166166

VERIFIED PAYMENT SYSTEM

BACKGROUND OF THE INVENTION

The present invention relates to electronic commerce and, more particularly, to a distributed payment system for implementing secure electronic commerce transactions

THE GLOBAL INTERNET

The Internet, in its widest sense, is becoming the global central nervous system, and is more and more often the medium for all kinds of transaction, from the personal to the multi-national. However, it is both insecure and impracticable to have to exchange primary data, such as data of diverse payment systems, each time that an electronic transaction takes place. At the same time, owners and controllers of data, including corporate, banking, and private entities, must be able to preserve their privacy and to control the mechanisms used for securely identifying themselves in order to:

access their own data;

verify their identity to each other, and

authorize transactions.

All parties to a transaction need an impartial record for the purposes of validation, automation, and reconciliation The present invention solves these problems.

ELECTRONIC COMMERCE

Electronic commerce is becoming more pervasive as the Internet and other communications networks are employed to facilitate consumer/vendor interactions. Beyond networks connecting banks and credit card companies to vendors for use in

electronic funds transfers and point of sale (EFTPOS) payment authorization and authentication, payments systems and transaction authentication systems for diverse and relatively secure electronic commerce (E-commerce) are being implemented globally, including through the Internet. However, such E-commerce and payment systems typically rely on subsequent verification; for example, a credit card user must verify a credit card bill days or weeks after a transaction by examining a credit card statement. No real-time verification over networks is possible using known E-commerce systems without requiring high amounts of network and bandwidth capabilities to authenticate and verify a client contemporaneously with a given E-commerce transaction.

Real-time verification and authentication may be implemented to some degree using a smart card and/or other payment systems such as debit card payments systems, in which clients verify transactions by utilizing their personal debit card at the time and location of the transaction. However, such debit cards generally require pre-loading of funds onto the debit card, which ties up financial resources on non-interest bearing debit cards and which reduces liquidity of the client. In addition, loss or theft of a debit card may be a significant problem for the unfortunate client. In the alternative, by minimizing the amount of pre-loaded financial amounts on a debit card to counter such concerns, the client is restricted as to the size and number of transactions between loading of additional money. This is unsuitable for any commercial transaction above, for example, U.S. $ 500.

Pays et al: "An Intermediation and Payment System Technology" Computer Networks and ISDN Systems, vol. 28, 1996, pages 1197-1206, describes a verified payment-enabling system as out in the preamble to claim 1. Tygar: "Atomicity in Electronic Commerce" Proceedings Of The Fifteenth Annual Acm Symposium On Principles Of Distributed Computing, 23-26 May 1996, pages 8-26, provides background information on electronic commerce and in particular on "Atomicity", that is the linking of logical operations so that either all or none are executed.

Thus, there is a need to provide the parties to a transaction, including both clients and vendors, with flexibility as well as security using real-time verification and authentication, as well as non-repudiation services.

In addition, known electronic commerce systems are unable to readily handle micropayments; that is, payments under a specified threshold, such as less than ten dollars or ten pounds. Micropayments are becoming more pervasive, for example, in downloading snippets of data over the Internet such as image files and icons, as well as service fees for access to on-line resources such as usage fees for accessing a website for information and/or software. In addition to such concerns as verification and authentication, there is a requirement for E-commerce to handle micropayments, and to charge the client with accrued micropayments in a single macro-settlement

A need also exists for an E-commerce system which provides secure and authenticated micropayments

In addition, many business transactions rely on a degree of trust and identification built up after extensive dealings When this level of trust has not been established by a prior relationship, which is increasingly common in the competitive and mobile marketplace, a need exists for enabling a transaction by providing identification, verification, non-repudiation, and payment services to the parties of the transaction.

A need also exists for an E-commerce system which provides secure and authenticated micropayments.

In addition, E-commerce through World Wide Web (WWW) interfaces such as browsers is becoming more popular. However, such browser-based implementations are relatively insecure, for example, in requiring the use of "cookies"; that is, browser information stored on the client's Internet-accessible computer which is known to compromise the privacy and security of the client.

A need exists for an E-commerce system, including Internet-based systems,

which do not rely on a browser and so does not present such concerns of reduced security and privacy concerns for clients

SUMMARY OF THE INVENTION

A trusted third party system and method are disclosed which enable secure electronic transactions across the whole transaction range, from very small to very large sums, accessed from all machines and devices with telecommunications capability, both for immediate or delayed payment settlement and for non-settlement transactions.

A distributed verified payment system (VPS) and method, as the trusted third party system, are disclosed which facilitate E-commerce through real-time authenticated electronic transactions with improved security, non-repudiation evidence, micropayment capabilities, etc. The disclosed VPS implements a dual-key identification authorization system, in which verified instructions must come separately and completely independently from the client and from the vendor before a transaction can be initiated This is not only more secure than taking instructions from one source only, as in a standard EFTPOS transaction, but it also makes it possible to combine flexibility with controlled payment systems Thus, the system acts like a tramtrack switching system, in that the client, the vendor, and their associated payment methods are known and fixed quantities and pre-registered within the authorization manager.

The client may choose the payment or approval method from within such payment or approval methods offered by him/her and accepted by the vendor, after agreeing to the amount and currency specified by the vendor. Approval and/or

payment is then always made within a closed system without either party having access to or knowing the details of the other's payment system Owners of payment systems, such as corporate/purchase cards, may authorize usage by third parties within specified limits, thus enabling them to monitor and control delegated authority.

In addition, real-time audit trails for all parties concerned are implemented by the disclosed system, in which client, vendors, and banks have access to transaction records and may trace transactions and generate reports for such secure transactions. The disclosed system is also software and/or hardware independent, in that the disclosed system may be implemented by any known networking configuration for any known electronic transaction, such as using mobile phones, palm-tops and digital television implementations for purchases and credit/debit payment arrangements for any form of commerce using electronic transactions

In addition, the system supports pre-registration of payment systems by financial institutions to improve the security of the process

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates the disclosed verified payment system;

FIG. 2 illustrates a hub of FIG. 1 in greater detail;

FIG. 3 illustrates a simplified flow diagram of operation of the verified payment system;

FIG. 4 illustrates a more detailed flow diagram of operation of the verified payment system;

FIGS 5-6 illustrate state diagrams for the processing of a transaction,

FIG. 7 illustrates a state diagram for processing to wait for client details; and

FIGS. 8-9 illustrate state diagrams for processing to attempt authorization of a transaction.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring now to FIG. 1, a verified payment system (VPS) 10 and method of operation are disclosed which include an account authority 12 connected through a network 14 to a plurality of distributed hubs 16-20, which function as authorization processors. All clients 22 and vendors 24 are connected to and through an electronic network 26, for example, the Internet, for allowing approvals and/or payments to be made between clients 22 and vendor 24 on a individual, per-transaction basis across the network 14 in a secure, efficient and inexpensive manner.

In the hubs 16-20, client information and vendor information are stored, as shown in FIG. 1, corresponding to respective clients 22 and vendors 24 In alternative and/or additional embodiments, some clients 22 and vendors 24 are respectively connected to the hubs 16-20 through a telephone or other communications system 28 connected to the hubs 16-20 through a gateway capable of processing telephone or other communications, such as cellular telephony. In addition, various entities such as banks 30 and payment system 32 such as credit and/or debit card issuing companies may be connected to local authentication servers 34 and/or gateways to the hubs 16-20 either directly or through the network

14

The network 14 may be a wide area network (WAN), a portion of the Internet, or other electronic network communications mechanisms. Each of the hubs 16-20 may also include or be operatively connected to one or more authentication systems, such as a local authentication server 34, for authenticating the electronic transaction requests registered by each client and each vendor for a given electronic transaction

Each of the hubs 16-20 may be embodied, for example, as shown in FIG. 2, in which communications from the Internet 26 are passed through at least one firewall 36 to a secure hub-internal network 38 having a web farm 40; that is, a plurality of web servers, such as "WINDOWS NT"-based servers, for processing Internet communications such as HTML and HTTP data packets embodying, for example, electronic transactions so that the web farm 40 supports transaction requests and authentication services from other hubs 16-20. The authentication servers 34 may authenticate the payment system details associated with an electronic transaction, such as valid credit card information, and then transmit the electronic transactions data to a bank 30 or other payments systems 32 for further authorization, settlement, and processing

The VPS 10 includes one or more databases maintained, for example, in a "WOLFPACK" SQL database server 42 which holds details on vendors 24, clients 22, and payment systems. The electronic transactions are transmitted through a router 44 and an inter-hub private WAN 14 to other hubs for communications between a client at one hub and a vendor at another hub, or vice versa, and/or for

communications with the account authority 12 to identify the hub which supports a given client or vendor indicating which hub services which client, and to initiate the exchange of data between hubs. Each of the hubs 16-20 provides services to its own respective vendors and clients, and also supports service requests from other hubs for its own clients and vendors; for example, requests for identification and authority. Configuration and management of the services performed by each of the hubs 16-20 may be implemented using the "MICROSOFT LOAD BALANCING SERVICES" technology.

FIG. 3 shows the general operation of the disclosed VPS 10 for use by clients 22 As used herein, the term "client" may refer to any client, customer, consumer, or other entity initiating and/or engaging in transactions from vendors, who may include merchants, sales representatives, wholesalers, retailers, etc Clients 22 utilize a computing device 48, and/or any device 50 with a communications capability to connect to the Internet 26, the telephone system 28, or other communications mechanisms, and thence to contact a merchant and/or vendor 24 electronically for the purposes of establishing an electronic transaction and/or for selecting goods, services, information, or other available materials or electronic goods and information such as archived data, on-line games, video clips, physical goods, etc. The selected materials may be delivered immediately, as in the case of software and/or music uploaded to the consumer's computing device 48, such as a palmtop or digital TV or a telephone 50, or may be delivered by other methods including physical delivery In addition, the selected materials may be on-line games or data which are accessible with usage fees charged concurrent with use.

The VPS 10 does not rely on any particular method of pre-selection of goods, which is always based on some communication directly between vendor and client

In summary, the VPS 10 enables payment of goods and services accessed via electronic mechanisms, including the Internet, mobile/cellular phones, digital TV, etc., following the same basic procedure, without any direct communication necessary between client and vendor. Once a client has selected and agreed to pay for such goods or services, the vendor 24 identifies himself/herself to the system 10, references the transaction, and gives the transaction amount and currency The client also identifies himself/herself to the system 10, chooses one of his/her pre-registered payment systems, and agrees to pay. The identities of both parties are verified, and the selected payment data are married together securely off-line. The transaction is authenticated in real-time via the appropriate banking or other credit gateway, and instructions are sent, if appropriate, for immediate or delayed settlement by the vendor's bank or payment agent The vendor is updated automatically with the authentication result, and an audit trail available to all parties to the transaction is updated. Each transaction is attached to vendor and VPS reference numbers facilitating checking and refunds A plurality of hubs provides resilience and scalability, with each hub providing authorization services to certain vendors and verification and information services on behalf of clients. A central account authority provides registration services indicating which hub services which client.

The vendor 24 requests transaction authorization from its respective hub, such as hub 16. The client 22 also requests payment authorization from the

vendor's hub Upon authentication of both the client 22 and the vendor 24, the corresponding hub associated with one or both of the clients 22 and the vendor 24 acts as the authorization processor to authorize the transaction and/or enables a payment to be made to the vendor 24 by the payment system 32, such as card issuers, banks, or other payment systems such as telephone or electricity companies, which ultimately charge the client 22 for the transaction The VPS 10 can also authorize a transaction without directly causing a payment to be made.

This dual-key transaction for verifying the payment information and client authenticity information provides greater security, in that both sets of information must come separately and completely independently before the transaction is initiated and/or completed.

FIG. 4 shows the transaction process of FIG 3 in greater detail, in which a vendor 24 generates and sends, in step 56, a request to the authorization processor 52, which is a specific hub 16-20 associated with the vendor to authorize the transaction (Tx) This may have been at the request of a client 22 who initiates a transaction in step 54 with a vendor 24. The authorization processor 52 then creates a transaction entry and searches for information about the vendor 24 in step 58, for example, to determine if the vendor 24 is a participant in the VPS 10 If so, the authorization processor 52 obtains the details 60 about the vendor 24 in preparation for payment of the transaction, and returns a message or code, such as a key, which may include a secret, to the vendor identifying the transaction Tx

The client 22 is informed of the transaction key, though not informed of the secret, and uses the transaction key to identify the transaction to the authorization

processor 52 in step 64 The VPS 10 provides a transaction ID and a value such as a "checksum" or a secret key to the vendor 24, and the client 22 may use the transaction ID to identify the transaction, but the VPS 10 and the vendor 24 never inform the client 22 of the secret key, which the VPS 10 includes in any communications with the vendor 24. This reduces the risk of fraud on the part of the client 24.

In an exemplary embodiment, the client 22 may be using a computer 48 and accessing a website of the vendor 24 for selecting goods or services to purchase from the vendor 24, and so in step 62, the vendor 24 redirects the browser of the client 22 to verification and payment selection screens with the transaction key as a parameter of the redirect of the client 22. The interface of the vendor 24 which is provided to the clients 22 may include a website and/or other graphic user interface (GUI) environments, such as a browser using plug-ins and/or scripts to support, for example, Active Server Pages technology and/or Commerce Server Order Processing Pipeline technology associated with "INTEL" and "MICROSOFT WINDOWS", as well as Perl scripts for Unix and/or Apache environments.

Alternatively, using a telephone 50, the client 22 may select goods or services from an automated telephone service of the vendor 24, for example, using a touch-tone telephone and a series of automated audio menus. Accordingly, in step 62, the vendor 24 redirects the client to a payment selection and authorization menu through the telephone 50, or the authorization processor 52 calls back the client 22 to allow the transaction to continue.

The client 22 thus sends a request for payment authorization and/or selection

in step 64 to the authorization processor 52. The authorization processor 52 then checks the authenticity of the client 22 and obtains the payment information corresponding to the client's selection of a payment system in step 66 From step 66, the client's details 68 are obtained and verified, possibly by requesting this service from another hub, and then used for authorizing payment.

Upon receiving both the vendor details 60 and client details 68 and verifying both vendor 24 and client 22, the authorization processor 52 sends an authorization message 70 to a payment system authorization receiving facility 72, and the payment system in turn authorizes the transaction and, in some cases, pays the vendor 24 for the authorized electronic transaction. The authorization processor 52 then informs the vendor 24 in step 74 and informs the client 22 in step 76 that the authorization has been completed, and so payment was initiated, and the vendor 24 then completes the transaction by sending the selected goods or services.

FIG. 5 illustrates a master diagram of the states of a transaction by the overall processing performed by the authorization processor 52 from step 58 of FIG. 4 to get and check the purported vendor to be an authorized vendor and to create a transaction entry, in which the authorization processor 52 generates a temporary transaction entry and then waits for the client details 68 to arrive and to be authenticated, the payment system (PS) authorization to be performed in step 72, and the notification of the respective client 22 and vendor 24.

FIG. 6 is an alternative state diagram of FIG. 5 illustrating transaction table states in a vendor hub, in which the status of the transaction is communicated to the vendor 24 prior to the vendor 24 completing the transaction with the purported

authorized client 22 If the client 22 cannot be authenticated, the vendor 24 is informed of the reasons, and so the request for transaction authorization in step 56 can be rejected. Otherwise, the vendor 24 may perform a fulfillment transaction or a normal transaction to complete the authorized transaction for an authenticated client 22. Other conditions such as refunds may also be handled.

FIG 7 illustrates the processing in FIG. 5 in the Waiting for Client Details state by the authorization processor 52 in step 66 of FIG. 4 to check and authenticate a purported client, in which the authorization processor 52 waits to receive registration information from the purported client Each authorized client has registered previously, so the authorization processor, upon receiving the client details, attempts to match the purported client with one of the authorized clients, and upon a match, obtains the client details 68

FIG. 8 illustrates the processing in FIG 5 in the Attempt Authorization state performed by the authorization processor 52 in steps 64, 66, and 70 of FIG. 4 to authorize a request for payment from the client 22 of FIG. 4 to present payment choices to the client 22, and to process the payment selection, which may be a Normal payment system, that is, a full amount of the transaction is applied to the payment system associated with the client; or which may be a Micropay payment system, that is, transaction charges less than a predetermined amount are accrued and applied latter to the client 22 after the accrued amount exceeds a predetermined threshold, or to reduce an outstanding float which is topped up when the float reaches, for example, zero.

In the case where the client details 68 are stored in a different hub from the

authorization processor, the status of a transaction is partially mirrored in the client hub in order to provide resiliency and a full transaction log available to the client. FIG. 9 shows the transaction table states of a client hub during the processing of a request for client details Such processing includes determining if account limits of a client 22 are exceeded by the client's choice, or if the Micropay transaction is authenticated and is an acceptable payment option between the client 22 and his/her authorized payment systems.

The account authority 12 is used by the Check Client process to identify which hub can provide the required client details

As discussed herein, a vendor 24 is defined as an organization which receives payments through the VPS 10. A client 22 is defined as an individual or corporate entity registered with the VPS 10 for the purpose of enabling transactions and/or paying for goods or services across an electronic network, such as, but not limited to, the Internet. A payment system, such as the payment systems 32, includes any system for making a payment or otherwise authorizing a transaction, such as by a credit/debit card, a direct debit card system, a bank account or access to a particular fund-transfer banking system, a utilities bill or billing account, etc. A receipt system is broadly defined as a system for accepting payment and may include such details as bank account or merchant numbers A payment system owner is a client who owns or holds the payment system

An authorized client is a client authorized to use the payment system by its owner. A client account is defined as the record of the client on the VPS system 10. A hub operator is defined as an organization operating a VPS hub 16-20 as a quasi-

independent supplier of the VPS 10 A financial settlement service is defined as an institution responsible for the actual transfer of funds, such as an acquiring bank for credit cards, but may include other financial institutions

Typically, the payment system owner is the individual holder of a credit card, but a payment system owner may also be an officer of a company holding a corporate credit card or purchase card, or, indeed, the accounts head who controls a billing account payment system. As described herein, an autopay feature is defined as a feature allowing a client to enter a uniquely assigned user name and/or a personal identification number (PIN) only once during a session rather than entering such data for each purchase. The payment system owner may be any individual holder of a payment method, such as a credit card owned by a client, with the holder being a company officer responsible for the payment method, such as an officer, an accounts head, and/or a procurement official of a company holding, for example, a corporate credit card and/or other billing accounts associated with use by the payment method.

Using the disclosed VPS 10, clients 22 are able to make payments to VPS vendors 24 via the Internet 26 or other communications networks The information and details about each client 22 associated with a credit card or other payment system 32 are never transmitted clear across the Internet 26 or other communication network, but instead are only transmitted in encrypted form to allow a client 22 to add or amend his/her account. Alternatively, Internet-based account modification may be avoided by allowing the client 22 to provide credit card details or other payment system details by facsimile or other secure data transmission mechanisms.

In addition, payment system details may be pre-registered by banks or other issues of credit/holders of accounts, allowing increased security in terms of checking delivery addresses against known correct addresses, for example, from the bank, and minimizing the data transmitted across communication channels such as the Internet.

The vendor 24 is never informed of the details of the credit card or other payment system 32 of the client unless such a payment system is managed by the vendor, such as a telephone account. Payments are generally made directly to a given vendor 24 engaged by the client 22 and the client 22 may choose to remain anonymous to the vendor Alternatively, the client may choose to allow the vendor to capture at least or at most the name and address information from a VPS database to minimize data entry and transmission from the client as well as minimizing exposure of the client's information to non-secure systems. In an alternative embodiment, the vendor 24 can send the name, address, and/or other details with the payment request to minimize the data entry required for a new user. The convenience to the client by this option may require the vendor to know when a client is a new user.

In some embodiments of the VPS, the Micropay feature may be implemented, in which very small payments, such as pence or cents may be made without incurring the overhead of a credit card transaction. There are two variants of Micropay: first, when the vendor accepts the risk of a bad debt, and second when the VPS takes an initial deposit and credit against the initial deposit using a pre-authorized automatic crediting and/or debiting payment mechanism. A key feature of the VPS implementation of Micropay is the enablement of multiple currency

payments by providing an automatic conversion to a common currency in the authorization processor.

Optionally, an Autopay feature may be implemented in which, with the client's explicit agreement, the identification process can be set to be transparent after a initial identification during a session involving a client with a specific vendor. Such transparent transaction processing provides a simpler process for a sequence of transactions, while maintaining comparable security.

Access and use of a given payment system 32, such as a credit card system, may be granted by the owner of the payment system to other VPS clients 22. The owner specifies credit restrictions for the authorized client and is able to view all transactions The authorized client is only able to see transactions which that client has instigated.

Clients 22 may be "pre-loaded" by financial settlement services, vendors or companies, such that the pre-loading process creates a set of inactive accounts which the designated client can activate through the use of a personal identification number (PIN) sent separately by the client. Pre-loaded accounts may be subsumed into an existing VPS account by the client, or may be used to create a new account

Vendors 24 may issue refunds through the VPS 10, and clients 22 and vendors 24 may authorize payments to other clients, such that the VPS 10 provides flexibility and adaptability to different marketing and sales methods.

Vendors 24 may choose to provide account facilities to specific clients or groups of clients These account systems may seek payment through a financial settlement service when the account exceeds a certain limit, in a form of Micropay,

or may submit invoices directly to the client. In the latter case, the VPS 10 is principally acting as a trusted accounting system.

Statements to clients 22 and vendors 24 may be available on-line. Other reports for banks 30, payment systems 32, and agents, and for managing the accounts of the organization may also be available.

The VPS 10 is highly secure, both in terms of its basic purpose and in terms of physical, procedural and programmatic access to secure information. In particular, clients 22, payment system owners and/or vendors 24 may stipulate certain minimum levels of security. For example, vendors 24 and/or clients 22 may insist on validation beyond the PIN level of security details before allowing the purchases above a certain amount.

In addition, the VPS 10 may be able to export accounting information, for example, outside the system 10 to an external accounting facility. The accounting information may include the number of normal transactions tallied according to the type of payment system and Micropay turnover to allow an external accounting system to bill the vendors.

The VPS 10 is intended to be as open as possible, for example, to adapt to meet the large potential of such Internet-based payments and E-commerce. The architecture of the VPS 10 allows for as many future options as possible. For example, the VPS 10 and associated payments systems 32 may encompass credit/debit cards, direct debit, in-store accounts, utilities bills and any other form or method for moving money from one place to another. The VPS 10 also performs client identification, for example, by receiving and accepting a simple user name

and password on a secure web connection Alternatively, any other form of identification and verification may be used, including smart cards, digital certificates and signatures, and/or biophysical/biometric-based identification methods. The payment systems 32 and/or the client data may be hosted by other organizations external to the VPS 10.

FEATURES OF THE VERIFIED PAYMENT SYSTEM

The VPS 10 is a value-added authentication and settlement system which is convenient to use and offers unprecedented levels of security. The VPS is a trusted third party system holding details of payment systems belonging to buyers, sellers and providers of credit, in a secure environment, to provide the link between the parties involved in electronic fund transfer or credit account transactions, such as banks and other providers of credit, buyers and sellers The VPS 10 permits these parties to authorize transactions and/or to exchange funds rapidly and efficiently, without disclosure or exposure to risk of sensitive data, and to automate their processes. Also, the VPS 10 provides an impartial, real-time audit trail to all parties - clients, vendors, banks, etc. - of all transactions for which the VPS 10 is the enabling service.

When a client first opens a VPS account on the Internet, the client enters credit card or other payment system details, including bank and credit accounts, through a secure interface to the VPS 10, such as a secure website or other secure data entry mechanisms. The relevant information is passed securely and protected, for example, by SSL encryption via a web server of the VPS 10, or other secure

encryption methods appropriate to the initiating device, to the back office thereof, where the information is held protected, encrypted, and off-line away from the web server Payment systems may be registered with the VPS 10 either off-line or directly by the card issuer or provider of credit, such as a telephone account, a retail store card, a company credit account, etc. VPS account holders, as clients using the VPS 10, may register as many payment systems as they wish in one virtual account, all accessed and controlled by the clients via the same unique ID.

Once the account is opened, the VPS account holder is never required to enter or convey payment card or personal details on the Internet or any other medium, but instead the VPS account holder identifies himself/herself, for example, by a unique user name and password, such as a personal identification number (PIN) plus optional additional security checks. Transactions are mediated via a unique dual key system: codes identifying the merchant, the transaction and the amount are sent from the merchant, while the client identifies himself/herself, chooses the payment system s/he wishes to use for the transaction, and confirms the client's willingness and assent to pay for a selected transaction These two streams of information from both the merchant and the client are coupled together in the authorization server 52 and sent to Payment System Authorization 72 and, if appropriate, across a fast telecommunications link to the merchant's selected payment system such as a bank.

Information about the success or failure of the transaction is then passed back to the Authorization Processor 52, where the success/failure information is recorded and passed on to the both the VPS web server and the merchant's server in

step 74, so that client and merchant can be quickly informed of the result within, for example, within three to seven seconds.

Each transaction is uniquely identifiable via codes assigned by the merchant and by the VPS 10, thus facilitating reference checks, monetary credits, and refunds. An autopay feature allows the client 22 to identify himself/herself only once for all transactions within a single session with a vendor 24, for example, on the respective vendor's website.

Very small payments may be specially processed, in which all payments below a minimum predetermined amount agreed to by each merchant are classed as micropayments and treated separately. Micropayments are part of a seamless service offered to merchants and account holders who use the VPS 10, by which such micropayments accrue and are totaled up until the account holder makes a transaction which causes the accrued sum owing above the threshold of the minimum amount. The VPS 10 then automatically seeks payment for the total of outstanding micropayments plus the new transaction. Merchants using the VPS 10 may thus choose from two payment options. Using the first option, merchants using the VPS 10 may choose to receive payment directly and to allow their clients to purchase goods and services on credit without pre-payment up to an agreed threshold. No payment is debited to the client until the threshold set by that merchant is reached, and the merchant then receives payment for all micro payment transactions as one consolidated sum. This allows the clients to purchase small goods and services incrementally, such as downloading small files of information or programs such as applets, as well as data such as search engine queries.

Using the second option, merchants participate in the general VPS micropayment system, which requires account holders to pay one initial opening deposit, with merchants receiving a consolidated payment, minus card and handling fees, monthly in arrears. The first time that an account holder makes a micro payment transaction from any merchant participating in the general VPS micropayment arrangement, s/he is debited with a pre-payment of the threshold amount, which may be, for example, a minimum of U S. $ 15. She/he can then buy goods and services across the whole range of merchants participating in the micropayment arrangement The client is not charged again until the payment threshold is reached The U.S dollar is normally used as a uniform currency unit for all micro-payment transactions globally Initial floats as the deposit are taken from an account holders' credit card or any other authorized payments system in dollars. Any payments in currencies other than the U S dollar are converted into U.S. dollars before deduction from remaining float funds, with the converted value being displayed to the client along with the original currency amount prior to their acceptance Consolidated funds owing to merchants are assessed in U.S. dollars although such funds may be converted into the merchant's currency of choice before transfer.

Cards and other payment systems and also personal details are registered with the VPS 10 on a VPS secure database 42 in a hub 16 which performs the function of an authorization processor 52, and such details are held securely offline, away from the interface with vendors 24, and so such details are never used or available on-line Account holders can register as many cards and other payment

systems as desired in one virtual wallet, such as payment systems including business and personal accounts paid monthly in arrears, accounts paid by direct debit etc. Such registered payment systems of an account holder are accessed via identity checks, and such card and other payment system details may be pre-registered by the issuer, so that card holders never have to put their card or personal details on-line Such off-line information gathering and retention ensures that addresses are true billing addresses, and so the VPS 10 is enabled to run accurate address checks on behalf of merchants without divulging any account holder information to the merchants.

In accordance with the standard initial operation of the VPS 10, the account holder chooses a unique combination of user name and alpha-numerical password as a PIN, and logs additional security information into the VPS 10 to be used as an identity check at any time thereafter. Random questions based on the additional security information are mandatory for all changes to a client's account, and such questions are optional for transactions and consultation of audit trails. PINs and additional security inputted by an account holder may be always disguised as asterisks or blank spaces onscreen. A prompt mechanism may be provided to help people with short memories. Other forms of identification and verification can be accommodated as deemed appropriate by banks, financial systems, and major users. The account holder also may choose spending limits to self-limit expenditure.

On-line audit trails having, for example, a resolution for time intervals down to the second, including for micropayments, are provided for users and vendors. Accounts can be controlled on-line by the user, so that details of purchases can be

checked and printed out, and personal, security and spending limits can be altered as desired. The account holder is thus in control of all electronic spending, across different banks, cards and websites, from a single online account

Additionally, an owner of a payment system such as the registered holder of a card or such like payment mechanisms may grant rights to use that payment system to other account holders on the VPS 10, which can be operated via the granted account holder's ID, with the charge going to the owner's payment system Spending limits are specified for the owner of the payment system and each grantee. Sub-accounts may also be limited to usage with certain vendors or categories of vendors. Spending limits may be a purely operational safeguard for account holders, while the true limitation on the use of any card or payment system is the credit limit on that card or system. Only the owner of each registered VPS account and sub-account may change details on an account.

All currency conversion is carried out by the normal operation of credit cards, banks, and financial systems. The account holder may therefore be allowed to always pay his/her bill in a selected or preferred currency, such as the currency of the country of the account holder, plus any conversion charges incurred in purchasing goods in a different currency, thus automating and providing security for electronic monetary transactions while providing the advantages of monetary conversion and use in the physical world.

If the account authority 12 detects, for example, three errors in security responses in one attempted transaction, the account may be frozen, and the VPS 10 logs every occurrence of a security error. Furthermore, for example, if the account

authority 12 detect six errors in different transactions in one period of twenty-four hours, the account may also frozen.

The VPS 10 initially uses a combination of user name, password and security checks, as in known telephone-based banking, to identify account holders, such as the use of random questions based on two words and one date. However, the VPS 10 may also be configured to accept other forms of identification and verification, such as digital certificates and signatures, voice recognition, iris recognition, thumb print recognition, and other known methods for authenticating a user accessing the VPS 10 as a purported authorized user. For example, identification via smartcards may be included in the authorization processor 52, and so the VPS 10 can therefore work well with smart card-based systems, providing direct links into account holder credit/debit card accounts, micro payments without pre-payments, online audit trails, etc

For merchants and vendors, the VPS 10 provides all participating merchants with a safe and cost-effective method for collecting payments. Payment may be made directly to merchants via their own banks and merchant numbers. The VPS 10 is designed to enable merchants to build client loyalty and brand recognition by, for example, assuring clients of security and privacy by both client and merchant participating in the VPS 10. Since the VPS 10 supports credit as well as debit operations, the VPS 10 also facilitates cash-based client incentive schemes and diverse kinds of loyalty-generating promotions conducted by the merchants. The VPS 10 may also provide a particular merchant with marketing and client intelligence about the merchant's own clients, sales patterns, and global report,

without divulging the client's details.

To use the VPS 10, a merchant is linked into the VPS 10 via a selection of simple or complex enabling and configuring communications software which suit most standard platforms and web servers Merchants use a set-up installation and configuration of the VPS 10 which may be appropriate to their platform and commerce server. For example, the VPS 10 may be integrated with the "MICROSOFT COMMERCE SERVER SUITE" of software and with any other widely available commerce enabling software. The VPS 10 is a very flexible system, designed to suit individual merchants' requirements and to open up new areas of E-commerce and web commerce, and so the VPS 10 works with clients to produce solutions to fit the commercial needs of each client.

The VPS 10 also fits well into normal bank software and procedures, in which real-time validation is directly integrated with the merchant's own transaction processes, allowing full automation, and so the VPS 10 may be easy to integrate with a merchant's site and should be simple and easy-to-use by clients Merchants receive payment for all standard credit or debit card transactions direct via their own merchant numbers The VPS 10 invoices the merchants for fees, for example, based on a flat fee per transaction, and monthly in arrears Merchants may choose to receive consolidated micropayments by bank transfer, directly to their merchant numbers or via the general VPS micropayment system. In the latter case, the merchants receive payment monthly in arrears minus card fees and VPS handling fees.

Merchants receive immediate notice of payment for each order, with such

notification being integrated as part of the merchant's transaction sequence, thus allowing automation and control over the security of the validation process Full integration with existing systems owned by the merchants and vendors also enables seamless integration with ordering, accounting and other software products.

To participate in the VPS 10 as acceptors of payment by credit or debit card, merchants using credit cards obtain E-commerce-enabled merchant numbers from their acquiring banks The VPS 10 may allocate Terminal ID (TID) numbers to merchants from the range set aside for each bank, and then the VPS 10 informs the bank so that settlement can be made directly to the merchant.

The VPS 10 uses a distributed hub arrangement in order to provide full scalability and optimum performance as a universal and global system Regional hubs 16-20, either single or clustered, guarantee fast reliable worldwide access and redundancy. Hubs are either operated directly by the VPS 10 or as a series of inter-locking joint ventures between the VPS 10 and a hub operator, such as a bank, a group of banks or other clearing houses or financial institutions. Merchants and account holders have one "home hub", as shown in FIG. 1, but VPS accounts may be used worldwide. Standard transactions are authenticated and settled via links between the merchant's hub and the merchant's corresponding bank, while micro-payment transactions may be processed via the account holder's hub.

Safe international direct debits are performed, such that the global banking system can be used to send sums from an account in a bank in one currency zone to an account in a bank in another currency zone. Businesses, merchants, and vendors may acquire funds; that is, receive payment into designated bank accounts, in at

least a core number of major international currencies, and the clients of the banks are able to pay at their end in the full range of currencies. Merchant and vendor companies are informed substantially instantly that expected funds are available and are to be received automatically within a set number of days, as specified by the acquiring bank and/or by regulatory mandates, for example, normally three business days

The VPS 10 supports such functionality to interact globally with vendors, clients, and hubs internationally using, for example credit or corporate purchase cards and other established banking systems and relationships as the medium of exchange. Thus, the VPS provides an automated managed facility for electronic payment/fund transfer, a real-time online audit trail for all parties, controlled payment routes, and a system for supporting multiple currencies. The VPS 10 offers such services by substantially or fully integrating with each vendor's database server. Also, vendors operating within the VPS 10 and receiving funds, for example, via merchant numbers must be approved by the banks which support the VPS 10, and so the VPS 10 is self regulating. Payment systems are registered securely within the VPS 10, with the VPS 10 acting as trusted third party, and are accessed by the use of identification or transaction reference numbers.

The shared payment system provided by the VPS 10 offers a secure and simple method of setting up international direct debit arrangements. The VPS 10 also links directly into the global banking system through individual banks 30 to provide real-time authentication and settlement direct to merchant accounts. However, vendors are never given the details of payment systems and thus cannot

abuse them, since the payment systems can only be used to transfer sums to merchant number accounts held by vendors within the VPS 10.

Credit card systems and other payment systems used exclusively for the transfer of funds from one source to another can be registered within the VPS 10 and locked to this exclusive use, thus providing an entirely secure closed circuit. Although the VPS 10 may operate via the Internet 26, the VPS 10 is not dependent upon the Internet 26, as all key processes performed by the VPS 10 occur off-line. Major clients, managing large fund flows, may choose to communicate with the VPS 10 via dedicated leased lines. In the case of direct debits and closed circuit usage, no sensitive information is ever exchanged via the Internet 26, thus avoiding the need for high level encryption, digital certificates etc. to be used by the VPS 10, which increases the complexity and cost of use of the VPS 10. Accordingly, the VPS 10 provides an extremely simple and safe method to transfer inter-currency commercial sums.

The VPS 10 also provides a universal and globally-expandable system for E-commerce, being a truly distributed system in which one ID allows users and vendors to mediate all transactions via the same globally accessible system, with the hub design provides quick service and back-up facilities. In addition, pre-registered credit cards may be used, so that new on-line registrations and address and personal information checks for each client for each credit card are not necessary. Furthermore, card issuers may open dormant VPS accounts on behalf of their card holders by registering card details plus names and address, as well as temporary PINs and a temporary user names for each account, which may also be generated for

this purpose by the VPS 10. Cardholders may then be given the temporary user name and ID needed to access their VPS account, following usual security procedures

Once the client gives his/her user name and ID, which may be temporary, and verifies his/her identity, through a secure VPS interface, s/he can activate the account and may elect to choose a new user name and PIN, extra ID checks, and a customized spending limit, and optionally to register other details including other payment systems and personal data. Clients may group all of their payment cards together in one account, accessed, for example, by the same security checks

Since basic VPS account information comes directly from the card issuer, such information includes the card billing address, which permits the VPS 10 to initiate and verify an accurate address check at the same time as transaction authentication. Such address checks allow merchants to check that the delivery address given on an order form corresponds to the billing address for the card.

The VPS 10 also operates with clients such that personal identification may be performed without additional hardware or software; that is, no special hardware or software is required by a client to use the VPS 10 The inputs from a client to identify himself/herself and to conduct a transaction with a vendor are not transferred through a web browser, and so there are no electronic wallets, or software such as "JAVA" applets or browser cookies required for operation of the VPS 10 Thus the VPS 10 may be compatible and may interface with all machines with a communications capability.

By not disclosing client information, secure sub-accounts may be

implemented, so that a father can authorize his children to use his credit card up to a fixed amount; a company can authorize a department or individual to use a corporate purchase card within a budget and within purchasing parameters, for example, the use of the account can be tied to specific goods, services, and/or vendors and clients. A supplier can authorize a client company to use a credit account, which can in turn be subdivided among departments and individuals. The account holder can monitor and control all transactions using his/her payment system via an on-line VPS audit trail Users are never given the details of the payment system, such as the card numbers used, or given VPS ID used by the account holder. Clients may have registered payment systems which they do not own but have permission to use and associated with their VPS virtual wallets with their other payment systems. Using VPS virtual wallets, clients may pay for goods and services and to monitor spending, via their own VPS ID. This very flexible system is also the basis for setting up store card accounts and direct debits, including payment of utilities and monthly credit accounts. In this case, the account holder gives the vendor permission to use his payment system, such as a credit card account, to take regular payment for agreed goods and services

OPERATION OF THE VERIFIED PAYMENT SYSTEM

Typically, the VPS 10 uses the following principal data for each client: name; address and contact details; E-mail address; security information such as user name, PIN, security prompts and authorization PIN for bulk loaded accounts; confirmation code such as a code by which a client informs potential fund

transferees to confirm that a user ID is typed correctly; payment systems available, such as credit card details, which may be limited to an arbitrary limit of twenty payment systems per user may be placed, possibly at the user interface (UI) level; a group name, such as the name of a company or family; the account type such as "corporate" or "private"; status information such as a "super" user, account disabled, etc.; client preferences such as anonymous, allow autopay, security levels, preferred payment system, etc.; credit limits for the payment system; vendor specific account information; and a minimum security level.

A client may add themselves to the VPS 10 upon being presented with the VPS 10 as a payment option during or pre-emptive of an on-line purchase. However, for groups, clients may be added by the group owner or a group manager. For groups, some payment systems may be hard coded and inaccessible to non-authorized clients. Clients or groups of clients may also be added through a "batch update" process and activated later by the client using, for example, an authorization PIN delivered separately.

Clients may make changes to their VPS accounts at any time, including user name, PIN, security details, personal credit limits, and type and identify of payment systems. Authorized clients may change their limits down from a maximum set by the account owner, or change their security levels up from the minimum set by the account owner. Clients may also generate and view various reports on their usage of the system. Once an account is deleted, or a user name is changed, the VPS account lies dormant for a predetermined period of, for example, six months before the previous user name can be re-used within the VPS 10.

To manage client accounts, the account administrator may add a new account, disable or enable an account, delete an existing accounting, change and/or view personal, security, and/or payment system details of the client associated with the account, and change and/or view client preferences.

The pre-loading of accounts is a customizable operation, since the data format for account information may be different for each payment system. The accounts may be pre-loaded into a holding table, and the corresponding account owner is notified of the holding table and the status of the pre-loading, for example, by a hardcopy letter to the owner. This notification may include an access code, so that the account owner can access the VPS 10 and use the access code to create a new account using a selected payment system 32, or add a new payment system to the owner's existing VPS account.

As to the vendors 24, the VPS 10 may retain the following principal data about each vendor. name, address; security user name; security PIN; authorizing payment system; bank information such as TID, sort code, and account number for payments; account, client, and transaction details for vendor-specific micropay or billing accounts, security/payment preferences, commission details; contacts; Internet Protocol (IP) Domain; and category of business. Each of the vendors is operatively connected to at least one of the hubs 16-20, which supports the vendor and manages all the transactions with the vendor and transaction-initiating clients. To be set-up, a vendor completes an agreement and provides bank authorization to the VPS 10 for third party TID payments and for a payment system, such as direct payments, or debit or credit cards, which allow fees to be extracted. These payment

systems are accounts in which payment is not made immediately and the vendor accepts the financial risk These payment systems, as deferred payment accounts, are either a set of normal billing accounts for, for example, blue chips or for an accruals-type of micropay account in which payment is only taken when the account reaches a certain level or alternatively after a predetermined time period, such as a month.

At least initially, vendor accounts may be created by VPS staff or agents thereof, although initial details may be entered by the vendor through the Internet and/or the World Wide Web. A payment system is specified by the vendor to allow fees to be extracted. A bank agreement is to be provided to configure the vendor's merchant IDs and TIDs or other payment systems. An attachment or installation kit may be conveyed to the client and/or to the vendor to perform acceptance tests with the VPS 10. The vendor is then ready for operation with the VPS 10.

Vendors may manage themselves in terms basic name and address details, payment preferences, client-based billing accounts, etc. For sensitive or secure items such as bank information, an error in which may cause the VPS 10 to stop working or to post to the wrong account, details are communicated directly and are modified directly by VPS staff.

Specific functionality performed at each vendor's systems may include: change/view trading name or address, personal security information, authorizing payment system, bank and/or TID information, preferences, and billing account client information.

For using the VPS 10, one form of vendor-specific payment methods may

11 SEP 2002

include a type of micropayment facility in which the client's payment system is only debited when a certain total value of transactions are reached Thus the client may have purchased, for example, four or five items over a couple of weeks before his/her card is debited, and/or when the total reaches, for example, U.S. $20 A second form is a "normal" billing account between the vendor and potentially a large client, in which the VPS 10 mediates the transactions and provides billing information to the vendor, but the vendor invoices the client directly The vendor sets a credit limit on the billing account, and such a payment system may be considered to be owned by the vendor and granted to clients, for example, through the agency of authorized clients.

The vendor may choose to pay money to a client, for example, as a reward for loyalty, as a refund, or as a payment of winnings or promotional activities of the vendor. The payment may be on the back of a transaction made earlier, so that the vendor does not need to know the clients details, as enforced by the VPS 10. A transaction code from the vendor is used to identify the client, the credit card or payment system information, and the refund as being performed appropriately. If the credit card is no longer valid, the money equivalent is transferred to an holding account and the client may be notified, for example, via E-mail. The client may then use an interface associated with the vendor and/or with the VPS 10 to specify which payment system is to be credited.

If the client of the credit card or other specified payment system is no longer on the account authority 12 of the VPS 10, the vendor is notified, and the VPS 10 undertakes to mail, send via facsimile, or send via E-mail a notification to the client

and to allow the issue to be resolved directly, but the VPS 10 does not divulge the clients personal details.

For daily settlement, the authorization processor 52 has approved the transaction, but funds are not be transferred until the next batch settlement with the payment system. For deferred fulfillment, the payment has been authorized, but the goods are not ready to ship Settlement is only sought when the vendor informs the VPS 10 that the goods are ready for shipment. Complexities arise if the authorization is lapsed, in which case it must be re-confirmed. For monthly billing, the vendor is informed of the purchases made through the payment system in question on demand This information and/or their own records, are used to create an invoice for that client

For payment on accumulation of enough debt, such as Micropay arrangements, transactions are accumulated until past a specific threshold. At this point a payment system authorization/settlement is attempted for the outstanding amount These transactions may either be through a general Micropay account or other accounts held with or through a vendor-specific holding account for that client in which the vendor takes a financial risk on the transaction.

To initiate an authorized payment, the vendor sends the following information directly to the payment system to allow the purchase request to be corroborated: a transaction code; the transaction amount; the transaction type or preference, such as deferred, immediate, account, Micropay, etc.; and additional security information such as a zip code or other confirmatory information. A transaction payment may also be split across several payment systems of a particular

client, such as U.S. $ 500 on one credit card and U S $ 400 on another credit card to overall charge U.S. $ 900 for the single transaction

If the client has a preferred payment system, then the preferred payment system is chosen automatically unless the transaction is Micropay and the preferred payment system does not support Micropay, or the preferred payment system is not supported by the vendor Normally, the user selects which payment system to be used from a list of available payment systems which are compatible with payment systems supported by a particular vendor.

After either success or failure of a transaction, the client is returned to an appropriate point such as the website where the client was present before initiating the transaction.

Autopay is a feature which may also be supported by the VPS 10 Autopay is a process by which a client merely confirms his/her personal VPS ID once in a session of transaction After the first payment in a session, a series of data transfers, which may optionally include browser-oriented cookies for Internet-based E-commerce, is used to confirm the identity of the client. Such cookies do not include secure information, are deleted on entry into a new session, and have a limited lifetime. Autopay may also time-out if there are too large gaps in time between individual transactions

The VPS 10 may also generate many different reports for different purposes, as described in Table 1. In general, report and statements include dates, vendor and transaction codes, and the sums involved. Such reports only include methods that allow the client to be identified if both a vendor and a client agree to such client

identification according to their preferences.

TABLE 1

Report	Description	Security
vendor statement	A statement of all transactions with a vendor in a given period. This statement can be filtered by credits, payments, deferred fulfillments, etc.	vendor/hub owner
vendor account statement	A statement of all transactions with a vendor on a vendor specific payment system.	vendor/hub owner/payment system owner (client)
client statement	All transactions for a client on all payment systems. Transaction by other clients using those payment systems are not shown.	client/hub owner
hub summary	A summary for a hub of the transactions in that period The purpose of this summary is to aid calculation of commission and similar fees	hub owner/VPS

SECURITY OF THE VERIFIED PAYMENT SYSTEM

Client, vendor and transaction security is provided by having all communications of secure data, such as user IDs, PIN amounts, etc., are, for example, encrypted to a SSL 40 bit level. Transfers of credit cards and other payment system details occur once only from the Client to the VPS 10, and are protected by at least, for example, 40 bit SSL. Additionally, the client has the option of communicating these details separately by facsimile or phone.

Internet security in the VPS 10 may be performed by tracking IP addresses for all transactions. IP addresses for vendors are checked against their domain names. IP addresses for clients are recorded to allow a backtrail in the event of a fraud. If two transactions are attempted by the same client at the same time, the client may optionally be alerted or informed by E-mail, for example, in the event

that the client's user details have been stolen.

Intra-hub security is implemented in a number of levels. At the top level, a supervisor controls the access rights of operators but may not themselves have rights beyond this management function. At least two passwords may be held by different individuals, and lodged with trusted third parties to cover emergency conditions. Details of encryption methods are to be known to the chief technology officer (CTO) of the VPS 10, as well as to any necessary delegates. Such details may be securely lodged externally. All source code supporting security is also password protected. The purpose of this top level of security is to access and manage the inherent security of the VPS 10. In general, users at this top level are restricted to limited areas of the VPS 10.

The second level of security allows management of internal users of the VPS 10. The users at this level and their properties and access privileges can only be changed by top level security people, but the second level users have the ability to grant access to operators of the VPS 10. In addition, these second level users are able to examine and/or generate audit trails as required. The audit trail for an acquiring bank may include all of the credit card details of a client

The third level of security includes normal users and staff of the VPS 10 who have access to client and vendor accounts, typically to amend details, enter credit card information received by fax, and confirm transactions to clients and vendors with appropriate identification. All sensitive data, such as payment system details, are held in the database 42 encrypted to a high level of security.

Inter-hub security is provided such that all communications between the

hubs 16-20 to each other and to the account authority 12 are encrypted to the highest level practicable. Operating system encryption features such as PPTP may be used Hash functions and other one-way functions may be used to increase the scrambling and security.

AUDIT TRAILS

Audit trails are provided for transactions within a hub, and transaction duplications occur when a vendor hub and a client hub are different, since a transaction is in the audit trail at each hub. Audit trails are generally filtered to preserve the privacy of the clients 22. However, an acquiring bank may have the right to audit certain client data of the VPS 10, but only as to transactions concerning authorizations of the bank

THE ACCOUNT AUTHORITY

The account authority 12 functions to prevent duplications of client IDs upon the adding of new clients The list of authorized clients and their client IDs are replicated from the account authority 12 to all hubs 16-20 for performance and resilience purposes. At each step of operation using the account authority 12 and/or the hubs 12-20, the electronic transaction, from request to settlement and consolidation, is treated as a series of "micro transactions". Any system failures provide for the VPS 12 to be brought back up and transactions in a dangerous state can be identified and resolved manually. For example, in a failure during authorization, items passed to the bank for authorization can be determined and checked as to which were received. Similarly, the sending of acceptances or

rejections to a vendor may also be identified in the event of system failure.

For such operational performance, the Microsoft Message Queuing (MSMQ) system may be used for communications between the hubs 16-20, which may guarantee the state of all communications Typically, in one embodiment, around 8 transactions per second per node can be supported on a single ISDN channel, up to 128 transaction per second (tps) on a 1 MB link, which is about 11 million transactions per day At this rate, the costs of a 1 MB pipe are insignificant compared to the benefits in providing such high speed transaction processing

MESSAGE FORMATS

A preferred embodiment of the VPS 10 uses the HTTP "POST" protocol to dispatch service requests, to receive service results, and to permit interaction with vendors and clients. Other embodiments would include message queuing services, DCOM, and so on. The formats of a number of example messages and responses for interfacing with components of the VPS 10 are described herein which form the kernel of the operational side of the VPS 10. In an Internet-based embodiment, post data is Universal Resource Locator (URL) encoded, and may be sent as if the post data were dispatched by a SUBMIT button or icon on a form of a GUI. The AuthorizeTransaction message may be purely intra-hub, while other messages such as CheckLimitsAndGetPSDetails, CheckLimitsAndAuthorizeMicropay, BulkNotification, and TransactionAbandoned may be inter-hub, or may be intra-hub if a client and vendor are on the same hub.

The AuthorizeTransaction message is a packet which is dispatched an authentication server queue, in which a request packet is sent as follows:

Name	Type	Description
Size	Short	Size of the packet (including this word)
Version	Short	Version of packet format. This allows more transparent upgrades of software
Vendor	Long	Identifies Vendor. Only needed for Tx Log.
ClientHub	Short	Hub where the client lives
ClientID	Long	ID of client
OurTxCode	GUID	
VendorTx	Char[20]	
ReceiptSystem	Int	
TxType	Short	Type of transaction Payment, Refund, Authentication
start	Datetime	When the tx was initiated (mainly for log)
CardNo	Char[20]	CardNo
Expiry	Char[4]	MMYY
Start	Char[4]	MMYY
Issue	Char[4]	
Amount	Currency	
Currency	Char[3]	Currency of Tx. Mainly for Txlog
Source	long	ID of machine which initiated the request. In the IP version, used to hold the socket no for writing the response back.

In response, the returned data packet includes the following:

Name	Type	Description
Size	Short	Size of packet
Version	short	Version of format
ResultCode	Short	Result of transaction (success, fail, error)
OurTxCode	GUID	
Our AuthCode	Long	A unique ID IF the transaction was authenticated
ResultCode	short	A code representing the result
Resultdetail	Char[20]	Text returned (authentication code ...)
Timestamp	datetime	When authenticated

The CheckLimitsAndGetPsDetails post is dispatched from a vendor hub to a client hub for the purpose of acquiring Payment System (PS) information for authentication. The client hub, using the ServicePaymentSystemInfoRequests message, checks that the account and payment system limits are not exceeded and

either returns an error or the payment system info. The request packet for the CheckLimitsAndGetPsDetails post includes:

Name	Type	Description
Size	Short	Size of the packet (including this word)
Version	Short	Version of packet format. This allows for more transparent upgrades of software
TxType	short	Payment, refund, micropay ...
VendorHub	Short	Hub Where Vendor is
Vendor	Long	Identifies Vendor. Only needed for Tx Log.
ClientHub	Short	Hub where the client lives
ClientID	Long	ID of client
OurTxCode	GUID	
VendorTxCode	Char[20]	Vendors transaction code
TransactionStartTime	Datetime	When the transaction started
PaymentSystem	Long	Payment System which the Vendor will attempt authorization on
PreviousPS	long	Previous payment system if a repeat attempt
Amount	Money	How much for
Currency	Char[3]	Currency of request
OriginalAmount	Money	What the request was for in original currency (mainly micropay)
OriginalCurrency	Char[3]	Original currency
Return IP	IP	Represents originating machine This will principally be used when we move to asynchronous processing
AddressNo	Long	Address Identification
Index	Short	Indicates if this is the first attempt at authorization or greater.

The corresponding response packet is:

Name	Type	Description
Size	Short	Size of the packet (including this word)
Version	short	Version of packet format. This allows more transparent upgrades of software
OurTxCode	GUID	
ResponseCode	short	ExceedsLimit(type), invalid system, invalid client, has PS details, has address
PaymentSystemDetails	Varchar[100]	May be empty

PaymentSystemID	Long	The same as requested
AddressInfo	Chars .	

The CheckLimitsAndAuthorizeMicroPay post is dispatched from a vendor hub to a client hub for the purpose of authorizing a micropayment. Expected responses are authorized or not The request packet sent is:

Name	type.	Description
Size	Short	Size of the packet (including this word)
Version	short	Version of packet format. This allows more transparent upgrades of software
VendorHub	Short	Hub Where Vendor is
Vendor	long	Identifies Vendor.
ClientHub	Short	Hub where the client lives
ClientID	long	ID of client
OurTxCode	GUID	
VendorTxCode	Char[20]	Vendors transaction code
TransactionStartTime	datetime	When the transaction started
PaymentSystem	Long	Payment System which the Vendor will attempt authorization on
Amount	Money	How much for
Currency	Char[3]	Currency of request
OriginalAmount	Money	How much was actually asked for
OriginalCurrency	Char[3]	And in what currency
Return Queue	Int	Represents originating machine (returning queue name will be based on this number)
AddressNo	Long	Address Identification. Hopefully, this won't happen but if it does... Also may not be relevant for Micropay, but
Index	Short	Indicates if this is the first attempt at authorization or greater.

5

The corresponding response packet is:

Name	Type	Description
Size	Short	Size of the packet (including this word)
Version	short	Version of packet format. This allows more transparent upgrades of software
OurTxCode	GUID	
ResponseCode	short	ExceedsLimit(type), invalid system, invalid client, OK, NOT Authorized,
OurAuthcode	long	If the hub authorizes something, it must uniquely identify it. The Vendor hub will

		have it's own number if appropriate (and a different hub), but can be reconciled in the OurAuthCodes table

The BulkNotification post or put includes any number of batched notifications which indicate that a transaction has been settled, a deferred fulfillment has been cancelled, or the settled transaction has been charged back and post-settlement cancellation is performed. The packet thus has a header indicating version, total size and number of entries in each of the three sections, followed by three sections with details on the items mentioned above The request packet is.

Name	Type	Description
Size	Short	Size of the packet (including this word)
Version	short	Version of packet format. This allows more transparent upgrades of software
SourceHub	Long	The hub the message comes from
NoSettledTransactions	Long	Number of entries in the 'settled transactions' section
NoCancelledDeferred	long	Number of deferred fulfillment Txs which have been cancelled
NoChargeBacks	Long	Number of 'bad' settled transactions
DATA	DATA	Block of data corresponding to the volumes of settled, cancelled and charged back respectively.

The Settled TX format is:

Name	Type	Description
OurTxId	GUID	Transaction that was settled
SettlementBatch	long	BatchNumber of the settlement
SettlementTime	Datetime	When it was settled

The Deferred FulfilmentCancellation format is:

Name	Type	Description
OurTxId	GUID	Transaction that was cancelled
CancellationTime	Datetime	When it was cancelled

The Charge Back format is:

Name	Type	Description
OurTxId	GUID	Transaction that was settled

A TransactionAbandoned packet is used to indicate that a transaction has been abandoned. If a transaction is rejected by the vendor hub's authentication server, the client may try another payment system, which implicitly informs the client hub of the failure, or the hubs may abort the transaction. If they abort, this packet is sent to synchronize the client hub, which only applies if the client and vendor hubs are distinct. If the hubs are the same, the vendor components perform all the writing and the client server components are passive. The request packet is:

Name	Type	Description
Size	Short	Size of the packet (including this word)
Version	Short	Version of packet format. This allows more transparent upgrades of software
OurTxCode	GUID	
ReasonCode	Short	Why we gave up (Client Abort, not authenticated, timeout....

Interfaces to the external world, such as requests from clients and vendors as well as notifications to vendors, are conducted via HTTP posts using SSL. The following requests are supported: Vendor Transaction Start, Vendor Fulfillment Notification, Vendor Credit against Transaction, and Client Transaction Payment Request. The Following notifications to vendors are supported: transaction complete (Aborted, Rejected, Approved), Fulfillment Expiration Notification, and Exception Notification. Each subsection herein identifies the post variables that are required and details the format of the return values possible. Return codes will be plain text, one field per line with a "Name = Value" format. For example:

OurTx=A23452-1234-232

IP=255 255.200.2

XML formatted messages may also be used. Encryption of the contents of the message may also be performed.

The Vendor Transaction Start message is sent by the vendor to indicate that the client wishes to make a purchase. The VPS 10 registers a transaction in a transaction table and returns the transaction code and IP address for future client communication. The parameters may be.

Name	Purpose	Constraints
MESSAGE	Indicates type of Message	"PAYMENT"
VendorTxCode	This identifies the Transaction to the Vendor	20 character max length. Unique for a given Vendor
Description	Free text summary of the products bought	64 characters.
Amount	Total Value of Transaction	Numeric string.
Currency	Currency of Transaction	As used in APACS (GBP, USD ..). Must be a 'supported' currency that may be vendor specific.
Deferred	Indicates that settlement is not to be sought until the vendor requests it (normally due to goods not being in stock)	"Y" or "N". Default is "N" if form variable not present
Micropay	Indicates that a Micropayment Method is required (vendor or client)	"Y" or "N". Default is "N" if form variable not present. Transactions below a certain Payment System Type defined level will ONLY be accepted as

		Micropay.
Zip	Zip Code. For use in reconciling the identity of the client	20 characters Max If this field is present then 'Country' must also be present

Name	Purpose	Constraints
Supply_Address	Indicates that the vendor wishes to receive the name and address of the client. This is performed automatically if the Vendor allows this (though with a note on of the Authorization Pages). It will be ignored if the Client profile demands privacy and the Client will be allowed a choice of canceling the Transaction or providing address details if the flag is "M" mandatory.	"Y", "N", "M" (Yes, No, Mandatory). Default is "N"
Notification_URL	A URL to return future notifications to (for this transaction and while active). Allows the Vendor more control over the organization of their site	A URL (Max 100 chars)

The message then returns

Name	Purpose	Constraints
Status	Indicates that the transaction can proceed or not. Try later indicates a transient system problem or planned downtime...	"OK", "TRY LATER", "MALFORMED REQUEST"
URL	Universal Resource Locator (URL) which the Vendor must use in redirecting the Client Browser	For example, "http://www.vps.com/ContinueTx.asp?VPS_TX=sadgsahjdghjas"
ICE_TX	Unique transaction identifier provided by the VPS 10 for referencing the transaction in later communications	32 chars
VPS_CHECK	A "secret" code not to be conveyed to clients which checks that messages are not generated by the client	4 chars
Reason	Only present if a request is malformed	Text string. Max

	(No Amount, for example). A free format string describing the error.	100 chars

A Vendor Fulfillment Notification message is sent when the vendor wishes to fulfil a deferred fulfillment transaction. The parameters are:

Name	Purpose	Constraints
MESSAGE	Indicates type of Message	"FULFILL TRANSACTION"
ICE_TX	Which transaction is to be fulfilled	20 chars (probably a GUID)
Post_Notify	In some cases we can simply return a code that indicates the state of the transaction (done, dropped). In others, however we must re-seek authorization By default we will provide an immediate return code where possible. However, it may be simpler for the Vendor to only process asynchronous responses.	"Y", "N". default is "N"
Notification_URL	A URL to return future notifications to (for this transaction and while active). Allows the Vendor more control over the organization of their site	IP

The message returns:

Name	Purpose	Constraints
RESULT	The return code indicates that the transaction is accepted, has expired, is not known or will take a little time to process. In this latter case a Transaction Complete Notification will be sent.	"ACCEPT", "EXPIRED", "UNKNOWN", "AUTHORIZING"

A Vendor Credit against Transaction message is sent to instigate a credit against a transaction. The credit may be simply for the purpose of refund or may be intended to pay winnings etc. The parameter are:

Name	Purpose	Constraints
MESSAGE	Indicates type of Message	"CREDIT"
ICE_TX	The transaction against which the credit must be made. This transaction will (indirectly) identify the Client and Payment System to use.	20 chars (probably a GUID)
AMOUNT	The value of the refund	Numeric string. Max 2 decimal places. Max Value 1,000,000.00 Default is the original Transaction amount
CURRENCY	Currency to be paid in	As used in APACS (GBP, USD ...). Must be a 'supported' currency that may be Vendor specific. Defaults to the original currency of Purchase
Notification_URL	URL for notifications to be posted to	URL (Max 100)

The message returns:

Name	Purpose	Constraints
RESULT	The return code indicates that the transaction being processed, is unknown or that the payment system is no longer Valid	"UNKNOWN", "CAN'T PROCESS", "AUTHORIZING"

A Client Transaction Payment Request is generated when the vendor has informed the VPS 10 of a pending request, and the vendor redirects the client, such as the client's browser, to be redirected to the respective hub of the client. The URL address used is specifically the one returned from the Vendor Transaction Start message. The parameters of the Client Transaction Payment Request are:

Name	Purpose	Constraints
ICE_TX	Identifies the transaction to the VPS 10	32 character max length.

The message has no specific return, which depends on the processing which occurs to respond to the request.

The Transaction Complete message is sent to the vendor website, which is specific by either a default URL or the one specified in the initial Transaction Request message, when an active transaction completes normally. The parameters are:

Name	Purpose	Constraints
MESSAGE	Indicates type of Message	"TRANSACTION COMPLETE", "FULFILLMENT COMPLETE", "CREDIT COMPLETE"
VendorTxCode	This identifies the Transaction to the Vendor. If the transaction is a deferred fulfillment or a credit against a transaction, this will be the original ICE Tx code.	20 character max length.
ICE_TX	Our transaction code	20 chars
VPS_CHECK	A "secret" which must match the original "secret" sent to the vendor	
Status	The result of the transaction. The status indicates authorization, rejection, client abort or system failure	"ACCEPT", "REJECT", "ABORT", "FAIL"
Timestamp	Time at which Transaction was accepted, rejected etc.	Date Time (?)

The message returns

Name	Purpose	Constraints
RESULT	Indicates that the Vendor has received the notification. In the case of a "SYSTEM ERROR", the transaction must be backed out.	"OK", "SYSTEM ERROR"
Timestamp	Date time when the Vendor completed	Date Time

	processing.	

A Fulfillment Expiry (or expiration) Notification message is sent to the vendor when a deferred fulfillment transaction passes a sell-by date of the transaction. This message is informational and is resent until a response is received, such as "OK" or "UNKNOWNTX" The parameters are:

Name	Purpose	Constraints
MESSAGE	Indicates type of Message	"FULFILLMENT EXPIRED"
ICE_TX	Identifies the transaction	
Vendor_TX	Their code for the Tx	
Reason	Indicates why the deferred transaction has expired	"TIMEOUT", "USERACCOUNT CANCELLED"
Timestamp	When this happened	

The message returns:

Name	Purpose	Constraints
RESULT	OK or unknown transaction.	"OK", "UNKNOWN TX"

A Status Request message allows the vendor to interrogate the VPS 10 concerning the exact state of a transaction The parameters include a transaction ID of the vendor or the VPS 10, a vendor code, and other information pertaining to the transaction. The message returns the status of the transaction, the amount, commencement time, and the time and nature of last action

By the foregoing, the disclosed verified payment system and method has been disclosed by way of the preferred embodiment However, numerous modifications and substitutions may be had without departing from the spirit of the invention. For example, while the preferred embodiment discusses an Internet-based configuration, it is wholly within the purview of the invention to contemplate primarily telephone-based configurations in the manner as set forth above, such that the disclosed system may be

implemented by any known networking configuration for any known electronic transaction, such as using mobile phones, palm-tops and digital television implementations for purchases and credit/debit payment arrangements for any form of commerce using electronic transactions In addition, the uniform currency used by the VPS 10 may be the British pound sterling, the Euro, the Eurodollar, or any other predetermined currency or monetary/financial denomination. Accordingly, the invention has been described by way of illustration rather than limitation

CLAIMS:

1. A verified payment-enabling system (VPS) (10) to enable all parties to an electronic/digital transaction, including a client (22) and a vendor (24), to mediate secure electronic/digital transactions, the VPS comprising:

a) a trusted third-party registration system enabling the secure, private registration of identification, verification, and payment data by clients, vendors, and payment systems, including banks; and

b) an audit trail generator for generating an audit trail of a respective electronic/digital transaction, with the audit trail being available to all parties of the electronic/digital transaction; and

characterised by:

c) a plurality of hubs (16-20), connected by a private network (14), and connected to the vendor, the client, and a payment system (32), the hubs having means (56, 60; 64, 68) for the vendor and client to separately communicate with the VPS system; and

d) an account authority providing registration services detailing which hub supports which client;

whereby said secure transactions are mediated without direct communications between the parties.

2. A VPS as claimed in claim 1, wherein the VPS (10) implements an autopay feature allowing a client (22) to identify himself/herself only once for all transactions within a single session with a vendor (24).

3. The VPS (10) of claim 1 or 2, wherein verified instructions from the vendor (24) to the client (22) in a respective electronic/digital transaction are separately received by a hub.

4. The VPS (10) of claim 1 or 2, wherein the hubs (16-20) store client and vendor data, including user names, digital certificates, and payments system data, and wherein

the hubs (16-20) prevent private data from being conveyed to the parties of a respective electronic/digital transaction during processing and completion of the electronic/digital transaction as a secured electronic/digital transaction.

5. The VPS (10) of claim 3, wherein each of the plurality of hubs (16-20) includes a respective authorization processor capable of authorizing and/or verifying electronic/digital transactions and/or initiating a payment through a financial institution.

6. The VPS (10) of claim 1 or 2, wherein a set of rights-to-use a respective payment system, including a credit card system, are granted by an owner of the respective payment system to clients of the VPS (10).

7. The VPS (10) of claim 1 or 2, wherein the vendor (24), responsive to authorization of the electronic/digital transaction, directs the client (22) to the authorization processor (12).

8. The VPS (10) of claim 7, wherein the client (22) and the vendor (24) are connected to the plurality of hubs (16-20) through at least one network (26) to initiate and enable the electronic/digital transaction.

9. The VPS (10) of claim 8, wherein the network (26) is one or more telecommunications system such as at least one of the Internet, satellite, cable, cellular, and infra-red communications systems; and

wherein the client (22) makes a transaction with the vendor (24) through an electronic interface.

10. The VPS (10) of claim 1 or 2, wherein the payment systems, including credit and/or debit card systems, can be pre-registered within a secure, universal system by the card issuers or other payment or credit system issuers.

11. The VPS (10) of claim 1 or 2, wherein the payment to complete the electronic/digital transaction is performed using a micropayment arrangement wherein purchases below a predetermined value are debited against a pre-paid credit amount, based on the U.S. dollar, belonging to the customer which is automatically replenished by debiting a pre-arranged payment system.