(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 September 2001 (13.09.2001)

PCT

(10) International Publication Number
WO 01/67307 A1

(51) International Patent Classification[7]: G06F 17/30

(21) International Application Number: PCT/US01/07408

(22) International Filing Date: 8 March 2001 (08.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/521,154 8 March 2000 (08.03.2000) US

(71) Applicant *(for all designated States except US)*: **IC UNIVERSE, INC.** [US/US]; 888 Heartwood Circle, Fruit Heights, UT 84037 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **BIORGE, James** [US/US]; 888 Heartwood Circle, Fruit Heights, UT 84037-2142 (US).

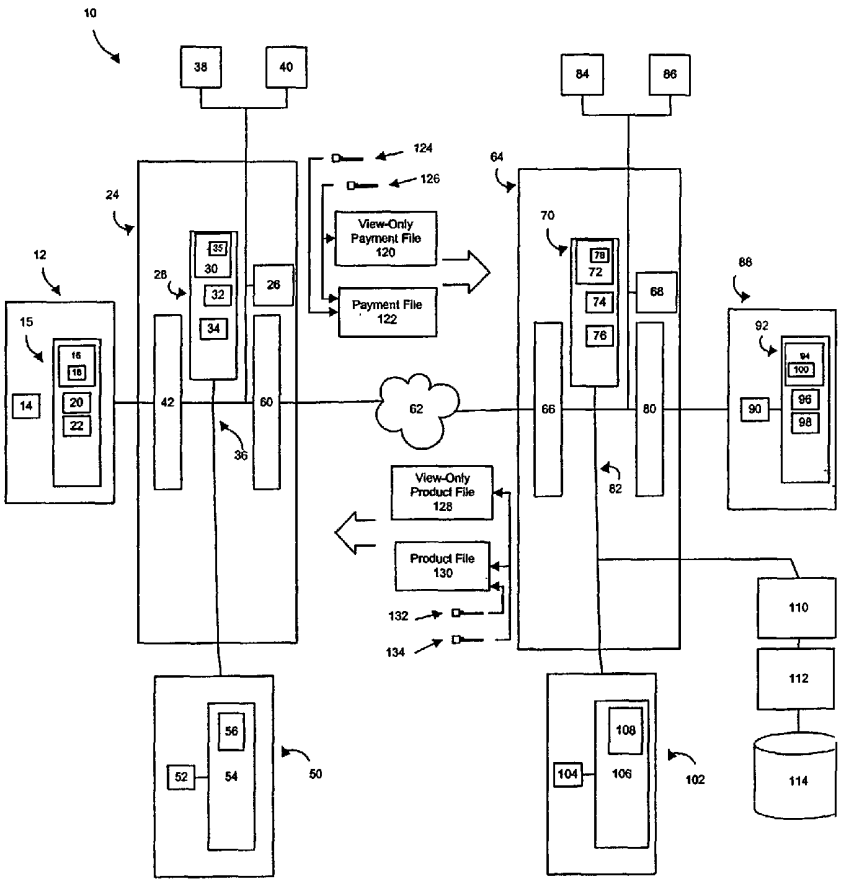
(74) Agent: **THOMPSON, John**; Madson & Metcalf, 15 West South Temple, Suite 900, Salt Lake City, UT 84101 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURED ELECTRONIC TRANSACTIONS



(57) Abstract: The present invention includes a buyer portable device (12) having a value stored thereon, a buyer base device (24), and a buyer provider device (50). A purchase amount is deducted from the buyer portable device and is sent to the buyer provider device. The buyer provider device generates and encrypts a payment file (122) and a view-only payment file (120) which confirms the existence of the payment file. The seller base device (64) transmits the view-only payment file and the payment file to a seller provider device (102). The seller provider device generates and encrypts a product file (130) and a view-only product file (128) which confirms the existence of the product file. The buyer provider device and the seller provider device decrypt the view-only product file and the view-only payment file respectively. Upon approval by the buyer and seller, user keys are exchanged to allow decryption of the product and payment files.

WO 01/67307 A1

IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR SECURED ELECTRONIC TRANSACTIONS

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to electronic transactions and, more specifically, to a system and method for ensuring transmittal of payment and product in transactions.

Relevant Technology

Electronic commerce is an expanding and dynamic form of business which is receiving growing acceptance. Although, the term "electronic commerce" is used loosely, it is frequently associated with transactions which occur over a network, such as the Internet. Internet commerce is attributed with an ever increasing portion of various markets and is a popular method for performing transactions. Numerous merchants have expanded into the Internet market and have noted the advantages in having an electronic presence. These advantages include reducing physical store location expenses and reducing inventory distributions to the various store fronts. Thus, merchants are able to consolidate their inventory in a central location and reduce expenses. Consumers enjoy the convenience in shopping on-line and avoiding crowds, parking, and difficulties in finding products.

Credit and debit card technology readily lends itself to electronic commerce. An account number may be readily transferred over the Internet and verified. Thus, a customer may enter or otherwise use the credit or debit card. Debiting or crediting is frequently performed first by the merchant before the customer receives the product. The customer is therefore at a disadvantage in that the customer has in effect transferred a payment before receiving the product. If the product is not sent or received, or if the product is received in unacceptable condition, the customer must seek recourse from the merchant or from the third party account holder. This is often an unpleasant and inconvenient task and may not remedy the situation to the customer's satisfaction.

Alternatively, the product may first be shipped or otherwise transmitted and then the customer's account may be debited or credited upon receipt. This scenario is unacceptable for merchants who must send products without first having assurances of payment. Thus, transactions which are not performed at store fronts are not simultaneous in that either one party or the other receives their compensation first.

In the information age, products may be embodied and sold as electronic signals, such as executable files, operational data, data structures, and so forth. Thus, the electronic signals may constitute software applications which may be purchased and downloaded. The electronic signals may also constitute various computer readable media such as text, audio, and video files. Such electronic signals are referred to herein collectively as product files. The customer may receive and store the purchased electronic signals on the customer's computer for use.

A common issue in a transaction involving a product file is to ensure that payment for the product file is confirmed before the product is sent. Likewise, it is a concern to ensure that receipt of the product file is verified before payment is sent. Given that the transaction is entirely based on the transfer of electronic signals, one entity may withhold their obligation in the transaction while receiving the benefit. The transfer of electronic signals which constitute payment and product may provide an opportunity for unscrupulous individuals to take advantage of the system.

A further innovation in the arena of electronic commerce is the introduction of processor chip cards or "smart cards." The so-called smart card is capable of processing instruction code and has far more advanced memory capability than the traditional magnetic strip cards. The smart card is able to process and manage transactions for a plurality of accounts stored on the card. The accounts may include debit, credit, and incentive accounts, which may be redeemable for goods and services. The smart card is capable of managing and maintaining running totals of the user's accounts. A smart card user may therefore store multiple accounts on a single smart card and enjoy the security and convenience of the smart card. Furthermore, the smart card may be readily integrated into electronic transaction technology. Given the

benefits of smart card technology, it is anticipated that it will ultimately replace magnetic strip cards.

Thus, it would be advantageous to prepare an electronic transaction system which incorporated smart card technology.

It would be an advancement in the art to provide simultaneous and secured exchanges in electronic transactions.

It would be a further advancement in the art to provide verifiable receipt of product files and payments during an exchange.

It would be yet another advancement in the art to provide a system and method which ensured that both parties accepted payment and product before releasing their owed compensation.

Such a device is disclosed and claimed herein.

SUMMARY OF THE INVENTION

The present invention incorporates a buyer portable device having a value stored thereon and a buyer provider device, in electronic communication with the portable device. The buyer portable device and the buyer provider device are configured to operate in conjunction to generate a view-only payment file and a payment file reflecting an adjustment to the value. A buyer base device is in electrical communication with the buyer portable device and the buyer provider device and is configured to transmit the view-only payment file and the payment file across the network.

A seller base device is also in electrical communication with the network. The invention may further include a seller portable device and seller provider device in electrical communication with the seller base device. The seller base device is configured to receive the view-only payment file and the payment file from the network during a transaction. The seller base device is further configured to transmit a view-only product file and a product file to the buyer base device.

In operation, a buyer accesses the network through the buyer base device. The buyer may then review a seller's site which is hosted on a seller base device. When the buyer may select one or more products on the site to purchase. The

products are capable of being embodied in a computer readable format and therefore may be electronically transmitted. To begin the transaction, the buyer places the buyer portable device in electrical communication with the buyer base device. The buyer base device deducts the purchase amount from the buyer portable device and relays the purchase amount to the buyer provider device.

The buyer provider device generates a payment file which constitutes payment and a view-only payment file which confirms the existence of the purchase amount file. The buyer provider device encrypts the view-only payment file with a buyer system key. The buyer provider device further encrypts the payment file with a buyer user key received from the buyer portable device and the buyer system key. The view-only payment file and the payment file are simultaneously sent to the seller base device.

The seller base device sends the view-only payment file and the payment file to a seller provider device which is in electrical communication with the seller base device. The seller base device retrieves the product and sends it to the seller provider device. The seller provider device generates a view-only product file and a product file. The product file contains the product and is encrypted with a seller user key and a seller system key. The seller user key may be retrieved from a seller portable device in electrical communication with the seller base device. The view-only product file confirms the existence of the product file and is encrypted with the seller system key.

The view-only product file and the product file are simultaneously sent to the buyer base device. The buyer base device then sends the product file and the view-only product file to the buyer provider device.

The buyer provider device and the seller provider device decrypt the view-only product file and the view-only payment file respectively. The buyer and seller are therefore able to confirm that the product file and the payment file are stored locally. Upon approval by the buyer and seller, the buyer and seller user keys are exchanged to allow decryption of the product and payment files. The buyer is then able to utilize the product. The seller may add the value reflected by the payment file to a value stored on the seller portable device.

In this manner transactions may be performed over a network, such as the Internet, that ensure that both parties receive their respective compensation. Payment may be immediately taken from a buyer's account and subsequently added to a seller's account. The product may be made immediately available to the buyer. The provider devices act as an escrow agent to ensure that there is authorization before decrypting and releasing their respective product and payment files.

The invention may also be used with shipment of tangible products. In this situation, the seller base device and the seller provider device are manually carried by the shipping agent. If the product is accepted, the buyer portable device is placed in electrical communication with the seller base device. The buyer user key is then transmitted to the seller provider device. The seller provider device is then able to unlock the payment file. The payment file may then be transferred to a seller portable device in electrical communication with the seller provider device.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other more detailed features of the present invention are more fully disclosed in the following specification, with reference to the accompanying drawings, in which:

Figure 1 is a schematic block diagram of a computer system suitable for implementing one embodiment of the invention;

Figure 2 is a flow diagram illustrating steps performed during operation of the invention;

Figure 3 is a flow diagram illustrating steps performed during operation of the invention;

Figure 4 is a flow diagram illustrating steps performed during operation of the invention;

Figure 5 is a flow diagram illustrating steps performed during operation of the invention; and

Figure 6 is a flow diagram illustrating steps performed during operation of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

A preferred embodiment of the invention is now described with reference to the Figures 1-6, where like reference numbers indicate identical or functionally similar elements. The components of the present invention, as generally described and illustrated in the Figures, may be implemented in a wide variety of configurations. Thus, the following more detailed description of the embodiments of the system and method of the present invention, as represented in the Figures, is not intended to limit the scope of the invention, as claimed, but is merely representative of presently preferred embodiments of the invention.

Various components of the invention are described herein as control programs. In one embodiment, the control programs may be implemented as software, hardware, firmware, or any combination thereof. For example, as used herein, a control program may include any type of computer instruction or computer executable code located within a memory device and/or transmitted as electronic signals over a system bus or network. An identified control program may, for instance, comprise one or more physical or logical blocks of computer instructions, which may be organized as an object, procedure, function, or the like.

Nevertheless, the identified control programs need not be located together, but may comprise disparate instructions stored in different locations, which together implement the described functionality of the control program. Indeed, a control program may comprise a single instruction, or many instructions, and may even be distributed over several different code segments, among different programs, and across several memory devices.

Referring to Figure 1, a schematic block diagram illustrating a computer system 10 of the present system is shown. The system 10 utilizes a buyer portable device 12 having a processor 14 and a memory 15 in electrical communication with one another. The memory 15 may include a read only memory (ROM) 16 having a control program 18 instructed to perform the functions of the present invention. The control program 18 would enable the portable device 12 to perform crypto-processing to encrypt and decrypt data files as required by the invention. The memory 15 may

further include a random access memory (RAM) 20 and a non-volatile memory 22. The RAM 20 serves as a short term memory for temporarily storing operational information. Information stored within the non-volatile memory 22 may include a PIN number or other authorization code as well as a user key 124 for use in encrypting certain data files as will be explained subsequently.

The non-volatile memory 22 may also contain monetary, financial, or incentive accounts reflecting certain amounts of value. Thus, the non-volatile memory 22 may include financial transaction data, credit or debit amounts, incentive credits, and the like as well as information relating to past transactions. The non-volatile memory 22 may therefore contain information sufficient to allow debiting or crediting of an account as would be required in a transaction.

The buyer portable device 12 is of a size and shape which allows a buyer to conveniently carry it in the palm of the buyer's hand. In one embodiment, the portable buyer device 12 may be a processor card or a smart card as it is sometimes referred to in the art. The portable buyer device 12 may be an International Standards Organization (ISO) type "7816 IC card" or it may be a Personal Computer Memory Card International Association (PCMCIA) type card. One of skill in the art will appreciate that the portable buyer device 12 may be embodied in numerous ways given the relative small size of processor and memory chips.

The buyer portable device 12 may be used as a debit or credit card to authorize payment of a transaction amount at the conclusion of a transaction. The buyer portable device 12 may also be used to store a running total of a debit or credit amount. As defined herein the term value refers to a debit or credit amount which may be deducted from or added to as required for the transaction.

The system 10 further comprises a buyer base device 24 which supports the interaction of the buyer portable device 12 with other components of the system 10. The buyer base device 24 further provides the support for completing transactions. The buyer base device 24 comprises a base processor 26 which is in electrical communication with a memory 28 having a ROM 30, RAM 32, and a non-volatile memory 34. The base device 26 further includes a control program 35 stored within

the ROM 30 to enable operation of the base device 26. The control program 35 instructs the processor 26 in operations relating to transactions and interfacing of components required in the system 10.

The memory 28 may be connected to the base processor 26 through a common bus 36. The base device 24 may further include an input device 38 such as a mouse, keyboard, and the like. The base device 24 may further include an output device 40 such as a display monitor, LED display, printer, and the like, to allow buyer interaction with the buyer base device 24.

The base device 24 further includes a portable interaction device 42 to enable electrical communication between the portable buyer device 12 and the base device 24. The portable interaction device 42 may provide communication through actual physical contact with the portable buyer device 42 or through wireless communication such as microwave, radio frequency, or infrared.

The system 10 further includes a buyer provider device 50 which may be embodied as the buyer portable device 12 and placed in electrical communication with the base device 24. Alternatively, the buyer provider device 50 may be embodied as an integrated circuit or microchip which is resident within the base device 24. In any of the embodiments the buyer provider device 50 may be removable to allow updating of the buyer provider device 50 as needed. The provider device 50 may be embodied with a processor 52 and a memory 54 in electrical communication with the processor 52. The memory 54 may be similar or equivalent to that of the base device 24. In one embodiment, the provider device 50 and the base device 24 may actually share memory 28, 54. The memory 54 includes a provider control program 56 to enable the operations of the provider device 50. The provider control program 56 is configured to perform crypto-processing to encrypt and decrypt data files as required by the invention. The provider device 50 serves to provide security with the electronic transactions as will be explained subsequently.

The base device 24 further includes a network interface device 60 to enable communication with a network 62. As defined herein, the network may include a local area network (LAN), wide area network (WAN), a global computer network,

such as the Internet, or a limited access network such as an Intranet. Thus, the term network 62 is used broadly herein to describe any number of electronic communication mediums between various computer stations.

In performing a transaction, the buyer base device 24 accesses a seller base device 64 through the network 62. In one embodiment, the seller base device 64 may be embodied similar or equivalent to the buyer base device 24. The seller base device 64 would therefore have a network interface device 66, a processor 68, and a memory 70. The memory 70 may include a ROM 72, a RAM 74, and a non-volatile memory 76. The ROM 72 may have stored thereon a seller control program 78. The seller base device 64 may further include a portable device interface 80 and a bus 76 to provide electrical communication for the components. The seller base device 64 may further include input and output devices 84, 86 to enable interaction with a seller.

The system 10 may further comprise a seller portable device 88 embodied as the buyer portable device 12 and having a processor 90 in electrical communication with a memory 92. The memory 92 may include a ROM 94, RAM 96, and non-volatile memory 98. The memory 92 may have a control program 100, stored in the ROM 94 to effect operation of the seller portable device 88. The control program 100 is configured to perform crypto-processing to encrypt and decrypt data files as required by the invention. The system 10 further includes a seller provider device 102 which may be physically resident on the seller device 64 or may be placed in electrical communication with the seller device 64. The seller provider device 102 may be embodied as the buyer provider device 50 with a processor 104 in electrical communication with a memory 106. The memory 106 includes a provider control program 108 to enable the operations of the seller provider device 102. As with the buyer provider device 50, the control program 100 is configured to perform crypto-processing to encrypt and decrypt data files as required by the invention. The seller provider device 102 may also encrypt data stored in the seller base device 64 to provide additional security for the buyer.

In one embodiment, the seller portable device 88 may be replaced with a system to accommodate numerous buyers and numerous products. In such an

embodiment, the seller base device 64 is in electrical communication with a database interface 110. The database interface 110 provides a gateway to the seller base device 64. The database interface 110 would further be in electrical communication with a database manager 112. The database manager 112 may be resident on a mainframe computer and is configured to perform operations such as those performed by the seller portable device 88. The database manager 112 is further in electrical communication with a database 114. The database 114 may provide numerous addressable datasets wherein product files are stored. The database manager 112 would perform encryption of the product files and decryption of the payment files as explained subsequently. Electronic payments for the products may be stored on the database 114.

In yet another embodiment, the system 10 would comprise both the seller portable device 88 and the database 114. The seller portable device 88 may be used to perform the various functions relating to encryption of the product file and decrypting and storing the payment. The database interface 110, the database manager 112, and the database 114 provide storage, management, and accessing of product files. Thus, a transaction involves retrieving the product file from the database 114 and uploading the payment to the seller portable device 88.

During a transaction the system generates a view-only payment file 120 and a payment file 122. The view-only payment file 120 and the payment file 122 are sent from the buyer base device 24 to the seller base device 64. In one embodiment, the payment file 122 is encrypted with a buyer user key 124. The view-only payment file 120 and the payment file 122 may also be encrypted with a buyer system key 126.

The system 10 further generates a view-only product file 128 and a product file 130. The view-only product file 128 and the product file 130 are sent from the seller base device 64 across the network 62 to the buyer base device 24. In one embodiment, the product file 130 is encrypted with a seller user key 132. The view-only product file 128 and the product file 130 may also be encrypted with a system key 126.

Referring now to Figure 2 and with continuing reference to Figure 1, a flow diagram 200 is shown illustrating steps performed from the perspective of a buyer. The objective is to complete an electronic transaction over the network 62 which insures that both the buyer and seller receive their compensation in the transaction.

In step 202, the process begins.

In step 204, a buyer enters a request to purchase a product. At this time it is contemplated that the buyer base device 24 is in electrical communication with the seller base device 64 over the network 62. The buyer base device 24 may be downloading documents reflecting products available for purchase through a conventional browser or through other network communication means. The products available for sale may be displayed on the output device 40. Upon entering a request through the input device 38 to purchase a product, the process continues to step 206.

In step 206, the purchase amount is stored in the memory 28 of the buyer base device 24. The buyer base device 24 then requests the purchase amount from the buyer portable device 12. The buyer portable device 12 verifies that there is sufficient value stored in the non-volatile memory 22 to perform the transaction. As previously stated, value may reflect a certain amount of credits, debits, incentive points, and so forth available for the transaction. If there is sufficient value stored in the buyer portable device 12, then the process continues to steps 208 and 210.

Steps 208 and 210 are performed simultaneously. In step 208, a view-only payment file 120 may be generated by the buyer provider device 50 or the buyer base device 24. The view-only payment file 120 is a data file which verifies the existence of a payment file 122. The payment file 122 is a reflection of an actual payment amount which is taken from the value stored on the buyer portable device 12. Thus, the payment file 122 may be a reflection of added credit or subtracted debit which adjusts the amount of value on the buyer portable device 12.

The view-only payment file 120 is generated only if there is sufficient value on the buyer portable device 12 and upon creation of a payment file 122. The view-only payment file 120 is sent to the buyer provider device 50 wherein it is encrypted through known cryptology methods. In one embodiment, the view-only payment file

120 is encrypted using a buyer system key 126. As defined herein, a system key is a key which is available to users of the system 10 described herein. The system key may be stored on the provider device 50 or on the buyer portable device 12. It is anticipated that the seller will have access to the buyer system key 126 to decrypt the view-only payment file 120.

In step 210, the payment file 122 is generated by adjusting the value on the buyer portable device 12. The payment file 122 reflects an actual payment for a product to be received. The payment file 122 may be sent to the buyer provider device 50 where it is encrypted using a buyer user key 124. As defined herein a user key is one which is associated with a transacting party and more specifically to a portable device used by the transacting party. Therefore, a user key remains confidential to the party and is not freely disseminated to transacting members of the system 10. The buyer user key 124 may be stored on the buyer portable device 12 and then sent to the buyer provider device 50. Alternatively, the payment file 122 may be encrypted by the buyer portable device 12 using the buyer user key 124.

The payment file 122 is further encrypted by the buyer provider device 50 with the buyer system key 126. Thus, encryption of the payment file 122 is a two step process which involves encryption by a buyer user key 124 and then encryption by a buyer system key 126. Decryption of the payment file 122 requires both the buyer system and user keys 124, 126.

Upon generation and encryption of the view-only payment file 120 and the payment file 122, both files are sent across the network 62 to the seller. In one embodiment, the view-only payment file 120 and payment file 122 are batched together. The view-only payment file 120 and the payment file 122 may also be encrypted by the buyer provider device 50 together using the buyer system key 126. It is preferred to transmit the view-only payment file 120 and the payment file 122 together as the view-only payment file 120 confirms the location and existence of the payment file 122.

In step 212, the seller base device 64 receives the view-only payment file 120. The view-only payment file 120 is temporarily stored in the memory 70. The view-

only payment file 120 is sent to the seller provider device 102 and is decrypted through the use of the buyer system key 126. The buyer system key 126 may be stored in the seller provider device 102. It is anticipated that users of the system 10 will have access to the system keys as required to open view-only files. Thus, the use of the system keys serves to prevent non-users of the system from accessing view-only payment files 120.

Once decrypted, the view-only payment file 120 may be sent to the seller base device 64. The seller may open the view-only payment file 120 to confirm that the buyer has sent the payment file 122 and to confirm the amount of the payment. The decrypted view-only payment file 120 may be displayed on the output device 86. If the seller approves the amount of the payment, the process continues to step 214. Otherwise, the process returns to step 204 wherein the buyer enters another purchase request.

In step 214, the payment file 122 is sent to the seller base device 64 and subsequently sent to the seller provider device 102. The seller provider device 102 stores the payment file 122 in the memory 106. The payment file 122 reflects actual payment for the transaction. Thus, the seller provider device 102 provides security for the temporary holding of the payment.

In step 216, the seller is assured of having received the payment file 122 by having viewed the view-only payment file 120. The seller base device 64 accesses the seller portable device 88 or the database manager 112 to verify the existence of the product. The seller portable device 88, the database manager 112, or the seller provider device 102 generates a view-only product file 128. The view-only product file 128 may be sent to the seller provider device 102 wherein it is encrypted with a seller system key 134. The seller system key 134 may be stored on the seller portable device 88 or on the seller provider device102. The view-only product file 128 is a reflection of a product file 130 and confirms the existence and transmittal of the product file 130.

A product file 130 is a product that the buyer is ultimately transacting to purchase. The product file 130 may constitute executable or operational data. Thus,

the product file 130 may include any number of software applications or various media such as text documents, songs, recordings, movies and so forth stored in an electronic format.

In step 216, the product file 130 is generated by accessing the computer readable medium wherein the product is stored. The product file 130 reflects the product and may therefore be a copy of the computer readable product. The product file 130 may be generated by the seller portable device 88, the database manager 112, or the seller provider device 102. Preferably, the product file 130 is not generated or stored in a decrypted format on the seller base device 64. The seller base device 64 is exposed to the network 62. Therefore, if a hacker were to break through a firewall on the seller base device 64 the hacker may be able to access the product file 130 without authorization. Once encrypted, the product file 130 may be stored in the seller base device memory 70.

The product file 130 is sent to the seller provider device 102 where it is temporarily stored. The seller provider device 102 requests and receives the seller user key 132 which, in one embodiment, is stored in the seller portable device 88. The product file 130 is then encrypted by the seller provider device 102 with the seller user key 132. The product file 130 may further be encrypted by the seller provider device 102 with the seller system key 134. The view-only product file 128 and the product file 130 are then transmitted simultaneously to the buyer base device 24.

In step 218, the view-only product file 128 and the product file 130 are received in the buyer base device 24. The view-only product file 128 and the product file 130 are sent to the buyer provider device 50 and stored in memory 54. The buyer provider device 50 decrypts the view-only product file 128 with the seller system key 134. The seller system key 134 may have been stored in the buyer portable device 12 or in the buyer provider device 50. Once again, it is anticipated that users of the system 10 will have access to the system keys 126, 134 discussed herein.

The product file 130 is stored in the memory 54 of the buyer provider device 50. The buyer is able to confirm receipt of the product file 130 by displaying the view-only product file 128 on the output device 40. If the buyer accepts the product

based on the view-only product file 128, then the buyer enters an authorization to transfer the buyer user key 124 to the seller base device 64. The process continues to step 218. If the buyer does not accept the product, the process continues to step 224.

In step 220, the buyer base device 24 confirms receipt of the seller user key 132 based on an acceptance by the seller of the payment file 122. The seller user key 132 may be stored in the buyer provider device 50 or in the buyer portable device 12. In step 220, the seller base device 64 confirms receipt of the buyer user key 124 which is similarly stored in the seller provider device 102 or in the seller portable device 88. If the buyer and seller user keys 124, 132 are not transmitted then the process continues to step 224.

In step 222, the buyer base device 24 receives a confirmation from the seller base device 64 that the buyer user key 124 was received. This confirmation is passed to the buyer provider device 50 or the buyer portable device 12 which has the seller user key 132. The seller user key 132 is then released and the buyer provider device 50 decrypts the product file 130. The product file 130 may then be transferred to the buyer portable device 12, buyer base device 24, or stored in any other suitable computer medium. If the buyer is unable to decrypt the product file 130 then the process continues to step 224.

In step 224, the transaction is aborted because the product or payment file 130, 122 was not accepted, the user keys 124, 132 were not transmitted, or the product or payment file 130, 122 did not open. In such an event, any adjustments made to the value stored on the buyer portable device 12 are reversed to reflect the amount of value prior to the aborted transaction. The process then continues to step 204.

In step 226, the process terminates reflecting the end of a completed transaction.

Referring to Figure 3, a flow diagram 300 illustrating the process of performing a transaction in accordance with the present invention is shown relative to the seller's perspective. In step 302, the process beings. In step 304, a purchase request has been entered by the buyer and this request is transferred to the seller base device 64.

The process continues to steps 306 and 308 which are performed simultaneously. In step 306, the view-only payment file 120 is transmitted over the network 62 and received at the seller base device 64. The seller base device 64 sends the view-only payment file 120 to the seller provider device 102. The seller provider device 102 decrypts the view-only payment file 120 with a buyer system key 126. The buyer system key 126 may be retrieved from the seller portable device 88 or may be resident on the seller provider device 102. Once decrypted, the seller may display the view-only payment file 120 on the output device 80.

In step 308, the payment file 122 is received by the seller base device 64 and stored in the seller provider device 92. The payment file 122 is thus stored until a confirmation is received that the buyer has received the product file 130.

In step 310, the seller determines whether or not the payment amount is acceptable based on an evaluation of the view-only payment file 120. It is preferable that the view-only payment file 120 and the payment file 122 be transmitted to the seller base device 64 together to ensure that both files are received and present. Thus, the view-only payment file 120 serves as verification of the existence and receipt of the payment file 122. If the payment amount is acceptable, the process continues to steps 312 and 314.

In step 312, the view-only product file 128 may be generated by the seller base device 64 or by the seller portable device 88, the seller provider device 102, the database manager 112, or a combination thereof. The view-only product file 128 is encrypted with a seller system key 134 prior to transmission. In one embodiment, the view-only product file 128 is sent to the seller provider device 102 where it is encrypted with a seller system key 134. Thus encrypted, the view-only product file 128 is sent to the buyer base device 24.

Step 314 is executed simultaneously with step 312. In step 314, the product file 130 is retrieved from the seller portable device 88, the database 114, or other computer readable memory in electrical communication with the seller base device 64. As previously mentioned, the product file 130 is a module representing the product that the buyer is purchasing. The product file 130 is sent to the seller provider

device 102 where it is encrypted using a seller user key 132. The seller user key 132 may be stored on the seller portable device 88 and sent to the seller provider device 102 for encryption. After encryption, the product file 130 is transmitted to the buyer base device 24.

In step 316, a query is made as to whether the buyer has accepted the product. Acceptance of the product is based on the buyer's examination of the view-only product file 128. If the product is acceptable to the buyer, the buyer portable device 12 releases the buyer user key 124 to the buyer base device 24. The buyer base device 24 transmits the buyer user key 124 to the seller base device 64. Upon receipt, the buyer user key 124 is stored in the seller provider device 102. Simultaneously, the seller may be reviewing the view-only payment file 120 to determine if the payment is acceptable. If so, the seller authorizes the seller portable device 88 to release the seller user key 132. The seller user key 132 is sent to the seller base device 64 which then sends the seller user key 132 to the buyer base device 24. If the product is not accepted by the buyer, the process returns to step 304 wherein the buyer may select another product.

In step 318, a decision is made to determine if the buyer user key 124 and the seller user key 132 have been exchanged. A confirmation may be sent by the buyer base device 24 to confirm receipt of the seller user key 132. If the user keys 124, 132 have been exchanged, then the process continues to step 320. Otherwise the transaction is aborted and the process returns to step 304 wherein the buyer may select a product.

In step 320, the buyer provider device 50 unlocks the product file 130 with the seller user key 132. At approximately the same time, the seller provider device 102 may unlock the payment file122 with the buyer user key 124. If the buyer provider device 50 is unable to open the product file 130, then the transaction is aborted and the process returns to step 304.

If the buyer provider device 50 is able to open the product file 130, then the opened product file 130 is sent to the buyer base device 24. The buyer is then able to access and use the product file 130. A confirmation that the buyer has opened the

product file 130 may be sent to the seller base device 64. The process further continues to step 322.

In step 322, the buyer has opened the product file 130. The seller provider device 102 similarly opens the payment file 122 using the buyer user and system keys 124, 126. The payment file 122 is sent to the seller base device 64. The seller base device 64 transfers the payment file 122 to a computer readable medium such as the seller portable device 88. The value represented by the payment file 122 may then added to a value stored on the nonvolatile memory 98 of the seller portable device 88. The value may be in the form of currency, credit, incentive points, or various other forms of incremental value. Alternatively, the payment file 122 may be sent to the database manager 112. The database manager 112 then adds the value represented by the payment file 122 to an addressable data segment in the database 114. In this manner, the seller may be compensated in the transaction.

In step 324, the transaction is completed and the process terminates.

Referring to Figures 4, 5, 6 a flow diagram 400 representing an overview of one method of performing the present invention is shown. In step 402, the process begins. In step 404, the buyer accesses the network 62 through the use of the buyer base device 24. In one embodiment, the buyer base device 24 may be embodied as a computer station and the network 62 may be embodied as the Internet. The buyer base device 24 may be continuously linked to the network 62 or the buyer base device 24 may log onto the network 62 as required.

In step 406, the buyer accesses the seller base device 64 across the network 62. In one embodiment, this may be accomplished by accessing a seller's website on the Internet. As such, the buyer may use a conventional web browser to retrieve the HTML documentation reflecting the seller's website. The seller's website may be hosted on the seller base device 64.

In step 408, the buyer decides to perform a transaction. This may be based on a product which the buyer sees listed on the seller's site. The buyer may enter one or more products that the buyer wishes to purchase. The products are those which may be stored and transmitted in an electronic format. Thus, the products may be software

applications or electronic forms of media such as audio, text, video and so forth.

In step 410, the buyer has selected one or more products to purchase. The buyer base device 24 returns with a request to insert the buyer portable device 12 into the interface device 42 so that the buyer base device 24 and the buyer portable device 12 are in electrical communication. The buyer portable device 12 is used to transfer payment for the transaction and for encryption of the payment file 122.

In step 412, the buyer base device 24 and the buyer portable device 12 generate and send encrypted signals between one another. The encrypted signals are used for security purposes to confirm that the devices 12, 24 are legitimate for use with one another. The encrypted signals further confirms that the buyer portable device 12 is compatible for use with the buyer base device 24.

In step 414, the buyer portable device 12 and the buyer base device 24 receive their respective encrypted signals. The encrypted signals are decrypted. In one embodiment, encryption and decryption may be based on a buyer system key 126 which is accessible by various devices of the system.

In step 416, a determination is made as to whether the buyer portable device 12 is a legitimate and compatible device. This determination is made based on the encrypted signals received by the buyer base device 24. In one embodiment, this determination may also be made by requiring the buyer to enter an authorization code, such as a PIN, into the input device 38. Through the use of an authorization code, the buyer base device 24 may determine if the buyer is a legitimate owner of the buyer portable device 12. If the buyer portable device 12 is not valid or if the authorization code is not correct, then the process returns to step 410. A prompt is then sent to request another buyer portable device 12. If the buyer portable device 12 is valid and the authorization code is correct, then the process continues to step 418.

In step 418, the buyer base device 24 accesses the buyer portable device 12 to determine the accounts that are stored on the buyer portable device 12. The buyer portable device 12 may contain a plurality of accounts including debit, credit, and incentive accounts. These accounts contain value which may be debited or credited as

required to complete the transaction. These accounts may be listed and displayed by an identifier on the output device 40.

In step 420, the buyer selects an account which will be used in the transaction to purchase the selected product.

In step 422, the buyer portable device 12 sends the appropriate key to unlock the selected account file. The accounts are locked to prevent unauthorized access and tampering with values in the accounts. Transmittal of a key may be based on the buyer entering an appropriate account number in the input device 38. If the key is not sent to the buyer base device 24, then the process returns to step 418 wherein the buyer selects another account. Otherwise, the process continues to step 424.

In step 424, the buyer base device 24 determines if there is value in the account for the transaction. This decision may determine if there is sufficient value in the account to purchase the selected product. If there is sufficient value, the process continues to step 426, otherwise the process returns to step 418 wherein the buyer selects another account.

In step 426, the value in the account is adjusted to reflect a payment amount. With a credit account the value is added and in a debit account the value is deducted is common practice.

In step 428, the view-only payment file 120 is generated and encrypted with a buyer system key 126 as previously described. In one embodiment, the generation of the view-only payment file 120 may be performed by the buyer portable device 12, the buyer provider device 50, or a combination thereof. The view-only payment file 120 is sent to the buyer provider device 50 where it is encrypted using a buyer system key 126. The view-only payment file 120 confirms the existence, amount of value, and presence of the payment file 122. However, the view-only payment file 120 does not actually constitute value.

In step 430, the payment file 122 is generated by the buyer portable device 12, the buyer provider device 50, or a combination thereof. The payment file 122 is further encrypted with buyer system and user keys 124, 126 as previously described. The payment file 122 is a reflection of the purchase price of the product and is derived

from the value in the selected account. The payment file 122 may be temporarily stored in the buyer provider device 50.

In step 432, the view-only payment file 120 and the payment file 122 are sent by the buyer base device 24 over the network 62 to the seller base device 64. In one embodiment, the view-only payment file 120 and the payment file 122 are batched together to ensure that they are jointly received. The view-only payment file 120 and payment file 122 may further be encrypted together with the buyer system key 126.

In step 434, the seller base device 64 receives the view-only payment file 120 and the payment file 122. The view-only payment file 120 and the payment file 122 may be received batched and encrypted together.

In step 436, the view-only payment file 120 and the payment file are stored in the seller provider device 102. The seller provider device 102 decrypts the view-only payment file 120 and the payment file 122 with the buyer system key 126. The buyer system key 126 may be stored on the seller provider device 102 or retrieved from the seller portable device 88. After decryption with the buyer system key 126, the seller provider device 102 stores the payment file 122 in its memory 96 and sends the now decrypted view-only payment file 120 to the seller base device 64.

In step 438, the seller accepts the value represented by the view-only payment file 120. Acceptance may be automated and performed by the seller base device 64 provided that the value satisfies the purchase price. Alternatively, the seller base device 64 may display the value on the output device 86 and the seller may manually enter an acceptance. If the value is not sufficient, the process returns to step 406 wherein the buyer returns to the seller's site. If the value is sufficient, the process continues to step 440.

In step 440, the product file 130 is accessed from a computer readable medium, such as the seller portable device 88 or the database 114. The seller portable device 88, the seller provider device, or these devices acting in conjunction generate a view-only product file 128 which confirms the identity and presence of the product file 130. The view-only product file 128 is sent to the seller provider device 102 wherein it is encrypted with the seller system key.

In step 442, the product file 130 is sent to the seller provider device 102. The product file 130 may be an electronic copy of the product stored in a computer readable medium. The seller provider device 102 encrypts the product file 130 using the seller user key 132 and the seller system key 134. In one embodiment, the view-only product file 128 and the product file 130 are batched together and jointly encrypted with the seller system key 134. The seller user key 132 may be retrieved from the seller portable device 88. In this manner, aspects relating to encryption may be performed by the seller provider device 102.

In step 444, the view-only product file 128 and the product file 130 are sent by the seller base device 64 via the network 62 to the buyer base device 24. The buyer base device 24 receives these files and, in one embodiment, sends them to the buyer provider device 50 for temporary storage.

In step 446, the view-only product file 128 is decrypted by the buyer provider device 50 using the seller system key 134. The view-only product file 128 and the product file 130 may be simultaneously decrypted using the seller system key 134. The decrypted view-only product file128 is sent to the buyer base device 24. The view-only product file 128 may be displayed on the output device 40. The buyer may then verify that the product file 130 has been received and is stored in the buyer provider device 50. If the buyer accepts the product based on the examination of the view-only product file 128, then the process continues to step 448. Otherwise, the process returns to step 406.

In step 448, the product file 130 and the payment file 122 are in the buyer provider device 50 and the seller provider device 102 respectively. The buyer provider device 50 and the seller provider device 102 may send confirmation of the receipt of the product file 130 and the payment file 122 to each other. The buyer base device 24 and the seller base device 64 may further send confirmation of acceptance of the product and payment files 122, 130 to one another.

The buyer provider device 50 then sends the buyer user key 124 to the seller base device 64 which in turn sends the buyer user key 124 to the seller provider device 92. Similarly, the seller provider device 102 sends the seller user key 132 to

the buyer base device 24 which in turn sends the seller user key 132 to the buyer provider device 50.

In step 450, the buyer provider device 50 decrypts the product file 130 with the seller user key 132. The product file 130 is then sent to the buyer base device 24 where it is accessible to the buyer. The seller provider device 102 decrypts the payment file 122 with the buyer user key 124. The payment file 122 is then sent to the seller base device 64 where it is accessible to the seller. After decryption, the buyer provider device 50 may delete the seller user key 132 and the seller provider device 92 may delete the buyer user key 124. In this manner, security of the buyer and user keys may be maintained.

In step 452, the payment file 122 may be sent to the seller portable device 88 or to the database 114. The value represented by the payment file 122 may then be added to an account in the seller portable device 88 or in the database 114.

In step 454, the transaction is complete and the process terminates.

The present invention provides a system and method to ensure that the buyer and seller receive their respective product and payment. From the buyer's side of operations, the invention requires the communication of the buyer portable device 12 which contains value and the buyer user key 124. The invention further requires the buyer provider device 50 which performs the encryption and decryption of the data files. Similarly, the invention requires a seller portable device 88 or database 114 having a seller user key 132 and a product. A seller provider device 102 is also required to perform the encryption and decryption of the data files. The buyer base device 24 and the seller base device 64 provides support for the transactions and interfacing with the network 62.

The portable devices 12, 88 provider devices 50, 102, and system and user keys 124, 126, 132, 134 operate in conjunction to prevent fraudulent transactions and unauthorized use. It is anticipated that the buyer base device 24, the buyer portable device 12, and the buyer provider device 50 operate in conjunction with buyer user and system keys 124, 126 to perform the functions of the invention from the buyer's

side. The absence of one of these components, or their equivalent, would prevent operation of the invention.

Of course, one of skill in the art will appreciate that variations on the present invention are possible and are included within the scope of the invention. For example, where the seller is embodied as a large entity, a seller portable device 88 is impractical to accommodate the magnitude of transactions that may be required. Therefore a database management system 110, 112, 114 configured for large scale operations is introduced as an alternative embodiment.

It is contemplated by the present invention that variations may be made on the location of the user and system keys and the devices which perform the encryption and decryption. For example, the seller user key 132 may be stored on the buyer portable device 12 and the buyer user key 124 may be stored on the seller portable device 88. The provider devices 50, 102 may then request the user keys 124, 132 for decryption. The system keys 126, 134 may also be stored on the portable devices 12, 88. The portable devices 12, 88 may further perform one or more of the encryption or decryption processes.

As the base devices 24, 64 are subject to hacker intrusions, it is preferable that no decrypted files are stored on the base devices 24, 64. Thus, the base devices 24, 64 do not perform encryption or decryption. The system and user keys 124, 126, 132, 134 are also not stored in the base devices 24, 64. Transactions may be performed in a network environment without intrusions into sensitive information on the buyer devices 24, 64. Account information is stored in the base devices 24, 64 only in an encrypted format to thereby thwart attempts to retrieve this information. The present invention ensures that product and payment delivery are completed in a secure fashion and further maintains the integrity of the transaction.

In an alternative method, the buyer base device 24 may interact with the database interface 110, database manager 112, and the database 114 to perform the transaction of the present invention. In such a method, the database 114 may store the product files 130 and accounts reflecting value. Thus, the database 114 may provide storage similar to that provided by the seller portable device 88. The database

manager 112 may be configured to interact with the database 114 to retrieve the required product files 130 and manage the accounts. This is advantageous where there are numerous products to offer or numerous accounts and transactions to manage. The incorporation of a database 114 or even a plurality of databases 114 enables scalability which may be required in an Internet environment. The database manager 112 may be further configured to perform the functions of the seller base device 64 and the seller provider device 102. The database interface 110 provides the gateway to the network 62 for transactions.

In this manner transactions may be performed over a network, such as the Internet, which ensures that both parties receive their respective compensation. Payment may be immediately taken from a buyer's account and subsequently added to a seller's account. The product may be made immediately available to the buyer. The provider devices act as an escrow agent to ensure that there is authorization before decrypting and releasing their respective product and payment files 130, 122.

Tangible products may also be purchased using aspects of the present invention. Such methods would require that the merchant or agent deliver the tangible product and manually provide a seller base device 64 and a seller provider device 102 in electrical communication with one another. The buyer portable device 12 may interface with the seller base device 64 and therefore eliminate the need for the network 62 or the seller base device 64. The buyer portable device 12 would transfer an amount of value stored therein to the seller base device 64.

The value may be encrypted by the buyer portable device 12 using the buyer user key. The buyer portable device 12 transfers the buyer user key 124 upon confirmation from the buyer. The buyer user key 124 is sent to the seller base device 64 and then sent to the seller provider device 102. The seller provider device 102 decrypts the payment file 122 with the buyer user key 124. The payment file 122 may then be transferred and stored as desired by the seller.

As a point-of-sale operation would not involve a network, certain components are not required. Specifically, buyer and seller system keys 126, 134 are not required because the tangible product may be examined. A seller user key 132 is also not

required as the tangible product is not encrypted. A buyer base device 24 is also not required as the buyer portable device may interface directly with the seller base device 64.

The present invention may be embodied in other specific forms without departing from its scope or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed and desired to be secured by United States Letters Patent is:

Claims

1. A system for performing a transaction over a network, the system comprising:

a buyer portable device having a value stored thereon;

a buyer provider device, in electrical communication with the portable device, the buyer portable device and the buyer provider device configured to operate in conjunction to generate a view-only payment file and a payment file reflecting an adjustment to the value;

a buyer base device in electrical communication with the buyer portable device and the buyer provider device and configured to transmit the view-only payment file and the payment file via the network; and

a seller base device configured to receive the view-only payment file and the payment file from the network, and configured to transmit a view-only product file and a product file to the buyer base device via the network.

2. The system of claim 1 wherein the view-only payment file is encrypted with a buyer system key prior to transmitting the view-only payment file via the network.

3. The system of claim 1 wherein the buyer portable device has stored thereon a buyer user key and the payment file is encrypted with the user key and a buyer system key.

4. The system of claim 3 wherein the buyer portable device is configured to effect transmission of the buyer user key to the seller base device.

5. The system of claim 1 wherein the view-only product file is encrypted with a seller system key.

6. The system of claim 1 wherein the product file is encrypted with a seller system key and a seller user key.

7. The system of claim 6 further comprising a seller portable device in electrical communication with the seller base device and having stored thereon a seller user key, the seller portable device configured to effect transmission of the user key to the buyer base device.

8. The system of claim 6 further comprising a seller provider device in electrical communication with the base device and configured to encrypt the product file.

9. A method for transacting over a network, the method comprising:

storing a value on a buyer portable device;

generating a view-only payment file and a payment file reflecting a payment;

adjusting the value on the buyer portable device to reflect the generation of the payment file;

encrypting the payment file with a buyer user key;

transmitting the view-only payment file and the payment file via the network to a seller;

receiving a view-only product file and a product file via the network from the seller; and

transmitting the buyer user key across the network to the seller.

10. The method of claim 9 further comprising, storing the buyer user key on the buyer portable device.

11. The method of claim 9 further comprising, encrypting the view-only payment file with a buyer system key prior to transmitting the view-only payment file via the network.

12. The method of claim 9 wherein encrypting the payment file with the user key further comprises encrypting the payment file with a buyer system key.

13. The method of claim 9 further comprising, receiving the view-only payment file and the payment file in a seller base device.

14. The method of claim 9 further comprising, encrypting the view-only product file with a seller system key.

15. The method of claim 14 wherein encrypting the view-only product file is performed by a seller provider device.

16. The method of claim 9 further comprising, encrypting the product file with a seller system key and a seller user key.

17. The method of claim 16 wherein encrypting the product file is performed by a seller provider device.

18. The method of claim 16 further comprising, storing the seller user key on a seller portable device, the seller portable device configured to effect transmission of the user key via the network.

19. The method of claim 9 further comprising opening the view-only product file to confirm receipt of the product file.

20. A computer readable medium having stored thereon computer executable instructions for performing a method for transacting over the network, the method comprising:

generating a view-only payment file and a payment file reflecting a payment;

receiving a buyer user key stored on a buyer portable device;

adjusting a value stored on the buyer portable device to reflect the payment;

encrypting the payment file with a buyer user key;

transmitting the view-only payment file and the payment file via the network to a seller;

receiving a view-only product file and a product file via the network from the seller; and

transmitting the buyer user key across the network to the seller.

21. The computer readable medium of claim 20 wherein the method further comprises, encrypting the view-only payment file with a buyer system key prior to transmitting the view-only payment file via the network.

22. The computer readable medium of claim 20 wherein encrypting the payment file with the user key further comprises encrypting the payment file with a buyer system key.

23. The computer readable medium of claim 20 wherein the method further comprises, encrypting the view-only product file with a seller system key.

24. The computer readable medium of claim 20 further comprising, encrypting the product file with a seller system key and a seller user key.

25. The computer readable medium of claim 24 further comprising, receiving the seller user key from a seller portable device.

26. A method for performing a transaction, the method comprising:

storing a buyer value on a buyer portable device;

interfacing the buyer portable device with a seller base device;

generating a payment file reflecting a payment;

adjusting the buyer value on the buyer portable device to reflect the generation of the payment file;

encrypting the payment file with a buyer user key;

transmitting the payment file to the seller base device;

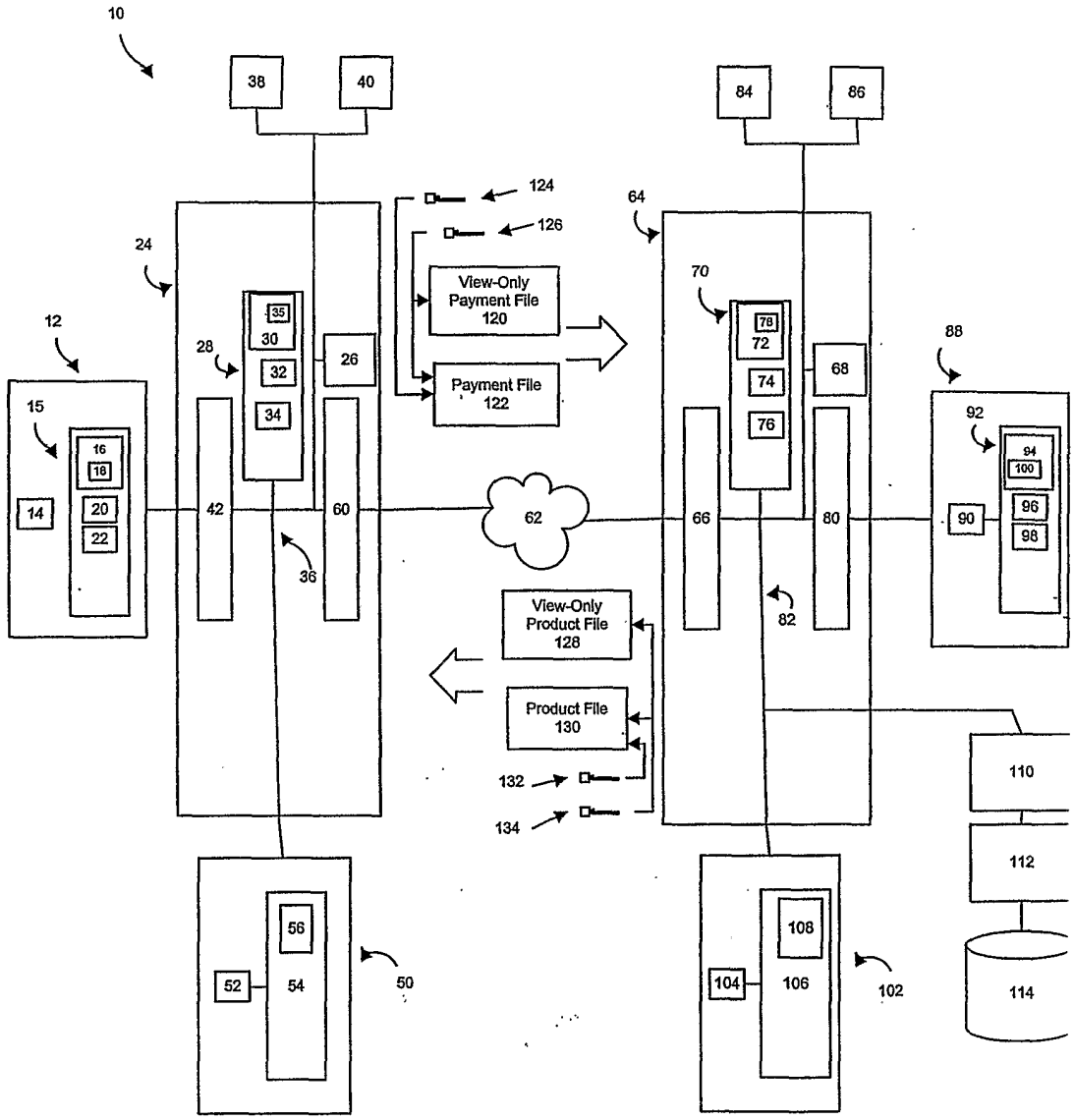
transmitting the buyer user key to the seller base device; and

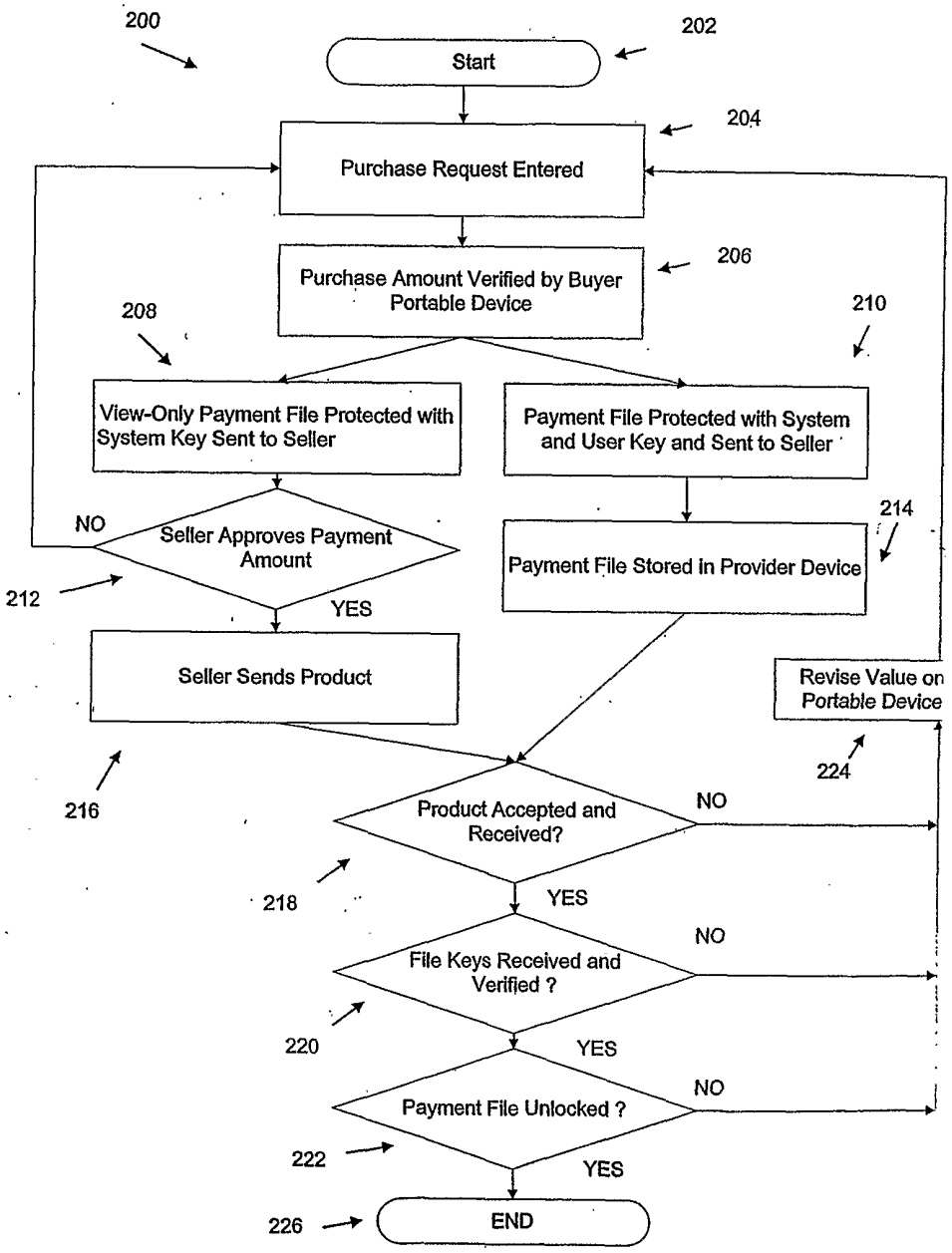
decrypting the payment file.

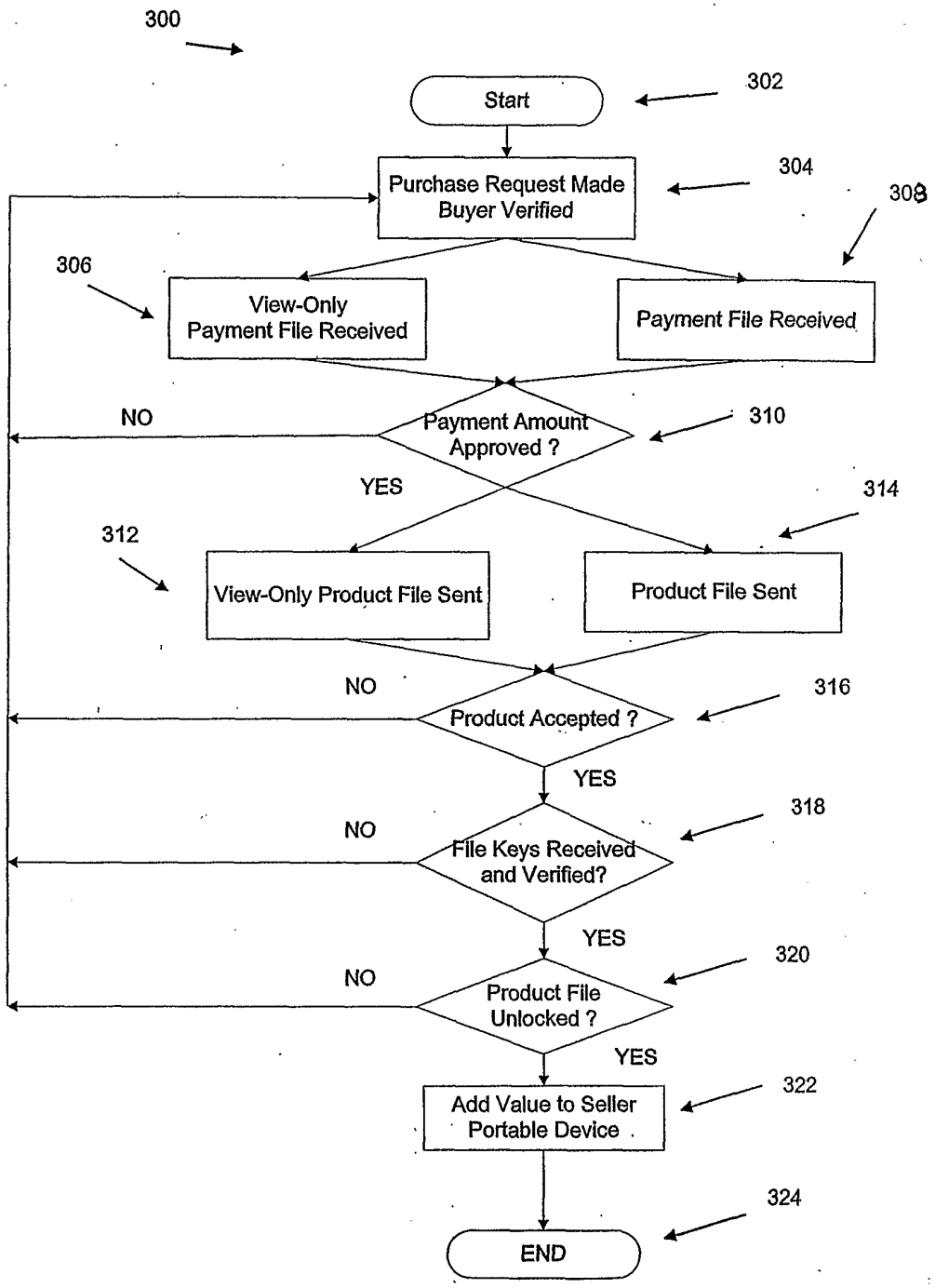
27. The method of claim 26 further comprising sending the payment file and the buyer user key to a seller provider device in electrical communication with the seller base device.

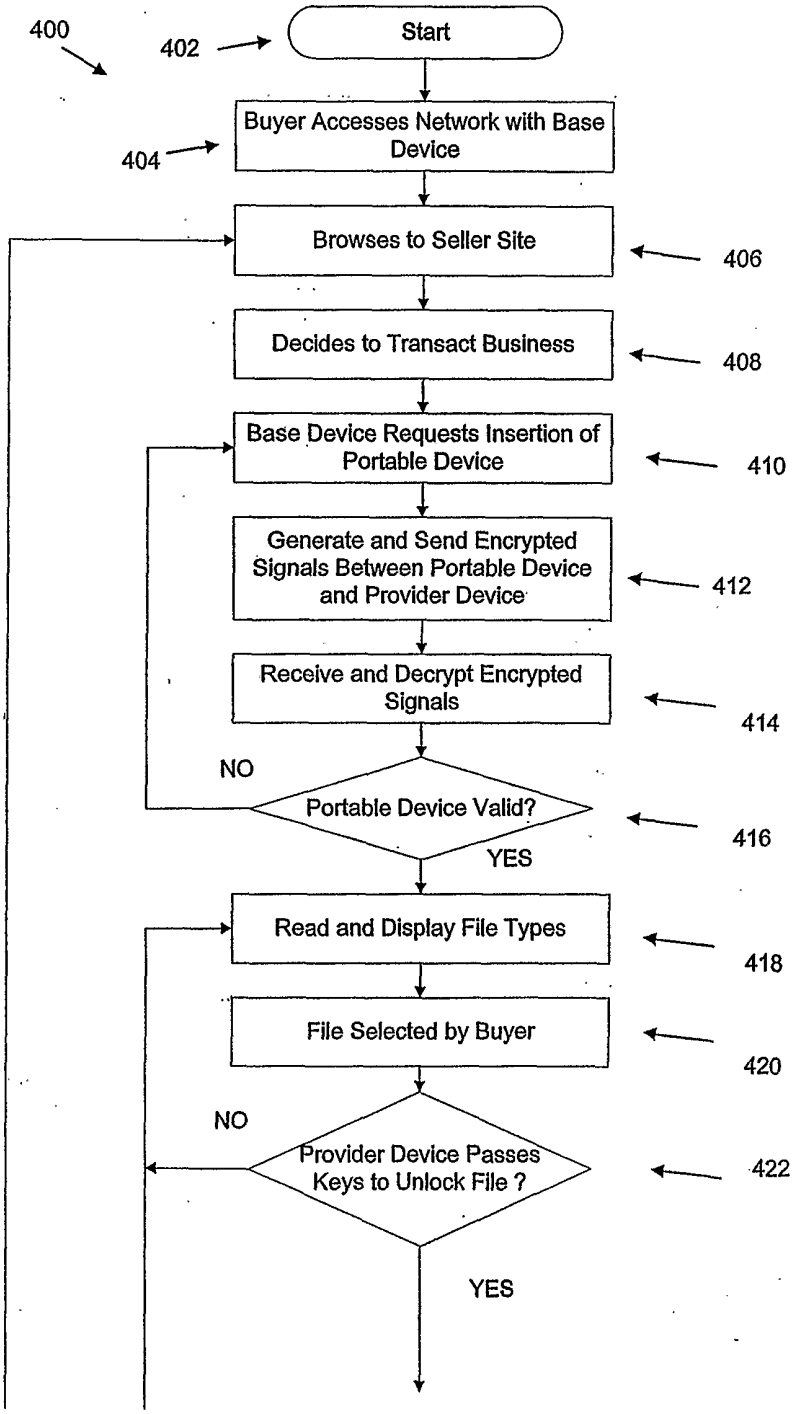
28. The method of claim 27 wherein decrypting the payment file is performed by the seller provider device.

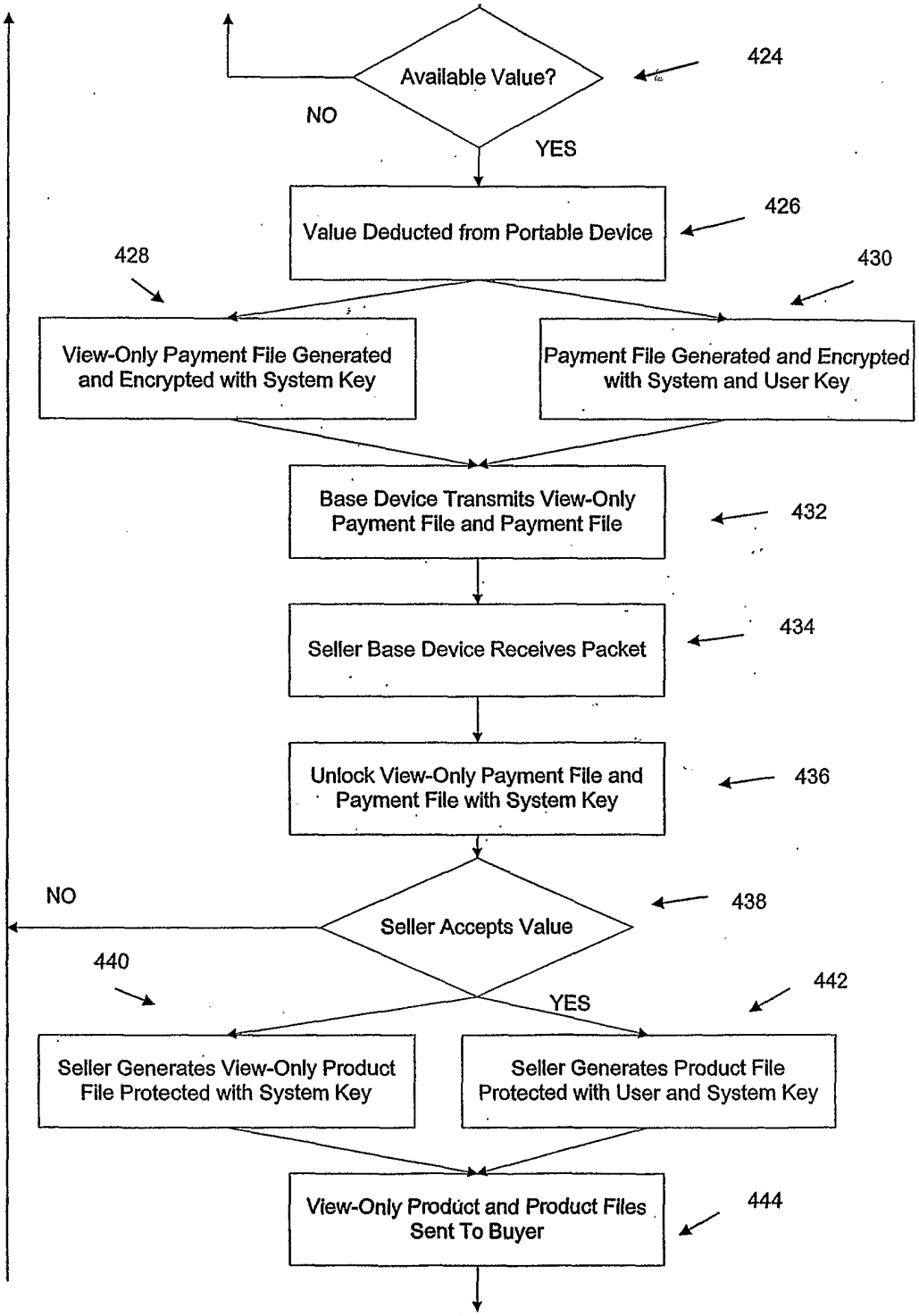
29. The method of claim 26 further comprising adjusting a seller value to reflect the addition of the payment file.

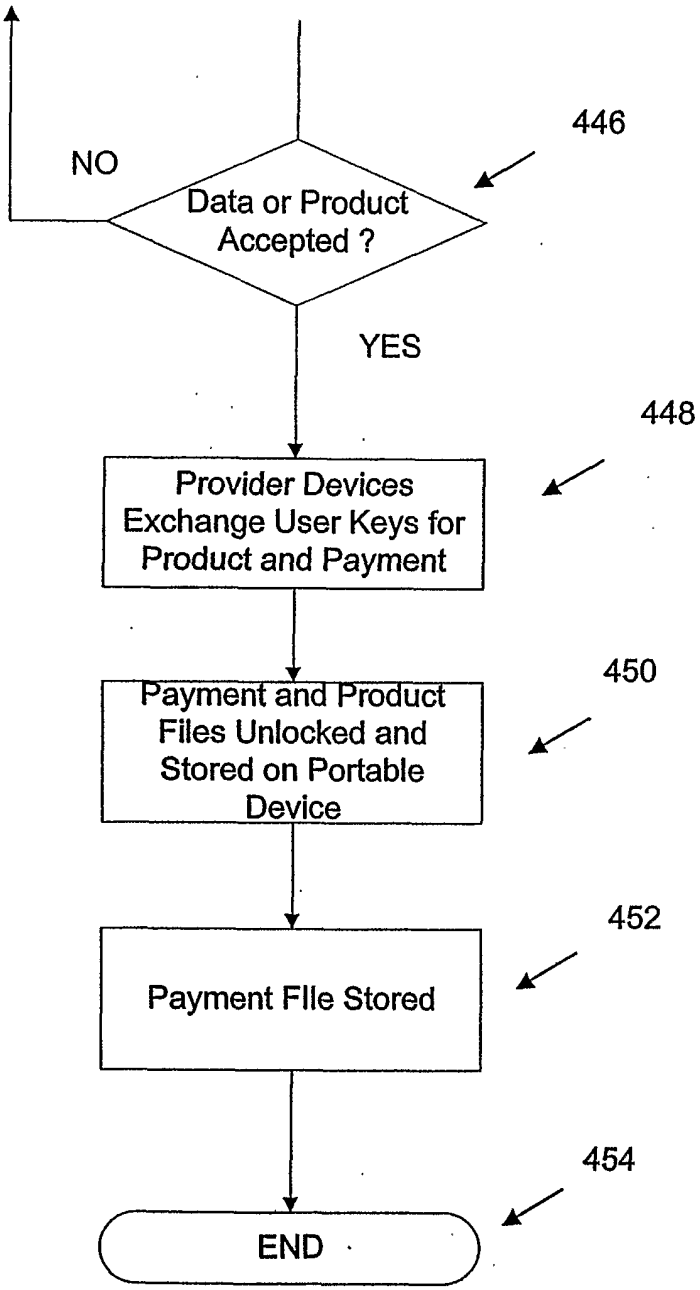

10
38
40
84
86
124
126
64
24
View-Only Payment File 120
70
12
28
35
30
32
34
26
78
72
74
76
68
88
Payment File 122
15
16
18
20
22
14
42
60
62
66
80
92
94
100
96
98
90
36
82
View-Only Product File 128
Product File 130
132
134
110
112
114
56
52
54
50
108
104
106
102


200
202
Start
204
Purchase Request Entered
206
Purchase Amount Verified by Buyer Portable Device
208
210
View-Only Payment File Protected with System Key Sent to Seller
Payment File Protected with System and User Key and Sent to Seller
214
NO
Seller Approves Payment Amount
212
YES
Payment File Stored In Provider Device
Seller Sends Product
Revise Value on Portable Device
224
216
Product Accepted and Received?
NO
218
YES
NO
File Keys Received and Verified ?
220
YES
NO
Payment File Unlocked ?
222
YES
226
END


300
Start
302
Purchase Request Made
Buyer Verified
304
308
306
View-Only
Payment File Received
Payment File Received
NO
Payment Amount
Approved ?
310
YES
314
312
View-Only Product File Sent
Product File Sent
NO
Product Accepted ?
316
YES
318
NO
File Keys Received
and Verified?
YES
320
NO
Product File
Unlocked ?
YES
Add Value to Seller
Portable Device
322
324
END


400
402
Start
404
Buyer Accesses Network with Base Device
Browses to Seller Site
406
Decides to Transact Business
408
Base Device Requests Insertion of Portable Device
410
Generate and Send Encrypted Signals Between Portable Device and Provider Device
412
Receive and Decrypt Encrypted Signals
414
NO
Portable Device Valid?
416
YES
Read and Display File Types
418
File Selected by Buyer
420
NO
Provider Device Passes Keys to Unlock File ?
422
YES


Available Value?
424
NO
YES
Value Deducted from Portable Device
426
428
430
View-Only Payment File Generated and Encrypted with System Key
Payment File Generated and Encrypted with System and User Key
Base Device Transmits View-Only Payment File and Payment File
432
Seller Base Device Receives Packet
434
Unlock View-Only Payment File and Payment File with System Key
436
NO
Seller Accepts Value
438
440
442
YES
Seller Generates View-Only Product File Protected with System Key
Seller Generates Product File Protected with User and System Key
View-Only Product and Product Files Sent To Buyer
444


NO
Data or Product Accepted ?
446
YES
Provider Devices Exchange User Keys for Product and Payment
448
Payment and Product Files Unlocked and Stored on Portable Device
450
Payment FIle Stored
452
END
454

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/07408

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F, 17/30
US CL :705/26, 27, 41

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/26, 27, 41

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,953,504 A (SOKAL et al.) 14 SEPTEMBER 1999, All.	1-29
A	US 5,806,045 A (BIORGE et al.) 08 SEPTEMBER 1998, All.	1-29
A	US 5,438,184 A (ROBERTS et al.) 01 AUGUST 1995, All.	1-29
A	US 5,727,249 A (POLLIN) 10 MARCH 1998, All.	1-29
A	US 5,917,168 A (NAKAMURA et al.) 29 JUNE 1999, All.	1-29

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 20 APRIL 2001	Date of mailing of the international search report 08 MAY 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JAMES TRAMMELL Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)★