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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 November 2017 (30.11.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/204996 A1

(51) International Patent Classification:
H04L 9/30 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/US2017/030121

(22) International Filing Date:
28 April 2017 (28.04.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/165,907 26 May 2016 (26.05.2016) US

(71) Applicant: **PEPSICO, INC.** [US/US]; 700 Anderson Hill Road, Purchase, New York 10577 (US).

(72) Inventor: **GONG, George Xu**; c/o PEPSICO, INC., 700 Anderson Hill Road, Purchase, New York 10577 (US).

(74) Agent: **RYGIEL, Mark W.** et al.; STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C, 1100 New York Avenue, NW, Washington, District of Columbia 20005 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, SA, 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.

(54) Title: SECURE GATEWAYS FOR CONNECTED DISPENSING MACHINES

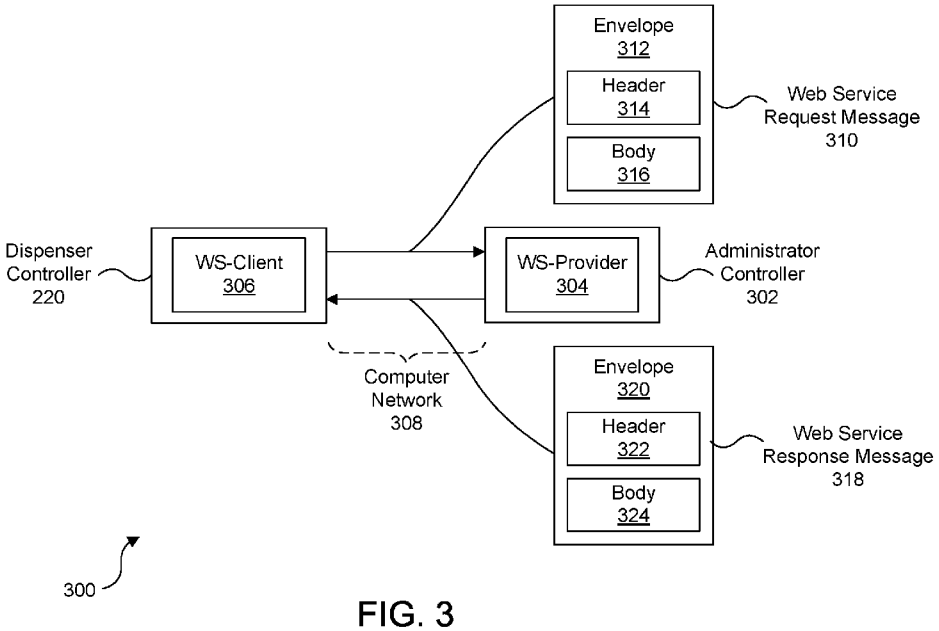

FIG. 3

(57) Abstract: The present disclosure is directed to systems and methods for securely providing telemetry data of a dispenser machine to an administrator system via an exposed web service over a computer network. To secure the exposed web service, the systems and methods of the present disclosure provide secure gateways at the dispenser machine and the administrator system that can provide one or more of message integrity, authentication, authorization, and confidentiality. The secure gateways are implemented separate from the applications creating web service request and response messages at the dispenser machine and the administrator system, respectively. Because the secure gateways are implemented separate from the applications creating the web service request and response messages, the applications creating the web service request and response messages can be created and modified without consideration to message security, which is handled transparently by the secure gateways.

WO 2017/204996 A1

[Continued on next page]

(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, ST, 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).

Published:

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

SECURE GATEWAYS FOR CONNECTED DISPENSING MACHINES

TECHINCAL FIELD

[0001] The described embodiments generally relate to connected machines, including connected dispensing machines.

BACKGROUND

[0002] Beverage dispensers are used to dispense beverages to customers at various locations, such as restaurants, cafeterias, theatres, and other entertainment and/or food service venues. Traditional beverage dispensers provide a limited number of beverage types the can be dispensed (e.g., between six and ten) and offer no advanced features. Newer beverage dispensers can provide a substantially larger number of beverage types and combinations due in large part to the fact that these dispensers are no longer mechanically confined to providing one or two beverage types per dispensing head. For example, newer beverage dispensers can use a single dispensing head to provide up to 1000 different beverage types and combinations.

[0003] A combination refers to a mixture of offered beverage types that can be automatically mixed and dispensed from a single dispensing head and represents one advanced feature offered by newer beverage dispensers. A dispensed combination can be, for example, a personal combination of offered beverage types selected by a customer at the beverage dispenser or one of a number of predefined combinations available to a customer to choose from at the beverage dispenser.

[0004] With increased sophistication in terms of the number of beverage choices available and other innovative features, it can be desirable for venue owners and/or operators to connect advanced beverage dispensers to an administrator system over a computer network to allow the advanced beverage dispensers to provide telemetry data to the administrator system. Telemetry data can include, for example, data collected at the advanced beverage dispensers related to consumption (e.g., amount of each beverage type and combination consumed at the advanced beverage dispensers) and status (e.g., current amount of ingredients and/or supplies at the advanced beverage dispensers). The administrator system can use the telemetry data to improve, for example, the operation,

maintenance, and/or overall logistics associated with running the advanced beverage dispensers.

[0005] In addition, it can be further desirable to connect other types of dispenser machines, such as those that dispense canned/bottled beverages, snacks, and/or other items, to an administrator system over a computer network for the same reasons. These dispenser machines are often referred to as vending machines.

BRIEF DESCRIPTION OF THE DRAWINGS/FIGURES

[0006] The accompanying drawings, which are incorporated herein and form a part of the specification, illustrate the present disclosure and, together with the description, further serve to explain the principles of the disclosure and to enable a person skilled in the pertinent art to make and use the disclosure.

[0007] FIG. 1 is a front perspective view of a beverage dispenser according to an embodiment of the present disclosure.

[0008] FIG. 2 is a block diagram of a beverage dispenser according to an embodiment of the present disclosure.

[0009] FIG. 3 is a system for providing telemetry data over a computer network according to an embodiment of the present disclosure.

[0010] FIG. 4 is a system for securely providing telemetry data over a computer network according to an embodiment of the present disclosure.

[0011] FIG. 5 is a flowchart of a method for collecting and securely transmitting a web service request message containing telemetry data to an administrator controller over a computer network according to an embodiment of the present disclosure.

[0012] FIG. 6 is a flowchart of a method for generating and transmitting a heartbeat message to an administrator controller over a computer network according to an embodiment of the present disclosure.

[0013] FIG. 7 is a flowchart of a method for securely receiving and processing a web service message containing telemetry data from a dispenser controller according to an embodiment of the present disclosure.

[0014] FIG. 8 illustrates an administrator controller for parallel and scalable processing of messages containing telemetry data according to an embodiment of present disclosure.

[0015] FIG. 9 illustrates a flowchart of a method for receiving and processing web service messages from dispenser machines according to an embodiment of the present disclosure.

[0016] FIG. 10 is a block diagram of an example computer system that can be used to implement aspects of the present disclosure.

[0017] The present disclosure will be described with reference to the accompanying drawings. The drawing in which an element first appears is typically indicated by the leftmost digit(s) in the corresponding reference number.

DETAILED DESCRIPTION

[0018] The present disclosure will now be described in detail with reference to embodiments thereof as illustrated in the accompanying drawings. References to "one embodiment", "an embodiment", "an exemplary embodiment", etc., indicate that the embodiment described can include a particular feature, structure, or characteristic, but every embodiment can not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to affect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

1. Overview

[0019] To allow a dispenser machine to provide telemetry data to an administrator system over a computer network, the administrator system can expose a web service to the dispenser machine. A web service is a messaging framework that is capable of exchanging messages over a computer network between a client and a server using internet technologies, such as Hypertext Transfer Protocol (HTTP), Extensible Markup Language (XML), and JavaScript Object Notation (JSON). In general, two types of messages are exchanged: request messages and response messages. The client sends a request message over the computer network to the server exposing the web service. The request message encodes arguments and a request to perform an operation (or run a subroutine) at the server with the arguments. After performing the operation with the

arguments, the host can return a response message over the computer network to the client with the result of the operation.

[0020] Web services have a layered architecture and typically include, from lowest to highest, at least a network layer, a transport layer, and a packaging layer. The network layer specifies the most basic communication needs of the web service, such as how data should be addressed, transmitted, and routed over the computer network. The transport layer is responsible for enabling application-to-application communication on top of the network layer and includes, for example, technologies such as HTTP. The packaging layer specifies the format data is to be packaged in before being transmitted over the network by the transport layer. Simple Object Access Protocol (SOAP) and REpresentational State Transfer (REST) are two of the most common packaging formats. SOAP defines an XML-based envelope for constructing the request and response messages described above. REST can use a wide variety of machine readable formats as an envelope for constructing the request and response messages, including XML and JSON.

[0021] The layers of the web-service architecture do not specifically address security concerns, such as message integrity, authentication, authorization, and confidentiality. Consequently, exposing a web service that offers a dispenser machine access to an administrator system over a computer network may undesirably offer other, non-authorized users and devices of the computer network access to the administrator system and the web service messages.

[0022] The present disclosure is directed to systems and methods for securely providing telemetry data of a dispenser machine to an administrator system via an exposed web service over a computer network. To secure the exposed web service, the systems and methods of the present disclosure provide secure gateways at the dispenser machine and the administrator system that can provide one or more of message integrity, authentication, authorization, and confidentiality. The secure gateways are implemented separate from the applications creating the request and response messages at the dispenser machine and the administrator system, respectively. Because the secure gateways are implemented separate from the applications creating the request and response messages, the applications creating the request and response messages can be created and modified without consideration to message security, which can be handled transparently by the secure gateways.

[0023] The present disclosure is further directed to systems and methods for parallel and scalable processing of web service messages containing telemetry data at an administrator system. The administrator system can receive a large number of web service messages containing telemetry data from many dispenser machines in a short amount of time. To receive and process those web service messages, the systems and methods of the present disclosure provide a message queuer to queue the web service messages (or at least the telemetry data in the web service messages) in a plurality of queues and a different thread or process ("thread") for each of the plurality of queues. Each thread can pull web service messages out of its assigned queue in the order they are stored within the assigned queue and process the telemetry data of the web service messages. The threads can run on one or more central processing unit (CPU) cores at the administrator system. This setup allows for horizontal scaling in terms of web service message processing throughput. For example, to increase web service message processing throughput, the number of CPU cores can be increased and/or the number of queues (and, correspondingly, number of threads assigned to the queues) can be increased.

[0024] The systems and methods for parallel and scalable processing of web service messages containing telemetry data at the administrator system can further ensure that the web service messages are processed in the order in which they are generated at their respective dispenser machines. This may be useful, for example, to ensure decisions related to the maintenance and operation of the dispenser machines are not being made based on old telemetry data.

[0025] To provide such ordered web service message processing functionality, the message queuer can place a web service message containing telemetry data into one of the plurality of queues based on the dispenser machine from which the web service message was received. For example, the message queuer can use a dispenser machine identifier included in the web service message to map the web service message to a particular one of the plurality of queues such that web service messages from the dispenser machine are placed in the same queue. In addition, once the message queuer has determined a particular one of the plurality of queues in which to place a web service message, the message queuer can insert the web service message into a particular position of the queue based on when the web service message was generated at the dispenser machine. For example, the message queuer can use a web service message sequence number or time stamp included in the web service message to insert the web service

message at a particular position in the queue such that the web service messages in the queue are stored in the order in which the web service messages were generated.

[0026] Before further describing these and other features of the present disclosure, an exemplary operating environment in which embodiments of the present disclosure can operate is provided in the following section.

2. Exemplary Operating Environment

[0027] FIG. 1 shows a dispenser 100 in which embodiments of the present disclosure can be implemented. Dispenser 100 can include a base 102 coupled to a body 108. Base 102 can serve to support body 108 in an upright position. Base 102 can include a drip tray 104 with a dispense location 106 located within the area occupied by drip tray 104. A user (e.g., a customer) can place his or her cup at dispense location 106 to receive his or her desired beverage.

[0028] Body 108 can include a user interface 110 for receiving commands from a user. User interface 110 can include a display screen 112 configured to display information to a user and/or receive commands from a user. Display screen 112 can be a touch screen, such as a liquid crystal display (LCD) touchscreen or a light emitting diode (LED) touchscreen. A user can initiate the dispensing of a beverage, e.g., by interacting with user interface 110 to make a selection of his or her desired beverage to be dispensed by dispenser 100.

[0029] FIG. 2 shows a block diagram 200 of components of a dispenser, such as dispenser 100 in FIG. 1, according to embodiments of the present disclosure. Block diagram 200 can include a dispensing manifold 210, such as one of the vertical dispensing manifolds described in U.S. Patent Application No. 15/016,466, filed February 5, 2016, which is incorporated herein by reference in its entirety.

[0030] Block diagram 200 can include one or more base liquid sources 230. Base liquid sources 230 can be, but are not limited to, a tap water source (e.g., tap water line) and a carbonated water source (e.g., carbonated water reservoir or carbonator). Base liquid sources 230 can be coupled to dispensing manifold 210 via base liquid delivery tubes 234. Valves/pumps 235 in communication with base liquid delivery tubes 234 can be configured to control the flow of base liquid through base liquid delivery tubes 234 and into dispensing manifold 210.

[0031] Block diagram 200 can include one or more ingredient sources 240. Ingredient sources 240 can include a plurality of ingredients 242 (242-1 through 242-n). Ingredients 242 can include liquid ingredients, such as but not limited to, sweeteners (e.g., sugars or artificial sweeteners), syrups, or flavorings (e.g., cola syrups or flavorings, brand soda syrups or flavoring (e.g., Mountain Dew® or Sierra Mist®), orange flavoring, lime flavoring, cherry flavoring, tea flavorings, etc.), or other liquid additives (e.g., vitamins, acids (e.g., citric acid), salts, or colorings). Ingredients 242 can be packaged within a container, such as but not limited to a cartridge or bag. Each ingredient 242 can be delivered to dispenser 210 via ingredient delivery tubes 244. Valves/pumps 245 in communication with ingredient delivery tubes 244 can be configured to control the flow of ingredients through ingredient tubes 244 and into dispensing manifold 210.

[0032] A dispenser controller 220 can be configured to control and receive commands from a user interface, such as user interface 110 in FIG. 1. Dispenser controller 220 can be configured to control operations of the dispenser represented by block diagram 200 based on, for example, commands received from the user interface. For example, dispenser controller 220 can control the dispensing of a beverage type or combination, both of which can be a mixture of a base liquid and one more ingredients 242 from dispensing manifold 210. Dispenser controller 220 can control the flow of a base liquid from base liquid sources 230 by controlling valve/pumps 235. Dispenser controller 220 can also control the flow of ingredients 242 from ingredient sources 240 by controlling valves/pumps 245. By controlling valves/pumps 245, dispenser controller 220 can control the pressure of an ingredient 242 within ingredient tubes 244.

[0033] In some embodiments, dispenser controller 220 can include and/or can be configured to read sensors 227. Sensors 227 can include pressure sensors for monitoring the pressure of a base liquid within a base liquid delivery tube 234 and/or for monitoring the pressure of an ingredient within an ingredient delivery tube 244. Sensors 227 can also include flow sensors (e.g., flow meters) for measuring the flow of base liquids and ingredients within delivery tubes 234 and 244, respectively, and/or for measuring the degree of uniform flow within dispensing manifold 210. In some embodiments, sensors 227 can include level sensors for measuring the amount of each ingredient 242 remaining within an ingredient source 240.

[0034] Sensors 227 can also include, but are not limited to sensors configured to monitor (1) carbon dioxide tank levels (e.g., one, two, or more carbon dioxide regulators); (2)

carbonization head pressure of a carbonator configured to carbonate water; (3) ambient temperature of a room (e.g., a backroom) in which base liquids and/or ingredients 242 are stored (thereby monitoring whether one or more base liquids and/or ingredients 242 are maintained at pre-determined temperature level or within a pre-determined temperature range); (4) water filtration system parameters (e.g., water pressure, differential pressure on filters) associated with the base liquids; (5) pH of water or carbonated water associated with the base liquids; (6) the expiration date of an ingredient container (e.g., by reading a bar code associated within an ingredient container) in which one of ingredients 242 is contained. Sensors 227 can be configured to transmit signals over a wired or wireless network to dispenser controller 220. Dispenser controller 220 can be configured to control the operations of the dispenser represented by block diagram 200 based on data (e.g., pressure and flow values) collected by sensors 227.

[0035] In some embodiments, dispenser controller 220 can further include an embedded computer 224. In some embodiments, embedded computer 224 can collect dispenser telemetry data including: (1) amounts of beverage types and combinations dispensed by dispensing manifold 210, (2) amounts of ingredients 242 remaining in ingredient sources 240, (3) user identification codes collected from a user interface of the dispenser machine, and (4) other data from sensors 227 mentioned above (e.g., flow data, ambient temperature of room where base liquids and/or ingredients 242 are stored, carbon dioxide tank levels, carbonization head pressure, water filtration system parameters, etc.). In some embodiments, embedded computer 224 can store the dispenser telemetry data and send the dispenser telemetry data to a controller of an administrator system over a computer network, such as the internet. The administration controller can be provided and/or managed by the operator of the dispenser represented by block diagram 200 or some other entity associated with the operation of the dispenser represented by block diagram 200.

[0036] In some embodiments, all or part of the stored telemetry data (e.g., the information related to the amounts of beverage types and combinations dispensed by dispensing manifold 210) can be periodically sent to the administrator controller. In some embodiments, all or part of the stored telemetry data (e.g., the other data from sensors 227 mentioned above) can be sent to the administrator controller based on alert levels or threshold levels associated with the stored telemetry data. For example, the stored telemetry data related to the ambient temperature of the room where the base liquids and/or ingredients 242 are stored can be sent to the administration controller when the

ambient temperature of the room passes a certain predetermined threshold that is outside or nearly outside an acceptable temperature range. In another example, the stored telemetry data related to the carbon dioxide tank levels can be sent to the administrator controller when the carbon dioxide tank levels pass a certain predetermined threshold indicating that the carbon dioxide tank levels are low or empty.

[0037] In some embodiments, the administrator controller can use the telemetry data to aid in the distribution of ingredients to the dispenser represented by block diagram 200 and/or in the maintenance of the dispenser represented by block diagram 200. In some embodiments, the administrator controller can use the telemetry data to track user preferences and consumption data (e.g., types and amounts of beverages dispensed by manifold 210), which can be analyzed to predict consumer trends and/or to support future business decisions as they relate to the dispenser represented by block diagram 200. In other embodiments, the administrator controller can use the telemetry data to improve the dispenser machine maintenance task, customer satisfaction, and/or predict parts failure in the dispenser machine and/or schedule preventative maintenance services of the dispenser machine.

3. Secure Gateways

[0038] To enable a dispenser machine to provide telemetry data to a controller of an administrator system over a computer network, the administrator controller can expose a web service to the dispenser machine. As discussed above, a web service is a messaging framework that is capable of exchanging messages over a computer network between a client and a server using internet technologies, such as Hypertext Transfer Protocol (HTTP), Extensible Markup Language (XML), and JavaScript Object Notation (JSON). In general, two types of messages are exchanged: request messages and response messages. The client sends a request message over the computer network to the server exposing the web service. The request message encodes arguments and a request to perform an operation (or run a subroutine) at the server with the arguments. After performing the operation with the arguments, the host can return a response message over the computer network to the client with the result of the operation.

[0039] FIG. 3 illustrates a system 300 for providing telemetry data over a computer network using an exposed web service according to an embodiment of the present disclosure. System 300 includes an administrator controller 302 and dispenser controller

220, which was described above in regard to FIG. 2. Dispenser controller 220 is provided by way of example and not limitation. Other dispenser controllers (e.g., dispenser controllers implemented in different dispenser machines) can be used in system 300 without departing from the scope and spirit of the present disclosure as would be appreciated by one of ordinary skill in the art.

[0040] In operation, a web service provider (WS-provider) 304 of administrator controller 302 exposes the web service that enables a web service client (WS-client) 306 of dispenser controller 220 to provide telemetry data to administrator controller 302 over a computer network 308, such as the internet. The telemetry data can include data collected from sensors 227, as described above in regard to FIG. 2, and other data collected from other sensors and/or peripherals of the dispenser machine in which dispenser controller 220 is implemented.

[0041] WS-client 306 can package the telemetry data in a web-service request message 310 that is formatted in accordance with Simple Object Access Protocol (SOAP), REpresentational State Transfer (REST), or some other packaging format. Web service request message 310 can include an envelope 312 containing an optional header 314 and a body 316. Header 314, when used, can include one or more blocks of information that specify how the message is to be processed by one or more receiving entities. Body 316 can include the telemetry data as one or more arguments and a request to perform an operation (or run a subroutine) at WS-provider 304 with the one or more arguments. The telemetry data and request to perform the operation can be expressed within body 316 in an XML or JSON syntax. The request to perform the operation can also be expressed outside body 316 in any number of forms, including as a uniform resource identifier (URI).

[0042] After WS-client 306 packages the telemetry data and request to perform the operation in web service request message 310, WS-client 306 can transmit web service request message 310 over computer network 308. In one embodiment, WS-client 306 transmits web service request message 310 over computer network 308 using HTTP or HTTP secure (HTTPS).

[0043] WS-provider 304 receives web-service request message 310 from WS-client 306 over computer network 308 and unpacks web service request message 310 to recover the one or more arguments that comprise the telemetry data and the request to perform the operation with the one or more arguments. WS-provider 304 subsequently performs the

operation with the one or more arguments that comprise the telemetry data and, optionally, packages the result of the operation into a web service response message 318. The operation can include, for example, parsing the telemetry data and populating a database with the various values of the telemetry data. The data in the database can subsequently be used to aid in the distribution of ingredients to the dispenser machine and/or in the maintenance of the dispenser machine. In some embodiments, the data in the database can be used to track user preferences and consumption data (e.g., types and amounts of beverages dispensed by the dispenser machine), which can be analyzed to predict consumer trends and/or to support future business decisions as they relate to the dispenser machine. In other embodiments, the data in the database can be used to improve the dispenser machine maintenance task, customer satisfaction, and/or predict parts failure in the dispenser machine and/or schedule preventative maintenance services of the dispenser machine.

[0044] Similar to web service request message 310, WS-provider 304 can format web service response message 318 in accordance with SOAP, REST, or some other packaging format. Web service response message 318 can include an envelope 320 containing an optional header 322 and a body 324. Header 322, when used, can include one or more blocks of information that specify how the message is to be processed by one or more receiving entities. Body 324 can include the result of the operation. The result of the operation can be expressed within body 324 in an XML or JSON syntax.

[0045] After WS-provider 304 packages the result of the operation in web service response message 318, WS-provider 304 can transmit web service response message 318 over computer network 308. In one embodiment, WS-provider 304 transmits web service response message 318 over computer network 308 using HTTP or HTTPS.

[0046] It should be noted that multiple dispensers and dispenser controllers, other than dispenser controller 220, can transmit web service request messages to administrator controller 302. These web service request messages can be processed similar to web service request message 310 as described above but may include different data (e.g., other than telemetry data) and/or requests to perform different operations or subroutines.

[0047] One problem with the web service exposed by WS-provider 304 and web services in general is that the layered architecture of web services does not specifically address security concerns, such as message integrity, authentication, authorization, and confidentiality. Consequently, exposing a web service that offers dispenser controller 220

and other dispenser controllers access to administrator controller 302 over computer network 308 may undesirably offer other, non-authorized users and devices of computer network 308 access to administrator controller 302 and the web service request and response messages 310 and 318.

[0048] To secure the exposed web service, secure gateways can be provided at dispenser controller 220 and administrator controller 302 that can provide one or more of message integrity, authentication, authorization, and confidentiality. The secure gateways can be implemented separate from the applications creating the request and response messages at dispenser controller 220 and administrator controller 302, respectively; i.e., separate from WS-client 306 and WS-provider 304. Because the secure gateways are implemented separate from WS-client 306 and WS-provider 304, these applications can be created and modified without consideration to message security, which can be handled transparently by the secure gateways.

[0049] FIG. 4 illustrates such a system 400 according to an embodiment of the present disclosure. In particular, system 400 has the same basic configuration and operates in the same basic manner as system 300 in FIG. 3 described above. However, dispenser controller 220 and administrator controller 302 in system 400 of FIG. 4 each further include a secure gateway. More specifically, dispenser controller 220 further includes a dispenser web service gateway (dispenser WS-gateway) 402 and administrator controller 302 further includes an administrator web service gateway (administrator WS-gateway) 404.

[0050] In operation, dispenser WS-gateway 402 is configured to intercept web service request message 310 generated by dispenser WS-client 306 before web service request message 310 is transmitted over computer network 308 to administrator controller 302. In one embodiment, WS-gateway 402 is implemented as an HTTP proxy server configured to intercept an HTTP request message containing web service request message 310 in the body of the HTTP request message.

[0051] Once dispenser WS-gateway 402 has intercepted web service request message 310, dispenser WS-gateway 402 can encrypt all, or at least a portion of, the telemetry data (or other data) in body 316 of web service request message 310 to generate a digital signature. Dispenser WS-gateway 402 can insert the digital signature into header 314 of web service request message 316. Administrator controller 302 can use the digital signature to authenticate the telemetry data (or at least the portion of the telemetry data

and/or other data that was signed); i.e., prove that the telemetry data came from dispenser controller 220.

[0052] In one embodiment, dispenser WS-gateway 402 can encrypt all, or at least a portion of, the telemetry data (or other data) in body 316 of web service request message 316 using a private key associated with dispenser controller 220. The private key associated with dispenser controller 220 is part of an asymmetric key pair that includes the private key and a public key. The public key can be made public or kept secret by administrator controller 302, whereas the private key is kept secret by dispenser controller 220 and not distributed. Administrator controller 302 can use the public key associated with dispenser controller 220 to verify (e.g., through decryption) the digital signature. If the verification is successful, administrator controller 302 can be sure that the private key associated with dispenser controller 220 was used to encrypt the telemetry data used to generate the digital signature because data encrypted with the private key can only be decrypted with the public key.

[0053] In another embodiment, rather than encrypt the telemetry data directly, dispenser WS-gateway 402 can encrypt a message digest that results from a one way hash of the telemetry data using the private key associated with dispenser controller 220. The one way hash can be used to ensure the integrity of the telemetry data and/or reduce processing time required to generate the digital signature.

[0054] Once dispenser WS-gateway 402 has intercepted web service request message 306, dispenser WS-gateway 402 can further encrypt all, or at least a portion of, the telemetry data (or other data) in body 316 of web service request message 310 to ensure confidentiality of the telemetry data as it traverses computer network 308. After encrypting the telemetry data, dispenser WS-gateway 402 can re-insert the encrypted telemetry data into body 316 of web service request message 316.

[0055] In one embodiment, dispenser WS-gateway 402 can encrypt all, or at least a portion of, the telemetry data (or other data) in body 316 of web service request message 316 using a public key associated with administrator controller 302. Like the public key associated with dispenser controller 220, the public key associated with administrator controller 302 is part of an asymmetric key pair that includes the public key and a private key. The public key is made public and distributed freely, whereas the private key is kept secret by administrator controller 302 and not distributed.

[0056] In another embodiment, dispenser WS-gateway 402 can encrypt all, or at least a portion of, the telemetry data (or other data) in body 316 of web service request message 316 using a symmetric key. Dispenser WS-gateway 402 can encrypt the symmetric key with the public key associated with administrator controller 302 and insert the symmetric key in header 314 or body 316 of web service request message 310.

[0057] After dispenser WS-gateway 402 has inserted the digital signature and/or encrypted the telemetry data in body 316, dispenser WS-gateway 402 can transmit web service request message 310 over computer network 308 using, for example, HTTP or HTTPS. Administrator WS-gateway 404 is configured to receive web service request message 310 over computer network 308 and perform one or more of decrypting the telemetry data, authenticating the telemetry data, and determining whether dispenser controller 220 is authorized to perform the requested operation (or requested subroutine) in web service request message 310.

[0058] If the telemetry data (or other data) in body 316 of web service request message 310 was encrypted with the public key associated with administrator controller 302, administrator WS-gateway 404 can decrypt the encrypted telemetry data using the private key associated with administrator controller 302. If the telemetry data (or other data) in body 316 of web service request message 310 was encrypted with a symmetric key as described above, administrator WS-gateway 404 can obtain an encrypted copy of the symmetric key from header 314 or body 316 of web service request message 310, decrypt the symmetric key using the private key associated with administrator controller 302, and then use the decrypted symmetric key to decrypt the encrypted telemetry data. Once decrypted, administrator WS-gateway 404 can replace the encrypted telemetry data in web service request message 310 with the decrypted telemetry data.

[0059] If authentication is to be performed, administrator WS-gateway 404 can extract the digital signature in header 314 of web service request message 310 and decrypt the digital signature using the public key associated with dispenser controller 220. The telemetry data (or other data) that was signed to create the digital signature can then be compared to the telemetry data in body 316 of web service request message 310 to authenticate that the telemetry data came from dispenser controller 220. In the instance where dispenser WS-gateway 402 created the digital signature from a one way hash of the telemetry data (or other data) in body 316 of web service request message 310, administrator WS-gateway 404 can perform the same one way hash of the telemetry data

in body 316 before comparing the telemetry data in body 316 to the decrypted digital signature.

[0060] If authorization is to be performed, administrator WS-gateway 404 can determine whether dispenser controller 220 is authorized to use the web service subroutine requested in web service request message 310. In one embodiment, administrator WS-gateway 404 can check a list of dispenser controllers and/or dispensers that are authorized to perform the requested operation in web service request message 310. If dispenser controller 220 or the dispenser in which dispenser controller 220 is implemented is on the list, administrator WS-gateway 404 can pass web service request message 310 to administrator WS-provider 304 for processing. On the other hand, if dispenser controller 220 or the dispenser in which dispenser controller 220 is implemented is not on the list, administrator WS-gateway 404 can discard web service request message 310, preventing web service request message 310 from being processed by administrator WS-provider 304.

[0061] In another embodiment, if authorization is to be performed, administrator WS-gateway 404 can determine whether a web service is published based on a configurable list of published web services. If not, the web service call of the non-published web service by a dispenser machine can be rejected and discarded. This mechanism protects any non-published web service and can be used to take a web service out of service at any time for whatever reason.

[0062] After receiving the web service request message 310 from administrator WS-gateway 404 (with any encrypted telemetry data in body 316 replaced with decrypted telemetry data), administrator controller 302 can process the web service request message 310 as described above in regard to FIG. 3. It should be noted that administrator WS-gateway 404 and dispenser WS-gateway 402 can each perform the functionality of the other gateway as described above to secure web service response message 318 similar to web service request message 310.

[0063] In one embodiment, not all web service request messages sent by dispenser controller 220 need to be signed and/or encrypted by dispenser WS-gateway 402. Such messages that are not signed and/or encrypted by dispenser WS-gateway 402 can be said to be sent "out-of-band," whereas messages that are signed and/or encrypted can be said to be sent "in-band".

[0064] For example, "heartbeat" messages can be generated by either dispenser WS-client 306 or dispenser WS-gateway 402 and sent to administrator controller 302 over computer network 308 out-of-band by dispenser WS-gateway 402. These heartbeat messages can be sent periodically or on a recurring basis to signal to administrator controller 302 that dispenser controller 220 (or the dispenser in which dispenser controller 220 is implemented) exists and is available.

[0065] Referring now to FIG. 5, a flowchart 500 of a method for collecting telemetry data and securely transmitting a web service request message containing the telemetry data from a dispenser machine to an administrator controller over a computer network according to an embodiment of the present disclosure is illustrated. The method of flowchart 500 can be implemented by dispenser WS-client 306 and dispenser WS-gateway 402 as described above and illustrated in FIG. 4. However, it should be noted that the method can be implemented by other dispenser WS-clients and dispenser WS-gateways as well. The steps of flowchart 500 performed by each of these applications are labeled in FIG. 5. It should be further noted that some of the steps of flowchart 500 do not have to occur in the order shown in FIG. 5.

[0066] The method of flowchart 500 begins at step 502. At step 502, telemetry data of the dispenser machine is collected. Telemetry data can include, for example, data collected at the dispenser machine related to consumption (e.g., amount of each item consumed at the dispenser machine) and status (e.g., current amount of ingredients, supplies, and/or items at the dispenser machine). The telemetry data can also include the specific types of data mentioned above with respect to FIG. 2.

[0067] After collecting the telemetry data at step 502, the method of flowchart 500 proceeds to step 504. At step 504, a web service request message is sent to the administrator controller, such as administrator controller 302 in FIG. 4, with the telemetry data and a request to perform an operation (or run a subroutine) with the telemetry data as an argument. The web service request message can be packaged in accordance with SOAP, REST, or some other packaging format. The web service request message can include an envelope containing an optional header and a body. The header, when used can include one or more blocks of information that specify how the message is to be processed by one or more receiving entities. The telemetry and the request to perform the operation can be expressed within the body in an XML or JSON syntax. The request to perform the operation can also be expressed outside the body.

[0068] After step 504, the method of flowchart 500 proceeds to step 506. At step 506, the web service request message is intercepted before being sent to the administrator controller over a computer network, such as the internet. An HTTP proxy can be used to intercept the web service request message.

[0069] After step 506, the method of flowchart 500 proceeds to step 508. At step 508, the telemetry data in the intercepted web service request message is optionally signed by encrypting the telemetry data or encrypting a one way hash of the telemetry data. The telemetry data or the one way hash of the telemetry data can be signed using a private key associated with the dispenser machine. The resulting digital signature can be inserted into a header of the web service request message.

[0070] After step 508, the method of flowchart 500 proceeds to step 510. At step 510, the telemetry data in the body of the web service request message is optionally encrypted. The telemetry data can be encrypted using a public key associated with the administrator controller or a symmetric key. If the symmetric key is used to encrypt the telemetry data, the symmetric key can be encrypted using the public key associated with the administrator controller and inserted in the header or body of the web service request message to enable the administrator controller to decrypt the encrypted telemetry data.

[0071] After step 510, the method of flowchart 500 proceeds to step 512. At step 512, the web service request message is transmitted to the administrator controller over the computer network. The web service request message can be transmitted over the computer network using HTTP or HTTPS.

[0072] Referring now to FIG. 6, a flowchart 600 of a method for generating and transmitting a heartbeat message from a dispenser controller to an administrator controller over a computer network according to an embodiment of the present disclosure is illustrated. The method of flowchart 600 can be implemented by dispenser WS-client 306 or dispenser WS-gateway 402 as described above and illustrated in FIG. 4. However, it should be noted that the method can be implemented by other dispenser WS-clients or dispenser WS-gateways as well.

[0073] The method of flowchart 600 begins at step 602. At step 602, a heartbeat message is generated. The heartbeat message can include identifiers, such as hardware identifiers, of the dispenser controller and/or the dispenser machine in which the dispenser controller is implemented.

[0074] After step 602, the method of flowchart 600 proceeds to step 604. At step 604, the heartbeat message is sent "out-of-band" over the computer network, such as the internet, to the administrator controller. Messages that are sent "out-of-band" are not signed and/or encrypted at the application level before being sent. The heartbeat messages can be generated and sent periodically or on a recurring basis to signal to the administrator controller that the dispenser controller (or the dispenser machine in which dispenser controller is implemented) exists and is available.

[0075] Referring now to FIG. 7, a flowchart 700 of a method for securely receiving and processing a web service request message containing telemetry data from a dispenser controller at an administrator controller according to an embodiment of the present disclosure is illustrated. The method of flowchart 700 can be implemented by administrator WS-gateway 404 and administrator WS-provider 304 as described above and illustrated in FIG. 4. However, it should be noted that the method can be implemented by other administrator WS-gateways and administrator WS-providers as well. The steps of flowchart 700 performed by each of these applications are labeled in FIG. 7. It should be further noted that some of the steps of flowchart 700 do not have to occur in the order shown in FIG. 7.

[0076] The method of flowchart 700 begins at step 702. At step 702, a web service request message is received from a dispenser machine over a computer network, such as the internet.

[0077] After step 702, the method of flowchart 700 proceeds to step 704. At step 704, the message is inspected to determine whether the message is a heartbeat message. If the message is a heartbeat message, the method of flowchart 700 proceeds to step 714 and the heartbeat message is processed. If the message is not a heartbeat message, the method of flowchart 700 proceeds to step 706.

[0078] At step 706, encrypted telemetry data in a body of the web service request message is decrypted. The telemetry data can be decrypted using a private key associated with the administrator controller or using a symmetric key included in a header or the body of the web service request message.

[0079] After step 706, the method of flowchart 700 proceeds to step 708. At step 708, the authenticity of the telemetry data is verified. In particular, a digital signature in the header of the web service request message is extracted and decrypted using the public key associated with the dispenser controller. The telemetry data that was signed to create the

digital signature can then be compared to the telemetry data in the body of the web service request message to authenticate that the telemetry data came from the dispenser controller. In the instance where the digital signature was created from a one way hash of the telemetry data in the body of the web service request message, the same one way hash of the telemetry data in the body can be performed before comparing the telemetry data in the body to the decrypted digital signature. If the telemetry data is determined to be not authentic based on the comparison (i.e., no match), the method of flowchart 700 proceeds to step 710 where the web service request message is rejected. On the other hand, if the telemetry data is determined to be authentic based on the comparison (i.e., a match), the method of flowchart 700 proceeds to step 712.

[0080] At step 712, a determination is made as to whether the dispenser controller is authorized to use the web service to perform the operation (or subroutine) in the web service request message. In one embodiment, a list of dispenser controllers and/or dispensers that are authorized to use the web service subroutine requested in the web service request message is checked. If the dispenser controller or the dispenser in which the dispenser controller is implemented is not on the list, the method of flowchart 700 proceeds to step 710 where the web service request message is rejected. On the other hand, if the dispenser controller or the dispenser in which dispenser controller is implemented is on the list, the method of flowchart 700 proceeds to step 714 where the web service request message is processed (e.g., as described above in regard to FIG. 3).

4. Parallel and Scalable Processing of Telemetry Data

[0081] Given that there can be several thousand or even several hundred thousand or more dispenser machines and/or other types of machines connected to an administrator system as described above, and that these machines can all send telemetry data concurrently to the administrator system, there is a further need for the administrator system to be able to receive and quickly process a large number of web service messages. In addition, there is a further need to provide such an administrator system with a throughput that can scale in an efficient manner as machines are connected to or disconnected from the administrator system.

[0082] FIG. 8 illustrates an administrator controller 800 for parallel and scalable processing of messages containing telemetry data according to an embodiment of the present disclosure. Administrator controller 800 has the same basic configuration and

operates in the same basic manner as administrator controller 302 in FIG. 4 described above. However, administrator controller 800 further includes a message queuer 802. It should be noted that administrator WS-gateway 404 is an optional component in administrator controller 800.

[0083] In operation, web service messages containing telemetry data from dispenser machines are first received and processed by administrator WS-gateway 404 as described above. After being processed by administrator WS-gateway 404, the web service messages are passed to message queuer 802.

[0084] Message queuer 802 includes a mapper 804 and a plurality of queues 806. Mapper 804 is configured to map or place each web service message into a respective one of queues 806. Queues 806 are data structures used to store the web service messages in memory.

[0085] To process the web service messages stored in queues 806, administrator WS-provider 304 includes a plurality of threads or processes ("threads") 808. A different one of threads 808 can be assigned to each queue 806. Each thread 808 can pull web service messages out of its assigned queue 806 in the order in which the web service messages are stored within the assigned queue 806 and process the telemetry data of the web service messages.

[0086] The processing of the telemetry data by threads 808 can include, for example, parsing the telemetry data and populating a database with the various values of the telemetry data. The data in the database can subsequently be used to aid in the distribution of materials (e.g., ingredients) to the dispenser machine and/or in the maintenance of the dispenser machine. In some embodiments, the data in the database can be used to track user preferences and consumption data (e.g., types and amounts of beverages dispensed by the dispenser machine), which can be analyzed to predict consumer trends and/or to support future business decisions as they relate to the dispenser machine. In other embodiments, the data in the database can be used to improve the dispenser machine maintenance task, customer satisfaction, and/or predict parts failure in the dispenser machine and/or schedule preventative maintenance services of the dispenser machine.

[0087] Threads 808 can run on central processing unit (CPU) cores 810 or virtual cores at administrator controller 810. Cores 810 can be implemented in or across one or more servers. Based on the number of cores 810, at least some of threads 808 can run in parallel to increase the throughput at which the web service messages are processed. To

further increase message processing throughput, the number of cores 810 can be increased and/or the number of queues 806 (and, correspondingly, number of threads 808 assigned to queues 806) can be increased. Such an increase can be made in response to an increase in the number of dispenser machines transmitting web service messages to administrator controller 800.

[0088] Mapper 804 can further be configured to ensure that the web service messages are processed in the order in which they are generated at their respective dispenser machines. This may be useful, for example, to ensure decisions related to the maintenance and operation of the dispenser machines are not being made based on old telemetry data or non-chronologically sequenced telemetry data.

[0089] To provide such ordered message processing functionality, mapper 804 can place a web service message containing telemetry data into one of queues 806 based on the dispenser machine from which the message was received. For example, mapper 804 can use a dispenser machine identifier included in the web service message to map the web service message to a particular one of queues 806 such that messages from the dispenser machine are placed in the same queue and, therefore, processed by the same thread 808.

[0090] The number of queues 806 and the number of threads 808 is typically much less than the number of dispenser machines sending web service messages to administrator controller 800. In such a scenario, mapper 804 can use a hash function to map the web service message to a particular one of queues 806. More specifically, mapper 804 can use the hash function to hash the dispenser machine identifier included in the web service message and use the resulting hash value to assign the web service message to the particular one of queues 806.

[0091] Once mapper 804 has determined a particular one of queues 806 in which to place a web service message, mapper 804 can insert the web service message into a particular position of the queue based on when the message was generated at the dispenser machine. For example, mapper 804 can use a message sequence number or time stamp included in the web service message to insert the message at a particular position in the queue such that the web service messages in the queue are stored in the order in which the messages were generated.

[0092] Referring now to FIG. 9, a flowchart 900 of a method for receiving and processing web service messages from dispenser machines is illustrated according to an embodiment of the present disclosure. The method of flowchart 900 can be implemented by

administrator controller 800 as described above and illustrated in FIG. 8. However, it should be noted that the method can be implemented by other administrator controllers as well. It should be further noted that some of the steps of flowchart 900 are optional and do not have to occur in the order shown in FIG. 9.

[0093] The method of flowchart 900 begins at step 902. At step 902, a web service message is received from a dispenser machine over a computer network, such as the internet.

[0094] After step 902, the method of flowchart 900 proceeds to step 904. At step 904, a hash of a dispenser machines identifier in the web service message is performed.

[0095] After step 904, the method of flowchart 900 proceeds to step 906. At step 906, one of a plurality of queues is identified based on the resulting hash value of the hash of the dispenser machine identifier. Because the same hash value is produced each time for the same dispenser machine identifier, the web service messages received from the dispenser machine will be placed in the same queue.

[0096] After step 906, the method of flowchart 900 proceeds to step 908. At step 908, the web service message is placed into the identified queue at a position determined based on when the web service message was generated at the dispenser machine. For example, a message sequence number or time stamp included in the web service message can be used to insert the message at a particular position in the queue such that the web service messages in the queue are stored in the order in which the messages were generated at the dispenser machine.

[0097] After step 908, the method of flowchart 900 proceeds to step 910. At step 910, the web service message is processed using one of a plurality of threads assigned to the queue in which the web service message is stored.

5. Example Computer System Implementation

[0098] It will be apparent to persons skilled in the relevant art(s) that various elements and features of the present disclosure, as described herein, can be implemented in hardware using analog and/or digital circuits, in software, through the execution of instructions by one or more general purpose or special-purpose processors, or as a combination of hardware and software.

[0099] The following description of a computer system is provided for the sake of completeness. Embodiments of the present disclosure can be implemented in hardware, or

as a combination of software and hardware. Consequently, embodiments of the disclosure may be implemented in the environment of a computer system or other processing system. An example of such a computer system 1000 is shown in FIG. 10. Blocks depicted in FIGS. 3, 4, and 8 may execute on one or more computer systems 1000. Furthermore, each of the steps of the methods depicted in FIGS. 5-7 and 9 can be implemented on one or more computer systems 1000.

[0100] Computer system 1000 includes one or more processors, such as processor 1004. Processor 1004 can be a special purpose or a general purpose processor. Processor 1004 is connected to a communication infrastructure 1002 (for example, a bus or network). Various software implementations are described in terms of this exemplary computer system. After reading this description, it will become apparent to a person skilled in the relevant art(s) how to implement the disclosure using other computer systems and/or computer architectures.

[0101] Computer system 1000 also includes a main memory 1006 (to store, for example, computer programs or other instructions that implement, at least in part, the blocks depicted in FIGS. 3, 4, and 8 and/or steps in FIGS. 5-7 and 9), preferably random access memory (RAM), and may also include a secondary memory 1008. Secondary memory 1008 may include, for example, a hard disk drive 1010 and/or a removable storage drive 1012, representing a floppy disk drive, a magnetic tape drive, an optical disk drive, or the like. Removable storage drive 1012 reads from and/or writes to a removable storage unit 816 in a well-known manner. Removable storage unit 1016 represents a floppy disk, magnetic tape, optical disk, or the like, which is read by and written to by removable storage drive 1012. As will be appreciated by persons skilled in the relevant art(s), removable storage unit 1016 includes a computer usable storage medium having stored therein computer software and/or data.

[0102] In alternative implementations, secondary memory 1008 may include other similar means for allowing computer programs or other instructions (e.g., computer programs or other instructions that implement, at least in part, the blocks depicted in FIGS. 3, 4, and 8 and/or steps in FIGS. 5-7 and 9) to be loaded into computer system 1000. Such means may include, for example, a removable storage unit 1018 and an interface 1014. Examples of such means may include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an EPROM, or PROM) and associated socket, a thumb drive and USB port, and other removable storage

units 1018 and interfaces 1014 which allow software and data to be transferred from removable storage unit 1018 to computer system 1000.

[0103] Computer system 1000 may also include a communications interface 1020. Communications interface 1020 allows software (e.g., software used to implement the blocks depicted in FIGS. 3, 4, and 8 and/or steps in FIGS. 5-7 and 9) and data to be transferred between computer system 1000 and external devices. Examples of communications interface 1020 may include a modem, a network interface (such as an Ethernet card), a communications port, a PCMCIA slot and card, etc. Software and data transferred via communications interface 1020 are in the form of signals which may be electronic, electromagnetic, optical, or other signals capable of being received by communications interface 1020. These signals are provided to communications interface 820 via a communications path 1022. Communications path 1022 carries signals and may be implemented using wire or cable, fiber optics, a phone line, a cellular phone link, an RF link and other communications channels.

[0104] As used herein, the terms "computer program medium" and "computer readable medium" are used to generally refer to tangible storage media such as removable storage units 1016 and 1018 or a hard disk installed in hard disk drive 1010. These computer program products are means for providing software (e.g., software used to implement the blocks depicted in FIGS. 3, 4, and 8 and/or steps in FIGS. 5-7 and 9) to computer system 1000.

[0105] Computer programs (also called computer control logic) are stored in main memory 1006 and/or secondary memory 1008. Computer programs may also be received via communications interface 1020. Such computer programs, when executed, enable the computer system 1000 to implement the present disclosure as discussed herein. In particular, the computer programs, when executed, enable processor 1004 to implement the processes of the present disclosure, such as any of the methods described herein. Accordingly, such computer programs represent controllers of the computer system 1000. Where the disclosure is implemented using software, the software may be stored in a computer program product and loaded into computer system 1000 using removable storage drive 1012, interface 1014, or communications interface 1020.

[0106] In another embodiment, features of the disclosure are implemented primarily in hardware using, for example, hardware components such as application-specific integrated circuits (ASICs) and gate arrays. Implementation of a hardware state machine

so as to perform the functions described herein will also be apparent to persons skilled in the relevant art(s).

6. Conclusion

[0107] Embodiments have been described above with the aid of functional building blocks illustrating the implementation of specified functions and relationships thereof. The boundaries of these functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternate boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed.

[0108] The foregoing description of the specific embodiments will so fully reveal the general nature of the disclosure that others can, by applying knowledge within the skill of the art, readily modify and/or adapt for various applications such specific embodiments, without undue experimentation, without departing from the general concept of the present disclosure. Therefore, such adaptations and modifications are intended to be within the meaning and range of equivalents of the disclosed embodiments, based on the teaching and guidance presented herein. It is to be understood that the phraseology or terminology herein is for the purpose of description and not of limitation, such that the terminology or phraseology of the present specification is to be interpreted by the skilled artisan in light of the teachings and guidance.

WHAT IS CLAIMED IS:

1. A dispenser controller comprising:

a dispenser web service client configured to construct a web service message comprising a header and a body, wherein the body contains telemetry data of a dispenser machine;

a dispenser web service gateway configured to:

intercept the web service message in a manner transparent to the dispenser web service client before the web service message is sent over a computer network to an administrator controller,

create a digital signature by signing at least a part of the telemetry data in the web service message with a private key associated with the dispenser controller,

insert the digital signature into the header of the web service message,

encrypt at least a part of the telemetry data in the body of the web service message, and

transmit the web service message, after inserting the digital signature into the header of the web service message and encrypting the at least a part of the telemetry data in the body of the web service message, to the administrator over the computer network.

2. The dispenser controller of claim 1, wherein the telemetry data includes both consumption data of the dispenser machine and status data of the dispenser machine.

3. The dispenser controller of claim 1, wherein the dispenser web service gateway is further configured encrypt the at least a part of the telemetry data in the body of the web service message using a public key associated with the administrator controller.

4. The dispenser controller of claim 1, wherein the dispenser web service gateway is further configured encrypt the at least a part of the telemetry data in the body of the web service message using a symmetric key.

5. The dispenser controller of claim 4, wherein the dispenser web service gateway is further configured to encrypt the symmetric key using a public key associated with the administrator controller.

6. The dispenser controller of claim 1, wherein the dispenser web service gateway is further configured to send a heartbeat message, without signing or encrypting data within the heartbeat message, to the administrator controller before transmitting the web service message to the administrator controller over the computer network, wherein the heartbeat message is used to signal that the dispenser machine exists to the administrator controller.

7. The dispenser controller of claim 1, wherein the dispensing machine dispenses beverages.

8. The dispenser controller of claim 1, wherein the computer network is the internet.

9. An administrator controller comprising:

an administrator web service gateway configured to:

receive a web service message comprising a header and a body over a computer network, wherein the header contains a digital signature and the body contains encrypted telemetry data of a dispenser machine,

authenticate the web service message using a public key associated with the dispenser machine;

authorize a request in the web service message based on an identity of the dispenser machine, and

decrypt the encrypted telemetry data in the body of the web service message; and

an administrator web service provider configured to process the web service message based on the request and the decrypted telemetry data after the web service message has been authenticated and the request authorized by the administrator web service gateway.

10. The administrator controller of claim 9, wherein the telemetry data includes both consumption data of the dispenser machine and status data of the dispenser machine.

11. The administrator controller of claim 9, wherein the administrator web service gateway is transparent to the administrator web service provider.

12. The administrator controller of claim 9, wherein the web service gateway is further configured to authorize the request in the web service message based on the identity of the dispenser machine only after authenticating the web service message.

13. The administrator controller of claim 9, wherein the request is to place the decrypted telemetry data into a database.

14. The administrator controller of claim 9, wherein the dispensing machine dispenses beverages.

15. The administrator controller of claim 9, wherein the computer network is the internet.

16. The administrator controller of claim 9, wherein the administrator web service gateway is further configured to receive a second web service message from a second dispensing machine.

17. A method comprising:

constructing a web service message comprising a header and a body, wherein the body contains telemetry data of a dispenser machine;

intercepting the web service message before the web service message is sent over the internet to an administrator controller;

creating a digital signature by signing at least a part of the telemetry data in the web service message with a private key associated with the dispenser controller;

inserting the digital signature into the header of the web service message;

encrypting at least a part of the telemetry data in the body of the web service message; and

transmitting the web service message, after inserting the digital signature into the header of the web service message and encrypting the at least a part of the telemetry data in the body of the web service message, to the administrator over the internet.

18. The method of claim 17, wherein the telemetry data includes both consumption data of the dispenser machine and maintenance data of the dispenser machine.

19. The method of claim 17, further comprising:

sending a heartbeat message, without signing or encrypting data within the heartbeat message, to the administrator controller before transmitting the web service message to the administrator controller over the internet, wherein the heartbeat message is used to register the dispenser machine with the administrator controller.

20. The method of claim 17, wherein the dispensing machine dispenses beverages.

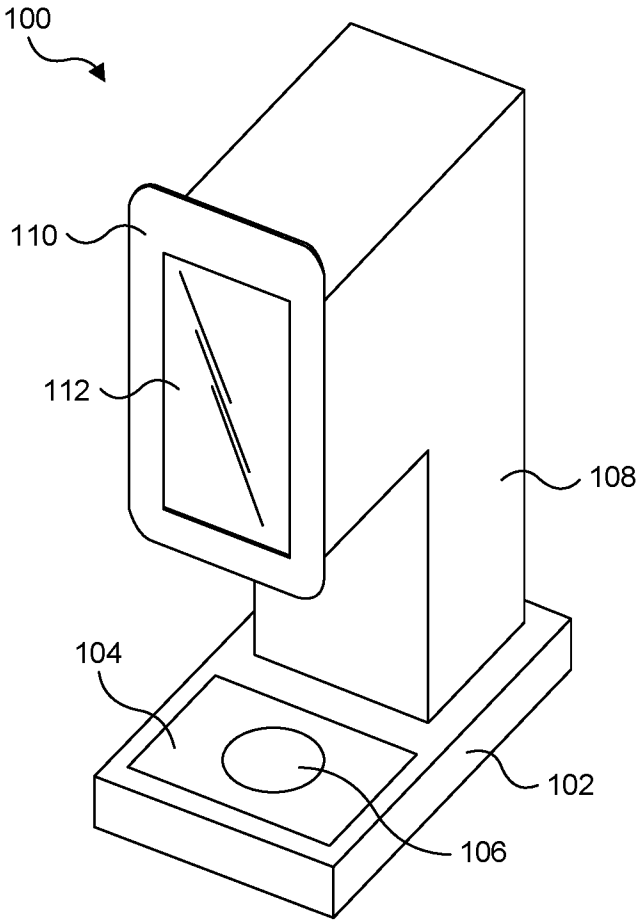

FIG. 1

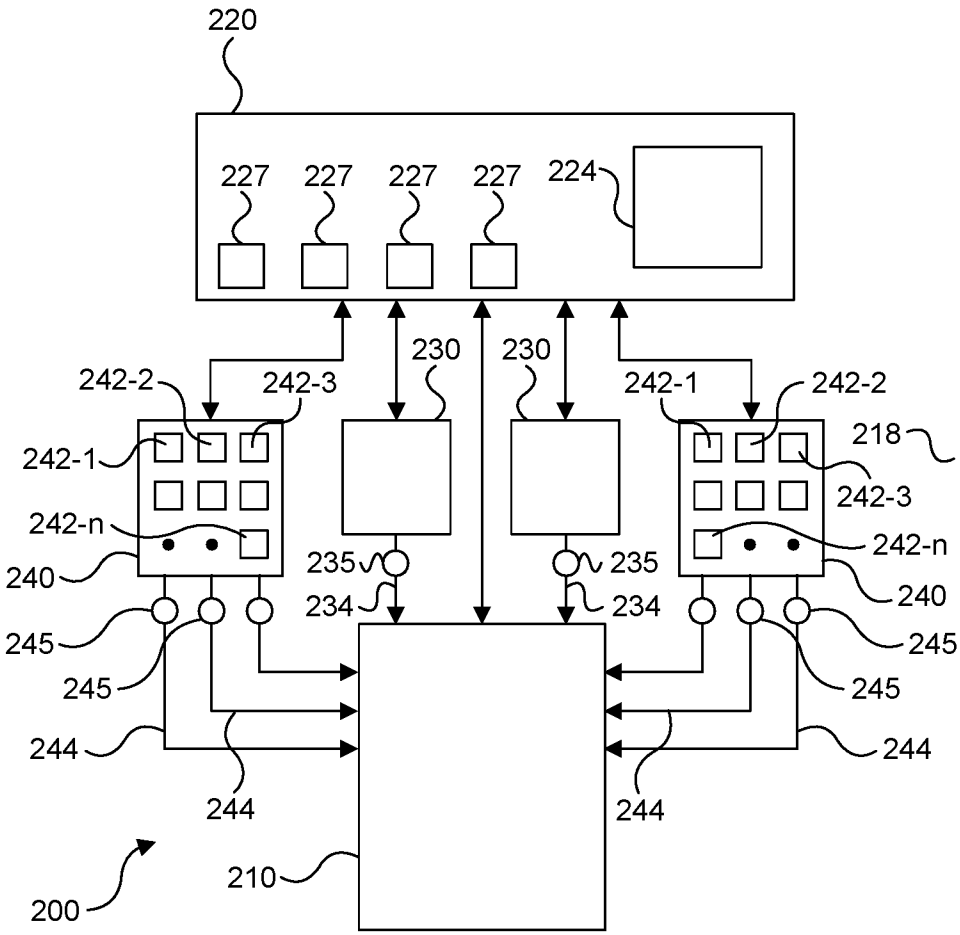
220
227
227
227
227
224
230
230
242-2
242-3
242-1
242-2
218
242-1
242-3
242-n
242-n
240
235
235
240
234
234
245
245
245
245
244
244
244
244
210
200

FIG. 2

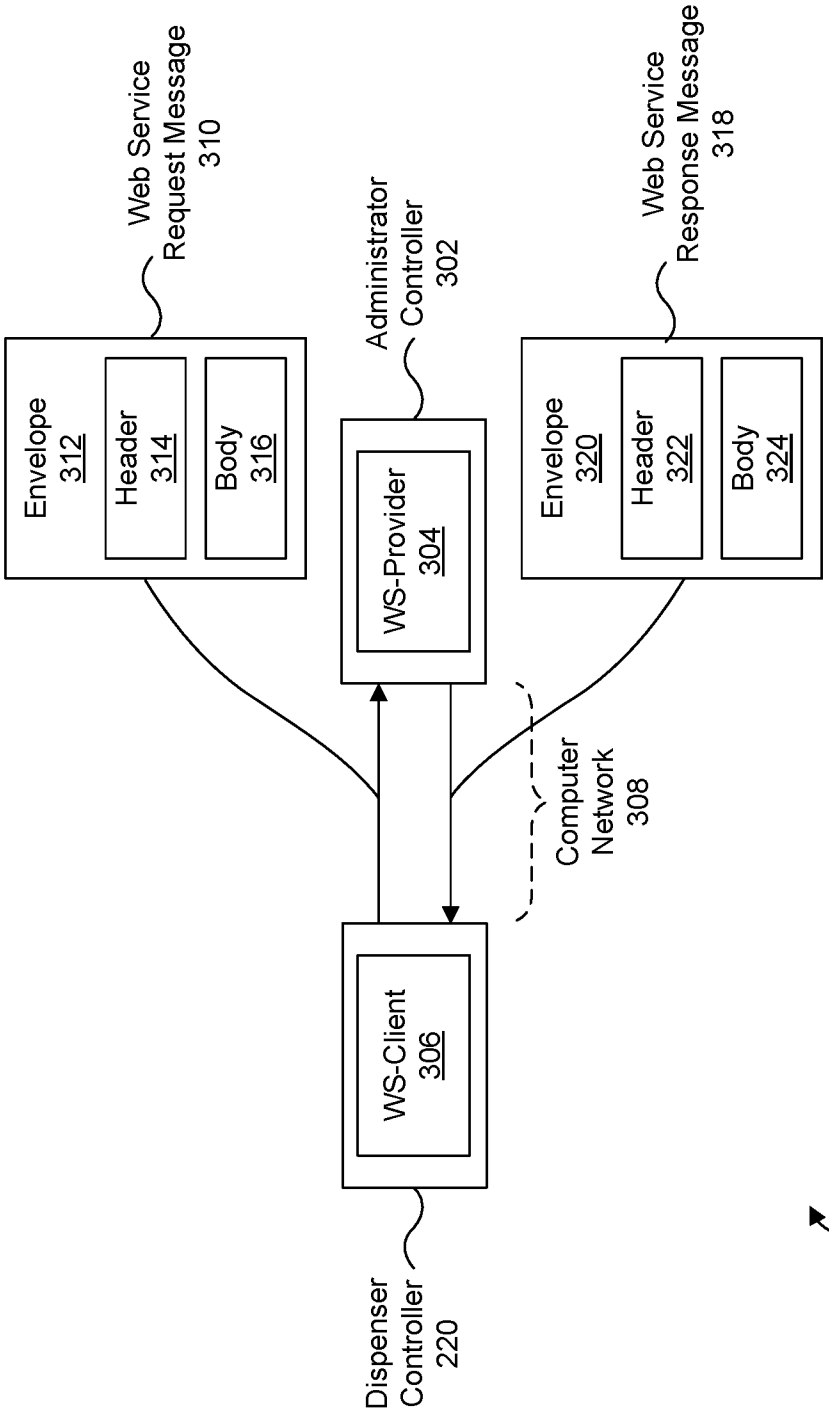
Web Service Request Message 310
Envelope 312
Header 314
Body 316
Administrator Controller 302
WS-Provider 304
Web Service Response Message 318
Envelope 320
Header 322
Body 324
Computer Network 308
WS-Client 306
Dispenser Controller 220
300

FIG. 3

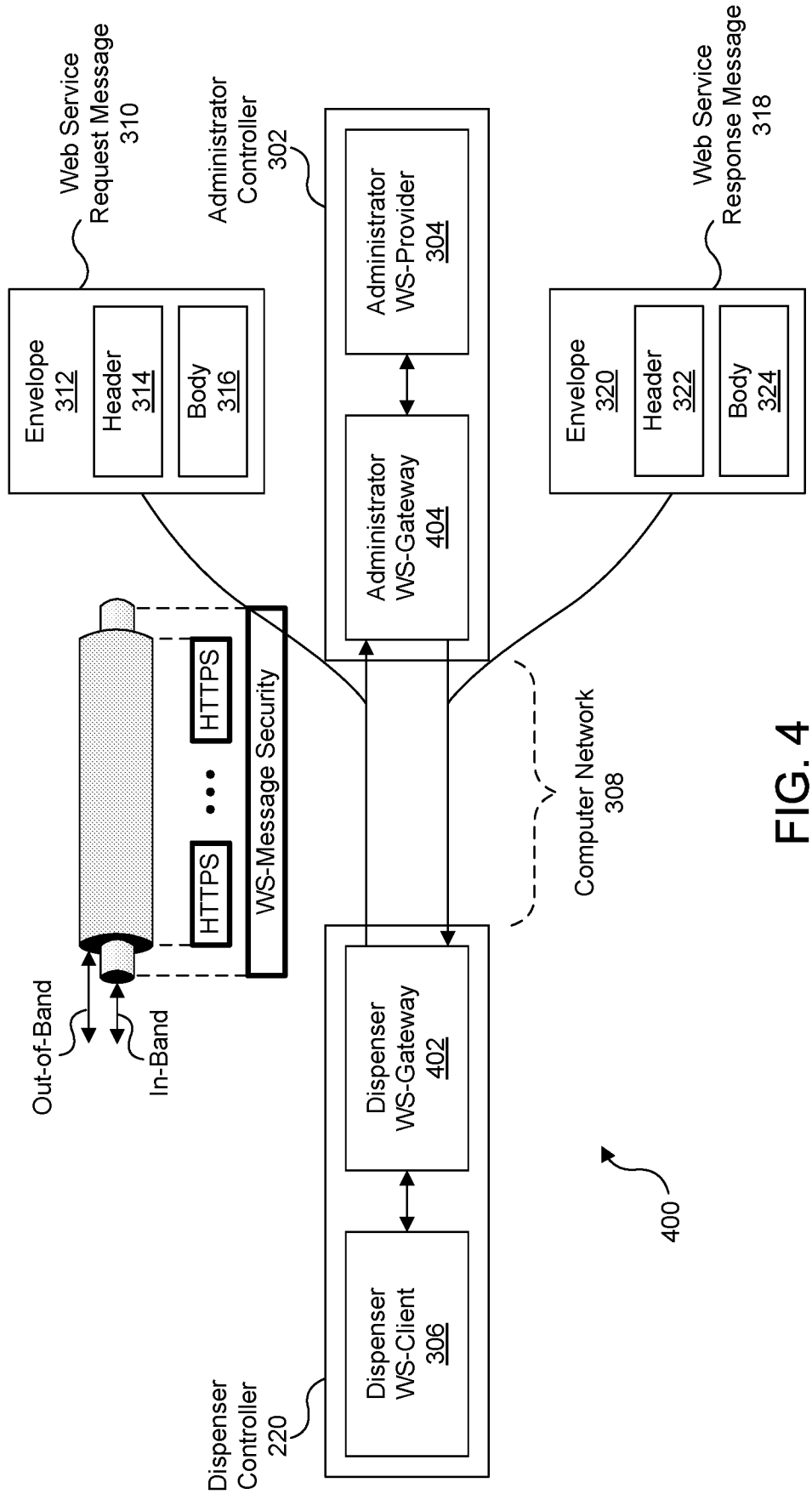
Web Service Request Message 310
Envelope 312
Header 314
Body 316
Administrator Controller 302
Administrator WS-Provider 304
Administrator WS-Gateway 404
Web Service Response Message 318
Envelope 320
Header 322
Body 324
HTTPS
HTTPS
WS-Message Security
Out-of-Band
In-Band
Computer Network 308
Dispenser WS-Gateway 402
Dispenser WS-Client 306
Dispenser Controller 220
400

FIG. 4

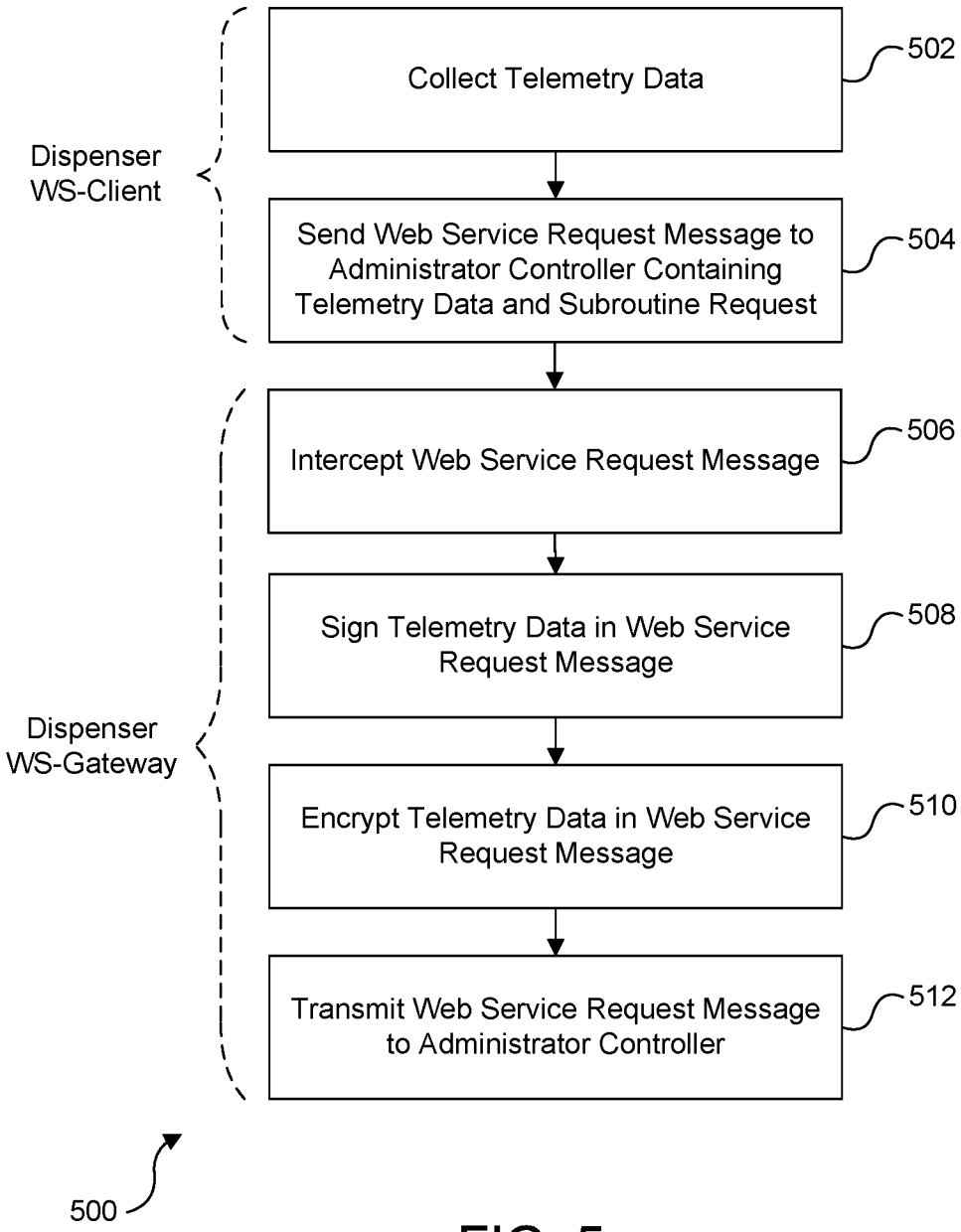
Collect Telemetry Data
502
Dispenser WS-Client
Send Web Service Request Message to Administrator Controller Containing Telemetry Data and Subroutine Request
504
Intercept Web Service Request Message
506
Sign Telemetry Data in Web Service Request Message
508
Dispenser WS-Gateway
Encrypt Telemetry Data in Web Service Request Message
510
Transmit Web Service Request Message to Administrator Controller
512
500

FIG. 5

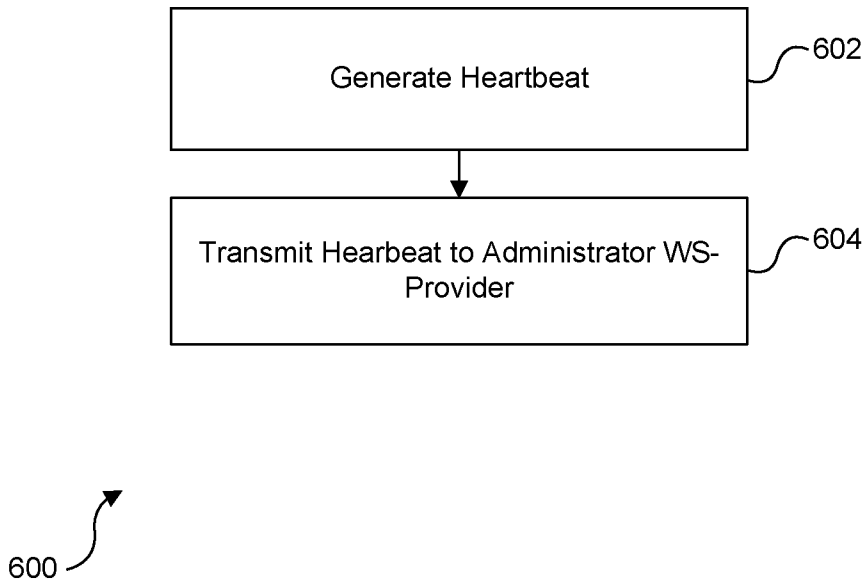
Generate Heartbeat
602
Transmit Hearbeat to Administrator WS-Provider
604
600

FIG. 6

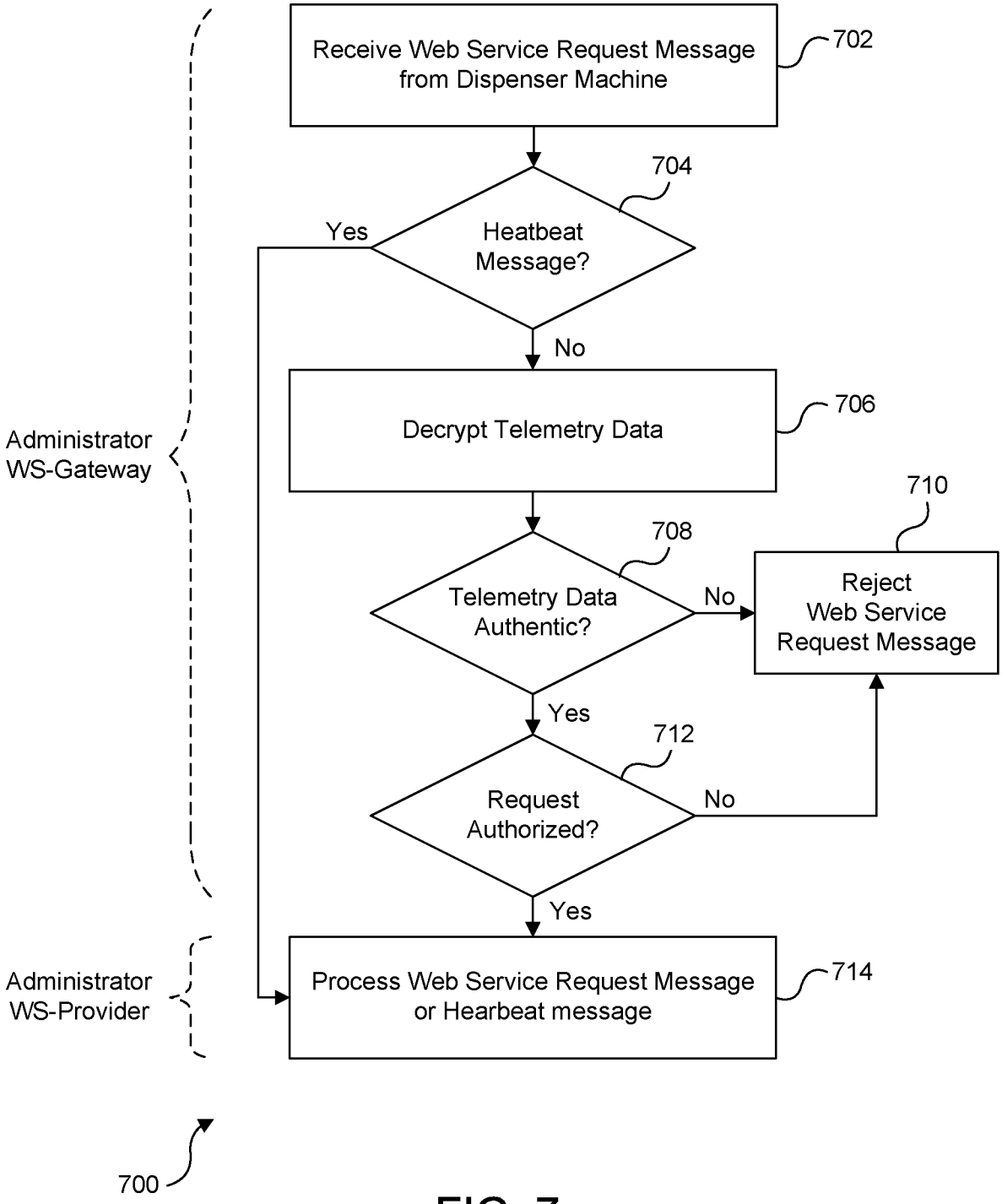
Receive Web Service Request Message from Dispenser Machine
702
704
Heatbeat Message?
Yes
No
Decrypt Telemetry Data
706
710
708
Telemetry Data Authentic?
No
Reject Web Service Request Message
Yes
712
Request Authorized?
No
Yes
Process Web Service Request Message or Hearbeat message
714
Administrator WS-Gateway
Administrator WS-Provider
700

FIG. 7

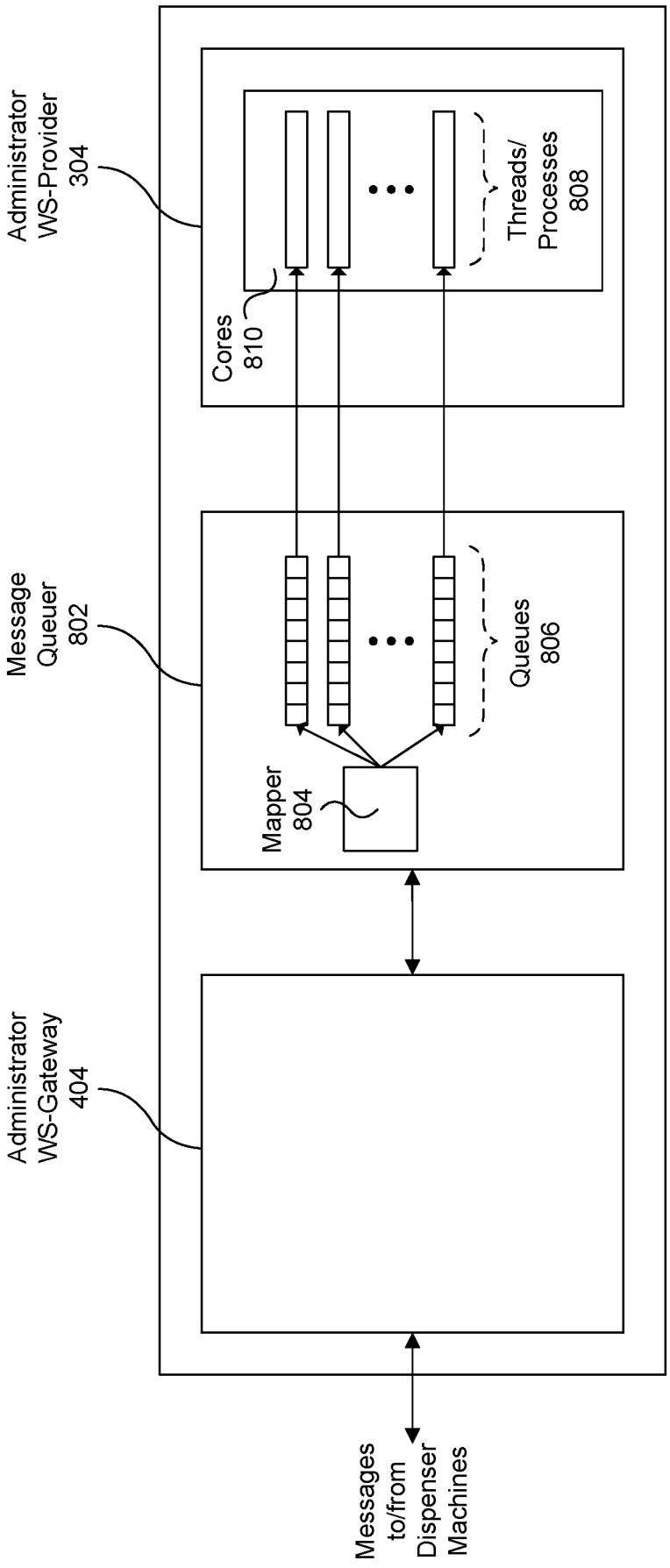
Administrator
WS-Provider
304
Cores
810
Threads/
Processes
808
Message
Queuer
802
Mapper
804
Queues
806
Administrator
WS-Gateway
404
Messages
to/from
Dispenser
Machines
Administrator
Controller
800

FIG. 8

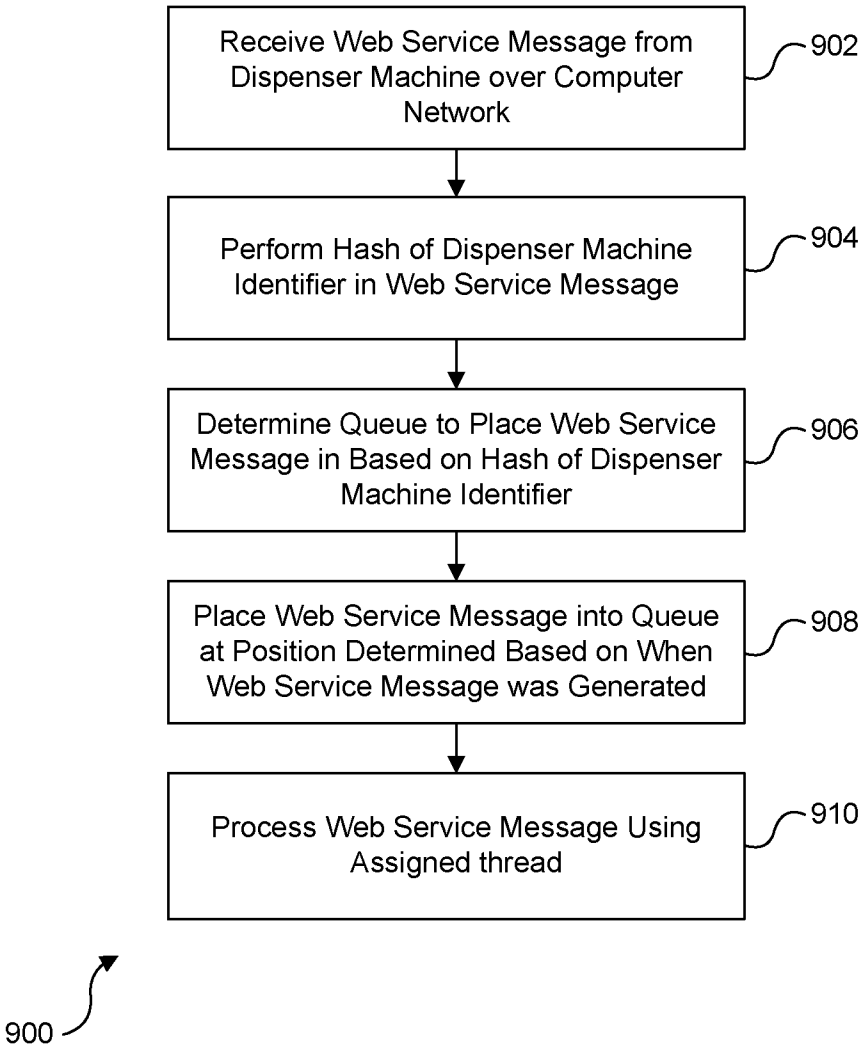
Receive Web Service Message from Dispenser Machine over Computer Network
902
Perform Hash of Dispenser Machine Identifier in Web Service Message
904
Determine Queue to Place Web Service Message in Based on Hash of Dispenser Machine Identifier
906
Place Web Service Message into Queue at Position Determined Based on When Web Service Message was Generated
908
Process Web Service Message Using Assigned thread
910
900

FIG. 9

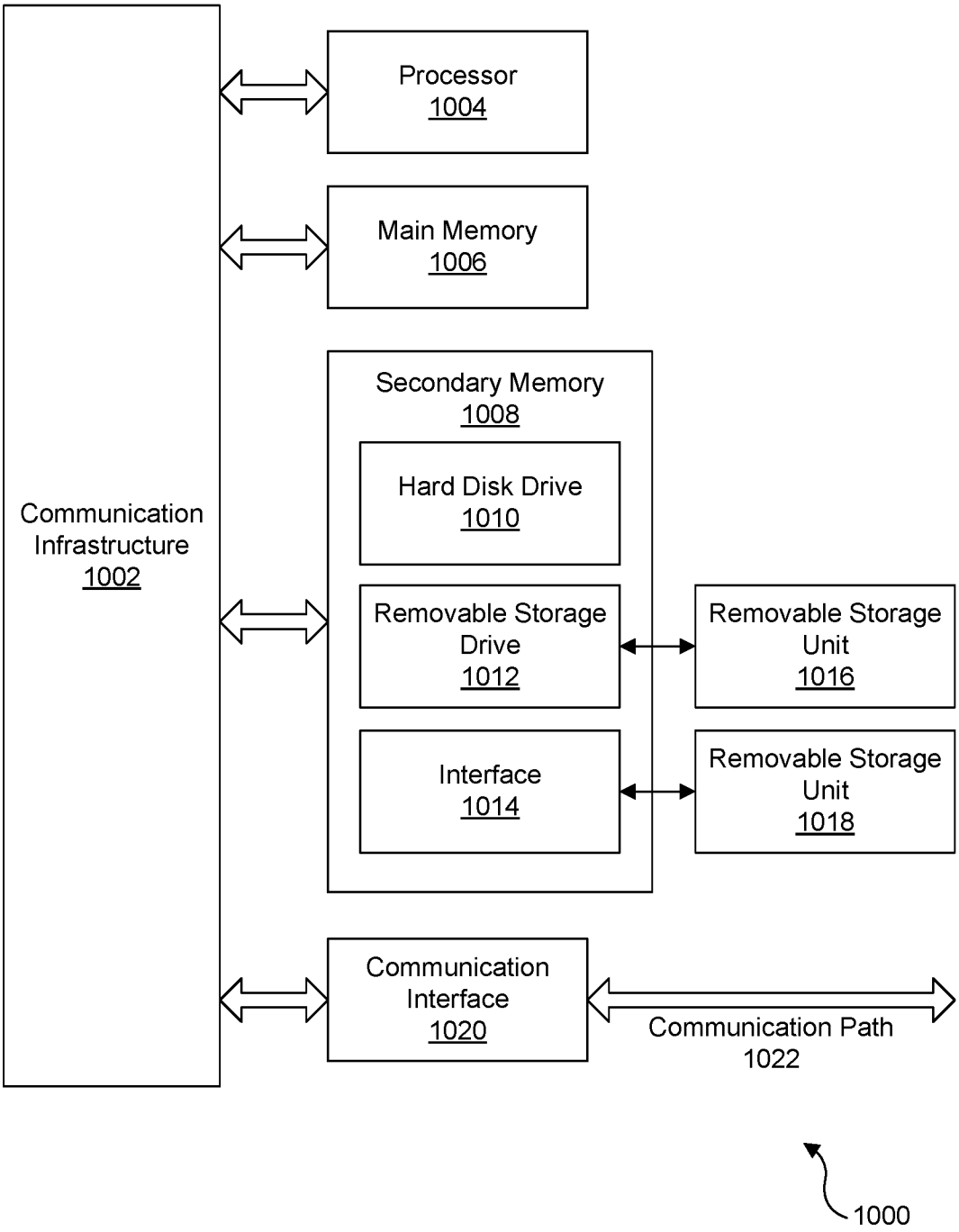
Communication Infrastructure 1002
Processor 1004
Main Memory 1006
Secondary Memory 1008
Hard Disk Drive 1010
Removable Storage Drive 1012
Interface 1014
Removable Storage Unit 1016
Removable Storage Unit 1018
Communication Interface 1020
Communication Path 1022
1000

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US17/30121

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
Group I: Claims 1-8 and 17-20; Group II: Claims 9-16

-***-Continued in extra sheet-***-

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
Claims 1-8 and 17-20

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US17/30121

A. CLASSIFICATION OF SUBJECT MATTER
IPC - H04L9/30, H04L9/32 (2017.01)
CPC - H04L9/30, H04L9/3247, H04L63/04

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)
See Search History document

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014/0341217 A1 (FIRESTAR SOFTWARE, INC.) 20 November 2014; paragraphs [0044]-[0046], [0050], [0056], [0085], [0089], [0112], [0192], [0269]	1-8, 17-20
Y	US 6,796,490 B1 (DRUMMOND, J et al.) 28 September 2004; figures 1, 2; column 5, lines 29-31; column 6, line 59 to column 7, line 5; column 8, lines 11-21	1-8, 17-20
Y	US 2005/0043011 A1 (MURRAY, T et al.) 24 February 2005; paragraphs [0038], [0052], [0212]	2, 7, 18, 20
A	US 2007/0106559 A1 (HARRELL, D) 10 May 2007; entire document	1-8, 17-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family 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 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	Date of mailing of the international search report
11 July 2017 (11.07.2017)	29 AUG 2017
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US17/30121

-***-Continued from Box No. III - Observations where unity of invention is lacking-***-

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fee must be paid.

Group I: Claims 1-8 and 17-20 are directed towards intercepting and encrypting a web service message before it is sent over a network using a dispenser web service gateway.
Group II: Claims 9-16 are directed towards authenticating a web service message using a public key by an administrator web service gateway.

The inventions listed as Groups I-II do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:

The special technical features of Group I include at least a dispenser controller comprising: a dispenser web service client configured to construct a web service message; a dispenser web service gateway configured to: intercept the web service message in a manner transparent to the dispenser web service client before the web service message is sent over a computer network; create a digital signature by signing at least a part of the telemetry data in the web service message with a private key associated with the dispenser controller, insert the digital signature into the header of the web service message, encrypt at least a part of the telemetry data in the body of the web service message, and transmit the web service message, which are not present in Group II.

The special technical features of Group II include at least an administrator web service gateway configured to: receive a web service message; authenticate the web service message using a public key; authorize a request in the web service message based on an identity of the dispenser machine, and decrypt the encrypted telemetry data in the body of the web service message; and an administrator web service provider configured to process the web service message based on the request and the decrypted telemetry data after the web service message has been authenticated and the request authorized by the administrator web service gateway, which are not present in Group I.

The common technical features shared by Groups I-II are a web service message comprising a header and a body, wherein the header contains a digital signature and the body contains telemetry data of a dispenser machine; an administrator controller; and a computer network.

However, these common features are previously disclosed by US 2005/0172024 A1 to CHEIFOT, A et al. (hereinafter "Cheifot"). Cheifot discloses a web service message comprising a header and a body, wherein the header contains a digital signature (an addressed message using an IP addressing scheme (web) contains a seed for encryption processes, control information labelled as PREAMBLE (header contains a digital signature); figure 1; paragraphs [0043], [0046]) and the body contains telemetry data of a dispenser machine; an administrator controller; and a computer network (number of items sold or remaining in a vending machine/LAN device (telemetry data of a dispenser machine) obtained by a sensor is provided as a unique source of data forwarded in a TAS message (the body) upstream on a network using an application custodian (administrator controller); paragraphs [0216], [0222], [0269], [0568]).

Since the common technical features are previously disclosed by the Cheifot reference, these common features are not special and so Groups I-II lack unity.