

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4772251号

(P4772251)

(45) 発行日 平成23年9月14日 (2011.9.14)

(24) 登録日 平成23年7月1日 (2011.7.1)

(51) Int. Cl. F 1
G 0 6 Q 20/00 (2006.01)
 G 0 6 F 17/60 4 0 2
 G 0 6 F 17/60 4 1 4

請求項の数 12 (全 15 頁)

(21) 出願番号	特願2001-575392 (P2001-575392)	(73) 特許権者	500557864
(86) (22) 出願日	平成13年4月11日 (2001.4.11)		マスターカード インターナショナル インコーポレーテッド
(65) 公表番号	特表2004-500671 (P2004-500671A)		アメリカ合衆国 ニューヨーク州 105
(43) 公表日	平成16年1月8日 (2004.1.8)		77-2509 パーチェス パーチェス
(86) 国際出願番号	PCT/US2001/011911		ストリート 2000
(87) 国際公開番号	W02001/078024	(74) 代理人	100147485
(87) 国際公開日	平成13年10月18日 (2001.10.18)		弁理士 杉村 憲司
審査請求日	平成20年4月4日 (2008.4.4)	(74) 代理人	100143568
(31) 優先権主張番号	60/195,963		弁理士 英 貢
(32) 優先日	平成12年4月11日 (2000.4.11)	(74) 代理人	100072051
(33) 優先権主張国	米国 (US)		弁理士 杉村 興作
(31) 優先権主張番号	09/809,367		
(32) 優先日	平成13年3月15日 (2001.3.15)		
(33) 優先権主張国	米国 (US)		

最終頁に続く

(54) 【発明の名称】 コンピューターネットワークを介して安全な支払いを実行する改良方法及びシステム

(57) 【特許請求の範囲】

【請求項 1】

支払いネットワークを介して支払い用の支払いアカウントを用いて取引を行う方法において、

(a) 前記支払いアカウントの発行者以外のサービスプロバイダが、第1の支払いアカウント番号を利用する前記取引の許可に対する第1の許可要求を受信し、この第1の許可要求において、

(i) 前記第1の支払いアカウント番号は、前記発行者以外の前記サービスプロバイダと関連するサービスプロバイダ識別番号を有するとともに第2の支払いアカウント番号と関連し、前記第2の支払いアカウント番号は前記発行者と関連する発行者識別番号を有し、前記第2の支払いアカウント番号は前記第1の許可要求に含まれず、

(i i) 前記第1の許可要求はアクワイヤラーと関連する第1のアクワイヤラーコードを含み、

(i i i) 前記第1の許可要求は、前記サービスプロバイダ識別番号に基づいて、前記支払いネットワークを経て前記サービスプロバイダに送ることができ、

(b) 前記サービスプロバイダが、前記第1の許可要求に回答して、前記第1の支払いアカウント番号及び前記サービスプロバイダに格納されたアカウント番号変換テーブルに基づいて、前記第2の支払いアカウント番号を検索し、前記取引の許可に対する第2の許可要求を前記第2の支払いアカウント番号を用いて送信し、前記第2の許可要求は前記サービスプロバイダと関連する第2のアクワイヤラーコードを含むと共に、前記発行者識別番

10

20

号に基づいて、前記支払いネットワークを経て前記発行者に送ることができ、

(c) 前記サービスプロバイダが送信した前記第2の許可要求に対する応答を前記発行者から受信し、該応答は前記第2のアクワイヤラーコードを含み、該コードに基づいて前記支払いネットワークを経て送ることができ、

(d) 前記サービスプロバイダが前記発行者から受信した前記第2の許可要求に対する応答に基づいて、前記サービスプロバイダが受信した前記第1の許可要求に対する応答を、前記サービスプロバイダが前記アクワイヤラーに送信し、この第1の許可要求に対する応答は前記第1のアクワイヤラーコードを含み、該コードに基づいて前記支払いネットワークを経て送ることができることを特徴とする取引方法。

【請求項2】

10

前記発行者からの前記第2の許可要求に対する応答は、更に、前記第2のアカウント番号を含み、前記サービスプロバイダにより送信される前記第1の許可要求に対する応答は前記第1の支払いアカウント番号を含むことを特徴とする請求項1記載の方法。

【請求項3】

メッセージ認証コードが取引データの少なくとも一部に基づいて前記アクワイヤラーにより生成され、前記第1の許可要求は1つの任意フィールドを含む複数のフィールドを有する標準トラックでフォーマットし、前記任意フィールドに前記メッセージ認証コードを置くことを特徴とする請求項1記載の方法。

【請求項4】

前記サービスプロバイダは、セキュリティモジュールを用いて前記第2の支払いアカウント番号に対する鍵を導出して、前記メッセージ認証コードを検証することを特徴とする請求項3記載の方法。

20

【請求項5】

通信ネットワークを介する加盟店との取引を、第2の支払いアカウント番号と関連する第1の支払いアカウント番号を用いて行う方法において、

(a) 一つ以上の取引明細に基づいてメッセージ認証コードを生成し、

(b) 少なくとも前記第1の支払いアカウント番号と前記メッセージ認証コードを前記加盟店に送信し、

(c) 前記加盟店が前記第1の支払いアカウント番号を用いて取引の支払いに対する第1の許可要求をサービスプロバイダに要求し、前記第2の支払いアカウント番号は前記第1の許可要求には含まれず、該要求は、あたかも支払いが慣例の磁気支払用カードでPOS端末で行われるようにフォーマットされ、該フォーマットは少なくとも任意データフィールドを含むトラックを有するものとし、該フィールドで前記メッセージ認証コードを送信し、

30

(d) 前記第1の支払いアカウント番号に対する許可要求に応答して、前記サービスプロバイダが、前記第1の支払いアカウント番号及び前記サービスプロバイダに格納されたアカウント番号変換テーブルに基づいて、前記第2の支払いアカウント番号を検索し、前記第2の支払いアカウント番号を用いて前記取引の支払いに対する許可を発行者に要求し、

(e) 前記発行者から受信した前記第2の支払いアカウント番号及びメッセージ認証コードに対する許可要求に対する応答に基づいて、前記サービスプロバイダが前記第1の支払いアカウント番号に対する許可要求を受諾又は拒否し、

40

前記第1及び第2の支払いアカウント番号はそれぞれサービスプロバイダ及び発行者識別番号を含み、前記発行者以外の前記サービスプロバイダは、前記サービスプロバイダ識別番号に基づいて支払いネットワークを経て前記加盟店の要求を受信し、且つ前記サービスプロバイダは前記第2の支払いアカウント番号を用いて支払いの許可に対する前記要求を発生し、該要求を前記発行者識別番号に基づいて前記支払いネットワークを経て送ることを特徴とする取引方法。

【請求項6】

前記サービスプロバイダは前記支払いに対する許可要求内に前記サービスプロバイダと

50

関連するアクワイヤラーコードを含み、前記発行者からの前記応答が前記サービスプロバイダに返送されることを特徴とする請求項5記載の方法。

【請求項7】

前記加盟店による前記要求は関連する加盟店アクワイヤラーコードを含み、且つ前記サービスプロバイダは前記受諾または拒否ステップに基づくメッセージを発生させ、該メッセージを前記関連する加盟店アクワイヤラーコードに送ることを特徴とする請求項6記載の方法。

【請求項8】

通信ネットワークを介して取引を行う方法において、

発行者識別番号を有する発行者が第1の支払いアカウント番号をコンピュータを有するユーザに発行し、前記発行者識別番号は前記第1の支払いアカウント番号と関連するものとし、

発行される各第1の支払いアカウント番号に対し一意の秘密鍵を発生するセキュリティモジュールを設け、

前記第1の支払いアカウント番号と関連する第2のアカウント番号を発生し、

サービスプロバイダが安全支払いアプリケーションを前記コンピュータに提供し、該アプリケーションは前記第2のアカウント番号と前記秘密鍵を含み、

前記安全支払いアプリケーションを前記コンピュータに格納し、

前記金融取引を行う加盟店を選択し、前記加盟店は関連するアクワイヤラーコードを有し、

前記加盟店が前記コンピュータに取引データを送り、

前記取引データに基づいてメッセージ認証コードをコンピュータ生成し、

前記コンピュータが、前記コンピュータ生成された前記メッセージ認証コードと前記第2のアカウント番号を含む標準トラックイメージフォーマットのトラックデータを前記加盟店に送信し、前記コンピュータ生成されたメッセージ認証コードは前記標準トラックイメージフォーマットの任意フィールドに直接に置かれ、

前記加盟店が前記データに基づいて第1の許可要求を発生し、

前記加盟店が前記第1の許可要求を前記サービスプロバイダに送信し、

前記サービスプロバイダが前記第1の許可要求を前記秘密鍵で検証し、

前記サービスプロバイダが、前記第2の支払いアカウント番号及び前記サービスプロバイダに格納されたアカウント番号変換テーブルに基づいて、前記第1の支払いアカウント番号を検索し、

前記サービスプロバイダが、前記第1の支払いアカウント番号を用いて第2の許可要求を該第1の支払いアカウント番号と関連する前記発行者識別番号を有する発行者に送信し、

前記発行者が前記第2の許可要求を許可または拒否することを特徴とする取引方法。

【請求項9】

前記トラックデータは任意データフィールドと、アカウント番号フィールドと、有効期限フィールドとを具え、前記トラックデータの送信ステップは、

前記メッセージ認証データを前記任意データフィールドに置き、

前記第2のアカウント番号を前記アカウント番号フィールドに置き、

有効期限を前記有効期限フィールドに置くことを特徴とする請求項8記載の方法。

【請求項10】

前記取引データは前記関連するアクワイヤラーコード及び取引額を含むことを特徴とする請求項9記載の方法。

【請求項11】

前記検証ステップは更に前記取引データを検証することを特徴とする請求項10記載の方法。

【請求項12】

前記第2の許可要求は前記サービスプロバイダと関連する第2のアクワイヤラーコード

10

20

30

40

50

を含み、更に、

前記許可または拒否ステップに基づいてメッセージを発生し、

前記メッセージを前記アクワイヤラーコードに基づいて前記サービスプロバイダに送り

、

前記加盟店の関連アクワイヤラーコードを用いて前記加盟店に前記メッセージを通知することを特徴とする請求項8記載の方法。

【発明の詳細な説明】

【0001】

(優先権出願)

本願は米国仮出願 60/195,863、2000年4月11日出願、発明の名称“Method and System for Conducting Secure Payments Over A Computer Network”(この出願は参考のためにここに包含されている)及び米国特許出願第09/809,367号、2001年3月15日出願、発明の名称“Method and System for Conducting Secure Payments Over A Computer Network”(この出願も参考のためにここに包含されている)を優先権主張するものであります。

【0002】

(技術分野及び発明の背景)

本発明は、通信ネットワークを介して安全な金融取引を実行する方法及びシステム、特にインターネットのようなコンピュータネットワークを介して支払いを安全に送信する方法及びシステム、及び公衆通信チャネルを介して機密情報を安全に送信する方法及びシステムに関するものである。

自明のように、オンラインコマースはここ数年の間にものすごい成長をとげているが、依然として多くの消費者がトラブルにみまわれ、個人金融情報をインターネットのような公衆ネットワークを介して利用することやクレジットカード番号や個人識別番号のような情報をインターネットのような公衆通信ネットワークを介して送信することに心配をぬぐえないでいる。その結果として、ここ数年間に亘って、多くの会社がコンピュータネットワークを介して行われる支払いのセキュリティを保証し、金融情報の盗聴や悪用の危険を低減させる最良の方法を見つける努力をしている。

【0003】

例えば、マイクロソフトに譲渡された米国特許第5,883,810号「Electronic Online Commerce Card With Transaction Proxy Number For Online Transactions(オンライン取引用のトランザクションプロキシ番号付き電子オンラインコマースカード)」は、各取引ごとに、一時的取引番号を付与し、該取引番号を永久アカウント番号と関連させるシステムを開示している。このシステムでは、取引番号を実クレジットカード番号のようにみなせ、顧客はこの取引番号を使用し、これを加盟店に顧客アカウント番号の代りとして提出することができる。このシステムでは、顧客は自分の実クレジットカード番号を公衆ネットワークを介して送信する必要はない。

【0004】

上記の第5,883,810号特許では、加盟店は取引番号を発行機関に送り、発行機関はこの取引番号をインデックスとして用いて実顧客アカウント番号をアクセスし、許可処理を行い、許可応答を取引番号の下で加盟店に返送する。その結果として、危険は最小になる。その理由は、顧客は取引番号を送るのみであるため、並びに代理番号は一回の買い物又は取引にのみ有効で、他の買い物又は取引に対し繰り返し使用できないため、盗聴するには極めて不利であるためである。(第2欄、第60-61行参照)。

【0005】

従来のシステムは改良の必要があり、特に各取引の実行ごとに、永久アカウント番号の送信の代わりに繰り返し発生される一意の取引番号の生成及び送信を行う必要なしに、安全な商取引をインターネットを介して実行する方法及びシステムが必要とされている。

【0006】

同時継続出願09/809,367号(2001年3月15日出願)の発明では、「仮」

10

20

30

40

50

アカウント番号を顧客に割り当て、顧客の支払いアカウント番号に暗号化してリンクさせる。支払いアカウント番号は、消費者が品物及び／又はサービスの支払いのために使用できる金融機関や他の機関により発行されたアカウント番号である。例えば、支払いアカウント番号はクレジットカードやデビットカードのような支払用カードからのアカウント番号、或いは顧客のコンピュータに格納されている電子マネーアプリケーションのような支払いアプリケーションのアカウントからのアカウント番号とすることができる。仮アカウント番号は加盟店には実支払いアカウント番号のように見える。即ち、仮アカウント番号は正当な支払いアカウント番号と同一の長さを有し、正当な識別番号（例えば、マスターカードインターナショナルインコーポレーテッド（「マスターカード」）に対しては「5」）で始まる。仮アカウント番号は顧客により顧客の全てのオンライン商取引に対して実アカウント番号の代わりに使用される。

10

【0007】

この同時継続出願の発明では、仮アカウント番号に基づく全ての取引を、各アカウント番号ごとに一意の秘密鍵を用いて暗号化して認証を行うのが好ましい。この認証は、公開鍵ペアの個人鍵に基づくもの（公開鍵認証）又は個人鍵以外の秘密鍵に基づくもの（秘密鍵認証）とすることができる。このようにすると、無許可の人が仮アカウント番号を突きとめたとしても、仮アカウント番号を用いて不正な取引を行うことはできない。

【0008】

このシステムは更に改良すべきであり、セキュリティを更に向上させて、公衆通信ラインを介して行われている商取引中送信されるメッセージや情報を保護すべきである。

20

【0009】

（発明の開示）

それゆえ、本発明では、支払いネットワークを用いて取引を行う方法において、サービスプロバイダは取引の許可(authorization)に対する第1の許可要求を第1の支払いアカウント番号を用いて受信し、

（i） 第1の支払いアカウント番号は前記サービスプロバイダと関連するBINコードを有するとともに第2の支払いアカウント番号と関連し、第2の支払いアカウント番号は該第2の番号の発行者と関連するBINコードを有し、

（ii） 前記第1の許可要求はアクワイヤラー(acquirer)と関連するアクワイヤラーコードを含み、

30

（iii） 前記第1の許可要求は、第1の支払いアカウント番号のBINコードに基づいて、支払いネットワークを経て前記サービスプロバイダに送ることができることを特徴とする。

【0010】

本発明の方法は、更に、前記第1の許可要求に応答して、前記サービスプロバイダは、前記取引の許可に対する第2の許可要求を第2の支払いアカウント番号を用いて送信し、第2の許可要求は該サービスプロバイダと関連する第2のアクワイヤラーコードを含むと共に、前記第2のBINコードに基づいて、支払いネットワークを経て前記発行者に送ることができることを特徴とする。

40

【0011】

更に、第2の許可要求に対する前記発行者からの応答を前記サービスプロバイダにより受信し、該応答は前記サービスプロバイダと関連するアクワイヤラーコードを含み、該コードに基づいて、支払いネットワークを経て送ることができることを特徴とする。更に、第1の許可要求に対する応答が前記サービスプロバイダにより、前記第2の許可要求に対する応答に基づいて、アクワイヤラーに送信され、前記第1の許可要求に対する応答はアクワイヤラーと関連するアクワイヤラーコードを含み、該コードに基づいて支払いネットワークを経て送ることができる。

【0012】

本発明の他の好適実施例では、通信ネットワークを介する加盟店(merchant)との取引を、

50

第2の支払いアカウント番号と関連する第1の支払いアカウント番号を用いて実行する方法において、

(a) 一つ以上の取引明細に基づいてメッセージ認証コードを生成し、

(b) 少なくとも前記第1の支払いアカウント番号とメッセージ認証コードを加盟店に送信し、

(c) 加盟店が取引の支払いに対する許可を前記第1の支払いアカウント番号を用いて要求し、該要求は、あたかも支払いが慣例の磁気支払用カードでポイントオブセールス（POS）端末で行われるようにフォーマットされ、該フォーマットは少なくとも任意データフィールドを含むトラックを有するものとし、該フィールドで前記メッセージ認証コードを送信し、

(d) 前記第1の支払いアカウント番号に対する許可要求に応答して、前記取引の支払いに対する許可を前記第2の支払いアカウント番号を用いて要求し、

(e) 前記第2の支払いアカウント番号及びメッセージ認証コードに対する許可要求に対する応答に基づいて、前記第1の支払いアカウント番号に対する許可要求を受諾又は拒否することを特徴とする。

【0013】

本発明の目的、特徴及び利点は本発明の好適実施例を示す添付図面について以下に記載する詳細な説明から更に明らかになる。

全図を通して、断らない限り、同一の符号及び番号は図示の実施例の同一の構成要素や構成部分やコンポーネントを示す。更に、本発明の要旨を図面を参照して好適実施例と関連して詳細に説明するが、特許請求の範囲で限定する本発明の範囲及び精神から逸脱することなく、多くの変更を加えることができること勿論である。

【0014】

（適実施例の詳細な説明）

安全支払いアプリケーション(Secure Payment Application)の初期化

本発明の好適実施例では、サービスプロバイダは、本発明の技術に従って実行すべき安全支払いシステムの安全支払いアプリケーション（SPA）を含むいくつかのコンポーネントを発行、保守及び／又は処理する。

【0015】

図1は、最初に、金融取引カードを保持するカード所有者がどのようにして安全支払いアプリケーションをサービスプロバイダ10からインターネットを介して得ることができるかを示したものである。最初に、本発明の利点を利用及び獲得するためには物理的カードは不要であり、金融取引を行うためにユーザ又は関係者を識別するとともにアカウントにリンクするアカウント番号を所有者（この場合にはカード所有者）に発行するだけであることを理解する必要がある。カード所有者は、インターネットを介して通信できるコンピュータや携帯電話や携帯情報端末（PDA）などの任意の適切なデバイスを用いて、サービスプロバイダと関連するウェブサーバにコンタクトすることができる。以下の説明を簡単とするために、カード所有者はインターネットを介して通信するためにコンピュータを使用するものとする。

【0016】

図1に示すように、サービスプロバイダ、例えばマスターカードインターナショナルインコーポレーテッド（又はマスターカードの代理業者）はその制御下に1以上の物理的セキュリティモジュール12を有する。これらのセキュリティモジュールはモジュール内に格納された情報の物理的保護を提供する。各セキュリティモジュールは1以上の「誘導鍵」を含み、これらの誘導鍵は、以下に説明するように、アカウント固有の秘密暗号鍵を生成及び再生成するために使用され、生成及び再生成された秘密鍵は安全支払いアプリケーションに付与される。

【0017】

最初に、本発明の好適実施例では、カード所有者はサービスプロバイダから安全支払いアプリケーション（SPA）を得る必要がある。SPAをダウンロードし初期化する好適な

10

20

30

40

50

手順は、

1. カード所有者はインターネットを介してサービスプロバイダのウェブサイト（直接或いは発行者のウェブサイトのような他のウェブサイトを経由して当該ウェブサイトに至るハイパーリンクを経て）コンタクトする。

2. カード所有者は、当業者に公知のSSL暗号方式の下で、(a)支払用カードアカウント番号、(b)カード有効期限及び(c)カード認証情報を送る。カード認証情報は、例えばカードのCVC2 valueを含むことができる。CVC2 valueはカードの署名パネルの隣に印刷される3桁又は4桁の値である。

3. サービスプロバイダは、カードアカウント番号及びカード有効期限の正当性を、カード所有者の支払用カードの発行者からゼロアmount許可を得ることにより確認する。例えば、マスターカードはこの許可をBanknet（商標）通信ネットワークを介して得ることができる。

10

4. サービスプロバイダは、カード所有者の支払用カードの発行者がサービスプロバイダにCVC2 valueを検証するための暗号鍵を提供した場合に、CVC2 valueを検証することができる。

5. サービスプロバイダは、他のカード認証情報を検証のために発行者に送ることにより他のカード認証情報を検証することができる。

6. サービスプロバイダ（SP）がカード所有者提供カードデータの正当性を確認した後、SPは仮アカウント番号及び秘密鍵を生成又は選択し、これらのデータ要素を安全支払いソフトウエアアプリケーションに埋込み、インターネットを介してSSL暗号方式の下で行うのが好ましいダウンロードのためにこのアプリケーションをカード所有者に使用可能にする。

20

【0018】

仮アカウント番号はそのBINとして仮アカウント番号用に確保された特殊BINを有する。仮アカウント番号の残りは、サービスプロバイダがテーブルルックアップ処理により「実」アカウント番号に翻訳することができる値である。

【0019】

割り当てられた特殊サービスプロバイダBINは多数のこのような特殊BINの組の中の一つとすることができ、この場合には各BINは特定の国又は地域及び/又は国又は地域内の特定の製品に対応させることができる。従って、割り当てられる特殊BINは提示された「実」アカウント番号の国及び/又は製品に対応するものとすることができる。

30

【0020】

サービスプロバイダがSPAに埋め込むのが好ましい秘密鍵は各カードアカウント番号ごとに一意であり、そのカードアカウント番号と誘導鍵を用いてセキュリティモジュール内で導出するのが好ましい。この誘導鍵自体も同一の又は他のセキュリティモジュール内で高レベル誘導鍵を用いて導出することができる。

【0021】

カード所有者は、安全支払いアプリケーションをダウンロードする前にパスワードをサービスプロバイダに供給するか、或いは安全支払いアプリケーションをカード所有者のコンピュータにインストールしているときにパスワードを選択することができる。パスワードを供給或いは選択する場合、その後カード所有者は安全支払いアプリケーションを起動するためにこのパスワードを入力することを要求される。カード所有者により選択されたパスワードはSPAに含まれる秘密鍵を暗号化するのに使用することができる。

40

【0022】

当業者であれば認識されるように、SPAはデジタルワレット（電子財布）アプリケーションの一部分としてダウンロードすることができる。SPAに加えて、デジタルワレットはカード所有者の個人情報とパース（財布）アプリケーションのような他のアプリケーションを格納することができる。

【0023】

カード固有秘密鍵の生成

50

以下の手順をサービスプロバイダ又はその代理業者により制御されるセキュリティモジュール 12 内で実行して安全支払いアプリケーションに含めるカード固有秘密鍵を得るのが好ましい。以下の手順は、カード所有者の支払用カードが 16 桁のアカウント番号を有するものとし、且つ当業者に既知のデータ暗号アルゴリズム (DEA) を 2 倍長鍵とともに使用するものとする。DEA は米国政府標準暗号アルゴリズムであり、連邦情報処理規格 (FIPS) 46-1 に記載されており、その全てがここに含まれているものとする。DEA は ANSI 規格 X9.32 にも定義されており、その全てもここに含まれているものとする。

【0024】

セキュリティモジュールは 16 バイトからなる誘導鍵というセキュア高レベル鍵を保持し、この誘導鍵を多数の又は全てのカードアカウント番号と一緒に使用し、カード所有者の 16 桁の支払いアカウント番号を与えられると、パー・カード鍵 (カード単位鍵) というカード固有秘密鍵を暗号手法で計算する。誘導鍵は各国ごとに、或いは各特殊バンク識別番号又は BIN ごとに一意にすることができる。

10

【0025】

好ましくは、手順は次のとおりである。

1. 支払いアカウント番号を各 4 ビットの 16 桁の 2 進化 10 進数とみなし、16 バイト誘導鍵の左側の 8 バイトを暗号化鍵として用いてこれらの 64 ビットを DEA 暗号化する。
2. 手順 1 の結果を 16 バイト誘導鍵の右側の 8 バイトを復号鍵として用いて DEA 復号化する。
3. 手順 2 の結果を 16 バイト誘導鍵の左側の 8 バイトを (再び) 暗号鍵として用いて DEA 暗号化する。
4. 手順 3 の結果を固有パー・カード鍵の左側の 8 バイトとして使用する。
5. 手順 3 の結果を 16 バイト誘導鍵の左側の 8 バイトを暗号鍵として用いて DEA 暗号化する。
6. 手順 5 の結果を 16 バイト誘導鍵の右側の 8 バイトを復号鍵として用いて DEA 復号化する。
7. 手順 6 の結果を 16 バイト誘導鍵の左側の 8 バイトを (再び) 暗号鍵として用いて DEA 暗号化する。
8. 手順 7 の結果を 16 バイト固有パー・カード鍵の右側の 8 バイトとして使用し、この鍵を安全支払いアプリケーション内に、このアプリケーションの通常の動作中にこの鍵が暴露されないように置く。

20

30

【0026】

カード所有者と加盟店との通信

図 2 は、本発明の代表的な実施例に従ってインターネットを介して安全支払いを実行する際のカード所有者 14 と加盟店 16 との間の情報の流れを示す。

SPA がカード所有者のコンピュータにインストールされたら、カード所有者は SPA を全てのインターネット支払いに使用するのが好ましく、SPA が全てのインターネット取引に対しカード所有者の仮アカウント番号を提供する。

40

【0027】

カード所有者が取引を行いたい希望を指示したら、加盟店はカード所有者のコンピュータに次のデータ要素: (1) アクワイヤラー BIN、(2) MID (アクワイヤラーに既知の加盟店識別子) 及び取引の日時 (GMT 又は等価時間) を送るのが望ましい。

【0028】

好ましくは、SPA はそれに埋め込まれた秘密鍵を用いて取引に関するメッセージ認証コード (MAC) を生成する。例えば、約 8 桁の 10 進数の MAC を次のデータ要素に基づいて生成することができる。

1. カード所有者の SPA に格納され且つ SPA が MAC を発生するたびに SPA によりインクリメントされる取引シーケンス番号。この取引シーケンス番号は、例えば 6 桁の

50

10進数とすることができる。

2. 加盟店から受信されるBIN、受信されなければゼロ（BINは、例えば6桁の10進数とすることができる）。

3. 加盟店から受信されるMID、受信されなければゼロ（MIDは、例えば6桁の10進数とすることができる）。

4. 加盟店から受信される日付け及び時刻（最も近い時間または分）（GMT）、受信されなければゼロ（日付は、例えば10桁の10進数とすることができる）。

5. カード所有者のために表示され、通常カード所有者から加盟店へのメッセージに含まれる取引額（取引額は、例えば8桁の10進数とすることができる）。

【0029】

加盟店はカード所有者のコンピュータからフルトラック-1イメージを、あたかも加盟店が磁気ストライプリーダを含むコンピュータと通信するかのように受信可能とするのが好ましい。（トラック-1イメージは支払用カードの磁気ストライプのトラック1上のデータをいう。）更に、加盟店はトラック-1データをアクワイヤラーに、まるで取引がポイントオブセールス（POS）取引であるように送ることができるのが好ましい。

【0030】

加盟店がフルトラック-1データを受け取ることができる場合には、MAC自体及びMACの基礎をなすデータ要素はトラック-1の任意データフィールド(任意に使用可能なデータフィールド)に置かれる。仮アカウント番号はトラック-1のアカウント番号フィールドに置かれ、カード有効期限データはトラック-1の有効期限フィールドに置かれる。

【0031】

MACをトラック-1の任意データフィールドで送ることにより、多くの加盟店はそれぞれのシステム及び/又はソフトウェアを変更する必要がない。その理由は、これらの加盟店はトラック-1の任意データを含むPOS取引をすでに処理することができるためである。他の加盟店は、POSを処理するシステム及び/又はソフトウェアを容易に使用可能にすることができる。

【0032】

加盟店がフルトラック-1データを受信できない場合には、仮アカウント番号をカード所有者の「実」アカウント番号の代わりに使用することを除いて、SPAは慣例のSSL支払いメッセージを送ることができる。加盟店は次に取引データを通常のごとくアクワイヤラーに送る。実際には、取引期間中、POS取引をトラック-1データで処理できない加盟店はMACを受信し処理する必要がないかもしれない。

【0033】

MACは、トラック-1の任意データフィールドで送る代わりに、他のフォーマットで送ることもでき、この場合には加盟店とアクワイヤラーはそれぞれのシステム及び/又はソフトウェアをこの他のフォーマットを処理するように変更する必要がある。

【0034】

カード所有者の取引メッセージの受信時に、加盟店はアクワイヤラーに対し慣例の許可要求をフォーマットする。トラック-1データを受け取ることができる加盟店は、この許可要求を、あたかもこれがPOS端末から発生したかのように正確にフォーマットし、カード所有者により供給されたトラック-1データに含める。

【0035】

加盟店がカード所有者取引に対し多数の許可/清算取引(multiple authorizing/clearing transactions)を開始する場合には、これらの取引の最初の取引のみをトラック-1データに含めるのが好ましい。後続の取引は仮アカウント番号と有効期限データのみを含み、通信販売取引とみなすことができる。これは、多数の清算を伴う定期循環支払いや分割支払いの全てに対し真である。

【0036】

許可要求のアクワイヤラー処理

図3は、本発明の代表的実施例におけるアクワイヤラー18と、サービスプロバイダ10

10

20

30

40

50

と、発行者 20 との間の通信を示す。

インターネット取引におけるトラックー 1 データの存在はインターネット加盟店から慣例の電話線を介して受信するアクワイヤラーに悪影響を与えないようにすべきである。その理由は、このような取引は慣例の P O S 端末からの取引と同一にフォーマットされるためである。しかし、（慣例の電話ではなく）インターネットを介して取引を受信するアクワイヤラーは、トラックー 1 データなしの取引はそのまま配達するとともにトラックー 1 データを用いる取引は、あたかも該取引が P O S 端末から到来するかのよう、異なる物理的ワイヤを経て配達する「変換ボックス」を必要とする。このような変換ボックスの設計は当業者が容易に実施し得る範囲のことである。

【0037】

アクワイヤラー 18 がインターネット加盟店 16 から許可要求メッセージを受信すると、アクワイヤラー 18 は発行者 B I N をその B I N テーブルでルックアップする。仮アカウント番号取引の場合には、「発行者」はサービスプロバイダの許可プロセッシングファシリティ 10 に対応し、これがこの要求を受信する。仮アカウント番号でなく実アカウント番号の場合には、通常の処理が行われる。

【0038】

いくつかの国はドメスティック（国内）取引を処理する特殊セキュリティモジュールを具えたファシリティを有し得る。このようなドメスティックファシリティの各々はサービスプロバイダの同意が得られる場合にのみセットアップするとともに、暗号鍵とアカウント番号変換データをその国の取引の処理のために保持するだけとするのが好ましい。このようなドメスティックファシリティを有する国では、全ての同一国の取引がこのファシリティに送られる。これは、望ましいなら、国内の個々の銀行に対し行うこともできる。ドメスティック取引を処理するドメスティックファシリティはドメスティック取引を中央処理ファシリティに行わせるよりも遥かに効率が良い。

【0039】

許可要求のサービスプロバイダ処理

サービスプロバイダは要求を受信すると、発行者 B I N から、アカウント番号が本当に仮アカウント番号であるか決定し、そうであれば、取引を特殊処理システムに送る。このシステムはテーブルルックアップ手法を用いて仮アカウント番号を「実」アカウント番号に変換する。システムが、トラックー 1 イメージが含まれていることを決定する場合には、システムはセキュリティモジュールを用いてこのカードアカウント番号に対し適切なカード毎の鍵(Per Card Key)を M A C の検証のために導出する。

【0040】

M A C を検証したら、システムはトラックー 1 の任意データエリア内の B I N を検査する。B I N がすべてゼロでない場合には、システムはこの B I N を取引のアクワイヤラー B I N と比較し、（加盟店はその取引を一括処理し、遅延した許可を得ることがあることを考慮に入れて）トラックー 1 の任意データエリアに含まれるデータ及び時間が正当であることを検証する。システムは、更に、許可要求額がトラックー 1 任意データエリア内の取引額（カード所有者により許可された額）を規定額（例えば 20 %）以上超えないことを検証する。

【0041】

アクワイヤラーはアクワイヤラーリファレンスデータ（アクワイヤラーリファレンス番号ともいう）内に M I D を含むことができる。23桁のアクワイヤラーリファレンスデータは必須「取引タイプ」インジケータ及び必須アクワイヤラー-B I N を含むものとするが、残りの桁はアクワイヤラーの任意使用用であり、場合により M I D を含むことができるものとする。サービスプロバイダはそのインターネットアクワイヤラーから、アクワイヤラーリファレンスデータ内に M I D を含むアクワイヤラーの指示を得ることができ、もしそうなら、これらのアクワイヤラーはアクワイヤラーリファレンスデータ内に M I D を含む。このようなアクワイヤラーの場合には、トラックー 1 イメージがアクワイヤラー B I N を含む場合、サービスプロバイダシステムはトラックー 1 任意データエリア内の M I D が

10

20

30

40

50

アクワイヤラーリファレンスデータ内のM I Dと一致することも検証することができる。

【0042】

サービスプロバイダシステムは、許可要求内の取引シーケンス番号との比較用に取引シーケンス番号(T S N)の履歴を蓄積することができる。この比較はある条件、例えばトラックー1の額が規定のしきい値(たとえば\$ 200)を超えるとトリガすることができる。このようなしきい値は、トラックー1イメージがアクワイヤラーB I Nを含まないときは低くすることができる。比較がトリガされると、システムはトラックー1任意データエリアに含まれる取引シーケンス番号を当該カードアカウント番号に対する取引シーケンス番号の蓄積履歴と比較することができる。現取引の取引シーケンス番号が(1)現アカウント番号に対する最小蓄積値より高く且つ(2)このアカウントに対する如何なる蓄積値にも一致しない場合には、現取引は先の正当取引からの不正なデータ再生ではないという妥当な保証が得られる。

10

【0043】

T S Nの蓄積履歴は所定数のT S Nに制限することができる。例えば、システムは特定のカードアカウント番号に対し受信された最新の10個の取引シーケンス番号を蓄積することができる。更に、取引シーケンス番号の検証はリアルタイムで行う必要はない。この検証はシステムが発行者から許可を得ている間に行うことができる。

【0044】

これらの検査の目的は、インターネット加盟店と結託して暗号化されてない取引データを得ることができる犯罪者が正当な取引からデータを不正に再生することを極めて困難にすることにある。

20

【0045】

サービスプロバイダシステムが上述した検証処理を終了したら(取引シーケンス番号検証の例外があり得る)、システムは発行者20に対する許可要求メッセージをフォーマットする。このメッセージは「実」アカウント番号と有効期限を含むが、他のトラックー1データを除外する。システムはアクワイヤラーB I Nを「仮」アクワイヤラーB I Nとして作用する特殊B I Nと置き換える。アクワイヤラーB I Nは、発行者がアクワイヤラーの代わりにサービスプロバイダに応答するように置き換えられる。

【0046】

アクワイヤラーと発行者がインターチェンジフィー(売上交換手数料)を正しく計算するためには、仮アクワイヤラーB I Nは、アクワイヤラーが位置する国又は同一のインターチェンジフィーを出力する他の国或いは地域に対応させるのが好ましい。各国が国と関連する特殊B I Nを有する場合には、サービスプロバイダはアクワイヤラーB I Nをアクワイヤラーの国と関連する特殊B I Nと置き換えることができる。アクワイヤラーの国が国と関連する特殊B I Nを持たない場合には、同一のインターチェンジフィーを生ずる他の国と関連する特殊B I Nを選択することができる。

30

【0047】

サービスプロバイダはデータベースに、アクワイヤラーからの許可要求で受信されたアクワイヤラーリファレンスデータ(以後「原アクワイヤラーリファレンスデータ」という)を格納する。発行者に対する許可メッセージのフォーマットにおいて、サービスプロバイダは原アクワイヤラーリファレンスデータを、仮アクワイヤラーB I Nと、適切な取引タイプインジケータと、サービスプロバイダが原アクワイヤラーリファレンスデータを見つけ出すために使用し得るインデックス値とを含む「仮」アクワイヤラーリファレンスデータと置き換える。

40

【0048】

ドメスティックファシリティが仮アカウント番号取引を処理するとき、このファシリティは上述のように動作する。しかし、このドメスティックファシリティはドメスティック発行者に対する取引のみを処理し、その結果、暗号鍵と当該国に適用されるアカウント番号変換テーブルエントリーを必要とするだけとするのが好ましい。

【0049】

50

許可要求の発行者処理

図4は、本発明の代表的実施例における発行者がサービスプロバイダから又は許可されたドメスティックプロセッシングファシリティから許可要求を受信した後の発行者20とサービスプロバイダ10とアクワイヤラー18との間の通信を示す。

【0050】

発行者20は取引を任意の他の取引と同様に許可する。発行者は許可応答を「仮」アクワイヤラーBINに返送し、これはサービスプロバイダファシリティかサービスプロバイダにより許可されたファシリティのいずれかである。

【0051】

サービスプロバイダ10は発行者からの許可応答を受信すると、アクワイヤラーBINを検査してそれが「仮」アクワイヤラーBINであるか決定する。そうであれば、サービスプロバイダは、許可応答が原フォーマットに「復元」する必要がある仮アカウント番号取引に対応することを決定する。従って、サービスプロバイダは「実」アカウント番号を仮アカウント番号に変換し、原取引内にあったアクワイヤラーリファレンスデータを復元する。次にサービスプロバイダは得られたメッセージを「実」アクワイヤラーに送信し、実アクワイヤラーは取引を通常のごとく処理し、許可応答を加盟店へ通常の方法で送る。加盟店は許可応答に、他の取引の場合のように応答する。

【0052】

決済及び清算 (Settlement and Clearing)

図5は本発明の代表的な実施例における決済や清算のための加盟店16とアクワイヤラー18と、サービスプロバイダ10又は支払いプロセッサ、例えばマスターカードのバンクネットと、発行者20との間の通信の流れを示す。

【0053】

清算メッセージは本質的に許可要求メッセージと同様に処理される。上述したように、(そのBINテーブル内のエントリーのために)アクワイヤラー18は仮アカウント番号を用いて清算メッセージをサービスプロバイダ10又は支払いプロセッサに自動的に送る。このファシリティにて、仮アカウント番号が「実」アカウント番号と置き換えられ、アクワイヤラーBINが「仮」アクワイヤラーBINと置き換えられ、アクワイヤラーリファレンスデータの残部が原アクワイヤラーレファレンスデータを得るためにサービスプロバイダが後で使用するインデックスと置き換えられる。これらの変更を与えられた清算メッセージが「実」カード発行者20に送信され、実カード発行者20が取引を通常の方法で処理する。アクワイヤラーがたまたま発行者でもある場合には、サービスプロバイダは清算された取引をアクワイヤラーに実アカウント番号及び適正な手数料計算と一緒に返送する。

【0054】

例外処理

取引に関するメッセージを発行者からアクワイヤラー又は加盟店に返送する必要があるときは、このメッセージは任意の取引メッセージを通常のごとく処理する発行者により処理される。発行者に知られている取引は「仮」アクワイヤラーBINを含むために、「仮」アクワイヤラーBINが取引メッセージをサービスプロバイダファシリティに送付せしめる。このファシリティにて、「実」アカウント番号が「仮」アカウント番号と置き換えられ、仮アクワイヤラーリファレンスデータが原アクワイヤラーレファレンスデータと置き換えられる。次に取引メッセージはアクワイヤラーに送られ、アクワイヤラーがこのメッセージを他のこのような取引メッセージと同様に処理する。

【0055】

ID用プラスチックカードの発行

場合によっては、カード所有者はインターネットを介してチケットを購入することができるが、カード所有者は、そのチケットが入場を許可するイベント会場に出かけると、そのチケットの正当性を認証するために取引に使用したカードの提示を要求される。

【0056】

このような場合に適応するために、サービスプロバイダは物理的プラスチックカードを発行し、カード所有者に郵送することができ、カード所有者はインターネット用の仮アカウント番号を取得する。これらのカードには「ID専用、取引には無効」と明記される。エンボス加工された符号化アカウント番号は仮アカウント番号であるが、CVC2は「実」支払用カードのものとすることができる。

【0057】

他の方法として、仮アカウント番号を用いてカード所有者を認証する正当な必要性を有する加盟店を（サービスプロバイダに適切な識別及び認証情報を与えることにより）サービスプロバイダに登録することができ、これらの加盟店にはそれらの登録の暗号化証明として秘密鍵又は証明書を付与する。その後、このような加盟店は、仮アカウント番号取引明細のコピーを取引データと「実」アカウント番号を得る加盟店の権利の両方を認証する暗号認証下で供給することにより、「実」アカウント番号をサービスプロバイダファシリティから得ることができる。次にサービスプロバイダは「実」アカウント番号を暗号化された形で加盟店に転送することができるため、カード所有者を「実」アカウント番号に対応するカードで識別することができる。

10

【0058】

本発明はインターネット上での支払いアカウント番号の使用に対し強化されたセキュリティをもたらす利点を提供する。

以上は本発明の原理を説明しているに過ぎない。当業者であれば、ここに明示又は明記されていないが、本発明の原理を具体化し、本発明の精神及び範囲に含まれる種々のシステム及び方法を考案することができる。

20

【図面の簡単な説明】

【図1】 本発明の方法に従って安全支払いアプリケーションをプロバイダからインターネットを介して取得するシステムのブロック図である。

【図2】 本発明の方法を用いて安全支払いをインターネットを介して行う際のカード所有者と加盟店との間の情報の流れを示す図である。

【図3】 本発明の方法におけるアクワイヤラーとサービスプロバイダと発行者との間の情報の流れを示す図である。

【図4】 本発明の方法における発行者とサービスプロバイダとアクワイヤラーとの間の情報の流れを示す図である。

30

【図5】 本発明の方法における決算及び清算用の加盟店とアクワイヤラーとの間の通信の流れを示す図である。

【図 1】

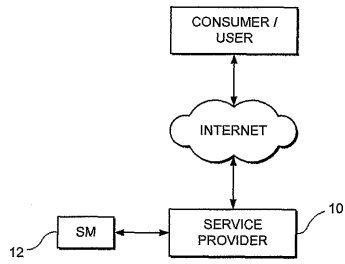


FIG. 1

【図 2】



FIG. 2

【図 3】

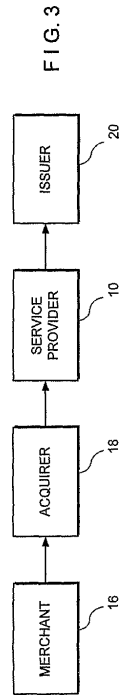


FIG. 5

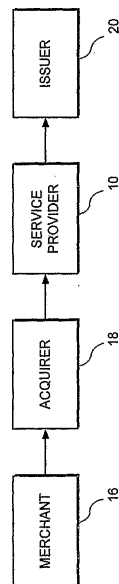
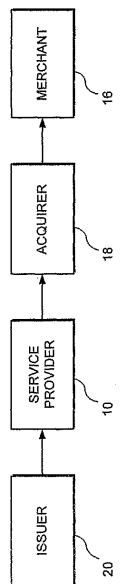


FIG. 4



フロントページの続き

- (72)発明者 エドワード ジェイ ホーガン
アメリカ合衆国 ニューヨーク州 10538 ラーチモント エヌ チャットワース アヴェニ
ュー 14
- (72)発明者 カール エム キャンベル
アメリカ合衆国 ペンシルヴェニア州 19073 ニュートン スクエアー マーリン ロード
809

審査官 阿波 進

- (56)参考文献 米国特許第6000832 (US, A)
国際公開第95/34042 (WO, A1)
国際公開第99/49424 (WO, A1)
国際公開第97/16897 (WO, A1)
VISA INTERNATIONAL ACQUIRER SERVICES, External Interface Specification — Authoriza
tion Record Formats, EIS1080 ver. 5.8, 1999年 4月 1日, [Internet Archive 2000
年8月19日], URL, [http://web.archive.org/web/20000819045331/www.visa.com/nt/suppl
iers/ipgs/zipfiles/authorizationRecords.zip](http://web.archive.org/web/20000819045331/www.visa.com/nt/suppliers/ipgs/zipfiles/authorizationRecords.zip)
- (58)調査した分野(Int.Cl., DB名)
G06Q 20/00