができる。クライアント1302は1つ以上のクライアントデータ保存部1308に接続される。クライアントデータ保存部1308を使用することにより、クライアント1302にローカルな情報 (例えば、クッキー及び／もしくは関連コンテクチュアルインフォメーション) を記憶することができる。同様に、サーバ1304は1つ以上のサーバデータ保存部1310に接続される。サーバデータ保存部1310を使用することにより、サーバ1304にローカルな情報を記憶することができる。

30

【0076】

上記において説明された事項・内容は種々の実施形態の例を含む。勿論、実施形態の内容を説明するという目的のためにコンポーネントや方法の考え得る全ての組み合わせを説明することは不可能である。しかし当業者であれば、多くの他の組み合わせ及び置換・変更が可能であることが理解できるであろう。従って、発明の詳細な説明 (実施形態) の内容は、本発明の精神及び範囲内にある置換、変更及び変形の全てを含むことを意図している。

【0077】

特に上記したコンポーネント、装置、デバイス、回路、システム等によって実行・発揮・達成される種々の機能については、当該コンポーネント等を説明するために使用された用語 (手段という用語を含む) は、特に別の (異なる) 説明がない限り、上記コンポーネント等の特定の機能を実行・発揮・達成する任意のコンポーネント等を意味する (例えば、機能的に均等なものも意味する・含む)。たとえ開示された構造と構造的に均等ではないものであっても、上記実施形態の例示的な態様・特徴の機能を実行・発揮・達成するものであれば、上記コンポーネント等に含まれる。この点に関連して言えば、上記実施形態は上記した種々の方法の行為・動作・ステップ及び／もしくはイベント・事象を実施するための、システムとコンピュータ実行可能命令を有するコンピュータ可読媒体とを含む。

40

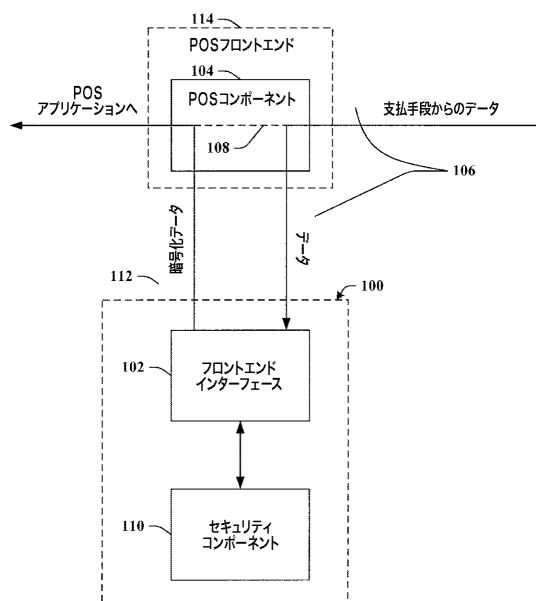
【0078】

また、1つの特定の特徴が幾つかの例の1つについて開示されてきたが、所定のもしく

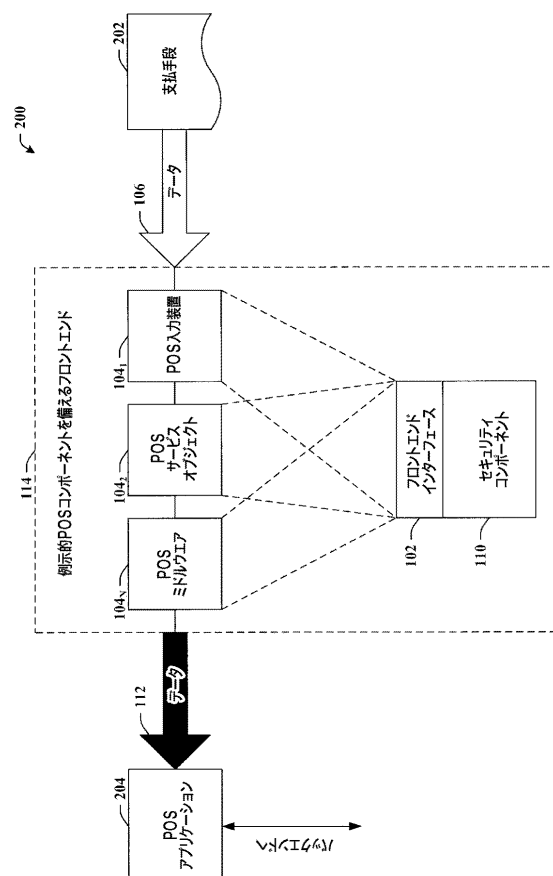
50

は特定の用途において必要で且つ有利な場合には、当該特徴は他の例の他の特徴（１つまたは複数の特徴）に組み合わせることができる。さらに、明細書もしくは特許請求の範囲において「含む」、「有する」及び「備える」という表現・用語が用いられる場合、そのような表現・用語は、他の要素が加えられ得ることを意図している。

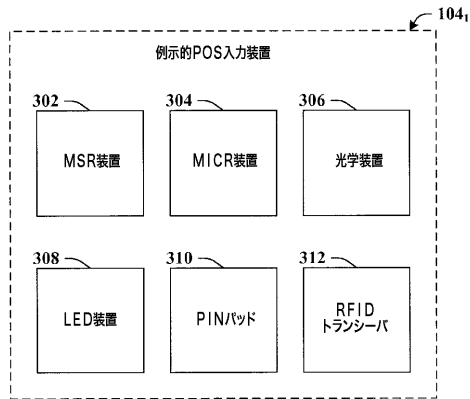
【図 1】



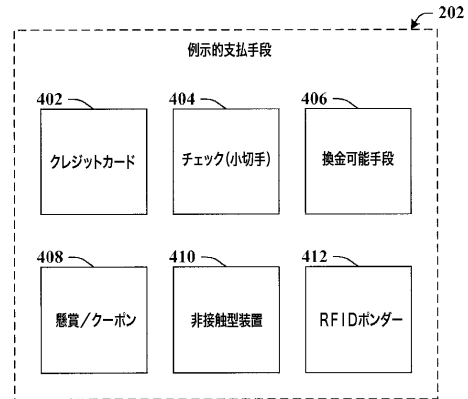
【図 2】



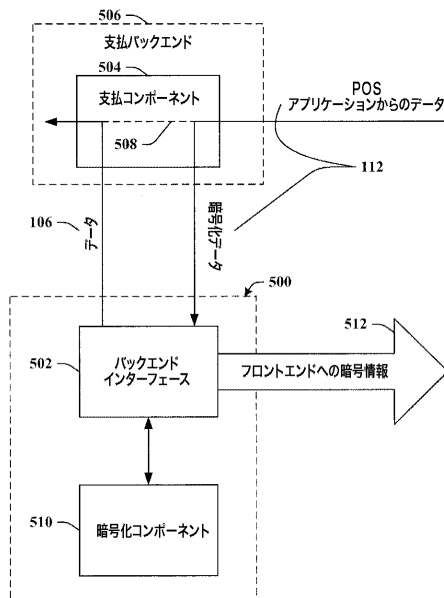
【図 3】



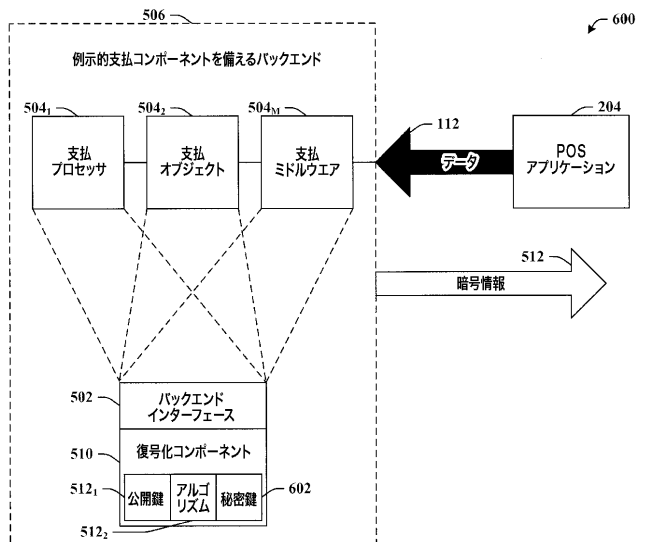
【図 4】



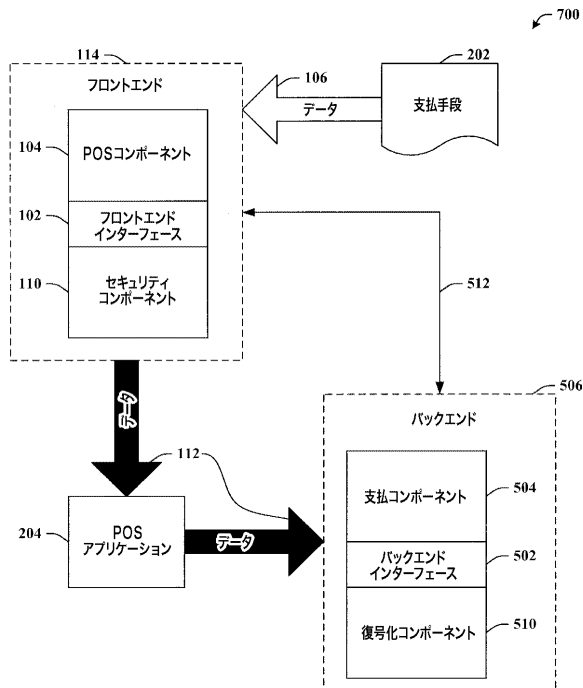
【図 5】



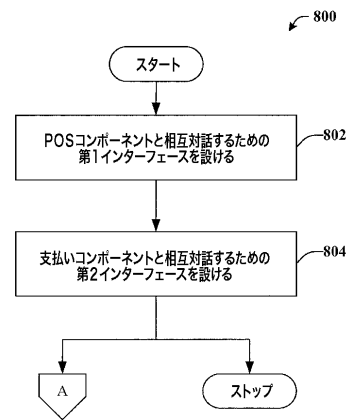
【図 6】



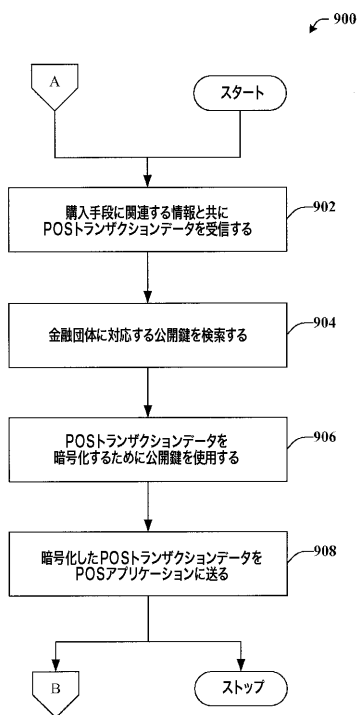
【図 7】



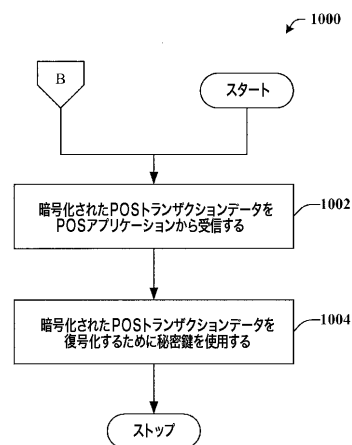
【図 8】



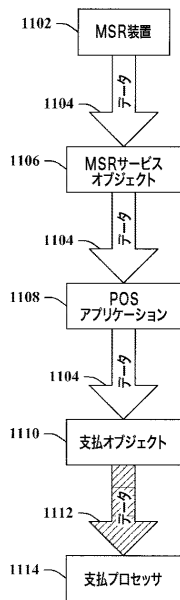
【図 9】



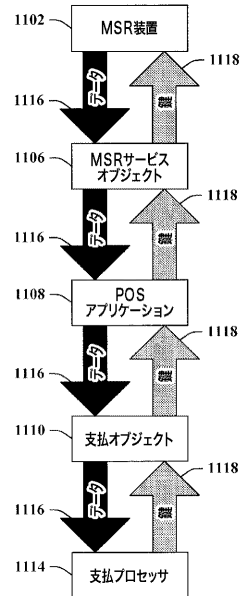
【図 10】



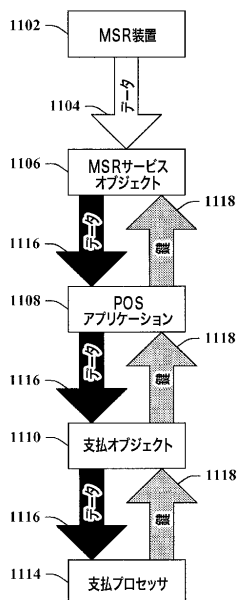
【図 1 1 A】



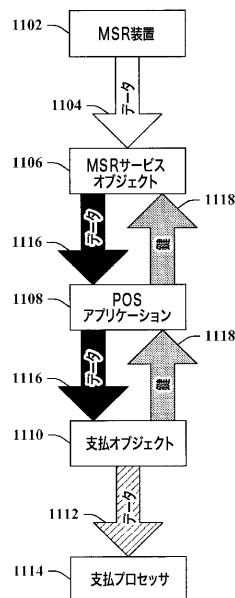
【図 1 1 B】



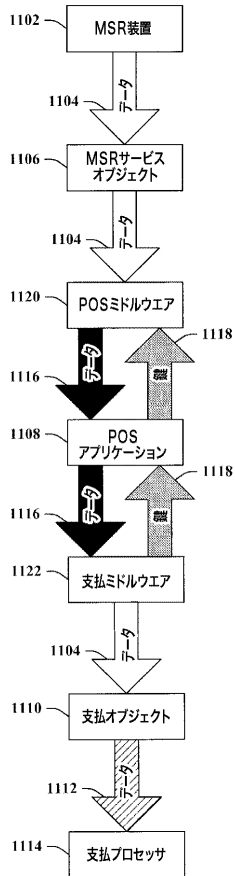
【図 1 1 C】



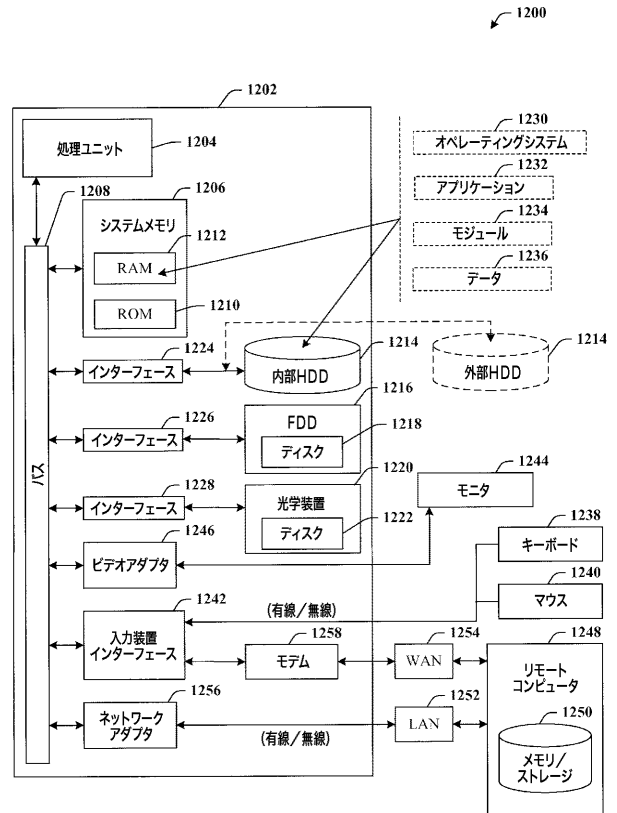
【図 1 1 D】



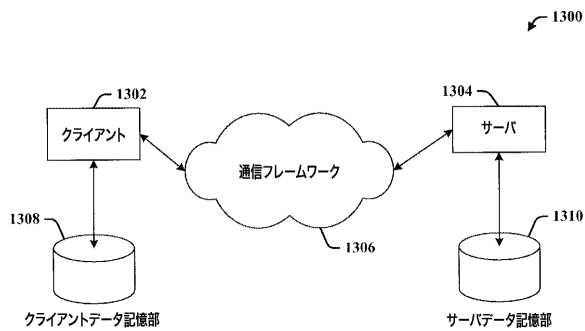
【図 1 1 E】



【図 1 2】



【図 1 3】



【国際調査報告】

INTERNATIONAL SEARCH REPORT		International application No. PCT/US2007/083551
A. CLASSIFICATION OF SUBJECT MATTER		
<i>H04L 9/08(2006.01)i, G06Q 20/00(2006.01)i</i>		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) IPC 8 : H04L, G06Q		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Korean Utility models and applications for Utility models since 1975 Japanese Utility models and applications for Utility models since 1975		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) eKIPASS(KIPO internal), "POS(Point-of-Sale) system", "PKI"		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,442,448 B1 (MICHAEL C. FINLEY et al.) 27 August 2002. see abstract and claims 1-52	1-20
Y	US 6,312,175 B1 (JACKSON LUM) 6 November 2001. see abstract and claims 1-10	1-20
Y	US 2002/0123970 A1 (HAROLD AARON LUDTKE et al.) 5 September 2002. see abstract and claims 1-69	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 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 27 FEBRUARY 2008 (27.02.2008)		Date of mailing of the international search report 27 FEBRUARY 2008 (27.02.2008)
Name and mailing address of the ISA/KR  Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140		Authorized officer LEE, Jun Seok Telephone No. 82-42-481-8199 

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2007/083551

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6,442,448 B1	27.08.2002	AU200053233A1 WO200075065A2	28.12.2000 14.12.2000
US 6,312,175 B1	06.11.2001	TW457446B US469435S1 US487088S1	01.10.2001 28.01.2003 24.02.2004
US 2002/0123970 A1	05.09.2002	US07251633B1	31.07.2007

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW

(72)発明者 チャールズ ジェイ. ウィリアムス

アメリカ合衆国 98052 ワシントン州 レッドモンド ワン マイクロソフト ウェイ
マイクロソフト コーポレーション インターナショナル パテント内

(72)発明者 クレイグ ジェンセン

アメリカ合衆国 98052 ワシントン州 レッドモンド ワン マイクロソフト ウェイ
マイクロソフト コーポレーション インターナショナル パテント内

Fターム(参考) 3E142 BA01 CA12 FA02 FA08 FA25 GA02 GA03 GA04 GA05 GA07

HA01 HA14 JA02 JA03

5B017 AA03 BA07 CA16

5J104 AA12 AA16 EA04 EA15 EA16 EA17 EA19 JA21 NA02 NA37

NA39 PA10