



**(43) International Publication Date**  
**31 December 2008 (31.12.2008)**

**(10) International Publication Number**  
**WO 2009/001355 A2**

- |                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>(51) International Patent Classification:</b><br><i>G06Q 30/00</i> (2006.01)                                                                                                             | <b>(81) Designated States</b> ( <i>unless otherwise indicated, for every kind of national protection available</i> ): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW. |
| <b>(21) International Application Number:</b><br>PCT/IL2008/000869                                                                                                                          | <b>(84) Designated States</b> ( <i>unless otherwise indicated, for every kind of regional protection available</i> ): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).                                                                                                            |
| <b>(22) International Filing Date:</b> 25 June 2008 (25.06.2008)                                                                                                                            | <b>Published:</b><br>— <i>without international search report and to be republished upon receipt of that report</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>(25) Filing Language:</b> English                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>(26) Publication Language:</b> English                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>(30) Priority Data:</b><br>60/945,951 25 June 2007 (25.06.2007) US                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>(71) Applicants and</b><br><b>(72) Inventors:</b> SALOMON, Yosef [IL/IL]; 5 Avrech Yeshay-hoo St., 69080 Tel Aviv (IL). TAMIR, Eran [IL/IL]; 11 Vinik Street, 75241 Rishon Le Zion (IL). |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>(74) Agents:</b> EITAN-MEHULAL LAW GROUP et al.; P.O. Box 2081 Industrial Zone, 46120 Herzlia (IL).                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**(54) Title:** DEVICE, SYSTEM, AND METHOD OF PROTECTED PURCHASING

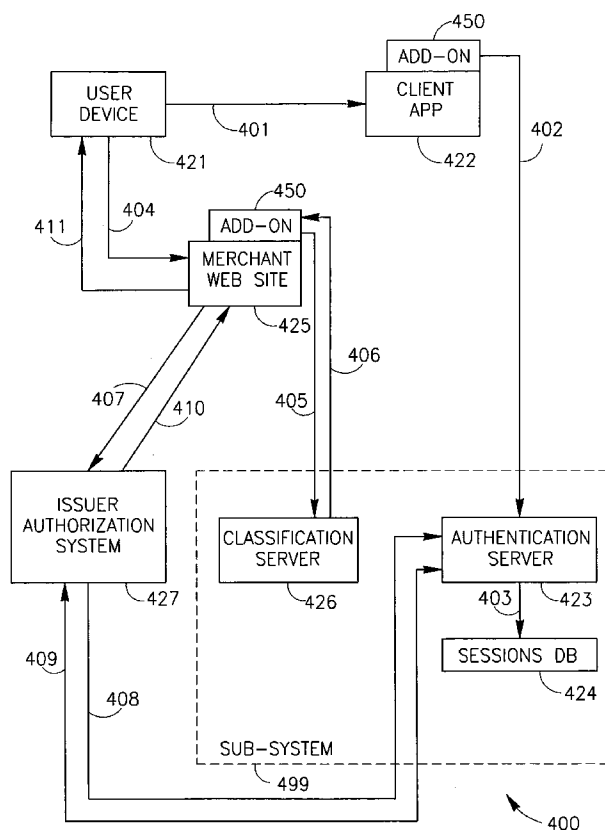


FIG. 4

**(57) Abstract:** Device, system, and method of protected purchasing. For example, a method for protected purchasing of items via a communication network having a server, the method including: receiving at the server a request from a user to purchase an item; based on a profile of the user, determining whether or not the item is approved for purchase by the user; and if the item is approved for purchase by the user, allowing processing of a transaction to purchase the item by the user.

## **DEVICE, SYSTEM, AND METHOD OF PROTECTED PURCHASING**

### **PRIOR APPLICATION DATA**

[001] This patent application claims benefit and priority of United States Provisional Patent Application Number 60/945,951, titled "Device, System, and Method of Protected Purchasing", filed on June 25, 2007, which is hereby incorporated by reference in its entirety.

### **FIELD**

[002] Some embodiments are related to the field of performing commercial transactions, for example, using online and offline commerce systems.

### **BACKGROUND**

[003] Some electronic communication systems allow users to engage in electronic commerce ("e-commerce"). For example, a user may utilize a Personal Computer (PC) connected to the Internet in order to purchase various products from a web-site of a merchant. The user may pay for the purchased products by entering his credit card details; and the purchased products are shipped by the merchant to a shipping address provided by the user.

[004] A user who is a parent may allow his child to utilize the parent's credit card in order to purchase online various products, for example, movies, books, or video games. Unfortunately, the unsupervised child may purchase online products that are inappropriate for children, or products that the parent does not approve of, for example, movies or video games that include violent content or sexual content.

### **SUMMARY**

[005] Some embodiments include, for example, devices, systems, and methods of protected purchasing.

[006] Some embodiments include, for example, a method for protected purchasing of items via a communication network having a server; and the method includes: receiving at the server a request from a user to purchase an item; based on a profile of the user, determining whether or not the item is approved for purchase by the user; and if the item is approved for purchase by the user, allowing processing of a transaction to purchase the item by the user.

[007] In some embodiments, the method includes: if the item is unapproved for purchase by the user, disallowing processing of the transaction to purchase the item by the user, and removing a visual representation of the item from a group of one or more visual representations of items available for purchase by the user.

[008] In some embodiments, disallowing includes: blocking submission of transaction data to a payment authorization system.

[009] In some embodiments, the profile of the user includes one or more lists selected from the group consisting of: a list of items that are pre-approved for purchase by the user; a list of items that are restricted for purchase by the user; a list of categories of items that are pre-approved for purchase by the user; and a list of categories of items that are restricted for purchase by the user.

[0010] In some embodiments, the profile of the user is based on an input received from a supervising user, wherein the supervising user is authorized to modify the user profile, and wherein the user is unauthorized to modify the user profile.

[0011] In some embodiments, the method includes: classifying the item as allowed for purchase or disallowed for purchase, based on a category to which the item belongs.

[0012] In some embodiments, the method includes: classifying the item as allowed for purchase or disallowed for purchase, based on a content of the item.

[0013] In some embodiments, the method includes: checking whether or not the user is authenticated, based on a query to a database able to store session identifiers or authenticated users; and if the user is unauthenticated, disallowing processing of the transaction to purchase the item by the user.

[0014] In some embodiments, receiving the request includes receiving the request through an Internet web-site.

[0015] In some embodiments, receiving the request includes receiving the request through a point-of-sale terminal.

[0016] Some embodiments include, for example, a system for protected purchasing of items via a communication network; and the system includes: a classification server to receive a request from a user to purchase an item; to determine, based on a profile of the user, whether or not the item is approved for purchase by the user; and if the item is approved for purchase by the user, to allow processing of a transaction to purchase the item by the user.

[0017] In some embodiments, if the item is unapproved for purchase by the user, the classification server is to generate output indicating to disallow processing of the transaction to purchase the item by the user and to remove a visual representation of the item from a group of one or more visual representations of items available for purchase by the user.

[0018] In some embodiments, the classification server is to generate output indicating to block submission of transaction data to a payment authorization system.

[0019] In some embodiments, the profile of the user includes one or more lists selected from the group consisting of: a list of items that are pre-approved for purchase by the user; a list of items that are restricted for purchase by the user; a list of categories of items that are pre-approved for purchase by the user; and a list of categories of items that are restricted for purchase by the user.

[0020] In some embodiments, the profile of the user is based on an input received from a supervising user, wherein the supervising user is authorized to modify the user profile, and wherein the user is unauthorized to modify the user profile.

[0021] In some embodiments, the classification server is to classify the item as allowed for purchase or disallowed for purchase, based on a category to which the item belongs.

[0022] In some embodiments, the classification server is to classify the item as allowed for purchase or disallowed for purchase, based on a content of the item.

[0023] In some embodiments, the system includes: an authentication server to check whether or not the user is authenticated, based on a query to a database able to store session identifiers or authenticated users; and if the user is unauthenticated, to disallow processing of the transaction to purchase the item by the user.

[0024] In some embodiments, the classification server is to receive the request through an Internet web-site.

[0025] In some embodiments, the classification server is to receive the request through a point-of-sale terminal.

[0026] Some embodiments may include, for example, a computer program product including a computer-useable medium including a computer-readable program, wherein the computer-readable program when executed on a computer causes the computer to perform methods in accordance with some embodiments of the invention.

[0027] Some embodiments may provide other and/or additional benefits and/or advantages.

### BRIEF DESCRIPTION OF THE DRAWINGS

[0028] For simplicity and clarity of illustration, elements shown in the figures have not necessarily been drawn to scale. For example, the dimensions of some of the elements may be exaggerated relative to other elements for clarity of presentation. Furthermore, reference numerals may be repeated among the figures to indicate corresponding or analogous elements. The figures are listed below.

[0029] Figures 1-6 are schematic block diagram illustrations of systems for protected purchasing, in accordance with some demonstrative embodiments of the invention.

### DETAILED DESCRIPTION

[0030] In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of some embodiments of the invention. However, it will be understood by persons of ordinary skill in the art that some embodiments may be practiced without these specific details. In other instances, well-known methods, procedures, components, units and/or circuits have not been described in detail so as not to obscure the discussion.

[0031] The terms “plurality” or “a plurality” as used herein include, for example, “multiple” or “two or more”. For example, “a plurality of items” includes two or more items.

[0032] Although portions of the discussion herein relate, for demonstrative purposes, to wired links and/or wired communications, some embodiments are not limited in this regard, and may include one or more wired or wireless links, may utilize one or more components of wireless communication, may utilize one or more methods or protocols of wireless communication, or the like. Some embodiments may utilize wired communication and/or wireless communication.

[0033] Some embodiments may be used in conjunction with various devices and systems, for example, a Personal Computer (PC), a desktop computer, a mobile computer, a laptop computer, a notebook computer, a tablet computer, a server computer, a handheld computer, a handheld device, a Personal Digital Assistant (PDA) device, a handheld PDA device, an on-board device, an off-board device, a hybrid device (e.g., a device incorporating functionalities of multiple types of devices, for example, PDA functionality and cellular phone functionality), a vehicular device, a non-vehicular device, a mobile or portable device, a non-mobile or non-portable device, a wireless communication station, a wireless communication device, a wireless Access Point (AP), a wireless Base Station (BS), a Mobile Subscriber Station (MSS), a wired or wireless Network

Interface Card (NIC), a wired or wireless router, a wired or wireless modem, a wired or wireless network, a Local Area Network (LAN), a Wireless LAN (WLAN), a Metropolitan Area Network (MAN), a Wireless MAN (WMAN), a Wide Area Network (WAN), a Wireless WAN (WWAN), a Personal Area Network (PAN), a Wireless PAN (WPAN), devices and/or networks operating  
5 in accordance with existing IEEE 802.11, 802.11a, 802.11b, 802.11g, 802.11n, 802.16, 802.16d, 802.16e, 802.16m standards and/or future versions and/or derivatives of the above standards, units and/or devices which are part of the above networks, one way and/or two-way radio communication systems, cellular radio-telephone communication systems, a cellular telephone, a wireless telephone, a Personal Communication Systems (PCS) device, a PDA device which  
10 incorporates a wireless communication device, a mobile or portable Global Positioning System (GPS) device, a device which incorporates a GPS receiver or transceiver or chip, a device which incorporates an RFID element or tag or transponder, a device which utilizes Near-Field Communication (NFC), a Multiple Input Multiple Output (MIMO) transceiver or device, a Single Input Multiple Output (SIMO) transceiver or device, a Multiple Input Single Output  
5 (MISO) transceiver or device, a device having one or more internal antennas and/or external antennas, a "smartphone" device, a wired or wireless handheld device (e.g., BlackBerry (RTM), Palm (RTM) Treo (TM)), a Wireless Application Protocol (WAP) device, or the like.

[0034] Some embodiments may be used in conjunction with one or more types of wireless communication signals and/or systems, for example, Radio Frequency (RF), Infra Red (IR),  
0 Frequency-Division Multiplexing (FDM), Orthogonal FDM (OFDM), OFDM Access (OFDMA), Time-Division Multiplexing (TDM), Time-Division Multiple Access (TDMA), Extended TDMA (E-TDMA), General Packet Radio Service (GPRS), extended GPRS, Code-Division Multiple Access (CDMA), Wideband CDMA (WCDMA), CDMA 2000, Multi-Carrier Modulation (MDM), Discrete Multi-Tone (DMT), Bluetooth (RTM), Global Positioning System  
5 (GPS), IEEE 802.11 ("Wi-Fi"), IEEE 802.16 ("Wi-Max"), ZigBee (TM), Ultra-Wideband (UWB), Global System for Mobile communication (GSM), 2G, 2.5G, 3G, Third Generation Partnership Project (3GPP), 3GPP Long Term Evolution (LTE), 3.5G, or the like. Some embodiments may be used in conjunction with various other devices, systems and/or networks.

[0035] The terms "wireless device" or "wireless computing device" as used herein include, for  
0 example, a device capable of wireless communication, a communication device or communication station capable of wireless communication, a desktop computer capable of

wireless communication, a mobile phone, a cellular phone, a laptop or notebook computer capable of wireless communication, a PDA capable of wireless communication, a handheld device capable of wireless communication, a portable or non-portable device capable of wireless communication, or the like.

[0036] The terms “web” or “Web” as used herein includes, for example, the World Wide Web; a global communication system of interlinked and/or hypertext documents, files, web-sites and/or web-pages accessible through the Internet or through a global communication network; including text, images, videos, multimedia components, hyperlinks, or other content.

[0037] The term “system” as used herein includes, for example, the a protected online transaction system in accordance with some embodiments

[0038] The term “merchant” as used herein includes, for example, an electronic commerce (“e-commerce”) web site, e.g., “eBay.com”, “Amazon.com”, or the like; and/or an offline commerce establishment or real-world non-virtual site (e.g., an offline store or shop).

[0039] The terms “web site” or “site” as used herein include, for example, a web site of a merchant.

[0040] The term “restricted merchant” as used herein includes, for example, an e-commerce web site that sell products that are by category restricted to the system. For example, if the system provides a protective layer for teenager users, then merchants of sexual materials or firearms are restricted merchants.

[0041] The term “user” as used herein includes, for example, the actual user who utilizes the payment method in order to perform an online purchase. In the example of a system that provides a protective layer for teenagers, the user is a teenager.

[0042] The term “activator” as used herein includes, for example, the initiator of the payment method who creates the user profile and deposits money into it. In the example of a system that provides a protective layer for teenagers, the activator is a parent of the teenager, a supervising user, or the like.

[0043] The terms “client” or “client application” as used herein includes, for example, an application that is installed on the computing device of the user.

[0044] The term “portal” as used herein includes, for example, a portal or interface to the system which performs services such as, for example, creating a new profile for an activator, modifying

details of an existing profile of an activator, viewing statistics or information on usage of an account of an activator, or the like.

[0045] The terms “server” or “server computer” as used herein include, for example, one or more server computer that store the system logic and algorithms and/or process the different requests. In some embodiments, multiple servers may be used, for example: an authentication server for user authentication; a users server to manage the user details (e.g., user profile, statistics regarding the user account, or the like); and a classification server to store algorithms for identifying and classifying products, as well as classified products data.

[0046] The term “issuer” as used herein includes, for example, an issuer or operator of a payment method; for example, a bank of financial institution that issues credit cards or debit cards; an online payment institution (e.g., PayPal); an issuer of a virtual or real-life prepaid card or secured card; or the like.

[0047] The term “authorization system” as used herein includes, for example, a system owned, controlled, or operated by an issuer, the system able to approves or deny a payment transaction placed by a user.

[0048] The terms “Merchant Category Code” or “MCC” as used herein include, for example, a code or a number (e.g., a four-digit number) used by the financial services industry or bankcard industry in order to classify merchants.

[0049] The terms “profile” or “user profile” as used herein include, for example, a profile of a user. In some embodiments, the user profile is defined by the activator, and not by the user.

[0050] The terms “online” and “offline” as used herein may refer, for example, to the location of the merchant and/or to the location in which payment takes place. For example, an “online” merchant includes an e-commerce web site; and an “online” payment method includes a payment method performed through a communication network (e.g., the Internet). An “offline” merchant includes, for example, a “brick and mortar” store, a real-life store or a physical store; and an “offline” payment method includes a payment method performed in the real-life store (e.g., physically handing over a credit card, or physically swiping a payment card).

[0051] The terms “card” or “payment card” as used herein includes, for example, a credit card, a debit card, a secured credit card, a secured debit card, a prepaid credit card, a prepaid debit card, a one-time payment card, a payment card that can be refilled or reloaded, a payment card associated with a bank account, a payment card unassociated with a bank account, or the like.



[0052] The term “payment method” as used herein includes, for example, a method of payment utilizing a payment card, a method of payment utilizing an online payment service (e.g., PayPal), a method of payment utilizing a direct debit from a bank account of the purchaser to a bank account of the merchant, or other suitable payment methods.

[0053] As an overview, in some embodiments, a system provides a protective layer on top of existing payment methods. The system is able to identify, before the actual purchase is executed, whether the product intended to be purchased is allowed or prohibited. This identification is done according to a pre-defined user profile, and the result is an approved transaction or a blocked transaction. The system utilizes a pre-authorization content filter, which identifies the product being purchased and matches the product to the user profile before the payment transaction takes place. In some embodiments, for example, the system may be used to allow protect or restricted online purchasing by teenage users; for example, an activator (a parent) may utilize the system to ensure that the user (a child or teenager) is not able to purchase products that include sexual content, violent content, or other content that the parent deems inappropriate.

[0054] In some embodiments, the system allow teenager users and pre-teenager users to use their pocket money in order to purchase on the Internet products that are pre-defined as “safe” for them. The system ensures that the user is not able to purchase any product that does not comply with the user’s pre-defined profile. For example, a teenager’s prepaid card is used by the system, and the system blocks any attempt to purchase alcohol, gambling services, gambling products, and products that contain sexual content or violent content.

[0055] In some embodiment, the system may be used with other implantations in order to restrict or limit the products that can be purchased online. For example, a family card allows families to better set the spending limits and control the family’s budget; a student card is funded by the student’s parents and can be used only for pre-approved purposes (e.g., payment of electricity bills, payment of dorms monthly rent, payment for food); an ecological card or environment-friendly card, which allows the system to block the purchase of non-environment-friendly products or services; and other suitable types of cards or blocking parameters.

[0056] In some embodiments, the system may include multiple components or modules, for example: user authentication module or component; integration with merchants module or component; integration with issuers module or component; client module or component; server

module or component; portal module or component for activating, modifying, and controlling the user account; and a users portal module or component.

[0057] In some embodiments, the system may include or may utilize multiple flows or algorithms, for example: account creation flow; product classification flow; regular transaction flow; session protected transaction flow; enhanced collaboration with merchants flow; and offline transaction flow.

[0058] In some embodiments, a user authentication component or module is used. In order to use the payment method, the user needs to authenticate with the system's authentication server. Upon authentication a unique digital signature is saved in the authentication server. In case of "session protected transaction" (e.g., as described herein with reference to Figure 4), the signature is attached to the shopping cart and is validated by the issuer approval server before approving the transaction. The digital signature has an expiration time, so the user may need to re-authenticate after a certain amount of time.

[0059] In some embodiments, the authentication may be done in one or more methods, for example: a username and password method, in which the user has to insert a fixed password (e.g., a sequence of characters, letters, digits, signs, or the like); a method in which the user has to answer a question selected randomly out of a list of pre-defined security questions; a two-factor authentication, in which the user, in addition to entering a password, needs to insert a token to the computer or computing device, such that even if his password was compromised, a third party may not access his account unless the third party has the physical token as well.

[0060] In some embodiments, each account supported by the system is associated with an activator and one or more users. Each one of them has a different authentication data, and upon authentication has different permissions in the system portal.

[0061] In some embodiments, an integration with merchants component or module is used, utilizing one or more levels of integration, for example, basic integration or enhanced integration.

[0062] The basic level of integration allows the user to use the system as a payment method. It requires the merchant to support the payment method that the system is attached to. For example, the system provides a protective layer on top of credit card, branded by Visa; and all the merchant has to do is to support the Visa payment method in his web site in order to be integrated with the system.

[0063] The enhanced level of integration may be implemented on top of the basic level of integration. The enhanced level of integration allows the merchant to tailor his web site to the specific user. A tailored web site helps to maximize the exposure of relevant products to the specific user. In addition, it may save the user the disappointment while trying to purchase items that do not comply with his profile. In the enhanced level of integration, the merchant may obtain statistical information from the system.

[0064] Additionally or alternatively, the enhanced level of integration may include, for example, receiving recommendations from the system regarding allowed products. For example the user tries to purchase a restricted product; instead of only blocking the purchase of the restricted product, the merchant's web site may ask the system to search for an allowed or pre-approved product which is similar to the required product (if such replacement product exists).

[0065] In some embodiments, in order to have an enhanced integration with the system, a merchant web site may be required to comply with a protocol (e.g., as described herein with reference to Figure 5). For example, a merchant ID and authentication identifier are used; this information is issued by the system in a manual procedure which identifies the merchant. Then the user is authenticated against the system authentication server; this protocol allows a merchant to identify a user in the merchant internal database by using the system authentication server. After the authentication, the merchant web site may query on a specific user profile from the system user's server. The protocol to query about the user's profile allows a web site to query the user's profile, for example, whether or not the user is allowed to purchase a category of products, or a specific product.

[0066] In some embodiments, the actual purchase using the system and the classification of products may be performed using the client, and may not require specific integration from the merchant, e.g., except for supporting the relevant payment method(s). In some embodiments, the flow of the actual purchase may be in accordance with "regular transaction" and "session protected transaction", e.g., as discussed herein with reference to Figures 3 and 4, respectively.

[0067] In some embodiments, an integration with issuers component or module may be used, for example, for system integration with credit card issuers and other card issuers. The integration with the issuer may be performed in two phases, for example, creation of an account, and actual payment transaction.

[0068] In the first phase, namely, account creation (e.g., as described herein with reference to Figure 1), while creating a new account, there are several information details that the activator needs to provide. For example, the activator may set payment details: the amount of money that he wants to charge into the new account; and how he selects to do that (for example, to charge his credit card, to use a wire transfer, to send a check by mail, or the like). Furthermore, the Activator may set the account profile both in terms of spending limitation and content limitation. The issuer portal transfers that data, after the account creation, to the system's server. The system server sends a password in exchange for that data, so that the Activator may start using the account. For example, in the implementation of a teenager's prepaid card, the activator (parent) needs to set the spending limitation (e.g., monthly, weekly, and/or daily), as well as the content limitation (e.g., no sexual content, no video games, or the like).

[0069] In the second phase, namely, payment transaction, two types of transaction integration may be available for issuers: a regular transaction (e.g., as described herein with reference to Figure 3), and a session protected transaction (e.g., as described herein with reference to Figure 4).

[0070] In the case of a regular transaction, there is no need for additional integration, since the system performs pre-transaction content filtering and then the transaction continues (e.g., if the product purchase is not blocked); accordingly, the card is being charged similarly to an ordinary credit card; other suitable payment methods may be used.

[0071] In the case of a session protected transaction, there is integration between the issuer and the system in the approval phase of the transaction. In the approval phase the issuer's authorization system checks the transaction for fraud, balance in the account, and other parameters. The issuer's authorization system checks with the system whether or not this specific account already authenticated, and whether or not this transaction was scanned and approved by the system's classification server. If the transaction was approved by the system, then the issuer authorization system approves the transaction; alternatively, the issuer authorization system blocks the transaction. In the integration utilizing session protected transaction, if the user did not authenticate against the system, he is not able to execute the actual purchase; thereby decreasing the fraud on the system. In some embodiments, the integration utilizing session protected transaction operates as a safety check, to ensure that the user did not bypass the system.

[0072] In some embodiments, a client component or module may be used. The client includes a software application running on the user's computing device. The client has two main functionalities: to initiate the authentication, and to identify merchant web sites and products.

[0073] With respect to initiation of the authentication, when starting to use the system, the user may activate the client and the user is prompted to authenticate. The client takes the authentication information and pass it securely (e.g., using SSL) to the system authentication server. In case the authentication succeeded, it returns the user profile.

[0074] With respect to identifying merchant web sites and products, the client is hooked to the user's browser and checks the URL that the user is browsing into. If it is a merchant site, the client identifies this case and sends the information to the system classification server. The classification server determines whether or not this site is allowed or not. Then, in allowed sites, the client may operate to identify each product and send it to the system server for classification. In some embodiments, once the product is classified, the client adds a visual and/or other (e.g., audible) notification of the analysis result, in order to convey to the user the classification results.

For example, a visual icon stating that the product is allowed for purchase by this user (namely, pre-approved for purchase) may be added in proximity to the product's name or description. In contrast, if a product is restricted from being purchased by the user (namely, may not be purchased by the user), an icon may indicate the restriction, or the client may remove any visual reference to the product. If the product is restricted, then the client may block the option of adding the product to the shopping cart; or may actively remove the product from the shopping cart if, for example, the classification took place after the product was added to the shopping cart

[0075] In some embodiments, the client may be implemented as an add-on or plug-in or extension to the user's web browser, for example, that needs to be downloaded and/or installed. In other embodiments, the system may utilize a client-less implementation; for example, users who do not wish to install an add-on application may navigate to a specific portal that replaces the client functionality, and from that portal they may navigate to merchant web sites. For demonstrative purposes, some of the Figures may include an add-on client, although other suitable implementations may be used.

[0076] In some embodiments, one or more system servers may be used, for example, an authentication server, a users server, and a classification server.

[0077] The authentication server performs user authentication; and manages the revocation lists in case the system identifies a user who tries to bypass the system or is suspended for various reasons. Each authentication has an expiration time. The authentication server may ask the user to re-authenticate if the expiration time elapses.

5 [0078] The users server stores information about the users, for example, account details, user profile, list of products purchased by a user, and other data relevant for managing the user account.

[0079] The classification server may classify products in substantially real time. The classification information may be stored in a products database, for example, in order to provide  
0 quicker answer starting from the second time that a particular product is queried. The actual classification may be performed using one or more filters that screen the product in a workflow. The filters may include, for example, web sites black lists, web sites white lists, text mining algorithms, advanced Natural Language Processing (NLP) algorithms, and image analysis algorithms.

5 [0080] In some embodiments, for example, black list of blocked web sites, and/or a white list of approved web sites, may be used, optionally utilizing MCCs. For example, in an implementation for a teenager card, any web site with MCC associated with pornography or gambling is automatically added to the black list. Additionally, the activator may manually add specific web sites to the user's black list or white list.

0 [0081] The text mining algorithms, for example, Text Frequency / Inverse Document Frequency (TF/IDF) algorithms, may check for number of occurrences of keywords and the value of each keyword in order to determine whether a product is allowed or restricted. The advanced NLP algorithms may operate on the products that the system has no certain determination about, e.g., resulted from using other filters. In some embodiments, the image analysis algorithms may be  
5 used, for example, to classify a product having an insufficient textual description; the classification server performs image analysis scan on the product image in order to obtain additional information to be used for product classification.

[0082] Some embodiments may utilize a portal for activating and controlling the user account, e.g., as described herein with reference to Figure 1. For example, upon creation of the account,  
0 the activator sets the profile for the user who will use the account for purchases. For each implementation of the system, different categories and values may be set in the account profile.

For example, in the implementation of a teenager card, the profile may include: user name; user gender; user age, or date of birth, or year of birth; user's address; home address or shipping address; method of authentication and an initial password; the initial amount of money available on the teenager card; the payment method to be used; the user profile; and other suitable parameters.

[0083] In some embodiments, the user profile may include, for example: limitations or restrictions on product content, e.g., level of violence or sexuality; limitations or restrictions of product content by classification, e.g., the parent wishes to prevent his child from purchasing computer games; limitations or restrictions on spending, e.g., setting monthly, weekly, and/or daily quota(s); maximum amount of money allowed to be spent in a single transaction; number of transactions allowed to be performed per day, per week, or per month; or the like.

[0084] In some embodiments, the activator may modify the user profile even when the account is active. Additionally, the activator may suspend or cancel the account. The settings may be managed and modified from the system portal. Upon login to the portal, the system identifies whether the logged-in person is an activator or a regular user, and provides access to different functionalities accordingly.

[0085] Some embodiments may utilize a users portal, for example, a platform that allows users and/or activators to obtain statistical and behavioral information about the usage of their account. For example, in the implementation of a teenager card, the user and/or the activator may be able to see information of the user's past purchases, as well as to analyze the personal history of purchases of the user. For example, the statistical analysis may indicate: the categories of products that the user purchased; the spending ratio in the last week or month; the average spending ratio per week or month; or the like. In some embodiments, the statistical information may be obtained using a web browser, a handheld device, a cellular phone, a computer, or the like.

[0086] In some embodiments, the system may be used outside of the e-commerce world, or in the real world, non-virtual world, or "brick and mortar" commerce. For example, integration with issuers may be performed with regard to offline payments. In such case, information about the purchased item(s) is sent to a server by a point-of-sale terminal (or other suitable money transfer device) in a real-world store, and the product information is verified by the profiling engine, e.g., as described herein with reference to Figure 6.

[0087] Figure 1 schematically illustrates a system 100 for protected purchasing, in accordance with some demonstrative embodiments of the invention. For demonstrative purposes, arrows 101-107 demonstrate a flow of account creation within system 100.

[0088] In system 100, an activator utilizes an activator device 121 to navigate to an issuer portal 122, and to request to create an account for a user (arrow 101).

[0089] The activator utilizes the activator device 121 to fill in the details required for creating the account (arrow 102). In some embodiments, the details may include, for example, payment information, budget limitations, and content limitations. The payment information includes, for example, the activator credit card details, the amount of money to deposit into the new account, whether the deposit is one-time or recurring, and the period of time for automatic reloading of deposits into the account. The budget limitations include, for example, limitations on daily spending, weekly spending, monthly spending, spending per product, spending per type of product (e.g., video games), or the like. The content limitations include, for example, limitations on the types of products the user may or may not purchase; e.g., the user is not allowed to purchase products having violent content, products having sexual content, or video games.

[0090] The issuer portal 122 checks whether or not the activator is an existing customer. If the activator is not an existing customer, the issuer portal 122 further checks the activator for fraud (arrow 103), for example, using a third party fraud detector 123, e.g., "The 41st Parameter" fraud detection and prevention solution.

[0091] The issuer portal 122 creates an account in the issuer system, charges the activator, and transfers the money into the created account (arrow 104). The created account is stored in an accounts database 124.

[0092] The issuer portal 122 sends the budget limitations information and the content limitations information to a users server 125 (arrow 105).

[0093] The users server 125 stores the user information in a users database 126 (arrow 106), and creates new passwords for the user and the activator.

[0094] The users server 125 sends back the passwords to the issuer portal 122 (arrow 107), so that the activator and the user may use the passwords.

[0095] In some embodiments, the users server 125 and the users database 126 may be part of a sub-system 199 which may be owned, controlled, operated by a first entity; whereas other



components of system 100 may be owned, controlled, and/or operated by one or more other entities.

[0096] Figure 2 schematically illustrates a system 200 for protected purchasing, in accordance with some demonstrative embodiments of the invention. For demonstrative purposes, arrows 201-207 demonstrate a flow of product classification within system 200.

[0097] In system 200, a user utilizes a user device 221 in order to open or launch a client application 222, through which the user enters user authentication data (arrow 201). The client application 222 may be implemented as a web browser or web navigation software; the client application 222 may include, may be associated with, or may allow utilization of, for example, an add-on 250, e.g., a browser plug-in or extension or add-on, or a web-based portal. Although an add-on component 250 is shown, for demonstrative purposes, other suitable components or modules may be used, for example, a web-based portal which may not necessarily require downloading of software and/or installation of software.

[0098] The add-on 250 sends the authentication data to an authentication server 223 (arrow 202).

[0099] The authentication server 223 attempts to authenticate the user; if the user passes the authentication, a protected session is stored in a sessions database 224 (arrow 203).

[00100] The authenticated user utilizes the user device 221 and the client application 222 in order to navigate to a merchant web site 225 (arrow 204).

[00101] The add-on 250 identifies the merchant web site 225, and sends identifying details of the merchant web site 225 to a classification server 226 for web site classification (arrow 205).

[00102] The classification server 226 checks whether or not the merchant web site 225 is allowed according to the user profile; the classification server 226 sends the response (e.g., allowed web site or restricted web site) back to the add-on 250 (arrow 206).

[00103] If the merchant web site 225 is an allowed web site, then the add-on 250 identifies each product that the user is browsing, and sends the product information to the classification server 226 for product classification (arrow 207).

[00104] The classification server 226 classifies the product and validates it against the user's profile, namely, determines whether or not the user is allowed to purchase this product according to the user's profile. A response (e.g., a binary approval or rejection response) is

returned by the classification server 226 to the add-on 250 (arrow 208), indicating whether a purchase of this product is allowed or blocked.

[00105] If the classification server 226 cannot determine whether or not the specific product is allowed, then, as a default, the specific product is blocked; and an alert is sent by the classification server 226 to an alert log 227 accessible by a system administrator (arrow 209).

[00106] In some embodiments, the authentication server 223, the sessions database 224, the classification server 226, and the alert log 227, may be part of a sub-system 299 which may be owned, controlled, operated by a first entity; whereas other components of system 200 may be owned, controlled, and/or operated by one or more other entities.

[00107] Figure 3 schematically illustrates a system 300 for protected purchasing, in accordance with some demonstrative embodiments of the invention. For demonstrative purposes, arrows 301-309 demonstrate a flow of performing a regular transaction using an account within system 300.

[00108] In system 300, a user utilizes a user device 321 in order to open or launch a client application 322, through which the user enters user authentication data (arrow 301). The client application 322 may be implemented as a web browser or web navigation software; the client application 322 may include, may be associated with, or may allow utilization of, for example, an add-on 350, e.g., a browser plug-in or extension or add-on, or a web-based portal. Although an add-on component 350 is shown, for demonstrative purposes, other suitable components or modules may be used, for example, a web-based portal which may not necessarily require downloading of software and/or installation of software.

[00109] The add-on 350 sends the authentication data to an authentication server 323 (arrow 302).

[00110] The authentication server 323 attempts to authenticate the user; if the user passes the authentication, a protected session is stored in a sessions database 324 (arrow 303).

[00111] The authenticated user utilizes the user device 321 and the client application 322 in order to navigate to a merchant web site 325 (arrow 304).

[00112] The add-on 350 identifies the merchant web site 325, and sends identifying details of the merchant web site 325 to a classification server 326 for web site classification (arrow 305).

[00113] The classification server 326 checks whether or not the merchant web site 325 is allowed according to the user profile; the classification server 326 sends the response (e.g., allowed web site or restricted web site) back to the add-on 350. If the merchant web site 325 is an allowed web site, then the add-on 350 identifies each product that the user is browsing, and sends the product information to the classification server 326 for product classification. The classification server 326 classifies the product and validates it against the user's profile, namely, determines whether or not the user is allowed to purchase this product according to the user's profile. A response (e.g., a binary approval or rejection response) is returned by the classification server 326 to the client application (arrow 306), indicating whether a purchase of this product is allowed or blocked.

[00114] If the product is allowed, the user may utilize the user device 321 to add the allowed product to the user's virtual shopping cart. If the product is not allowed, the add-on 350 blocks the user's ability to add the product to the user's virtual shopping cart.

[00115] The merchant web site 325 sends the user's shopping cart (which includes only allowed products) to an issuer authorization system 327 (arrow 307), where the transaction is validated and either approved or rejected.

[00116] The issuer authorization system 327 sends back to the merchant web site 325 a response indicating approval or rejection of the transaction (arrow 308).

[00117] Accordingly, the user device 321 receives a notification indicating whether the transaction was executed or failed (arrow 309).

[00118] In some embodiments, the authentication server 323, the sessions database 324, and the classification server 326, may be part of a sub-system 399 which may be owned, controlled, operated by a first entity; whereas other components of system 300 may be owned, controlled, and/or operated by one or more other entities.

[00119] Figure 4 schematically illustrates a system 400 for protected purchasing, in accordance with some demonstrative embodiments of the invention. For demonstrative purposes, arrows 401-411 demonstrate a flow of performing a session protected transaction using an account within system 400.

[00120] In system 400, a user utilizes a user device 421 in order to open or launch a client application 422, through which the user enters user authentication data (arrow 401). The client application 422 may be implemented as a web browser or web navigation software; the client

application 422 may include, may be associated with, or may allow utilization of, for example, an add-on 450, e.g., a browser plug-in or extension or add-on, or a web-based portal. Although an add-on component 450 is shown<sup>a</sup>, for demonstrative purposes, other suitable components or modules may be used, for example, a web-based portal which may not necessarily require  
5 downloading of software and/or installation of software.

[00121] The add-on 450 sends the authentication data to an authentication server 423 (arrow 402).

[00122] The authentication server 423 attempts to authenticate the user; if the user passes the authentication, a protected session is stored in a sessions database 424 (arrow 403).

) [00123] The authenticated user utilizes the user device 421 and the client application 422 in order to navigate to a merchant web site 425 (arrow 404).

[00124] The add-on 450 identifies the merchant web site 425, and sends identifying details of the merchant web site 425 to a classification server 426 for web site classification (arrow 405).

5 [00125] The classification server 426 checks whether or not the merchant web site 425 is allowed according to the user profile; the classification server 426 sends the response (e.g., allowed web site or restricted web site) back to the add-on 450. If the merchant web site 425 is an allowed web site, then the add-on 450 identifies each product that the user is browsing, and sends the product information to the classification server 426 for product classification (arrow  
0 405). The classification server 426 classifies the product and validates it against the user's profile, namely, determines whether or not the user is allowed to purchase this product according to the user's profile. A response (e.g., a binary approval or rejection response) is returned by the classification server 426 to the add-on 450 (arrow 406), indicating whether a purchase of this product is allowed or blocked.

5 [00126] If the product is allowed, the user may utilize the user device 421 to add the allowed product to the user's virtual shopping cart. If the product is not allowed, the add-on 450 blocks the user's ability to add the product to the user's virtual shopping cart.

[00127] The merchant web site 425 sends the user's shopping cart (which includes only allowed products) to an issuer authorization system 427 (arrow 407), where the transaction is  
0 validated and either approved or rejected.

[00128] The issuer authorization system 427 queries the authentication server 423 to check whether or not the particular user has an authenticated session (arrow 408). Additionally, the issuer authorization system 427 may check whether the products of the current transaction are allowed or restricted.

[00129] The authentication server 423 sends back to the issuer authorization system 427 a response indicating that the user is authenticated or non-authenticated (arrow 409).

[00130] Accordingly, the issuer authorization system 427 sends back to the merchant web site 425 a response indicating approval or rejection of the transaction (arrow 410); and the user device 421 receives a notification indicating whether the transaction was executed or failed (arrow 411).

[00131] In some embodiments, the authentication server 423, the sessions database 424, and the classification server 426, may be part of a sub-system 499 which may be owned, controlled, operated by a first entity; whereas other components of system 400 may be owned, controlled, and/or operated by one or more other entities.

[00132] Figure 5 schematically illustrates a system 500 for protected purchasing, in accordance with some demonstrative embodiments of the invention. For demonstrative purposes, arrows 501-506 demonstrate a flow of enhanced collaboration with merchants within system 500.

[00133] In system 500, a user utilizes a user device 521 in order to open or launch a client application 522, through which the user enters user authentication data (arrow 501). The client application 522 may be implemented as a web browser or web navigation software; the client application 522 may include, may be associated with, or may allow utilization of, for example, an add-on 550, e.g., a browser plug-in or extension or add-on, or a web-based portal. Although an add-on component 550 is shown, for demonstrative purposes, other suitable components or modules may be used, for example, a web-based portal which may not necessarily require downloading of software and/or installation of software.

[00134] The add-on 550 sends the authentication data to an authentication server 523 (arrow 502).

[00135] The authentication server 523 attempts to authenticate the user; if the user passes the authentication, a protected session is stored in a sessions database 524 (arrow 503).

[00136] The authenticated user utilizes the user device 521 and the client application 522 in order to navigate to a merchant web site 525 (arrow 504).

[00137] The merchant web site 525 has enhanced integration with system 500; accordingly, upon login of the user to the merchant web site 525, the merchant web site sends a query about the user profile to a users server 526 (arrow 505).

[00138] The users server 526 replies by sending back to the merchant web site 525 user's information (arrow 506), for example, fields of interest to the user, categories in which the user is allowed to purchase or is blocked from purchasing, or the like. The user's information may be utilized by the merchant web site 525 in order to tailor the user experience, as well as the products offered to the user, to the user's preferences and purchase restrictions.

[00139] In some embodiments, the actual purchase of a product by a user from a merchant web site 525 may be performed, for example, using flows similar to the flows described with reference to Figures 3 and 4.

[00140] In some embodiments, the authentication server 523, the sessions database 524, and the users server 526, may be part of a sub-system 599 which may be owned, controlled, operated by a first entity; whereas other components of system 500 may be owned, controlled, and/or operated by one or more other entities.

[00141] Figure 6 schematically illustrates a system 600 for protected purchasing, in accordance with some demonstrative embodiments of the invention. For demonstrative purposes, arrows 601-606 demonstrate a flow of an offline transaction utilizing system 600.

[00142] In system 600, a user utilizes a payment article 621, for example, a payment card, at an offline merchant location in order to purchase one or more products. For example, the user may swipe a credit card or a debit card at a Point of Sale (POS) terminal 622 (arrow 601), and may optionally perform other or additional operations, e.g., enter a PIN or code, sign with a pen, sign with an electronic pen, beam or wireless transfer user data or user identity data, or the like.

[00143] The POS terminal 622 sends to an authentication server 623, for example, user authentication information as well as details of the purchased products (arrow 602).

[00144] The authentication server 623 verifies the details of the payment article 621 versus the additional information entered by the user at the POS terminal 622. If the user is identified, the purchase details are sent from the authentication server 623 to a classification server 624 (arrow 603), in order to analyze the purchased products based on the user profile.

[00145] The classification server 624 sends to the authentication server 623 a response indicating approval and/or denial (arrow 604). For example, the response may indicate that all the products that the user attempts to purchased are allowed; the response may indicate that all the products that the user attempts to purchase are denied; or the response may indicate that one or more of the products that the user attempts to purchase are allowed and one or more of the products that the user attempts to purchase are denied.

[00146] The authentication server 623 sends the verification and/or denial information to the POS terminal 622 (arrow 605).

[00147] The POS terminal 622 sends a query to a card issuer authorization system 625, the query representing an attempted purchase of only the products that were approved by the classification server 624 (arrow 606).

[00148] The issuer authorization system 625 sends a query to the authentication server 623, in order to determine whether or not the particular user has an authenticated session and whether or not the products that the user attempts to purchase are approved (arrow 607).

[00149] The authentication server 623 sends a response to the issuer authorization system 625, indicating whether the transaction is approved or denied (arrow 608).

[00150] The issuer authorization system 625 sends a response to the POS terminal 622, indicating whether the transaction is approved or denied (arrow 609).

[00151] In some embodiments, the authentication server 623 and the classification server 626 may be part of a sub-system 699 which may be owned, controlled, operated by a first entity; whereas other components of system 600 may be owned, controlled, and/or operated by one or more other entities.

[00152] In some embodiments, one or more components described herein may be implemented using suitable hardware components and/or software components, for example, a processor, a memory unit, a storage unit, an input unit, an output unit, a wireless or wired communication unit, an Operating System (OS), one or more software applications, or the like.

[00153] Some embodiments may utilize client/server architecture, publisher/subscriber architecture, fully centralized architecture, partially centralized architecture, fully distributed architecture, partially distributed architecture, scalable Peer to Peer (P2P) architecture, or other suitable architectures or combinations thereof.

[00154] Discussions herein utilizing terms such as, for example, “processing,” “computing,” “calculating,” “determining,” “establishing,” “analyzing,” “checking,” or the like, may refer to operation(s) and/or process(es) of a computer, a computing platform, a computing system, or other electronic computing device, that manipulate and/or transform data represented as physical (e.g., electronic) quantities within the computer’s registers and/or memories into other data similarly represented as physical quantities within the computer’s registers and/or memories or other information storage medium that may store instructions to perform operations and/or processes.

[00155] Some embodiments may take the form of an entirely hardware embodiment, an entirely software embodiment, or an embodiment including both hardware and software elements. Some embodiments may be implemented in software, which includes but is not limited to firmware, resident software, microcode, or the like.

[00156] Furthermore, some embodiments may take the form of a computer program product accessible from a computer-usable or computer-readable medium providing program code for use by or in connection with a computer or any instruction execution system. For example, a computer-usable or computer-readable medium may be or may include any apparatus that can contain, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device.

[00157] In some embodiments, the medium may be or may include an electronic, magnetic, optical, electromagnetic, InfraRed (IR), or semiconductor system (or apparatus or device) or a propagation medium. Some demonstrative examples of a computer-readable medium may include a semiconductor or solid state memory, magnetic tape, a removable computer diskette, a Random Access Memory (RAM), a Read-Only Memory (ROM), a rigid magnetic disk, an optical disk, or the like. Some demonstrative examples of optical disks include Compact Disk – Read-Only Memory (CD-ROM), Compact Disk – Read/Write (CD-R/W), DVD, or the like.

[00158] In some embodiments, a data processing system suitable for storing and/or executing program code may include at least one processor coupled directly or indirectly to memory elements, for example, through a system bus. The memory elements may include, for example, local memory employed during actual execution of the program code, bulk storage, and



cache memories which may provide temporary storage of at least some program code in order to reduce the number of times code must be retrieved from bulk storage during execution.

[00159] In some embodiments, input/output or I/O devices (including but not limited to keyboards, displays, pointing devices, etc.) may be coupled to the system either directly or through intervening I/O controllers. In some embodiments, network adapters may be coupled to the system to enable the data processing system to become coupled to other data processing systems or remote printers or storage devices, for example, through intervening private or public networks. In some embodiments, modems, cable modems and Ethernet cards are demonstrative examples of types of network adapters. Other suitable components may be used.

[00160] Some embodiments may be implemented by software, by hardware, or by any combination of software and/or hardware as may be suitable for specific applications or in accordance with specific design requirements. Some embodiments may include units and/or sub-units, which may be separate of each other or combined together, in whole or in part, and may be implemented using specific, multi-purpose or general processors or controllers. Some embodiments may include buffers, registers, stacks, storage units and/or memory units, for temporary or long-term storage of data or in order to facilitate the operation of particular implementations.

[00161] Some embodiments may be implemented, for example, using a machine-readable medium or article which may store an instruction or a set of instructions that, if executed by a machine, cause the machine to perform a method and/or operations described herein. Such machine may include, for example, any suitable processing platform, computing platform, computing device, processing device, electronic device, electronic system, computing system, processing system, computer, processor, or the like, and may be implemented using any suitable combination of hardware and/or software. The machine-readable medium or article may include, for example, any suitable type of memory unit, memory device, memory article, memory medium, storage device, storage article, storage medium and/or storage unit; for example, memory, removable or non-removable media, erasable or non-erasable media, writeable or re-writeable media, digital or analog media, hard disk drive, floppy disk, Compact Disk Read Only Memory (CD-ROM), Compact Disk Recordable (CD-R), Compact Disk Re-Writeable (CD-RW), optical disk, magnetic media, various types of Digital Versatile Disks (DVDs), a tape, a cassette, or the like. The instructions may include any suitable type of code, for example, source

code, compiled code, interpreted code, executable code, static code, dynamic code, or the like, and may be implemented using any suitable high-level, low-level, object-oriented, visual, compiled and/or interpreted programming language, e.g., C, C++, Java, BASIC, Pascal, Fortran, Cobol, assembly language, machine code, or the like.

[00162] Functions, operations, components and/or features described herein with reference to one or more embodiments, may be combined with, or may be utilized in combination with, one or more other functions, operations, components and/or features described herein with reference to one or more other embodiments, or vice versa.

[00163] While certain features of some embodiments have been illustrated and described herein, many modifications, substitutions, changes, and equivalents may occur to those skilled in the art. Accordingly, the following claims are intended to cover all such modifications, substitutions, changes, and equivalents.

## CLAIMS

What is claimed is:

1. A method for protected purchasing of items via a communication network having a server,  
5 the method comprising:  
receiving at the server a request from a user to purchase an item;  
based on a profile of the user, determining whether or not the item is approved for purchase  
by the user; and  
if the item is approved for purchase by the user, allowing processing of a transaction to  
0 purchase the item by the user.
2. The method of claim 1, comprising:  
if the item is unapproved for purchase by the user, disallowing processing of the transaction  
to purchase the item by the user, and removing a visual representation of the item from a  
5 group of one or more visual representations of items available for purchase by the user.
3. The method of claim 2, wherein disallowing comprises:  
blocking submission of transaction data to a payment authorization system.
- 0 4. The method of claim 1, wherein the profile of the user comprises one or more lists selected  
from the group consisting of:  
a list of items that are pre-approved for purchase by the user;  
a list of items that are restricted for purchase by the user;  
a list of categories of items that are pre-approved for purchase by the user; and  
5 a list of categories of items that are restricted for purchase by the user.
5. The method of claim 1, wherein the profile of the user is based on an input received from a  
supervising user, wherein the supervising user is authorized to modify the user profile, and  
wherein the user is unauthorized to modify the user profile.  
0
6. The method of claim 1, comprising:

classifying the item as allowed for purchase or disallowed for purchase, based on a category to which the item belongs.

7. The method of claim 1, comprising:  
classifying the item as allowed for purchase or disallowed for purchase, based on a content of the item.
8. The method of claim 1, comprising:  
checking whether or not the user is authenticated, based on a query to a database able to store session identifiers or authenticated users; and  
if the user is unauthenticated, disallowing processing of the transaction to purchase the item by the user.
9. The method of claim 1, wherein receiving the request comprises receiving the request through an Internet web-site.
10. The method of claim 1, wherein receiving the request comprises receiving the request through a point-of-sale terminal.
11. A system for protected purchasing of items via a communication network, the system comprising:  
a classification server to receive a request from a user to purchase an item; to determine, based on a profile of the user, whether or not the item is approved for purchase by the user; and if the item is approved for purchase by the user, to allow processing of a transaction to purchase the item by the user.
12. The system of claim 11, wherein if the item is unapproved for purchase by the user, the classification server is to generate output indicating to disallow processing of the transaction to purchase the item by the user and to remove a visual representation of the item from a group of one or more visual representations of items available for purchase by the user.

13. The system of claim 12, wherein the classification server is to generate output indicating to block submission of transaction data to a payment authorization system.
- 5 14. The system of claim 11, wherein the profile of the user comprises one or more lists selected from the group consisting of:  
a list of items that are pre-approved for purchase by the user;  
a list of items that are restricted for purchase by the user;  
a list of categories of items that are pre-approved for purchase by the user; and  
0 a list of categories of items that are restricted for purchase by the user.
15. The system of claim 11, wherein the profile of the user is based on an input received from a supervising user, wherein the supervising user is authorized to modify the user profile, and wherein the user is unauthorized to modify the user profile.
- 5 16. The system of claim 11, wherein the classification server is to classify the item as allowed for purchase or disallowed for purchase, based on a category to which the item belongs.
17. The system of claim 11, wherein the classification server is to classify the item as allowed  
0 for purchase or disallowed for purchase, based on a content of the item.
18. The system of claim 11, comprising:  
an authentication server to check whether or not the user is authenticated, based on a query  
to a database able to store session identifiers or authenticated users; and if the user is  
5 unauthenticated, to disallow processing of the transaction to purchase the item by the user.
19. The system of claim 11, wherein the classification server is to receive the request through an Internet web-site.
- 0 20. The system of claim 11, wherein the classification server is to receive the request through a point-of-sale terminal.

1/6

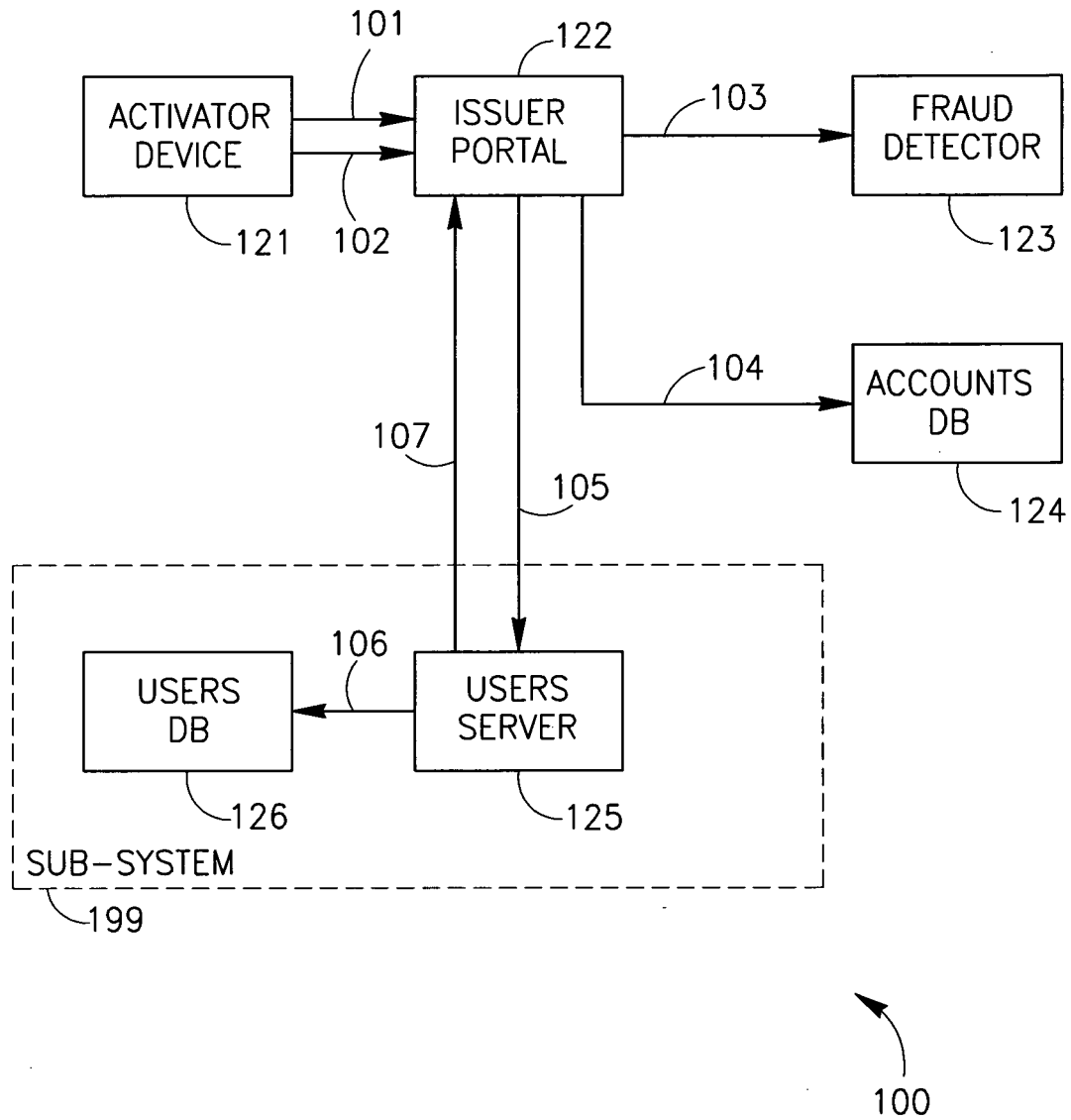


FIG. 1

2/6

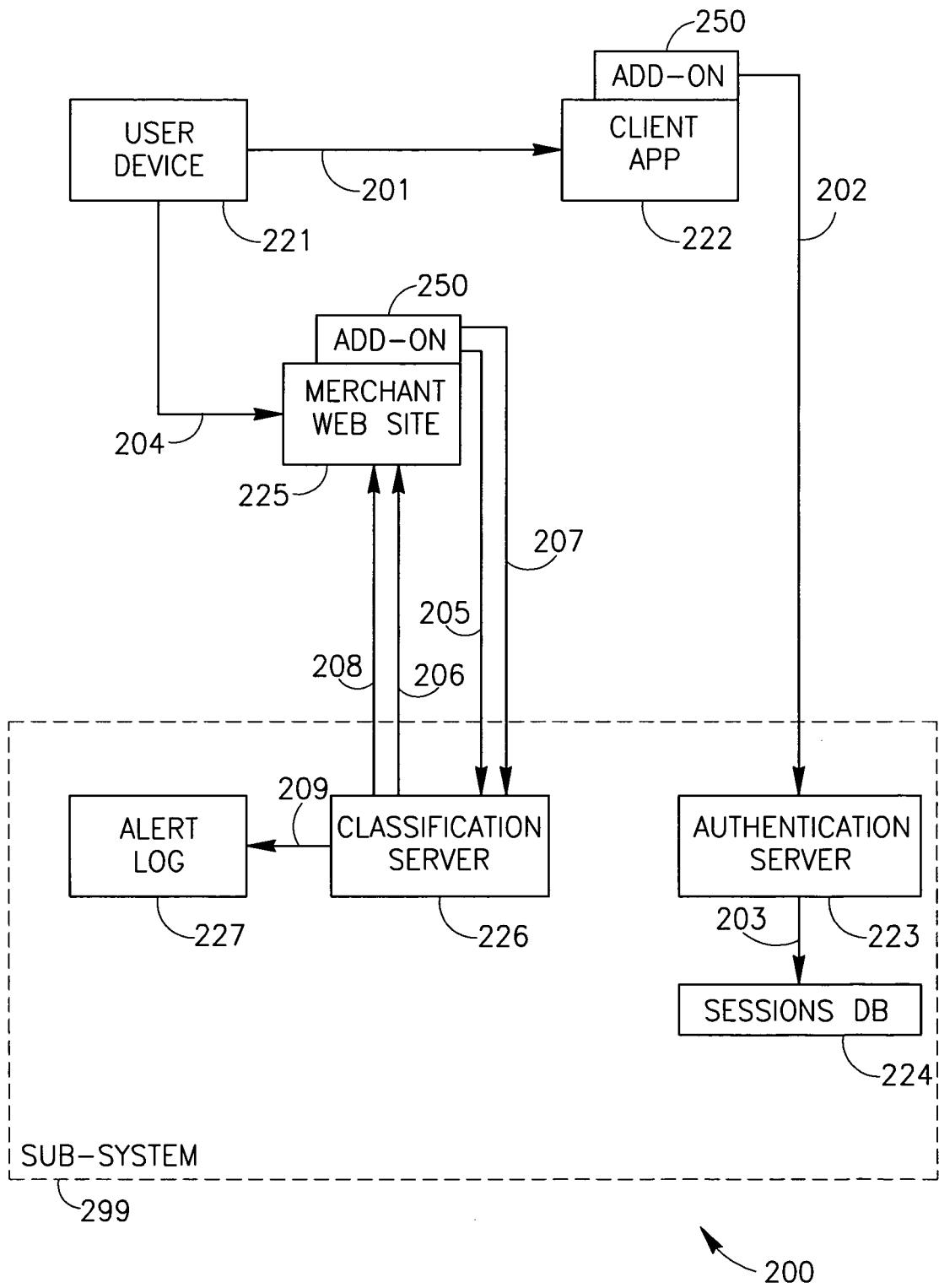


FIG. 2

3/6

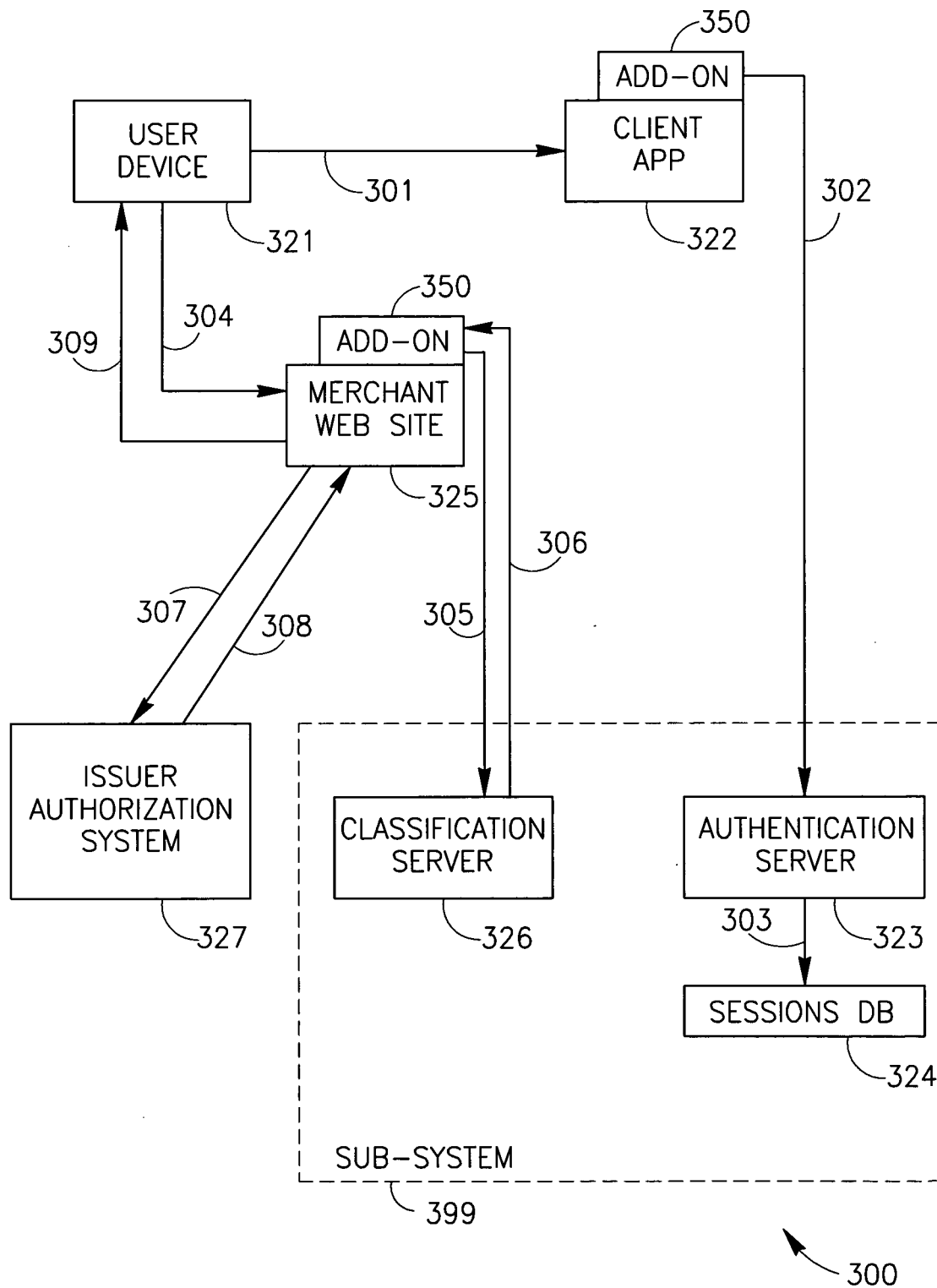


FIG. 3



4/6

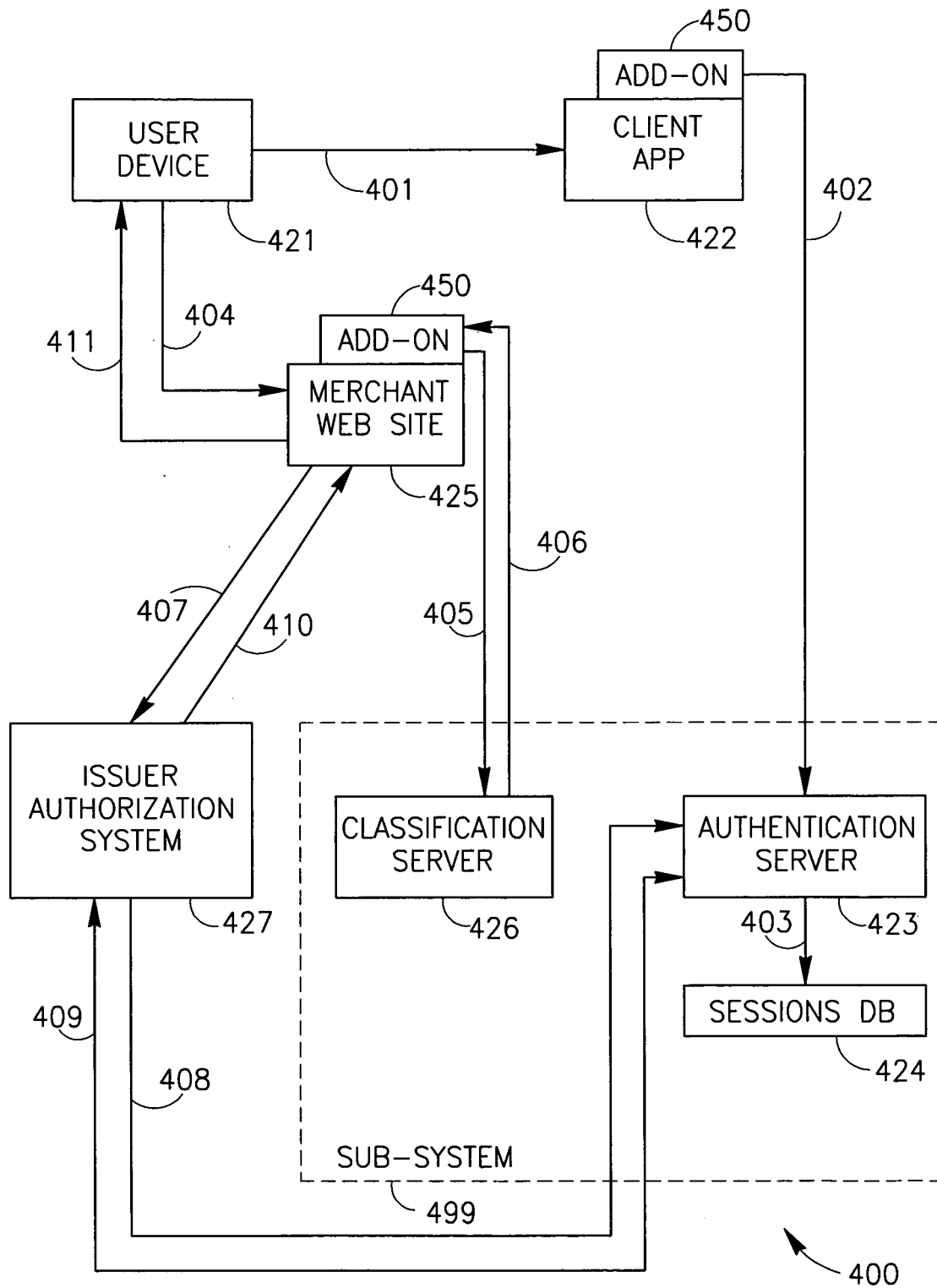


FIG. 4

5/6

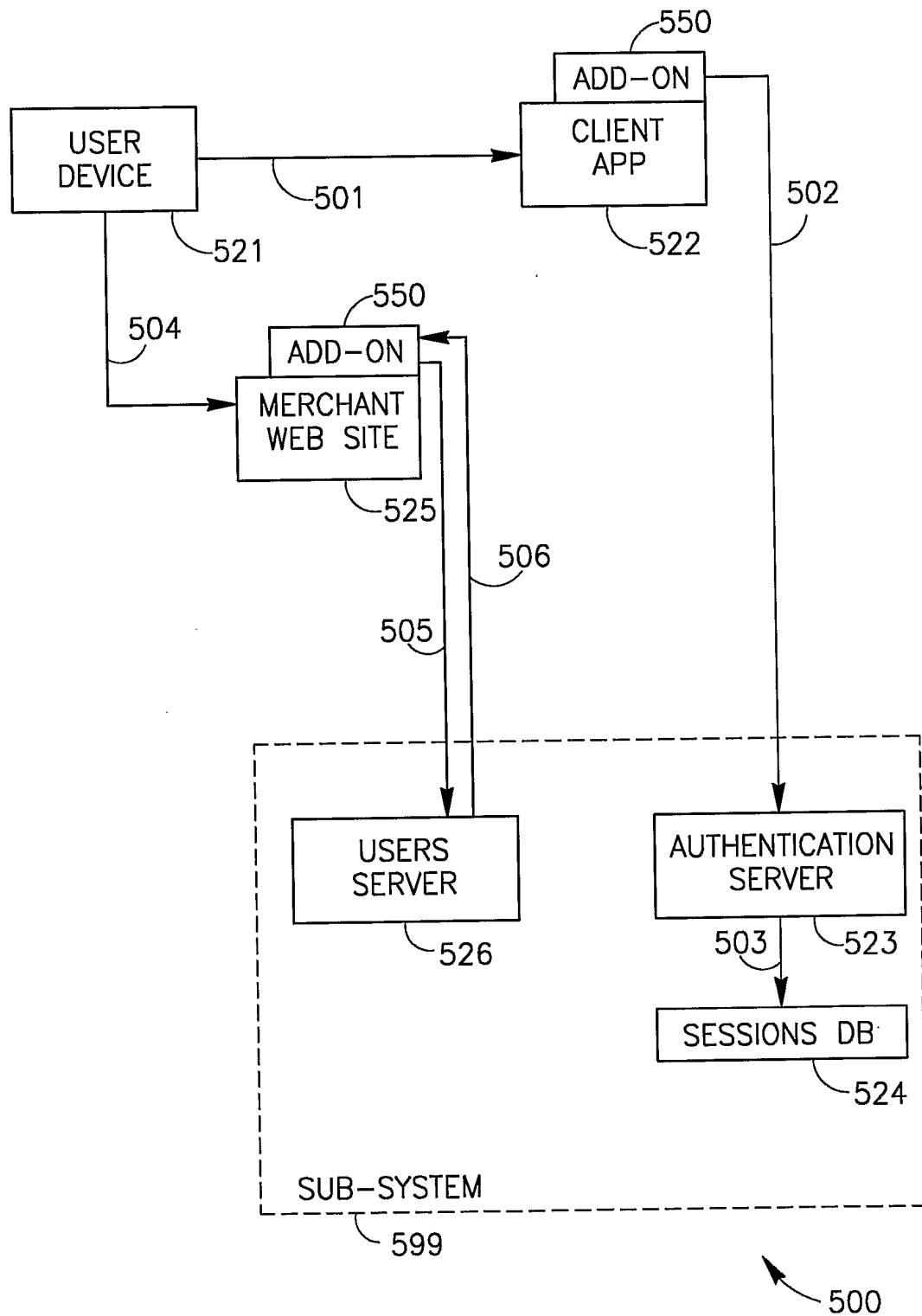


FIG. 5

6/6

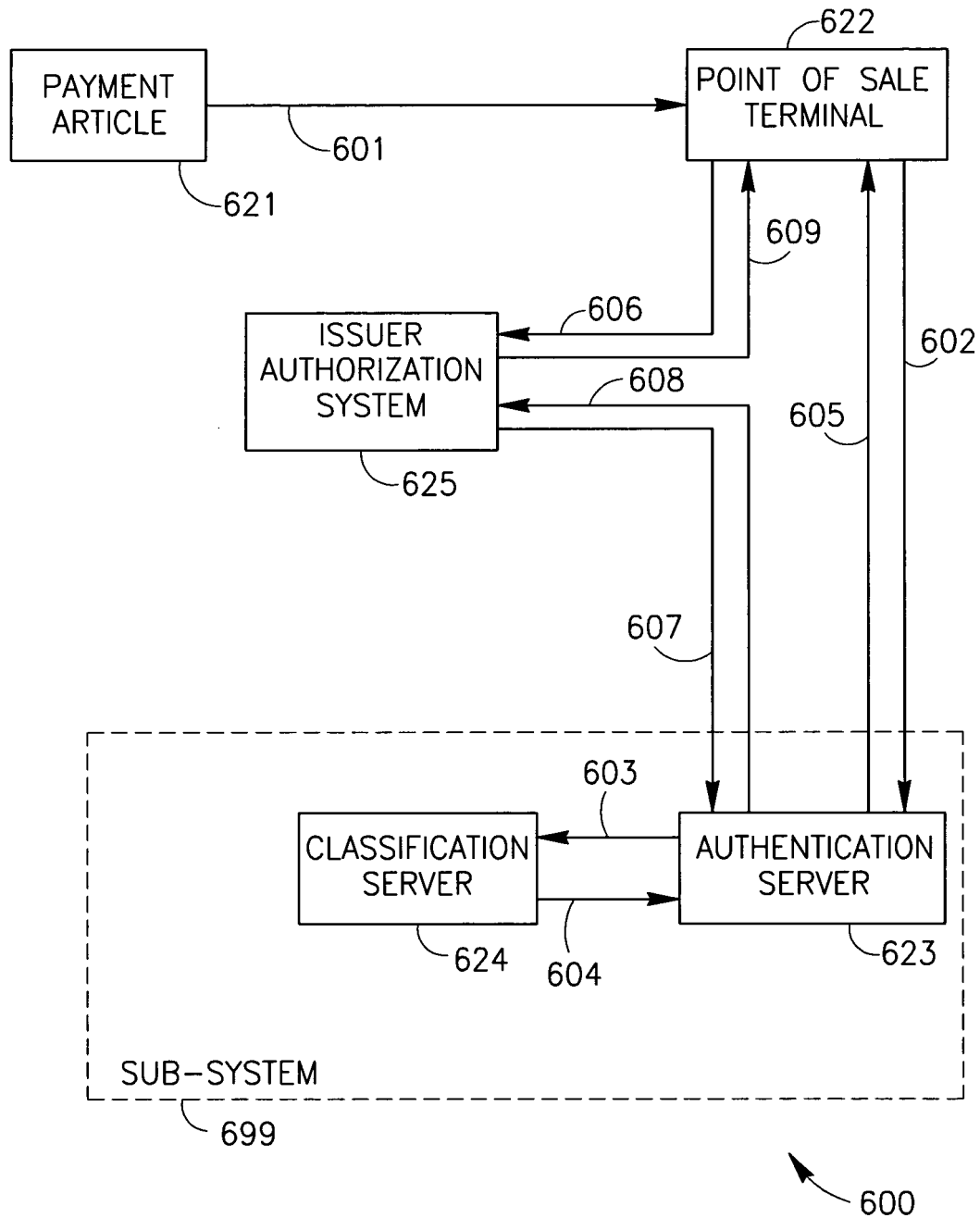


FIG. 6