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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 November 2004 (18.11.2004)

PCT

(10) International Publication Number
WO 2004/100497 A1

(51) International Patent Classification[7]: H04L 29/06, 29/08

(21) International Application Number: PCT/US2004/011476

(22) International Filing Date: 14 April 2004 (14.04.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/414,174 15 April 2003 (15.04.2003) US

(71) Applicant *(for all designated States except US)*: **AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY, INC.** [US/US]; American Express Tower, World Financial Center, New York, NY 10285-4900 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KEENAN, Sean, M.** [US/US]; 10852 N 120th Place, Scottsdale, AZ 85259 (US). **TURKO, Bill** [US/US]; 17005 N 45th Avenue, Glendale, AZ 85308 (US). **MORGAN, Bob** [CA/US]; 7235 W. La Senda Drive, Glendale, AZ 85310 (US).

(74) Agent: **HERNANDEZ, Gilberto**; McDermott, Will & Emery, 227 West Monroe Street, Chicago, IL 60606 (US).

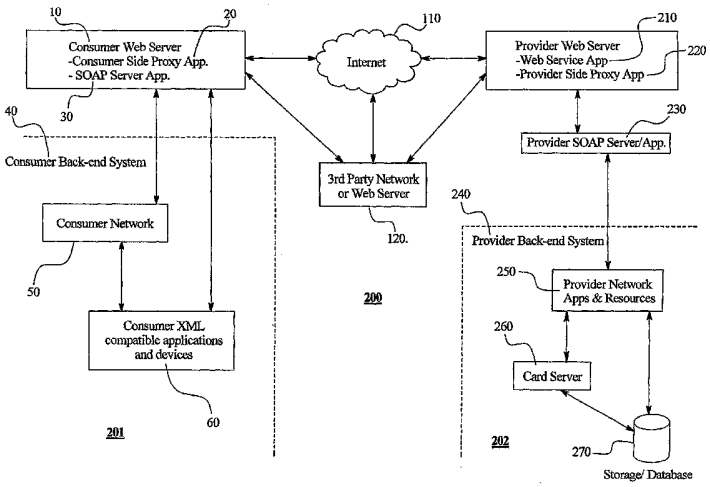
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, 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, 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, IT, LU, 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:**
— *with international search report*

*[Continued on next page]*

(54) **Title:** A TRANSACTION CARD INFORMATION ACCESS WEB SERVICE




(57) **Abstract:** There is provided a platform neutral method and system for retrieving card information in an extensible markup language (XML) format over the internet via a web service comprising the steps of formulating a simple access object protocol (SOAP) request for the selected information at a consumer application, transmitting the SOAP request to the web service over the internet, receiving the SOAP requests at a provider web service, routing the information request for card information to a provider back-end network, processing the information request and retrieving the selected card information and forwarding to the web service application, formatting the retrieved selected card information in an XML format and formulating a SOAP reply, transmitting the SOAP reply to the consumer over the internet, receiving the SOAP reply at a consumer web server application, reading the XML formatted stored value card information, and routing the XML formatted information to a consumer back-end application or end-point access devices.

WO 2004/100497 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

*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.*

# A TRANSACTION CARD INFORMATION ACCESS WEB SERVICE

## FIELD OF THE INVENTION

[ 0001] The present invention generally relates to computerized information systems and information retrieval from a provider computer system. More particularly, the present invention relates to a system and method for requesting and delivering selected stored value card information in an extensible markup language (XML) format via the internet using a web service that uses simple object access protocol (SOAP) as the communications protocol between the web service provider and consumer.

## BACKGROUND OF THE INVENTION

[ 0002] Authorized consumers, merchants or customers often want to check or verify information relating to transaction cards, such as stored value or gift cards. Such information may include the remaining balance on the stored value card or recent transactions carried out using the card. Existing methods of retrieving such information typically require consumers or merchants to authenticate their authorized status and identification at an information providing system or network. In existing methods, authentication for a merchant, consumer or user is generally carried out via Single Sign On (SSO) through a web channel which requires that the merchant access a designated web site, and, once there, to manually key in or enter appropriate information and data so that desired or selected card information can be correctly requested and retrieved.

[ 0003] Also, merchants or consumers are typically required to complete an authentication procedure multiple times on their own computerized network and on the information provider's computerized network. Typically, a merchant initially authenticates identifications (ID) and passwords for authorized users to use the

merchant network. This can be cumbersome and time consuming for merchants that have many users authorized to request transaction card information. When a merchant or consumer, via an employee or user, accesses a provider website or computing environment, the merchant must also authenticate at the information provider's computing environment or network as noted above. This process can be unduly repetitive and time consuming if a merchant has a large number of users that may require access to the card information since existing information retrieval methods require that all users authenticate at the information provider's network each time transaction card information is requested.

[ 0004] Additionally, existing card information retrieval methods require dedicated communication lines for a continuous connection between the information provider network and the merchant network such that information can be requested and delivered in a reliable and secure manner. The need for dedicated communication lines can result in an information retrieval method and system that is expensive.

[ 0005] Further, many existing information retrieval systems require that both the information providing system and the receiving merchant or consumer system have or operate on the same operating system or platform so that communications and the exchange of information between the systems can be conveniently carried out. This aspect can be a drawback if the operating systems or platforms of the information provider and merchant systems are not the same. In such a case, communication and information retrieval may not be possible or may be very limited due to the differences in system platforms. One solution to this drawback requires one party to procure a computing system having a compatible operating system, platform or interface to the other party's system so that the parties can communicate and exchange information in a reliable and consistent manner. This approach can lead

to increased costs for the party procuring the additional computing system and results in one party having two incompatible computing systems.

[ 0006] Moreover, existing information retrieval methods and systems often use communication protocols and data formats that are compatible with the operating system or platform of the information providing system. As a result, the card information received from the information provider typically comes in a format that is compatible with only a limited number of applications and devices on the merchant's network. This is a drawback since the merchant may want to ability to manipulate the received information in a variety of both current and future applications and devices on his system.

[ 0007] There is thus a need for a method and system for accessing or requesting transaction card information in a platform-neutral way from an information provider system and delivering the information to a merchant or consumer system. There is also a need for a method and system for requesting and receiving transaction card information without having to repeatedly authenticate at the information provider's system each time card information is requested. There is also a need for a method and system for requesting and receiving transaction card information and delivering the transaction card information in a standardized format to enable a merchant to receive, process, store, display and manipulate the received transaction card information in a variety of merchant applications and/or to integrate the received information into a variety of existing or new merchant end-point access devices or applications.

## SUMMARY OF THE INVENTION

[ 0008] The present invention provides a method for retrieving selected stored value card information in a standard format over a public interconnected network via a

provider web service comprising the steps of formulating a simple access object protocol (SOAP) request in a consumer network operating on a first platform, transmitting the SOAP request to the provider web service over the public interconnected network, receiving the SOAP request at a provider web service running a web server application, reading the SOAP request to determine the card information being requested, generating and routing an internal information request for the requested card information to a provider back-end network operating on a second platform, processing the information request and retrieving the selected card information from a storage location and forwarding the retrieved information to the web service application, formatting the retrieved card information in an XML format and formulating a SOAP reply, transmitting the SOAP reply from the web service application to the consumer web server application over the public interconnected network, receiving the SOAP reply at the consumer web server application, reading the SOAP reply to parse out the XML formatted selected card information, and routing the XML formatted selected card information to one or more consumer back-end applications or end-point access devices on the consumer network.

[ 0009] The method for retrieving selected stored value card information in a standard format over a public interconnected network via a provider web service can further comprise the steps of encrypting the SOAP request and providing the SOAP request with a consumer digital signature, verifying that the consumer digital signature on the received encrypted SOAP request corresponds to an authorized consumer and then decrypting the SOAP request, encrypting the SOAP reply and providing the SOAP reply with a provider digital signature, and verifying that the provider digital signature on the received encrypted SOAP reply corresponds to the provider and then decrypting the SOAP reply.

[ 0010] It is an object of the present invention to provide a method and system for requesting and receiving selected XML formatted stored value information via the internet using a web service in a way that allows minimal integration of provider and merchant computer systems and provides a standard interface between both systems.

[ 0011] It is an object of the present invention to provide a method and system for requesting and receiving selected XML formatted stored value card information via a web service directly to a merchant's applications and end point access devices without requiring the merchant to authenticate each time information is requested.

[ 0012] It is an object of the present invention to provide a method and system for a web service that provides the capability for merchants to retrieve and display stored value card transactions processed and stored by a card provider system via the internet at a merchant chosen location such as one or more merchant retail locations.

[ 0013] It is an object of the present invention to provide a method and system for a web service that can provide selected transaction card information to a requesting merchant or consumer, including stored value card transaction history and balance for a specific stored value card or gift card.

[ 0014] It is an object of the present invention to provide stored value card information access to merchants and consumers that use the Internet as the means for transmission of business or other designated information without requiring dedicated communications lines between the provider and merchant or consumer.

[ 0015] It is an object of the present invention to provide a method and system for merchants and consumers to retrieve card information via a standard web service such that independent of the operating system or platform used by the merchant or consumer.

[ 0016] It is an object of the present invention to provide a method and system for a web service that can provide selected information, such as stored value card information, without requiring a merchant or user to authenticate at a provider's system, network or web applications.

[ 0017] It is an object of the present invention to provide a method and system for an information access web service that can provide requested information or data in a standardized XML format to enable and allow convenient integration into a plurality of end point access applications and devices, including, among others, static or dynamic world wide web pages, including among other applications web browsers, intranet, internet, and extranets, Point of Sale (POS) devices, cash registers, personal display assistants (PDAs), smart cards, transaction cards having smart chips or integrated circuit chips, kiosk applications, and back office applications such as Microsoft Office, PowerPoint, Database applications and E-mail applications and other electronic access systems.

[ 0018] It is an object of the present invention to provide a method and system for an information access web service that can use third party proxy applications to initiate connections and provide secure communication and transactions between a provider and merchant or consumer to request and receive selected card information.

[ 0019] It is an object of the present invention to provide a method and system for an information access web service that can use third party proxy applications to generate, track, encrypt, and decrypt simple object access protocol (SOAP) requests and replies for selected information and to transmit SOAP requests and replies over the internet between the web service and the merchant or consumer.

[ 0020] It is an object of the present invention to provide a method and system for information access that can use third party proxy applications to track and store

transmitted and received SOAP requests and replies and to generate reports on web service activity.

[ 0021] It is an object of the present invention to provide a method and system for an information access web service that can provide selected transaction card information to a user, consumer or card member without requiring phone calls to or interaction with an integrated voice response (IVR) system or customer service representatives.

[ 0022] It is an object of the present invention to provide a method and system for an automated web service for retrieval of selected transaction card information without requiring interaction with or intervention by a provider customer service representative thereby reducing the time to request and receive the desired card information.

[ 0023] The following drawings and description set forth additional advantages and benefits of the invention. More advantages and benefits will be obvious from the description and may be learned by practice of the invention.

## BRIEF DESCRIPTION OF THE DRAWINGS

[ 0024] The present invention may be better understood when read in connection with the accompanying drawings, of which:

[ 0025] Figures 1A and 1B illustrate a flow chart of the steps of one preferred method for requesting and retrieving selected information over the internet via a web service according to the present invention;

[ 0026] Figure 2 illustrates a block diagram representation of a system where the method of Figure 1 can be implemented;

[ 0027] Figure 3 illustrates a block diagram representation of a second system where the method of Figure 1 can be implemented; and

[ 0028] Figure 4 illustrates a block diagram representation of a third system where the method of Figure 1 can be implemented.

## DETAILED DESCRIPTION

[ 0029] One embodiment of the present invention provides a web service that enables authorized merchants or customers to request and receive selected transaction card information over the internet from an information provider system or network in a standard format. The standard format will enable convenient integration of the transaction card information into existing and future consumer applications and end-point access devices or machines.

[ 0030] Using the method and system described herein, a consumer or merchant can request and receive selected transaction card information in an extensible markup language (XML) format via the internet using a web service preferably described in the web services description language (WSDL) that uses simple object access protocol (SOAP) as the communications protocol between the web service provider and merchant or consumer. The system and method of the present invention is platform neutral such that the requesting merchant or consumer systems may function in one platform or operating system and the provider system can operate in a different platform.

[ 0031] Those of skill in the art will readily recognize that the retrieved information can be any information related to transaction cards including card holder information, transaction card history, stored value card balance, card credit limit information or any other transaction card available from the information provider system or network. Additionally, those of skill in the art will readily recognize that the system and method of the present invention can be use to request and retrieve information for any number of well known types of transaction cards including a stored value card, a gift card, a credit card, a smart card, a bank card, a charge card or a financial card.

[ 0032] Referring to Figures 1A and 1B, there is shown a flow chart with steps for a preferred method 100 for requesting and retrieving stored value information over the internet 110 via a web service 210 according to the present invention. A block diagram of a system 200 where the method 100 of Figures 1A and 1B can be implemented is shown in Figure 2.

[ 0033] In Step S10, a request for selected information is generated at a merchant or consumer back-end system 40 of a merchant or consumer system 201 or first operating system. The information or data request can be generated by a consumer, such as a merchant, at a consumer stored value application 60. The consumer stored value application 60 can be running on any one of a machine, computer or device at a consumer location, such as a merchant retail location. The machine, computer or device can be a card reader, a computer terminal, a Point of Sale (POS) terminal, a cashier terminal, a back-office terminal or any other machine that can generate an information request for transaction card information.

[ 0034] An information request can be initiated or generated at a consumer application or device 60 by methods and means well known to those of skill in the art including swiping the magnetic stripe of a transaction card in a card reader device or by inputting transaction card account information at computer or machine for processing by the consumer application 60. The information request can also be initiated or generated at the consumer application or device 60 via a smart card and smart card reader device as is also well known to those of skill in the art. The smart card can be a transaction card having an embedded smart chip or integrated circuit chip with appropriate applications and data storage capability. The information request generated by the consumer application 60 will have a format corresponding to the operating system or platform of the consumer system 201.

[ 0035] In Step S20, the card information request is passed from the consumer back-end system 40 to a simple object access protocol (SOAP) application 30 running on a consumer web server 10. The card information request can be forwarded to the SOAP application 30 directly from the consumer application 60 that generates the information request or through intermediary resources 50 in the consumer back-end system 40. The SOAP application preferably runs on the consumer web server 10 and comprises computer instructions and/or software that convert the information requests into an extensible markup language (XML) formatted SOAP request. Additionally, if the information request was generated by a smart card or transaction card with a smart chip, those of skill in the art will recognize that the information request may have been generated as an XML formatted SOAP request and thus no conversion may be necessary. The XML formatted SOAP request is now forwarded to a consumer side proxy application 20.

[ 0036] In an alternate embodiment without a SOAP application 30 on the consumer web server 10, the generated information request is forwarded to the consumer side proxy application 20. The information request is forwarded to the consumer side proxy application 20 directly from the consumer application 60 that generates the information request or through intermediary resources 50 in the consumer back-end network 40. Also, the consumer side proxy application 20 comprise computer instructions and/or software to convert the information request into an XML formatted SOAP request.

[ 0037] In Step S30, the XML formatted SOAP request is processed by the consumer side proxy application 20. The consumer side proxy application 20 will generate and assign a transaction number to the SOAP request for tracking and record keeping purposes. The consumer side proxy application 20 will execute an encryption

algorithm to encrypt the XML formatted SOAP request. Additionally, consumer side proxy application 20 will add the consumer's digital signature to the SOAP request. Additionally, the consumer side proxy application 20 preferably computes a consumer digital signature for SOAP request message intended for the information provider. The consumer digital signature is then added to the SOAP request payload along with the encrypted message. The consumer side proxy application 20 also possesses decryption capabilities to decrypt SOAP replies received from the provider web service 210.

[ 0038] In this embodiment, the consumer web server 10 has a separate consumer side proxy application 20 and a SOAP server application 30 performing particular functions. However, those of ordinary skill in the art will readily recognize that the functions and capabilities of the consumer side proxy application 20 and the SOAP server application 30 can also be accomplished by code or software for a consumer web server application and that each application can run on one or multiple computing machines.

[ 0039] In Step S40, the encrypted SOAP request is then transmitted to the information provider's web service 210 by the consumer web server application or consumer side proxy application 20. The encrypted SOAP request with the consumer's digital signature is preferably transmitted over a public interconnected network or internet to the provider's web service 210 at a designated uniform resource locator (URL) address. Simultaneously, a separate out-of-band transmission or message is transmitted to a designated third party computer system 120 for recording that a SOAP request for card information was sent from a consumer to the provider at the provider's web service. Those of skill in the art will readily recognize that the third party system 120 can include, among other components and devices, web servers, application servers and databases. Those of skill in the art will also recognize that the out-of-band

transmission or message sent to the third party 120 is optional and done as an enhancement aspect. Thus, step S40 can be carried out with or without the out-of-band transmission or message to the third party 120.

[ 0040] Transmission of the encrypted SOAP request for card information over the internet 110 permits the consumer to request desired information over a readily available communications medium without requiring dedicated communications lines between the consumer and the information provider. Additionally, encryption of the message guarantees confidentiality of the transmitted SOAP request message and digital signing of the message guarantees the integrity of the message. Moreover, the use of a standard XML formatted SOAP request, enable the consumer to communicate, request and receive selected card information in a standardized manner independent of the platforms being used by the internal systems of the consumer and the provider. The consumer is thus able to request and the provider is able to deliver transaction card information in cases where the merchant and provider have different or non-compatible operating systems or platforms. The platforms could be among other including Microsoft Windows 2000, Windows NT, Macintosh OS, IBM JAVA operating system, IBM S/390, UNIX, SOLARIS, LINUX and Novell NETWARE among other platforms well known to those of skill in the art.

[ 0041] In Step S50, the web service provider receives the merchant's encrypted XML formatted SOAP request at a provider side proxy application 220 loaded on a provider web server 210. The provider side proxy application 220 and the consumer side proxy application 20 preferably provide similar functions: transmission and receipt of SOAP messages, encryption and decryption of SOAP messages, and insertion and verification of consumer and provider signatures. The proxy applications 20 and 30 are preferably provided by a third party 120 having expertise in software application that

provide such transaction and security functions, features and capabilities. Such third parties 120 can include commercial providers that offer these software and software applications to the public, e.g., computer applications provided by a company such as Flamenco Networks located at 400 NorthWinds Center West, 11605 Haynes Bridge Road, Suite 600, Alpharetta, GA 30004. However, those of skill in the art will readily recognize that the these functions can be implemented by the consumer and provider through the use of commercially available software that can then be loaded onto the consumer's and provider's web servers. Moreover, those of skill in the art will readily recognize that the consumer and provider proxy applications 20 and 220 used in a preferred method 100 and system 200 are features that provide security for the information being requested and delivered over the internet. As such, the method 100 and system 200 disclosed can function without the use of the proxy applications 20 and 220, albeit with information transactions that may be less secure.

[ 0042] In Step S60, the provider side proxy application 220 verifies the digital signature attached to the SOAP request. The digital signature ensures that the SOAP request message received is from the intended consumer party and that the message has not been and was not tampered with in transit. The provider side proxy application can then verify or confirm that the consumer or merchant sending the SOAP request is authorized to request and receive transaction card information via the web service 210. For example, to confirm that a merchant is authorized to request and receive stored value card information from the information provider's stored value card applications and devices 260 and 270. Once the consumer digital signature is verified, the provider side proxy application 220 generates an out-of-band message and transmits the message to the third party computer system 120 for recordation that the SOAP request was received from the merchant or consumer at the provider's web server 210. Again, those of skill in

the art will also recognize that the out-of-band transmission or message sent to the third party 120 is optional and done as an enhancement aspect.

[ 0043] The sent and received messages indicating that SOAP requests were sent and received by the consumer or provider are preferably stored at the third party system 120. This information can later be accessed by either the consumer or provider through a web services network provided by a third party or at the third party system 120. The provision of services through web services networks is known to those of skill in the art. Further, the stored confirmation messages can be used to create and generate reports relating to web service 210 activity or to confirm that SOAP messages were sent or received by either the consumer or the provider.

[ 0044] In Step S70, the provider side proxy application 220 decrypts the SOAP request. The decrypted SOAP request is then routed to a provider side SOAP server application 230.

[ 0045] In Step S80, the SOAP server application 230 parses the XML formatted SOAP requests and determines what information has been requested by the consumer. In one embodiment, the requested information is selected transaction card information such as transaction history and balance information for a store value card or gift card. Those of skill in the art will recognize that the requested information could be any other information relating to a transaction card that is stored and available from the provider computer system. Once, this determination has been made, the SOAP server application 230 creates an information request compatible with the provider back-end system 240 which is operating in a provider platform. The provider platform or operating system can be the same or different than the consumer platform. The information request created by the SOAP server application 230 is then routed to the provider's back-end system 240 for processing and retrieval of the requested information.

[ 0046] The steps of Figure 1A continue and are shown in Figure 1B as depicted by the bubble Step A which indicates that the web service method 100 continues over to Figure 1B.

[ 0047] In Step S90, the information request is processed by the provider back-end system 240 via multiple transactions through designated computer resources and applications on the provider's internal network 250. The provider's internal resources 250 can access and retrieve the requested transaction card information directly from an appropriate database or storage location 270 or via a dedicated card server application 260 that can access and retrieve the requested transaction card information from an appropriate database or storage location 270 and pass it back through via the provider network resources and applications 250. The retrieved transaction card information is then routed to the provider SOAP server application 230.

[ 0048] In Step S100, the retrieved card information is converted to a standard XML format. The SOAP server application 230 then packages the retrieved information in an XML formatted SOAP reply and routes it to the provider side proxy application 220 at the web server 210.

[ 0049] In Step S110, the provider proxy application 220 will encrypt the received SOAP reply containing the retrieved information and include a digital signature in the SOAP reply uniquely corresponding to the provider.

[ 0050] In Step S120, the encrypted XML formatted SOAP reply with the provider's digital signature is transmitted or sent to the merchant's web server or web server application 10 over the internet 110. Simultaneously, an out-of-band message is generated by the provider side proxy application 220 and transmitted to the third party computer system or webs server application 120 for recordation that the SOAP reply was sent from the provider's web server application 210 to the consumer web server 10.

[ 0051] In Step S130, the consumer web server 10 receives the provider's SOAP reply at the merchant side proxy application 20. In Step S140, the consumer side proxy application 20 verifies the digital signature attached to the received SOAP reply corresponds to the information provider. The digital signature confirms that the provider sending the SOAP reply is coming from the information provider's web service 210 in response to the merchant's SOAP request. Once the digital signature on the SOAP reply is verified, an out-of-band message is generated and transmitted to the third party computer system or web server application 120 for recordation that the provider information SOAP reply was received at the merchant's web server 10.

[ 0052] In Step S150, the merchant side proxy application 20 decrypts the received SOAP reply and generates the XML formatted SOAP reply. The decrypted SOAP reply is then forwarded to the consumer SOAP server or application 30.

[ 0053] In Step S160, the SOAP server application 30 processes the SOAP reply and routes the XML formatted transaction card information to the consumer back-end system 40. The received XML formatted transaction card information may include information such as stored value card transaction history and balance. The consumer could have also, if authorized, requested and received other transaction card information from the provider system.

[ 0054] The SOAP server application 30 is preferably a separate application from the consumer side proxy application 20 and may run on the same or separate machine or computer. However, if a SOAP server application was not used in the system 200, the functions of the SOAP server application 30 could be accomplished by the consumer side proxy application 20 by additional appropriate software on the consumer side proxy application 20. In such a case, the consumer proxy application 20 would process the

SOAP reply and route the received XML formatted transaction card information to the consumer back-end system 40.

[ 0055] In Step S170, the XML formatted card information is received at intermediate applications or machines 50 in the consumer or merchant network 50 and then routed to consumer selected applications and devices 60 that can process and display the XML formatted card information. Alternatively, the XML formatted card information can be routed directly to the consumer selected applications and devices 60 for processing and displaying the XML formatted card information.

[ 0056] Since the requested information is received in the agreed upon standard format, i.e., in XML format, the merchant or consumer can process or manipulate the received information via existing applications 60 on the merchant's back end system 40. Further, the consumer or merchant can develop new applications and devices 60 to manipulate, process, store and display transaction card information from the provider system 202 since the information is received in a standardized XML format. As a result, the consumer or merchant can access the received information or data in a variety of devices and at many locations, including merchant retail locations, and present the information in an individualized manner suitable to the consumer, merchant, users and customers.

[ 0057] The received XML formatted information permits the consumer or merchant to display, process, store or integrate the received card information into existing applications including static or dynamic world wide web pages, which include among other applications web browsers, intranet, internet, and extranets, PowerPoint or Microsoft Word, smart card applications among other applications. The received XML formatted information can also be sent directly to end-point access devices having XML compatible applications, including among others merchant terminals, POS devices, cash

registers, PDAs, smart cards, transaction cards having embedded smart chips or integrated circuit chips with data storage capability and kiosks that are provided by the merchant for processing and displaying.

[ 0058] Figure 3 shows a block diagram representation of a second system 300 where the method 100 of Figures 1A and 1B for retrieving stored value information over the internet 110 via a web service 210 can be implemented. The system 300 of Figure 3 comprises a consumer network or system 301 operating on a first platform or operating system, and a provider network or system 302 operating on a second different platform or operating system.

[ 0059] The consumer network 301 comprises a web server 310 which can comprise a consumer side proxy application that connects the consumer network 301 to the internet 110. The web server 310 can also comprises a SOAP server application which would communicate with the back-end resources in the consumer network 301, including a Point of Sale (POS) terminal or machine 360, and a back office computer or terminal 363. The POS machine 360 and the back office computer 363 can initiate a request for selected information from the provider web service 210 and can also process and display XML formatted information received from the provider web service 210. The consumer network 301 also comprises a computer or machine 350 that can communicate directly with the third party network or application 120 to conveniently access and requests reports and statistics relating to information requested and received from the provider web service 210.

[ 0060] The SOAP server application on the web server 310 will receive the back-end request for selected information and create an XML formatted SOAP request which will be forwarded to the consumer side proxy application on the web server 310. The consumer side proxy application will assign a transaction number to SOAP requests,

encrypt and decrypt SOAP requests and replies, and transmits out-of band messages to the third party network or application indicating transmission or receipt of SOAP requests and replies. If no SOAP server application is included in the web server 310, the consumer side proxy application will also receive the back-end request for selected information and create an XML formatted SOAP request.

[ 0061] The information provider network 302 comprises a provider side SOAP server 330 with a SOAP server application and a web service application or provider side proxy application that connects the provider network 302 to the internet 110. The SOAP server application will communicate with the back-end resources of the information provider network 302. The provider side proxy application or web server application receives SOAP requests from the consumer network 301 and SOAP replies from the SOAP server application for processing. The provider side proxy application or web server application will encrypt and decrypt SOAP requests and replies and transmit out-of band messages to a third party network to indicate transmission or receipt of SOAP requests and replies. The SOAP server application will formulate requests for information and transmit the requests to the back-end system of the provider network 302. The back-end system of the provider system 302 will retrieved the requested information via multiple commands and means well known to those of ordinary skill in the art. The SOAP server application will then receive the retrieved information from the back-end system and formulate SOAP replies that are sent to the provider side proxy application.

[ 0062] Figure 4 shows a block diagram representation of a third system 400 where the method of Figures 1A and 1B for retrieving stored value information over the internet 110 via a web service 410 can be implemented The system 400 of Figure 4 comprises a consumer network or system 401 operating on a first platform or operating

system, and a provider network or system 402 operating on a second different platform or operating system.

[ 0063] The consumer network 401 comprises a consumer side proxy application 420 that resides on a web server that connects the consumer network 401 to the internet 110 and a client computer 360 in the consumer back-end system 340. The client computer 360 will initiate a request for selected information from the provider web service 410 and will also process and display XML formatted information received from the provider web service 410. The consumer side proxy application 420 receives requests for card information generated in the consumer system back-end 340 and creates an XML formatted SOAP request. The consumer side proxy application 420 assigns a transaction number to the SOAP requests, encrypts and decrypts SOAP requests and replies and transmits out-of band messages to a third party network indicating transmission or receipt of SOAP requests and replies.

[ 0064] The information provider network 402 comprises a provider side proxy application 425 that connects the provider network 402 to the internet 110 and that resides on a provider web server 410 or other server machine. The provider side proxy application 425 receives SOAP requests from the consumer network 401 and SOAP replies from the provider back-end system 440 and processes the requests and replies. The provider side proxy application 425 encrypts and decrypts SOAP requests and replies, and transmits out-of band messages to a third party network to indicate transmission or receipt of SOAP requests and replies. The provider side proxy application 425 will formulate SOAP replies when the provider network does not have a dedicated SOAP server application.

[ 0065] The provider network 402 also comprises a provider web service application 410 that can reside on two web servers 430A and 430B. The web servers

430A and 430B can execute redundant and identical applications and functions, or can execute specific non-redundant applications and functions. The web servers 430A and 430B provide the provider network's 402 connection to the internet 110 and will preferably each contain the provider side proxy application 425 which will receive and transmit all SOAP requests and replies. The web servers 430A and 430B may contain a SOAP server application to process SOAP requests and to formulate SOAP replies. If no SOAP server application is provided in the provider side network, the processing of SOAP requests and formulation of SOAP replies will be carried out by the provider side proxy application 425. Further, the provider web service application 410 is connected to a load balancer 427 which ensures that incoming traffic is routed to the appropriate web server 430A and 430B.

[ 0066] The provider web servers 430A and 430B are connected to a second load balancer 433 which will appropriately route a request for information through a first internal provider system firewall 445 which protectively controls the flow of information or messages to the back-end system 440 of the provider network 402. Having passed through the first firewall 445, requests for information are routed to one of two application servers 444A & 444B situated behind the first firewall 445. The application servers 444A & 444B can be redundant back-up to one another, or may be serve different portions 450 and 460 of the provider network 402. If the application servers 444A and 444B serve different portions 450 and 460 of the provider network 402, the load balancer 433 will route the request for information to the appropriate portion of the back-end system 440. Information requests proceed, through a second firewall 455 and 457, to the appropriate system resources and machines 450 and 460 in the back-end of the provider system 440 from which the requested information may be retrieved through multiple commands and means well known to those of ordinary skill in the art.

[ 0067] The invention has been described and illustrated with respect to certain preferred embodiments by way of example only. Those of ordinary skill in the art will recognize that the preferred embodiments may be altered or amended without departing from the true spirit and scope of the invention. Therefore, the invention is not limited to the specific details, representative devices, and illustrated examples in this description. The present invention is limited only by the following claims and equivalents.

**We Claim:**

1. A method for retrieving selected transaction card information in a standard format over a public interconnected network via a provider web service, comprising the steps of:

a) formulating a simple object access protocol (SOAP) request for transaction card information;

b) transmitting said SOAP request to the provider web service over the public interconnected network;

c) receiving said SOAP request at a provider web service;

d) reading said SOAP request to determine the transaction card information being requested;

e) retrieving the transaction card information from a storage location and forwarding the transaction card information to said web service;

f) formatting said transaction card information in an extensible markup language (XML) format and formulating a SOAP reply; and

g) transmitting said SOAP reply over the public interconnected network.

2. The method of claim 1 further comprising the steps of:

h) receiving said SOAP reply at a consumer web server application;

i) reading said SOAP reply to parse out said XML formatted transaction card information; and

j) routing said XML formatted transaction card information to one or more consumer back-end applications or end-point access devices.

3. The method of claim 2 further comprising the steps of:

prior to transmitting said SOAP request, encrypting said SOAP request, and providing said SOAP request with a consumer digital signature;

after receiving said SOAP request, verifying that said consumer digital signature on said received encrypted SOAP request corresponds to an authorized consumer and then decrypting said SOAP request;

prior to transmitting said SOAP reply, encrypting said SOAP reply, and providing said SOAP reply with a provider digital signature; and

after receiving said SOAP reply, verifying that said provider digital signature on said received encrypted SOAP reply corresponds to said provider, and then decrypting said SOAP reply.

4. The method of claim 3, further comprising the steps of:

generating and transmitting an out-of-band message to a selected third party application indicating that said SOAP request was sent to said web service;

generating and transmitting an out-of-band message to said selected third party application acknowledging that said SOAP request was received at said web service application;

generating and transmitting an out-of-band message to said selected third party application indicating that said SOAP reply was sent to said consumer web server application; and

generating and transmitting an out-of-band message to said selected third party application acknowledging that said SOAP reply was received at said consumer web server application;

whereby said third party application is adapted to store a plurality of received messages confirming that said SOAP request and said SOAP reply were transmitted and received by a consumer and provider network.

5. The method of claim 1, wherein said transaction card is a stored value card, a gift card, a credit card, a smart card, a bank card, a charge card or a financial card.

6. The method of claim 1, wherein said transaction card information is card transaction history and balance of said transaction card.

7. A method for retrieving selected transaction card information in a standard format over a public interconnected network via a provider web service, comprising the steps of:

a) formulating a simple object access protocol (SOAP) request for transaction card information at a web server application in a consumer network operating on a first platform;

b) transmitting said SOAP request to the provider web service over the public interconnected network;

c) receiving said SOAP request at a provider web service application of the provider web service;

d) reading said SOAP request to determine the transaction card information being requested;

e) generating and routing an internal information request based on said received SOAP request to a provider back-end network operating on a second platform;

f) retrieving said transaction card information from a storage location and forwarding the transaction card to said web service application;

g) formatting said retrieved transaction card information in an extensible markup language (XML) format and formulating a SOAP reply containing said XML formatted transaction card information;

h) transmitting said SOAP reply to said consumer web server application over the public interconnected network;

i) receiving said SOAP reply at said consumer web server application;

j) reading said SOAP reply to parse out said XML formatted transaction card information; and

k) routing said XML formatted transaction card information to one or more consumer back-end applications or end-point access devices.

8. The method of claim 7 further comprising:

prior to transmitting said SOAP request to said provider web service, encrypting said SOAP request, and providing said SOAP request with a consumer digital signature;

after receiving said SOAP request at said provider web service application, verifying that said consumer digital signature on said received encrypted SOAP request corresponds to an authorized consumer and then decrypting said SOAP request;

prior to transmitting said SOAP reply to said consumer web server application, encrypting said SOAP reply, and providing said SOAP reply with a provider digital signature; and

after receiving said SOAP reply at said consumer web server application, verifying that said provider digital signature on said received encrypted SOAP reply corresponds to said provider, and then decrypting said SOAP reply.

9. The method of claim 8, further comprising:

generating and transmitting an out-of-band message to a selected third party application indicating that said SOAP request was sent to said web service;

generating and transmitting an out-of-band message to said selected third party application acknowledging that said SOAP request was received at said provider web service application;

generating and transmitting an out-of-band message to said selected third party application indicating that said SOAP reply was sent to said consumer web server application; and

generating and transmitting an out-of-band message to said selected third party application acknowledging that said SOAP reply was received at said consumer web server application;

whereby said third party application is adapted to store a plurality of received messages confirming that said SOAP request and said SOAP reply were transmitted and received by a consumer and provider network.

10. The method of claim 7, wherein said transaction card is a stored value card, a gift card, a credit card, a smart card, a bank card, a charge card or a financial card.

11. The method of claim 7, wherein said selected card information is card transaction history and balance of said transaction card.

12. The method of claim 7, where said first platform and said second platforms are different operating systems.

FIG. 1A

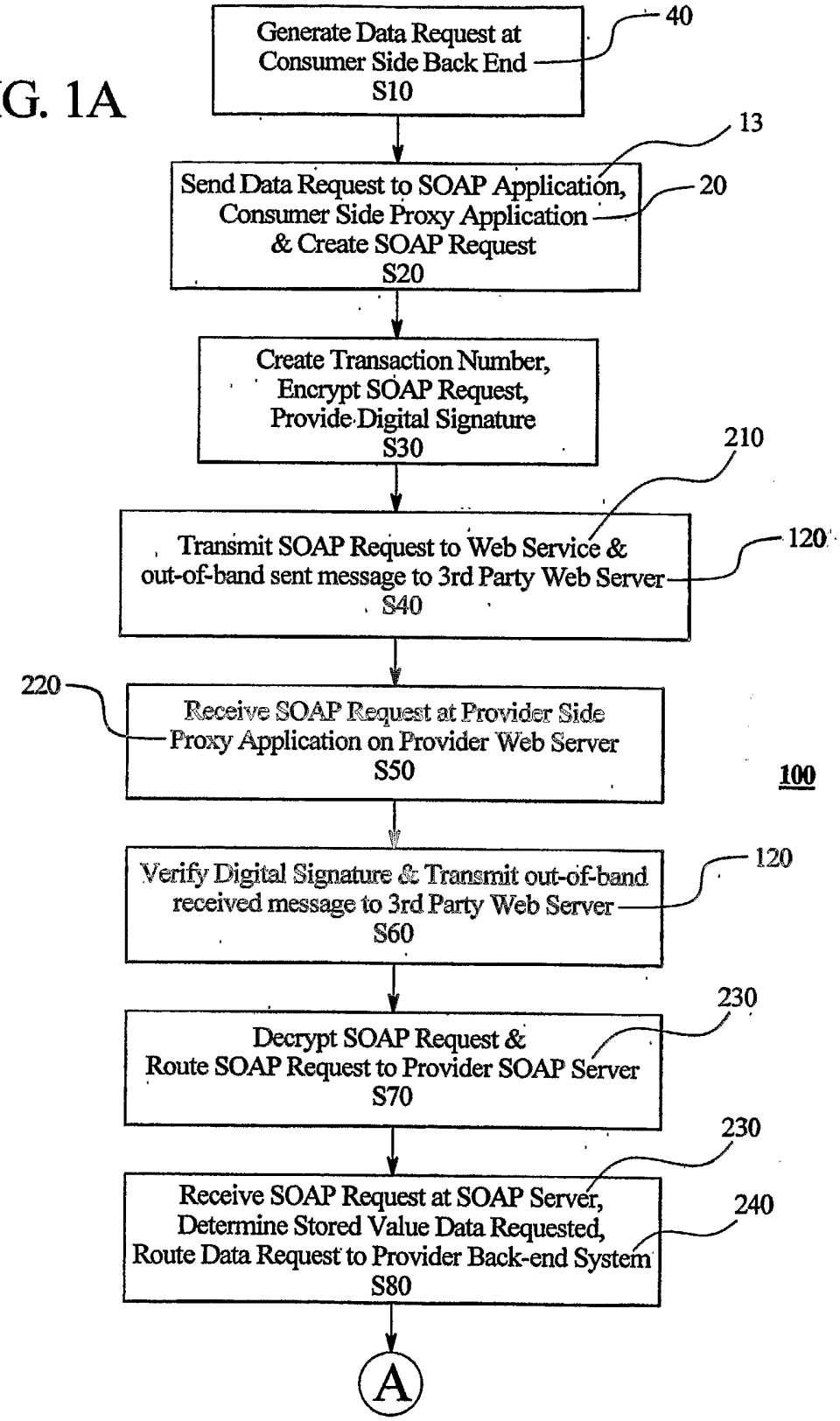
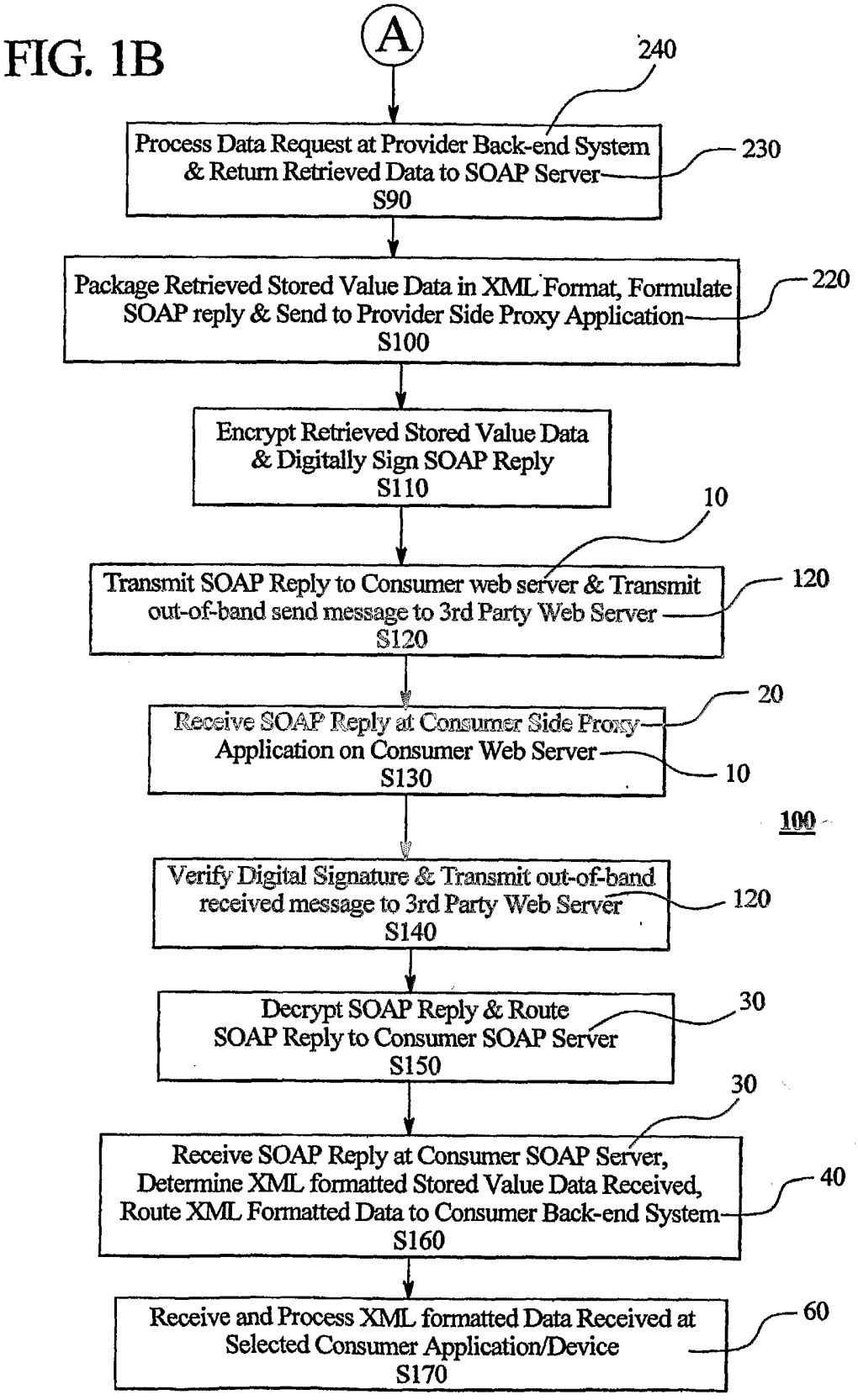

Generate Data Request at Consumer Side Back End S10
40
Send Data Request to SOAP Application, Consumer Side Proxy Application & Create SOAP Request S20
13
20
Create Transaction Number, Encrypt SOAP Request, Provide Digital Signature S30
Transmit SOAP Request to Web Service & out-of-band sent message to 3rd Party Web Server S40
210
120
Receive SOAP Request at Provider Side Proxy Application on Provider Web Server S50
220
100
Verify Digital Signature & Transmit out-of-band received message to 3rd Party Web Server S60
120
Decrypt SOAP Request & Route SOAP Request to Provider SOAP Server S70
230
Receive SOAP Request at SOAP Server, Determine Stored Value Data Requested, Route Data Request to Provider Back-end System S80
230
240
A

FIG. 1B


A
240
Process Data Request at Provider Back-end System & Return Retrieved Data to SOAP Server
S90
230
Package Retrieved Stored Value Data in XML Format, Formulate SOAP reply & Send to Provider Side Proxy Application
S100
220
Encrypt Retrieved Stored Value Data & Digitally Sign SOAP Reply
S110
10
Transmit SOAP Reply to Consumer web server & Transmit out-of-band send message to 3rd Party Web Server
S120
120
Receive SOAP Reply at Consumer Side Proxy Application on Consumer Web Server
S130
20
10
100
Verify Digital Signature & Transmit out-of-band received message to 3rd Party Web Server
S140
120
Decrypt SOAP Reply & Route SOAP Reply to Consumer SOAP Server
S150
30
Receive SOAP Reply at Consumer SOAP Server, Determine XML formatted Stored Value Data Received, Route XML Formatted Data to Consumer Back-end System
S160
30
40
Receive and Process XML formatted Data Received at Selected Consumer Application/Device
S170
60

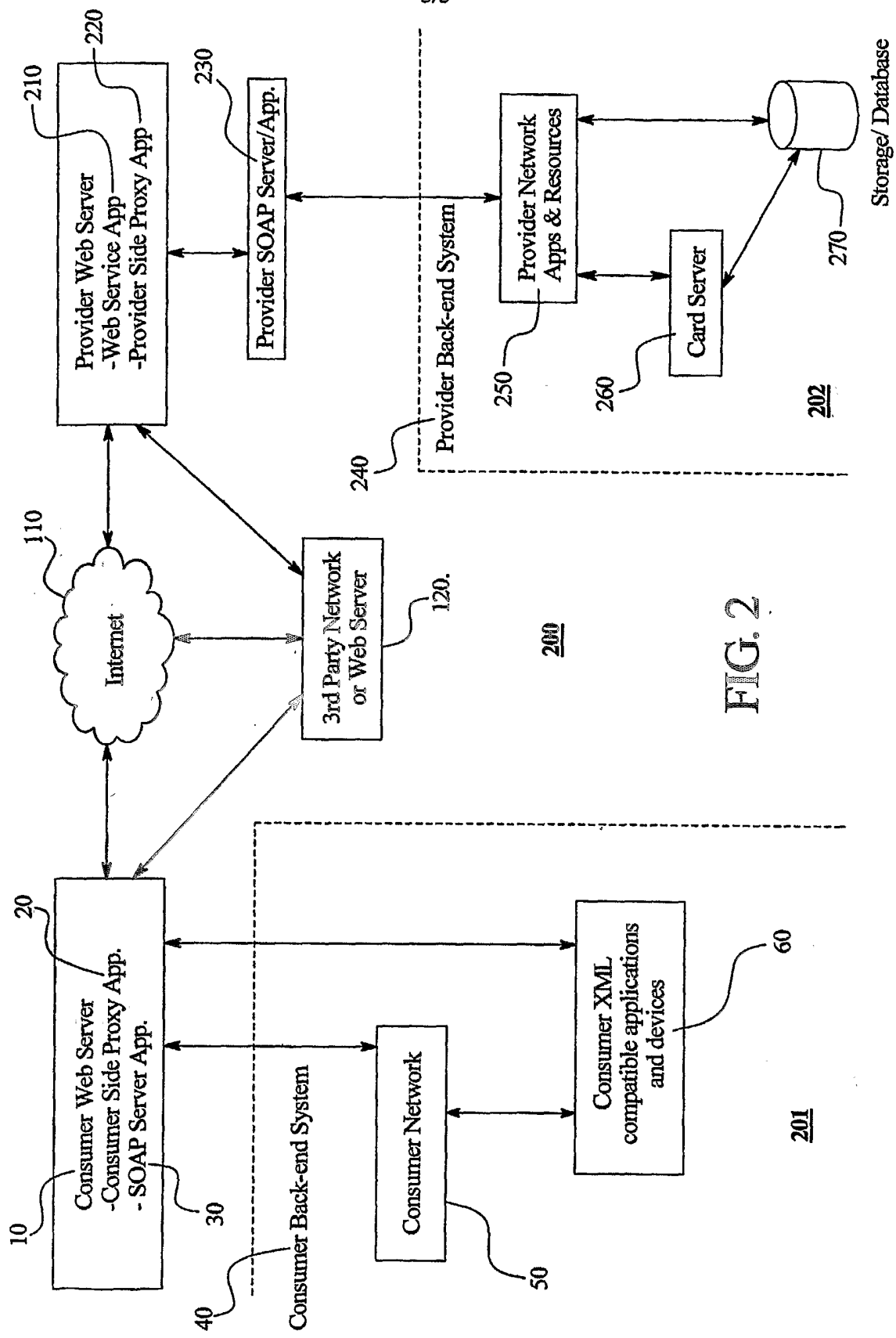
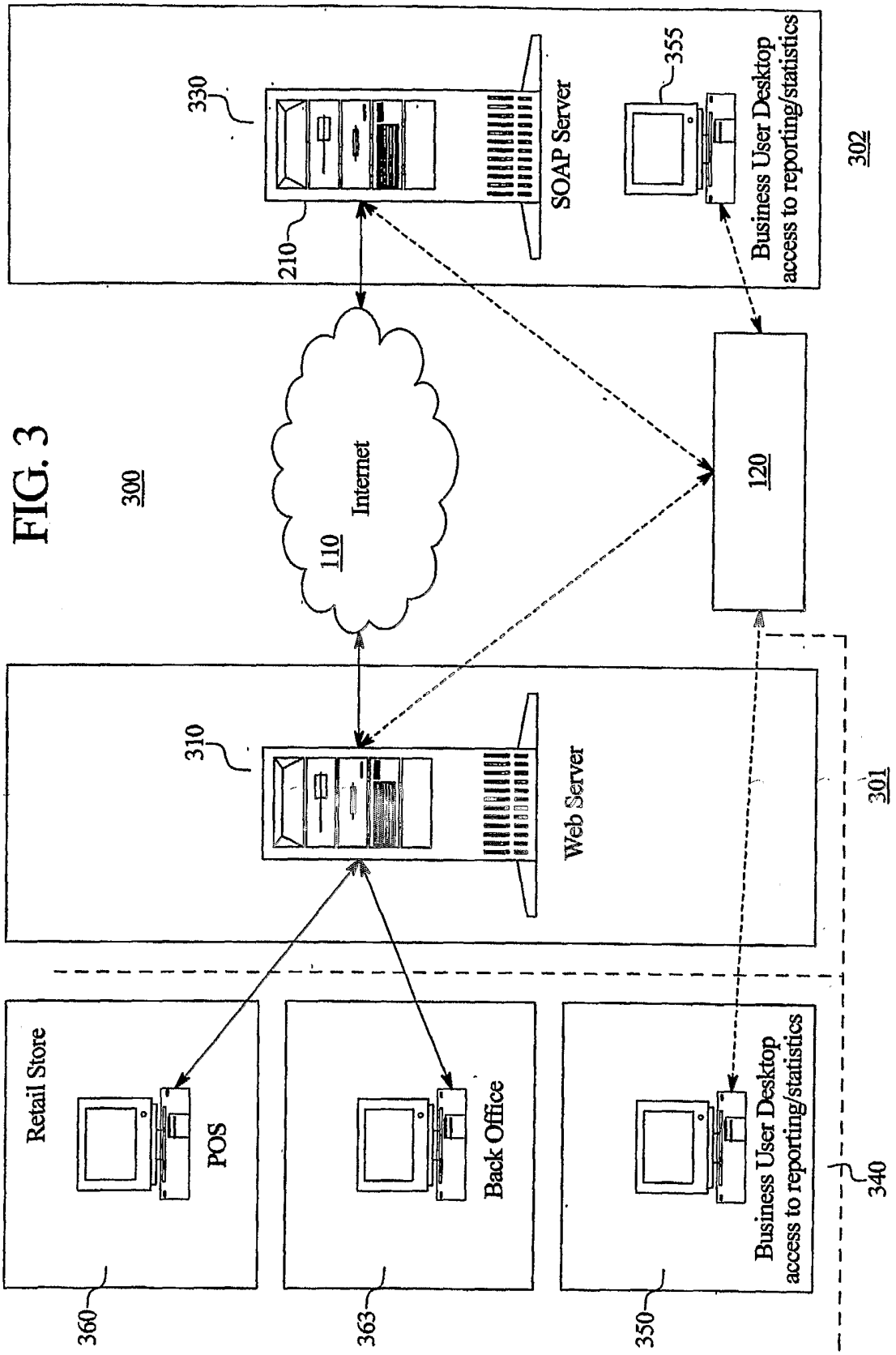

Consumer Web Server
-Consumer Side Proxy App.
- SOAP Server App.
Consumer Back-end System
Consumer Network
Consumer XML compatible applications and devices
201
Internet
3rd Party Network or Web Server
200
Provider Web Server
-Web Service App
-Provider Side Proxy App
Provider SOAP Server/App.
Provider Back-end System
Provider Network Apps & Resources
Card Server
Storage/ Database
202
10
20
30
40
50
60
110
120.
210
220
230
240
250
260
270

FIG. 2

FIG. 3


300
330
210
SOAP Server
355
Business User Desktop
access to reporting/statistics
302
Internet
110
120
310
Web Server
301
Retail Store
POS
Back Office
Business User Desktop
access to reporting/statistics
340
360
363
350

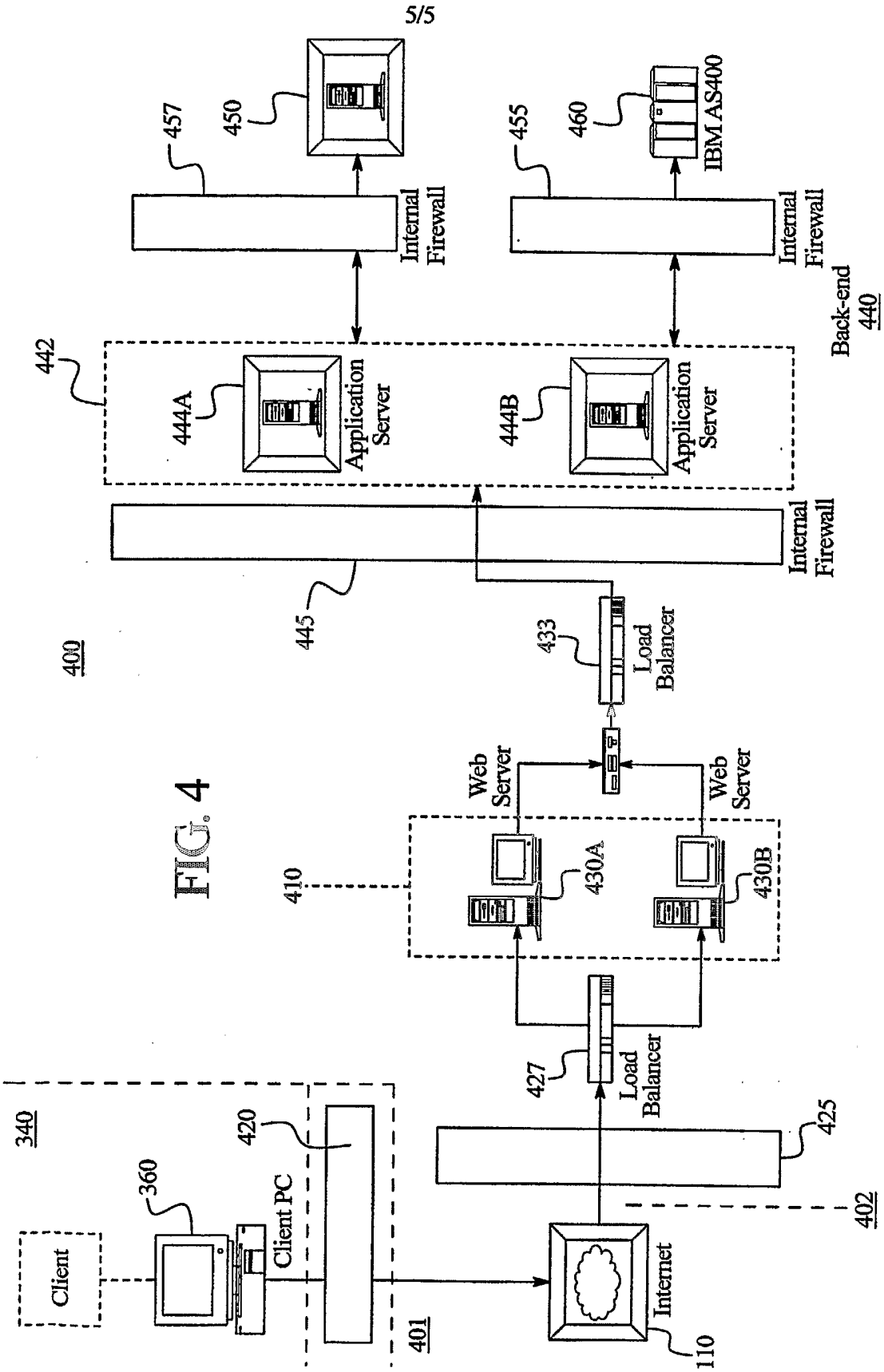

Client
360
Client PC
420
340
401
Internet
110
402
425
Load Balancer
427
Web Server
Web Server
410
430A
430B
Load Balancer
433
400
445
Internal Firewall
442
444A
Application Server
444B
Application Server
Internal Firewall
Back-end
440
457
450
Internal Firewall
455
460
IBM AS400

FIG. 4

# INTERNATIONAL SEARCH REPORT

International Application No
[redacted]/US2004/011476

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L29/08

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

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

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

EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | WO 03/024054 A (DELFINO JEAN-SEBASTIEN MICHEL ; PRZYBYLSKI PIOTR (CA); IBM UK (GB); BE) 20 March 2003 (2003-03-20) abstract page 1, line 1 - page 7, column 5 page 10, column 21 - column 28 | 1-12 |
| A | MARTIN G. NYSTROM: "Securing Web Services"'Online! 18 August 2002 (2002-08-18), XP002291164 Retrieved from the Internet: URL:http://www.shebeen.com/securews/> 'retrieved on 2004-07-04! Abstract IV Security solutions | 1-12 |

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 4 August 2004 | 07/10/2004 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,<br>Fax: (+31–70) 340–3016 | Bertolissi, E |

# INTERNATIONAL SEARCH REPORT

International Application No
[redacted]/US2004/011476

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| L | SECURITY FOCUS: "LIbrary entry"<br>SECURITY FOCUS WEB SITE, 'Online!<br>18 August 2002 (2002-08-18), XP002291165<br>Retrieved from the Internet:<br>URL:http://www.securityfocus.com/library/3<br>900> 'retrieved on 2004-08-04!<br>Document used for dating XP002291164.<br>----- | |
| A | HERDA S: "Non-repudiation: Constituting<br>evidence and proof in digital cooperation"<br>COMPUTER STANDARDS AND INTERFACES,<br>ELSEVIER SEQUOIA. LAUSANNE, CH,<br>vol. 17, no. 1, 1995, pages 69-79,<br>XP004046750<br>ISSN: 0920-5489<br>Abstract<br>2. Non-repudiation<br>7. Non-repudiation mechanisms<br>----- | 12 |
| A | US 6 457 066 B1 (AL-GHOSEIN MOHSEN ET AL)<br>24 September 2002 (2002-09-24)<br>abstract<br>figures 2,3A,3B<br>----- | 1-12 |
| A | WO 02/082305 A (GRUETZNER DR MATTHIAS ;<br>EIBACH WOLFGANG (DE); IBM DEUTSCHLAND<br>(DE); KU) 17 October 2002 (2002-10-17)<br>abstract<br>----- | 1-12 |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US2004/011476

| Patent document cited in search report | | Publication date | Patent family member(s) | | Publication date |
|---|---|---|---|---|---|
| WO 03024054 | A | 20-03-2003 | CA | 2357168 A1 | 10-03-2003 |
| | | | WO | 03024054 A2 | 20-03-2003 |
| US 6457066 | B1 | 24-09-2002 | NONE | | |
| WO 02082305 | A | 17-10-2002 | CA | 2436888 A1 | 17-10-2002 |
| | | | WO | 02082305 A2 | 17-10-2002 |
| | | | EP | 1388084 A2 | 11-02-2004 |
| | | | TW | 561751 B | 11-11-2003 |
| | | | US | 2004073661 A1 | 15-04-2004 |