

(51) International Patent Classification:
G06F 15/173 (2006.01)(21) International Application Number:
PCT/US2013/046749(22) International Filing Date:
20 June 2013 (20.06.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/547,716 12 July 2012 (12.07.2012) US(71) Applicant: **BANK OF AMERICA CORPORATION**
[US/US]; 214 N. Tryon Street, Mailcode NC1-027-20-05,
Charlotte, North Carolina 28255 (US).(72) Inventors: **RICE, Joseph Allen**; c/o Bank of America, 214
N. Tryon Street, Mailcode: NC1-027-20-05, Charlotte,
North Carolina 28255 (US). **CASTAGNA, Brandon Mat-**
thew; c/o Bank of America, 214 N. Tryon Street, Mail-
code: NC1-027-20-05, Charlotte, North Carolina 28255
(US).(74) Agents: **RAVULA, Surendra K.** et al.; Banner & Witcoff,
Ltd., 10 South Wacker Drive, Suite 3000, Chicago, Illinois
60606 (US).(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC,
SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).**Declarations under Rule 4.17:**

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

[Continued on next page]

(54) Title: OPTIMIZED SERVICE INTEGRATION

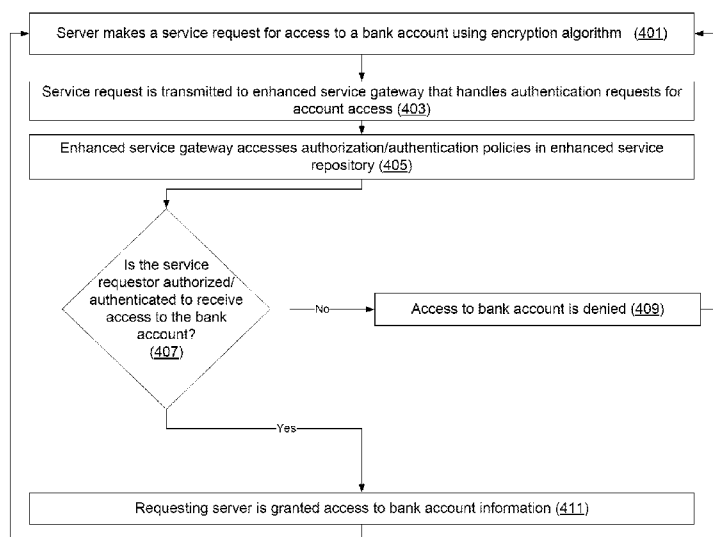


FIG. 4

(57) Abstract: An optimized service mediation framework may use customized tokens for reducing cost and latencies per transaction. In particular, a token service and an integration service may function together to generate customized tokens for use by network components within a transaction pathway. Each network component may access information with the token for a predetermined time period and/or for a predetermined number of service calls for service processing tasks related to mapping, security, governing, bridging, transforming, orchestrating, generating events, managing workloads, routing, validating, managing cache, encrypting, queuing and staging, commodity services, transaction management, and quality of service (QoS)/resiliency, among other things.

WO 2014/011376 A1



Published:

— *with international search report (Art. 21(3))*

OPTIMIZED SERVICE INTEGRATION

CROSS REFERENCE TO RELATED APPLICATIONS

[01] This international application claims priority to U.S. Application Serial No. 13/547,716 filed on July 12, 2012, and entitled “Optimized Service Integration.” U.S. Application Serial No. 13/547,716 is further a continuation-in-part of U.S. Application Serial No. 13/181,145 filed on July 12, 2011, and entitled “Service Mediation Framework.” U.S. Application Serial No. 13/547,716 is also a continuation-in-part of U.S. Application Serial No. 13/181,141 filed on July 12, 2011 and entitled “Dynamic Provisioning of Service Requests.” U.S. Application Serial No. 13/547,716 is also a continuation-in-part of U.S. Application Serial No. 13/181,151 filed on July 12, 2011 and entitled “Virtual Private Internet.” All of these applications are herein incorporated by reference in their entirety.

TECHNICAL FIELD

[02] Aspects of the invention generally relate to an optimized implementation of service integration via the use of extensible tokens. Each component of a network may use these tokens to perform common service processing tasks driven by standardized service policies that may be managed in a centralized repository.

BACKGROUND

[03] The Internet provides ubiquitous connectivity that is quick, open, and enables clear communication and exchange of ideas. Unfortunately, the Internet is not secure enough for many confidential, proprietary exchanges that occur within private networks such as those maintained by corporations, schools, governmental agencies, and the like.

[04] A private network (e.g., a corporate network) utilizes encryption to create a protected network that is secure. However, a private network is not open enough and instead creates barriers to agility. In particular, services within a private network are routed and accessed by point-to-point connections that are customized for each service. When changes need to be made to how services are provisioned and/or when new services need to be offered, there is no central place to advertise or manage access to the changes and/or new services. There is also no consistent way to connect users to each service in a secure, reliable and easy-to-provision way.

- [05] Today, in large corporations, there are tens of thousands of servers that function as hard-wired and hand-configured components. Under this scenario, it is very difficult to connect together a system that provides adequate speed, security, agility, and extensibility. In particular, this network configuration makes organizing cross-connectivity and integration across groups of people in a corporation challenging.
- [06] Moreover, network processes in private networks are implemented manually and in an ad-hoc way using information technology (IT) systems for performing steps such as defining, designing, procuring, building, developing, testing, promoting, certifying, and launching physical servers, network connectivity, and/or security capabilities. To implement these processes, conventional networks within an organization such as a corporation include tightly coupled layers of network components, manual configurations, and/or embedded code.
- [07] Increasingly, businesses need the ability to deploy IT systems in a fast, robust, secure, and extensible way. Moreover, services within and across business domains need to be connected in a governed and agile way.
- [08] Therefore, there is a need for a network implementation that would allow network components within a private network (e.g., corporate network, and the like) to have the same ease of connectivity as the Internet but also allow the ability to enforce policies and security as in a private network

BRIEF SUMMARY

- [09] In light of the foregoing background, the following presents a simplified summary of the present disclosure in order to provide a basic understanding of some aspects of the invention. This summary is not an extensive overview of the invention. It is not intended to identify key or critical elements of the invention or to delineate the scope of the invention. The following summary merely presents some concepts of the invention in a simplified form as a prelude to the more detailed description provided below.
- [10] Aspects of the disclosure address one or more of the issues mentioned above by disclosing methods, non-transitory computer readable media, and apparatuses for implementing common tasks such as security, content-based routing, logging, message format translation, and protocol bridging via extensible tokens within a

private network. This scheme may be implemented by using tokens that are valid for predetermined time intervals and conditions to reduce the latencies and cost per transaction within a service mediation framework.

- [11] Other aspects of the disclosure relate to an enhanced service DNS server which may resolve service uniform resource locators (URLs) into service addresses, an enhanced service router that may be configured to interpret the services being called and to route the requests in a way that delivers the best quality of service, an enhanced service repository that may serve as a secure, central, easy-to-use storage device to discover and publish new services or content within a private network, and an enhanced service gateway that may aid in deploying and registering services.
- [12] Yet other aspects of the disclosure relate to an optimized service mediation framework that allows devices within a network to communicate with one another in a standardized format and handle service requests via extensible tokens.
- [13] Aspects of the disclosure may be provided in a computer-readable medium having computer-executable instructions to perform one or more of the process steps described herein.

BRIEF DESCRIPTION OF THE DRAWINGS

- [14] The present invention is illustrated by way of example and is not limited in the accompanying figures in which like reference numerals indicate similar elements and in which:
- [15] Figure 1 shows an illustrative operating environment in which various aspects of the disclosure may be implemented.
- [16] Figure 2 is an illustrative block diagram of workstations and servers that may be used to implement the processes and functions of one or more aspects of the present disclosure.
- [17] Figure 3 shows an example network within an organization such as a bank that includes various service mediation framework devices for handling data communicated within the network, in accordance with at least one aspect of the disclosure.

- [18] Figure 4 shows an example method using the service mediation framework in accordance with at least one aspect of the disclosure.
- [19] Figure 5a shows a first implementation of extensible tokens within a service mediation framework, in accordance with at least one aspect of the disclosure.
- [20] Figure 5b shows a second implementation of extensible tokens within a service mediation framework, in accordance with at least one aspect of the disclosure.
- [21] Figure 6 shows various fields that may be a part of three different types of tokens, in accordance with at least one aspect of the disclosure.

DETAILED DESCRIPTION

- [22] As discussed above, there is a need for entities to deliver services and/or products better, faster, and cheaper in a way that allows for high availability, maximizing flexibility, and improving speed to market. The islands of infrastructure common in today's network systems need to be changed into networks that deliver composite services across business domain boundaries.
- [23] Figure 1 illustrates an example of a suitable computing system environment 100 that may be used according to one or more illustrative embodiments. The computing system environment 100 is only one example of a suitable computing environment and is not intended to suggest any limitation as to the scope of use or functionality contained in the disclosure. The computing system environment 100 should not be interpreted as having any dependency or requirement relating to any one or combination of components shown in the illustrative computing system environment 100.
- [24] The disclosure is operational with numerous other general purpose or special purpose computing system environments or configurations. Examples of well known computing systems, environments, and/or configurations that may be suitable for use with the disclosed embodiments include, but are not limited to, personal computers (PCs), server computers, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

- [25] With reference to Figure 1, the computing system environment 100 may include an enhanced network services device 101 wherein the processes discussed herein may be implemented. The enhanced network services device 101 may have a processor 103 for controlling overall operation of the enhanced network services device 101 and its associated components, including random-access memory (RAM) 105, read-only memory (ROM) 107, communications module 109, and memory 115. Processor 103 and its associated components may allow the enhanced network services device 101 to run a series of computer-readable instructions related to providing common service functions such as security, routing, and logging of messages by accessing information stored in an extensible token. Processor 103 may also direct enhanced network services device 101 to perform tasks such as orchestration, message format translation, and protocol bridging within a private network.
- [26] Enhanced network services device 101 typically includes a variety of computer readable media. Computer readable media may be any available media that may be accessed by enhanced network services device 101 and include both volatile and nonvolatile media, removable and non-removable media. By way of example, and not limitation, computer-readable media may comprise a combination of computer storage media and communication media.
- [27] Computer storage media include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. Computer storage media include, but is not limited to, random access memory (RAM), read only memory (ROM), electronically erasable programmable read only memory (EEPROM), flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to store the desired information and that can be accessed by enhanced network services device 101.
- [28] Communication media typically embodies computer readable instructions, data structures, program modules or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any information delivery media. Modulated data signal includes a signal that has one or more of its characteristics set

or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media.

- [29] Computing system environment 100 may also include optical scanners (not shown). Exemplary usages include scanning and converting paper documents, *e.g.*, correspondence, data, and the like to digital files.
- [30] Although not shown, RAM 105 may include one or more applications representing the application data stored in RAM 105 while the enhanced network services device 101 is on and corresponding software applications (*e.g.*, software tasks) are running on the enhanced network services device 101.
- [31] Communications module 109 may include a microphone, keypad, touch screen, and/or stylus through which a user of enhanced network services device 101 may provide input, and may also include one or more of a speaker for providing audio output and a video display device for providing textual, audiovisual and/or graphical output.
- [32] Software may be stored within memory 115 and/or storage to provide instructions to processor 103 for enabling enhanced network services device 101 to perform various functions. For example, memory 115 may store software used by the enhanced network services device 101, such as an operating system 117, application programs 119, and an associated database 121. Also, some or all of the computer executable instructions for enhanced network services device 101 may be embodied in hardware or firmware.
- [33] Enhanced network services device 101 may operate in a networked environment supporting connections to one or more remote computing devices, such as computing devices 141, 151, and 161. The computing devices 141, 151, and 161 may be personal computing devices or servers that include many or all of the elements described above relative to the enhanced network services device 101. Computing device 161 may be a mobile device communicating over wireless carrier channel 171.
- [34] The network connections depicted in Figure 1 include a local area network (LAN) 125 and a wide area network (WAN) 129, but may also include other networks.

When used in a LAN networking environment, enhanced network services device 101 may be connected to the LAN 125 through a network interface or adapter in the communications module 109. When used in a WAN networking environment, the enhanced network services device 101 may include a modem in the communications module 109 or other means for establishing communications over the WAN 129, such as the Internet 131 or other type of computer network. It will be appreciated that the network connections shown are illustrative and other means of establishing a communications link between the computing devices may be used. Various well-known protocols such as TCP/IP, Ethernet, FTP, HTTP and the like may be used, and the system can be operated in a client-server configuration to permit a user to retrieve web pages from a web-based server. Any of various conventional web browsers can be used to display and manipulate data on web pages.

- [35] Additionally, one or more application programs 119 used by the enhanced network services device 101, according to an illustrative embodiment, may include computer executable instructions for invoking functionality related to communication including, for example, email, short message service (SMS), and voice input and speech recognition applications (e.g., for transmitting service request information and/or receiving service responses, and the like). In addition, the application programs 119 may include computer executable instructions for invoking user functionality related to accessing a centralized repository for performing various service tasks like routing, logging, and protocol bridging.
- [36] Embodiments of the disclosure may include forms of computer-readable media. Computer-readable media include any available media that can be accessed by an enhanced network services device 101. Computer-readable media may comprise storage media and communication media and in some examples may be non-transitory. Storage media include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer-readable instructions, object code, data structures, program modules, or other data. Communication media include any information delivery media and typically embody data in a modulated data signal such as a carrier wave or other transport mechanism.

- [37] Although not required, various aspects described herein may be embodied as a method, a data processing system, or as a computer-readable medium storing computer-executable instructions. For example, a computer-readable medium storing instructions to cause a processor to perform steps of a method in accordance with aspects of the disclosed embodiments is contemplated. For example, aspects of the method steps disclosed herein may be executed on a processor 103 on enhanced network services device 101. Such a processor may execute computer-executable instructions stored on a computer-readable medium.
- [38] Referring to Figure 2, an illustrative system 200 for implementing example embodiments according to the present disclosure is shown. As illustrated, system 200 may include one or more workstation computers 201. Workstations 201 may be local or remote, and may be connected by one of communications links 202 to computer network 203 that is linked via communications links 205 to enhanced network services device 101. Workstations 201 may include many of the same hardware/software components as enhanced network services device 101. In some embodiments, workstations 201 may represent data stores for storing service policy data and metadata used by enhanced network services device 101. In other embodiments, workstations 201 may represent various types of enhanced network services devices 101 within network 200, including a device offering an integration service, a device offering a token service, an enhanced service DNS server, enhanced service router, enhanced service repository, and/or an enhanced service gateway. In system 200, enhanced network services device 101 may be any suitable server, processor, computer, or data processing device, or combination of the same. Enhanced network services device 101 may be used to process the instructions received from one or more users or one or more other devices (e.g., workstations 201).
- [39] Computer network 203 may be any suitable computer network including the Internet, an intranet, a wide-area network (WAN), a local-area network (LAN), a wireless network, a digital subscriber line (DSL) network, a frame relay network, an asynchronous transfer mode (ATM) network, a virtual private network (VPN), or any combination of any of the same. Communications links 202 and 205 may be any communications links suitable for communicating between workstations 201 and

enhanced network services device 101, such as network links, dial-up links, wireless links, hard-wired links, and the like.

- [40] The steps that follow in the Figures may be implemented by one or more of the components in Figures 1 and 2 and/or other components, including other computing devices.
- [41] In accordance with various aspects of the disclosure, methods, computer-readable media, and apparatuses are disclosed that allow an entity, such as a company, government agency, university, and the like, to implement advanced methodologies for the creation of a framework that may allow network components to receive service policy information in a standardized format from a centralized repository. In general, within the framework, the content of various messages and/or tokens associated with service requests transported within the network may drive the integration of the network components. The data within a message and/or token may be used to describe how a message may need to be processed by any one of the network components. The framework may define common functions such that any vendor or technology implementation within the network will be the same. The framework may facilitate standard network tasks such as routing, authentication, authorization, auditing, and transformations. These tasks may be executed dynamically based on the content of the message/token.
- [42] As used herein, a service request may relate to a variety of services provided by the network maintained by an organization. For instance, if the organization is a bank, the network maintained by the bank may provide services such as opening a bank account, registering for a credit card, and/or applying for a loan.
- [43] Each network component within the service framework may possess enhanced features that allow the component to access a datastore of detailed service policy metadata and data and implement service functions based on the service policy metadata/data. For instance, when the enhanced network services device 101 is an enhanced service router and/or an enhanced service DNS server, the device 101 may access routing policy information to determine a service address of a service provider and/or service routing policy information to transmit the service request to a preferred service provider of the requested service. In addition, when the enhanced network services device 101 is an enhanced service gateway, the device 101 may access and

implement other types of service policy information, such as those related to security (e.g., authentication and/or authorization), protocol bridging, and format translation. Moreover, when the enhanced network services device 101 is a service repository, the device 101 may store and/or export service policy data/metadata in a common format (e.g., based on a standard) and may include information on all of the common service policies commonly used within a private network. When the enhanced network services device 101 is a device offering an integration service, device 101 may analyze information associated with a service request to populate fields of a customized token for use by other network components. In addition, when the enhanced network services device 101 is a device offering a token service, device 101 may generate and digitally sign tokens for use by network components.

- [44] Figure 3 shows an example network 300 within an organization such as a bank that includes various service mediation framework devices for handling data communicated within the network 300, in accordance with certain aspects of the disclosure. Various departments with the bank may communicate over network 300 and each department may have its own enhanced service gateway. For example, Figure 3 shows an enhanced service gateway for an e-Commerce department 305, treasury and global banking department 307, deposits department 309, credit card department 311, and home loans department 313. One of ordinary skill in the art would recognize that each of the service gateways 305-313 may in fact be a cluster of service gateways 305-313 located within each bank department.
- [45] In the network 300, a client device 301 (e.g., user terminal, network server, and the like) within the bank may request a service in a variety of ways, including by a user inputting a service uniform resource locator (URL) into a browser running on device 301 and/or through a message transmitted from the client device 301. In some embodiments, client device 301 may actually represent multiple client devices 301. When a user of client device 301 initiates a web service by inputting a service URL into a browser, the service request may be transmitted to an enhanced DNS server 303, and the enhanced service DNS server 303 may resolve the service URL (e.g., the URL of a service provider) into a service address of a service provider for the service URL. For example, a service URL for accessing sports content may be “sports,” meaning that a user may access a preferred service provider for sports content within

a private network by typing in the word “sports” into a browser. Similarly, the service URL for accessing the latest news content may be “news,” and the service URL for accessing the latest weather information may be “weather.” One of ordinary skill in the art would recognize that alternative naming conventions may be used to designate a service URL.

- [46] In general, a service request may represent a higher order construct that specifies a desired resource. For instance, if a user initiates a service request for “sports,” the enhanced service DNS server 303 may access policy definition metadata stored on an enhanced service repository 317 that specifies a particular sports content provider. If the same user initiates this service request at a later date, the policy definition metadata for this service request may have changed during the interim; if so, the enhanced service DNS server 303 may access policy definition metadata that specifies that the service request for “sports” should be routed to a different sports content provider.
- [47] Other types of service requests may not involve a user-web service interaction; these service requests may be communicated directly between different network components. These server-server service interactions may involve various network resources (e.g., enhanced service gateways 305-313, enhanced service router 315, and the like) and may request that a service provider (e.g., one of the servers within the network) perform various network service tasks (e.g., authentication, logging, format translation, and the like) for a service requestor server. Similar to the user-web service interaction described in the previous paragraph, the service requestor (e.g., enhanced service router 315, enhanced service gateways 305-313, and the like) may access relevant service policy information stored in enhanced service repository 317 to perform the requested service. Also, as before, the service requestor may access and implement a service task that is consistent with the latest version of the service policy information stored in enhanced service repository 317.
- [48] In general, when the service request is a web-based browser interaction, the request may first be routed to an enhanced service DNS server 303 within the bank network 300, which may access routing policy metadata and data for the service request from the enhanced service repository 317. In some aspects, the enhanced service repository 317 may export a file including the routing policy information in Extensible Markup

Language (XML) format to the enhanced service DNS server 303. Once the enhanced service DNS server 303 obtains the routing information (e.g., a destination service address), server 303 may route the service request to an appropriate enhanced service gateway 305-313 that may handle the service request.

- [49] For server-server service interactions, when a client device 301 requests a service, the service request may not be first routed to the enhanced service DNS server 303. Instead, these service requests may be routed directly to an enhanced service router 315 and/or enhanced service gateways 305-313 (discussed further below). For instance, the service router 315 may aid in routing a service request to a predetermined queue for any message-oriented middleware.
- [50] In the process of routing the service request to one or more enhanced service gateways 305-313, the service request may also be routed to enhanced service router 315, which may also aid in routing the service request to an appropriate destination (e.g., across firewalls, and the like). In conventional systems, to access a service, a user must select a conventional URL on a web browser to call a web page. When the URL is selected, the user is connected to a single backend system (e.g., the service provider server) based on the URL. The enhanced service router 315, on the other hand, may allow a client device 301 to request a service using content-based routing. With this approach, instead of always using the same route to connect to a service provider or instead of using the same service provider to handle a given type of service request, the enhanced service router 315 may access routing policy metadata and data in enhanced service repository 317 to dynamically determine the best possible route and/or the best possible service provider for a given service request at the time that the service request is made. For instance, one service provider may be better than another service provider because of lower cost associated with providing the service.
- [51] Each of the enhanced service gateways 305-313 and the enhanced service router 315 may access metadata and data stored in enhanced service repository 317 to determine relevant policies that may need to be enforced on the service request. In some aspects, each of the components 301-317 within network 300 may be appliances configured to receive/transmit data from/to any other component 301-317 in XML format, among other formats. In addition, each appliance may be configured to

employ Extensible Stylesheet Language Transformations (XSLT) to allow one appliance to communicate with another appliance in a standard format.

- [52] Once the service request is routed to the appropriate destination (e.g., one of the enhanced service gateways 305-313), one of the enhanced service gateways 305-313 may transmit an appropriate response back to client device 301. Once again, in order to route the response to the service request back to client device 301, one of the enhanced service gateways 305-313 may access routing policy information from service repository 317.
- [53] In some aspects, the information stored within the enhanced service repository 317 may be updated periodically when the need arises. For instance, when a new service comes online within one of the departments within the bank, a set of policies governing that service may be added to enhanced service repository 317. Similarly, information within the enhanced service repository 317 may be updated when a service needs to be routed differently (e.g., because an older service URL has now become inactivated, and the like). In this way, the implementation of service policies may be automated and data-driven rather than driven through manual intervention.
- [54] The enhanced service gateways 305-313 may be configured to control a variety of service policies. Just as the enhanced service DNS server 303 and the enhanced service router 315 may access and implement routing policies by accessing policy metadata and data from the enhanced service repository 317, the enhanced service gateways 305-313 may access and implement other service policies stored in enhanced service repository 317, as outlined below.
- [55] The enhanced service repository 317 may store data related to operational (e.g., run-time) policies such as those relating to mapping, security, governing, bridging, transforming, orchestrating, generating events, managing workloads, routing, validating, managing cache, encrypting, queuing and staging, commodity services, transaction management, and quality of service (QoS)/resiliency, among other things, for use/access by any network component. Policies related to mapping may involve mapping abstract service names to concrete service names based on information within a service request (e.g., mapping an easy-to-understand term to a complex information technology (IT) function, operation, and/or endpoint, and the like). Policies related to security may include details on security functions such as

authentication (e.g., establishing identity through a credential), authorization (e.g., determining if access is authorized for a privileged resource), and auditing of services and/or service requests.

- [56] Meanwhile, policies related to governing may describe various methodologies for policy enforcement (e.g., at runtime and the like). For instance, policies may be enforced at various levels such as at the contract/client-operation level, option level, quality of service (QoS) or service level management (SLM) level, audit level, and/or the user level. Consider a scenario where bank is trying to open a new credit card account for a user. A policy enforced by contract/client operation may dictate that only those authorized persons in the credit card department of the bank may request to open a bank account. In other words, authorized personnel in the credit card department may possess a “contract” that allows them to request the client operation of opening a credit card account. Enforcing a policy at an option level may allow for control of service requests at a more granular level. For instance, a policy may specify options of how to open a variable interest rate credit card account or a fixed interest rate credit card account. In addition, a policy enforced at the QoS and/or SLM level relates to controlling concurrency and/or time-outs by client, provider, operation, contract, or option. For instance, a policy enforced at the QoS and/or SLM level may specify how many authorized personnel in the credit card department in one branch location may request to open a credit card account at the same time. Another policy enforced at the QoS and/or SLM level may specify the frequency and/or duration with which a given bank employee may request to open a credit card account for a customer.
- [57] In addition, a policy enforced at the audit level may relate to capturing data needed for triage or for rejected requests. For instance, a policy enforced at the audit level may specify how to notify (e.g., immediately, via a phone call, and the like) a customer when a wire transfer over a predetermined threshold value fails. Finally, a policy enforced at the user level may specify how different users should be treated differently. For example, a bank customer who is a high net worth individual may obtain a higher level of service (e.g., more prompt service, and the like) than an upper middle class individual, and user policies may specify these differences in service level for the two types of individuals.

- [58] Policies related to bridging may govern conversion of protocols and/or credentials so that they are compatible with one another (e.g., to allow one application to communicate with another). For instance, bridging policies may allow for compatibility between various types of credentials such as certificates (X.509 and the like) and tokens (e.g., tokens based on the Security Assertion Markup Language (SAML), OAuth, and the like). In addition, bridging policies may allow for converting data between various types of protocols such as Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Short Message Service (SMS), and the like.
- [59] Policies related to transforming may govern translation of data from one format (e.g., Simple Object Access Protocol (SOAP), fixed positional format that delimits fields, variable delimited format such as those that use commas to separate fields, industry standard formats, custom formats, and the like) to another. In yet other embodiments, policies in this category may also relate to enriching (e.g., adding/supplementing) data/messages and/or filtering (e.g., removing a few fields/characters) data/messages. Policies related to filtering may define techniques (e.g., via style sheet filters, and the like) to strip away information that is not needed in a service transaction. For instance, if a network is providing a service related to obtaining a credit card, a filtering policy may specify that confidential and/or sensitive information such as the social security number of the service requestor be removed from the service request before transmitting the service request to a company that prints credit cards.
- [60] Policies related to orchestration (e.g., business process management) may govern how multiple messages are split/merged and how complicated service requests may be divided into sub-requests. In some embodiments, business process management policies may describe orchestration of discrete services into a composite service. These policies may also govern process choreography (e.g., creating a workflow or sequence of steps) and complex event processing (e.g., analyzing a pattern/trend of events and making conclusions based on the pattern/trend to take an action).
- [61] Policies related to generating events may govern handling of performance logging, error logging, alerts, fraud events, and business events. Performance logging may relate to measuring, logging, and displaying (e.g., asynchronously so that these steps do not interfere with a transaction/message) the performance of any transaction or

message so that users may track the performance. Meanwhile, error logging may relate to recording error messages for triage. Policies related to alerts may govern how, when, and under what protocol (e.g., Simple Network Management Protocol (SNMP), and the like) alerts are generated for a variety of different events, including usage (e.g., for detailing how often a certain service is being used) and availability (e.g., for detailing the availability of a given service provider). Policies related to fraud events may detail how fraud events (e.g., unauthorized accessing of an account, and the like) are detected and logged. Finally, policies related to business events may detail how sales opportunities within an entity such as a company are generated, logged, and analyzed to determine if there are future sales opportunities for the entity. In general, policies related to logging may include information on when to log data (e.g., when a service request is made to measure performance metrics of the network such as the amount of time that the network takes to fulfill the service request, when access to a privileged network resource is granted or denied, when fraud is committed on the network, and the like).

- [62] Policies related to workload management may govern how workloads are distributed across multiple devices within a network (e.g., through load balancing). In other words, policies related to workload management may include information on how many and which network components may participate in responding to a service request (connection distribution, local load balancing, virtual machine (VM) level workload management, and the like). These policies may include those related to load balancing of incoming service requests (e.g., via self-balancing of workloads to distribute workloads to peer devices) or load balancing of outgoing service requests (e.g., based on a list of load balancer groups or endpoints, based on instances of Java virtual machines (JVMs), and the like).
- [63] Policies related to routing may govern various types of routing mechanisms in a service-oriented architecture, including fixed routing, content-driven routing, and context-driven (e.g., cost, availability and the like) routing. Policies related to fixed routing may allow for a one-to-one mapping for each service request (e.g., a single destination for each request). Meanwhile, policies related to content-driven routing may allow for profiling of content within each request to determine a destination. Finally, context-based routing may allow for routing requests based on dynamically

evaluating criteria such as cost, availability, and performance (e.g., response time) of various service providers.

- [64] In general, policies related to routing may define how to decide where to route a given service request or a response to a service request (e.g., DNS/QUEUE resolution, site selection, content or context based routing, and the like). The service mediation framework may employ a sophisticated and dynamic means of routing a message which is ultimately decoupled from the mediation logic. For a given service, there may be distinct data-types which may be marshaled from consumer to one or more providers. For any given service, there may be a single canonical data type on which the service may route the message. Across multiple services, there may be multiple canonicals which may be employed to facilitate normalization of data from service consumer to service provider. To maximize reuse, common routing implementations (or strategies) may need to be defined which work across all services with varying canonical data-types. Furthermore, different routing strategies may utilize varied logical parameters depending on the business requirement.
- [65] To facilitate dynamic content-based routing across this diverse system, each routing strategy may contain a capability to support multiple data formats. In this implementation, the service may contain a reference to a strategy. After mediating to the service canonical, the service mediation framework may pass the underlying canonical message to the strategy. Based on the type of message, the routing strategy may contain metadata for extracting logical routing fields from the specific payload content based on the data-type. Once the varied routing formats are normalized through the logical routing field extraction process, the routing strategy may execute the business logic to determine the service provider to which the message needs to be routed.
- [66] For instance, an example of context-based routing or decisioning, triggered by a run-time context, includes cost/performance-based routing (based on comparative costs per transaction and availability to lower-cost cloud computing versus higher cost and more resilient internal services on an entity controlled network). In this example, a service request may be routed in network 300 based on the lowest cost provider that meets the minimum availability and performance service level agreements (SLAs) for each request type. Another example of context-based routing or decisioning,

triggered by a run-time context, includes value-based service level management, where the business value (transaction amount or business impact of failure) for each transaction type (or service request type) may be coded as metadata in enhanced service repository 317 and is used to determine which transactions (or requests) may be guaranteed processing and which may be throttled or redirected when resources become constrained or demand exceeds rated capacity. Yet another example of context-based routing or decisioning, triggered by a run-time context, includes resource-based timing, where the amount of resources (e.g., threads, memory, connections, time-out values, and the like) may be allocated based on granular measurements of available resources by provider and service type. A final example of context-based routing or decisioning, triggered by a run-time context, may include the use of alternate path triggers. In this example, when virtual machine work-load management is configured, a service gateway 305-313 may determine that only some traffic may be served using dynamic content (from the active service provider virtual machine instances). Service gateways 305-313 may then route excess traffic to alternate internal service providers or adjust cache parameters in the message response header to trigger service of some requests via cached content that is still relevant but aged to a greater degree until demand subsides or additional dynamic service providers become available or more responsive.

- [67] In general, the ability of an enhanced service repository 317 to define significant triggers (driven by environment or run-time context) and to render resultant actions in a common way (e.g., XML) which may be acted upon by a diverse set of vendor tools throughout the network or even across multiple divisional or corporate boundaries may represent a breakthrough extension of federated connectivity and service management.
- [68] Policies related to validating may include those that validate files such as those written in Extensible Markup Language (XML), validate a schema of a service request (e.g., reject malformed request formats that do not conform to a prescribed format), and validate against a broad range of other threats (e.g., Structured Query Language (SQL) injection, distributed denial of service (DDoS), cross-site scripting, recursion attacks, and the like).

- [69] Policies related to managing cache may govern various types of caching methodologies (e.g., based on representational state transfer (REST), based on Hypertext Markup Language (HTML) objects, based on web services, and the like). Policies that govern REST-based caches (e.g., those that allow standard integration for name/value pairs of content) may enable stateless integration without losing the state across a cluster, policies that govern caching based on HTML objects may enable standard HTML and image caching, and policies that govern web service level caching may enable service and database caching to reduce backend service calls and/or database reads.
- [70] Policies related to encrypting may govern various types of encryption (e.g., coding) methodologies, such as encryption at the transport layer (e.g., creation of a tunnel and encryption of data that is transported through the tunnel), encryption at the field level (e.g., encryption of data elements for Payment Card Industry (PCI) compliance), and encryption via a hardware security module (HSM) (e.g., to store private keys used for encryption to deliver Federal Information Processing Service (FIPS) level 2 and/or 3).
- [71] Policies related to queuing and staging may govern various communication methodologies, including publication/subscription (e.g., for creating a one-to-many publication path involving creation and updating of topics so that those that subscribe to a given topic receive the updates), request/response (e.g., transmitting a message and receiving a response), datagrams (e.g., one way communication), asynchronous communication (e.g., receiving a response anytime (e.g., without waiting) in the future after a request is sent, synchronous communication (e.g., waiting for a response to be received immediately after a request is sent), and messaging (e.g., delivering a string of messages stored in a queue when appropriate).
- [72] Policies related to commodity services may govern log services and token services. Policies related to log services may enable recording of performance data, audit data, business events, fraud data, and the like onto a disk. Policies related to a token service may enable issuance of tokens in a predetermined format with predetermined fields to protect the tokens from tampering and to realize integration as a service.
- [73] Policies related to transaction management may specify details about transactions, such as whether a unit of work (UOW) can be defined (e.g., defining a set of required

steps for a transaction to occur) and how each step of the transaction should be rolled back (e.g., undone) if any one of the steps in the transaction fail to occur.

- [74] Policies related to QoS/resiliency may govern service level agreements (SLAs) (e.g., determining if a service provider is meeting a predetermined service level such as a time expectation for performing a service, taking actions based on whether a service provider is meeting or not meeting the predetermined service level), timeouts (e.g., waiting for a predetermined amount of time for an event to occur and releasing resources required for the wait even if the event has not occurred after the predetermined amount of time has elapsed), and sliding timers (e.g., a method to vary the wait time for an event to occur based on various factors).
- [75] In a typical multinational firm or federated enterprise that spans many large divisions, there may be multiple distributed information repositories (e.g., enhanced service repositories 317). Each may use a different vendor solution for storing and managing services or integration flows or connections. By including an integrated metadata repository (e.g., enhanced service repository 317), network 300 may have the flexibility to store and manage service or connectivity-related metadata (such as service or operation names, Web Services Description Language (WSDL) or interface details, authentication credentials, authorization credentials, authorization contracts or entitlements (either at the user or system level), triggers for actions such as logging, service level management and throttling, and multi-factor content-based routing, end-point and load balancer details, transformation and orchestration logic or rules, service-bus or segment mapping or other decisioning criteria) across this flexible array of departmental or divisional repositories while still being able to federate into a common repository that can normalize the information via a common application programming interface (API) or file interface specification and translate the enterprise view of the design-time data into run-time flows, routes or policies that can be enforced or executed in real-time as part of the cross-vendor service mediation framework (potentially interfacing to off-premise resources or entities via a virtual private internet connectivity.)
- [76] As an example, assume that a multi-division bank stores web service information in each division using division specific repositories (e.g., enhanced service repositories 317). In this example, division A may use a first commercially available repository,

division B may use a second commercially available repository, division C may use a home-grown repository, and division D may use a third commercially available repository. All of this service metadata may be integrated/imported using a common repository with a common interface or file format (e.g., a common API). This federated data may drive enterprise level reports showing holistic cross-divisional service interactions. The enterprise metadata may be used to create XML-formatted control files that enable any node of the network (comprising a vast array of diverse vendor tools configured to act as service mediation framework components such as service routers 315 or service gateways 305-313). This implementation may transform what used to be thousands of independent and uncoordinated vendor point solutions into a grid of interconnected and highly integrated common components that respond to centrally managed instructions or policies.

- [77] A common set of policies can be described via various tools and ultimately stored in open formats such as a common XML format to describe run-time policy statements. The enterprise repository (e.g., enhanced service repository 317) may manage this combination of enterprise service metadata and enterprise policies to control and manage connectivity, security, failover, route-away, logging, transformation and translation, orchestration and context based decisioning. The run-time context (real-time performance, cost, availability, quality-of-service (QoS), run-time characteristics such as resource usage and availability) may be measured and fed-back or made available to any node of the service mediation framework or to the enterprise repository itself to enable situation specific actions (context aware decisions).
- [78] Examples of the types of metadata stored in enhanced service repository 317 may include the name of a given service request, the network route that needs to be taken to reach a service provider for each service request, logging information related to the service request, the expected amount of time for getting a response to the service request, and the like. In general, metadata may include any piece of information that defines the interaction between a service requestor and a service provider, determines the route that a service request must take to get to a service provider, and/or authenticates or authorizes a service request. The enhanced service repository 317 may also include a list of common functions for a given service and/or the policies that guide the use of these functions. The enhanced service repository 317 may

export a file in a standardized format (e.g., XML) that any element (e.g., server) may process. The exported file may include information that allows the servers within a network to communicate about services via common protocols.

- [79] The specific service policy information stored in enhanced service repository 317 may be driven by a variety of factors, including which client device 301 is requesting the service, the type of service that the client device 301 is requesting, the time of day, the content of the service request message, and/or an overriding policy of the bank, among other things.
- [80] In certain aspects, the enhanced service repository 317 may define enough policies and metadata to cover all or a vast majority of all of the interaction points within an entity such as an organization. In some embodiments, the enhanced service repository 317 may export the policy information for service requests in a standard way. The data stored in and transmitted by the enhanced service repository 317 and/or the enhanced service DNS server 303 may be in a variety of formats, including XML.
- [81] In this way, if an organization (e.g., a financial institution, and the like) adds a new feature that depends on a service to its corporate network 300, the wait time for integrating the new feature to the corporate network 300 may be reduced drastically. Also, if changes are made to existing services, these changes may also be implemented in network 300 much more quickly. Thus, potential delays to market share that depend on this new feature may also likewise be reduced.
- [82] Figure 4 shows an example method using the service mediation framework, in accordance with certain aspects of the disclosure. The example of Figure 4 focuses on a service request that involves authorization and authentication of a service request for access to a bank account. The method shown in Figure 4 may start out at step 401 where a first server (e.g., a client device 301) within the bank may make a first request for access to a bank account using a given message encryption algorithm. The process may then move to step 403 where the service request may be transmitted to an enhanced service gateway (e.g., service gateways 305-313) that handles service requests for access to bank accounts.
- [83] Then, in step 405, the appropriate enhanced service gateway 305-313 may then access authentication/authorization policy metadata within enhanced service repository 317

to authenticate and/or authorize the requesting server for access to the bank account. The policies accessed by the enhanced service gateway 305-313 may include verifying the identity credential (e.g., a security token, a cryptographic key, and the like) of the requesting server, entitlement policies for information related to the bank account, and the like.

- [84] The process may then move to step 407 where the enhanced service gateway 305-313 may analyze the authentication/authorization service policies retrieved from the enhanced service repository 317 to determine if the service requestor should be given access to information in the bank account.
- [85] Assume that in this case one of the policies accessed includes a verification of the encryption algorithm used by the requesting server in the service request for access to the bank account. Assume also that an approved list of encryption algorithms for service requests for accessing bank accounts as stored in enhanced service repository 317 has been recently modified to exclude the type of encryption algorithm used by the requesting server in this case. In this case, the process may then move to step 409 where the enhanced service gateway 305-313 may deny the requesting server access to the bank account based on the use of an unapproved encryption algorithm (e.g., a security risk). The requesting server may then modify the encryption algorithm used to make the service request and resubmit the request in step 401.
- [86] Finally, if the requesting server is authorized/authenticated to receive access to information in the bank account, the enhanced service gateway 305-313 may grant the requesting server access to the bank account information in step 411.
- [87] In accordance with at least one aspect of the disclosure, an incoming service request may include content which will uniquely identify how to process the transaction. To identify the service mediation implementation, a token may be used to lookup a specific implementation in a shared metadata repository via a specific component, the service repository (both of which may be variations of service repository 317). Information in the service repository may reference the location of a distinct component in the shared metadata repository called the integration specification. The contents of the integration specification may identify all facets of integration between the service consumer and provider and the service mediation framework operates on this set of data for the execution of the mediation.

- [88] An example of the dynamic mediation logic captured in the integration specification of the service may be the metadata related to the publication of audit, or logging data. Via the integration specification, the service mediation framework may use bits of data specifically defined for audit to specify an alternative location for auditing as well as the specific data to be sent to the auditing system.
- [89] In accordance with aspects of the disclosure, extensible tokens (e.g., a set of computer-readable and/or computer-executable instructions) may be used to provide an integration service to determine and implement relevant policies. Each token may serve as a virtual service gateway and may be valid for a predetermined interval and/or for a predetermined number of service calls, thereby reducing the latencies associated with repeated service calls to a given resource over a period of time. After the predetermined interval has elapsed and/or after the predetermined number of service calls has been reached, a new token may need to be requested by one of the network components. In this way, instead of having a network device (e.g., a service gateway) as the policy enforcement point for each transaction, policies could be enforced once per interval, thereby reducing risk, overhead, and associated cost. In general, tokens establish the system, service, or end-to-end identity across a context. Tokens may be extended to add more information to each context, delivering more and more of the core integration functions that may otherwise be only possible via an in-line (e.g., in the communication path from a service requestor to service provider) service gateway.
- [90] Figure 5a shows a first implementation of extensible tokens within a service mediation framework, in accordance with certain aspects of the disclosure. In the example of Figure 5a, each service requestor 501 may communicate with network components such as service gateways, service routers, and/or service DNSs 503 that lie in the communication path to service providers 505. The service gateway, router, and/or DNS 503 may communicate (e.g., as a token agent for requesting customized tokens via a service call) with a network appliance that offers an integration service 507 to implement relevant policies via extensible tokens. The network appliance that offers the integration service 507 may transmit a token relevant to a given service request by receiving a generic token from a device that offers a token service 509. The token service 509 may transmit a token in a predetermined format with

predetermined fields and the relevant set of policies received from enhanced service repository 511 to the integration service 507. The integration service 507 may process the relevant policies and assist the token service to customize the generic token to populate each field of the token with a predetermined value prior to transmitting the customized token to device 503.

- [91] The process of creating a customized token for a given service request may involve calculation of complex parameters (e.g., parameters related to where to route, what transformations to make, and the like) based on knowledge of the service requestor, service provider, and policies (e.g., all of the policies associated with the integration functions discussed earlier) associated with the service request.
- [92] Once device 503 receives a token responsive to a given service request, device 503 may cache the token in a local memory for future use. Device 503 may also use the information within the token to route the service request to the correct service provider 505. In doing so, device 503 may transmit the token to the next intermediate device (not shown in Figure 5a) in the communication path to service provider 505. The intermediate device may also cache a copy of the received token prior to transmitting the token to any other intermediate devices (which may similarly cache the received token) in the communication path. In this way, each network device in the communication path to a service provider may maintain a local copy of the token and may access the token when future service requests require access of the information in the token. Thus, as long as a relevant token stored within a network device remains valid, the network device may use the information stored in the token to implement policies such as routing and protocol bridging to communicate with a service provider 505.
- [93] In accordance with aspects of the disclosure, a customized token may specify the conditions under which it is valid. For instance, a token may be valid for 100 service requests to the same service provider; alternatively or additionally, a token may be valid for a predetermined length of time (e.g., 30 days). After the token is no longer valid, device 503 may request another token from integration service 507.
- [94] Figure 5b shows a second implementation of extensible tokens within a service mediation framework, in accordance with certain aspects of the disclosure. In the example shown in Figure 5b, service requestors 501 may directly communicate with

integration service 507 to cause the generation of a customized token for one or more service requests. As before, integration service 507 may communicate with token service 509 to customize a generic token using policies from enhanced service repository 511. In this example, either the device implementing the integration service 507 or the service requestor 501 (e.g., via customized, re-usable computer-readable instructions executing on integration service 507 or requestor 501) may communicate with the appropriate service provider 505 once a customized token has been generated. If the device implementing the integration service 507 communicates with a service provider 505, the device implementing the integration service 507 may cache each customized token and function both as a token agent and as a service gateway, service router, and/or service DNS 503 for implementing relevant policies for a given service request based on information in the appropriate token. In other embodiments, a customized token may be transmitted from the device implementing integration service 507 to service requestor 501. In this scenario, service requestor 501 may function as a token agent and cache the received token and use the information contained in the token to communicate with the correct service provider 505. In this example, the service requestor 501 may store a software agent that functions to interact with an integration service 507.

- [95] Similar to the implementation shown in Figure 5a, the tokens generated through the implementation shown in Figure 5b may specify the conditions (e.g., length of time, number of service calls, and the like) under which the token is valid.
- [96] One of ordinary skill in the art would understand that devices 501-511 shown in Figures 5a and 5b may include one or more components of enhanced network services device 101.
- [97] Through implementation of tokens and a token service, aspects of the disclosure allow for dramatic reduction of overhead from integration and the generation of new modes of operation such as transaction tracing via a trace token and/or cost, performance, or availability-based routing. For instance, a token may store information related to the path that the token traversed to complete each service request (e.g., a transaction), the performance (e.g., time, reliability, and the like) of each network component in completing each step of the service request, and the function accomplished at each network component during each step of the service request. Once a token has stored

all of this information, the token service 509 may cause display of the information onto a dashboard for easy analysis by users. In this way, a token may serve as a trace token to allow users to determine the performance, cost, and availability of network components in the service pathway during the lifecycle of the service request. Using the information gathered by the token and displayed on the dashboard, future service requests may be routed differently to increase performance, reduce cost, and the like.

- [98] Figure 6 shows various fields that may be a part of three different types of tokens, in accordance with certain aspects of the disclosure. In particular, Figure 6 depicts fields that may be a part of an end-to-end token 601, service token 609, and a trace token 635. An end-to-end token 601 may include an original requestor ID field 603, a requestor channel code field 605, and a gateway segment field 607. The original requestor ID field 603 may represent an identification associated with a service requestor application (e.g., a serial number of an application located at a predetermined branch of a company at a predetermined location). The requestor channel code field 605 may represent the type of channel (e.g., classification) used by the requesting application (e.g., branch location, automated teller machine (ATM), mobile device, and the like). The gateway segment field 607 may represent the segment (e.g., physical location of network components) of network infrastructure used by the service requestor to transmit a request to a given service provider (e.g., to isolate unrelated network traffic within different segments).
- [99] A service token 609 may include a requestor application ID field 611, provider segment field 613, abstract service name field 615, abstract operation name field 617, rules table field 619, end-point field 621, concrete service name field 623, concrete operation name field 625, time to live field 627, refresh time field 629, usage limit field 631, and timeout field 633. The requestor application ID field 611 may represent an identification associated with a service requestor application (e.g., application located at a predetermined branch of a company at a predetermined location).
- [100] The requestor application ID field 611 of the service token 609 may be the same as the original requestor ID field 603 of the end-to-end token 601 for the first “hop” of a transaction pathway. For instance, if an application stored on a computing device associated with a bank teller transmits a first service request to open an account to a

first network component (e.g., a customer database) and the first network component in turn transmits a second service request to a second network component (e.g., credit card account database), each network component (or associated application) will have an associated requestor ID. For the first hop of the transaction pathway in this example, the original requestor ID field 603 and the requestor application ID field 611 will be the same (e.g., the ID associated with the application stored on the computing device associated with the bank teller). For the second hop of the transaction pathway in this example, the original requestor ID field 603 and the requestor application ID field 611 will be different; in particular, the original requestor ID field 603 will remain the ID associated with the application stored on the computing device associated with the bank teller whereas the requestor application ID field 611 will be the ID associated with a relevant application in the customer database that calls an application within the credit card account database. In this way, the values of fields 603-607 within end-to-end token 601 may persist over the entire transaction pathway whereas the values of fields 611-633 of service token 609 may change from hop to hop of the transaction pathway.

- [101] The provider segment field 613 may represent a pool of gateways (or an endpoint for a given pool of gateways) through which a service request must travel to arrive at a given service provider (e.g., a first pool of gateways associated with a given branch location in a first state versus a second pool of gateways associated with a given branch location in a second state). The abstract service name field 615 may represent an easy-to-understand name (e.g., open an account) associated with a service being requested by a service requestor. The abstract operation name field 617 may represent an easy-to-understand sub-category (e.g., open a fixed interest rate account, open a variable interest rate account, and the like) under the abstract service name field 617.
- [102] The rules table field 619 may represent a list of information (e.g., an XML table provided by a service requestor to an integration service 507 that includes metadata to distinguish between various service names/operation names) that may be used by integration service 507 to map between a concrete and abstract service name and/or between a concrete and abstract operation name.

- [103] The end-point field 621 may represent the address (e.g., uniform resource locator (URL) and/or queue) of the end-point for providing a concrete service and/or operation. The concrete service name field 623 may represent the specific service name (e.g., open credit card account) associated with a service being requested by a service provider. The concrete operation name field 625 may represent the specific operation name (e.g., open a credit card account with a fixed interest rate, open a credit card account with a variable interest rate, and the like) associated with a service being requested by a service provider.
- [104] The time to live field 627 may represent the amount of time (e.g., in seconds) for which a given service request is valid. The refresh time field 629 may represent the amount of time (e.g., in seconds) after which the service token 609 may need to be refreshed with a new token. The usage limit field 631 may represent the maximum number of invocations of a service specified by service token 609 after which the service token 609 may need to be refreshed with a new token. The timeout field 633 may represent the amount of time (e.g., in milliseconds) that a service requestor should wait for a response to a given service request.
- [105] A trace token 635 may include a requestor application ID field 637, concrete service name field 639, concrete operation name field 641, and a list of applications and timestamps along the transaction path field 643. The requestor application ID field 637 of trace token 635 may include the same information as the requestor application ID field 611 of service token 609. The concrete service name field 639 of trace token 635 may include the same information as the concrete service name field 623 of service token 609. The concrete operation name field 641 of trace token 635 may include the same information as the concrete operation name field 625 of service token 609. Finally, the list of applications and timestamps along the transaction path field 643 may represent an up-to-date list of service requestor applications and timestamps associated with these applications for each service requestor up to a given hop in the transaction path. Using this field, as a service request is transmitted to each successive hop, the list of service requestor applications and timestamps along the transaction path field 643 is extended with the service requestor application and timestamp information for that hop.

- [106] Each of the tokens mentioned above may be digitally signed to prevent tampering. Also, each token may be cached at different points along the transaction pathway. For instance, the end-to-end token 601 may be cached at the first hop (e.g., a service gateway) in the transaction pathway. Meanwhile, a different service token 609 may be cached at each hop of the transaction pathway (e.g., because the requestor application ID changes from one hop to the next). A different trace token 635 may be cached at each service provider in a transaction pathway (e.g., because the list of service requestor applications and timestamps along the transaction path field 643 is extended at each successive hop of the transaction path).
- [107] In addition to the three tokens mentioned above, aspects of the disclosure also allow for the use of system certificates which may include various fields related to authentication. For instance, a system certificate may include fields related to a system ID (e.g., an identifier associated with a hardware component that represents a given service requestor) and/or a test/production indicator (e.g., an indicator that prevents a test system from calling a production provider and vice versa). System certificates may be cached at a service requestor and may prevent man-in-the-middle attacks (e.g., mutual secure socket layer (SSL) or authentication).
- [108] One of ordinary skill in the art would understand that tokens 601, 609, and 635 and system certificates may include additional or alternative fields that allow the tokens/certificates to implement each function of an integration service 507.
- [109] It should be noted that the term policy, as used throughout this disclosure, may be a generalization that describes the definition of any run-time decision or action driven by an implicit decision (automatically without any pre-configuration on the part of the user) or an explicit decision (driven by the presence of content in the request or via configuration of metadata in a repository or system of record where the threshold or data to drive that action is maintained).
- [110] Embodiments of the disclosure allow for the creation of a run-time agent in any language or programming construct running on any platform that can understand and execute a given policy or conditional run-time action driven by either content in the message or response, by context based on local measurement of conditions, or via configuration and relationships between associated data elements or objects. This agent may then act on a service token or similar policy token which contains policy

information such as routing, transformation, or SLA management data. Any intermediate agent may identify the context of the message and inject a suitable service or policy token for action either within that node or on a node downstream from that node that will later interact with the message.

- [111] In addition, any number of design-time systems or tools may be created that allow both the definition of policy or run-time actions, groups, or bundles and their association with service objects such as the service requestor, service provider, the service, the operation, or some combination of the four (often called the service contract).
- [112] Policies may also be expressed in any number of industry standard or proprietary policy dialects. If expressed in these formats, the policy may be more readily reused and attached across diverse systems, but this complicates the application of logic to limit the possible combinations and attachments of policies to service objects. Keeping the policies as centralized configurations defining relationships within a single user interface may afford the ability to manage all interactions and combinations assuring that only valid, certified, pretested, or desired combinations or attachments are permitted.
- [113] Aspects of the invention have been described in terms of illustrative embodiments thereof. Numerous other embodiments, modifications and variations within the scope and spirit of the appended claims will occur to persons of ordinary skill in the art from a review of this disclosure. For example, one of ordinary skill in the art will appreciate that the steps illustrated in the illustrative figures may be performed in other than the recited order, and that one or more steps illustrated may be optional in accordance with aspects of the invention.

What is claimed is:

1. A non-transitory computer-readable storage medium having computer-executable program instructions stored thereon that when executed by a processor, cause the processor to perform:
 - (a) receiving, from a client device, a service request associated with a service;
 - (b) transmitting the service request to an integration service;
 - (c) receiving, from the integration service, a customized token for handling the service request;
 - (d) caching the customized token;
 - (e) analyzing information within the customized token to determine a plurality of policies for handling the service request; and
 - (f) based on the analysis, routing the customized token to a service provider.
2. The non-transitory computer-readable storage medium of claim 1, wherein the service request includes an Extensible Markup Language (XML) table with rules for distinguishing between a plurality of services.
3. The non-transitory computer-readable storage medium of claim 1, wherein the service request is chosen from the group consisting of: opening a bank account, registering for a credit card, and applying for a loan.
4. The non-transitory computer-readable storage medium of claim 1, wherein the customized token includes a requestor application ID field, a provider segment field, an abstract service name field, and a concrete service name field.
5. The non-transitory computer-readable storage medium of claim 1, wherein the customized token includes a time to live field, a refresh time field, a usage limit field, and a timeout field.
6. The non-transitory computer-readable storage medium of claim 1, wherein the customized token comprises a service token.
7. The non-transitory computer-readable storage medium of claim 1, wherein the analyzing comprises determining an address of the service provider associated with the service request.

8. The non-transitory computer-readable storage medium of claim 1, wherein the customized token is valid for a predetermined number of service requests.

9. The non-transitory computer-readable storage medium of claim 8, wherein the processor further performs: after the predetermined number of service requests, receiving a new customized token from the integration service.

10. The non-transitory computer-readable storage medium of claim 1, wherein the customized token is valid for a predetermined length of time.

11. A computer-assisted method comprising:

receiving, through a communication module associated with the computer, a service request associated with one of a plurality of available services and a rules table for distinguishing between the plurality of available services;

transmitting, through the communication module, the service request and the rules table to a token service;

receiving, through the communication module, a generic token with predetermined fields in a predetermined format;

using the rules table, calculating, at a processor associated with the computer, parameters for placement in each of the predetermined fields of the generic token;

transmitting the calculated parameters to the token service; and

based on the calculated parameters, receiving, from the token service, a customized token storing the calculated parameters.

12. The computer-assisted method of claim 11, further comprising: transmitting, through the communication module, the customized token to a service gateway.

13. The computer-assisted method of claim 11, wherein the rules table comprises an Extensible Markup Language (XML) table with rules for distinguishing between the plurality of available services.

14. The computer-assisted method of claim 11, wherein the calculated parameters relate to at least one integration function chosen from the group consisting of: mapping, security, governing, bridging, transforming, orchestrating, generating events, managing workloads, routing, validating, and encrypting.

15. The computer-assisted method of claim 11, wherein the predetermined fields include a requestor application ID, provider segment, abstract service name, concrete service name, and a usage limit.

16. A system comprising:

a service repository configured to store a plurality of service policy metadata associated with a plurality of service processing tasks, wherein the plurality of service processing tasks include entitlement, routing, workload management, logging, protocol bridging, format translation, filtering, and business process management, wherein the plurality of service policy metadata are periodically updated when a new service comes online and older service policy information becomes obsolete;

a token service configured to access the plurality of service policy metadata stored in the service repository to generate a customized token for handling a given service request; and

a service gateway configured to receive, cache, and analyze information in the customized token for performing at least one of the plurality of service processing tasks associated with the given service request.

17. The system of claim 16, wherein the customized token is valid for at least one of a predetermined time period and a predetermined number of service calls.

18. The system of claim 16, wherein the customized token includes a plurality of predetermined fields and wherein at least one of the plurality of predetermined fields is a list of service requestor applications and timestamps associated with each device along a transaction pathway.

19. The system of claim 16, wherein the customized token includes a plurality of predetermined fields for routing the given service request to a predetermined service provider, for mapping the given service request into a concrete service name, and for authenticating a requestor of the given service.

20. The system of claim 16, wherein the token service is configured to generate a new customized token after a predetermined time period.

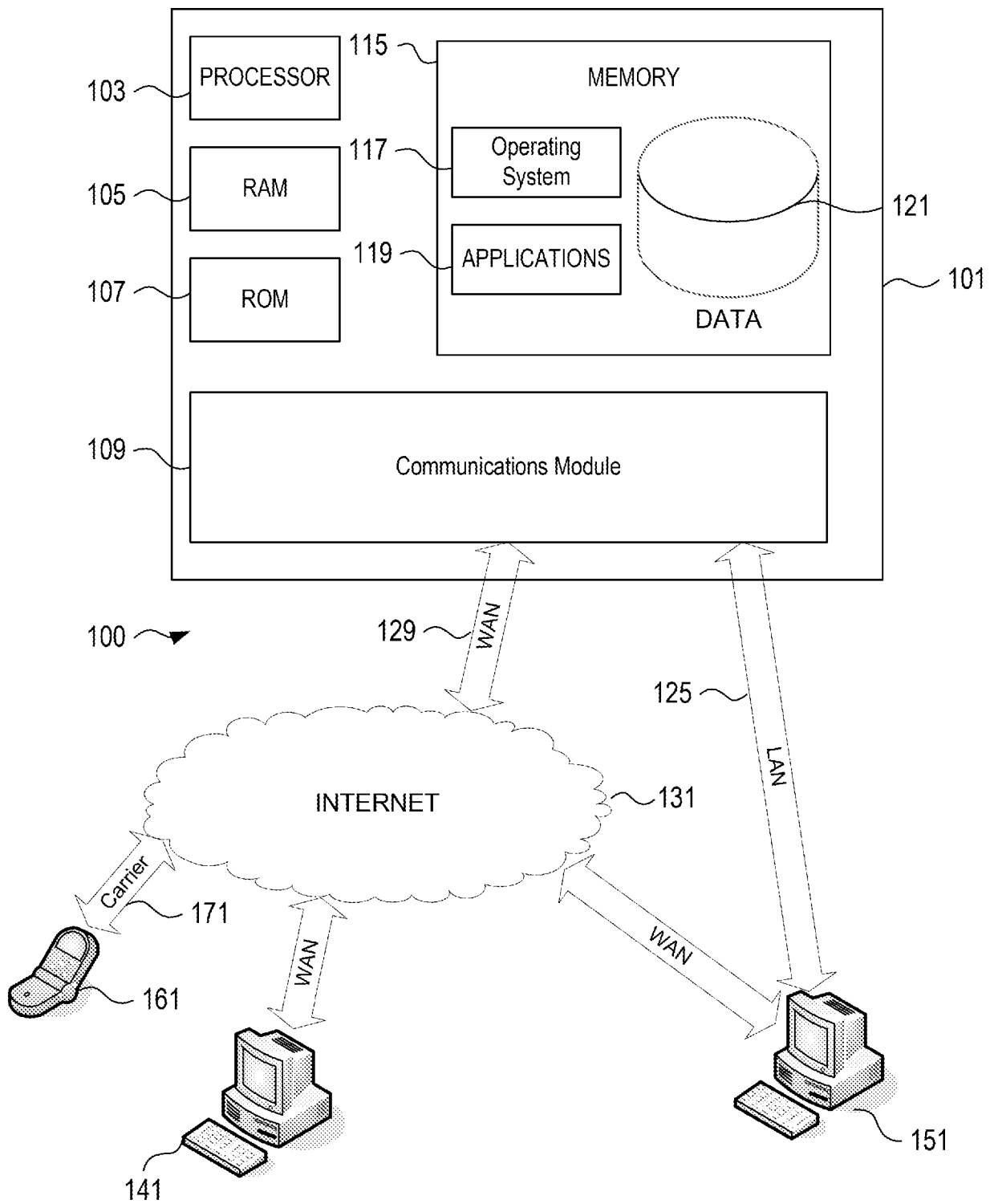


FIG. 1

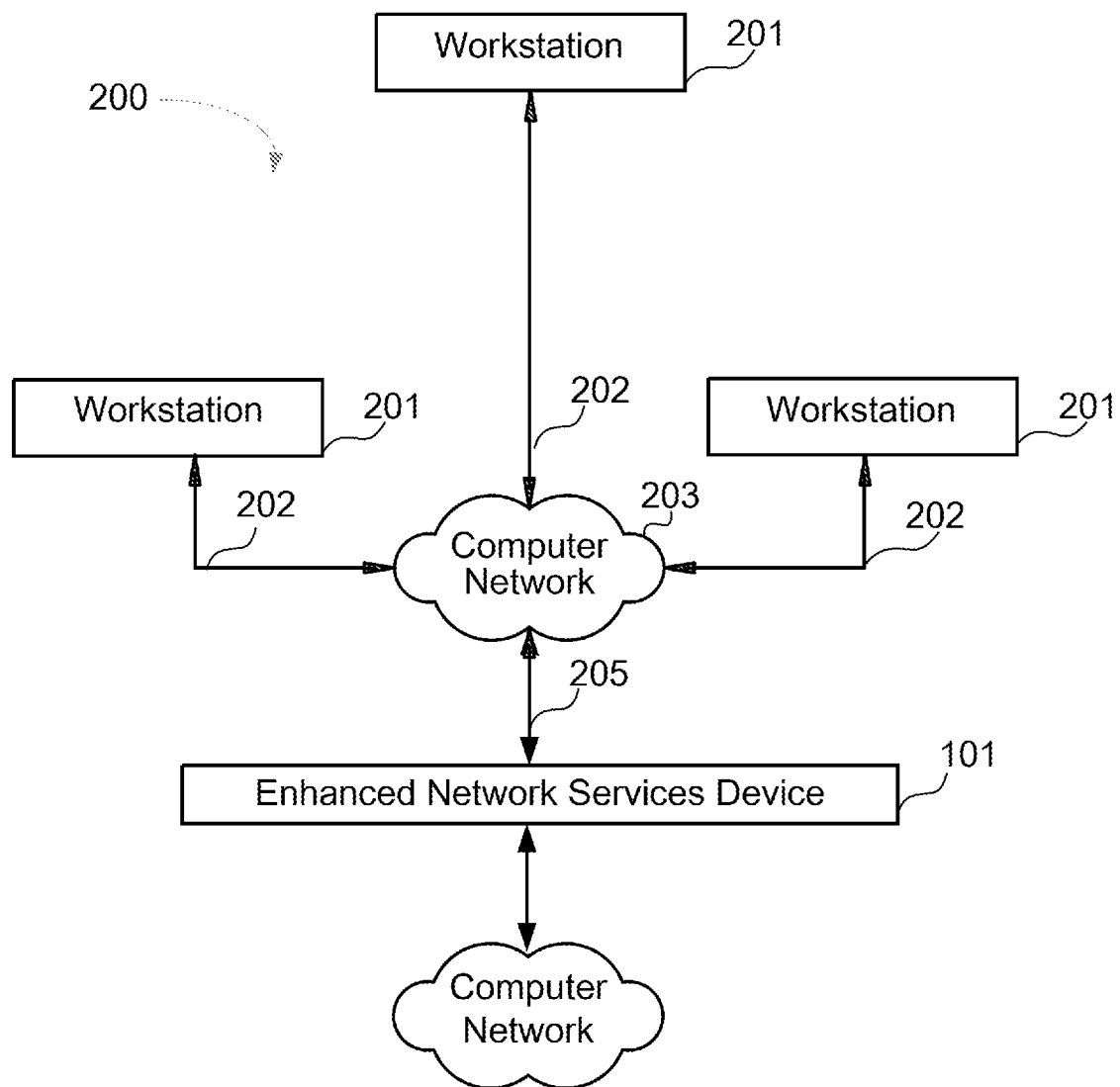


FIG. 2

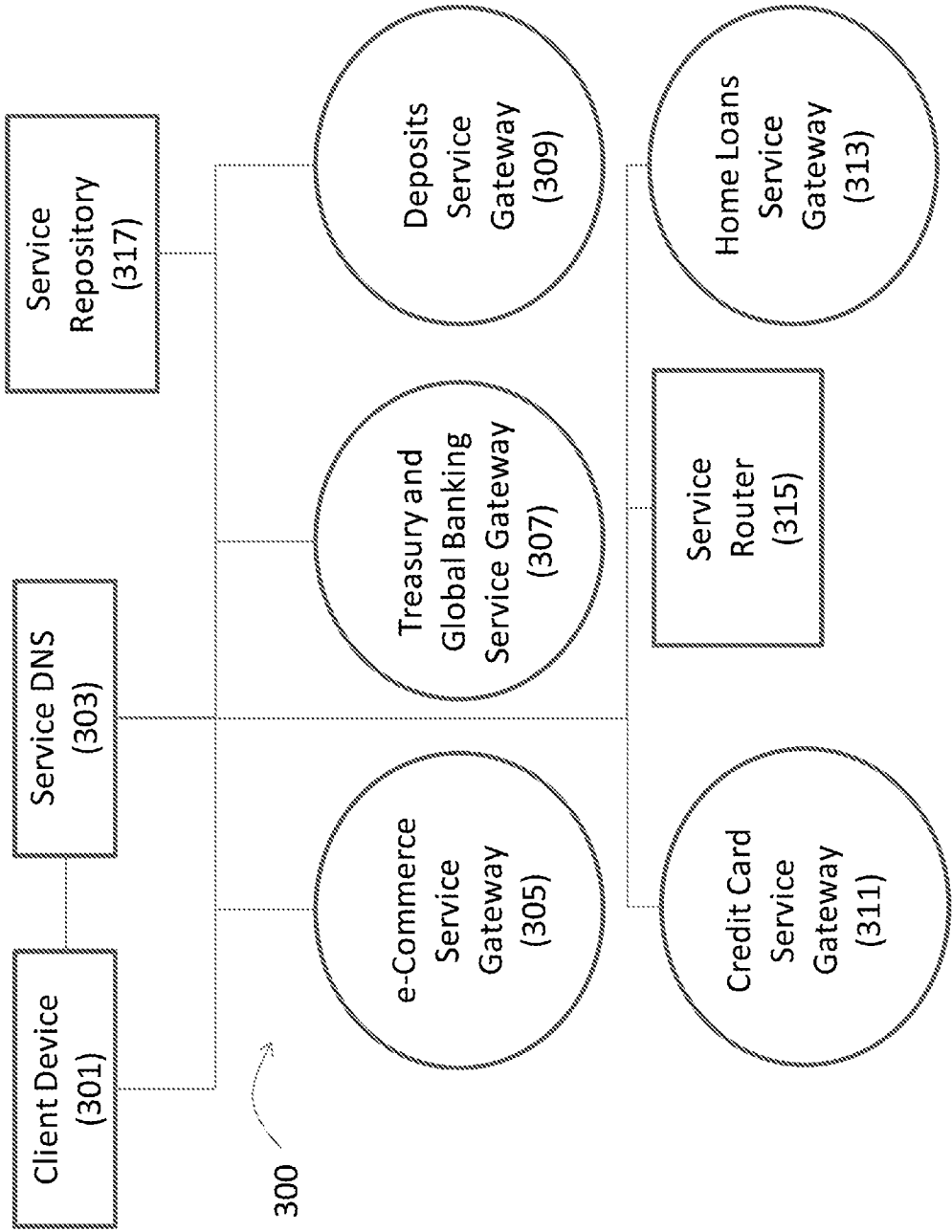


FIG. 3

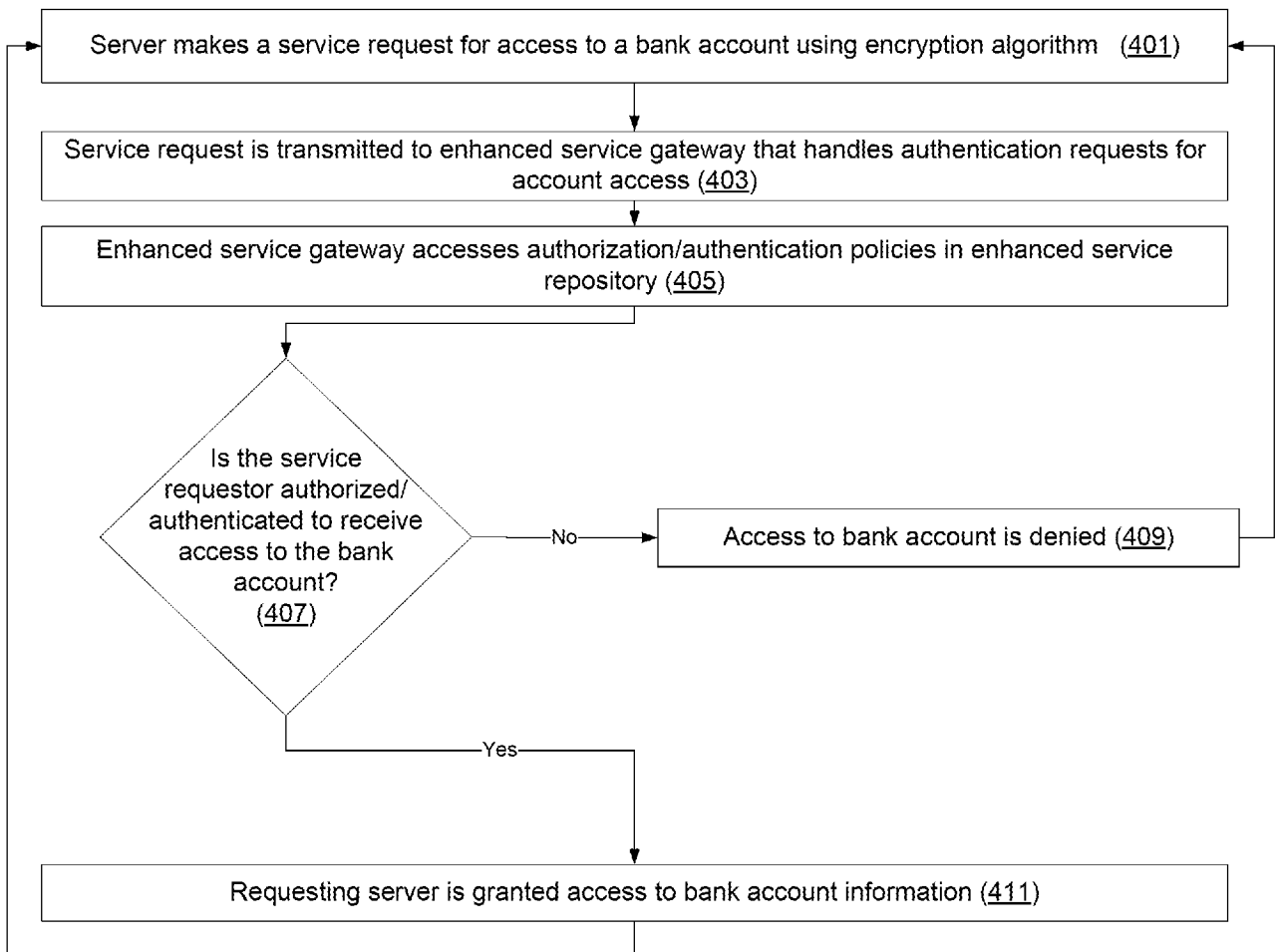


FIG. 4

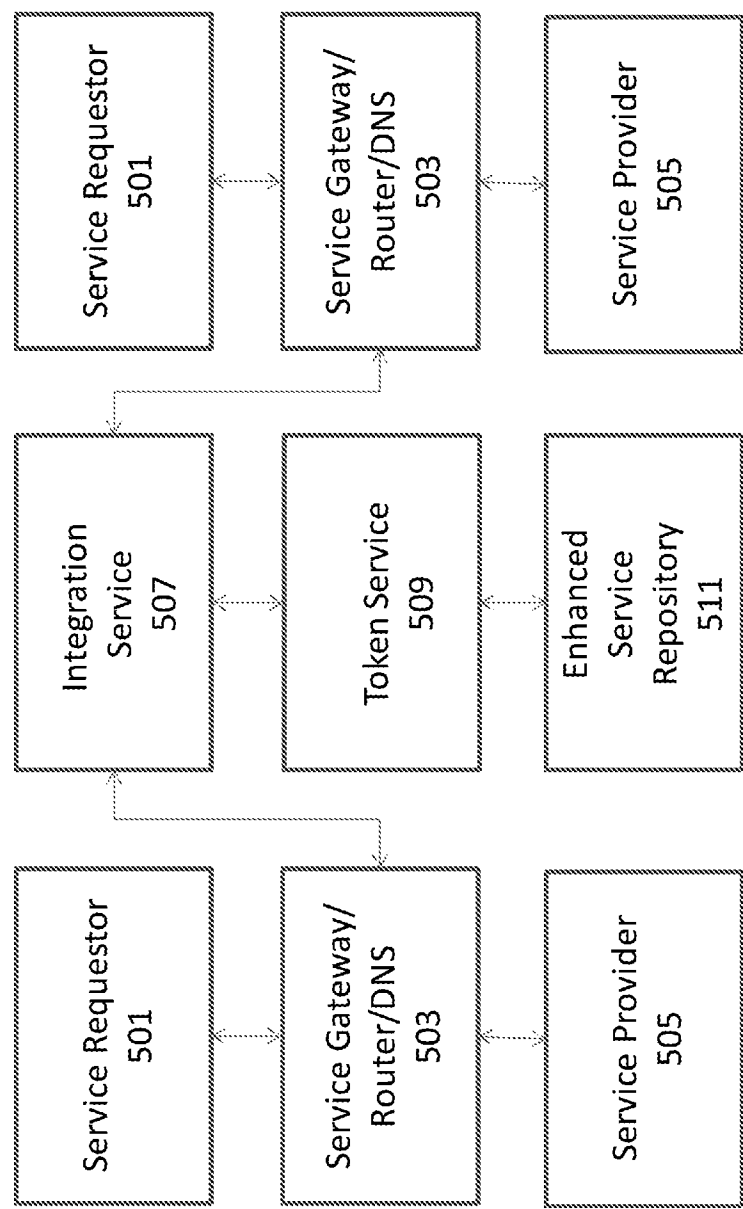


FIG. 5a

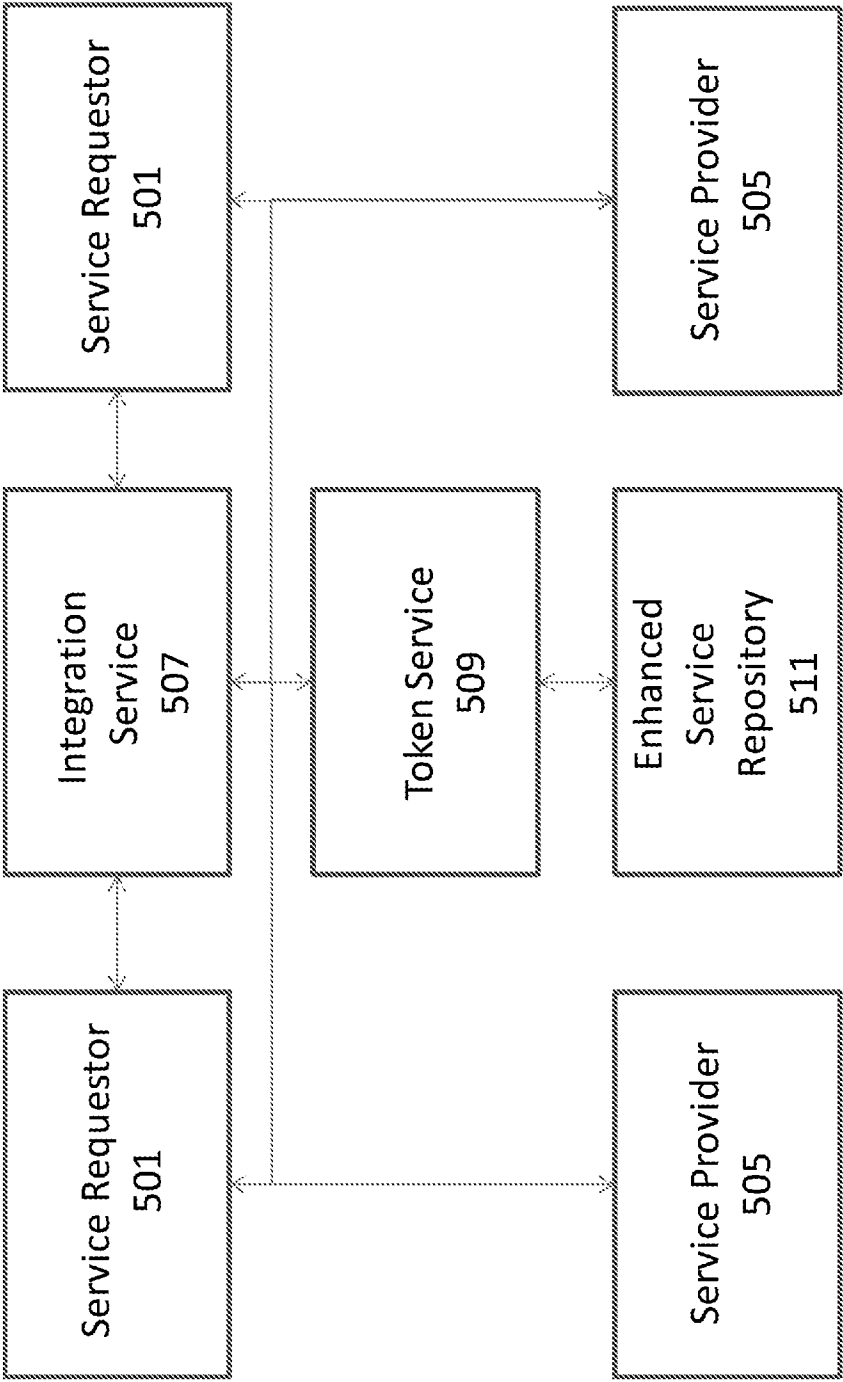


FIG. 5b

End-to-end Token (601)	Service Token (609)	Trace Token (635)
Original Requestor ID (603)	Requestor Application ID (611)	Requestor Application ID (637)
Requestor Channel Code (605)	Provider Segment (613)	Concrete Service Name (639)
Gateway Segment (607)	Abstract Service Name (615)	Concrete Operation Name (641)
	Abstract Operation Name (617)	List of apps and timestamps Along the transaction path (643)
	Rules Table (619)	
	End-point (URL/Queue) (621)	
	Concrete Service Name (623)	
	Concrete Operation Name (625)	
	Time to live (seconds) (627)	
	Refresh time (seconds) (629)	
	Usage Limit (invocations) (631)	
	Timeout (milliseconds) (633)	

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/046749

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 15/173 (2013.01)

USPC - 709/226

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(8) - G06F 15/173, G06F 17/30, G06F 15/16, H04L 9/00 (2013.01)

USPC - 709/226, 726/8, 709/229, 713/155

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC - H04L 29/00, G06F 9/06, H04L 12/00, H04L 12/66, H04L 29/08648, H04L 63/08, H04L 63/101, G06F 21/41, H04L 63/0209, H04L 63/0815, H04N 7/165, H04N 21/2543, H04L 63/20, H04L 29/06462, H04L 63/0428, H04N 21/47202, H04L 29/08576 (2013.01)

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

Orbit, Google Patents, Google Scholar, Google.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2006/0041669 A1 (BEMMEL et al) 23 February 2006 (23.02.2006), entire document	1-20
Y	US 2006/0282660 A1 (VARGHESE et al) 14 December 2006 (14.12.2006), entire document	1-20
Y	WO 2012/073027 A2 (HUNTER) 07 June 2012 (07.06.2012), entire document This document can be viewed by entering the doc number at the following url: http://worldwide.espacenet.com/numberSearch?locale=en_EP	4, 15
Y	US 2011/0264865 A1 (MOBARAK et al) 27 October 2011 (27.10.2011), entire document	5
A	US 2006/0123472 A1 (SCHMIDT et al) 08 June 2006 (08.06.2006), entire document	1-20
A	US 2012/0110199 A1 (MAO et al) 03 May 2012 (03.05.2012), entire document	1-20
A	US 2001/0011250 A1 (PALTENGHE et al) 02 August 2001 (02.08.2001), entire document	1-20
A	US 2011/0231921 A1 (NARAYANAN et al) 22 September 2011 (22.09.2011), entire document	1-20

☐ Further documents are listed in the continuation of Box C.

* 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 application or patent 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

02 August 2013

Date of mailing of the international search report

28 AUG 2013

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents

P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Blaine R. Copenheaver

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774