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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 March 2004 (11.03.2004)

PCT

(10) International Publication Number
WO 2004/021130 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2003/027010

(22) International Filing Date: 27 August 2003 (27.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/229,959 27 August 2002 (27.08.2002) US

(71) Applicants: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Boulevard, Foster City, CA 94404 (US). **VISA U.S.A., INC.** [US/US]; 123 Mission Street, San Francisco, CA 94105 (US).

(72) Inventors: **HUANG, Jean**; 16 Northwood Drive, Orinda, CA 94563 (US). **REDMOND, Eric**; 220 Eagle Trace Drive, Half Moon Bay, CA 94019 (US). **HEISINGER, Pete**; 170 Swett Road, Woodside, CA 94062 (US).

(74) Agents: **NG, Horace, H.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 94111 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), 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, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK (utility model), SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

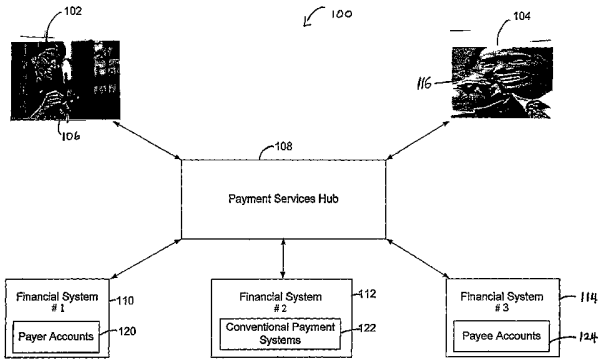
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, NI, NO, NZ, OM, PG, PH,*

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR FACILITATING PAYMENT TRANSACTIONS USING ACCESS DEVICES



(57) Abstract: A payment system for facilitating a payment transaction between a payer and a payee is disclosed. The payment system includes an access device, a payee device, and a services hub. The services hub is configured to communicate with the access device and the payee device; maintain information relating to a payer account and access device information associated with the payer account, the payer account being linked to the access device; generate a tracer ticket in response to a request issued by the payer using either the access device or the payee device, the tracer ticket containing information relating to the payment transaction; validate the access device; and authorize the payment transaction against the payer account. Upon receiving the request from the payee device for the tracer ticket, the services hub generates the tracer ticket and forwards a copy thereof to the payer via the payee device. Upon receiving the copy of the tracer ticket, the payer uses the access device to communicate with the services hub and forward the received copy of the tracer ticket to the services hub. The services hub then validates the access device based on the access device information. Upon validation of the access device, the services hub checks the copy of the tracer ticket forwarded by the access device against the previously generated tracer ticket. If the copy of the tracer ticket forwarded by the access device corresponds to the previously generated tracer ticket, the services hub authorizes the payment transaction against the payer account.

WO 2004/021130 A2

PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

Published:

— *without international search report and to be republished upon receipt of that 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.

METHOD AND SYSTEM FOR FACILITATING PAYMENT TRANSACTIONS USING ACCESS DEVICES

BACKGROUND OF THE INVENTION

[0001] The present invention relates generally to the field of financial transaction processing and, more specifically, to a method and system for facilitating payment transactions using portable electronic devices.

[0002] A typical consumer generally maintains a number of financial accounts. For example, a consumer may have a number of credit and/or charge accounts issued by various financial institutions or merchants as well as the more traditional banking accounts, such as, savings and checking accounts. When making payments, most consumers usually choose either a charge account or a checking account. In the case of a credit purchase, a charge is made against a credit account, and in the case of a debit purchase, a transaction amount is debited against a checking account.

[0003] Various financial accounts are typically offered and maintained by different financial or business institutions. In most cases these accounts are supported by different payment systems and underlying financial networks. For example, a credit account may be issued via a bank or a retail merchant and the payments are processed via credit card payment networks; a debit account may be maintained by an institutional bank; and the transactions are handled by debit card networks.

[0004] The physical presentation instruments of a financial account can be a magnetic stripe card, a chip card or a check book. Financial transactions are typically conducted using these presentation instruments and compatible point-of-sale devices at designated card acceptance locations. The cardholder can also provide account information over the Internet in an on-line payment environment.

[0005] With a plethora of financial offerings, it is typical for today's consumer to have a number of credit cards, various merchant charge cards, debit cards (DDA-demand deposit accounts), etc. Since different institutions respectively maintain different financial accounts and disparate systems, these institutions generally do not communicate with one another, and there is a lack of uniformity in accessing customer accounts. If access to all accounts is desired when making payments, a consumer must carry all corresponding presentation instruments and understand the locations and terms by which these instruments

are accepted. This may prove to be an inconvenience if a large number of presentation instruments are involved.

[0006] In addition, physically carrying presentation instruments also poses a significant security risk. For example, the presentation instrument could get stolen or misplaced, or account information which is typically printed on the presentation instrument may be accessed relatively easily by unauthorized third parties to conduct illegitimate transactions. While it is true that most presentation instruments have a single security level, such as, a signature, a password or logon identification or the like, for authenticating user access to the associated accounts, this single security level does not always provide sufficiently high security assurance that may be deemed desirable for financial transactions. In many commercial transactions, only a single signature, which may be forged with relative ease, is required to consummate a transaction. And in some cases, such as, online transactions conducted on the Internet, no signature is even needed.

[0007] Hence, it would be desirable to have a method and system that is capable of providing a uniform secure access via consumer chosen electronic devices to various financial accounts without requiring a consumer to carry the corresponding presentation instruments. It is also desirable to control all such accounts for various financial institutions in tandem from a single interface.

[0008] Furthermore, technological advancements have contributed to the increasingly popular use of wireless communication devices. Examples of such wireless communication devices are cell phones, portable digital assistants (PDAs) and the like. One reason for this increasing popularity is the improved portability of smaller wireless communication devices and ubiquitous network access.

[0009] Another reason for the increasing popularity is the enhanced functionality of these wireless communication devices. Many wireless communication devices are now able to perform a number of different tasks. More functionality and applications are being developed and added to accommodate the needs of consumers. For example, some cell phones not only provide traditional telephonic functions but they also offer more advanced functions, such as, the capability to allow a user to access and navigate the Internet or otherwise conduct transactions.

[0010] Therefore, it would also be desirable to have a method and system that is capable of using the enhanced functionality of portable communication devices to allow a consumer to use a uniform method to access multiple financial accounts for everyday financial activities.

SUMMARY OF THE INVENTION

[0011] A method and system is disclosed for electronically connecting any payer to any payee to facilitate a financial transaction across or between payment processing systems. Among other advantages, the system provides a single interface for accessing various accounts belonging to payers and payees. This functionality can enable consumers to pay for purchased goods and/or services at merchant locations or pay individuals without having numerous payment cards in their possession by using personal access devices such as a cell phone, a personal digital assistant (PDA), a regular telephone, or a personal computer with Internet access.

[0012] As another example, payers can use such access devices to transfer payment amounts from one or more accounts to one or more payee accounts. This single interface point includes a personal access device and its communication network with a payment services hub. Initially, a registration process occurs at a payment services hub. Users, such as, payers and payees, register their accounts and associated information. Examples of such accounts are credit card accounts, merchant charge accounts, demand deposit accounts (DDAs), and the like. Users can also register access devices such as cell phones, land line telephones and PDAs used to communicate with the payment services hub. It should be noted that payee registration is optional in some exemplary embodiments.

[0013] After registration, the payment services hub can be used to facilitate the transfer of payment amounts from a payer account to a payee account even if the accounts are supported by different payment systems.

[0014] According to one exemplary method, to initiate a payment request, a registered access device belonging to a payer is used to contact the payment services hub. Upon receiving the payment request, the payment services hub first authenticates the payer's identity and the registered access device. If authentication is successful, the payment services hub generates a tracer ticket for linking the payer to the payee. In one embodiment, the tracer ticket is a data record containing various transaction-related information in an encrypted and digitally signed format. Among other attributes, the tracer ticket can include the authorized payment amount and the payer and payee account information for the subject transaction.

[0015] Upon receiving the tracer ticket, the payer forwards this information to the payee. In turn, the payee uses the payee's registered access device to contact the payment services hub. Here, the payee requests payment by providing the tracer ticket information to the payment services hub. Payment is authorized if the tracer ticket information provided

matches the payment terms of the ticket that was previously generated by the payment services hub. Advantageously, the payment services hub facilitates a two-tier process where tracer ticket generation is separated from the payer authorization process.

[0016] According to another aspect, the payer can register multiple accounts from which payments can be made. Thus, upon payer request, the payment services hub is configured to make a payment from one or more payer accounts to a payee account.

[0017] According to another aspect, an exemplary method is disclosed for processing a payment amount to be transferred. This method includes the steps of receiving a payment request from a payee device such as a POS (point of sale) device, and providing a tracer ticket to the payee device. This tracer ticket is then displayed to the payer on the payee device. After the tracer ticket is reviewed by the payer, the method includes the steps of establishing communication with the payment services hub through the payer's access device, and submitting the tracer ticket information via the payer access device. Thereafter, the method validates that the tracer ticket provided to the payee device corresponds to the tracer ticket information received from the payer access device. If validation is successful, the payment request is processed.

[0018] According to another exemplary embodiment, the present invention of the payment service hub is implemented as a computer software product executable by a computer and network system infrastructure. This computer software product includes programming code for receiving a payment request along with the payer identification information from a payee device, and for providing a tracer ticket to the payee device. The computer software product further includes programming code for establishing communication with a payer access device based on the provided payer identification information, and for accepting the tracer ticket information from the payer access device. Further, programming code of the payment services hub is included for validating that the tracer ticket information submitted by the payer corresponds to the payee's tracer ticket information, and for processing the payment request such that the designated amount is later transferred or credited to a payee account.

[0019] Another exemplary method of transferring a payment amount from a first account to a second account is disclosed. The first account may be a payer account while the second account is a payee account. This method includes the steps of registering the first account with the payment services hub, and registering a communication device associated with the first account. Further steps include using the communication device to request access to the payment services hub, and authenticating the access request using a number

associated with the communication device. This number may be a cell phone number or telephone number, for example. Next, steps of requesting transfer of the payment amount from the first account to the second account, and generating the tracer ticket are implemented. Note that the tracer ticket contains designations for the payment amount, the first account and the second account.

[0020] According to another exemplary aspect, a method of processing a payment amount is disclosed. The method includes the steps of using a first communication device to request a tracer ticket; and receiving the tracer ticket. As an example, the first communication device can be a land-line telephone. Further, the method includes the steps of using a second communication device and the tracer ticket to request the payment amount; and authorizing transfer of the payment amount from a payer to a payee. Note that the second communication device may be a payee's cell phone.

[0021] A further understanding of the nature and advantages of the present invention herein may be realized by reference to the remaining portions of the specification and the attached drawings. References to "steps" of the present invention should not be construed as limited to "step plus function" means, and are not intended to refer to a specific order for implementing the invention. Further features and advantages of the present invention, as well as the structure and operation of various embodiments of the present invention, are described in detail below with respect to the accompanying drawings. In the drawings, the same reference numbers indicate identical or functionally similar elements.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] Fig. 1 is a simplified block diagram illustrating the overall architecture of a payment system for facilitating payment transactions in accordance with one exemplary embodiment of the present invention;

[0023] Fig. 2 is a simplified block diagram illustrating an exemplary embodiment of a payment services hub in accordance with the present invention;

[0024] Fig. 3 is a flow diagram illustrating an exemplary method of registering users of the payment system in accordance with the present invention;

[0025] Fig. 4 is a flow diagram illustrating a first exemplary method of using the payment system to pay merchants in accordance with the present invention;

[0026] Fig. 5 is a flow diagram illustrating a second exemplary method of using the payment system to pay merchants in accordance with the present invention;

[0027] Fig. 6 is a flow diagram illustrating a third exemplary method of using the payment system to pay merchants in accordance with the present invention; and

[0028] Fig. 7 is a flow diagram illustrating an exemplary method of using the payment system to pay individuals in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0029] The present invention in the form of one or more exemplary embodiments will now be described.

[0030] Fig. 1 is a simplified block diagram illustrating the overall architecture of a payment system 100 for facilitating payment transactions in accordance with one exemplary embodiment of the present invention. According to the exemplary embodiment, the payment system 100 is provided for facilitating a financial transaction between a payer 102 and a payee 104. The payment system 100 may use mobile communication and Internet based technologies to facilitate such a financial transaction. The payment system 100 includes a payment services hub 108 that manages and coordinates financial transactions among payers, payees, financial institutions and underlying payment processing services.

[0031] The payment services hub 108 can communicate with a number of financial systems 110, 112 and 114 maintained by third parties, such as, a bank card issuer, a merchant acquirer, a financial institution, and a business entity, etc. These financial systems offer different types of financial and/or payment services, such as, credit services, debit services, ACH, electronic fund transfers. A payment service hub acts as an integrator that bridges these financial services in support of payers and payees and their associated access devices.

[0032] The payment services hub 108 uses selective third party payment services to complete payment transactions between payer account issuers and payee account issuers. For example, referring to Fig. 1, payer account 120 is handled by a first financial system 110, conventional payment services 122 are offered by a second financial system 112, and a payee account 124 is handled by a third financial system 114. Payment services offered by payment services hub 108 will be further described below. Communications between the payment services hub 108 and the financial systems 110, 112 and 114 are conducted via computer networks, such as, the Internet, or dedicated private communication links. In an exemplary embodiment, the payment services hub 108 employs an end-to-end network and system security, and federated access controls. One skilled in the art can easily implement various techniques for secure communication.

[0033] In addition, the payment services hub 108 also includes a number of communication interfaces (not shown) to allow communication with access devices. Furthermore, the payment services hub 108 provides a uniform interface to facilitate the authorization and settlement of the payment transactions between disparate payment processing systems. Thus, the payment services hub 108 can allow secure payment transactions to occur between any financial accounts through the access devices chosen by the payer and payee, respectively.

[0034] As will be further described below, for example, a payer 102 can use the payment system 100 to pay for goods and/or services purchased from a merchant/payee 104. More specifically, the payer 102 may utilize an access device, such as, a cell phone 106, to contact the payment services hub 108 to effect payment for a purchase to the payee 104. The payee 104 in turn can collect the payment via an access device such as regular telephone 116. The payment services hub 108 utilizes an electronic tracer ticket (not shown) to associate the payer 102 and the payee 104 and ensure that the payment transaction to be completed is authorized. The function and use of the tracer ticket will be further demonstrated below.

[0035] The payment services hub 108 communicates with the relevant financial systems that respectively maintain the payer account and the payee account as well as other payment processing systems that may be needed and effect transfer of funds between the accounts. For example, if the payer account is a credit card account, the payment services hub 108 coordinates all the relevant activities amongst the issuer financial system, the acquirer financial system and the processing network to effect the payment authorization and the transfer of funds between the issuer financial system and the acquirer financial system. The payment services hub 108 can support smart cards, personal identification numbers, biometric mechanisms and other techniques for payment authentication and authorization.

[0036] Fig. 2 is a simplified block diagram illustrating an exemplary embodiment of the payment services hub 108 in accordance with the present invention. The payment services hub 108 may comprise software components, hardware components, or a combination of both. Hardware components include, for example, switches, routers, groups of modem cards for dial-in users, voice response units, and/or a gateway cards for connections to a local area and external networks. The software components of the payment services hub 108 described here can be implemented in a distributed or integrated manner depending on the system capabilities and agreements of the participating financial

institutions. Based on the disclosure provided herein, a person of ordinary skill in the art will know of other ways and/or methods to implement the payment services hub 108 in accordance with the present invention.

[0037] Referring to Fig. 2, the payment services hub 108 has a number of modules as shown. These modules can include one or more program codes or applications for performing desired tasks. The modules include a tracer ticket issuance module 202 for generating tracer tickets, a service profiles module 204 for maintaining user service profiles and personal preferences, a user registration module 206 for registering payers and, optionally, for registering payees, an operating regulations module 208 for providing technical and business operating regulations that govern the use of the services, an access authentication module 210 for maintaining and enforcing authentication schemes or profiles relating to access devices, a tracer ticket services module 212 for providing a number of services specific to the tracer tickets, and a payment system interface module 214 for communicating and message formatting transactions for various payment services.

[0038] As mentioned above, tracer tickets are generated by the tracer ticket issuance module 202. Such a tracer ticket associates a payer and a payee to authorize the transfer of payment amounts from the payer to the payee. In one exemplary embodiment, a tracer ticket is a secure financial token representing a collection of payment terms containing pertinent payment authorization, and clearing and settlement information required by the downstream payment processing systems. This information includes, for example, an identification number associated with the tracer ticket, a payment amount, payee name, payer name, transaction details, password, digital certificate, digital signature, account information, payment instructions, payee's identity, e-mail addresses and other pertinent transaction information. The tracer ticket may also represent a payment assertion made by payer and/or the payment system 100.

[0039] If the payee's name, identity, and/or the account information is not specified at the time of tracer ticket issuance, possession of the tracer ticket constitutes a rightful claim to the payment amount, provided other transaction conditions have been satisfied. Note that rightful possession of the tracer ticket is validated by the payment system 100, which validates the payee's (the ticket bearer) knowledge of the payment terms by verifying knowledge that should only be known to the payee. The use of tracer tickets will be further described below.

[0040] The service profiles module 204 receives and maintains various types of information from users. Users include payers and, optionally, payees. This information

includes, for example, personal preferences, security preferences, payment profiles and device information relating to access devices that will be used to access the payment services hub 108.

[0041] The user registration module 206 registers and maintains payer and/or payee information, such as, information relating to accounts and their associated access devices. More specifically, a user (either a payer or a payee) provides a list of accounts that are to be serviced and/or managed by the payment services hub 108. Each account may be associated with one or more access devices, such as, a cell phone, a PDA, a traditional telephone, a personal computer, a point-of-sale device, etc. Information relating to these access devices is registered or linked to a specific account.

[0042] Payment services hub 108 only allows access devices (and no other devices) that are linked to an account (i.e., registered access devices) to be used to conduct a payment transaction in connection with that account. For example, a payer may provide information relating to his/her checking account to the payment services hub 108 and link that account to a particular cell phone. As a result, the payment services hub 108 only allows that particular cell phone to be used for transacting business in connection with that payer's checking account.

[0043] The operating regulations module 208 defines and maintains regulations that govern the user' activities. Users, including payers and payees, of the payment system 100 are required to abide by the applicable operating regulations. These regulations include business regulations, such as, service agreements, privacy regulations and dispute resolution, insurance policy and escrow policy, etc. For example, dispute resolution regulations specify a party's recourse when that party fails to receive funds that are supposed to have been transferred by the payment system 100. These regulations also include technical regulations that need to be complied with for communication with the payment services hub 108. For example, a regulation may specify technical and network criteria that must be complied with before a financial institution is allowed to communicate with the payment services hub 108.

[0044] The access authentication module 210 stores and maintains respective authentication schemes for registered access devices. Different access devices may utilize different authentication schemes, such as, user ID/password, PKI or digital certificate, smart card, and biometric information including fingerprint, voice print, retina scan and any other unique identification information, etc. This provides additional security against unauthorized use of registered access devices. For example, a stolen access device, albeit registered,

cannot be used to effect a payment transaction using the payment services hub 108 if the access device cannot be authenticated.

[0045] Tracer ticket services module 212 provides services that are specific to the processing of tracer tickets. These services may include acquisition, authentication, authorization, settlement, audit and dispute resolution relating to the payment transactions initiated by the tracer ticket.

[0046] Payment system interface module 214 provides the ability to format, translate, and route the payment transactions to appropriate payment networks, e.g., ATM networks, credit card networks, ACH networks, etc. for completing the payment transactions originated by the payment system 100.

[0047] Fig. 3 illustrates an exemplary method for registering users, such as payers, with the payment system 100. To use the payment system 100, it is preferred that the payer 102 provides certain registration information. In an exemplary embodiment, the registration information is collected by the payment services hub 108, more specifically, the user registration module 206, via a user interface that is accessible through the Internet.

[0048] At step 302, the registration process is initiated by the payer 102 online. The payer 102 uses, for example, a computer 301 to access one of the affiliated registration web sites of the payment system 100. The web site provides an introduction that describes the payment services, provides demonstrations, and thereafter, if the payer 102 wishes to proceed, initiates a registration process. Services related to the registration process may be hosted by the payment system 100, generic service providers designated to set up register and qualify user accounts, or an account issuer website (i.e., a bank or a financial institution). In addition, although not shown, the registration process may occur over the telephone or via regular postal mail services.

[0049] At step 304, payer information is provided to the payment services hub 108. The payer 102 fills out a registration form, and provides the requested information to register the accounts that are to be serviced by the payment system 100. For example, the payer 102 may provide a name, address, bank account numbers, credit card numbers, and other pertinent information. Further, access devices 322 that will be used to communicate with the payment services hub 108 are registered by the payer 102. These access devices may be a cell phone, a PDA, a traditional telephone, a computer and the like. More specifically, the payer 102 specifies how the access devices are to be linked to the registered accounts. For example, the payer 102 can link all the access devices to all registered accounts. Alternatively, certain designated accounts may be linked only to certain access devices. For

example, the payer's registered credit card account may be linked with a registered cell phone, but not with a registered PDA.

[0050] The registration process of the payment services hub 108 also captures information that is needed to authenticate the registered access devices for security reasons. The payment services hub 108 is designed to support a number of authentication schemes used by various access devices. For example, a fingerprint, a voice print over the telephone, logon identification and password may be captured and stored by the payment services hub 108.

[0051] Other information relating to personal preferences and payment profiles 312 may also be captured by the payment services hub 108 during the registration process. For example, the payer 102 can specify accounts from which payment for goods and/or services are automatically made if the conditions of the purchase satisfy the established payment profile. In another example, the payer 102 directs that a registered account specifically be charged for purchases from designated merchants. Further, as shown, the payer 102 can provide updated information as needed for profile management at step 312. Such information can be, for example, personal preferences, security preferences, payment profiles and session preferences.

[0052] As part of the registration process, certain information, such as, legal information and user operating regulations is provided to the payer 102. Such information includes security agreements, privacy, arbitration, insurance, escrow policies, etc. As an example, a user agreement may state that the payer must pay for goods and/or services as agreed between the payer 102 and a merchant from whom the goods and services were purchased. As another example, the user agreement may require that the payer 102 submit all disagreements for arbitration. If payer 102 agrees with the legal and user operating regulations, the payer 102 is registered with the payment system 100.

[0053] At step 306, the payer's account is activated. The payer 102 is guided through a test run, illustrating operations of the payment services provided by the payment system 100. First, a dummy tracer ticket for demonstration purposes is created by the payment services hub 108 for use during the test run. An identification number and a pass code are generated in association with the dummy tracer ticket. The payer 102 is then directed by the payment services hub 108 to activate a registered access device for the test run. The payment services hub 108 then contacts the activated registered access device.

[0054] At step 308, communication is established between the payment services hub 108 and the registered access device 322. The payer 102 is asked by the payment services

hub 108 to provide the dummy tracer ticket. In response, the payer 102 uses the registered access device 322 to enter the identification number and the pass code associated with the dummy tracer ticket. If the identification number and/or the pass code is incorrect, or, if payment services hub 108 is unable to contact the registered access device 322, a troubleshooting dialog is initiated by the registration web site.

[0055] Otherwise, at step 310, registration is confirmed. The payer 102 is prompted to confirm registration of the indicated accounts and access devices 322. In turn, the payer 102 provides the requested confirmation, whereupon a registration-complete acknowledgment is sent by payment services hub 108 to the payer 102.

[0056] As mentioned above, it should be noted that a payee 104 may also be registered with the payment services hub 108. A registered user can be either a payer 102 or a payee 104. Registering a payee 104 requires less information. A payee 104 only needs to provide sufficient information to identify the accounts that are to be serviced by the payment services hub 108. Once registration is completed, the payment services hub 108 can be used by the payer 102 to effect a payment transaction to pay the payee 104.

[0057] Fig. 4 is a flow diagram illustrating a first exemplary method of using the payment system 100 to pay the payee 104 in accordance with the present invention. More specifically, among multiple payment options at the merchant location, the payer 102 chooses the payment system 100 to pay for goods and/or services purchased from the merchant/payee 104.

[0058] At step 402, the payer 102 initiates the payment process by selecting at the POS device 403 an option offering payment services by the payment system 100. In one exemplary embodiment, the POS device 403 is a conventional payment device connected to the payment services hub 108 via the merchant back office systems. In another exemplary embodiment, the POS device 403 can include authentication mechanisms, such as, biometrics (e.g., fingerprint), smart card, user ID/password and the like. These security mechanisms are used to authenticate and authorize the payer's access to the payment services hub 108. For example, after selecting the payment services provided by the payment system 100, a payer 102's fingerprint may be captured by the POS device 403 and forwarded to the payment services hub 108 for validation with a fingerprint verification service to ensure that only an authorized payer can initiate the payment process.

[0059] At step 404, the payment services hub 108 is contacted by the POS device 403 to obtain a tracer ticket. As previously noted, the tracer ticket functions to authorize payment of the designated amount. Registered payee/merchant account information and other

pertinent information are retrieved from various databases (not shown) for generating the tracer ticket. Examples of such information are payee's (merchant) profile, security preferences profile, access device (POS) profile, and payment profile.

[0060] A merchant profile includes a merchant name, types of business and other pertinent information. Security preferences profile includes authentication choices such as payee identification and password, digital certificate, and the like. Access device profile includes authentication and device type information for registered access devices, in this exemplary embodiment, POS device 403. These profiles are evaluated to determine whether the tracer ticket will be generated, and what information is to be included in the tracer ticket. Further, the tracer ticket generation is separate from the payer authorization and tracer ticket validation processes to further enhance overall security. As discussed below at step 406, after the tracer ticket is generated, the tracer ticket number is displayed at the POS device 403. The payer 102 uses the tracer ticket number and a registered access device 322 to authorize payment.

[0061] At step 406, to provide the requested tracer ticket, a payment amount is required by the payment services hub 108. Thus, a dialog is initiated between the payment services hub 108 and the POS device 403 to obtain this payment amount. The merchant/payee 104 is prompted for a payment amount and any payment terms, if applicable. The payment amount could be the total purchase price of the goods and/or services, for example. Payment terms may relate to how the payment is to be made, for example. Upon receiving the payment amount data, the tracer ticket is forwarded to the POS device 403 as illustrated at step 408. The POS device 403, in turn, displays the tracer ticket number for retrieval by payer 102.

[0062] At step 410, the payer authorization process is initiated. Specifically, the payer 102 uses the access device 322 to contact the payment services hub 108. This authorization process is separate from the tracer ticket generation process. Thus, while the tracer ticket is generated by using the POS device 403 to contact the payment services hub 108, the authorization process is implemented by using the registered access device 322 to contact the payment services hub 108. This two-tier process further increases overall security within the payment system 100.

[0063] At step 412, contact is established. The payment services hub 108 then authenticates access by the payer 102. Specifically, the payment services hub 108 retrieves stored registration information to validate the access device 322. This registration information is used to confirm that access device 322 is indeed linked to the payer 102. The

payment services hub 108 employs two or more security levels for authenticating the payer 102. A first security level uses a digital identification associated with the access device 322, and a second security level is a logon id/password. As an example, if the access device 322 is a cell phone, the cell phone number is used for authentication. A second security level can be a user ID/password, smart card, etc. Further yet, fingerprint, voice print authentication may be used for the first, second or third security level, where appropriate. The desired security level and authentication methods can be configured according to the user's preference and operating regulations.

[0064] At step 414, the payment services hub 108 retrieves various payer account information. This information comprises personal preferences, security preferences, access device information and payment profiles. Personal preferences include display interface preferences. Security preferences include authentication choices such as password, voice print, biometrics, and the like. Access device information includes cell phone and PDA information, for example. Payment profile information contains information specifying how an account is linked to the registered access device 322. This information is used to authenticate the payer 102, and the access device 322 and to evaluate the criteria of the tracer ticket generations and verification services, and what information is required in the tracer ticket. Optionally, the payment services hub 108 can interact with a conventional payment infrastructure 401 to obtain payer account information 415. Payer account information 415 is an additional profile layer that is set up by the payer 102 within the conventional payment infrastructure 401.

[0065] At step 416, a dialog (step 417) is established between the payment services hub 108 and the payer's access device 322. The payer 102 is prompted to enter the tracer ticket number previously obtained at step 408. In response, the payer 102 uses the access device 322 to enter the tracer ticket number, whereupon, the payment services hub 108 begins to verify the tracer ticket information. The payment services hub 108 retrieves the related transaction and merchant information, which is compared and checked against the tracer ticket information.

[0066] In one exemplary embodiment, where two or more registered accounts exist, the payer 102 is prompted to select the desired account from which payment will be made. For example, the payer 102 can choose a DDA (checking) account rather than a credit account for a particular transaction. Payment is then initiated through a financial system associated with the DDA account via the payment system interface 214. In another

exemplary embodiment, the payer 102 can split the payment amount between two or more registered accounts.

[0067] Upon proper authentication, the payment services hub 108, more specifically, the payment system interface module 214 directs the conventional payment infrastructure 401 to process payment authorization according to established payment processing techniques, as illustrated in steps 429, 419 and 421. Once payment is authorized, the conventional payment infrastructure 401 forwards an acknowledgement to the payer and/or payee via the payment services hub 108. As shown at steps 420 and 422, the paid/approved response can be delivered to the POS device 403 and/or the access device 322 to inform the parties regarding the outcome of the financial transaction.

[0068] Fig. 5 is a flow diagram illustrating another exemplary method of using the payment services hub 108 to pay merchants in accordance with the present invention.

[0069] Specifically, the payer 102 does not originate contact with the payment services hub 108 after the tracer ticket is generated and displayed at the POS device 403. Rather, the payer 102 is contacted by the payment services hub 108 to validate the tracer ticket information. Accordingly, other than steps 506, 507 and 510, all of the steps of Fig. 5 remain the same as those described with reference to Fig. 4.

[0070] As noted, at step 404, the POS device 403 contacts the payment services hub 108 to obtain a tracer ticket. This begins step 506 wherein a dialog between the payment services hub 108 and the POS device 403 is initiated. Here, the payee/merchant 104 is directed to enter a payment amount, and any other payment terms, if applicable, along with payer 102's identification information. Upon receiving the payment information, the payment services hub 108 creates and forwards the tracer ticket to the POS device 403, as illustrated at step 408. The POS device 403, in turn, displays the tracer ticket number for retrieval by the payer 102. Thereafter, the payer 102 retrieves the tracer ticket, and awaits contact by the payment services hub 108.

[0071] At step 507, the payment services hub 108 initiates contact with the payer 102. Here, the payment services hub 108 retrieves payer 102's personal profiles to contact the access device 322, previously registered by payer 102. Note that one or more access devices may be registered, in which case, the payment services hub 108 contacts the first registered access device, based on a hierarchy established by the payer 102 at registration. If the call is not answered, the next preferred access device is called, etc., until contact is established with the payer 102.

[0072] After contact is established, the payer 102 is authenticated by the payment services hub 108 to determine whether the payer 102 is an authorized user with the access device 322. This authentication process was previously described with reference to steps 412-414 of Fig. 4. After authentication, the payer's profile and preferences are retrieved, the tracer ticket information is verified, and the designated payment amount is transferred in the same manner described with reference to steps 412-421 of Fig. 4.

[0073] Fig. 6 is a flow diagram illustrating yet another exemplary method of using the payment system 100 to pay merchants in accordance with the present invention. Specifically, the payer 102 can obtain a tracer ticket in advance from the payment services hub 108. This tracer ticket is then presented to a merchant 104 for payment. By obtaining a tracer ticket in advance, the tracer ticket can be used as a pre-authorized payment token.

[0074] At step 601, the payer 102 employs the access device 322 to contact the payment services hub 108 for the purpose of obtaining the tracer ticket. At step 602, the payment services hub 108 authenticates the access device 322 (and payer 102). Authentication may be implemented using a number associated with the access device 322. The number may be a telephone number, for example, where the access device 322 is a telephone. If an incorrect telephone number is detected, access to the payment services hub 108 is denied. This authentication process was previously described with reference to steps 412-414 of Fig. 4.

[0075] At step 604, the payment services hub 108 retrieves various payer account information, including personal preferences, security preferences, access device information and payment profiles.

[0076] At step 606, a transactional dialog (step 608) is initiated between the payment services hub 108 and the access device 322. The payer 102 is prompted for certain information. This information includes a payment amount, payment terms and payee information, for example. After the information is received, a tracer ticket is provided to the payer 102 via the access device 322. Optionally, the tracer ticket is given an expiration time or date; i.e., the tracer ticket has a limited lifetime. The limited lifetime duration provides an additional level of security.

[0077] At step 610, the payer 102 wishes to pay for the purchased goods and/or services at a registered merchant/payee 104 location. To initiate payment, the payer 102 uses the POS device 403 to select the payment services offered by the payment system 100.

[0078] At step 612, the payer 102 is prompted by the payment services hub 108 to enter the tracer ticket number that was previously provided by the payment services hub 108. In response, the payer 102 enters the tracer ticket number at the POS device 403.

[0079] At step 614, the payment services hub 108 (step 616) begins to verify the tracer ticket information. For example, the payment services hub 108 retrieves payment profiles related to the payer 102 and the payee/merchant 104, which are compared and checked against the tracer ticket information. If the tracer ticket has an expiration time, the expiration time is checked to make sure that the tracer ticket is still valid. Thereafter, if the tracer ticket is determined to be valid, the payment amount is captured from the tracer ticket dialog to begin processing the payment request. This payment request is then sent via a payment system interface module 214 to the conventional payment infrastructure 620, which uses conventional techniques to process the request as illustrated in steps 622 and 624. Thereafter, an approved/disapproved response is provided to the payment services hub 108, which conveys the response via the interface 214 to the POS device 403 at step 618.

[0080] Fig. 7 is a flow diagram illustrating an exemplary method of using payment system 100 to pay an individual payee 104. At step 701, this payment process is initiated, wherein the payer 102 employs the access device 322 to contact the payment services hub 108. The purpose of this communication is to obtain a tracer ticket from the payment services hub 108.

[0081] At step 702, the payment services hub 108 establishes contact and authenticates access by the access device 322. At step 704, the payment services hub 108 retrieves various payer account information including personal preferences, security preferences, access device information and payment profiles. As previously noted as an example, if the access device 322 is a cell phone, then its cell phone digital identification is used for authentication, along with other authentication techniques such as user ID and password, depending on payer 102's preferences.

[0082] At step 706, a transactional dialog (step 708) is initiated between the payment services hub 108 and the access device 322. The payer 102 is prompted for various required information such as a payment amount and payment terms for the transaction. A one-time password for use by the individual payee 104 is further provided. By providing a password, access to the payment services hub 108 by unregistered individual payees can be authenticated. This authentication provides an additional level of security. Upon receiving the required information, a tracer ticket is created and provided to the payer 102 via the access device 322.

[0083] At step 710, a transaction confirmation is sent to the payer 102. At step 712, the payer 102 conveys both the password and the tracer ticket number to the individual payee 104 within the appropriate time frame prior to the expiration of the tracer ticket.

[0084] At step 714, the individual payee 104 uses the unregistered access device 726 to log on to the payment services hub 108. As shown, the access device 726 may be a computer, a cell phone, a PDA, a regular telephone and the like.

[0085] At step 715, the payment services hub 108 receives the logon request and authenticates access by the individual payee 104, an unregistered user of the payment system 100.

[0086] At step 716, the payment services hub 108 attempts to retrieve various payee account information, including personal preferences, security preferences, access device information and payment profiles and determines that the logon user is unregistered.

[0087] At step 718, a transactional dialog (step 719) is initiated between the payment services hub 108 and the access device 726. The individual payee 104 is prompted for both the tracer ticket number and the associated one-time password that were received from the payer 102. Upon receiving this information, the payment services hub 108 verifies the tracer ticket information, captures the payment amount. The payee 104 is further prompted for the additional account information in order to complete the payment transaction via the conventional payment infrastructure 720. The payment services hub 108 uses the payment system interface module 214 to send a payment request to the conventional payment infrastructure 720. The payment infrastructure 720 then uses conventional techniques to process the payment request as illustrated in steps 719 and 724. Thereafter, the conventional payment infrastructure 720 sends, via the interface 214, an approved/disapproved response to the payment services hub 108.

[0088] In turn, at step 719, the payment services hub 108 conveys this response to the individual payee 104 via the access device 726. In this manner, the method of the present invention is used to facilitate electronic transfer of payments between individuals. As an example, the payer 102 can use this method to pay for items purchased from an auction website, such as, eBay. The individual payee 104 indicates a preference to receive a U.S. postal money order for the sold items. The payer 102 then dials into the payment services hub 108, and obtains a tracer ticket incorporating all of the individual payee preferences. The tracer ticket and associated password are then conveyed to the individual payee 104. The individual payee 104 can then use this information to claim the U.S. postal money order at a designated location.

[0089] Note, however, that registration is optional for the individual payee 104. Preferably, both the payer 102 and the individual payee 104 are registered with the payment system 100, as previously described with reference to Fig. 3. Once a password and tracer ticket number have been provided, the individual payee can collect the payment amount from any desired location or online where the payment system 100 is accepted for payment processing.

[0090] While the above is a complete description of exemplary specific embodiments of the invention, additional embodiments are also possible. Thus, the above description should not be taken as limiting the scope of the invention, which is defined by the appended claims along with their full scope of equivalents.

WHAT IS CLAIMED IS:

1. A method for facilitating a payment transaction between a payer and a payee, comprising:

collecting registration information from the payer, the registration information including information relating to a payer account and access device information associated with the payer account;

directing a services hub to generate a tracer ticket in response to a request issued by the payer, the tracer ticket containing information relating to the payment transaction;

forwarding information relating to the tracer ticket to the payer;

establishing communication between the services hub and an access device linked to the payer account;

validating the access device based on the access device information;

using the access device to transmit to the services hub the forwarded information relating to the tracer ticket received by the payer;

confirming the information relating to the tracer ticket transmitted by the access device; and

upon confirmation of the information relating to the tracer ticket transmitted by the access device, authorizing the payment transaction against the payer account.

2. The method of claim 1 further comprising:

in response to the request issued by the payer and prior to generating the tracer ticket, obtaining authentication information from the payer and verifying the authentication information to ensure that the payer is authorized to request the tracer ticket.

3. The method of claim 2 wherein the authentication information includes a password, login ID or biometric information.

4. The method of claim 1 wherein establishing communication between the services hub and the access device comprises:

using the access device to contact the services hub.

5. The method of claim 1 wherein establishing communication between the services hub and the access comprises:

directing the services hub to contact the access device.

6. The method of claim 1 wherein the access device is selected from the group comprising a telephone, a cell phone, a PDA and a personal computer.

7. The method of claim 1 wherein authorizing the payment transaction against the payer account comprises:

directing a transfer of fund from the payer account to a payee account.

8. The method of claim 1 wherein forwarding information relating to the tracer ticket to the payer comprises:

displaying the information relating to the tracer ticket to the payer on a payee device located at a payee location.

9. The method of claim 8 wherein the payee device is a point-of-sale device.

10. A method for facilitating a payment transaction between a payer and a payee, comprising:

collecting registration information from the payer, the registration information including information relating to a plurality of payer accounts belonging to the payer and access device information associated with the plurality of payer accounts, wherein each payer account is associated with one or more of a plurality of access devices;

directing a services hub to generate a tracer ticket in response to a request issued by the payer, the tracer ticket containing information relating to the payment transaction;

forwarding information relating to the tracer ticket to the payer;

establishing communication between the services hub and one of the plurality of access devices;

validating the access device that is in communication with the services hub;

using the access device that is in communication with the services hub to transmit to the services hub the forwarded information relating to the tracer ticket received by the payer;

confirming the information relating to the tracer ticket transmitted by the access device; and

upon confirmation of the information relating to the tracer ticket transmitted by the access device, authorizing the payment transaction against the payer account.

11. The method of claim 10 further comprising:

in response to the request issued by the payer and prior to generating the tracer ticket, obtaining authentication information from the payer and verifying the authentication information to ensure that the payer is authorized to request the tracer ticket.

12. The method of claim 11 wherein the authentication information includes a password, login ID or biometric information.

13. The method of claim 11 wherein establishing communication between the services hub and one of the plurality of access devices comprises:

using the one of the plurality of access devices to contact the services hub.

14. The method of claim 11 wherein establishing communication between the services hub and one of the plurality of access devices comprises:

directing the services hub to contact the plurality of access devices in sequential order until one of the plurality of access devices is successfully contacted.

15. The method of claim 10 wherein the plurality of access devices include a telephone, a cell phone, a PDA and a personal computer.

16. The method of claim 10 wherein authorizing the payment transaction against the payer account comprises:

directing a transfer of fund from one or more of the plurality of payer accounts to a payee account.

17. The method of claim 10 wherein forwarding information relating to the tracer ticket to the payer comprises:

displaying the information relating to the tracer ticket to the payer on a payee device located at a payee location.

18. The method of claim 17 wherein the payee device is a point-of-sale device.

19. A method for facilitating a payment transaction between a payer and a payee, comprising:

collecting registration information from the payer, the registration information including information relating to a payer account belonging to the payer and access device information associated with the payer account;

using an access device to contact a services hub to request a tracer ticket, the tracer ticket containing information relating to the payment transaction;

validating the access device based on the access device information;

upon validation of the access device, directing the services hub to generate the tracer ticket;

forwarding information relating to the tracer ticket from the services hub to the access device;

using a payee device to transmit to the services hub the forwarded information relating to the tracer ticket received by the access device;

confirming the information relating to the tracer ticket transmitted by the payee device; and

upon confirmation of the information relating to the tracer ticket transmitted by the payee device, authorizing the payment transaction against the payer account.

20. The method of claim 19 further comprising:

in response to the request for the tracer ticket and prior to generating the tracer ticket, obtaining authentication information from the payer and verifying the authentication information to ensure that the payer is authorized to request the tracer ticket.

21. The method of claim 20 wherein the authentication information includes a password, a login ID or biometric information.

22. The method of claim 19 wherein the tracer ticket has an expiration time; and wherein confirming the information relating to the tracer ticket transmitted by the payee device comprises:

checking whether the tracer ticket has expired.

23. The method of claim 19 wherein a password is associated with the tracer ticket; and

wherein confirming the information relating to the tracer ticket transmitted by the payee device comprises:

checking whether the information relating to the tracer ticket transmitted by the payee device includes the password associated with the tracer ticket.

24. The method of claim 19 further comprising:

prior to confirming the information relating to the tracer ticket transmitted by the payee device, checking the payee device to determine if the payee device is registered with the services hub.

25. The method of claim 19 wherein the access device is selected from the group comprising a telephone, a cell phone, a PDA and a personal computer.

26. The method of claim 19 wherein authorizing the payment transaction against the payer account comprises:

directing a transfer of fund from the payer account to a payee account.

27. The method of claim 19 wherein the payee device is selected from the group comprising a telephone, a cell phone, a personal computer and a point-of-sale device.

28. A payment system for facilitating a payment transaction between a payer and a payee, comprising:

an access device;

a payee device; and

a services hub configured to:

communicate with the access device and the payee device;

maintain information relating to a payer account and access device information associated with the payer account, the payer account being linked to the access device;

generate a tracer ticket in response to a request issued by the payer using either the access device or the payee device, the tracer ticket containing information relating to the payment transaction;

validate the access device; and

authorize the payment transaction against the payer account;

wherein:

upon receiving the request from the payee device for the tracer ticket, the tracer ticket is generated and a copy thereof is forwarded to the payer via the payee device;

upon receiving the copy of the tracer ticket, the payer uses the access device to communicate with the services hub and forward the received copy of the tracer ticket to the services hub;

the services hub validates the access device based on the access device information;

upon validation of the access device, the services hub checks the copy of the tracer ticket forwarded by the access device against the previously generated tracer ticket; and

if the copy of the tracer ticket forwarded by the access device corresponds to the previously generated tracer ticket, the services hub authorizes the payment transaction against the payer account.

29. The payment system of claim 28 further comprising:

a plurality of financial systems;

wherein the services hub is further configured to communicate with the plurality of financial systems to facilitate the payment transaction between the payer and the payee.

30. The payment system of claim 28 wherein:

prior to generating the tracer ticket, the services hub is further configured to obtain authentication information from the payer and verify the authentication information to ensure that the payer is authorized to request the tracer ticket.

31. The payment system of claim 30 wherein the authentication information includes a password, login ID or biometric information.

32. The payment system of claim 28 wherein:

upon receiving the request from the access device for the tracer ticket, the services hub validates the access device based on the access device information and, upon validating the access device, the services hub generates the tracer ticket and forwards a copy thereof to the access device;

upon receiving the copy of the tracer ticket, the payer provides the copy of the tracer ticket to the payee;

the payee uses the payee device to transmit the copy of the tracer ticket to the services hub; and

upon receiving the copy of the tracer ticket from the payee device, the services hub checks the copy of the tracer ticket from the payee device against the previously generated tracer ticket; and

if the copy of the tracer ticket from the payee device corresponds to the previously generated tracer ticket, the services hub authorizes the payment transaction against the payer account.

33. The payment system of claim 28 wherein the access device is selected from the group comprising a telephone, a cell phone, a PDA and a personal computer.

34. The payment system of claim 28 wherein the payee device is a point-of-sale device.

35. The payment system of claim 28 wherein the tracer ticket has an expiration time; and

wherein when the services hub checks the copy of the tracer ticket, the services hub also checks to see if the previously generated tracer ticket has expired.

36. A payment system for facilitating a payment transaction between a payer and a payee, comprising:

a plurality of access devices;

a payee device;

a plurality of financial systems; and

a services hub configured to:

communicate with the plurality of access devices and the payee device;

maintain information relating to a plurality of payer accounts belonging to the payer and access device information associated with the plurality of payer accounts, each payer account being linked to one or more of the plurality of access devices;

generate a tracer ticket in response to a request issued by the payer using either one of the plurality of access devices or the payee device, the tracer ticket containing information relating to the payment transaction;

validate the plurality of access devices; and

authorize the payment transaction against one or more of the plurality of payer accounts in cooperation with one or more of the plurality of financial systems;

wherein:

upon receiving the request from the payee device for the tracer ticket, the services hub generates the tracer ticket and forwards a copy thereof to the payer via the payee device;

upon receiving the copy of the tracer ticket, the payer uses one of the plurality of access devices to communicate with the services hub and forward the received copy of the tracer ticket to the services hub;

the services hub validates the access device that is used by the payer to forward the copy of the tracer ticket;

upon validation of the access device, the services hub checks the copy of the tracer ticket forwarded by the access device against the previously generated tracer ticket; and

if the copy of the tracer ticket forwarded by the access device corresponds to the previously generated tracer ticket, the services hub authorizes the payment transaction against one or more of the plurality of payer accounts in cooperation with one or more of the plurality of financial systems.

37. The payment system of claim 36 wherein:

prior to generating the tracer ticket, the services hub is further configured to obtain authentication information from the payer and verify the authentication information to ensure that the payer is authorized to request the tracer ticket.

38. The payment system of claim 37 wherein the authentication information includes a password, login ID or biometric information.

39. The payment system of claim 36 wherein:

upon receiving the request from one of the plurality of access devices for the tracer ticket, the services hub validates the access device based on the access device information and, upon validating the access device, the services hub generates the tracer ticket and forwards a copy thereof to the access device;

upon receiving the copy of the tracer ticket, the payer provides the copy of the tracer ticket to the payee;

the payee uses the payee device to transmit the copy of the tracer ticket to the services hub; and

upon receiving the copy of the tracer ticket from the payee device, the services hub checks the copy of the tracer ticket from the payee device against the previously generated tracer ticket; and

if the copy of the tracer ticket from the payee device corresponds to the previously generated tracer ticket, the services hub authorizes the payment transaction against one or more of the plurality of payer accounts in cooperation with one or more of the plurality of financial systems.

40. The payment system of claim 36 wherein the plurality of access devices include a telephone, a cell phone, a PDA and a personal computer.

41. The payment system of claim 36 wherein the payee device is a point-of-sale device.

42. The payment system of claim 36 wherein the tracer ticket has an expiration time; and

wherein when the services hub checks the copy of the tracer ticket, the services hub also checks to see if the previously generated tracer ticket has expired.

43. A payment system for facilitating a payment transaction between a payer and a payee, comprising:

a tracer ticket for specifying one or more terms associated with the payment transaction;

a services hub configured to generate the tracer ticket in response to a request from the payer and to maintain information relating to a payer account and access device information associated with the payer account; and

a payer access device registered with the services hub and configured to communicate with the services hub, the payer access device being linked to the payer account;

wherein in response to the request, the services hub generates the tracer ticket for the payment transaction and forwards a copy thereof to the payer;

wherein the payer uses the payer access device to transmit the copy of the tracer ticket to the services hub;

wherein upon receiving the copy of the tracer ticket from the payer access device, the services hub validates the payer access device using access device information and verifies that the copy of the tracer ticket corresponds to the previously generated tracer ticket; and

wherein upon validation of the payer access device and the verification of the copy of the tracer ticket, the services hub authorizes the payment transaction against the payer account.

44. The payment system of claim 43 further comprising:

a payee access device for receiving or transmitting the copy of the tracer ticket to the payer.

45. The payment system of claim 44 wherein the payee access device is configured to receive the copy of the tracer ticket from the services hub.

46. The payment system of claim 43 wherein the payer access device is selected from the group comprising a telephone, a cell phone, a PDA, and a personal computer.

47. The payment system of claim 44 wherein the payee access device is selected from the group comprising a telephone, a cell phone, a PDA, a personal computer, and a point-of-sale device.

48. The payment system of claim 43 wherein the tracer ticket is a secure financial transaction token representing a collection of payment-related terms.

49. The payment system of claim 43 wherein the one or more terms is a payment assertion from the payer access device or payment system.

50. The payment system of claim 43 wherein the one or more terms is selected from the group comprising a payer's name, an identification, a password, a digital certificate, a digital signature, account information, a payment amount, payment instructions, a payee's identity and an e-mail address.

51. The payment system of claim 43 wherein the tracer ticket is a unique digital token dynamically issued by the services hub.

52. The payment system of claim 43 wherein the services hub validates payer or payee entitlement to possess the copy of the tracer ticket.

53. The payment system of claim 43 wherein the services hub validates payee entitlement by validating the payee's knowledge of payment terms.

54. A computer software product designed to facilitate a payment transaction between a payer and a payee, comprising:

programming code for maintaining information relating to a payer account and access device information associated with the payer account;

programming code for receiving a payment request from a payee device;

programming code for providing a first tracer ticket to the payee device in response to the payment request;

programming code for establishing communication with a payer access device;

programming code for validating the payer access device based on the access device information to ensure that the payer access device is linked to the payer account;

programming code for receiving a second tracer ticket from the payer access device; and

programming code for validating that the first tracer ticket corresponds to the second tracer ticket; and

programming code for authorizing the payment transaction against the payer account if the first tracer ticket is successfully validated against the second tracer ticket.

55. The computer software product of claim 54 further comprising:

programming code for interfacing with one or more financial systems to effectuate the payment transaction against the payer account.

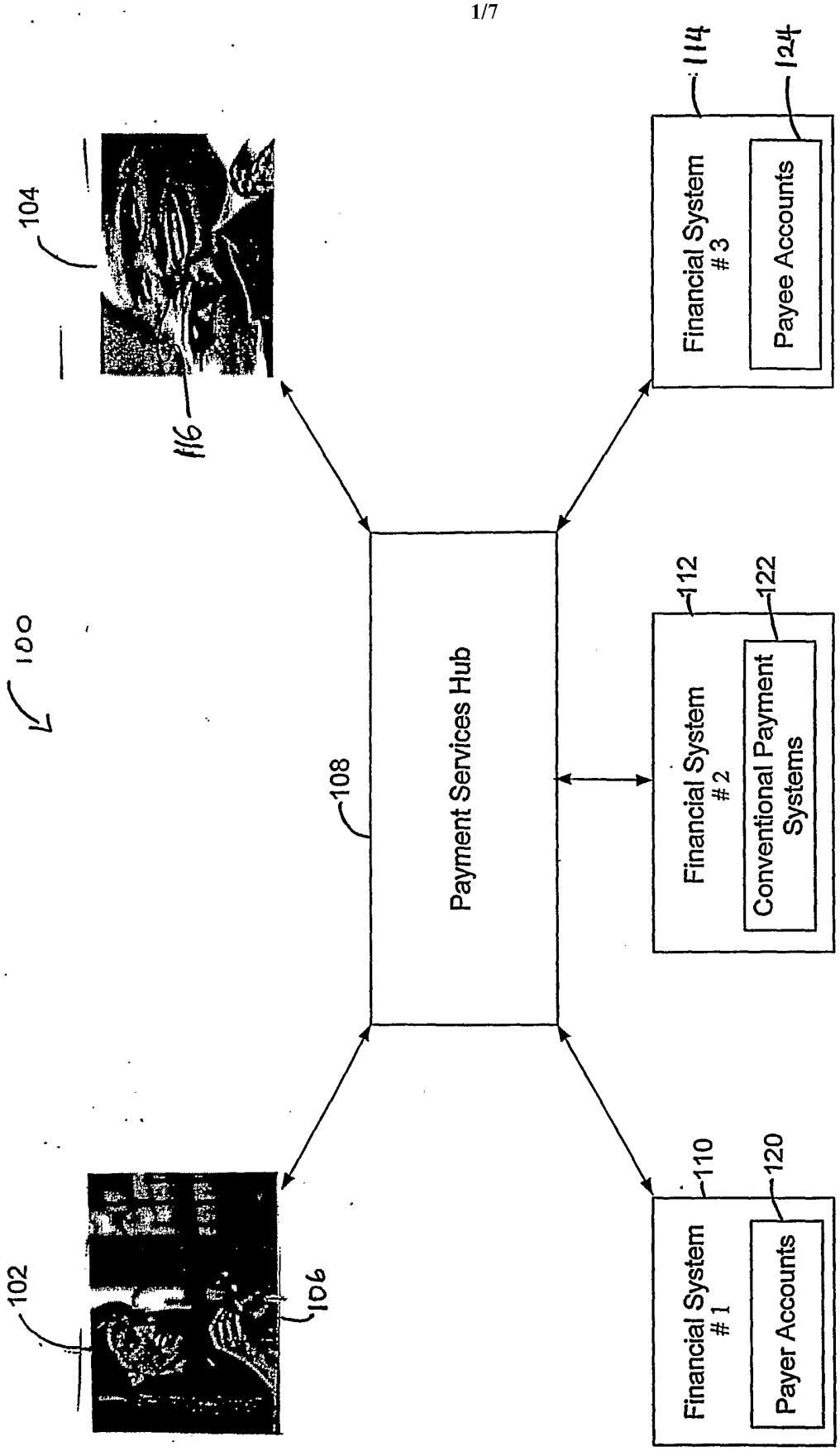

100
102
104
106
108
Payment Services Hub
110
Financial System #1
120
Payer Accounts
112
Financial System #2
122
Conventional Payment Systems
114
Financial System #3
124
Payee Accounts
116

Figure 1

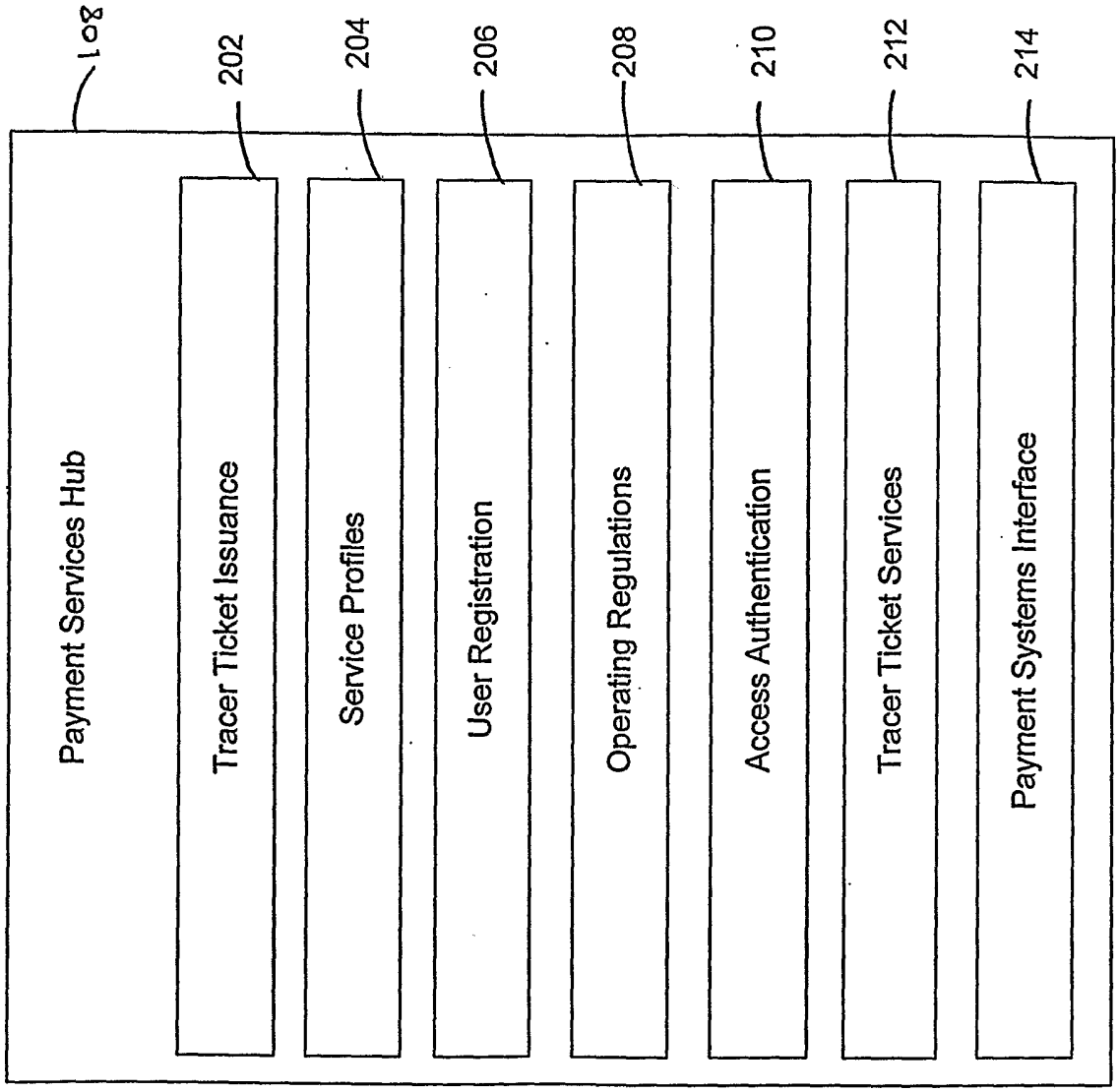

108
Payment Services Hub
202
Tracer Ticket Issuance
204
Service Profiles
206
User Registration
208
Operating Regulations
210
Access Authentication
212
Tracer Ticket Services
214
Payment Systems Interface

Figure 2

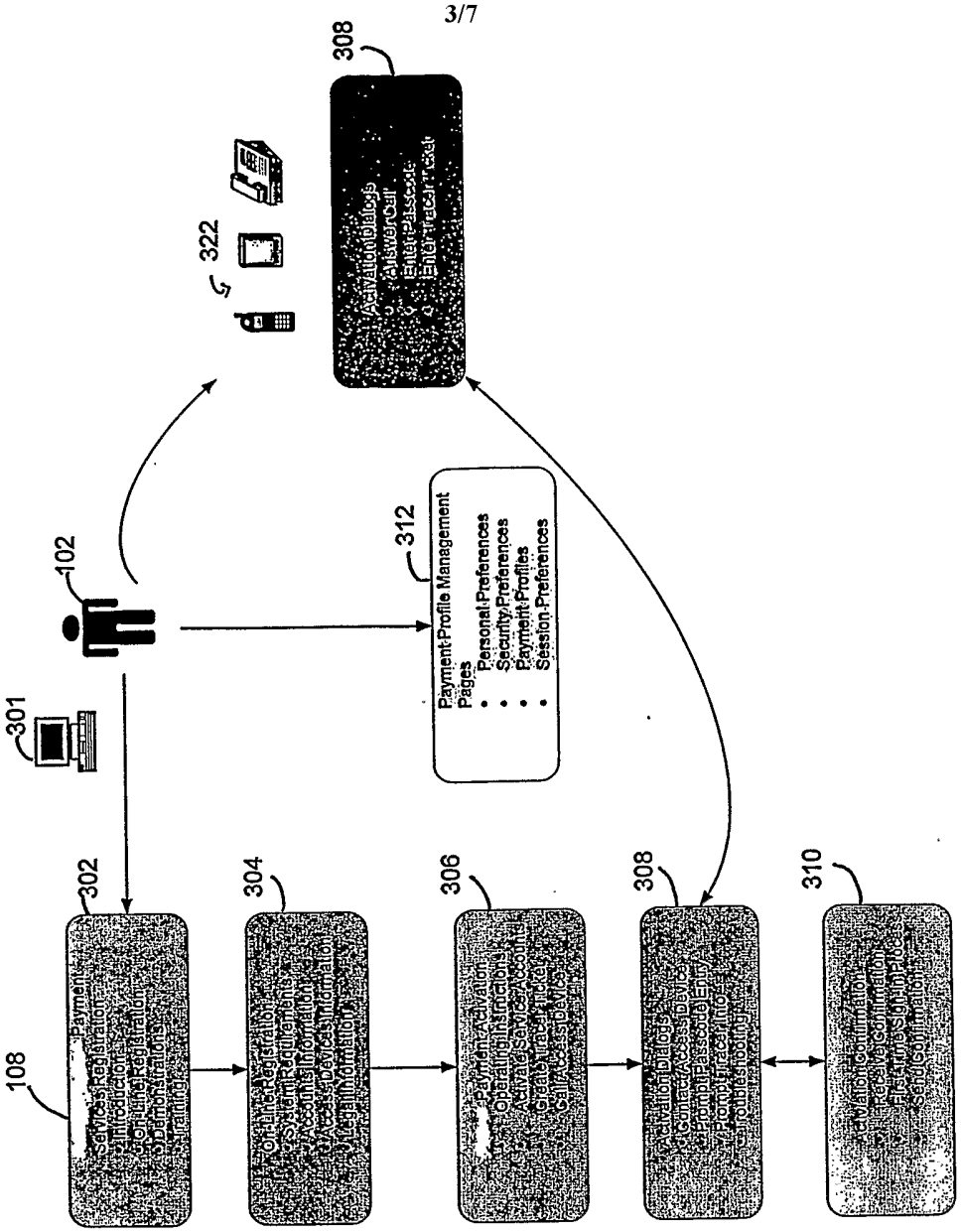

308
322
102
312
Payment Profile Management Pages
Personal Preferences
Security Preferences
Payment Profiles
Session Preferences
301
302
304
306
308
310
108

Figure 3

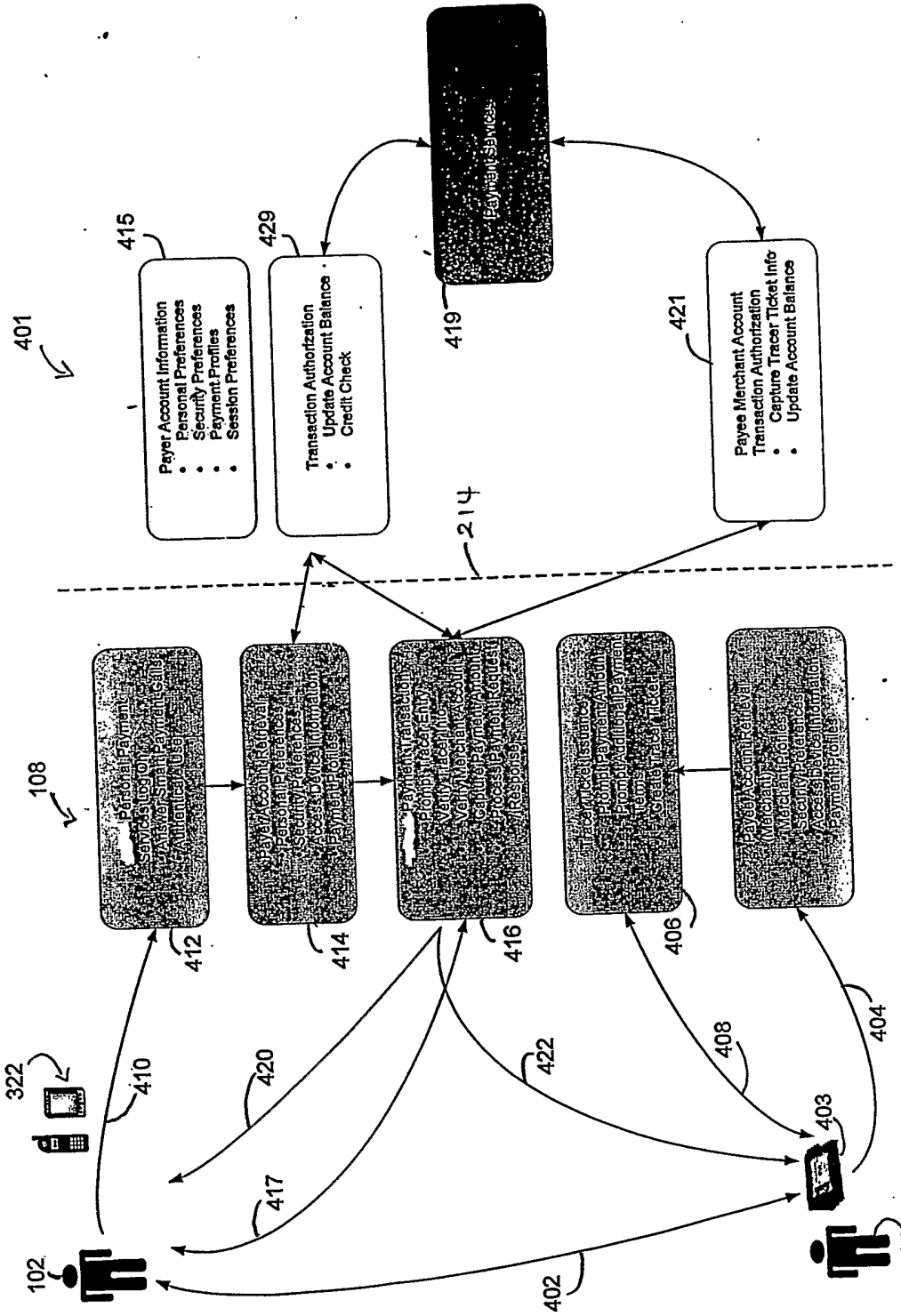

401
415
Payer Account Information
Personal Preferences
Security Preferences
Payment Profiles
Session Preferences
429
Transaction Authorization
Update Account Balance
Credit Check
419
Payment Services
421
Payee Merchant Account
Transaction Authorization
Capture Tracer Ticket Info
Update Account Balance
214
108
412
414
416
406
322
410
420
422
408
404
403
417
102
402
104

Figure 4

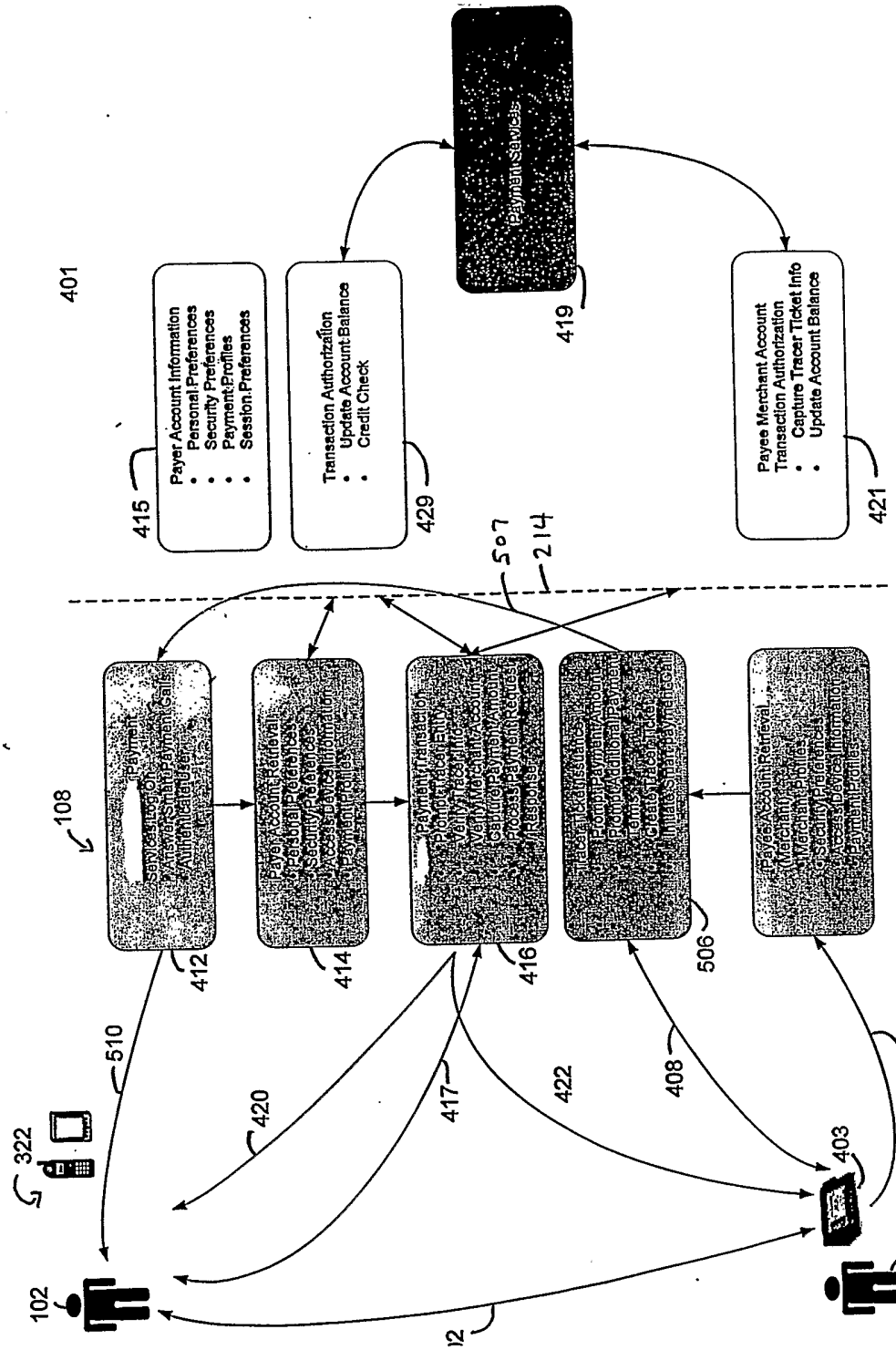

401
Payer Account Information
Personal Preferences
Security Preferences
Payment Profiles
Session Preferences
415
Transaction Authorization
Update Account Balance
Credit Check
429
Payment Services
419
Payee Merchant Account
Transaction Authorization
Capture Tracer Ticket Info
Update Account Balance
421
507
214
108
412
414
416
506
510
420
417
422
408
404
322
403
102
104
12

Figure 5

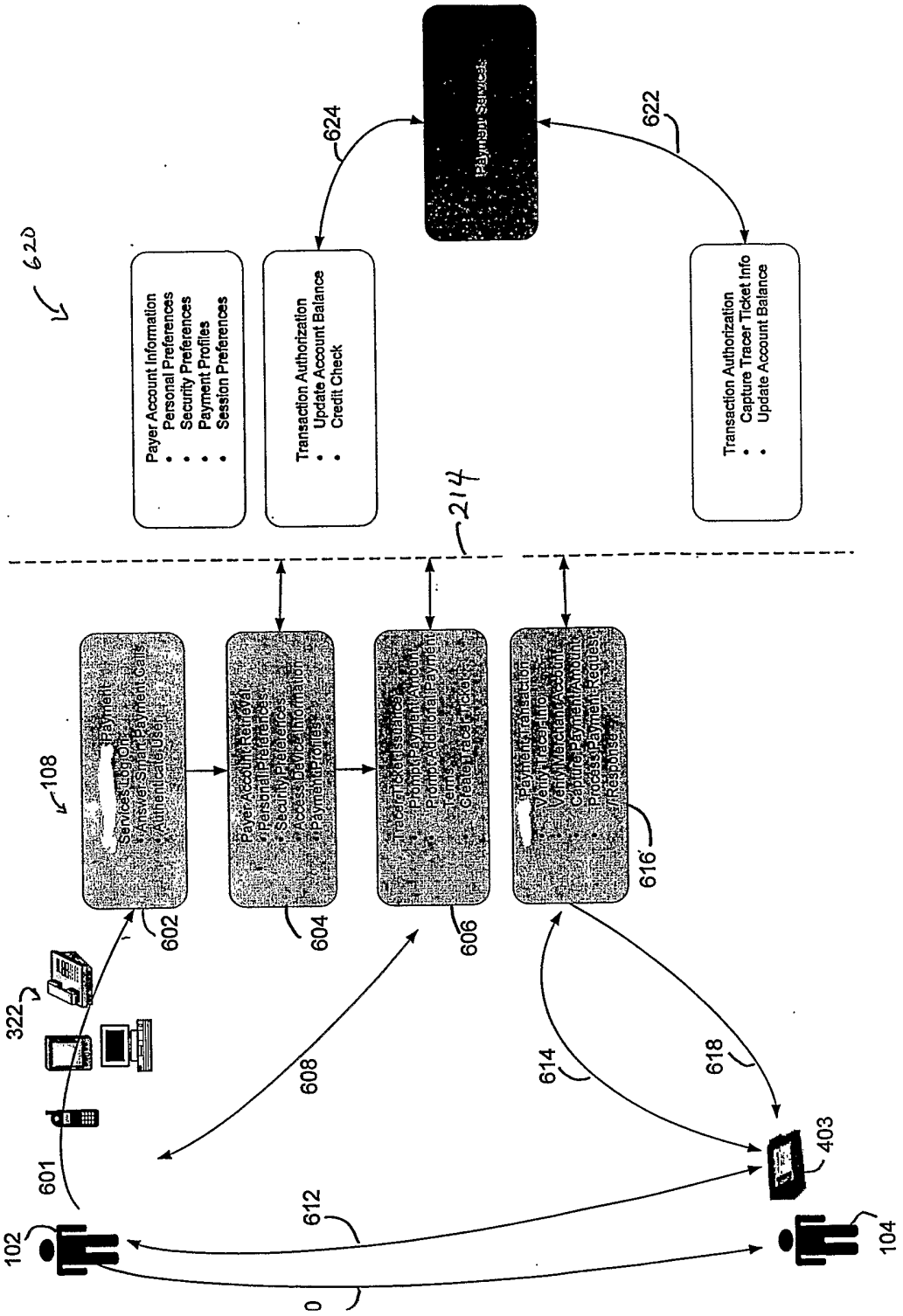

620
624
622
Payer Account Information
Personal Preferences
Security Preferences
Payment Profiles
Session Preferences
Transaction Authorization
Update Account Balance
Credit Check
Transaction Authorization
Capture Tracer Ticket Info
Update Account Balance
214
108
602
604
606
616
322
601
608
614
618
403
612
102
104
0

Figure 6

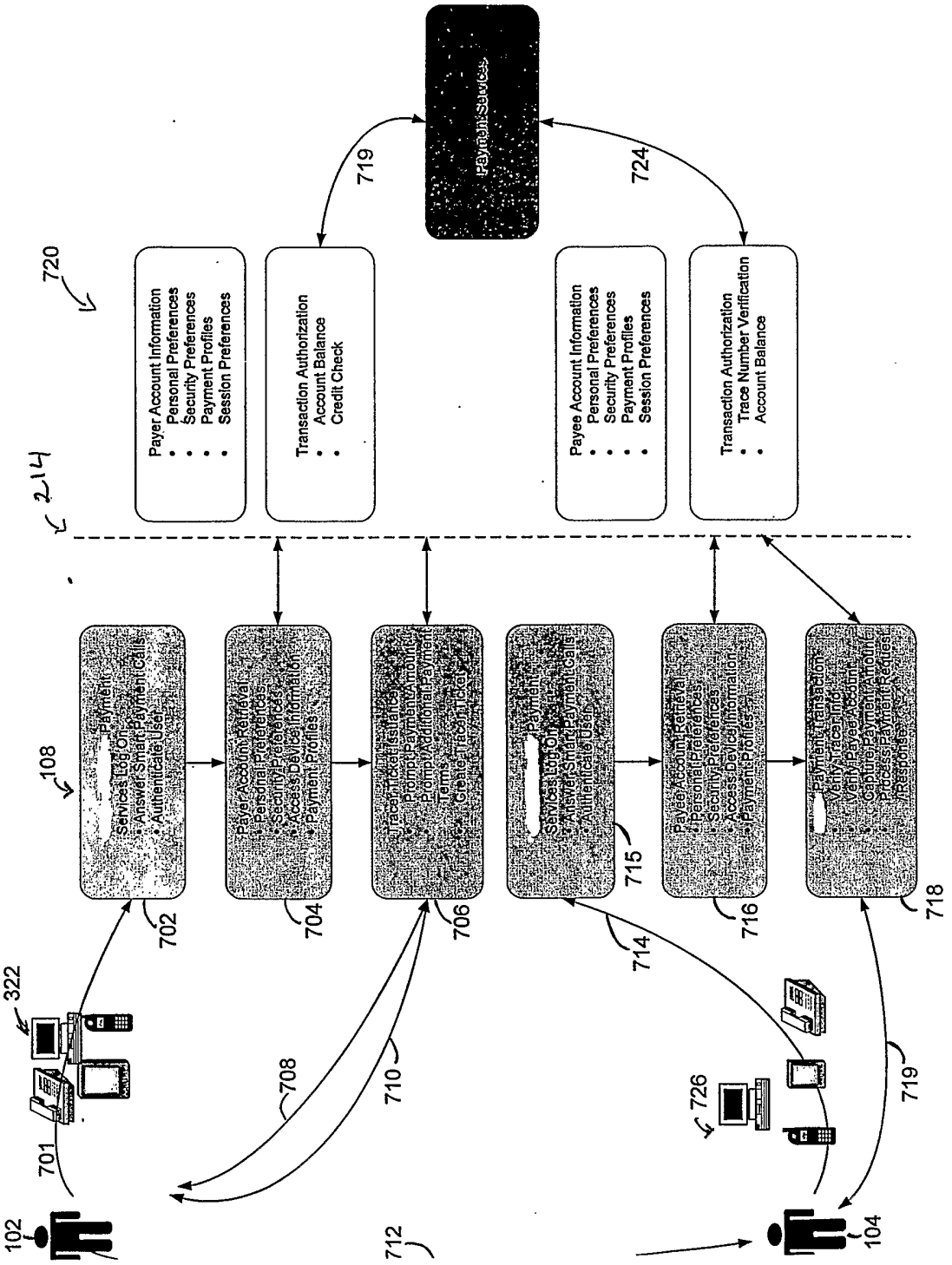

Payment Services
719
724
720
214
Payer Account Information
Personal Preferences
Security Preferences
Payment Profiles
Session Preferences
Transaction Authorization
Account Balance
Credit Check
Payee Account Information
Personal Preferences
Security Preferences
Payment Profiles
Session Preferences
Transaction Authorization
Trace Number Verification
Account Balance
108
702
704
706
715
716
718
714
322
701
102
708
710
712
726
719
104

Figure 7