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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 October 2006 (26.10.2006)

PCT

(10) International Publication Number
WO 2006/113834 A2

(51) International Patent Classification:
G06Q 30/00 (2006.01)

(21) International Application Number:
PCT/US2006/014801

(22) International Filing Date: 19 April 2006 (19.04.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/672,754	19 April 2005 (19.04.2005)	US
11/376,535	15 March 2006 (15.03.2006)	US
11/379,143	18 April 2006 (18.04.2006)	US
11/379,133	18 April 2006 (18.04.2006)	US

(71) Applicant *(for all designated States except US)*: **MICROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, Washington 89052-6399 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **JOHNSON, Bruce, E.** [US/US]; 14150 NE 20th St #108, Bellevue, Washington 98007 (US). **WEBSTER-LAM, Chung** [GB/US]; 1221 1st Ave #815, Seattle, Washington 98101 (US).

(74) Agents: **LEE, Adrian, J.** et al.; WORKMAN NYDEGGER, 1000 Eagle Gate Tower, 60 East South Temple, Salt Lake City, Utah 84111 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

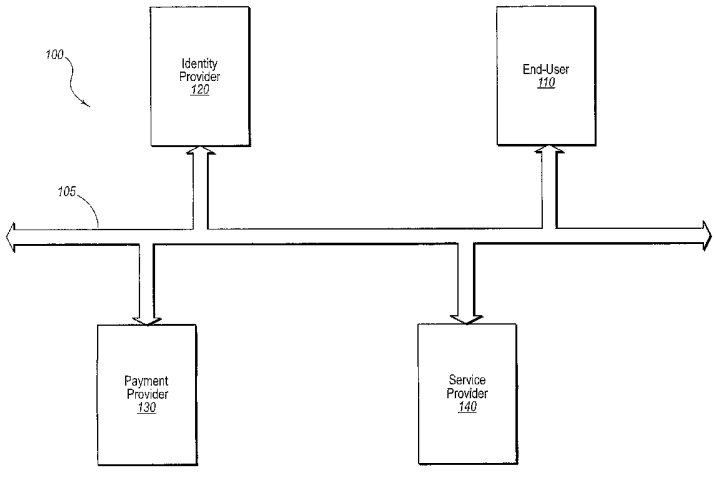
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT,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

Published:

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

[Continued on next page]

(54) Title: NETWORK COMMERCIAL TRANSACTIONS



(57) Abstract: Current embodiments provide for authorization and payment of an online commercial transaction between a purchaser and a merchant including verification of an identity of the purchaser and verification of an ability of the purchaser to pay for the transaction, where the identity provider and the payment provider are often different network entities. Other embodiments also provide for protocols, computing systems, and other mechanisms that allow for identity and payment authentication using a mobile module, which establishes single or multilevel security over an untrusted network (e.g., the Internet). Still other embodiments also provide for a three-way secure communication between a merchant, consumer, and payment provider such that sensitive account information is opaque to the merchant, yet the merchant is sufficiently confident of the consumer's ability to pay for requested purchases. In yet another embodiment, electronic billing information is used for authorization, auditing, payment federation, and other purposes.

WO 2006/113834 A2

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.

NETWORK COMMERCIAL TRANSACTIONS

FIELD OF INVENTION

The present invention relates to networked transaction systems and methods for conducting online transactions.

BACKGROUND

The proliferation of networked computer systems has opened up new possibilities with respect to how corporations and individuals conduct business. For example, end-users connected to a network, (e.g., the Internet), via a networked device such as a computer, PDA, cellular phone, etc., may conduct commercial transactions over the network to purchase services and/or merchandise, conduct financial transactions, or otherwise conduct business or perform personal transactions over the network. An inherent problem linked with online transactions is security, particularly when the transfer of moneys, funds and/or financial, personal or other confidential information is involved in the transaction.

Many conventional online transactions are conducted according to one of two different, but related, models. Both models employ a browser as the interface for handling information transfer between parties involved in the transaction. In the first model, a merchant offers goods or services online via a browser. The term "merchant" refers herein generally to any entity offering goods and/or services for purchase. The term merchant is not used to describe any particular commercial status or to describe a licensed seller, unless specifically stated. Rather, the term describes generically any seller or entity offering good and/or services for purchase or sale. The term service provider is used herein interchangeably with the term merchant and, unless otherwise stated, have the same meaning.

In a conventional online transaction, a merchant may have a website that describes, displays or otherwise offers goods and/or services for sale. An end-user indicates a desire to purchase one or more goods or services, typically by selecting the item via the browser interface. The browser then displays a transaction page that allows the end-user to select one or more payment types and to input information needed to complete the transaction. For example, the transactional page displayed by the browser may permit the end-user to select a payment type, such as credit card (e.g., VISA, MasterCard, American Express, etc.) and to

input transactional information such as credit card number, card expiration date, etc. The transactional page may also query the end-user for personal information such as name, billing address, shipping address, etc. The end-user then submits the information and the merchant processes the submitted information.

In this first model, the merchant typically "owns" the website. That is, the merchant maintains the website, is responsible for the content, and receives and processes the transactional information provided by the end-user. The merchant may establish an account with the end-user before conducting the first transaction and the end-user may then access that account via a user established login and password each time the end-user conducts a transaction with the merchant. That is, the end-user typically chooses a login name and a password to be used in subsequent sessions or transactions. After the end-user has submitted the information queried by the transactional page(s), the merchant processes the information to make sure the information is sufficient to complete the transaction. For example, the merchant may ensure that the credit card number is valid and has sufficient funds to cover the cost of the goods and/or services.

The second model typically includes a third party transaction provider that handles the payment portion of the transaction. The third party forms a relationship with both the end-user and the merchant. In particular, the end-user may establish an account with the third party that can be accessed via a login and password as discussed above. To establish the account, the end-user may provide personal and payment information to the third party (i.e., the end-user may provide personal information identifying the user and payment information such as one or more credit card numbers, expiration dates, etc.) The end-user may also establish an electronic funds account by providing money to the third party transaction provider, the balance of which can be used to purchase online goods and/or services. The third party archives the account information provided by the end-user and/or maintains the end-user's balance.

The third party also establishes a relationship with the merchant, wherein the third party handles the payment processing of the transaction. In particular, the third party agrees to make payments to the merchant when an end-user with an account requests a transfer of funds to make a purchase. The merchant may provide the option of using the third party by

signaling the availability of this option on its website where the goods and services are being sold. For example, when a user visits a merchant's website and decides to make a purchase, the user may then be presented with an option to pay for the purchase using the third party transaction provider.

When the end-user selects the option to pay for the purchase using the third party transaction provider, the end-user's browser is redirected to a website belonging to the third party transaction provider. The end-user then logs into his/her account via the login/password combination and selects a payment type (e.g., credit card) to use in the transaction, or requests a transfer of funds from the user's funds account to the merchant's account. Once the merchant determines that payment has been transferred appropriately by the transaction provider, the merchant can proceed to ship the purchased product or provide the purchased service to the end-user. In the second model, the third party is responsible for maintaining end-user personal and financial information and for processing the transaction.

BRIEF DESCRIPTION OF DRAWINGS

In the drawings, each identical or nearly identical component that is illustrated in various figures is represented by a like numeral. For purposes of clarity, not every component may be labeled in every drawing. In the drawings:

FIG. 1 illustrates a block diagram of a networked computer system for performing online transactions, in accordance with one embodiment of the invention;

FIG. 2 illustrates a diagram of a system and method for initiating and performing identity verification in an online transaction, in accordance with one embodiment of the invention;

FIG. 3 illustrates a diagram of a system and method for performing payment negotiation, verification and/or certification in an online transaction, in accordance with one embodiment of the invention;

FIG. 4 illustrates a networked computer system for conducting online transactions, wherein transactions are handled, at least in part, by transaction software installed on computers connected to the network, in accordance with one embodiment of the present invention;

FIG. 5 illustrates a networked computer system for conducting online transactions, wherein transactions are handled, at least in part, by transaction software installed on computers connected to the network, in accordance with another embodiment of the present invention;

FIG. 6 illustrates a networked computer system for conducting licensing for applications installed on an end-user computer, wherein the license is obtained via an online transaction, in accordance with one embodiment of the present invention;

FIG. 7A illustrates a system used for authenticating a mobile module to a network for establishing a secure communication therewith in accordance with example embodiments;

FIG. 7B illustrates a system used for authenticating a user to a network using a mobile module when establishing a secure communication channel in accordance with example embodiments;

FIG. 7C illustrates a system configured for single or multilevel verification of various different services using a mobile module in accordance with example embodiments;

FIG 8 illustrates a three-way secure exchange of payment information and payment federation in accordance with example embodiments;

FIG 9 illustrates various uses of a commercial transaction subsystem and bill presentation in accordance with example embodiments;

FIG 10 illustrates the use of payment options and rules for determining what type of payment provider should be used for a commercial transaction in accordance with example embodiments; and

FIG 11 illustrates a subscriber identity module (SIM) device configured with a firewall for conforming to established radio network communication protocols when used for commercial transactions in accordance with example embodiments.

SUMMARY OF THE INVENTION

Conventional online transactions, for example, the purchase of goods and/or services over a network, are vulnerable to security breaches resulting in loss of personal, financial and/or other confidential information. Moreover, in an untrusted network (e.g., the Internet), both merchants and purchasers are at risk for entering into a transaction with a bad actor such that one side of the bargain is not upheld. Conventional online transaction models may also

require a merchant to archive purchaser's confidential information and may require them to handle payment aspects of the transaction. In addition, conventional online transaction models are awkward for the purchaser and produce a generally unintuitive transaction experience. For example, conventional online transactions are conducted via a browser using a login/password paradigm that is confusing and difficult to manage.

Applicant has identified and appreciated that delegating at least some of the transactional responsibilities handled by the purchaser and browser in conventional models to lower level systems (and away from the browser and end-user), may facilitate a simpler and more secure online commercial transactions framework. For example, one or more transactional tasks may be handled by the operating system at one or both of the end-user and merchant, where information may be more securely safeguarded. By embedding one or more tasks in the operating system, users may be relieved of some of the burden of transferring transactional information, making the experience more intuitive and enhancing security. Moreover, the merchant may be relieved of maintaining purchaser information, handling of payment information and/or processing the transaction.

Applicant has further appreciated that problems associated with validating the identity of a purchaser may be mitigated by exploiting technologies more secure and convenient than the login/password model. In one embodiment, identity information about a purchaser is provided by a subscriber identity module (SIM) card which stores identity information about the end-user that can be issued programmatically, creating a less confusing and more straightforward purchasing experience. Moreover, embodiments herein provide for protocols, methods, computing systems, and other mechanisms configured for single or multilevel authentication using a SIM device over an otherwise untrusted or unsecure network (e.g., the Internet).

Applicant has further appreciated that providing various transactional elements of online commercial transactions using generally disinterested third parties mitigates risks involved for both the purchaser and the merchant. In one aspect of the invention, a commercial transaction system is provided wherein a first network entity provides verification of a purchaser's identity and a different network entity provides verification of a

user's ability to pay for the purchase, such that a merchant and a purchaser that are strangers to one another may conduct a transaction in relative security.

Still other embodiments allow for a three-way secure commercial transaction between a merchant, consumer, and payment provide in such a way that sensitive billing account information is opaque to the merchant or third parties. In such an embodiment, payment tokens are passed via the consumer between the merchant and payment provider. Such payment tokens are encrypted or signed in such a way that the merchant and others do not control or obtain any sensitive account information for the consumer. Nevertheless, the merchant can still confidently validate the payment token indicating the consumer's ability to pay for services and/or goods provided.

In another embodiment, electronic billing information is used for payment authorization, auditing, and other purposes. In this embodiment, various network entities (e.g., the consumer, merchant, payment provider, etc.) are provided with a machine readable electronic bill, which is used to automatically request and validate payment, create a transaction history, present a more accurate description of paid for services/goods, and for other purposes in an online commercial transaction. This billing information may also be used for payment federation of a single payment from a consumer to various business associates for the merchant. For example, the merchant may have a contractual relationship with various business associates that provide services and/or goods in the commercial transaction. The electronic billing information can include those portions of payments that are to be distributed among the various associates such that payment federation can automatically occur without any need for user interaction or separate auditing and payment mechanisms.

Provided herein are also mechanisms for automated decisions of a commercial transaction using rules or constraints defined by any number of network entities including the consumer, merchant, payment provider, etc. For example, payment options accepted by the merchant may be compared with payment options available to the consumer. Based on such comparison, the consumer may be presented only with those options that match. Alternatively, the payment option may automatically be chosen based on such comparison and/or based on additional rules or constraints. For instance, the consumer may limit the type

of payments based on an established trust with the merchant. Of course, there may be many other types of rules and/or constraints that determine various actions that can occur in the commercial transaction.

DETAILED DESCRIPTION

Conventional models for networked commercial transactions focus on the browser as the interface for requesting and submitting personal and financial information between an end-user purchaser and a merchant or service provider, whether it be directly through the merchant or via a third party transaction provider. In the first instance, the merchant is burdened with creating and maintaining an infrastructure capable of querying, obtaining, handling and processing personal and financial information, typically with some minimum level of security. Moreover, the merchant may be responsible for maintaining accounts and account information for each of its customers (which typically includes both confidential personal and financial information).

A purchaser must relinquish personal information (e.g., name, address, phone number, etc.) and financial information (e.g., debit and credit card numbers and expiration dates, banking account numbers, etc.) to complete a transaction. At some level, the purchaser must trust that the merchant is an honest broker and will operate in good faith, using the information only as authorized. Likewise, a merchant must trust that a purchaser is who he/she represents and that the payment information provided is truly associated with the end-user making the purchase. There may be no sure way for a merchant to validate the identity of the purchaser and/or the validity of the payment information. In a distributed networked environment, purchasers may have to rely on the reputation of the merchant, which may limit the sources from which the purchaser is willing to conduct transactions. The merchant may have to operate with even less conviction that the purchaser is a good faith, bone fide purchaser. In an untrusted network, this model may present undue risks on one or both parties.

Even when an established and merited trust has developed between a purchaser and a merchant, databases storing customer information maintained by the merchant may be susceptible to hacking, information theft and even bad actors within an otherwise honest and trustworthy business. Third party transaction providers are also susceptible to electronic

theft, security breaches, etc. More sophisticated "spy-ware" programs allow hackers to record keystrokes and obtain screen shots of computers that have been compromised, making browser based transactions particularly vulnerable to electronic theft. Accordingly, purchasers conducting online commercial transactions according to conventional methods and models may be vulnerable to dissemination and unauthorized use of their confidential personal and financial information.

Conventional commercial transaction models typically require a purchaser to establish an account with each merchant with which the purchaser wants to conduct a commercial transaction. Generally, the account is protected and accessed via a login name and password, requiring a purchaser to manage multiple login and passwords and maintain which login/password combination corresponds to which account. Some customers may resort to storing their login/password combinations locally on their computer, or using the same login/password combination for all accounts. Both attempts to manage multiple accounts are vulnerable to theft, hacking, and/or other security breaches.

For example, a customer is at risk of having all of his/her accounts breached should the single login/password combination be obtained by electronic theft. In addition to the inherent security risks associated with conventional login/password paradigms, purchasers may find the account login procedure an awkward transaction experience. In particular, having to login to an account when a purchase is desired makes the transaction less convenient, as a purchaser must, in one way or another, produce this information before a transaction can be completed. Moreover, with third party transaction providers, the purchaser is redirected from a merchant's website to the third party transaction provider's website. This step is not intuitive and, at best, is cumbersome and confusing to the purchaser.

Applicant has identified and appreciated that delegating at least some of the transactional responsibilities handled by the purchaser and browser in conventional models to lower level systems (and away from the browser and end-user), may facilitate a simpler and more secure online commercial transactions framework. In one embodiment, one or more transactional tasks are handled by the operating system (or some other trusted subsystem) at one or both of the end-user and merchant, where information may be more securely safeguarded. By embedding one or more tasks in the operating system, users may be relieved

of some of the burden of transferring transactional information, making the experience more intuitive and enhancing security. Moreover, the merchant may be relieved of maintaining purchaser information, handling of payment information and/or processing the transaction.

Applicant has further appreciated that problems associated with validating the identity of the user may be mitigated by exploiting technologies more secure and convenient than the login/password model. In one embodiment, identity information about a purchaser is provided by a subscriber identity module (SIM) card which stores identity information about the end-user that can be issued programmatically. In another embodiment, identification information is provided by a smart card embedded or otherwise coupled to a network device from which a purchaser conducts an online commercial transaction. Use of any of various chip or card based identity means allows a purchaser to link his or her identity with a particular device, such as a cellular phone or a networked computer.

The term "programmatically" and/or "automatically" refers to actions performed substantially without manual or operator involvement. In particular, programmatic or automatic refers to actions initiated and/or performed by one or more computer programs. For example, providing identification information by requesting a user (e.g., purchaser) to provide login and/or password information would not be considered programmatic as the substance of the action is performed by the user. However, an action wherein a program issues identification information (e.g., a SIM number, network address hardware ID, etc.) without requesting the user to input the information would be considered programmatic. Note that such automatic operations may be implemented by either software or hardware components.

Applicant has further appreciated that distributing various transactional elements of online commercial transactions over different network devices, facilitates more secure commercial transactions over an untrusted network. In one embodiment, an identity provider and a payment provider, both separate and distinct network entities from the end-user, merchant and each other, provide verification support during a commercial transaction. The term "network entity" refers herein to a network presence and may be one or a combination of end-user/purchaser, identity provider, payment provider, merchant, etc. A network entity may have a presence on a network via one or multiple network nodes. For example, multiple

networked devices may operate under the auspices of a single network entity, such as an identity provider utilizing multiple servers to conduct online business, or an end-user connected to a network via a cellular phone and a personal computer. A network entity may be a business such as a bank or retailer, or an individual such as an end-user.

In one embodiment, various elements of an online transaction are distributed over separate and independent network entities. For example, the identity provider may provide identity validation in the form of an identity token, which the merchant can use to verify the identity of the purchaser. The identity token may include one or more identity credentials of the end-user. The identity token may be issued based on the identity information provided by the end-user/purchaser, for example, the subscribe number from the SIM card, a network address (e.g., a Network Interface Card (NIC) identification, World Wide Name (WWN), etc.), login information, etc. Similarly, the payment provider may provide verification of the end-user's ability to pay in the form of a payment token. In addition, the payment provider may handle payment transactions on behalf of the purchaser in satisfaction of the purchase of goods and/or services from the merchant. The above described framework allows, *inter alia*, a purchaser and merchant that are strangers to conduct an online commercial transaction in an untrusted network environment in relative confidence, as discussed in further detail in the various exemplary embodiments provided below.

For example, one embodiment provides for a three-way secure communication between a merchant, consumer, and payment provider during a commercial transaction for purchasing services and/or goods in either an online or retail environment. As will be discussed in greater detail below, payment tokens are passed from the payment provider to the merchant via the consumer. Such payment tokens offer proof of the consumer's ability to pay for the service and/or goods by allowing the merchant to validate the authenticity of the token directly with the payment provider. Although such payment tokens uniquely identify the authorization of payment for the services and/or goods, sensitive information about the billing account for the consumer is either not included within the token or otherwise encrypted so as to be invisible to the merchant. Accordingly, the consumer's sensitive information is opaque to the merchant, thereby allowing the consumer to confidently purchase items from the merchant even when no trusted relationship exists between them.

Further, because the merchant can validate the payment token directly with the payment provider, the merchant can deliver the items with confidence of the consumer's ability to pay for such services and/or goods without maintaining financial information about the consumer (e.g., credit card numbers, account information, etc.). In addition, because the payment provider can validate the authenticity of the payment token as coming from the consumer, the payment provider can confidently transfer funds to the merchant; thus completing the three-way secure commercial transaction.

As previously mentioned, other embodiments for the framework provided herein move portions of the transaction to more secure subsystems of a computing device (e.g., the operating system). This advantageously allows for numerous capabilities including: an abstraction model for allowing legacy applications to provide in-band online commercial transaction experience; additional types of fraud protection; bill capture and presentation for auditing, payment federation, and other payment or authentication purposes; service provider code execution for additional security and merchant specific functionality; multilevel authentication; and other features. For example, such abstraction model allows legacy and other applications to provide a user with an online purchase and payment capabilities as if such transaction occurs directly within the application, although portions of the commercial transaction are performed out-of-band. Examples, include catalog purchase (e.g., Amazon, Sears, etc.), direct purchase of multimedia content from within the multimedia application, download software/games in trial mode and automatically unlock them through in-band payment model, enable payment for subscription based services such as simple message service through email, etc.

Further, in another embodiment, the framework captures and presents electronic bills in the above three-way secure (and other) commercial transactions as a mechanism for additional authentication, auditing, payment federation, and other purposes will be described in greater detail below. Moreover, by moving the commercial transaction to more secure portions of the subsystem, other embodiments allow a merchant to run specific code on a machine (e.g., additional user authentication, payment rules/mechanisms, user experience, etc.) with confidence that such code will not be hacked or otherwise compromised. Of

course, as described in greater detail below, Applicant has further realized other advantageous features through the use of the abstraction model provided herein.

In another embodiment, Applicant also provides for an overall system and protocol that uses a mobile module for secure communication and authentication of identity and payment capabilities for a variety of different services. For example, a subscriber identity module (SIM) (or other similar mobile module) can be used to authenticate a user and/or device to a service or server in a multilevel validation environment. In such embodiment, the mobile module (and possibly even the user) is authenticated over a network independent of the network mobile infrastructure for the mobile module. Thus, the system validates the possession of a mobile module through authentication of an active billing account with the mobile infrastructure. This establishes a secure communication with a computing device connected to the mobile module and a service (e.g., a Web Services (WS)) using existing secure protocols (e.g., WS-Authentication, WS-Security, and other similar protocols). Such secure communication can also be used to authenticate the user through other protocols and data exchanges between the mobile module and the mobile infrastructure—as described in greater detail below. Further, other embodiments provide for a protocol and state machine that abstract the computing device (used in the communication over the independent network) from the mobile infrastructure. Accordingly, the mobile module itself becomes a mobile terminal and the computing device becomes a peripheral device, thus complying with current wireless standards such as 3GPP (3rd Generation Partnership Project).

FIG. 1 illustrates a block diagram of a commercial transaction system 100, comprising a plurality of network nodes including an end-user (purchaser) computer 110, a merchant computer 140, an identity provider computer 120, and a payment provider computer 130. Each of the above nodes may include one or more computing devices interconnected via network 105. It should be appreciated that the end-user computer, merchant 140, identity provider 120 and payment provider 130 may be associated with a network entity, such as an individual, company or business. For example, end-user computer 110 typically is associated with an individual that employs the computer to access resources on the network and merchant computer 140 may be associated with a corporation or business offering goods and/or services for sale. The one or more computing devices that form each mentioned

component in commercial transaction system 100 may operate as the point of entry, computing platform and/or vehicle by which the associated network entities communicate over the network.

Note that although embodiments provided herein may be described in an online purchasing environment, embodiments can also be used in a direct retail transaction. For example, the above and following description of a commercial transaction can apply to a consumer purchasing products in a retail store, wherein payment, identity, authorization, and other embodiments are used. Accordingly, the use of an online experience for describing embodiments herein is for illustrative purposes only and is not meant to limit or otherwise narrow the scope of embodiment unless otherwise explicitly claimed.

Also note that network 105 may be any type of network in any type of configuration that interconnects and allows nodes connected to the network to communicate. Nodes or devices may be connected to the network via copper (e.g., Category 5) cable, optical connections, wireless or any combination thereof. Information may be transferred using any low level protocol such as Ethernet and/or any information protocol such as TCP/IP. The network 105 may have any number of devices connected to it and may be a trusted (e.g., intranet) or an untrusted network (e.g., LAN/WAN, Internet, etc.), or a combination of both. The computers connected to the network may be any type of device including, but not limited to, one or any combination of a mobile phone, a desktop computer, a tablet personal computer, a server, workstation, etc.

FIG. 2 illustrates a diagram of a system and method for initiating and performing identity verification in an online transaction, in accordance with one embodiment of the invention, and FIG. 3 illustrates a diagram of a system and method for performing payment negotiation, verification and/or certification in an online transaction, in accordance with one embodiment of the invention. The methods may be used separately or in combination to perform an online transaction between an end-user/purchaser and a merchant. In the following description, unless specifically pointed out, no distinction is made between the network entity and its associated networked devices. For example, "identity provider" is used generically to describe the identity provider as an entity (e.g., a bank, government organization, agency, etc.) and as the computing devices that the entity utilizes to perform

various network functions, such as providing identity verification for an end-user, or otherwise operating on the entity's behalf.

An end-user computer 110 may place an order 242 with a merchant 140. The order 242 may be any indication that the end-user would like to purchase one or more goods and/or services from the merchant 140. For example, the order 242 may result from end-user selecting a good or service via a web browser displaying pages resident at the website of a merchant, or may result from choosing an option from an application running locally, as described in further detail below. As an example of the first instance, the merchant 140 may provide a website to display or otherwise offer for sale goods and/or services that it provides, or may provide an online catalog of merchandise. The order 242 may be any type of indication that end-user would like to purchase one or more goods and/or services from the merchant 140.

As an example of the second instance and as an alternative to selecting one or more goods and services from a merchant's website, order 242 may originate from an application or other program local to the end-user computer 110. For example, an end user may create, produce or edit a document via a word processing application, design a slide show using a presentation application and/or manipulate images or graphics for a poster or brochure using an imaging application. The application may include an option under the print menu that allows the document to be printed by a third party to, for example, take advantage of printing features that may not be locally available, or to otherwise exploit professional printing services. When the option is selected, the application may send, via the network, order 242 to the merchant 140. It should be appreciated that order 242 may be any indication to purchase any good and/or service, as the aspects of the invention are not limited in this respect.

In response to order 242, merchant 140 may request that end-user 110 provide an indication of the end-user's identity and/or verification that the end-user is indeed who he/she purports to be (step 205). For example, merchant 140 may not know anything about the source of order 242 and may desire information about the identity of the end-user and/or assurance that the end-user is not spoofing his/her identity. Alternatively, the merchant 140 may send a notice or indication that payment is required for the service and demand that a payment token be provided. To obtain a payment token, it may be necessary to first establish

an identity via an identity token, as described in further detail below. In either case, end-user 110 may respond to the request by the merchant 140 by enlisting the services of identity provider 120 (step 215).

To obtain an identity token, end-user 140 provides identity information to identity provider 120. Identity information may include any information that enables the identity provider 120 to distinguish between end-user utilizing end-user computer 110 and the various other end-users to which identity provider may provide services. For example, the identity information may include a unique identifier associated with the hardware of end-user computer 110. In one embodiment, the identity information is provided by a SIM card issuing an identifier unique to the subscriber. Identity information may include providing a unique hardware number of the network interface card (NIC) of the end-user computer 110, a world wide name (WWN) or other network address of end-user computer 110 or any other means by which end-user computer 110 may be identified, including (in some embodiments) an established login name/password combination.

Identity provider 120 uses the identity information to locate identity credentials associated with the end-user. For example, identity provider 120 may include a database that stores identity information and credentials on a plurality of end-users. The identity information may be used to index into the database to obtain the correct identity credentials. The identity provider 120 may be any type of entity. For example, identity provider 120 may be a mobile phone company that uses the subscriber number provided by the end-user's SIM card to locate the appropriate identification information. In one embodiment the subscriber number is used to locate and obtain information provided by the end-user at the time of subscription to the cell-phone or other device exploiting SIM technology. The identity provider 120 may be a bank, a government agency (such as the registry of motor vehicles (RMV)), or any other facility that maintains identification information or credentials associated with end-users.

In response to the identity information provided by the end-user, identity provider 120 provides an identity token to end-user computer 110 that provides identity authentication and/or credentials about the end-user (step 225). The identity token may be any type of electronic message that another network device can use to authenticate, verify and/or

determine an end-user's identity. For example, the identity token may include identity credentials of the end-user. Identity credentials may include, but are not limited to, any one of or combination of name, birth date, address, telephone number, email address, etc.

The identity token may include an electronic signature from the identity provider 120 certifying that the identity credentials are correct. In this way, a merchant and/or payment provider may rely on a disinterested third party (i.e., an identity provider), rather than the representations of an arbitrary end-user. The identity token may be encrypted before being transmitted over the network and decrypted when received by the desired network device (e.g., merchant, payment provider, etc., as discussed in further detail below), to protect against eavesdroppers on the network. In other embodiments, the payment token is merely a certification of the end-user's identity without accompanying identity information.

The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140. Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-users that are frequent purchasers, or who received a coupon, promotional offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.

Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the

identity token itself (step 265) (e.g., by assuming the identity token is valid or otherwise processing the token). Optionally, a response may be returned from the merchant 140 to the end-user computer 110, where the response may include a message of whether the identity token is valid, of any applicable discount or promotional offers, and/or any other type of message, as the invention is not limited in this respect (step 265).

After the merchant 140 has processed the identity token and/or has received a validation for the identity token from the identity provider 120, the merchant 140 may request that the end-user provide verification or validation of an ability to pay and/or provide an indication of how the end-user would like to pay for the goods or services. The merchant 140 may make the request via a payment token request (step 305 in FIG. 3). In response to the payment token request, the end-user computer 110 may enlist the services of a payment provider 130. Payment provider 130 may be associated with a third party that maintains financial and payment information about various end-users, such as a financial institution, or a third party broker that handles financial transactions and payment procedures.

The end-user computer 110 may solicit a payment token from a payment provider 130 (step 315) by transmitting the identity token to payment provider 130. Alternatively, the end-user may request a payment token by logging onto the payment provider 130 in a manner similar to that discussed in connection with the identity provider 120 (i.e., by providing an identifier such as a SIM subscriber number, NIC address and/or using a login/password combination). It should be appreciated that the end-user may request a payment token in other ways, as the invention is not limited in this respect. In addition, the end-user may send information about the purchase, such as the price and nature of the purchase so that the payment provider can verify that the end-user is capable of paying. However, providing purchase information is not required, as it may not be necessary or it may be handled in subsequent steps of the transaction.

Payment provider 130 processes the identity token (or other provided identifier) to locate information about the end-user. For example, the payment provider 130 may access a database of payment information based on the identity credentials transmitted with the identity token. Payment provider 130 may determine what payment capabilities and options the identified end-user has available. The payment provider 130 may then verify that the

end-user has the ability to pay, and in response generate and transmit a payment token to the end-user computer 110 (step 325). The payment token may indicate the end-user's ability to pay and/or a certification that the payment provider 130 is willing to handle the transaction on the end-user's behalf. The end-user computer 110 may then forward the payment token to the merchant 140 (step 335).

The merchant 140 processes the payment token such that the merchant 140 is satisfied that the end-user is able to pay for the goods or services (step 365). For example, the merchant 140 may ask the payment provider 130 to validate the payment token (steps 345, 355) or may simply validate it itself (step 365) (e.g., by assuming the payment token is valid or otherwise processing the token). The merchant 140 may then begin the process of providing the goods and/or services to the end user. Because the payment provider 130 may be a disinterested third party, merchant 140 may treat the payment token essentially as payment and may not have to wait until the transaction is fully processed.

When a merchant deals directly with the end-user in conventional transactional models, the merchant may have to ensure that the payment information provided by the end-user is correct and sufficient. For example, a merchant may have to run a provided credit card number through the credit card system to query whether the number is valid, the card is valid, there are sufficient funds and/or the card is correctly associated with the identity provided by the end-user. If something doesn't check out, the transaction may have to be canceled, terminated or abandoned. Moreover, the termination of the transaction may happen after the end-user perceives the transaction to be complete and is no longer accessing the network and/or is no longer accessing the merchant's website, etc.

The merchant may then have to notify the end-user that there was a problem with transaction and the end-user will have to go through the transaction again to correct the problem (e.g., by correctly inputting payment information, specifying a different card with sufficient funds, etc.). In some instances, the end-user may not be notified and the commercial transaction may never be completed.

In various embodiments discussed herein, because a payment token will not be issued unless the end-user payment information is correct, sufficient funds are available, and/or the payment provider otherwise certifies that it will pay on the end-user's behalf, the merchant

can proceed with the transaction immediately. Any deficiencies in the transaction may be identified in real-time and addressed so that all parties can be relatively certain that there expectations are being met with respect to completion of the transaction.

In addition, because the payment provider may handle the financial transaction (e.g., handling the credit card, transferring funds, etc.), the merchant may be relieved of establishing and maintaining the infrastructure necessary to, for example, process credit card numbers or otherwise handle payment procedures and funds transfer. The payment token, in some cases, operates as an assurance that the payment provider will transmit the designated funds, for example, by wiring the money or enacting an electronic transfer of funds to the merchant. The payment token may also be an assurance that the payment will be made by non-electronic means such as a promise to issue to the merchant a check or other negotiable instrument.

From the perspective of the merchant, the commercial transaction is substantially risk free as the identity of the end-user and the payment verification is handled by third parties and is therefore less susceptible to fraud, spoofing and even innocent mistakes in providing personal and financial information. Therefore, merchants may be more willing to conduct online commercial transactions with unknown end-users over an untrusted network. From the perspective of the end-user, personal and financial information resides with entities either that already maintain the information and/or that the end-user has an established relationship with. Confidential personal and financial end-user information need not be provided to the merchant, mitigating the vulnerabilities of having confidential information misused or misappropriated. As a result, end-users may be more willing to conduct commercial transactions with unknown merchants without having to worry about whether the merchant is trustworthy or not.

In some conventional commercial transaction models, identity information and payment information are input by the user and processed by either a third party or the merchant. As discussed above, these models are awkward, inefficient and time consuming for the user. In addition, conventional models present numerous issues regarding security of an end-user's confidential information as well as making a merchant vulnerable to fraud and/or susceptible to failure to pay by an end-user. Applicant has appreciated that

commercial transaction software installed on each of the computers employed in various commercial transactions may mitigate or eliminate concerns over security and fraud. In addition, many of the actions handled by the end-user and merchant in conventional models may be performed by the commercial transactions software, making the transaction simpler and more intuitive to the end-user.

FIG. 8 illustrates an example of using some of the features described above for a three-way secure communication and various trust boundaries that may be established during a commercial transaction. As will be described in greater detail below, this model allows for single or subscription payments, as well as payment federation such that a service or merchant can aggregate payment for smaller companies; thus enabling the customer to pay a single bill. As shown, a distributed system 800 is configured to facilitate a commercial transaction between a consumer 810, merchant 830, and a payment provider 805. A payment trust boundary 815 divides the merchant 830 from the consumer 810/payment provider 805 such that a trusted relationship exists between the payment provider 805 and the consumer 810 or customer computing device (i.e., the consumer has appropriately identified or authenticated itself to the payment provider using any of the available mechanisms as described herein). Accordingly, the consumer 810 can utilize this trusted relationship to authorize payment to the merchant 830 for various types of payments and various types of services.

For example, assume that the merchant 830 requires reserve payment for a product (e.g., a custom item that requires prepayment like a car, computer, etc.), which the consumer 810 wishes to purchase. Prior to requesting payment authorization, however, the user of the consumer 810 computing device may require appropriate authentication as described herein. Once the user authenticates, the consumer 810 computing device can appropriately request payment from the payment provider 805 through any various mechanisms as also described herein. For example, the consumer 810 may provide the payment provider with billing or other request information that is signed or otherwise encrypted by the consumer's 810's computing system. This authenticates the request for validation of the account holder's (i.e., the consumer's) ability to appropriately pay (i.e., the user has a prepaid account, credit account, or other billing account such as a mobile subscription as described below). If

successful, a payment token is issued and the funds are then reserved for guaranteeing payment. Such payment token is typically then signed and/or otherwise encrypted by the payment provider (e.g., a mobile web server as described herein) and passed to the consumer 810 client. The consumer 810 passes the payment token back to the merchant 830, which verifies the token against the payment provider, and if successful completes the order.

Once the item is ready for delivery (e.g., the custom item has been built), the merchant 830 can use the reserve payment token to request payment from the payment provider 805. Note that the amount of the request for payment may be different than the amount reserved. Nevertheless, the payment provider 805 verifies and returns a payment response to the merchant 830 and/or consumer 810. If approved the merchant 830 can ship (or otherwise provide) the order to the customer 810 and be provided with payment thereof. If, on the other hand, the payment is rejected or further user interaction is required, the merchant 830, payment provider 805, and/or consumer 810 can choose what course of action to take. For example, if the amount requested by the merchant 830 does not match the funds reserved, the payment provider 805 and/or merchant 830 may request authorization from the consumer 810 for the new amount. Alternatively, the payment provider 805 may require user input authorizing the transfer of funds regardless of any change in reserved and requested payment amounts. Of course, other actions and procedure for completing the commercial transaction are also contemplated herein.

Note that although the above three-way secure payment mechanism was used to purchase a reserve item, the single payment may also apply to other services and/or goods. For example, the single payment mechanism may apply to a software program that is ready for immediate download. Alternatively, or in conjunction, the single payment may unlock various levels of a program that was downloaded (e.g., student version, professional version, or other separate functionality). In fact, as will be appreciated the above single payment can be used for a variety of different types of purchases, some in a slightly modified payment form.

For example, suppose the consumer 810 wants to setup a subscription with a merchant 830 for continual service (e.g., a newspaper or magazine subscription, movie subscription, gaming application, or other pay-as-you go goods and/or services). Accordingly, the

merchant 830 will challenge the consumer 810 for a payment token, and thus the consumer 810 client may interact with the user requesting authorization to proceed as described herein. Similar to above, the consumer 810 signs or otherwise encrypts the request for payment (e.g., using electronic billing information as described herein below) and send such request to the payment provider 805 (e.g., a mobile operator, credit card company, pre-paid or other type of third party service, etc.). This authenticates the request and verifies the account holder (i.e., the consumer or customer) has sufficient initial funds. If successful, a payment token is issued, signed and/or otherwise encrypted, and returned to the consumer 810 client, which passes the payment token back to the subscription merchant 830. The merchant 830 then verifies the authentication of the token and completes the subscription setup.

Note that typically the payment token is stored at the merchant 830 and periodically used when requesting subscription payment from the payment provider 805. Accordingly when processing subscription payment, the merchant 830 retrieves the payment token and sends it to the payment provider 805 for payment settlement. The payment provider 805 verifies and returns a payment response to the merchant 830 and/or consumer 810. If an approved response is returned, the subscription merchant 830 will receive payment during the next payment provider 805 account payment run. If the payment request is rejected, however, the payment provider 805 and/or merchant 830 may respond appropriately. For example, the merchant 830 (or payment provider 805) may contact (e.g., via email) the user or consumer 810 informing them of the outstanding payment. The consumer 810 can then perform a single payment as described above or setup another subscription payment through either the same of different payment provider 805. Of course, the merchant 830, payment provider 805, and/or consumer 810 may have other rules or requirements for processing these and other payment authorizations, as will be described in greater detail below.

As previously mentioned, other embodiments allow for federation of a single consumer 810 payment to a plurality of business associates or subsidiaries with a contractual arrangement. Often business relationships are complex and require distribution of payments for various services and/or goods provided within a particular business model. For instance, when purchasing a trip from a travel agent 830, a consumer 810 may be provided with a package deal including flight arrangements, hotel accommodations, transport services, etc.

The merchant 830, who typically contracts out many of such services and/or goods, must then keep detailed accounting of such commercial transaction in order to make appropriate payments to its business associates. In order to alleviate the complexity of such accounting and other tasks, embodiments herein provide for an automatic payment federation to business associates within a particular type of relationship on a per transaction basis.

For example, a car rental service (e.g., business associate "A" 820) may require payment from merchant 830 as part of a holiday package sale. An insurance company (e.g., business associate "B" 825) may charge the merchant 830 on a per transactional fee basis. Based upon the business associate trust boundary 835, payments are automatically federated to each business associate (e.g., "A" 820 and "B" 825) when a single payment is made to the merchant 830. In other words, the consumer 810 or payment provide 805 makes a single payment to the merchant 830; however, all subsidiaries with a business relationship according to the trust boundary for the business model 835 can be appropriately paid. Note that such payment will typically be tied to the electronic billing statement as described in greater detail below. More specifically, various portion of an electronic bill for capture, presentation, and other purposes can correspond to what portion of payment should be federated to each business associate. Further, each of these portions may be signed and/or encrypted such that particular information about the payment is opaque to the consumer 810, payment provider 805, or amongst the various business associates 820, 825 as defined by the various trust boundaries 815, 825.

Note that although the above payment federation model was described with regards to a travel agent experience, other business relationships also exist that can use this embodiment. For example, companies who build items with multiple components purchased through various vendors, product providers who buy materials for there product and make payments based on a per item bases, payments for multimedia products who pay royalties based on each sale, or any other type of business model that bundles or otherwise can calculate and make payments to business associates on a per item basis may also use embodiments described herein. As such, the above use of the travel agent for describing various embodiments herein is for illustrative purposes only and is not meant to limit or otherwise narrow embodiments described herein.

FIG. 4 illustrates a networked computer system for handling commercial transactions, in accordance with one embodiment of the present invention. Networked computer system 400 may be similar to computer system 100 illustrated in FIG. 1. However, in FIG. 4, each of computers in system 400 includes local installations of commercial transactions software 485. In particular, end-user or consumer computer 410, identity provider 420, payment provider 430 and merchant 440 include commercial transactions software 485a-485d, respectively. The commercial transactions software locally installed at each of the computers in the system may be the same, or may be customized for the particular computer in view of which role(s) the computer plays in the transaction (i.e., whether the computer operates as an end-user node, a merchant node, identity provider node, payment provider node, etc., or some combination of the above). In either case, each installation is configured to communicate with installations on other networked computers to perform online transactions. For example, each installation may be configured to communicate with installations on networked computers so as to perform the methods illustrated in FIG. 2 and/or FIG. 3.

In one embodiment, the local installation of the commercial transaction software 485a on identity provider 420 can create an identity token identifying the end-user utilizing end-user computer 410. Furthermore, the commercial transaction software 485a on identity provider 420 can forward the identity token to the end-user computer 410, the payment provider 430, the merchant 440, and/or any other computer, as the invention is not limited in this respect. The local installation of the commercial transaction software 485b on the end-user computer 410 can issue identity information (so as to identify the end-user) in response to an indication to conduct an online transaction between the end-user and a merchant. The local installation of the commercial transaction software 485c installed on payment provider 430 can receive the identity token and generate a payment token verifying an ability of the end-user to pay (e.g., the payment token) for the online transaction. The local installation of the commercial transaction software 485d installed on the merchant 440 can receive the verification of the ability of the end-user to pay before proceeding with the online transaction.

In one embodiment, each of the computers in system 400 operates using a local installation of a same or similar operating system 495. For example, each of the computers in system 400 may operate using the Microsoft Windows® operating system. Commercial

transactions software 485 may be a subsystem of the operating system. In this way, the various computers employed in a commercial transaction communicate in a consistent and known fashion. Since the commercial transactions software is communicating directly over the network and handling the validation, verification and security, the end-user and merchant need not know anything about one another, and more importantly, may not need to establish any trust relationship. In addition, because certain portions of the transactions are handled by the operating system, much of the transaction may be performed substantially invisible to the user, without requiring confusing and oftentimes awkward involvement by the end-user.

By having the commercial transactions software on each computer, various encryption techniques may be used during transmission of information from one computer to another. Moreover, further security features may be included such as identity tokens and/or payment tokens that are valid for a limited time period. For example, an identity token may include a time component that specifies a time after which any component receiving and processing the token should deem it invalid, and not honor the token as verification of identity and/or payment. The commercial transactions software components may programmatically process any time limits associated with a token. This may prevent tokens obtained by "fishing" from being used inappropriately at a later date.

It should be appreciated that the commercial transaction software need not be part of the operating system, but may be any program or group of programs local to computers involved in a commercial transaction that can communicate with one another over the network. For example, the commercial transaction software may be an application developed by a third party that can be installed on the computers to operate on or independent of the operating system installed on the computer. The application may be configured to operate with any one or combination of operating systems so as to be available to computers or devices of a wide range of capabilities and configurations, and not limited to any particular operating system, processor, instruction set, etc.

FIG. 5 illustrates a commercial transaction initiated by an end-user selecting one or more desired goods and/or services, wherein the transactional components of the purchase are handled, at least in part, by a transaction software subsystem distributed as part of the operating system of the various computers involved in one or more transactions. An end-user

connected to network 505 through end-user computer 510 may be running an application 555. Application 555 may be a browser displaying the website of a business that offers merchandise or services for sale. Application 555 may be an application that provides an option to engage in an online transaction, such as an imaging editing program that allows users to manipulate images.

The end-user may select one or more goods or services to purchase via application 555. For example, the end-user may wish to have an edited image professionally printed on photo quality paper. Application 555 may include such an option under the print menu. The print option, when selected, may generate a window or dialog box listing all of the available printing options, including services available over the network. For example, the print option may list service providers 540a, 540b and 540c as options for providing the printing service. When the user selects one of the service providers, an online commercial transaction as described above may be initiated. In particular, the service provider may request that the end-user provide an identity token. In response, application 555 (or an application embedded in commercial transactions software 585), may generate a dialog box or interface listing available identity providers. For example, as described in greater detail below, the dialog box may list identity providers 520a, 520b and 520c as possible identity providers that the user may select to handle identification verification.

FIG. 9 illustrates the use of a trusted commercial subsystem and other features in a distribute system and in accordance with example embodiments. As shown, a local computing device 920 within distributed system 900 is configured to provide an online or local retail transaction in accordance with embodiments described herein. Note that although the trusted commercial transaction subsystem 965 is shown only as part of the local computing device 920, similar subsystems may also reside on other network entities. Further note that although various components or modules may be described herein as residing on any particular network entity, such components or modules may be distributed throughout the computing system and reside on any number of network entities (i.e., portions may exist on one or more network entities). Accordingly, the specific aesthetic layout and use of a particular module by a network device or entity is used herein for illustrative purposes only and is not meant to limit or otherwise narrow the scope of embodiments herein.

Regardless of the distribution and aesthetic layout of the computing system 900, as previously described there exists a trust boundary 906 separating the trust relationship between the various components. Although the relationship may be divided up differently, in the present example the trusted relationship exists between the payment provider 990 and the trusted commercial transaction subsystem 965. This advantageously allows for many features that current commercial systems cannot provide. For example, the trust boundary 906 abstracts applications 925 from the commercial transaction with the merchant. Accordingly, legacy and other applications 925 can provide an in-band experience to the end user 940, although much of the functionality appears out-of-band. For instance, in the above example of allowing a professional image printing on photo quality paper, the selection within the pull down menu, the identity validation, payment options, and other components for assisting the user in such service purchase appears as part of the application 925. Accordingly, the application 925 when receiving input to purchase services and/or goods can make a purchase call 930 into the trusted commercial transaction subsystem 965, which is then used to generate dialog boxes, receive user 940 input 935, and otherwise automatically communicate with the merchant 905 and/or payment provider 990 as described herein.

In other words, the user 940 does not need to necessarily trust the application 925 or the merchant 905 in the commercial transaction. In stead, the trust is limited to the subsystem 965 of the present framework, which reduces the degree or levels of trust needed to confidently and securely perform a commercial transaction. That is, the account details 950 for the user 940, which include sensitive information 955 that the user 950 is unwilling or uncomfortable to publicly share (e.g., credit card information, personal information, user names/passwords, etc.), are accessed via either direct user input 935 to the subsystem 965 or from secure 960 account information store 945. As such, applications 925, merchant 905, and other components are abstracted away from financial and other billing account details 955 controlled by the subsystem 965 as described herein. This is very different from current commercial transaction models described above where applications 925 or merchants 905 maintain and control account information. Accordingly, this and other embodiments described herein advantageously provide for additional layers of security during such commercial transactions. This is a much more directed trust relationship in order to minimize

the number of components or organizations that have access to or touch the very sensitive financial data.

Also shown in FIG. 9, and similar to the three-way secure commercial transaction described above, the trust boundary 906 also indicates a secure communication between the payment provider and the trusted commercial transaction subsystem 965. Accordingly, the subsystem 965 authenticates to the payment provider(s) 990 in any one of numerous ways described herein, allowing for secure communication therewith. Similar to above, local computing device (which can be a handheld portable device as described below in a local retail transaction, a personal computer in an online transaction, or other similar device as described herein) desires various services and/or goods offered by merchant(s) 905. In this example, billing information 910 is presented to the local computing device 920 for authentication, auditing, and other purposes as used in example embodiments described herein. Such billing information may include, but is not limited to, cost of the merchandise and/or services, detailed description of the commercial transaction, merchant 905 specific information, federation payment information, type of transaction (e.g., single payment, subscription, etc.), or other types of billing information. The bill information 910 may also include other information such as merchant constraints and payment options as described in greater detail below.

In one embodiment, the bill information 910 is an electronic bill configured to be machine readable, which provides for many advantageous abilities of the current commercial transaction system. For example, one embodiment provides that the billing information 910 can be part of the payment token request 980 (or otherwise delivered in another communication to the payment provider 990) as previously described. As such, the bill information may be used by the payment provider 990 for payment token validation 940. More specifically, the bill information 910 provided from the consumer or local computing device 920 can be compared with the payment token 985 information provided from the merchant 905 in the payment token validation 904. Accordingly, if the bill information 910 for the payment token validation 904 matches the bill information 910 from the token request 980, the payment provider 990 can be further assured of the authenticity of the payment token 985 and the validity of the merchant.

Note that how the bill information 910 from the merchant is relayed to the payment provider 990 (as well as other components herein) may vary. For example, the bill information 910 sent from the merchant 905 to the payment provider 990 may be a copy of the bill information 910 sent to the trusted commercial transaction subsystem 965 or client 920. Alternatively, or in conjunction, the bill information 910 may be a signed and/or encrypted version from the payment provider 990, routed via the consumer or local computing device 920. In either case, the payment provider can do the comparison previously described for authentication of the payment token 985.

Further note that such billing information 910 as used by the payment provider 990 can also be used to give a more detailed description of charges associated with a bill that will subsequently be presented to the user 940 for charges on the user's account. Because this can also be a machine readable bill 910, the local computing device 920 can match up the bill information 910 with that previously received by the merchant 905 for further authorization of payment to the merchant 905. In other words, if the bill information 910 within the bill from the payment provider 990 does not match any received from the merchant 905, then the charges may be considered fraudulent.

In another embodiment, the merchant 905 can use the bill information 910 for auditing, user and other authentication purposes, payment federation, etc. For example, the merchant can sign or otherwise encrypted portions of the bill information 910. This allows for multiple advantageous features in embodiments described herein. For example, the bill information 910 may be part of the payment token 985 received by the payment provider via the local computing device 920. The merchant 905 can check the validity of the billing information 910 for authenticating that the payment token 985 came from the client 920 or trusted commercial transaction subsystem 965. Similarly, the during the payment token validation 904, the merchant 905 can use billing information 910 received from the payment provider 990 to validate or authenticate the payment provider 990 and/or local computing device 920. In other words, because the bill information 910 is routed to the payment provider via the subsystem 965 or consumer 920, billing information received from the payment provider that matches that sent to the client 920 can authenticate both the client 920 and payment token 985 from the payment provider 990.

Note that in another embodiment, as briefly described above, the bill information 910 can also be used by the merchant for payment federation. In this embodiment, various portions of the bill information 910 may be machine readable for determining what portions of funds from the payment provider 990 (upon successful payment authentication) should be distributed to business associates as previously described. Note that in this embodiment, typically portions of the bill information 910 will be encrypted or otherwise opaque to the user 940 (or consumer client 920), payment provider 990, or other components not part of a business relationship with the merchant 905. This also uniquely identifies the business associate in the billing federation, and can be used thereby for authentication purposes. More specifically, the various portions of the bill information 910 specific to a business associate can be encrypted using a key specific such business associate, thus the billing information may only be seen by the merchant 905 and the specific business associate. In other embodiments, however, the portions of the bill for payment distribution or federation are only signed by the merchant 905 to make then opaque to other components in the system 900.

Of course, as will be recognized, other uses of the billing information 910 can be used for various purposes. For example, the billing information 910 can also be used for auditing purposes, product distribution reconciliation, or any other well known business and other purposes. Accordingly, the above use of the bill information 910 for authorization, identification, payment federation, or any other purpose is used for illustrative purposes only and is not meant to limit or otherwise narrow the scope of embodiments unless otherwise explicitly claimed.

Note that the trust boundary 906 and the subsystem 965 also have other advantageous features in other embodiments described herein. For example, as shown in FIG. 9, payment provider code 970 within the subsystem 965 allows for securely running code specific to one or more payment providers 990. Such code can be used for further authorization specific to the payment provider, e.g., biometric, radio frequency identification (RFID), user name/password, or any numerous additional authentication techniques. In other words, due to the trusted relationship that the payment provider 990 has with the subsystem 965, the payment provider can run trusted code for its specific business purpose.

The use of such code 970 also allows for a more integrated in-band user experience that can be controlled by the payment provider 990 or any other component that has a trusted relationship with the subsystem 970. For example, although not shown, a trusted relationship may exist between some merchants 905 and the subsystem 965 for allowing trusted code thereof to be run by the subsystem 965. As such, the merchant 905, payment provider 990, or any other component involved in the commercial transaction, may provide an integrated user experience that appears as if ran from within the application 925 (legacy or otherwise); however, many of the events occur out-of-band. For instance, in the above example of a photo quality print of an image by a professional service, the dialog boxes, payment options, or any other number of features presented to the user or application functionality (e.g., in response to user input) may be controlled by the code 970 specifically provided by the various trusted network entities (e.g., the payment provider 990, the merchant 905, etc.). Accordingly, as will be described in greater detail below, this code can also be used when evaluating payment options and other constraints from the merchant 905 and/or payment provider 990.

As mentioned above, in one embodiment, the selected service provider or merchant transmits any requirements to the identity provider with the request for identity verification. For example, service provider may be selling goods or services that require a minimum age or is restricted to a certain geographical location. Accordingly, the listing of identity providers may be limited to those that can provide identity credentials that satisfy the requirements of the service provider. For example, the list of identity providers may be restricted to those that can provide age verification or current address information, such as the RMV.

Likewise, a dialog box may be generated listing options for payment providers. For example, the dialog box may list payment providers 530a, 530b and 530c, which may include a credit card company, a bank offering electronic debit services, or a private third party offering financial services, respectively. As with the identity request, the selected service provider may include any payment requirements associated with the purchase. For example, the service provider may only accept a certain type of credit card. The payment requirements may then be reflected in the available payment providers listed or enabled in the payment

provider selection dialog box. After a payment provider is selected, payment certification may proceed and the transaction may be completed.

Note that other embodiments also provide for comparison of merchant constraints (e.g., available payment options, age restrictions, etc.) with consumer rules for determining various actions that may be taken. FIG. 10 illustrates such an embodiment, wherein a distributed system 1000 is configured to programmatically determine actions based on such things as merchant constraints 1010 and/or consumer rules 1035. For instance, merchant 1020 can define within the merchant constraints 1010 payment providers 1005 or types of payment acceptable for purchasing services and/or goods thereof. Decision module may then present such constraints to the user, e.g., in a user interface requesting user input 1040 for choosing one or more of the available payment options. Based on the user input 1040, the appropriate payment provider 1005 may be contacted for proper funding of the services and/or goods.

In another embodiment, consumer rules 1035 can also be used in addition to, or in place of, the merchant constraints 1010. For example, consumer rules 1035 may indicate that only certain types of payments can be made for certain types of merchants 1020. More specifically, the consumer rules 1035 may indicate that if a merchant 1020 is not registered or otherwise trusted, that only payments that can be reversed may be used for purchased made from the merchant 1020.

Of course, as described above, other merchant rules 1010 and consumer constraints 1035 can be used by decision module 1030 when determining actions to take in a commercial transaction. In fact, the merchant constraints 1010 and consumer rules 1035 may be compared for compatibility and other purposes. For example, the available payment options from the merchant 1020 can be compared to payment providers 1005 available or allowable by the consumer when presenting the user with a selection of payment providers 1005. Of course, the payment selection may also occur automatically based on such things as a default setting, provider ratings or preferences, or any other number of option settings. If fact, any number of actions may occur based on the implementation of the various merchant 1010 and/or consumer 1035 rules. For example, if the rules (merchant 1010 or consumer 1035) fail or are otherwise violated, additional input from the merchant 1020 or user 1040 (either

automatically based on additional rules or settings) may be needed to resolve conflicts or other discrepancies. Accordingly, any particular action taken when implement the constraints and/or rules defined are used herein for illustrative purposes only and are not meant to limit or otherwise narrow embodiments provided herein.

Further note that, as described above, the merchant constraints 1010 may be included within the billing information or provided separately to the consumer. Also note that the comparison of various rules and actions taken thereby may all occur under the covers, i.e., without the knowledge of the user and/or other system components. In addition, note that the present system is not limited to just constraints or rules defined by either the consumer or the merchant. For example, the payment provider may also define various restrictions that can also be considered in conjunction or instead of the consumer and/or merchant rules. Accordingly, the above use of merchant and consumer constraints for determining various actions (such as payment provider options) is used herein for illustrative purposes only and is not meant to limit or otherwise narrow embodiments herein described unless otherwise explicitly claimed.

In conventional online transactions, it may be difficult for both the end-user and/or the service provider to know for certain when a transaction is complete and whether the goods or services have been successfully delivered. For example, an end-user may select a software package for download over the network, or an end-user may purchase songs, movies or other electronic media. Sometimes a network connection may be disrupted before the download can be completed. Under such circumstances, the end-user may be tempted to select the merchandise again, but may be hesitant because the end-user does not know whether he or she will be double charged for the purchase. Likewise, the service provider may not know if a download was completed successfully and may double charge when a user attempts to remedy the disruption by selecting the merchandise again.

Applicant has appreciated that providing logging or auditing capabilities in the commercial transactions software may eliminate some of the uncertainties with respect to electronic downloads. For example, final execution of the payment option may depend on a signal from the auditing feature that the download is complete. That way, if a download is interrupted, the end-user can be certain that the selected payment option did not go through.

For example, commercial transactions software 585 from FIG. 5 (or other subsystems or network entity components as described herein) may include a logging feature that records all of the various steps of the commercial transactions conducted by the machine. The logging information may be used as proof of purchase or to otherwise memorialize transactions. In addition, commercial transactions software 585 may include monitoring capabilities for electronic downloads, which sends a verification of a successful download, only after which final payment will be made. By making payment contingent on a signal that the transfer of goods or services was completed successfully, issues of double billing may be addressed and substantially eliminated.

Software has been developed by companies to handle a wide variety of tasks including familiar word and document processing, spreadsheets, imaging editing, to more specialized tasks such as video editing, computer graphics software, web-content development applications, portfolio management software, etc. However, to own software that handles each task that an end-user may want to perform may be prohibitively expensive. Software packages can cost anywhere from hundreds to thousands to tens and even hundreds of thousands of dollars to obtain a single license. Moreover, an end-user may need the services of a particular application only occasionally or sporadically, such that the cost of purchasing the application may not be justified.

Applicant has appreciated the benefits of enabling an end-user to utilize software in a pay-as-you-go environment. In particular, an end-user may be charged only for the amount of time spent using the application, rather than paying the retail price for the software (where many of the features and/or the application would go largely unused). FIG. 6 illustrates a networked computer system having a commercial transaction framework that allows an end-user to pay for the amount of time spent using the application. Networked computer system 600 includes a network 605 interconnecting end-user node 610 to a plurality of identity providers 620, a plurality of payment providers 630, and plurality of service providers 640.

End-user node 610 may be a computer running on an operating system 695. Installed on the end-user computer may be a plurality of software applications 655. The software applications may have come bundled with the computer at purchase, may have been downloaded freely over a network, or otherwise distributed (often for free or for a nominal

charge, or for registering with the vendor) by the seller of the application. Application 655 may be any type of application and any number of applications may be installed on the computer. Service providers 640 may be associated with one or more applications installed on end-user computer 610. For example, service provider 640a may be one or more computers owned by the developer and seller of application 655a. Similarly, service providers 640b and 640c may be associated with applications 655b and 655c, respectively.

In the pay-as-you-go model, the service provided by the service providers is a license to use the associated applications installed on the computer. For example, when software (e.g., applications 655) is freely distributed, it may be initially disabled so that users cannot run the application without first obtaining a license from the seller of the application. The license may be obtained by initiating a commercial transaction with one or more of the service providers 640. For example, application 655a may be a desktop publishing application that an end-user would like to use for a couple hours to design a card or brochure. When the end-user opens application 655a, the end-user is notified that the end-user needs to purchase a license to use the application. For example, a dialogue box may appear listing the characteristics and prices of the various for-use licensing capabilities.

A license may be for a specified amount of time, for example, an hour or a day. The license may expire once the application has been closed down, or the license could remain active until the term has expired. The license could be based on operations or tasks that allow an end-user to complete one or more jobs or employ one or more desired features. Additional features to be used may increase the cost of the license. It should be appreciated that a license having any desired terms may be negotiated, as the aspects of the invention are not limited in this respect.

Once the end-user has selected a license option, the end-user may be instructed to select an identity provider and/or payment provider, or one or the other may be selected by default to initiate an online transaction. The transaction may be handled by commercial transaction software 685 substantially as described in any of the foregoing or following embodiments. When service provider receives a payment token from one of the payment providers 620, the service provider may transmit a license according to the terms agreed upon at the initiation of the transaction.

The received license may be processed by generic license service 690 so that the appropriate accessibility to the application may be invoked. The generic license service may then issue an enable key to application 655 so that the user may run the software and utilize its functionality according to the license. The enable key may include any information the application may need to provide the necessary services for the term indicated in the license. The enable key may include a password provided by the service provider such that the application knows that the license is valid and/or may simply rely on the representation from generic license service 690 that a valid license has been obtained. Once the application is operating, metering engine 694 may be notified to keep track of time and to indicate to the application when the license has expired. Alternatively, the application may be programmed to periodically query the metering engine and then disable itself when the license has expired. Moreover, by querying the metering engine, the application may give periodic warnings or updates to the user about the amount of time remaining in the purchased license, should the license include a term.

When the end-user is finished he may choose to have the completed product professionally printed and select a print option that initiates another online transaction such as the transaction described in connection with FIG. 5. The pay-as-you-go license may provide users with much more flexibility and give them access to software that they would not have had prior access to due to the cost of buying the software package with a lifetime license. In addition, software vendors can capitalize on revenue from user's who were unwilling to pay full retail price, but willing to pay for limited use and/or limited functionality.

Software piracy impacts profits across the entire software industry. User's of unlicensed software cost businesses relatively substantial amounts each year. Once a software product has been purchased, the seller has little control over where and to how many computers the software is installed. Illegally providing software for download over the Internet provides an even more pervasive method to distribute and obtain software that the end-user has not paid for. Applicant has appreciated that providing a relatively secure and simple commercial transactions framework with a pay as you go license scheme, for example, the framework described in the embodiment illustrated in FIG. 6, may mitigate or eliminate the piracy problems. Since the software is distributed freely by the seller, end-users can

appropriate the software anyhow they see fit. Since the software is enabled only through paying for a term license or task license, end-users are substantially limited in their ability to misuse the software.

As previously described, embodiments herein allow for authentication for identity and/or payment purposes using a mobile module (e.g., a subscriber identity module (SIM)) tied to a particular billing account of a mobile infrastructure or operating system. Unlike typical standards for mobile communications (e.g., Global Systems for Mobile communications (GSM), 3rd Generation Partnership Project, and other similar protocols), which occurs via a trusted radio network, authentication in accordance with embodiments herein takes place over an independent untrusted data network (e.g., the Internet). As a result, embodiments herein address many of the additional security concerns imposed by the use of such mobile modules (SIMs) in a Web Services and other independent network protocol environments. Such security concerns include among other things: determining a trusted network endpoint for the authentication of a server; authentication of a client to a mobile module or SIM device; authentication of a user to the SIM device; authentication of the SIM and authentication server; establishment of a secure network connection between the mobile module and network authentication server; and authentication of the user to the network authentication server.

Moreover, in order to comply with GSM, 3GPP, and other standards, additional requirements are placed on the terminal equipment, which will interact with the mobile module or SIM device. More specifically, the GSM, 3GPP, and other similar standards require that the SIM restrict access to certain types of information, including encryption keys, to the mobile terminal. In order to satisfy these requirements, embodiments herein provide an abstraction security profile that delegates processing and decoding of certain messages and security to the SIM device itself. For example, as shown in FIG. 11, a firewall 1090 defines a state machine and protocol messages for abstracting a SIM 1085 from a host device 1075 when communicating over an independent network 1060. More specifically, the firewall 1090 uses a formal state machine that limits or restricts the number and/or sequence of commands sent from a read driver within the host 1075 to the SIM 1085 itself. Accordingly, the SIM device 1080 (e.g., a cellular phone, SIM interface, etc.—note that "mobile module"

represents a generic term for a "SIM", but is used herein interchangeably unless otherwise specifically claimed) becomes the mobile terminal and the host device 1075 becomes a peripheral that complies with the communication protocol 1055 for the mobile network 1050. The following describes in greater detail some of the state machines and protocols used to address some of the additional security requirements and concerns outlined above.

Embodiments herein define a security profile for authentication over the untrusted independent network (i.e., a network independent of a radio network corresponding to the mobile module's infrastructure or operator system) in terms of various security levels that a given security token may represent. These include, but are not limited to, device security level, network security level, user security level, and service security level. At each level are different requirements and procedures for obtaining a security token. Accordingly, as described in greater detail below, each security level represents a differing level of authentication in the security model and each has certain requirements and/or assurances. Further, it should be noted that each security level may or may not be independent of the others. For example, it may not be necessary to establish a device security level before a network or user security level can be achieved; however, for proper assurances such hierarchical procedure may be desirable.

A device security level indicates physical possession of a mobile module, e.g., a SIM device such as a cellular phone. A device token (i.e., a SIM security token with a device security level) is typically issued locally by the mobile module or SIM device upon proper authentication by a user thereto. Such requirements for authenticating a user to the mobile module are normally set by the mobile infrastructure or mobile operator. Further, device authentication is usually enforced by the SIM device, however, other embodiments may provide for the use of other components in the authentication process. For example, the SIM or other device may require a password before the mobile module or other device will issue a device token. Of course, other forms of credentials for authentication on the device level are also contemplated herein.

In one embodiment, a SIM device requires the client or host computer to authenticate or identify itself to the mobile module before a device security token will issue. Further, the lifetime of a device token is typically controlled by the mobile module or SIM device using

policy set by the mobile infrastructure. In one embodiment, the lifetime or other requirements set by the mobile operator may be dynamically configured through the independent and/or radio network. If the device token does not have lifetime or other restrictions, typically the SIM does not require the user to re-authenticate to the mobile module more than once.

The network security level indicates an authenticated connection between the mobile module or SIM and the mobile infrastructure or network over the untrusted independent network. The network security level can be established without user presence or user interaction assuming an unlocked SIM device is accessible by the client or host computer. Typically, the network security level is a single factor authentication, which asserts proof of possession of the SIM device to the mobile infrastructure or operator. Typically, the mobile infrastructure will issue a network security token via an authentication server and through a challenge response type mechanism before issuing a network security token to a client or host computing device. This network security level token can then be used in subsequent authentication phases and provides transport level security to encrypt and/or sign further interactions between a client and an authentication server and/or mobile infrastructure.

FIG. 7A illustrates an independent network 700 configured to issue a network level security token for establishing a transport level secure communication between client and an authentication server. Typically, the client or host computing device 710 (which may be a personal computer, mobile phone, or other portable or non-mobile computing device) initiates the authentication request by sending a network security token request 725 to the mobile infrastructure 720 via the authentication/trusted server 715 (note, however, that the request may also be initiated by another device such as the SIM 705 itself). Usually, the request 725 will be unsigned when received by the authentication server 715, which can then sign and/or encrypt the request prior to sending to the mobile infrastructure 720 for validating that the request comes from the authentication server 715. The trusted server 715 can then query the mobile infrastructure 720 or mobile operator for a challenge 730, which will then be sent to the mobile module 705. The mobile module 705 uses a secret 740 shared between it and the mobile infrastructure 720 for generating a challenge response 735, which is then forwarded to

the client 710—note that typically the secret will be SIM 705 specific and set by the mobile operator 720.

The client 710 will use the challenge response 735 to generate a request security token response, which may also include the SIM identity and the challenge 730 for authentication purposes. Typically, the client will request that the mobile module 705 sign and/or encrypt the request security token response with the device's 705 shared secret 740 or other key such as the SIM's device token—although this may or may not be necessary. The request security token response and the challenge response 735 therein can be validated using, e.g., the shared secret 740. Note, as previously mentioned, that the request security token response may or may not be signed and/or encrypted by the same key used to generate the challenge response 735. In any event, if the mobile infrastructure 720 validates the challenge response 735 (i.e., the challenge response is valid and the mobile module has an active billing account), the mobile infrastructure 720 and/or authentication server 715 can respond by generating a message that contains a network security token 745 with encrypted session key(s), which are signed and/or encrypted using the shared secret 740. The message can further be signed using either the authentication server's 715's own security token (e.g., X.509 cert, Kerberos cert, etc.) or using the mobile infrastructure's 720's security token. The client 710 can then verify the signed message and pass the encrypted network session key(s) to the SIM 705 for decryption. Using the shared secret 740, the mobile module 705 can then return the un-encrypted session key(s) 750 to the client 710.

Note that in the above issuance of the network security token 745, the mobile module 705 typically needs an active billing account in good standing on the mobile infrastructure 720. Accordingly, upon verification of the challenge response 735 and such active billing account information, a trust may be established between the SIM 705 and mobile infrastructure 720 creating a virtual secure channel. The session key(s) 750 are then delegated or passed from the mobile module 705 to the software platform or stack of the host computing device 710 and from the mobile operator 720 to the authentication server 715 (if necessary). Note the physical proximity of the mobile module 705 with the host computing device 710 (which may be connected thereto via USB port, Bluetooth, or other wireless or wired connection) and the trusted relationship between the mobile infrastructure 720 and the

authentication server 715. These session key(s) 750 are then used by the client 710 and trusted server 715 for establishing a secure communication 755.

Note that there may be a second mode of operation for authenticating the mobile module 705, which may be used by the mobile infrastructure 720. In this case, the client host 710 may request that the SIM 705 generate and sign its own challenge (typically in the form of a Nonce). The client 710 can then attach the information as part of the device token when request the network security token 725 from the trusted server 715 or mobile infrastructure 720. If the mobile operator 720 can verify that the device token contains a valid challenge-response 735, it may directly issue a network token 745 back to the client 710 for decryption of session key(s) as described above.

As will be described in greater detail below, typically this network level security token 745 is required for allowing a client access to an authenticated service token, which can be used to request services and/or goods from third party services. Note also that in order to obtain the network token, the above presumes that the client or host computer device 710 has successfully determined the network endpoint for the authentication server 715 and/or mobile infrastructure 720. Additionally, it presumes that the client 710 and the user (not shown) have already authenticated to the SIM device 705. As described above, the network security level token 745 is used in subsequent authentication phases and provides transport level security to encrypt and sign further interactions between the client 710 and the trusted server 715. The lifetime of the network token 745 (and other tokens) is controlled by the authentication server 715 or mobile operator 720. Because the network token 745 servers as a session context between the SIM device 705 and the mobile infrastructure 720, the lifetime may be limited to hours or days, number of bytes passed, and/or may only be valid if the mobile module 705 is properly connected to the client 710.

As previously mentioned, a user security level indicates a user has authenticated to the network (the trusted server 715, mobile infrastructure 720, or other service) usually by providing information stored outside the SIM 705 or host computing device 710. Accordingly, the user security level in conjunction with the network security level establishes a multifactor authentication based on proof of possession of the SIM 705 and some outside knowledge (e.g., a user name/password). Typically, the trusted server 715 or the mobile

infrastructure 720 are the only components to issue a user level security, however, in some instances a third party service may also issue such user tokens. Accordingly, the mobile infrastructure 720 (or other service as the case may be) will verify a user through a challenge response mechanism before issuing a user security level token back to client 710. Note that the user security token is used by the client to sign and/or encrypt requests for service tokens as described below. It may not be recommended for the client to send a user security token to any service other than the trusted server (since typically no other service will be able to verify/use it). As with the above network token 745, the user token may have a limited lifetime controlled by the mobile operator 720, and may be limited by time duration, the number of bytes passed, and/or by the existence of the connection between the mobile module 705 and the client 710.

FIG. 7B illustrates an independent network 700 configured to issue a user level security token for establishing a multilevel secure communication between client 710 and an authentication server 715. The user network authentication phase allows the mobile operator 720 (or other server) to verify that a known person is in possession of a known device 705. Effectively the user to network phase is a two factor authentication phase and prevents the network from distributed denial of service attacks. In addition, it protects the user by preventing a stolen SIM device 705 from being inappropriately used.

The host computing device 710 may issue a request for user token 765, which is sent to the mobile infrastructure 720 via the trusted server 715. Usually, the request 765 will be unsigned when received by the authentication/trusted server 715, which can then sign and/or encrypt the request prior to sending to the mobile infrastructure 720 for validating that the request comes from the authentication server 715. The trusted server 715 can then query the mobile infrastructure 720 or mobile operator for a challenge 770, which will then be sent to the mobile module 705. Note that the challenge 770 may be generated using a different algorithm than the challenge 730 used for authenticating the device 705 to the network. The client 710 will extract the challenge 770 from the token message and pass it to the mobile module 705, indicating that this is a user authentication. Accordingly, the SIM 705 will request user credential(s) 775 from the client 710. The host computer 710 will then query the user 760 for user input 780, and return it to the mobile module 705. The SIM 705 or client

710 may optionally decide that the user input 780 or credential(s) should be encrypted with the network security key (i.e., the session key(s) 750 previously obtained.

Using the user input 780, the mobile module 705 will generate a challenge response 785 and return it to the client 710, which will generate and send a request security token response that includes, e.g., a SIM identifier, the challenge 770, and the challenge response 785. Typically, the client 710 will request that the mobile module 705 sign and/or encrypt the request security token response with the network security token 745, the shared secret key 740, or a SIM 705 specific key. Similar to above, the request security token response and the challenge response 785 therein can be validated using, e.g., the shared secret 740, or other mobile module 705 specific key. Note, as previously mentioned, that the request security token response may or may not be signed and/or encrypted by the same key used to generate the challenge response 785. In any event, if the mobile infrastructure 720 validates the challenge response 785 (i.e., the user credentials provided are proper), the mobile infrastructure 720 and/or authentication server 715 can respond by generating a message that contains a user security token 795 with encrypted user key(s), which are signed and/or encrypted using the shared secret 740 or other device 705 specific key. The message can further be signed using either the authentication server's 715's own security token (e.g., X.509 cert, Kerberos cert, etc.) or using the mobile infrastructure's 720's security token. The client 710 can then verify the signed message and pass the encrypted user session key(s) to the SIM 705 for decryption. Using the shared secret 740 (or other key as the case may be), the mobile module 705 can then return the un-encrypted user key(s) 790 to the client 710; thus authenticating the user to the network 792.

The user to service authentication phase provides a mechanism for the mobile network operator 720 to provide authentication on behalf of third party services. Similar to the user to network security level, the user to service phase is a multifactor authentication phase and prevents the network from issuing service tokens without a user 760 having been present during at least one phase of authentication. There are typically two modes of operation of the authentication server 715 regarding how service tokens are issued. First, if the user 760 has previously acquired a user token, the trusted server 715 may consider the user 760 to be authenticated and automatically issue a service token (provided that the request

for service token is appropriately signed with the user token 790, 795. If, on the other hand, the mobile infrastructure 720 has not issued a user token 790, 795, the user 760 will be required to authenticate in a manner similar to that outlined above for requesting a user token 795, 790.

FIG. 7C illustrates how the various network entities communicate over the independent network 700 when establishing secure communication between a client 710 and third party server 728. As mentioned above, the mobile device 705 and user 760 can authenticate to the mobile operator system 720 as previously described. Accordingly, a secure communication exists between the authentication server 715 and the client 710 upon proper validation of a billing account for the mobile device 705 and authentication of possession thereof by the user 760. The trusted server 715 (or mobile infrastructure 720 as the case may be) can then issue service tokens 724 for various services when, e.g., the client 710 wishes to purchase services and/or goods from a third party service 728. Accordingly, the client 710 can issue a service token 726 to the third party server, which then validates the token 722 through the authentication server 715. Note that the third party server 728 may or may not require additional authentication and can use various mechanisms as previously described for performing such validation. Also note that the use of the service token 726 not only establishes a secure communication between the client 710 and third party server 728, but may also indicate the user's 760's ability to pay for one or more services and/or goods in a manner similar to that previously described.

Note that typically up until the service token is issued to the client 710, the security tokens issued are of no value to any other service other than the authentication server 715. The reason is that the security hierarchy can prevent any outside party from properly decoding a device token, a network token, or even a user token, as they all derive from the root or shared key 740 known only to the SIM device 705 and the mobile infrastructure 720. It is typically after the authentication server 715 issues a service token 724 that an arbitrary third party 728 web service can make use of a security token 724. Also note that the above security tokens and messages (e.g., challenges, challenge responses, etc.) may take on various formats or schemas. For example, the tokens and/or messages may be XML, binary, or other similar encoding format, which can be issued by the mobile operator 720 who may or may

not wish to expose certain elements of the network to SIM communications to intermediate parties.

The above use of a portable hardware device 705 for authentication, identity, and/or payment validation can be used for purchasing online or local retail service and/or goods (e.g., online newspaper, music, software application, or other goods and service) or for an allowing access to an application running on the local PC or client 710 (e.g., Word®, Adobe Photoshop, Print program, pay-as-you go software, etc.). Accordingly, the above embodiments are especially advantageous for unlocking freely distributed protected software or content (e.g., music, videos, games, etc.) on a plurality of hosting devices 710. In other words, a license now becomes tied to the portable mobile device 705, which can be authenticated as described above allowing for a portable digital identity not tied to a limited set of computing devices. As such a user 760 goes to a friend's house and does not have to bring all of his/her programs or other protected content; it's all accessible and authenticated via the portable device 705.

As should be appreciated from the foregoing, there are numerous aspects of the present invention described herein that can be used independently of one another, including the aspects that relate to identity tokens, payment tokens, selecting one of a number of identity providers, selecting one of a number of payment providers, and the presence of commercial transaction software on an end-user system, a service provider system, an identity provider system, and a payment provider system. It should also be appreciated that in some embodiments, all of the above-described features can be used together, or any combination or subset of the features described above can be employed together in a particular implementation, as the aspects of the present invention are not limited in this respect.

The above-described embodiments of the present invention can be implemented in any of numerous ways. For example, the embodiments may be implemented using hardware, software or a combination thereof. When implemented in software, the software code can be executed on any suitable processor or collection of processors, whether provided in a single computer or distributed among multiple computers. It should be appreciated that any component or collection of components that perform the functions described above can be

generically considered as one or more controllers that control the above-discussed functions. The one or more controllers can be implemented in numerous ways, such as with dedicated hardware, or with general purpose hardware (e.g., one or more processors) that is programmed using microcode or software to perform the functions recited above.

It should be appreciated that the various methods outlined herein may be coded as software that is executable on one or more processors that employ any one of a variety of operating systems or platforms. Additionally, such software may be written using any of a number of suitable programming languages and/or conventional programming or scripting tools, and also may be compiled as executable machine language code. In this respect, it should be appreciated that one embodiment of the invention is directed to a computer-readable medium or multiple computer-readable media (e.g., a computer memory, one or more floppy disks, compact disks, optical disks, magnetic tapes, etc.) encoded with one or more programs that, when executed, on one or more computers or other processors, perform methods that implement the various embodiments of the invention discussed above. The computer-readable medium or media can be transportable, such that the program or programs stored thereon can be loaded onto one or more different computers or other processors to implement various aspects of the present invention as discussed above.

It should be understood that the term "program" is used herein in a generic sense to refer to any type of computer code or set of instructions that can be employed to program a computer or other processor to implement various aspects of the present invention as discussed above. Additionally, it should be appreciated that according to one aspect of this embodiment, one or more computer programs that, when executed, perform methods of the present invention need not reside on a single computer or processor, but may be distributed in a modular fashion amongst a number of different computers or processors to implement various aspects of the present invention.

Various aspects of the present invention may be used alone, in combination, or in a variety of arrangements not specifically discussed in the embodiments described in the foregoing, and the aspects of the present invention described herein are not limited in their application to the details and arrangements of components set forth in the foregoing description or illustrated in the drawings. The aspects of the invention are capable of other

embodiments and of being practiced or of being carried out in various ways. Various aspects of the present invention may be implemented in connection with any type of network, cluster or configuration. No limitations are placed on the network implementation. Accordingly, the foregoing description and drawings are by way of example only.

Use of ordinal terms such as "first", "second", "third", etc., in the claims to modify a claim element does not by itself connote any priority, precedence, or order of one claim element over another or the temporal order in which acts of a method are performed, but are used merely as labels to distinguish one claim element having a certain name from another element having a same name (but for use of the ordinal term) to distinguish the claim elements.

Also, the phraseology and terminology used herein is for the purpose of description and should not be regarded as limiting. The use of "including," "comprising," or "having," "containing," "involving," and variations thereof herein, is meant to encompass the items listed thereafter and equivalent thereof as well as additional items.

CLAIMS

1. A method of authorizing an online transaction between a purchaser and a merchant, the method comprising acts of:

providing, via an identity provider, verification of an identity of the purchaser; and

providing, via a payment provider, verification of an ability of the purchaser to pay for the transaction, wherein the identity provider and the payment provider are different network entities.

2. The method of claim 1, further comprising an act of providing, via the purchaser, identification information to facilitate the identity provider in verifying the identity of the purchaser.

3. The method of claim 2, wherein the act of providing identification information includes an act of providing a subscriber identity module (SIM) number, a network address, or a unique hardware identification (ID).

4. The method of claim 2, wherein the act of providing identification information includes providing identification information programmatically, via an end-user computer associated with the purchaser, the identification information provided upon an indication by at least one application operating on the end-user computer that the purchaser intends to make a purchase.

5. The method of claim 1, wherein the act of providing verification of the ability of the purchaser to pay is performed by the payment provider only after the identity of the purchaser is verified.

6. The method of claim 5, wherein the payment provider employs the identity verification to perform the payment verification.

7. The method of claim 1, wherein the identity provider is a bank or a government agency.

8. The method of claim 1, wherein the identify provider provides identification verification via an identity token to be received by the payment provider, and wherein the payment provider provides payment verification via a payment token to be received by the merchant.

9. The method of claim 8, wherein the identity token includes a predetermined interval of time during which the identity token can be processed, wherein, when the predetermined interval of time expires, the identity token is considered invalid.

10. The method of claim 8, wherein the payment token includes a predetermined interval of time during which the payment token can be processed, wherein, when the predetermined interval of time expires, the payment token is considered invalid.

11. A computer system having a plurality of nodes interconnected via a network, the computer system adapted to conduct an online transaction between a purchaser and a merchant, the computer system comprising:

a first node configured to provide verification of an identity of the purchaser; and

a second node configured to provide verification of an ability of the purchaser to pay for the transaction, wherein the first node and the second node are associated with different network entities.

12. The computer system of claim 11, further comprising a purchaser node associated with the purchaser, the purchaser node adapted to provide identification information to facilitate the first node in verifying the identity of the purchaser.

13. The computer system of claim 12, wherein the purchaser node provides a subscriber identity module (SIM) number, a network address, or a unique hardware identification as the identification information.

14. The computer system of claim 12, wherein the purchaser node includes an end-user computer that provides the identification information programmatically when a signal to initiate the transaction is issued by at least one application operating on the end-user computer.

15. The computer system of claim 11, wherein the second node provides verification of the ability of the purchaser to pay only after the first node verifies the identity of the purchaser.

16. The computer system of claim 15, wherein the second node employs the identity verification to perform the payment verification.

17. The computer system of claim 11, wherein the first node is associated with a network entity that is a bank or a government agency.

18. The computer system of claim 11, wherein the first node provides identification verification via an identity token to be received by the second node, and wherein the second node provides payment verification via a payment token to be received by the merchant.

19. The computer system of claim 18, wherein the identity token includes a predetermined interval of time during which the identity token can be processed, wherein when the predetermined interval of time expires, the identity token is considered invalid.

20. The computer system of claim 18, wherein the payment token includes a predetermined interval of time during which the payment token can be processed, wherein when the predetermined interval of time expires, the payment token is considered invalid.

21. A distributed program for conducting online transactions, the program having a plurality of software components distributed over a computer system having a plurality of nodes interconnected via a network, each of the plurality of components configured to communicate over the network with at least one other of the plurality of software components, the distributed program comprising:

a first component installed on a first node from which an end-user accesses the network, the first component adapted to provide an identifier over the network in response to an indication to conduct a transaction between the end-user and a merchant, the identifier associated with the end-user and/or the first node;

at least one second component of the distributed program installed on at least one second node, the at least one second component configured to receive the identifier and to provide verification of an ability of the end-user to pay for the transaction; and

a third component of the distributed program installed on a third node associated with the merchant, the third component configured to receive the verification of the ability of the end-user to pay before proceeding with the online transaction.

22. The distributed program of claim 21, wherein the at least one second component comprises:

an identification component of the distributed program installed on an identifier node associated with at least one identity provider, the identification component configured to

receive the identifier and provide an identity token verifying the identity of the end-user based on the identifier; and

a payment component of the distributed program installed on a payment node associated with at least one payment provider, the payment component configured to receive the identity token and to provide a payment token based on identity token, the payment token include the verification of the ability of the end-user to pay.

23. A computer system having a plurality of nodes interconnected via a network, the computer system adapted to facilitate an online transaction between a purchaser and a merchant providing one or more goods, services, or both, the computer system comprising:

a first network device associated with the purchaser, the first network device adapted to programmatically issue identification information indicative of the purchaser upon an indication from the purchaser to initiate the transaction, wherein the identification information is not a purchaser established password; and

a second network device associated with an identity provider, the second network device adapted to receive the identification information and to issue an identity token that verifies the identity of the purchaser for the transaction.

24. A method of authorizing an online transaction between a purchaser and a merchant, the method comprising acts of:

generating an identity token that provides verification of an identity of the purchaser, based on identification information other than a purchaser established password; and

generating a payment token that provides verification of an ability of the purchaser to pay for the transaction.

25. At a computing device in a distributed network environment, a method of authenticating a mobile module of portable device as being tied to a billing account of a mobile infrastructure in order to allow a user access to services, goods, or both, by validating the mobile module over a network independent of the mobile infrastructure's radio network, the method comprising:

receiving a request to authenticate a mobile module when attempting to gain access to services, goods, or both;

receiving one or more credentials from the mobile module used by a mobile infrastructure in validating billing account information thereof;

sending the one or more credentials to the mobile infrastructure over an independent network separate from the mobile infrastructure's radio network; and

receiving over the independent network authentication information corresponding to an activation status for the mobile module's billing account on the mobile infrastructure, thus allowing for a portable digital identity for controlling access to the services, goods, or both.

26. The method of claim 25, wherein the mobile module is a subscriber identity module (SIM) for the mobile infrastructure, and wherein the one or more credentials includes information based on a challenge from the mobile infrastructure and a shared key between the SIM and the mobile infrastructure.

27. The method of claim 26, wherein the SIM is included within a piece of hardware other than a radio transmission device and is attached to the computing device via one or more hard wired or wireless ports.

28. The method of claim 26, wherein the SIM is directly attached to the computing device via a special hardware connection designed specifically for the SIM.

29. The method of claim 25, wherein the services, goods, or both, are requested from a remote service connected to the independent network.

30. The method of claim 29, wherein the independent network includes the Internet.

31. The method of claim 30, wherein the services, goods, or both, are freely distributed over the Internet and reside on a local computing device, and wherein the authentication of the mobile module allows the contents of the services, goods, or both, to be unlocked on the local computing device.

32. The method of claim 25, wherein the services, goods, or both, are one or more of: a software program on the computing device; a piece of hardware attached to the computing device; multimedia content for consumption by the computing device; or access to the computing device itself.

33. The method of claim 32, wherein the services, goods, or both, have multiple levels of available access, and wherein based on the authentication of the mobile device one or more of the available levels is activated.

34. The method of claim 25, wherein the method further comprises:

based on the activation status of the mobile module, determining if a contract agreement made between a merchant for the services, goods, or both, and the mobile infrastructure requires the user to enter one or more user input credentials for authenticating the user, wherein if true the method further includes:

sending a request to the user to input the one or more user input credentials; and

based on the user input, determining if the user is authorized to access the protected service.

35. The method of claim 34, wherein the user input credentials are stored at one or more of the mobile module, the mobile infrastructure, or a server corresponding to the merchant.

36. The method of claim 25, wherein if the mobile module is not authenticated by the mobile infrastructure, the method further comprises:

receiving over the independent network a deactivation message for deactivating the mobile module.

37. At a mobile infrastructure in a distributed network environment, a method of authenticating a mobile module of a portable device as being tied to a billing account of the mobile infrastructure in order to allow a user access to services, goods, or both, by validating the mobile module over a network independent of the mobile infrastructure's radio network, the method comprising:

receiving a request to authenticate a mobile module when a user is attempting to gain access to services, goods, or both, wherein the mobile module corresponds to a billing account of a mobile infrastructure, and wherein the request is received over an independent network separate from the mobile infrastructure's radio network;

receiving over the independent network one or more credentials from the mobile module; and

based on validation of the one or more credentials, sending over the independent network authentication information corresponding to an activation status for the mobile module's billing account, thus allowing for a portable digital identity for controlling access to the services, goods, or both, via two independent networks.

38. The method of claim 37, wherein the mobile module is a subscriber identity module (SIM) for the mobile infrastructure, and wherein the method further includes:

sending a challenge to the SIM device over the independent network;

receiving a response that includes the one or more credentials, which correspond to information within the challenge and a shared key between the SIM and the mobile infrastructure; and

based on the response to the challenge, authenticating the SIM's activation status according to information for the billing account.

39. The method of claim 38, wherein the request, the one or more credentials, and authentication information is routed to the mobile infrastructure via a trusted server and wherein the authentication establishes a trusted communication between the SIM and the trusted server.

40. The method of claim 38, wherein the SIM is part of a device that cannot communicate to over the mobile infrastructure's radio network.

41. The method of claim 37, wherein the services, goods, or both, are requested from a remote service connected to the independent network.

42. The method of claim 37, wherein the independent network includes the Internet.

43. The method of claim 42, wherein the services, goods, or both, are freely distributed over the Internet and reside on a local computing device, and wherein the authentication of the mobile module allows the contents of the services, goods, or both, to be unlocked on a local computing device.

44. The method of claim 37, wherein the services, goods, or both, are one or more of: a software program on a computing device; a piece of hardware attached to the computing device; multimedia content for consumption by the computing device; or access to the computing system itself.

45. The method of claim 37, wherein the method further comprises:

based on the activation status of the mobile module, determining if a contract agreement made between a merchant for the services, goods, or both, and the mobile infrastructure requires a user to enter one or more user input credentials for authenticating the user, wherein if true the method further includes:

sending a request to the mobile module to prompt the user to input the one or more user input credentials; and

based on the user input, determining if the user is authorized to access the protected service.

46. The method of claim 34, wherein the user input credentials are stored at one or more of the mobile module, the mobile infrastructure, or a server corresponding to the merchant.

47. The method of claim 37, wherein if the mobile module is not authenticated by the mobile infrastructure, the method further comprises:

sending a deactivation message over the mobile infrastructure's radio network, the independent network, or both, for deactivating the mobile module.

48. A portable device used to interface a mobile module with a local computing machine used in authenticating the mobile module as having a valid billing account for a mobile infrastructure in order to allow a user access to services, goods, or both, the portable device comprising:

a case holder for securing holding a mobile module that has a billing account with a mobile infrastructure used to validate the mobile module when attempting to gain access to services, goods, or both, on a local computing machine;

an interface that allows the portable device to:

send one or more credentials from the mobile module to the local computing device for authenticating the mobile module to the mobile infrastructure, and

receive authentication information from the local computing device that validates a status for the billing account,

wherein the interface allows the sending and receiving of information over an independent network separate from the mobile infrastructure's radio network, thus allowing

for a portable digital identity for controlling access to the services, goods, or both via two independent networks.

49. The portable device of claim 48, wherein the mobile module is a subscriber identity module (SIM) for the mobile infrastructure, and wherein the one or more credentials includes information based on a challenge from the mobile infrastructure and a shared key between the SIM and the mobile infrastructure.

50. The portable device of claim 49, wherein the case holder is a piece of hardware other than a radio transmission device and then interface allows for the portable device to attach to the local computing device via one or more hard wired or wireless ports.

51. The portable device of claim 49, wherein the independent network includes the Internet.

52. The portable device of claim 49, wherein the services, goods, or both, are freely distributed over the Internet and reside on the local computing device, and wherein the authentication of the mobile module allows the contents of the services, goods, or both, to be unlocked on the local computing device.

53. The portable device of claim 49, wherein the services, goods, or both, are one or more of: a software program on the local computing device; a piece of hardware attached to the local computing device; multimedia content for consumption by the local computing device; or access to the local computing device itself.

54. The portable device of claim 53, wherein the services, goods, or both, have multiple levels of available access, and wherein based on the authentication of the mobile device one or more of the available levels is activated.

55. The portable device of claim 49, wherein the interface is further used to receive user credentials for validating the user.

56. The portable device of claim 55, wherein the user input credentials are stored at one or more of the mobile module, the mobile infrastructure, or a server corresponding to the merchant.

57. At a computing device in a distributed network environment, a method of allowing access to freely distributed services, goods, or both, on a computing device configured to authenticate a portable device as being tied to a billing account of a mobile

infrastructure over a network independent of the mobile infrastructure's radio network, the method comprising:

receiving at a local computing device one or more freely distributed service, goods, or both, that includes protected content that only authorized computing devices are allowed access thereto;

receiving one or more credentials from a mobile module used by a mobile infrastructure in validating billing account information thereof;

sending the one or more credentials to the mobile infrastructure over an independent network separate from the mobile infrastructure's radio network;

receiving over the independent network authentication information corresponding to an activation status for the mobile module's billing account on the mobile infrastructure; and

based on the authentication information, receiving a license that allows the local computing device access to a least a portion of the protected content, thus allowing a portable digital identity to access the services, goods, or both, on a plurality of different computing devices without restricting a number of computing devices licensed to access the protected content.

58. The method of claim 57, wherein the freely distributed services, goods, or both, are received via the independent network or purchased at a store and directly installed on the local computing device.

59. The method of claim 57, wherein the license is limited in lifetime, whether the mobile module is connected to the local computing machine, or both.

60. The method of claim 57, wherein the mobile module is a subscriber identity module (SIM) for the mobile infrastructure, and wherein the one or more credentials includes information based on a challenge from the mobile infrastructure and a shared key between the SIM and the mobile infrastructure.

61. The method of claim 57, wherein the SIM is included within a piece of hardware other than a radio transmission device and is attached to the computing device via one or more hard wired or wireless ports.

62. The method of claim 57, wherein the SIM is directly attached to the local computing device via a special hardware connection designed specifically for the SIM.

63. The method of claim 57, wherein the services, goods, or both, are requested from a remote service connected to the independent network.

64. The method of claim 57, wherein the independent network includes the Internet.

65. The method of claim 57, wherein the services, goods, or both, are one or more of: a software program on the local computing device; a piece of hardware attached to the local computing device; or multimedia content for consumption by the local computing device.

66. The method of claim 57, wherein the services, goods, or both, have multiple levels of available access, and wherein based on the license one or more of the available levels is activated.

67. In a computing system tied to a distributed network, a method of using a single portable hardware device for allowing access to protected services, goods, or both, that require either single-factor or multifactor authentication, the method comprising:

sending one or more credentials from a mobile module to a local computing device that requests access to protected services, goods, or both, in order to allow the local computing device access thereto if the mobile module has an active billing account with a mobile infrastructure, which is configured to also authenticate a user in a multifactor process, and wherein the one or more credentials for the mobile module are sent over an independent network separate from the mobile infrastructure's radio network;

receiving, from the local computing device, authentication information corresponding to an activation status for the mobile module's billing account; and

based on the authentication information, determining if the protected services, goods, or both, further require user authentication, wherein if true the method further comprises:

sending a request for one or more user input credentials for comparison with a securely stored version thereof; and

based on information about the comparison, determining if the user is authorized to access the protected services, goods, or both, for allowing.

68. The method of claim 67, wherein the one or more user input credentials are encrypted using a shared key between the mobile module and the mobile infrastructure, the method further comprising:

sending the encrypted one or more user input credentials to the local computing device for transfer to the mobile infrastructure via the independent network for comparison thereof;

receiving the information about the comparison indicating that the user as appropriately authenticated to the mobile infrastructure; and

sending a license to the local computing device allowing the user access to protected services, goods, or both.

69. The method of claim 68, wherein the license is limited based on: lifetime, the proximity of the mobile module to the local computing device, or both, and wherein upon expiration of the license the user and the mobile module are required to re-authenticate to the mobile infrastructure in order to gain further access to the protected services, goods, or both.

70. The method of claim 68, wherein the one or more user input credentials are specific to a merchant of the goods, services, or both, and wherein the merchant has a trusted contractual relationship with the mobile infrastructure that indicates that the one or more user credentials are needed for authentication purposes.

71. The method of claim 68, wherein the protected services, goods, or both, correspond to an application running on the local computing device connected to the mobile module.

72. The method of claim 67, wherein the protected services, goods, or both, correspond to an application running on the local computing device connected to the mobile module, and wherein the one or more user input credentials are stored on the local computing device.

73. The method of claim 67, wherein the protected services, goods, or both, are remotely controlled by a service in the distributed system, and wherein the one or more user input credentials are stored at a remote server.

74. The method of claim 67, wherein the mobile module is a subscriber identity module (SIM), and wherein the one or more credentials are determined based on a challenge

from the mobile infrastructure and a shared key between the SIM device and the mobile infrastructure.

75. The method of claim 74, wherein the SIM is included within a piece of hardware other than a radio transmission device and is attached to the computing device via one or more hard wired or wireless ports.

76. The method of claim 74, wherein the SIM is directly attached to the local computing device via a special hardware connection designed specifically for the SIM.

77. The method of claim 67, wherein the services, goods, or both, are one or more of: a software program on the local computing device; a piece of hardware attached to the local computing device; or multimedia content for consumption by the local computing device.

78. At a mobile infrastructure tied to a distributed network, a method of using a single portable hardware device for allowing access to protected services, goods, or both, that require either single-factor or multifactor authentication, the method comprising:

receiving one or more credentials from a mobile module indicating a request for access to protected services, goods, or both, in order to allow a local computing device access thereto, wherein the one or more credentials for the mobile module are received over an independent network separate from the mobile infrastructure's radio network;

using the one or more credentials for authenticating the mobile module as having an active billing account with the mobile infrastructure, which is configured to also authenticate a user in a multifactor process; and

determining if the protected services, goods, or both, further require user authentication, wherein if true the method further comprises:

sending over the independent network a request for one or more user input credentials for comparison with a securely stored version thereof,

receiving the one or more user input credentials over the independent network, wherein the one or more user input credentials received are encrypted using a shared key between the mobile module and the mobile infrastructure,

based on the comparison of the encrypted one or more user input credentials with the securely stored version thereof, sending information indicating the

authentication of the user to the mobile infrastructure allowing a issuance of a license for providing the local computing device access to the protected services, goods, or both.

79. The method of claim 78, wherein the license is limited based on: lifetime, the proximity of the mobile module to the local computing device, or both, and wherein upon expiration of the license the user and the mobile module are required to re-authenticate to the mobile infrastructure in order to gain further access to the protected services, goods, or both.

80. The method of claim 78, wherein the one or more user input credentials are specific to a merchant of the goods, services, or both, and wherein the merchant has a trusted contractual relationship with the mobile infrastructure that indicates that the one or more user credentials are needed for authentication purposes.

81. The method of claim 78, wherein the protected services, goods, or both, correspond to an application running on the local computing device connected to the mobile module.

82. The method of claim 78, wherein the mobile module is a subscriber identity module (SIM), and wherein the one or more credentials are determined based on a challenge from the mobile infrastructure and a shared key between the SIM device and the mobile infrastructure.

83. The method of claim 82, wherein the shared key for encrypting the one or more user credentials is different from the shared key used for the one or more credentials from the mobile module.

84. In a distributed system, a computing framework used to abstract a host computer from a mobile operator system when connecting a mobile module thereto in order to label the host computer as peripheral equipment rather than a mobile terminal subject to strict requirements of the mobile operator system, the computing framework comprising:

a subscriber identity module (SIM) that includes information associated with a billing account for a mobile operator system;

a host computer connecting the SIM to the mobile operator system over a network independent of the mobile operator system's radio network in order to authenticate the billing account information for the SIM;

a SIM driver attached to the host computer for reading information from the SIM for use in at least authenticating the SIM to the mobile operator system over the independent network; and

an interface acting as a firewall between the SIM and the SIM driver that defines a protocol used to protect the SIM from attack by restricting one or more of a number, sequence, or length, of commands sent between the SIM driver and the SIM.

85. The computing framework of claim 84, wherein the SIM is connected to the host computer through a hardware port, wireless port, or both.

86. The computing framework of claim 84, wherein the interface is part of a portable device used in connecting the SIM to the host computer.

87. The computing framework of claim 86, wherein the portable device is not configured for radio communications over the mobile operator system's network.

88. The computing framework of claim 84, wherein the authentication of the SIM over the independent network is used for gaining access to the host computing device.

89. The computing framework of claim 84, wherein the authentication of the SIM is used for gaining access to services, goods, or both, offered over the independent network.

90. The computing framework of claim 84, wherein the authentication of the SIM device is for services, goods, or both, offered over the independent network and associated with a software application running on the host computer separate from a Web browsing application.

91. The computing framework of claim 84, wherein the protocol includes a formal state machine that is used to keep track of the one or more of the number, sequence, or length of the communications between the SIM driver and the SIM.

92. In a computing system tied to a distributed network, a method of establishing transport level secure communications between a client and a server over an otherwise insecure network by establishing a secure tunneling between a mobile module connected to the client and a mobile infrastructure associated therewith in order to delegate session keys to at least a software stack on the client for one or more of encryption or signing purposes, the method comprising:

identifying one or more credentials of a mobile module connected to a host computer;

sending the one or more credentials to a mobile infrastructure for authentication of a valid billing account for the mobile module, wherein the request is sent over an independent network separate form a radio network corresponding to the mobile infrastructure; and

based on the authentication, receiving from the mobile module a session key for use in a transport level secure communication over the independent network between the host computer and a server.

93. The method of claim 92, wherein the mobile module is a subscriber identity module (SIM) for the mobile infrastructure, and wherein the one or more credentials includes information based on a challenge from the mobile infrastructure and a shared key between the SIM and the mobile infrastructure.

94. The method of claim 93, wherein the SIM is included within a piece of hardware other than a radio transmission device and is attached to the computing device via one or more hard wired or wireless ports.

95. The method of claim 93, wherein the independent network includes the Internet.

96. The method of claim 93, wherein the server is part of a framework that has a trusted relationship with the mobile infrastructure such that the session keys are also passed from the mobile infrastructure to the server for the transport level secure communication with the host computer.

97. The method of claim 96, further comprising:

requesting a connection to a third party server not part of the framework;

receiving another session key for secure communication between the host computer and the third party server; and

using the another session key for transport level secure communication with the third party server.

98. The method of claim 97, wherein prior to using the another session key for communicating with the third party, the method further comprises:

sending the another session key and a token to the third party server, wherein the third party server validates the another session key by authenticating the token through the trusted server that is part of the framework; and

based on the authentication of the token, using the another session key for secure communication with the third party server.

99. The method of the claim 98, wherein the third party server is a merchant of services, goods, or both, and wherein a user must also authenticate to the third party server by providing user input credentials.

100. The method of claim 99, wherein authentication of the SIM to the mobile infrastructure by validating the billing account thereof is used as verification of a payment funds for the services, goods, or both, when making a purchase from the merchant.

101. The method of claim 93, wherein the session key expires based on one or more of a lifetime of the session key or a number of messages encrypted, signed, or both, with the session key, whereupon expiration the SIM is required to reauthorize with the mobile infrastructure for further secure communication between the host computer and the server.

102. The method of claim 93, wherein the SIM is externally connected to the host computer, yet maintained within physical close proximity thereto.

103. The method of claim 102, wherein the physical close proximity is within 10 yards.

104. The method of claim 103, wherein the external connection is a wireless connection.

105. The method of claim 93, wherein the session key is derived from the SIM and the mobile infrastructure based on a shared secret between the SIM and the mobile infrastructure.

106. The method of claim 93, wherein the session key is received from the mobile infrastructure encrypted by a shared key between the SIM and the mobile infrastructure, wherein prior to receiving the session key from the SIM the method further comprises:

sending the encrypted key to the SIM for decryption thereof using the shared key in order to provide the session key to the host computer without compromising the shared key.

107. In a mobile infrastructure tied to a distributed network over an otherwise insecure network independent of the mobile infrastructure's radio network, a method of establishing transport level secure communications between a client and a server over

insecure network by establishing a secure tunneling between a mobile module connected to the client and the mobile infrastructure in order to delegate session keys to a trusted server for one or more of encryption or signing purposes, the method comprising:

receiving one or more credentials of a mobile module connected to a host computer, wherein the one or more credentials are received over an independent network separate from a radio network corresponding to the mobile infrastructure;

authenticating the one or more credentials as being part of a valid billing account for the mobile module; and

based on the authentication, sending a session key to a server for use in a transport level secure communication over the independent network between the host computer and the server.

108. The method of claim 107, wherein the mobile module is a subscriber identity module (SIM) for the mobile infrastructure, and wherein the one or more credentials includes information based on a challenge from the mobile infrastructure and a shared key between the SIM and the mobile infrastructure.

109. The method of claim 108, wherein the independent network includes the Internet.

110. The method of claim 108, wherein the server is part of a framework that has a trusted relationship with the mobile infrastructure such that the session keys are also passed from the mobile infrastructure to the server for the transport level secure communication with the host computer.

111. The method of claim 108, wherein authentication of the SIM to the mobile infrastructure by validating the billing account thereof is used as verification of available payment funds for services, goods, or both, when making a purchase from a merchant.

112. The method of claim 108, wherein the session key expires based on one or more of a lifetime of the session key or a number of messages encrypted, signed, or both, with the session key, whereupon expiration the SIM reauthorizes with the mobile infrastructure for further secure communication between the host computer and the server.

113. The method of claim 108, wherein the session key is derived from the SIM and the mobile infrastructure based on a shared secret between the SIM and the mobile infrastructure.

114. At a host computer in a distributed computing system, a method of establishing secure communication between the host computer and a server by using a protocol that authenticates a subscriber identity module (SIM) to a mobile infrastructure over a network connection independent from a radio network associated therewith, the method comprising:

creating a request for a session key which includes a computed challenge response from a subscription identity module (SIM) attached to a host computer attempting to establish a secure communication with a server, wherein the challenge response is used to authenticate the SIM to a mobile infrastructure that holds billing status information thereof;

sending the request for a session key to the server, which has a trusted relationship with the mobile infrastructure, the request for the session key sent over a network independent of a radio network related to the mobile infrastructure;

receiving a response to the request for a session key, which includes the session key and is signed, encrypted, or both, by mobile infrastructure using a shared key, which indicates that the SIM appropriately authenticated to the mobile infrastructure using the challenge response;

sending the session key to the SIM for validation using the shared key, which establishes a tunneled communication between the SIM and the mobile infrastructure; and

upon validation of the session key, allowing the host computer to use the decrypted session key for secure communicating with the server.

115. The method of claim 114, wherein the response to the request for the session key is signed by the server, the mobile infrastructure, or both.

116. The method of claim 114, wherein the challenge response includes a Nonce signed by SIM using the shared key such that the challenge response is self generated by the SIM.

117. The method of claim 114, wherein the shared key is SIM specific.

118. The method of claim 114, wherein the request for the session key is signed, encrypted, or both, using a token specified by the server.

119. The method of claim 114, wherein the request for the session key is singed, encrypted, or both, using a token specific to the host computer.

120. The method of claim 114, wherein prior to sending the challenge response, a challenge is received that is used by the SIM to generate the challenge response.

121. The method of claim 114, wherein upon authenticating the SIM to the mobile infrastructure, the method further comprises the following for authenticating a user to the mobile infrastructure over the independent network:

creating a request for a user token used in authenticating a user to one or more of the mobile infrastructure, the server, or other third party services;

sending the request for the user token to the server over the network independent of the radio network related to the mobile infrastructure;

receiving a response to the request for a user token, which includes a challenge generated from the mobile infrastructure;

sending the challenge to the SIM indicating that the challenge corresponds to a user authentication in order to prompt the SIM to request one or more user credentials;

receiving user input specifying the one or more user credentials, which are then forwarded to the SIM for determining an appropriate challenge response;

sending the challenge response that includes the one or more user credentials to the server;

receiving the user token that is signed, encrypted, or both, using the shared key by the mobile infrastructure indicating that the user has appropriately authenticated; and

sending the user token to the SIM for validation using the shared key; and

upon validation of the session key, allowing the host computer to use the user token in subsequent communication to the server or a third party services for secure communications therewith.

122. The method of the claim 121, wherein the user token is used to request a service session key that is sent to third party service, and wherein the third party service validates the service session key through the server.

123. The method of the claim 122, wherein the service session key is provided by the server in a token separate from the user token upon request from the host computer and authentication of the user to the server.

124. At a mobile operator system in a distributed computing environment, a method of establishing secure communication between a host computer and a server by using a protocol that authenticates a subscriber identity module (SIM) to the mobile operator system over a network connection independent from a radio network associated therewith, the method comprising:

receiving a request for a session key which includes a computed challenge response from a subscription identity module (SIM) attached to a host computer attempting to establish a secure communication with a server, which has a trusted relationship with a mobile infrastructure corresponding to the SIM, wherein the request for the session key sent over a network independent of a radio network related to the mobile infrastructure

using the challenge response to authenticate the SIM has having a valid billing account with the mobile infrastructure;

securing the session key by signing, encrypting, or both, using a shared key, which indicates that the SIM appropriately authenticated to the mobile infrastructure using the challenge response;

sending a response to the request, which includes the session key, to the host computer for allowing the attached SIM to validate the session key using the shared key, which establishes a tunneled communication between the SIM and the mobile infrastructure; and

sending the session key to the server for establishing a network level secure communication with between the server and the host computer.

125. The method of claim 124, wherein the response to the request for the session key is signed by the server, the mobile infrastructure, or both.

126. The method of claim 124, wherein the challenge response includes a Nonce signed by SIM using the shared key such that the challenge response is self generated by the SIM.

127. The method of claim 124, wherein the shared key is SIM specific.

128. The method of claim 124, wherein the request for the session key is signed, encrypted, or both, using a token specified by the server.

129. The method of claim 124, wherein the request for the session key is singed, encrypted, or both, using a token specific to the host computer.

130. The method of claim 124, wherein prior to sending the challenge response, a challenge is received that is used by the SIM to generate the challenge response.

131. The method of claim 124, wherein upon authenticating the SIM to the mobile infrastructure, the method further comprises the following for authenticating a user to the mobile infrastructure over the independent network:

receiving a request for a user token used in authenticating a user to the mobile infrastructure, the request for the user token received over the network independent of the radio network;

sending a challenge generated from the mobile infrastructure for requesting the SIM to obtain one or more user credentials;

receiving a challenge response that includes the one or more user credentials;

based on the validation of the one or more user credentials, securing a user token by signing, encrypting, or both, using the shared key indicating that the user has appropriately authenticated to the mobile infrastructure; and

sending the user token to the SIM for validation using the shared key in order to allow the host computer to use the user token in subsequent communication to the server or a third party services for secure communications therewith.

132. At a consumer computing device in a distributed system, a method of providing a secure commercial transaction for online purchase of services, goods, or both, by establishing a three-way exchange of data between computing devices for a consumer, merchant, and payment provider, the method comprising:

sending an online request to purchase one or more services, goods, or both, offered by a merchant;

receiving billing information from the merchant, which includes a cost associated with the purchase of the one or more services, goods, or both;

sending a request for payment authorization for the cost from a consumer computing device to at least one payment provider, wherein the consumer has a billing account with the at least one payment provider;

receiving from the at least one payment provider a payment token as proof of an ability for the consumer to pay for at least a portion of the one or more services, goods, or both, wherein the payment token uniquely identifies the authorization of payment for the at least a portion of the cost without providing sensitive information about the billing account for the consumer;

sending the payment token from the consumer computing device to the merchant, wherein the merchant uses the payment token to validate payment with the payment provider, which makes the sensitive information about the billing account opaque to the merchant while still providing for secure payment validation; and

receiving acknowledgment of the validity of the payment token indicating appropriate transfer of the one or more services, goods, or both, from the merchant to the consumer.

133. The method of claim 132, wherein the billing information further includes one or more of a description of the services, goods, or both, available payment options from the merchant, or merchant specific information.

134. The method of claim 133, wherein the billing information is presented to the at least one payment provider when requesting the payment authorizing for the services, goods, or both.

135. The method of claim 134, wherein the payment token includes the billing information, which is then signed, encrypted, or both, by the at least one payment provider for validating the payment token and for matching the payment token to the request for payment authorization from the consumer.

136. The method of claim 135, wherein the request for payment authorization, the presentation of the billing information to the at least one payment provider, and the sending of the payment token to the merchant occur automatically without interaction from the consumer.

137. The method of claim 133, wherein based on the available payment options provided by the merchant the method further includes:

presenting the consumer with a user interface that shows one or more of the available payment options;

receiving user input from the consumer selecting the at least one payment provider; and

based on the user input, establishing a communication channel between the consumer computing device and the at least one payment provider for requesting the payment authorization.

138. The method of claim 132, wherein the at least one payment provider is chosen based on a default payment provider preset by the consumer.

139. The method of claim 132, wherein the at least one payment provider is one of a mobile infrastructure that has billing account information for a SIM device owned by the consumer, a credit card company for the consumer, a prepay service for the consumer, or a banking account for the consumer.

140. The method of claim 132, wherein the commercial transaction is a seamless in-band experience in that the payment and selection of the service, goods, or both, are integrated into a single application that is not part of a web browser.

141. The method of claim 132, wherein the payment token expires after some predetermined time period, frequency of use, or both, set by the at least one payment provider.

142. The method of claim 132, wherein the cost is variable and presented in the billing information as a range of values.

143. The method of claim 132, wherein the payment token is revocable by the consumer, the at least one payment provider, or both.

144. The method of claim 132, wherein the cost is over a predetermined amount allowed by the at least one payment provider, and wherein additional user interaction is needed for authorization of the payment token.

145. The method of claim 132, wherein the payment token is signed, encrypted, or both, by the at least one payment provider, and wherein the validation of the payment token to the at least one payment provider includes validating the signature, the encryption, or both.

146. The method of claim 132, wherein the one or more services, goods, or both, require subscription or multiple payments, and wherein the payment token can be used multiple times for such payment.

147. The method of claim 132, wherein the one or more services, goods, or both, require subscription or multiple payments, and wherein the payment token is valid for only a single payment of the subscription or multiple payments, and wherein additional tokens are needed for subsequent payments.

148. At a merchant computing device in a distributed system, a method of performing a secure commercial transaction when allowing a purchase of services, goods, or both, by establishing a three-way exchange of data between computing devices for a consumer, merchant, and payment provider, the method comprising:

receiving an online request to purchase one or more services, goods, or both, offered by a merchant;

sending billing information to a consumer, which includes a cost associated with the purchase of the one or more services, goods, or both;

receiving a payment token from the consumer as an offer of proof of an ability for the consumer to pay for at least a portion of the one or more services, goods, or both, wherein the payment token uniquely identifies an authorization of payment by a payment provider for the at least a portion of the cost without providing sensitive information about a billing account of the consumer with the payment provider;

sending a request for validation of the payment token to the payment provider, thus allowing the merchant to securely validate payment of at least a portion of the cost while making the sensitive information about the billing account opaque to the merchant; and

based on validation of the payment token, sending an acknowledgment of the validity of the payment token indicating appropriate transfer of the one or more services, goods, or both, from the merchant to the consumer.

149. The method of claim 148, wherein the billing information further includes one or more of a description of the services, goods, or both, available payment options from the merchant, or merchant specific information.

150. The method of claim 149, wherein the payment token includes the billing information, which is signed, encrypted, or both, by the at least one payment provider for validating the payment token and for matching the payment token to a request for payment authorization from the consumer.

151. The method of claim 148, wherein the payment token expires after some predetermined time period, frequency of use, or both, set by the payment provider.

152. The method of claim 148, wherein at least a portion of the cost is variable and presented in the billing information as a range of values.

153. The method of claim 148, wherein the payment token is revocable by the consumer, the payment provider, or both.

154. The method of claim 148, wherein the cost is over a predetermined amount allowed by the payment provider, and wherein additional user interaction is needed for authorization of the payment token.

155. The method of claim 148, wherein the one or more services, goods, or both, require subscription or multiple payments, and wherein the payment token can be used multiple times for such payment.

156. At a payment provider computing device in a distributed system, a method of authorizing payment in a commercial transaction for a purchase of services, goods, or both, by establishing a three-way exchange of data between computing devices for a consumer, merchant, and payment provider, the method comprising:

receiving a request for payment authorization from a consumer purchasing one or more services, goods, or both, from a merchant, wherein the request for payment authorization includes billing information for a cost associated with the purchase;

based on a billing account status for the consumer, sending a payment token to the consumer as proof of an ability for the consumer to pay for the one or more services, goods, or both, wherein the payment token uniquely identifies the authorization of payment for the one or more services, goods, or both, without providing sensitive information about the billing account for the consumer;

receiving from the merchant a request to validate the payment token; and

based on the comparison of the payment token with the billing information from the request for payment authorization, sending an acknowledgment of the validity of the payment token indicating that payment will be provided to the merchant upon appropriate transfer of the one or more services, goods, or both, to the consumer.

157. The method of claim 156, wherein the billing information further includes one or more of a description of the services, goods, or both, available payment options from the merchant, or merchant specific information.

158. The method of claim 156, wherein the at least one payment provider is one of a mobile infrastructure that has billing account information for a SIM device owned by the consumer, a credit card company for the consumer, a prepay service for the consumer, or a banking account for the consumer.

159. The method of claim 156, wherein the payment token expires after some predetermined time period, frequency of use, or both, set by the payment provider.

160. The method of claim 156, wherein the cost is variable and presented in the billing information as a range of values.

161. The method of claim 156, wherein the payment token is revocable by the consumer, payment provider, or both.

162. The method of claim 156, wherein the cost is over a predetermined amount allowed by the payment provider, and wherein additional user interaction is needed for authorization of the payment token.

163. The method of claim 156, wherein the payment token is signed, encrypted, or both, by the payment provider, and wherein the validation of the payment token to the payment provider includes validating the signature, the encryption, or both.

164. The method of claim 156, wherein the one or more services, goods, or both, require subscription or multiple payments, and wherein the payment token can be used multiple times for such payment.

165. The method of claim 156, wherein the one or more services, goods, or both, require subscription or multiple payments, and wherein the payment token is valid for only a single payment of the subscription or multiple payments, and wherein additional tokens are needed for subsequent payments.

166. In a distributed computing system for executing an online commercial transaction, a method of making payment authorization based on an electronic bill presentation for maintaining a record of the online transaction for auditing, fraud protection, and other purposes, the method comprising:

receiving at a consumer computing device an electronic bill that includes a description and cost for purchasing of one or more services, goods, or both, from a merchant during an online commercial transaction thereof; and

sending a copy of the electronic bill to a payment provider for authorizing payment of the one or more services, goods, or both.

167. The method of claim 166, wherein one or more portions of the electronic bill are encrypted by the merchant in order to make the one or more portions opaque to the consumer, payment provider, or both.

168. The method of claim 167, wherein the one or more portions of the electronic bill that are encrypted are used for automatic payment federation to one or more business associates of the merchant.

169. The method of claim 166, further comprising:

storing a copy of the electronic bill on the consumer computing device;

receiving a payment request from the payment provider for charges corresponding to payment to the merchant, wherein the payment request includes a copy of the electronic bill from the merchant; and

comparing the stored copy of the electronic bill with the copy received from the payment provider for auditing the appropriate payment made to the merchant.

170. The method of claim 166, wherein a copy of the electronic bill is signed by the merchant, the method further comprising:

receiving from the payment provider a payment token for authorizing the payment of the one or more services, goods, or both, wherein the token includes the signed copy of the electronic bill; and

sending the payment token to the merchant for authorization of payment, wherein the merchant can validate the payment token as coming from the consumer based on the signed copy of the electronic bill.

171. In a distributed computing system for executing an online commercial transaction, a method of authorizing payment for services, goods, or both, from a merchant based on an electronic bill presentation for maintaining a record of the online transaction for auditing, fraud protection, and other purposes, the method comprising:

receiving at a payment provider an electronic bill that includes a description and cost for purchasing of one or more services, goods, or both, by a consumer computing device during an online commercial transaction; and

sending a payment token to the consumer that includes a copy of at least a portion of the electronic bill for authorizing payment of the one or more services, goods, or both, from a merchant.

172. The method of claim 171, wherein one or more portions of the electronic bill are encrypted by the merchant in order to make the one or more portions opaque to the consumer, payment provider, or both.

173. The method of claim 172, wherein the one or more portions of the electronic bill that are encrypted are used for automatic payment federation to one or more business associates of the merchant.

174. The method of claim 171, further comprising:

storing a copy of the electronic bill on the payment provider computing device;

receiving a payment request from the merchant for payment of charges corresponding to the one or more services, goods, or both, wherein the payment request includes a copy of at least a portion of the electronic bill from the merchant; and

comparing the stored copy of the electronic bill with the copy of at least a portion of the received electronic bill from the merchant for authorizing appropriate payment thereto.

175. The method of claim 171, wherein a copy of the electronic bill is signed by the merchant, the method further comprising:

sending a payment token to the consumer that includes the signed copy of the electronic bill, which the merchant can used to validate that the payment token is part of a commercial transaction originating between the merchant and consumer;

receiving from the merchant a request to authorize the payment token for the one or more services, goods, or both; and

sending the an acknowledgment of the validity of the payment token to the merchant for allowing the merchant to transfer the one or more services, goods, or both to the consumer.

176. In a distributed computing system for executing an online commercial transaction, a method of validating payment authorization based on an electronic bill presentation for maintaining a record of the online transaction for auditing, fraud protection, and other purposes, the method comprising:

sending to a consumer computing device an electronic bill that includes a description and cost for purchasing of one or more services, goods, or both, from a merchant during an online commercial transaction thereof; and

receiving a payment token that includes at least a portion of the electronic bill for validating that the payment token is part of a commercial transaction originating between the merchant and the consumer.

177. The method of claim 176, wherein one or more portions of the electronic bill are encrypted by the merchant in order to make the one or more portions opaque to the consumer, the payment provider, or both.

178. The method of claim 177, wherein the one or more portions of the electronic bill that are encrypted are used for automatic payment federation to one or more business associates of the merchant.

179. The method of claim 176 further comprising:

sending the payment token to a payment provider for authorizing the payment of the one or more services, goods, or both, wherein the token includes the signed copy of the electronic bill;

receiving validation of the payment token from the service provider indicating the consumer's ability to pay for the one or more services, goods, or both; and

based on the authorization, sending the one or more services, goods, or both, to the consumer for completing the commercial transaction.

180. In a distributed system, a method of automatic payment distribution to a series of business associates with a predefined business relationship based on a single payment from a consumer for an online commercial transaction, the method comprising:

receiving a single online payment for services, goods, or both, offered by a merchant that has a contractual business relationship with at least one other business associate that assists in providing at least a portion of the services, goods, or both;

based on the contractual relationship defined, identifying a portion of the single online payment as belonging to the at least one business associate; and

automatically transferring the portion of the payment to an account for the at least one business associate in order to federate payment to the merchant and at least one business associate based on a trusted relationship and policy associated therewith.

181. The method of claim 180, wherein the portion is further identified based on a portions designated within bill information generated by the merchant that is presented to a consumer that authorized the single payment.

182. The method of claim 181, wherein the portion is signed by the merchant in order to make the payment federation transparent to the consumer.

183. In a distributed online system for performing a commercial transaction, a method of presenting a consumer with payment options based on analysis of a electronic bill and policies or rules defined by a merchant, consumer, or both, the method comprising:

receiving at a consumer device an electronic bill that includes information about a purchase request for goods, services, or both, from a merchant;

comparing information from within the electronic bill with one or more predefined rules from the consumer, merchant, or both; and

based on the comparison, determining an appropriate action that meets the requirements of the one or more predefined rules.

184. The method of claim 183, wherein the one or more predefined rules are a list of available type of payment options for the merchant, consumer, or both, and wherein the action chooses from the list one or more payments options for presentation to a user.

185. The method of claim 184, wherein the one or more predefined rules limit the type of payment based on a trust relationship with the merchant and the information within the electronic bill identifies the trust relationship based on a signature, encryption, or both from the merchant.

186. The method of claim 184, wherein the one or more predefined rules limit the type of payment based on the available payment types for the consumer compared with the type of payments accepted by the merchant.

187. The method of claim 184, wherein the one or more predefined rules limit the type of payment based on the total cost of the one or more services, goods, or both.

188. The method of claim 184, wherein the information within the electronic bill further includes rules for the merchant such that the rules for the merchant are compared with the rules for the consumer.

189. The method of claim 188, and wherein any conflicts between the rules for the merchant and the rules for the consumer are resolved in favor of the merchant, or the commercial transaction is cancelled.

190. The method of claim 184, wherein the commercial transaction is a pay as you go subscription, and wherein the one or more rules limit the duration of the subscription based on a payment amount, period of time, or both.

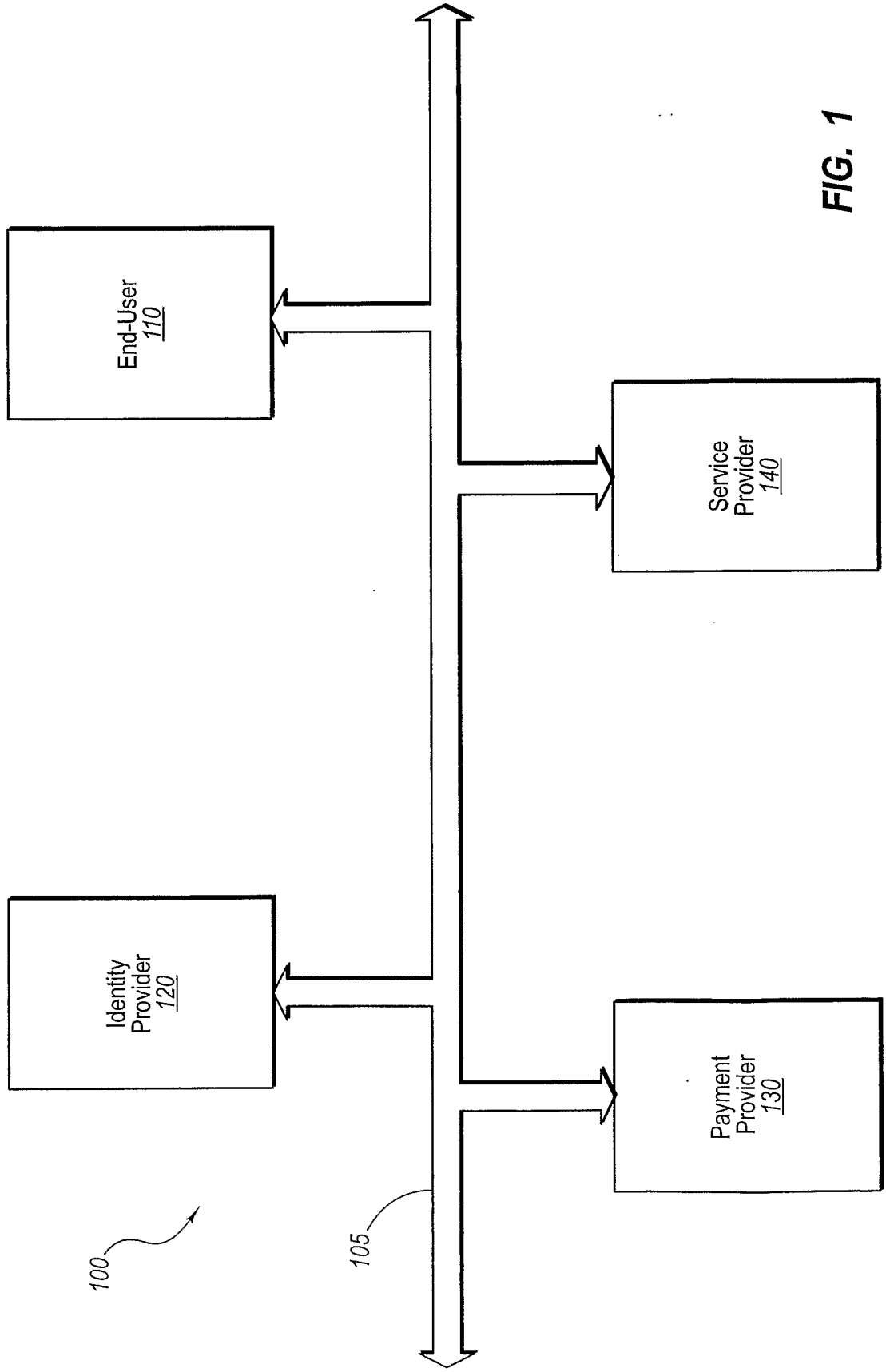

End-User
110
Service
Provider
140
Identity
Provider
120
Payment
Provider
130
100
105

FIG. 1

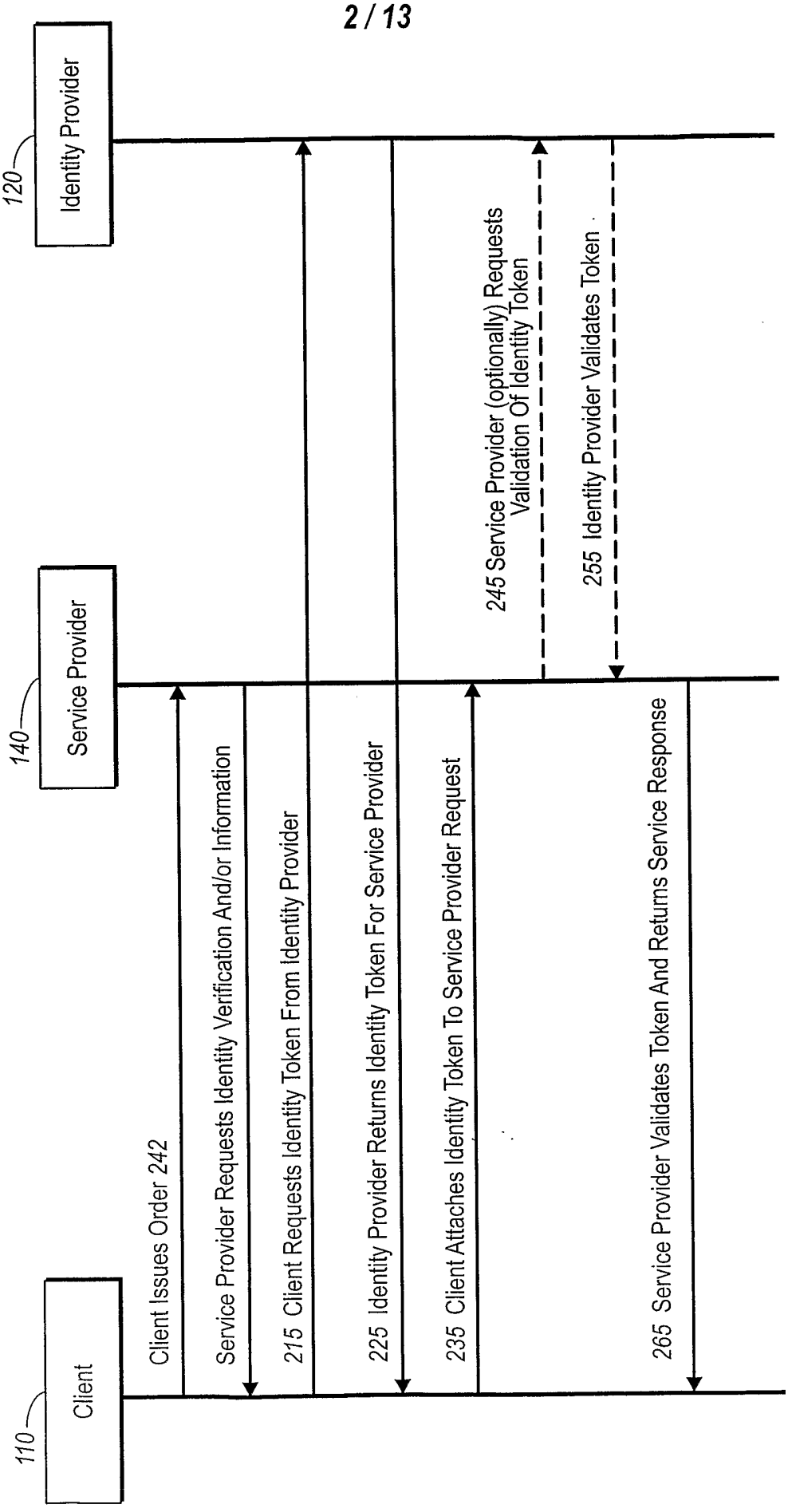

Client
110
Service Provider
140
Identity Provider
120
Client Issues Order 242
Service Provider Requests Identity Verification And/or Information
215 Client Requests Identity Token From Identity Provider
225 Identity Provider Returns Identity Token For Service Provider
235 Client Attaches Identity Token To Service Provider Request
245 Service Provider (optionally) Requests Validation Of Identity Token
255 Identity Provider Validates Token
265 Service Provider Validates Token And Returns Service Response

FIG. 2

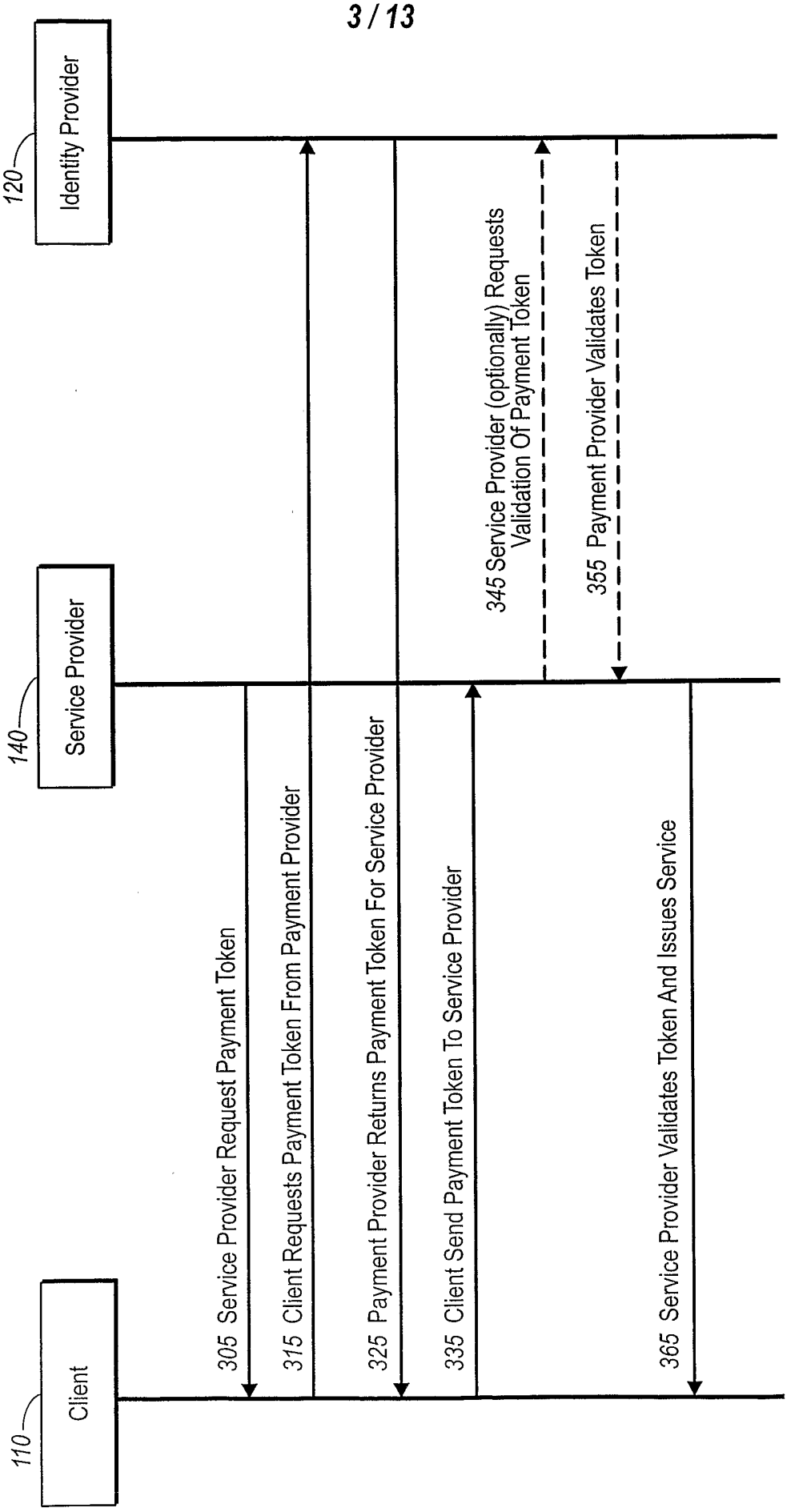

Identity Provider
120
Service Provider
140
Client
110
305 Service Provider Request Payment Token
315 Client Requests Payment Token From Payment Provider
325 Payment Provider Returns Payment Token For Service Provider
335 Client Send Payment Token To Service Provider
345 Service Provider (optionally) Requests Validation Of Payment Token
355 Payment Provider Validates Token
365 Service Provider Validates Token And Issues Service

FIG. 3

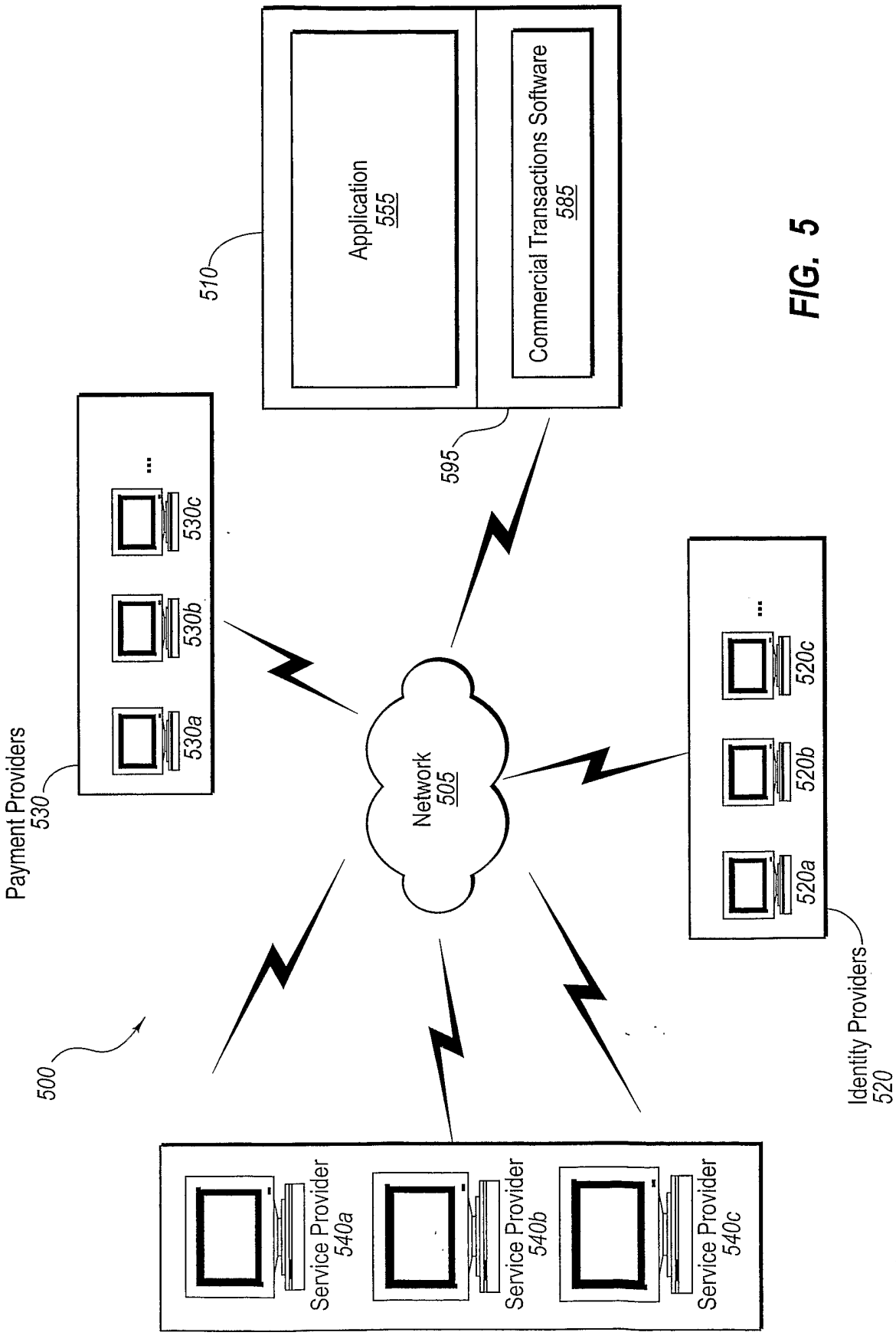

510
Application
555
Commercial Transactions Software
585
595
Payment Providers
530
530a
530b
530c
Network
505
Identity Providers
520
520a
520b
520c
500
Service Provider
540a
Service Provider
540b
Service Provider
540c

FIG. 5

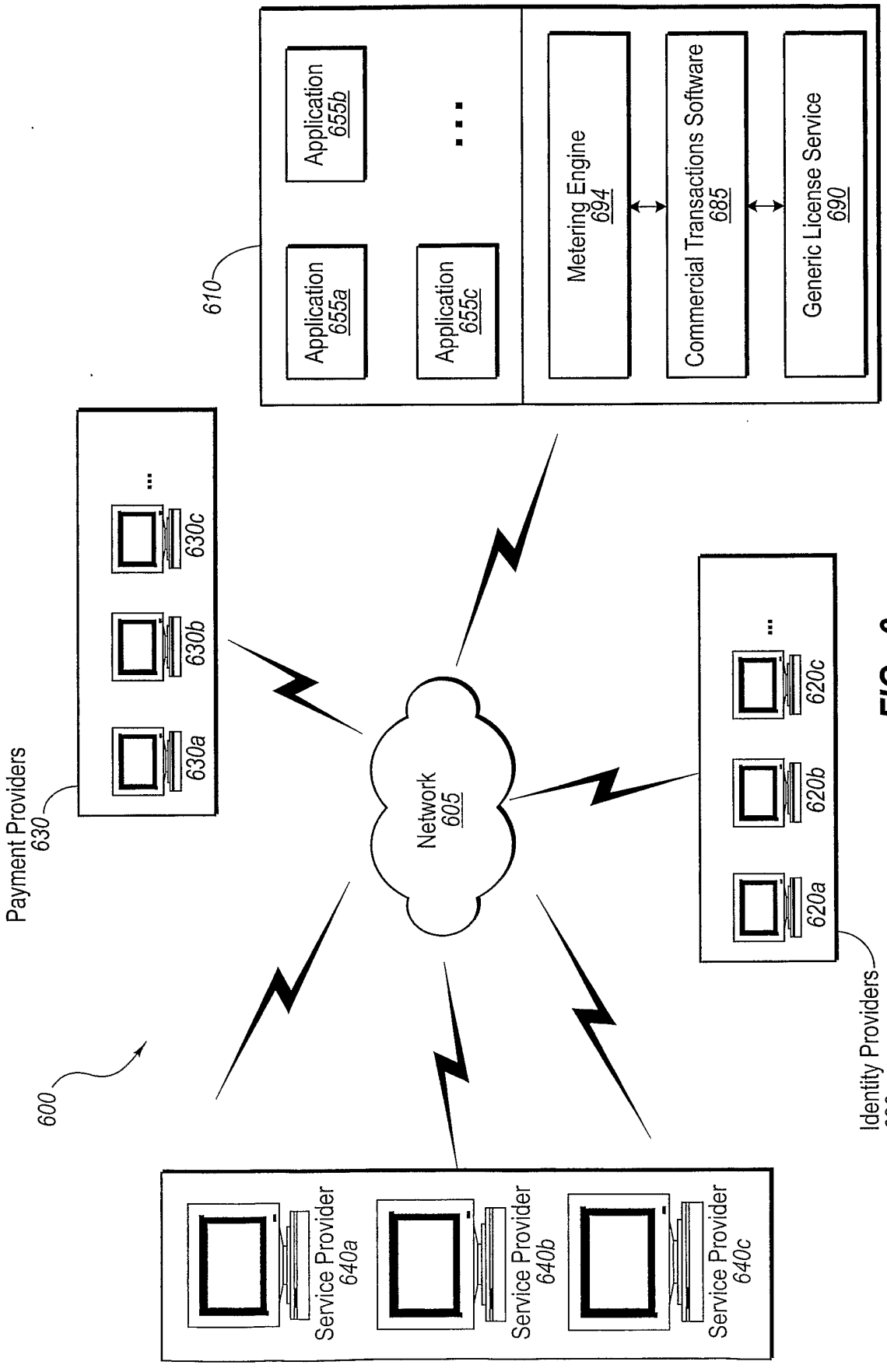

600
610
Application 655a
Application 655b
Application 655c
Metering Engine 694
Commercial Transactions Software 685
Generic License Service 690
Payment Providers 630
630a
630b
630c
Network 605
Identity Providers 620
620a
620b
620c
Service Provider 640a
Service Provider 640b
Service Provider 640c

FIG. 6

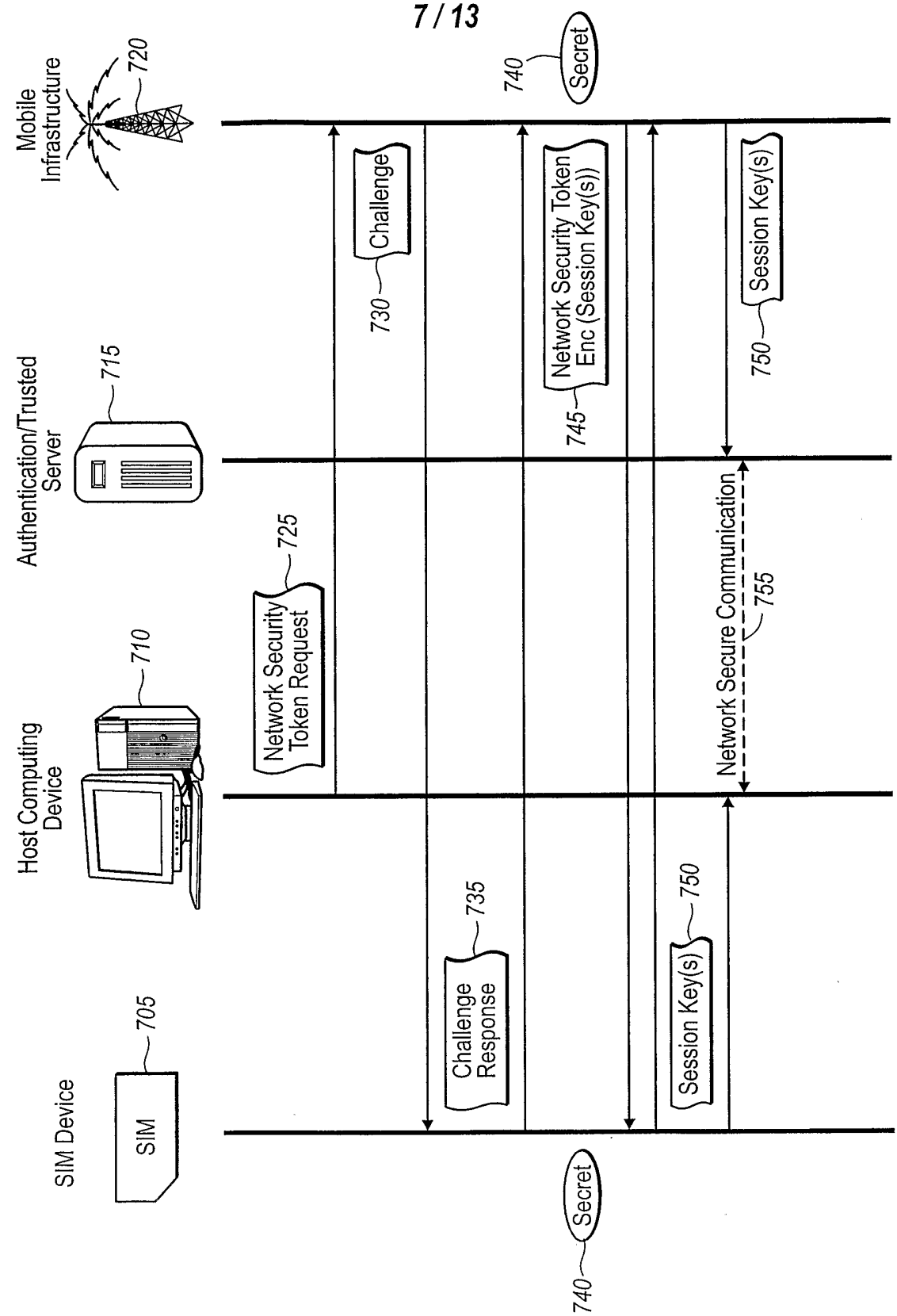

Independent Network 700
SIM Device
SIM
705
Host Computing Device
710
Authentication/Trusted Server
715
Mobile Infrastructure
720
Network Security Token Request
725
Challenge
730
Challenge Response
735
Secret
740
Network Security Token Enc (Session Key(s))
745
Session Key(s)
750
Network Secure Communication
755

FIG. 7A

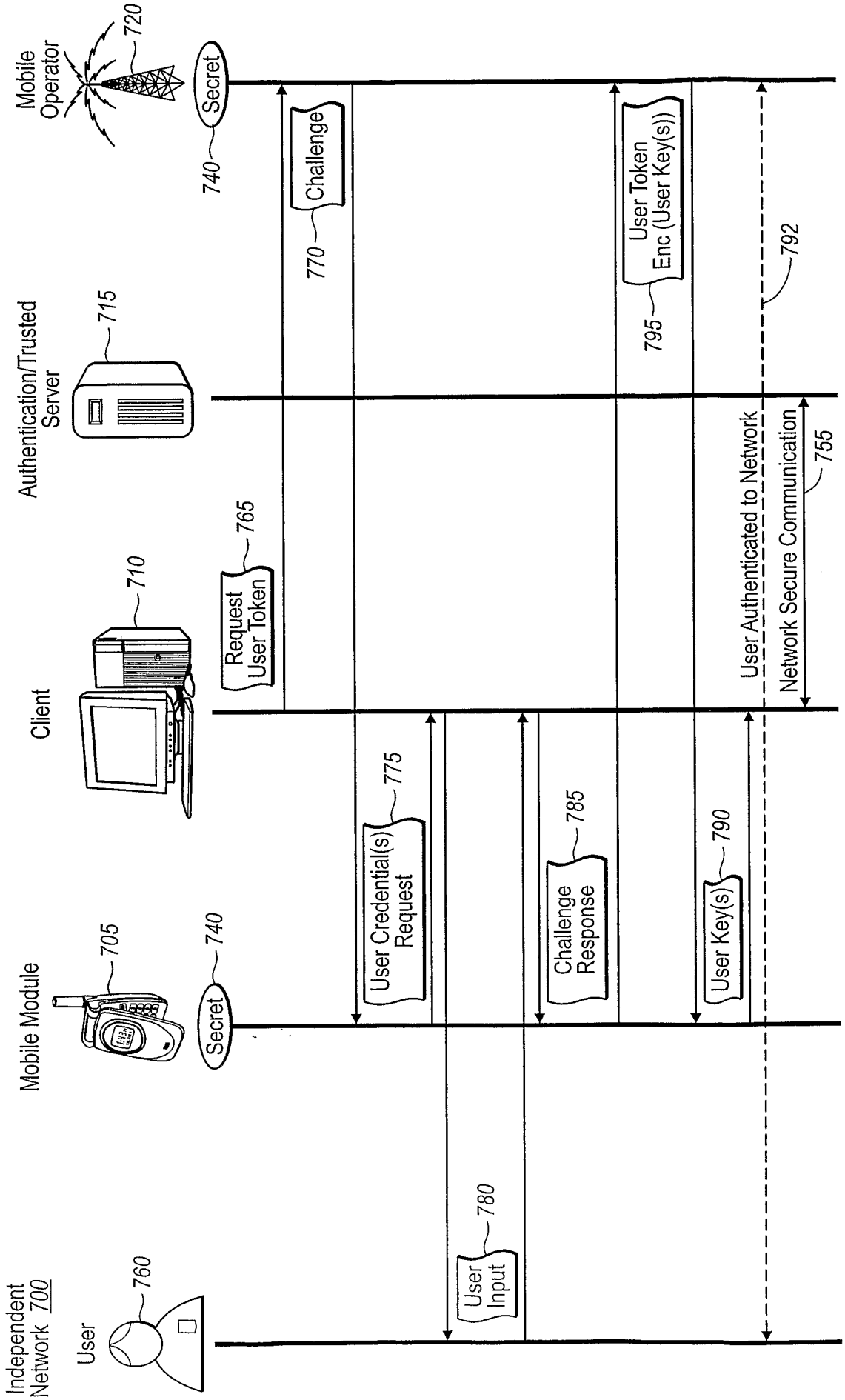

Independent Network 700
User
760
Mobile Module
705
Client
710
Authentication/Trusted Server
715
Mobile Operator
720
Secret
740
Secret
740
Request User Token
765
Challenge
770
User Credential(s) Request
775
User Input
780
Challenge Response
785
User Key(s)
790
User Token Enc (User Key(s))
795
792
User Authenticated to Network
Network Secure Communication
755

FIG. 7B

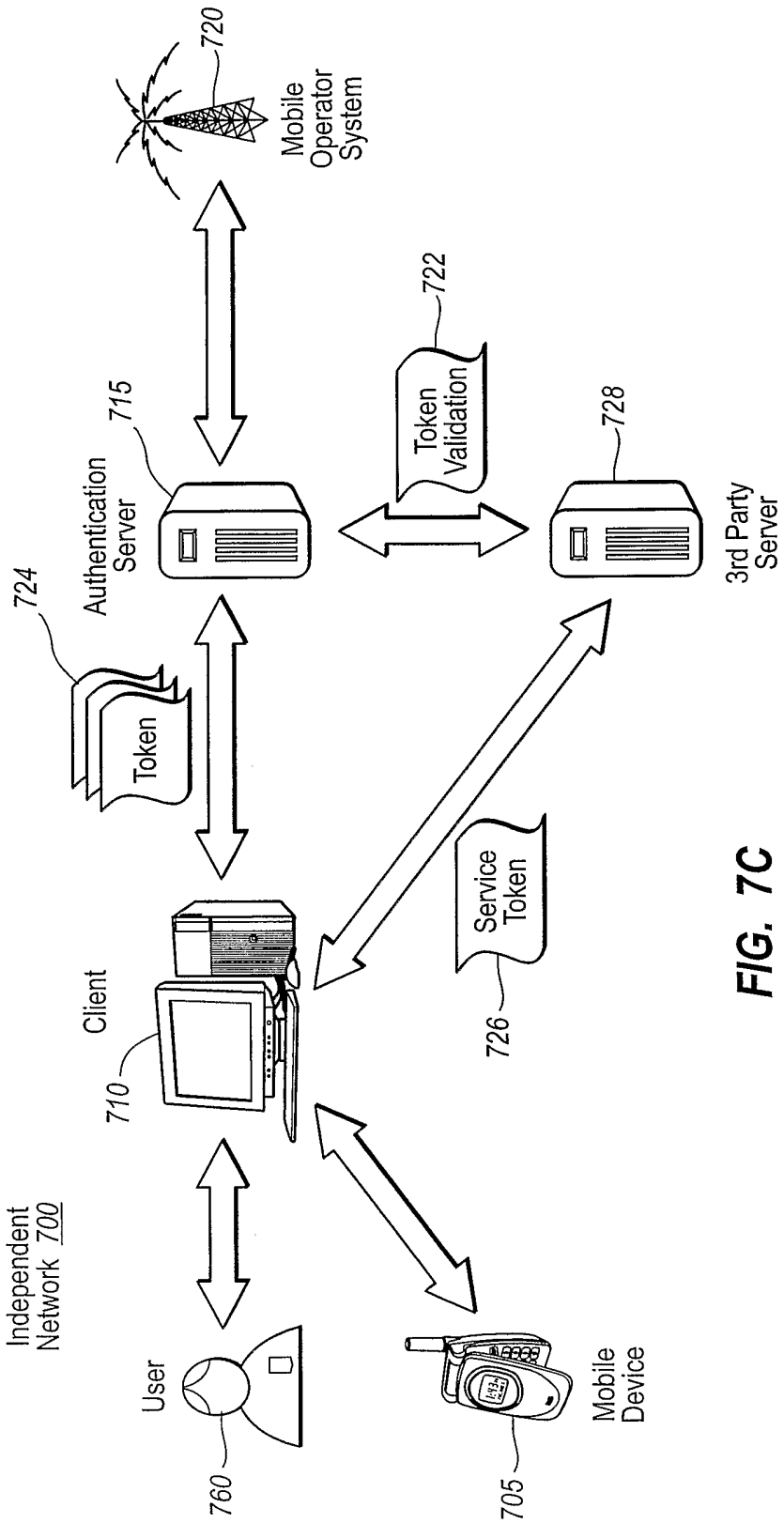

720
Mobile Operator System
722
Token Validation
715
Authentication Server
728
3rd Party Server
724
Token
Service Token
726
Client
710
Independent Network 700
User
760
Mobile Device
705

FIG. 7C

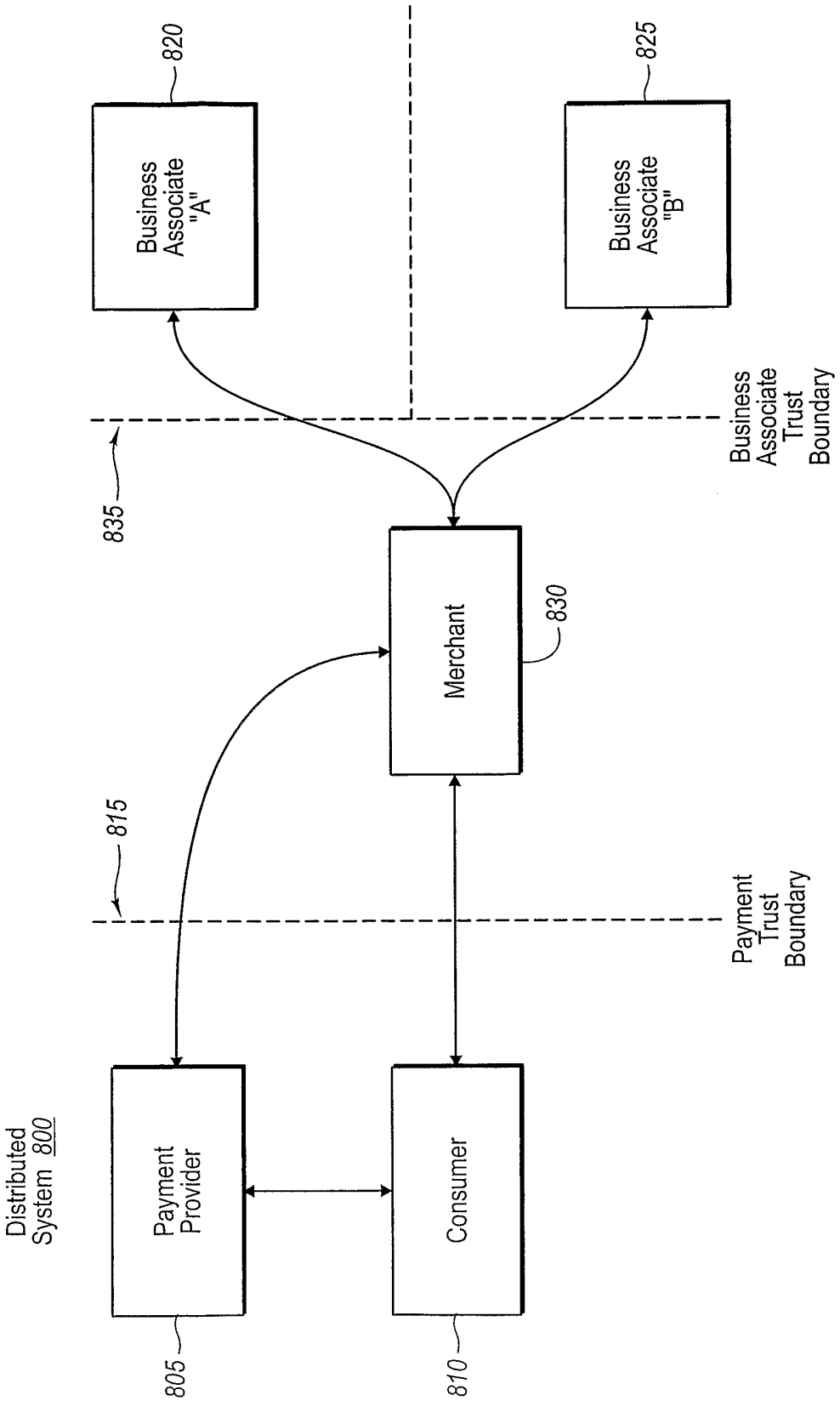

Distributed System 800
Payment Provider
805
Consumer
810
Payment Trust Boundary
815
Merchant
830
Business Associate Trust Boundary
835
Business Associate "A"
820
Business Associate "B"
825

FIG. 8

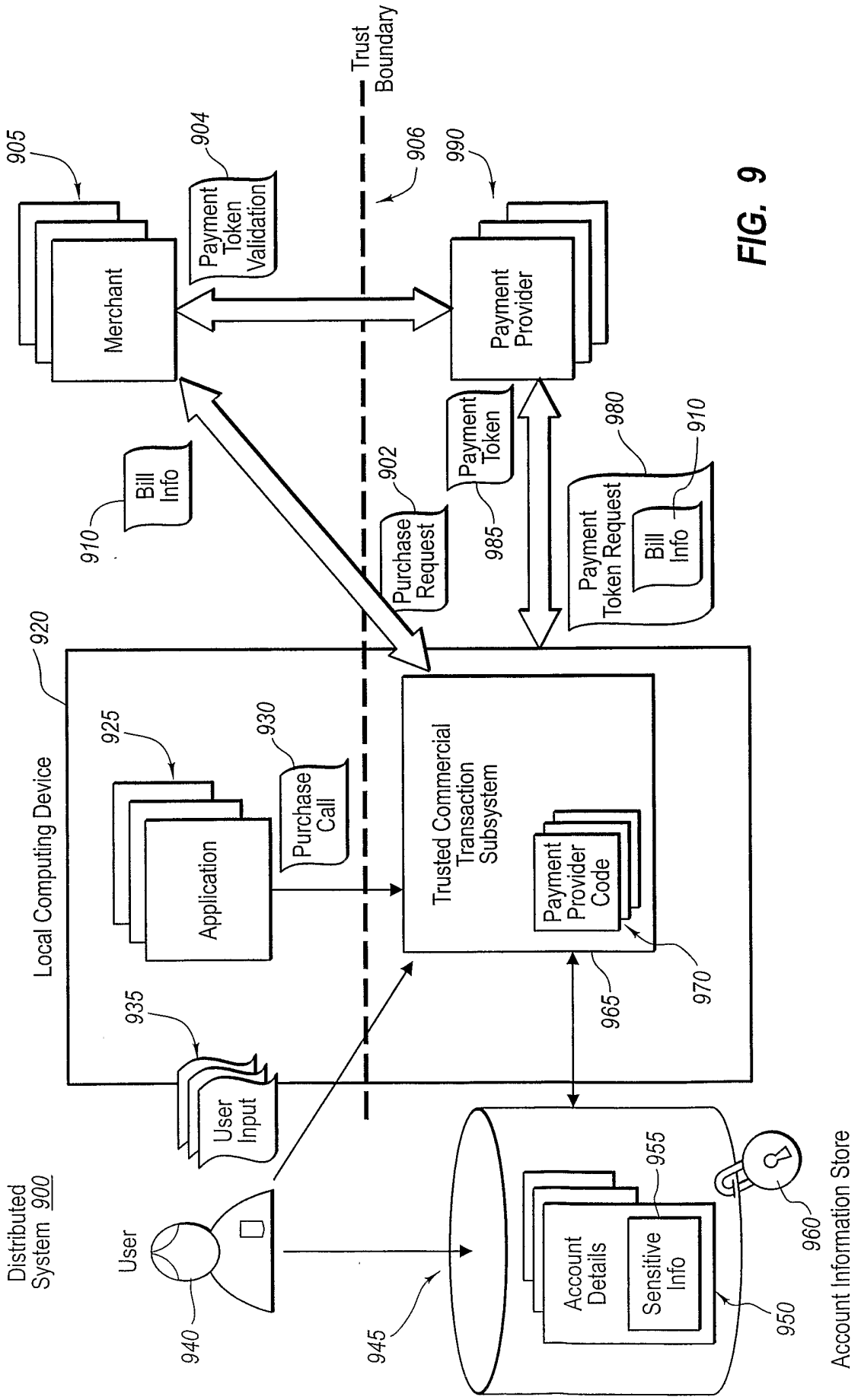

Distributed System 900
Trust Boundary
905
Merchant
904
Payment Token Validation
906
990
Payment Provider
910
Bill Info
902
Purchase Request
985
Payment Token
980
Payment Token Request
910
Bill Info
920
Local Computing Device
925
Application
930
Purchase Call
Trusted Commercial Transaction Subsystem
Payment Provider Code
970
965
935
User Input
User
940
945
955
Account Details
Sensitive Info
950
960
Account Information Store

FIG. 9

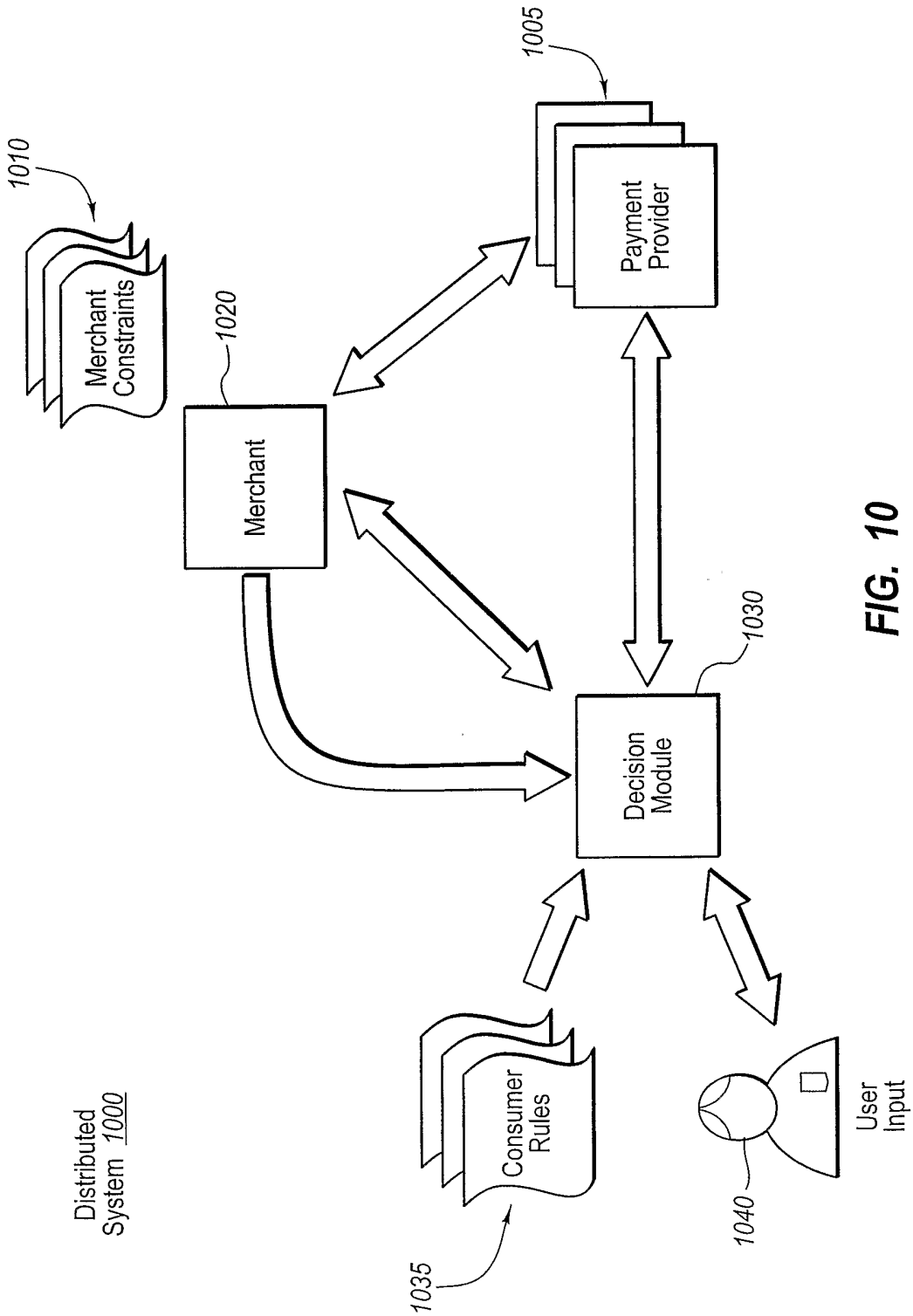

Distributed System 1000
1010
Merchant Constraints
1020
Merchant
1005
Payment Provider
1030
Decision Module
1035
Consumer Rules
1040
User Input

FIG. 10

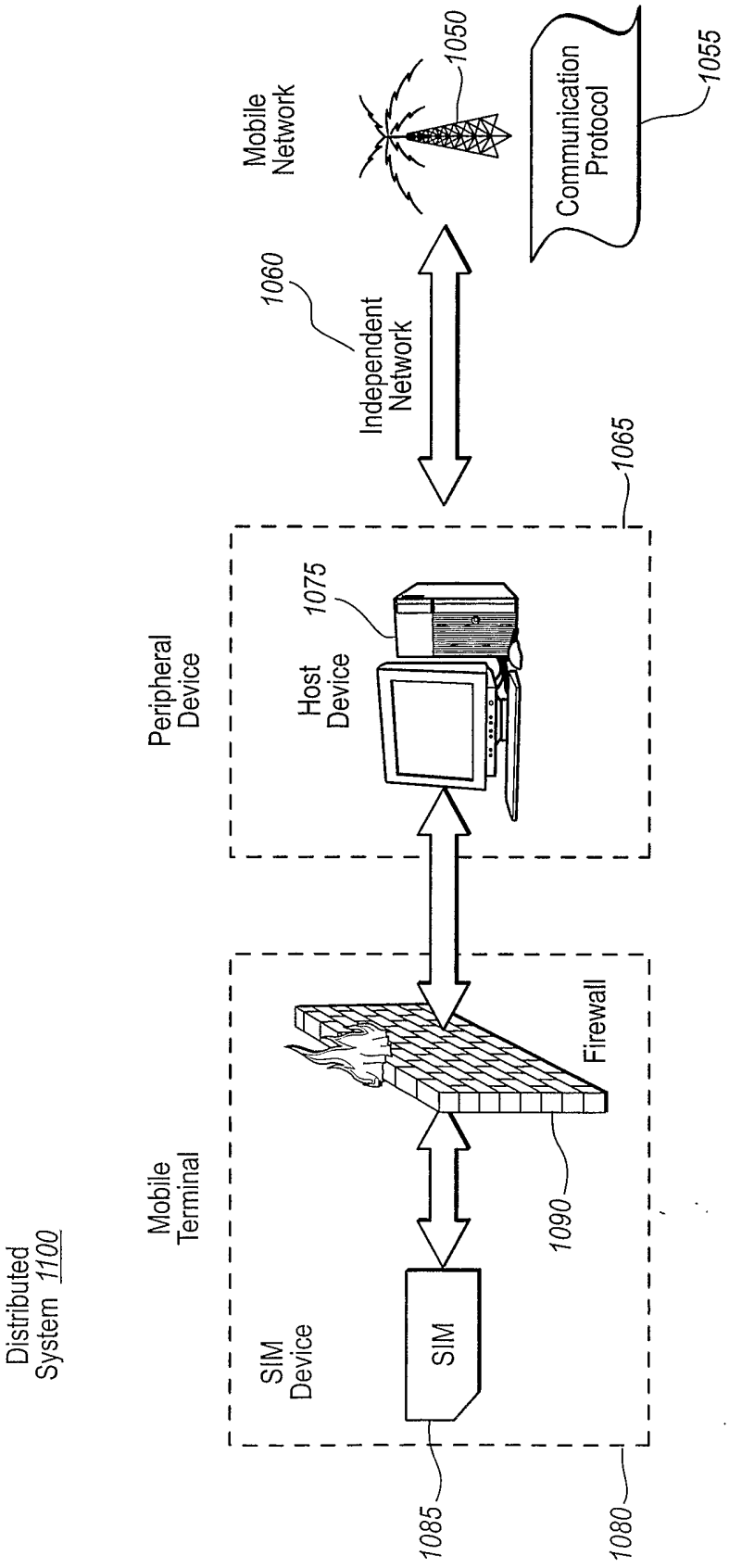

Distributed System 1100
Mobile Terminal
SIM Device
SIM
1085
1080
1090
Firewall
Peripheral Device
Host Device
1075
1065
Independent Network
1060
Mobile Network
1050
Communication Protocol
1055

FIG. 11