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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 December 2020 (17.12.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/251744 A1

(51) International Patent Classification:
G06F 21/00 (2013.01) *G06Q 99/00* (2006.01)
G06Q 20/22 (2012.01) *H04L 9/00* (2006.01)

(21) International Application Number:
PCT/US2020/034444

(22) International Filing Date:
24 May 2020 (24.05.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/859,586 10 June 2019 (10.06.2019) US
16/580,863 24 September 2019 (24.09.2019) US

(71) Applicant: **DOCUSIGN, INC.** [US/US]; 221 Main Street, Suite 1000, San Francisco, CA 94105 (US).

(72) Inventors: **WISE, Joshua D.**; c/o DocuSign, Inc., 221 Main Street, Suite 1000, San Francisco, CA 94105 (US). **WISHAN, Brian**; c/o DocuSign, Inc., 221 Main Street, Suite 1000, San Francisco, CA 94105 (US). **WANG, Bei**; c/o DocuSign, Inc., 221 Main Street, Suite 1000, San Francisco, CA 94105 (US). **LOUIE, Darren**; c/o DocuSign, Inc., 221 Main Street, Suite 1000, San Francisco, CA 94105 (US). **WALSH, Blake Thomas**; c/o DocuSign, Inc., 221 Main Street, Suite 1000, San Francisco, CA 94105 (US).

(74) Agent: **JACOBSON, Anthony** et al.; Fenwick & West LLP, Silicon Valley Center, 801 California Street, Mountain View, CA 94041 (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, JO, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, 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,

(54) Title: SYSTEM AND METHOD FOR ELECTRONIC CLAIM VERIFICATION

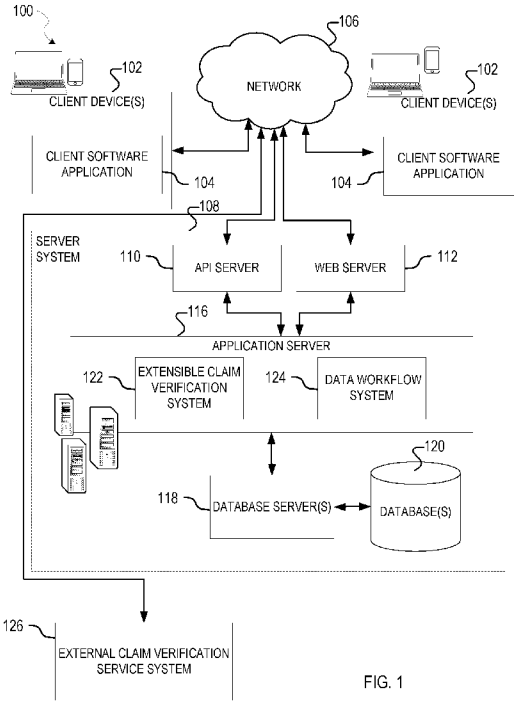


FIG. 1

(57) Abstract: Various embodiments support or provide for an extensible electronic claim verification system that offers extensible support for electronic verification by one or more external electronic claim verification services that are external to the extensible electronic claim verification system. For some embodiments, the extensible claim verification system is readily configurable (e.g., by a user) to add or remove access to one or more external claim verification services available for use through the extensible electronic claim verification system by a client device. Some embodiments implement the extensible support by using a unified protocol for interfacing with different external claim verification services. By use of the unified protocol, various embodiments enable an external claim verification service to plug into an extensible claim verification system, thereby permitting a user to extend support of the extensible claim verification system to different types of external claim verification services.

WO 2020/251744 A1

[Continued on next page]

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))*

SYSTEM AND METHOD FOR ELECTRONIC CLAIM VERIFICATION

TECHNICAL FIELD

[0001] The present disclosure relates generally to electronic verification, and, more particularly, various embodiments described herein provide for systems, methods, techniques, instruction sequences, and devices that support electronic verification of claimed information, such as electronic verification of information claimed about a user.

BACKGROUND

[0002] Today, execution of a data workflow by one entity (e.g., business organization) can often involve or necessitate verification of certain information by another entity, such as via an electronic service (e.g., online service) provided by the other entity (e.g., third-party organization). Examples of such information include information claimed by an entity or user, also referred herein as claimed information or a claim. For data workflows involving user input, the ability to verify certain information (e.g., user claimed information) based on the user input can be crucial for successful workflow completion. For instance, verifying information regarding the identity of a user, such as verifying information claiming to be alternative or additional forms of identification for the user (e.g., social security number, passport number, driver license number, etc.), can facilitate additional identity assurances of the user during various data workflows. This type of verification can be important (or even required in certain legal jurisdictions) where a data workflow involves, for example: a user electronically signing a legal document (e.g., via a website); or a user electronically completing a form and some portion of the user-provided information needs to be verified before the form is considered complete or accurate. Verifying user-provided information can also be important (or required) in a data workflow where the age or location of a user needs to be verified before the user can consent to an activity or transaction. Sometimes, such information verification is not possible by one entity (e.g., relying party) without the assistance or involvement of another entity (e.g., third-party or non-third-party verification provider).

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] In the drawings, which are not necessarily drawn to scale, like numerals may describe similar components in different views. To easily identify the discussion of any particular element or act, the most significant digit or digits in a reference number refer to the figure number in which that element is first introduced. Some embodiments are illustrated by way of example, and not limitation, in the figures of the accompanying drawings.

[0004] **Figure 1** is a block diagram showing an example data system that includes an extensible claim verification system that can provide access to an external claim verification service, according to some embodiments.

[0005] **Figure 2** is a block diagram illustrating an extensible claim verification system, according to some embodiments.

[0006] **Figure 3** is a diagram illustrating an example data workflow interfacing with and using an example external claim verification service, according to some embodiments.

[0007] **Figure 4** is a diagram illustrating example data interactions with an example extensible claim verification system, according to some embodiments.

[0008] **Figures 5** and **6** are flowcharts illustrating example methods for extensible claim verification, according to some embodiments.

[0009] **Figure 7** presents a screen shot of an example graphical user interface (GUI) for managing one or more external claim verification services, according to some embodiments.

[0010] **Figure 8** is a block diagram illustrating a representative software architecture, which may be used in conjunction with various hardware architectures herein described, according to various embodiments of the present disclosure.

[0011] **Figure 9** is a block diagram illustrating components of a machine able to read instructions from a machine storage medium and perform any one or more of the methodologies discussed herein according to various embodiments of the present disclosure.

DETAILED DESCRIPTION

[0012] Various embodiments relate to electronic verification of a claim by an external claim verification service, which may be a service operated by a third-

party entity (e.g., external claim verification service provider). In particular, various embodiments described herein support or provide for an extensible electronic claim verification system (also referred to herein as an extensible claim verification system) that offers extensible support for electronic verification by one or more external electronic claim verification services (also referred to herein as external claim verification services) that are external to the extensible electronic claim verification system. For some embodiments, the extensible claim verification system is readily configurable (e.g., by an individual user or an admin user through a graphical user interface (GUI)) to add or remove access to one or more external claim verification service available for use through the extensible claim verification system by a client device. Some embodiments implement the extensible support by using a unified protocol for interfacing with different external claim verification services. By use of the unified protocol, various embodiments enable a user of an external claim verification service to plug into an extensible claim verification system, thereby permitting a user to extend support of the extensible claim verification system to different types of external claim verification services. With respect to a given entity, the unified protocol can enable the extensible claim verification system to interface with (e.g., interact with) an external claim verification service that is implemented or operated by a third-party entity, or an external claim verification service that is proprietary to (e.g., custom-built for) the given entity. To enable interfacing with extensible claim verification system, a given external claim verification service can be designed or implemented to support the unified protocol.

[0013] According to some embodiments, an extensible claim verification system described herein can provide a data workflow that relies on verification of one or more external claim verification services. An example of such a data workflow can include, without limitation, one that involves the electronic signing of a document by a user whose identity is to be verified by way of an external identification verification service (as used herein, a type of external claim verification service). In particular, the extensible claim verification system can enable a client of an electronic signature service (or digital certificate service) to implement their own custom claim verification service for use in an electronic signature workflow (or a digital certificate workflow), such as a custom claim

verification service that implements an authentication mechanism to challenge a user when the user accesses a document to electronically sign the document. The client in this case represent an entity that is relying on verification of one or more claims (e.g., user identity claims) prior to permitting the user to electronically sign the document.

[0014] After an extensible claim verification system described herein is configured to access a particular extensible claim verification service, the extensible claim verification system can receive from a client device (e.g., one operating a data workflow) a request to verify by the particular extensible claim verification service one or more claims for a particular user. As noted herein, an example of a claim submitted for verification can include one relating to verifying an identity of the particular user. Additionally, the received request may be one generated by the client device to authenticate access of a particular data workflow (e.g., electronic signature or digital certificate workflow) by the particular user. Eventually, a response to the received request (response provided by the extensible claim verification system to the client device) can determine whether the access is authenticated at the client device.

[0015] Based on the request, some embodiments direct (e.g., redirect via a web browser redirect) the particular user to an external claim verification service that is to verify at least one claim (of the one or more claims specified by the request). Once directed to the external claim verification service, the external claim verification service can cause the user to perform one or more actions (e.g., complete one or more steps) to verify the at least one claim. One of those actions can include, without limitation, the user authenticating their self with the external claim verification service based on credentials (e.g., username and password) provided by the user. For some embodiments, after the one or more actions are completed by the user, the external claim verification service directs (e.g., redirects) the user back to the extensible claim verification system described herein. Additionally, the external claim verification service can provide (e.g., with the redirection) a response to the extensible claim verification system, where the response can comprise data that includes a value for the at least one claim, that evidences whether the at least one claim was verified (e.g., "True" or "False" value to indicate validation), or that evidences whether the user successfully completed

the one or more actions. The evidence data can be signed by the external claim verification service (e.g., using a private key) to ensure integrity of the evidence data.

[0016] After the external claim verification service directs the user back to the extensible claim verification system, the extensible claim verification system can generate a response to the request from the client device based on the response the extensible claim verification system received from the external claim verification service. The particular data workflow operating on the client device can rely on the data (e.g., evidence data) included within the response received from the extensible claim verification system. Where the particular data workflow involves electronic signing of a document, the data workflow may or may not allow the user to proceed with electronically signing the document based on the data from the response. For instance, the particular data workflow can permit the user to electronically sign if the data indicates that identity claims for the user submitted to the external claim verification service are verified (which, for example, can be used in the issuance of a digital certificate for purposes of digital signing a document). Further, the particular data workflow can record an event (e.g., successful or unsuccessful verification of claims) in a transaction history based on the data included within the response.

[0017] As used herein, a claim can comprise a request for data provided by a claim verification service or an assertion of information that can be verified (e.g., as accurate or inaccurate, correct or wrong, etc.) by a claim verification service. For instance, a claim for a user can comprise an assertion of information regarding the user (e.g., information claiming to identify the user, such as different forms of identification) that can be verified by a claim verification service. Examples of a claim for identifying a user can include, without limitation, a social security number associated with a user, an e-mail address associated with a user, a driver license number of a user, a passport number of a user, a legal name associated with a user, a username, and the like. Other examples of a claim regarding a user can include, without limitation, a residential address of the user, a billing address of the user, a country of citizenship of the user, one or more privileges/permissions associated with the user, account information for the user, and the like

[0018] As used herein, an external identification verification service can comprise an external claim verification service that verifies a claim relating to the identity of a user (e.g., based on user-provided information). For an external identification verification service, the verification of an identity of a user based on a claim can simply comprise the user authenticating with the external identification verification service.

[0019] As used herein, verifying a particular claim can comprise submitting asserted information of the particular claim to an external electronic verification service and receiving a verification result from the external electronic verification service indicating whether the asserted information was successfully verified (e.g., as accurate). Additionally, or alternatively, verifying a particular claim can comprise submitting the identifier of the particular claim (e.g., label associated with particular claim, such as "e-mail address") to an external electronic verification service and receiving a value for the particular claim (e.g., john_smith@domain.com) from the external electronic verification service, thereby obtaining a value for the particular claim.

[0020] The description that follows includes systems, methods, techniques, instruction sequences, and devices that embody illustrative embodiments of the disclosure. In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide an understanding of various embodiments of the inventive subject matter. It will be evident, however, to those skilled in the art, that embodiments of the inventive subject matter may be practiced without these specific details. In general, well-known instruction instances, protocols, structures, and techniques are not necessarily shown in detail.

[0021] Reference will now be made in detail to embodiments of the present disclosure, examples of which are illustrated in the appended drawings. The present disclosure may, however, be embodied in many different forms and should not be construed as being limited to the embodiments set forth herein.

[0022] **Figure 1** is a block diagram showing an example data system 100 that includes an extensible claim verification system 122 that can provide access to an external claim verification service, according to some embodiments. As shown, the data system 100 includes multiple client devices 102, a server system 108, an external claim verification service system 126, and a network 106 (e.g., including

Internet, wide-area-network, local-area-network, wireless network, etc.) that communicatively couples them together. As also shown, the data system 100 includes a data workflow system 124 that can support operation of a data workflow, such as an electronic signature or digital certificate workflow, that relies on verification of a claim via the extensible claim verification system 122. Each client device 102 can host a number of applications, including a client software application 104. Each client software application 104 may communicate data with one or more other instances of the client software application 104, or with the server system 108 via a network 106. Accordingly, each client software application 104 can communicate and exchange data with another client software application 104 and with the server system 108 via the network 106. Additionally, the external claim verification service system 126 can communicate and exchange data with the server system 108 via the network 106. The data exchanged between the client software applications 104, between a client software application 104 and the server system 108, and between the server system 108 and the external software service server can include, without limitation, requests, responses, and authentication data (e.g., authentication token).

[0023] The external claim verification service system 126 can host a software application that provides an external claim verification service, which is external to a computing entity (e.g., the client devices 102 or the server system 108) but accessible by the computing entity over the network 106 via a software component. For instance, the extensible claim verification system 122 on the server system 108 can access the external claim verification service provided by the external claim verification service system 126. The extensible claim verification system 122 can comprise one or more computing devices that host the software application providing an external claim verification service.

[0024] The server system 108 provides server-side functionality via the network 106 to a particular client software application 104. While certain functions of the data system 100 are described herein as being performed by the extensible claim verification system 122 on the server system 108, it will be appreciated that the location of certain functionality within the server system 108 is a design choice. For example, it may be technically preferable to initially deploy certain technology and functionality within the server system 108, but to later migrate this

technology and functionality to the client software application 104 where a client device 102 provides enhanced data object functionality.

[0025] The server system 108 supports various services and operations that are provided to the client software application 104 by the extensible claim verification system 122. Such operations include transmitting data from the extensible claim verification system 122 to the client software application 104, receiving data from the client software application 104 to the extensible claim verification system 122, and the extensible claim verification system 122 processing data generated by the client software application 104. This data may include for example, data objects, requests, responses, public/private keys, hash values, access rights data, license data, and authentication data. Data exchanges within the data system 100 may be invoked and controlled through operations of software component environments available via one or more endpoints, or functions available via one or more user interfaces (UIs) of the client software application 104, which may include web-based UIs provided by the server system 108 for presentation at the client device 102.

[0026] With respect to the server system 108, each of an API server 110 and a web server 112 is coupled to an application server 116, which hosts the extensible claim verification system 122 and the data workflow system 124. The application server 116 is communicatively coupled to a database server 118, which facilitates access to a database 120 that stores data associated with the application server 116.

[0027] The API server 110 receives and transmits data (e.g., API calls, commands, data objects, requests, responses, public/private keys, hash values, access rights data, license data, and authentication data) between the client device 102 and the application server 116. Specifically, the API server 110 provides a set of interfaces (e.g., routines and protocols) that can be called or queried by the client software application 104 in order to invoke functionality of the application server 116. The API server 110 exposes various functions supported by the application server 116 including, without limitation: user registration; login functionality; data object operations (e.g., generating, storing, retrieving, encrypting, decrypting, transferring, access rights, licensing, etc.); interview sessions functionality; business process operations (e.g., starting, generating, etc.); user communications; and calendar functionality.

[0028] Through one or more web-based interfaces (e.g., web-based UIs), the web server 112 can support various functionality of the extensible claim verification system 122 of the application server 116 including, without limitation: user registration; login functionality; configuring access to an external claim verification service with respect to the extensible claim verification system 122, and activating or deactivating access to an external claim verification service through the extensible claim verification system 122. Additionally, the web server 112 can provide a set of HTTP endpoints or webhooks that can be called by the client software application 104 or by an external claim verification service provided by the external claim verification service system 126.

[0029] The application server 116 hosts a number of applications and subsystems, including the extensible claim verification system 122, which supports various functions and operations with respect to various embodiments described herein. For instance, the extensible claim verification system 122 can support one or more of the following functions: configuring access to an external electronic claim verification service provided by the external claim verification service system 126; receiving a request from a client device 102 for verifying a set of claims for a user by the external electronic claim verification service; based on the configured access to the external electronic claim verification service, responding to the request by causing a user at a client device 102 to be directed to the external electronic claim verification service to verify the set of claims for the user; receiving, from the external electronic claim verification service, a first response relating to verification of the set of claims; and providing, to a client device 102, a second response based on the first response. More regarding various embodiments of a software component relational system is described with respect to **Figure 2**.

[0030] The application server 116 hosts the data workflow system 124, which can support operation of a data workflow that relies on (or is augmented by) verification of a claim via the extensible claim verification system 122.

[0031] The application server 116 is communicatively coupled to a database server 118, which facilitates access to database(s) 120 in which may be stored data associated with the extensible claim verification system 122. Data associated with the extensible claim verification system 122 can include, without limitation: data

for configuring access by the extensible claim verification system 122 to an external claim verification service provided by the external claim verification service system 126; transaction information regarding one or more operations performed by the extensible claim verification system 122 (e.g., in connection with a response); and authentication data.

[0032] **Figure 2** is a block diagram illustrating an extensible claim verification system 200, according to some embodiments. For some embodiments, the extensible claim verification system 200 implements at least some part of the extensible claim verification system 122 described above with respect to **Figure 1**. As shown, the extensible claim verification system 200 comprises a client interface 202, an external claim verification service interface 204, an external claim verification service manager 206, a claim verification orchestrator 208, and a transaction tracker 210. For various embodiments, the components and arrangement of components shown may vary from what is illustrated in **Figure 2**. For instance, the extensible claim verification system 200 can include more or fewer components than the components shown in **Figure 2**.

[0033] The client interface 202 facilitates or supports data communication with a computing device that is operating as a client device and interacting with the extensible claim verification system 200. Likewise, the external claim verification service interface 204 facilitates or supports data communication with a computing device that is operating as provider of one or more external claim verification services (e.g., the external claim verification service system 126) and that is interacting with the extensible claim verification system 200.

[0034] The external claim verification service manager 206 facilitates or supports management of a set of external claim verification services accessible through the extensible claim verification system 200, which can include adding, configuring, and removing access to an external claim verification service the extensible claim verification system 200. The external claim verification services can be provided by one or more different external claim verification service systems or different external claim verification service providers. Configuring access to a particular external claim verification service can comprise a user specifying an address (e.g., URL or network address) for an endpoint of the particular external claim verification service, or specifying the version of unified protocol being used to

access the particular external claim verification service. For some embodiments, the external claim verification service manager 206 presents a graphical user interface for performing management functions on the extensible claim verification system 200 with respect to an external claim verification service. A user accessing the external claim verification service manager 206 can include an individual user or an admin user associated with an organization using the extensible claim verification system 200 to access one or more external claim verification services, such as an organization that offers or uses a data workflow that relies on claim verification. The user configuring access to an external claim verification service by the extensible claim verification system 200 can be different from a user for whom a claim is being verified. For some embodiments, a client device (e.g., one operating a data workflow) can request a listing of external claim verification services (e.g., via a REST API) that are configured for access through the extensible claim verification system 200 and available for use.

[0035] The claim verification orchestrator 208 facilitates or supports operations performed by the extensible claim verification system 200, such as operations relating to requests and responses exchanged between the extensible claim verification system 200 and one or more computing devices (e.g., a client device 102, the data workflow system 124, the external claim verification service system 126) to facilitate use of an external claim verification service as described herein. According to some embodiments, the claim verification orchestrator 208 uses a unified protocol for interacting with an external claim verification service, thereby enabling the extensible claim verification system 200 to provide extensible support (e.g., plug-in support) for external claim verification services of different types and from different providers (e.g., third-party or client-proprietary external claim verification services). Depending on the embodiment, the unified protocol can be based on Security Assertion Markup Language (SAML) (e.g., SAML 2.0) or OpenID (e.g., OpenID Connect 1.0). For some embodiments, the unified protocol can be based on other protocols. For some embodiments, the claim verification orchestrator 208 causes the extensible claim verification system 200 to operate in accordance with the various methodologies discussed herein, such as those described with respect to **Figures 3** through **6.**

[0036] The transaction tracker 210 facilitates or supports tracking claim verification request sessions between a client device that is requesting use of an external claim verification service available through the extensible claim verification system 200, and an external claim verification service system that is providing the external claim verification service requested for use. The transaction tracker 210 can record transaction information regarding one or more operations performed by the extensible claim verification system 200 in response to a claim verification request from a client device. Each claim verification request received by the extensible claim verification system 200 can be uniquely associated with a transaction identifier, and the transaction identifier can be used in the transaction information recorded by the transaction tracker 210. The transaction identifier can be used to track a claim request session on the extensible claim verification system 200. Additionally, the transaction tracker 210 can enable the extensible claim verification system 200 enable a lockout status for a particular claim verification request on a lockout threshold, where an enabled lockout status can prevent a user from further attempts to have an external claim verification service verify a claim. Depending on the embodiment, the lockout threshold can be associated with an individual transaction identifier. For instance, for each claim verification request received by the extensible claim verification system 200, the lockout threshold can limit the number of attempts by a user associated with the claim verification request to successfully have a claim verified by the external claim verification service. Additionally, or alternatively, the lockout threshold can be associated with individual external claim verification services that can be accessed by the extensible claim verification system 200. For instance, for each external claim verification service, the lockout threshold can limit the number of claims that can be verified by a given external claim verification service (e.g., limit over a time period, such as a day). In this way, the lockout threshold can throttle the number of claims that the given external claim verification service is requested to verify. The lockout threshold can be configured by a user administrating or managing the extensible claim verification system 200 (e.g., the same user managing the configured access to one or more external claim verification services on the extensible claim verification system 200). For instance, each external claim verification service, each individual

relying party, or each individual using the relying party can be associated with its own respective lockout threshold.

[0037] Figure 3 is a diagram illustrating an example data workflow 300 interfacing with and using an example external claim verification service 310, according to some embodiments. In particular, by use of various embodiments described herein (e.g., the extensible claim verification system 122 or 200), the data workflow 300 can use the external claim verification service 310 to verify a set of claims for a user. The data workflow 300 can represent, for example, an electronic signing workflow that permits a user to electronically sign a document. The external claim verification service 310 can represent one being provided by an external claim verification service system (e.g., 126). For some embodiments, in response to a request from a client device operating the data workflow to verify a set of claims for a user, at operation 302 an extensible claim verification system described herein causes a user to be directed (e.g., redirected from the extensible claim verification system) to the external claim verification service 310. The extensible claim verification system can provide the external claim verification service 310 (e.g., with the redirection) a request specifying the set of claims to be verified by the external claim verification service 310.

[0038] Once the user is directed to the external claim verification service 310, a verification process 312 can start and execute one or more verification steps 314-1 through 314-*N* with respect to the user, which can cause the user to perform a set of actions (e.g., interactions) with respect to the external claim verification service 310 (e.g., through a graphic user interface). For instance, verification step 314-1 can comprise an authentication step, whereby the user authenticates with the external claim verification service 310 using user credentials (e.g., username and password). For some embodiments, the external claim verification service 310 only provides the extensible claim verification system with a response upon the user successfully completing each of the verification steps 314-1 through 314-*N*. For various embodiments, how the user completes the verification steps 314-1 through 314-*N* can determine whether at least some or all of the set of claims are successfully verified. Though not illustrated with respect to the data workflow 300, some embodiments support requesting multiple claims from multiple external claim verification services. For example, a user can be redirected to the

external claim verification service 310, the user can be redirect back to the data workflow 300 after the external claim verification service 310 has fulfill a claim request, and the data workflow 300 can redirect the user to another external verification service to fulfill another claim request. This can continue until all claim request for the data workflow 300 are fulfilled, at which point claim values can be returned to a relying party.

[0039] Eventually, at operation 304, the external claim verification service 310 causes the user to be directed (e.g., redirected from the external claim verification service 310) back to the extensible claim verification system. The external claim verification service 310 can also send a response (e.g., with the redirection) to the extensible claim verification system, which can comprise data regarding verification of the set of claims by the external claim verification service 310. This response can be signed by the external claim verification service 310 (e.g., using its private key), thereby ensuring the integrity of the response. After the extensible claim verification system receives a response (at operation 304), the data workflow 300 may resume operation based on the data provided in the response. For instance, the extensible claim verification system can provide a response to a client device operating the data workflow 300 and, based on that response, the client device may or may not resume operation of the data workflow 300.

[0040] For some embodiments, the extensible claim verification system and the external claim verification service 310 use a unified protocol based on SAML to interact with each other. For instance, using a unified protocol based on SAML 2.0, the extensible claim verification system can redirect a user to the external claim verification service 310 and send the external claim verification service 310 a claim verification request by using a POST or GET method with an *AuthNRequest* request at operation 302, and the external claim verification service 310 can eventually redirect the user back to the extensible claim verification system and send a response to the extensible claim verification system by using use a POST method with a SAML Response at operation 304. Depending on the embodiments, a SAML request or SAML response can comprise values for one or more of the following attributes.

- **Issuer string**: A unique identifier associated with the provider of an external claim verification service (e.g., 310), which can be included in SAML responses.
- **Assertion Consumer URL**: This is where the extensible claim verification system will direct (e.g., redirect) users to start the authentication request.
- **SAML Attribute Name**: This will be the attribute that the extensible claim verification system will look for in the SAML response from an external claim verification service (e.g., 310). This could be, for example, an email address or a simple result code that states a verification pass or fail.
- **Certificate:** This certificate will be used by the extensible claim verification system to verify the signature of a signed SAML response from an external claim verification service (e.g., 310).

[0041] For some embodiments, the extensible claim verification system and the external claim verification service 310 use a unified protocol based on OpenID Connect to interact with each other. For instance, using a unified protocol based on OpenID Connect 1.0, the extensible claim verification system can redirect a user to the external claim verification service 310 and send the external claim verification service 310 a claim verification request by using a GET method with a *redirect_uri* request at operation 302, and the external claim verification service 310 can eventually redirect the user back to the extensible claim verification system and a response to the extensible claim verification system by using use a POST method with a *callback* at operation 304. Depending on the embodiments, the *redirect_uri* request at request operation 302 can comprise a query string with values for one or more of the following example parameters.

- **code**: An authorization code (e.g., OAuth authorization code), which can be used with an authentication token (OAuth token) endpoint of a client device/data workflow to retrieve an access token or ID token.
- **claim_request**: Describes a set of claims (e.g., identity claims) that are being requested for verification by an external claim verification service (e.g., 310). This can comprise a JSON Web Token (JWT) having body with values for one or more of the following attributes:

- **iss** = Identifier associated with the extensible claim verification system.
- **iat** = Issued at timestamp.
- **exp** = Expiration timestamp, for when this JWT should be considered invalid by the external claim verification service (e.g., 310).
- **session_id** = A transaction identifier (e.g., key) for identifying this particular transaction with a request from a client device.
- **requested_claims** = A set of claims that the extensible claim verification system is requesting an external claim verification service (e.g., 310) to verify. For instance, to a request to verify someone's full name of "Darren H K Louie," this attribute set as follows can be used:

```
"requested_claims": {
        "identity_verified_fullname": {
        "essential": true,
        "input_options": [
                {
                        "option_name":
                        "expected_fullname",
                        "option_value": {
                        "string_value": "Darren H K
                        Louie"
                        }
                }
        ]
        }
},
```

The use of a JWT in a request from an extensible claim verification system represents an example of some embodiments using an authentication token embedded with claim identifiers. Depending on the embodiments, the *callback* at operation 304 can comprise values for one or more of the following example parameters:

- **claim_response**: This can be signed by a key (e.g., private key) associated with the external claim verification service (e.g., 310). This can comprise a Jason Web Token (JWT) having body with values for one or more of the following attributes:
    - **claims** = The exact claims that were requested and verified by the external claim verification service (e.g., 310). For instance, in response to the example request described earlier:

```
"claims": {
        "identity_verified_fullname": "Darren H K Louie"
}
```

    - **iat** = Issued at timestamp.
    - **exp** = Expiration of this response and when the extensible claim verification system should consider this response (e.g., to prevent replay attacks).
    - **iss** = Identifier associated with the external claim verification service (e.g., 310).
    - **session_id** = The transaction identifier (e.g., key) associated with the request that this response is responding to, which can mitigate reply attacks and can also mitigate playing a successful claim response against a different session on the client device than the system intended. This transaction identifier can correlate to a matching protected (e.g., signed) session identifier that the system asks that the client device also provide to complete the request.

The use of a JWT in a response from an external claim verification service represents an example of some embodiments using an authentication token embedded with a claim value or a claim verification value.

[0042] Though certain embodiments are described herein as using SAML or OpenID Connect, various embodiments can use different or alternative technologies to implement the methodologies described herein.

[0043] **Figure 4** is a diagram illustrating example data interactions with an example extensible claim verification system 412, according to some embodiments. In particular, **Figure 4** illustrates data interactions between the extensible claim verification system 412 and a data workflow system 410, and the

extensible claim verification system 412 and an external claim verification service system 414. For some embodiments, the external claim verification service system 414 supports or provides an external claim verification service for access and use by the extensible claim verification system 412. The data workflow system 410 can operate or support operation of a data workflow (e.g., an electronic signature or digital certificate workflow) that relies on a set of claims to be verified by an external claim verification service. With respect to the extensible claim verification system 412, the data workflow system 410 could serve as a client device and the external claim verification service system 414 could serve as an external claim verification provider (e.g., external identity verification provider). For some embodiments, the extensible claim verification system 412 is similar to other extensible claim verification systems described herein (e.g., 122 and 200).

[0044] During operation, at operation 420, the data workflow system 410 sends a request to the extensible claim verification system 412 to verify of a set of claims for a particular user by an external claim verification service provided by the external claim verification service system 414. Additionally, the request can include a request to authenticate the particular user for the data workflow system 410, which may permit the particular user to log into the data workflow system 410 and access a particular data workflow. In this way, the extensible claim verification system 412 can serve as an account system/server for handling authentication for the data workflow system 410. In response to the request from the data workflow system 410, the extensible claim verification system 412 can request that the particular user consent to the extensible claim verification system 412, the external claim verification service system 414, or both, accessing data (e.g., claim values) relating to the particular user. Upon the particular user consenting, the extensible claim verification system 412 can proceed with servicing the request.

[0045] For some embodiments, operation 420 involves the data workflow system 410 using a POST method or a GET method to request the extensible claim verification system 412 (through identity/auth endpoint thereof) to authenticate the particular user. Depending on the embodiments, the request can comprise values for one or more of the following example parameters, which can be based on an OpenID Connect:

- **client_id**: An identifier associated with the data workflow system (e.g., 410).
- **redirect_uri**: A redirect universal resource indicator (URI) for the data workflow system (e.g., 410).
- **request**: A request object that describes the particular user being authenticated and specifies a set of claims to be verified via the extensible claim verification system (e.g., 412). The request object can comprise a token (e.g., signed binary-serialized token) with one or more of the following example parameters:
    - **Data Workflow Indentifier(s)**: One or more identifiers associated with a data workflow involving the particular user.
    - **UserId**: Identifier associated with the particular user.
    - **UserSiteId**: A site identifier, in case the same UserID exists in multiple sites.
    - **Issued**: The time at which the token was issued, which can determine when the token expired (e.g., token expires 5 minutes after issuance).
- **claims**: A set of claims that the data workflow system (e.g., 410) is requesting the extensible claim verification system (e.g., 412) to verify using an external claim verification service of the external claim verification service system (e.g., 414). This parameter can be based on to the "claim" of OpenID Connect. Additionally, this parameter can comprise an encoded claim request object, which can comprise one or more of the following example parameters:
    - **Id_token**: An identifier associated with the ID token in which claim values are to be returned.
    - **Claim_name**: An identifier for a claim for which verification is requested. The identifier can comprise, for example, a claim name or label.
    - **Provider**: An identifier associated with the external claim verification service or provider that is being requested to verify the specified claim via the extensible claim verification system (e.g., 412).

The following is an example of how values of these parameters can be stored in a claim request object of operation 420.

```
{
    "id_token": {
        "claim_name": {
            "provider": string,
        }
    }
}
```

[0046] At operation 422, the extensible claim verification system 412 causes the particular user to be directed (redirected) from the extensible claim verification system 412 to the external claim verification service system 414 and, in turn, the external claim verification service system 414 can attempt to authenticate the particular user (e.g., based on user credentials provided by the particular user). The particular user can be directed to the external claim verification service system 414 with a request for the external claim verification service system 414 to verify at least one of the claims (in the set of claims) using an external claim verification provided by the external claim verification service system 414. The particular user can be prompted for consent to use the external claim verification service (e.g., if the service is operated by a third-party relative to the system 414).

[0047] At operation 424, the external claim verification service system 414 and the extensible claim verification system 412 can exchange code (e.g., OAuth authorization codes) for an access token or identifier token. Once the external claim verification service system 414 receives an access/identifier token from the extensible claim verification system 412 (using the exchange code), the external claim verification service system 414 can access APIs (e.g., REST APIs) available on the extensible claim verification system 412, which can permit the verification process on the external claim verification service system 414 to continue.

[0048] At operation 426, the external claim verification service system 414 calls on the extensible claim verification system 412 to continue authentication of the particular user on the extensible claim verification system 412. For instance, the external claim verification service system 414 can call a REST API of the extensible claim verification system 412 (e.g., based on access granted by the

access/identifier token received by operation 424) to complete an authentication challenge on the extensible claim verification system 412.

[0049] At operation 428, the external claim verification service system 414 causes the particular user to be directed (redirected) back from the external claim verification service system 414 to the extensible claim verification system 412. The particular user can be directed back to the extensible claim verification system 412 with a response that comprises at least one claim verification value for at least one claim requested to be verified at operation 422. The response from the external claim verification service system 414 to the extensible claim verification system 412 can comprise an authentication token, which can further be embedded with one or more values that verify the set of claims (specified at operation 422). The authentication token can indicate successful authentication of the particular user by the external claim verification service system 414.

[0050] At operation 430, the extensible claim verification system 412 sends a response to the data workflow system 410 that at least indicates whether the particular user was successfully authenticated by the extensible claim verification system 412. The response can comprise one or more values that verify the set of claims requested for verification at operation 420. Additionally, the response can comprise the values of the set of claims. The extensible claim verification system 412 generates the response (sent at operation 430) based on the response the extensible claim verification system 412 receives from the external claim verification service system 414. For instance, the extensible claim verification system 412 can condition successful authentication of the particular user by the extensible claim verification system 412 on whether the response from the external claim verification service system 414 (at operation 428) indicates that authentication of the particular user was successful by the external claim verification service system 414, or whether the set of claims (requested for verification at operation 422) was successfully verified by the external claim verification service system 414. Additionally, at least one of the values verifying the set of claims can originate from a value provided in the response from the external claim verification service system 414 to the extensible claim verification system 412 (at operation 428). The response from the extensible claim verification system 412 to the data workflow system 410 can comprise an

authentication token, which can further be embedded with one or more values that verify the set of claims (specified at operation 420). The authentication token can indicate successful authentication of the particular user by the extensible claim verification system 412, and can be configured to authenticate the particular user at the data workflow system 410.

[0051] For some embodiments, operation 430 involves the extensible claim verification system 412 using a POST method to send a response comprising an authentication/identifier token to the data workflow system 410 to authenticate the particular user at the data workflow system 410. Depending on the embodiments, the token can comprise values for one or more of the following parameters, which can be based on an OpenID Connect ID Token:

- **claim_name**: An identifier for a claim for which a verification response is provided. The identifier can comprise, for example, a claim name or label.
- **value**: A value or verification value provided (e.g., by the external claim verification service of system 414) for the claim specified by **claim_name**.
- **provider**: An identifier associated with the external claim verification service or provider that provides verification of the specified claim via the extensible claim verification system (e.g., 412).
- **acquired_time**: Timestamp at which the claim value or claim verification value was obtained from the external claim verification service via the extensible claim verification system (e.g., 412).

The following is an example of how values of these parameters can be stored in a response of operation 430.

```
"claim_name":
{
        "value": value,
        "provider": "string",
        "acquired_time": uint
}
```

[0052] **Figures 5** and **6** are flowcharts illustrating example methods for extensible claim verification, according to some embodiments. It will be understood that example methods described herein can be performed by a machine in accordance with some embodiments. For example, any one of the methods 500, 600 can be

performed by the extensible claim verification system 200 described above with respect to **Figure 2**. An operation of various methods described herein can be performed by a hardware processor (e.g., a central processing unit or graphics processing unit) of a computing device (e.g., a desktop, server, laptop, mobile phone, tablet, etc.), which can be part of a computing system based on a cloud architecture. Example methods described herein may also be implemented in the form of executable instructions stored on a machine-readable medium or in the form of electronic circuitry. For instance, the operations of a method 500 of **Figure 5** can be represented by executable instructions that, when executed by a processor of a computing device, cause the computing device to perform the method 500. Depending on the embodiment, an operation of an example method described herein can be repeated in different ways or involve intervening operations not shown. Though the operations of example methods can be depicted and described in a certain order, the order in which the operations are performed may vary among embodiments, including performing certain operations in parallel.

[0053] Referring now to **Figure 5**, the method 500 begins with operation 502 receiving, at the extensible claim verification system (e.g., 200), user input data from a client device, where the user input data can relate to adding (or removing) access of an external claim verification service (e.g., provided by the external claim verification service system 126) by an extensible claim verification system. According to some embodiments, the extensible claim verification system (e.g., 200) presents a user with a graphical user interface, such as one similar to a graphical user interface 700 illustrated by **Figure 7**. Subsequently, at operation 504, the extensible claim verification system (e.g., 200) can configure access to the external claim verification service (e.g., of 126) based on the user input data.

[0054] At operation 506, the extensible claim verification system (e.g., 200) receives a request from a client device (e.g., one different from the client device involved in operation 502) for verifying a set of claims for a user. According to some embodiments, a claim of the set of claims comprises an asserted data value regarding the user that is to be verified by the external electronic claim verification service. The data value can represent an assert of information regarding the user, such as identity information (e.g., social security number, passport number, etc.)

or residential user. For some embodiments, the request is associated with an electronic signature or digital certificate workflow operating on the client device, such as a data workflow for the user to electronically sign a document.

[0055] In response to the request, at operation 508, the extensible claim verification system (e.g., 200) causes the user to be directed (e.g., redirected) to the external claim verification service based on the configured access to verify the set of claims. The external electronic claim verification service can cause the user to perform a set of actions (e.g., steps with respect to the external electronic verification service) to verify the set of claims for the user. For some embodiments, causing the user to be directed to the external electronic claim verification service comprises using a universal resource locator-based redirection to the external electronic claim verification service. Additionally, for some embodiments, causing the user to be directed to the external electronic claim verification service comprises providing the external electronic claim verification service with the set of claims to be verified for the user.

[0056] At operation 510, the extensible claim verification system (e.g., 200) receives from the external claim verification service (e.g., of 126) a first response relating to verification of the set of claims. The first response can comprise a claim verification value that indicates whether the asserted data value for a claim (in the set of claims) has been verified (e.g., whether verification was successful or not). For example, the asserted data value can comprise information associated with identifying the user, thereby facilitating identity verification of the user. The first response can comprise a data value for a claim (in the set of claims) specified by the request received at operation 506, thereby enabling the client device to obtain the data value for the claim from the external claim verification service (e.g., of 126). For instance, for a claim regarding the e-mail address of the user, the first response can comprise a data value that specifies a verified e-mail address of the user. Additionally, the first response can comprise a result of the user authenticating with the external electronic claim verification service (e.g., of 126). For some embodiments, the first response comprises an authentication token, such as an access token or an ID token generated by a user authenticating with the external electronic claim verification service. Additionally, for some embodiments, the authentication token of the first response is embedded with a

claim value or a claim verification value for at least one claim in the set of claims. For some embodiments, the first response is signed by the external claim verification service (e.g., using a private key of the external claim verification service). Additionally, for some embodiments, the transaction identifier is used to store data that has been verified based on the first response, thereby providing persistent evidence that proves that the verification has occurred.

[0057] At operation 512, the extensible claim verification system (e.g., 200) provides (e.g., sends) to the client device a second response based on the first response received at operation 506. Where the first response (at operation 506) comprises a claim verification value (e.g., verification passed or failed, or copy of the value of a claim) for at least one claim in the set of claims, the second response provided to the client device (at operation 512) can comprise the claim verification value for the at least one claim in the set of claims. For some embodiments, the second response is signed by the extensible claim verification system (e.g., using a private key of the extensible claim verification system). For some embodiments, the second response comprises an authentication token, such as an access token or an ID token generated by a user authenticating with the extensible claim verification system (e.g., 200). Further, for some embodiments, the authentication token of the second response is embedded with a claim verification value for at least one claim in the set of claims (as provided from the first response from the external electronic claim verification service). The authentication token of the second response can be configured to authenticate the user at the client device, which in turn can facilitate authenticated access by the user of a data workflow operating on the client device. For some embodiments, the second response is signed by the external claim verification service (e.g., using a private key of the extensible claim verification system).

[0058] Referring now to the **Figure 6**, the method 600 begins with operations 602 through 606, which, according to some embodiments, are respectively similar to operations 502 through 506 described above with respect to the method 500 of **Figure 5**. The method 600 continues with operation 608, where in response to the request received at operation 606, the extensible claim verification system (e.g., 200) generates a transaction identifier (ID) associated with the received request. The transaction identifier can be generated based on an identifier associated with

a data workflow (operating on the client device) that is relying on a response (second response provided at operation 618) from the extensible claim verification system (e.g., 200).

[0059] According to some embodiments, the extensible claim verification system (e.g., 200) logs, in a data structure (e.g., database), information regarding a set of operations performed by the extensible claim verification system (e.g., 200) in response to the received request at operation 606. The transaction information logged in the data structure can comprise the transaction identifier generated at operation 608 in associated with the request. Additionally, the transaction information logged in the data structure can comprise a requester client identifier associated with the client device (that sent the request received at operation 606) and an external claim verification service identifier associated with the external claim verification service identifier (to which access was configured at operation 604). Depending on the embodiment, the information stored within the data structure can be used for auditing operations performed by the extensible claim verification system. The following illustrates the structure of an example of a table that can be stored within the data structure.

Column Name	**Type**	**Description**
EntryId	Guid	The primary key for the table
TransactionId	String	The transaction ID that this audit entry is for
RequestorClientId	Guid	The client ID of the requesting client
ClaimId	Integer	The foreign key of the external claim being requested
ClaimProviderId	Guid	The client ID of the external claim provider
UserId	Guid	The user ID of the user being authenticated
EventTime	DateTime	The UTC DateTime of the audit event

[0060] At operation 610, the extensible claim verification system (e.g., 200) requests consent from the user to access the external electronic claim verification service (e.g., of 126) in connection with verifying the set of claims for the user. For some embodiments, the consent is facilitated by the extensible claim verification system (e.g., 200) presenting the user with a graphical user interface that solicits the user's permission to use the external electronic claim verification service to verify the set of claims or access, which can involve the external

electronic claim verification service accessing data (e.g., identity data) associated with the user.

[0061] The method 600 continues with operations 612 and 614, which, according to some embodiments, are respectively similar to operations 508 and 510 described above with respect to the method 500 of **Figure 5**. At operation 616, the extensible claim verification system (e.g., 200) determines whether to enable a lockout status of the request based on the first response received at operation 614. For some embodiments, the determining at operation 616 comprises determining whether the first response (received at operation 606) indicates that the user failed to access the external electronic claim verification service. In response to determining that the first response indicates that the user failed to access the external electronic claim verification service, the extensible claim verification system (e.g., 200) can determine whether the user transgressed a lockout threshold for accessing the external electronic claim verification service, and if so (e.g., attempts to verify the set of claims have been exhausted), may enable a lockout status for the request. Once the lockout status of the request is enabled, the extensible claim verification system (e.g., 200) can prevent a user from further attempts to verify the set of claims via the external electronic claim verification service (e.g., of 126). Additionally, if the external electronic claim verification service (e.g., of 126) sends the first response (received at operation 614) after the lockout status is enabled, the extensible claim verification system (e.g., 200) can ignore the first response. Depending on the embodiment, the lockout threshold can be associated with the request received at operation 606. For instance, based on a transaction identifier, the extensible claim verification system (e.g., 200) can track how many attempts to verify claims are performed for a given request (received at operation 606), and each transaction identifier is allowed a configurable number of attempts to verify the set of claims. Alternatively, or additionally, the lockout threshold can be associated with the external electronic claim verification service (e.g., of 126). For instance, the lockout threshold can be based on a limit intended to throttle (e.g., over a period of time, such an hour or a day) how many requests to verify a claim are sent to a particular external electronic claim verification service.

[0062] The method 600 continues with operation 618, which, according to some embodiments, is respectively similar to operation 512 described above with respect to the method 500 of **Figure 5**.

[0063] **Figure 7** presents a screen shot of an example graphical user interface (GUI) 700 for managing one or more external claim verification services, according to some embodiments. The GUI 700 can be one generated or otherwise presented by an extensible claim verification system (e.g., 200) to add or remove access to an external claim verification service by the extensible claim verification system. As shown, the GUI 700 comprises a listing of identity (ID) verification workflows (ID verification workflows 1, 2, and 3) configured on an extensible claim verification system (e.g., 122, 200), each of which is configured with access to an external claim verification service (external ID verification services 1, 2, and 3 respectively) and associated with an electronic signature or digital certificate workflow. As shown, a graphical button 702 can permit a user to add a new ID verification workflow that has configured access to an external claim verification service, as described herein. As also shown, a graphical element 704 can permit a user to edit, deactivate, or remove an ID verification workflow listed on the GUI 700. The GUI 700 presents a status (e.g., active/inactivate) for each ID verification workflow.

[0064] Various embodiments described herein can be implemented by way of the example software architecture illustrated by and described with respect to **Figure 8** or by way of the example machine illustrated by and described with respect to **Figure 9**.

[0065] **Figure 8** is a block diagram illustrating an example of a software architecture 802 that can be installed on a machine, according to some example embodiments. **Figure 8** is merely a non-limiting example of a software architecture, and it will be appreciated that many other architectures can be implemented to facilitate the functionality described herein. The software architecture 802 can be executing on hardware such as a machine 900 of **Figure 9** that includes, among other things, processors 910, memory 930, and I/O components 950. A representative hardware layer 804 is illustrated and can represent, for example, the machine 900 of **Figure 9**. The representative hardware layer 804 comprises one or more processing units 806 having associated

executable instructions 808. The executable instructions 808 represent the executable instructions of the software architecture 802, including implementation of the methods, modules, and so forth of **Figures 1-6**. The hardware layer 804 also includes memory or storage modules 810, which also have the executable instructions 808. The hardware layer 804 may also comprise other hardware 812, which represents any other hardware of the hardware layer 804, such as the other hardware illustrated as part of the machine 900.

[0066] In the example architecture of **Figure 8**, the software architecture 802 can be conceptualized as a stack of layers, where each layer provides particular functionality. For example, the software architecture 802 may include layers such as an operating system 814, libraries 816, frameworks/middleware 818, applications 820, and a presentation layer 844. Operationally, the applications 820 or other components within the layers may invoke API calls 824 through the software stack and receive a response, returned values, and so forth (illustrated as messages 826) in response to the API calls 824. The layers illustrated are representative in nature, and not all software architectures have all layers. For example, some mobile or special-purpose operating systems may not provide a frameworks/middleware 818 layer, while others may provide such a layer. Other software architectures may include additional or different layers.

[0067] The operating system 814 may manage hardware resources and provide common services. The operating system 814 may include, for example, a kernel 828, services 830, and drivers 832. The kernel 828 may act as an abstraction layer between the hardware and the other software layers. For example, the kernel 828 can be responsible for memory management, processor management (e.g., scheduling), component management, networking, security settings, and so on. The services 830 may provide other common services for the other software layers. The drivers 832 can be responsible for controlling or interfacing with the underlying hardware. For instance, the drivers 832 may include display drivers, camera drivers, Bluetooth® drivers, flash memory drivers, serial communication drivers (e.g., Universal Serial Bus (USB) drivers), Wi-Fi® drivers, audio drivers, power management drivers, and so forth depending on the hardware configuration.

[0068] The libraries 816 may provide a common infrastructure that can be utilized by the applications 820 and/or other components and/or layers. The libraries 816 typically provide functionality that allows other software modules to perform tasks in an easier fashion than by interfacing directly with the underlying operating system 814 functionality (e.g., kernel 828, services 830, or drivers 832). The libraries 816 may include system libraries 834 (e.g., C standard library) that may provide functions such as memory allocation functions, string manipulation functions, mathematic functions, and the like. In addition, the libraries 816 may include API libraries 836 such as media libraries (e.g., libraries to support presentation and manipulation of various media formats such as MPEG4, H.264, MP3, AAC, AMR, JPG, and PNG), graphics libraries (e.g., an OpenGL framework that can be used to render 2D and 3D graphic content on a display), database libraries (e.g., SQLite that may provide various relational database functions), web libraries (e.g., WebKit that may provide web browsing functionality), and the like. The libraries 816 may also include a wide variety of other libraries 838 to provide many other APIs to the applications 820 and other software components/modules.

[0069] The frameworks 818 (also sometimes referred to as middleware) may provide a higher-level common infrastructure that can be utilized by the applications 820 or other software components/modules. For example, the frameworks 818 may provide various graphic user interface (GUI) functions, high-level resource management, high-level location services, and so forth. The frameworks 818 may provide a broad spectrum of other APIs that can be utilized by the applications 820 and/or other software components/modules, some of which can be specific to a particular operating system or platform.

[0070] The applications 820 include built-in applications 840 and/or third-party applications 842. Examples of representative built-in applications 840 may include, but are not limited to, a home application, a contacts application, a browser application, a book reader application, a location application, a media application, a messaging application, or a game application.

[0071] The third-party applications 842 may include any of the built-in applications 840, as well as a broad assortment of other applications. In a specific example, the third-party applications 842 (e.g., an application developed using the

Android™ or iOS™ software development kit (SDK) by an entity other than the vendor of the particular platform) can be mobile software running on a mobile operating system such as iOS™, Android™, Windows® Phone, or other mobile operating systems. In this example, the third-party applications 842 may invoke the API calls 824 provided by the mobile operating system such as the operating system 814 to facilitate functionality described herein.

[0072] The applications 820 may utilize built-in operating system functions (e.g., kernel 828, services 830, or drivers 832), libraries (e.g., system libraries 834, API libraries 836, and other libraries 838), or frameworks/middleware 818 to create user interfaces to interact with users of the system. Alternatively, or additionally, in some systems, interactions with a user may occur through a presentation layer, such as the presentation layer 844. In these systems, the application/module "logic" can be separated from the aspects of the application/module that interact with the user.

[0073] Some software architectures utilize virtual machines. In the example of **Figure 8**, this is illustrated by a virtual machine 848. The virtual machine 848 creates a software environment where applications/modules can execute as if they were executing on a hardware machine (e.g., the machine 900 of **Figure 9**). The virtual machine 848 is hosted by a host operating system (e.g., the operating system 814) and typically, although not always, has a virtual machine monitor 846, which manages the operation of the virtual machine 848 as well as the interface with the host operating system (e.g., the operating system 814). A software architecture executes within the virtual machine 848, such as an operating system 850, libraries 852, frameworks/middleware 854, applications 856, or a presentation layer 858. These layers of software architecture executing within the virtual machine 848 can be the same as corresponding layers previously described or can be different.

[0074] **Figure 9** illustrates a diagrammatic representation of a machine 900 in the form of a computer system within which a set of instructions can be executed for causing the machine 900 to perform any one or more of the methodologies discussed herein, according to an embodiment. Specifically, **Figure 9** shows a diagrammatic representation of the machine 900 in the example form of a computer system, within which instructions 916 (e.g., software, a program, an

application, an applet, an app, or other executable code) for causing the machine 900 to perform any one or more of the methodologies discussed herein can be executed. For example, the instructions 916 may cause the machine 900 to execute any one of methods 500, 600 described above with respect to **Figures 5** and **6**. Additionally, or alternatively, the instructions 916 may implement the extensible claim verification systems of **Figures 1** and **2**. The instructions 916 transform the general, non-programmed machine 900 into a particular machine 900 programmed to carry out the described and illustrated functions in the manner described. In alternative embodiments, the machine 900 operates as a standalone device or can be coupled (e.g., networked) to other machines. In a networked deployment, the machine 900 may operate in the capacity of a server machine or a client machine in a server-client network environment, or as a peer machine in a peer-to-peer (or distributed) network environment. The machine 900 may comprise, but not be limited to, a server computer, a client computer, a personal computer (PC), a tablet computer, a laptop computer, a netbook, a set-top box (STB), a personal digital assistant (PDA), an entertainment media system, a cellular telephone, a smart phone, a mobile device, a wearable device (e.g., a smart watch), a smart home device (e.g., a smart appliance), other smart devices, a web appliance, a network router, a network switch, a network bridge, or any machine capable of executing the instructions 916, sequentially or otherwise, that specify actions to be taken by the machine 900. Further, while only a single machine 900 is illustrated, the term "machine" shall also be taken to include a collection of machines 900 that individually or jointly execute the instructions 916 to perform any one or more of the methodologies discussed herein.

[0075] The machine 900 may include processors 910, memory 930, and I/O components 950, which can be configured to communicate with each other such as via a bus 902. In an embodiment, the processors 910 (e.g., a central processing unit (CPU), a reduced instruction set computing (RISC) processor, a complex instruction set computing (CISC) processor, a graphics processing unit (GPU), a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a radio-frequency integrated circuit (RFIC), another processor, or any suitable combination thereof) may include, for example, a processor 912 and a processor 914 that may execute the instructions 916. The term "processor" is intended to

include multi-core processors that may comprise two or more independent processors (sometimes referred to as "cores") that may execute instructions contemporaneously. Although **Figure 9** shows multiple processors 910, the machine 900 may include a single processor with a single core, a single processor with multiple cores (e.g., a multi-core processor), multiple processors with a single core, multiple processors with multiples cores, or any combination thereof.

[0076] The memory 930 may include a main memory 932, a static memory 934, and a storage unit 936 including machine-readable medium 938, each accessible to the processors 910 such as via the bus 902. The main memory 932, the static memory 934, and the storage unit 936 store the instructions 916 embodying any one or more of the methodologies or functions described herein. The instructions 916 may also reside, completely or partially, within the main memory 932, within the static memory 934, within the storage unit 936, within at least one of the processors 910 (e.g., within the processor's cache memory), or any suitable combination thereof, during execution thereof by the machine 900.

[0077] The I/O components 950 may include a wide variety of components to receive input, provide output, produce output, transmit information, exchange information, capture measurements, and so on. The specific I/O components 950 that are included in a particular machine will depend on the type of machine. For example, portable machines such as mobile phones will likely include a touch input device or other such input mechanisms, while a headless server machine will likely not include such a touch input device. It will be appreciated that the I/O components 950 may include many other components that are not shown in **Figure 9**. The I/O components 950 are grouped according to functionality merely for simplifying the following discussion, and the grouping is in no way limiting. In various embodiments, the I/O components 950 may include output components 952 and input components 954. The output components 952 may include visual components (e.g., a display such as a plasma display panel (PDP), a light-emitting diode (LED) display, a liquid crystal display (LCD), a projector, or a cathode ray tube (CRT)), acoustic components (e.g., speakers), haptic components (e.g., a vibratory motor, resistance mechanisms), other signal generators, and so forth. The input components 954 may include alphanumeric input components (e.g., a keyboard, a touch screen configured to receive alphanumeric input, a photo-

optical keyboard, or other alphanumeric input components), point-based input components (e.g., a mouse, a touchpad, a trackball, a joystick, a motion sensor, or another pointing instrument), tactile input components (e.g., a physical button, a touch screen that provides location and/or force of touches or touch gestures, or other tactile input components), audio input components (e.g., a microphone), and the like.

[0078] In further embodiments, the I/O components 950 may include biometric components 956, motion components 958, environmental components 960, or position components 962, among a wide array of other components. For example, the biometric components 956 may include components to detect expressions (e.g., hand expressions, facial expressions, vocal expressions, body gestures, or eye tracking), measure biosignals (e.g., blood pressure, heart rate, body temperature, perspiration, or brain waves), identify a person (e.g., voice identification, retinal identification, facial identification, fingerprint identification, or electroencephalogram-based identification), and the like. The motion components 958 may include acceleration sensor components (e.g., accelerometer), gravitation sensor components, rotation sensor components (e.g., gyroscope), and so forth. The environmental components 960 may include, for example, illumination sensor components (e.g., photometer), temperature sensor components (e.g., one or more thermometers that detect ambient temperature), humidity sensor components, pressure sensor components (e.g., barometer), acoustic sensor components (e.g., one or more microphones that detect background noise), proximity sensor components (e.g., infrared sensors that detect nearby objects), gas sensors (e.g., gas detection sensors to detect concentrations of hazardous gases for safety or to measure pollutants in the atmosphere), or other components that may provide indications, measurements, or signals corresponding to a surrounding physical environment. The position components 962 may include location sensor components (e.g., a Global Positioning System (GPS) receiver component), altitude sensor components (e.g., altimeters or barometers that detect air pressure from which altitude can be derived), orientation sensor components (e.g., magnetometers), and the like.

[0079] Communication can be implemented using a wide variety of technologies. The I/O components 950 may include communication components 964 operable

to couple the machine 900 to a network 980 or devices 970 via a coupling 982 and a coupling 972, respectively. For example, the communication components 964 may include a network interface component or another suitable device to interface with the network 980. In further examples, the communication components 964 may include wired communication components, wireless communication components, cellular communication components, near field communication (NFC) components, Bluetooth® components (e.g., Bluetooth® Low Energy), Wi-Fi® components, and other communication components to provide communication via other modalities. The devices 970 can be another machine or any of a wide variety of peripheral devices (e.g., a peripheral device coupled via a USB).

[0080] Moreover, the communication components 964 may detect identifiers or include components operable to detect identifiers. For example, the communication components 964 may include radio frequency identification (RFID) tag reader components, NFC smart tag detection components, optical reader components (e.g., an optical sensor to detect one-dimensional bar codes such as Universal Product Code (UPC) bar code, multi-dimensional bar codes such as Quick Response (QR) code, Aztec code, Data Matrix, Dataglyph, MaxiCode, PDF417, Ultra Code, UCC RSS-2D bar code, and other optical codes), or acoustic detection components (e.g., microphones to identify tagged audio signals). In addition, a variety of information can be derived via the communication components 964, such as location via Internet Protocol (IP) geolocation, location via Wi-Fi® signal triangulation, location via detecting an NFC beacon signal that may indicate a particular location, and so forth.

[0081] Certain embodiments are described herein as including logic or a number of components, modules, elements, or mechanisms. Such modules can constitute either software modules (e.g., code embodied on a machine-readable medium or in a transmission signal) or hardware modules. A "hardware module" is a tangible unit capable of performing certain operations and can be configured or arranged in a certain physical manner. In various example embodiments, one or more computer systems (e.g., a standalone computer system, a client computer system, or a server computer system) or one or more hardware modules of a computer system (e.g., a processor or a group of processors) are configured by software

(e.g., an application or application portion) as a hardware module that operates to perform certain operations as described herein.

[0082] In some embodiments, a hardware module is implemented mechanically, electronically, or any suitable combination thereof. For example, a hardware module can include dedicated circuitry or logic that is permanently configured to perform certain operations. For example, a hardware module can be a special-purpose processor, such as a field-programmable gate array (FPGA) or an application-specific integrated circuit (ASIC). A hardware module may also include programmable logic or circuitry that is temporarily configured by software to perform certain operations. For example, a hardware module can include software encompassed within a general-purpose processor or other programmable processor. It will be appreciated that the decision to implement a hardware module mechanically, in dedicated and permanently configured circuitry, or in temporarily configured circuitry (e.g., configured by software) can be driven by cost and time considerations.

[0083] Accordingly, the phrase "module" should be understood to encompass a tangible entity, be that an entity that is physically constructed, permanently configured (e.g., hardwired), or temporarily configured (e.g., programmed) to operate in a certain manner or to perform certain operations described herein. Considering embodiments in which hardware modules are temporarily configured (e.g., programmed), each of the hardware modules need not be configured or instantiated at any one instance in time. For example, where a hardware module comprises a general-purpose processor configured by software to become a special-purpose processor, the general-purpose processor can be configured as respectively different special-purpose processors (e.g., comprising different hardware modules) at different times. Software can accordingly configure a particular processor or processors, for example, to constitute a particular hardware module at one instance of time and to constitute a different hardware module at a different instance of time.

[0084] Hardware modules can provide information to, and receive information from, other hardware modules. Accordingly, the described hardware modules can be regarded as being communicatively coupled. Where multiple hardware modules exist contemporaneously, communications can be achieved through

signal transmission (e.g., over appropriate circuits and buses) between or among two or more of the hardware modules. In embodiments in which multiple hardware modules are configured or instantiated at different times, communications between or among such hardware modules can be achieved, for example, through the storage and retrieval of information in memory structures to which the multiple hardware modules have access. For example, one hardware module performs an operation and stores the output of that operation in a memory device to which it is communicatively coupled. A further hardware module can then, at a later time, access the memory device to retrieve and process the stored output. Hardware modules can also initiate communications with input or output devices, and can operate on a resource (e.g., a collection of information).

[0085] The various operations of example methods described herein can be performed, at least partially, by one or more processors that are temporarily configured (e.g., by software) or permanently configured to perform the relevant operations. Whether temporarily or permanently configured, such processors constitute processor-implemented modules that operate to perform one or more operations or functions described herein. As used herein, "processor-implemented module" refers to a hardware module implemented using one or more processors.

[0086] Similarly, the methods described herein can be at least partially processor-implemented, with a particular processor or processors being an example of hardware. For example, at least some of the operations of a method can be performed by one or more processors or processor-implemented modules. Moreover, the one or more processors may also operate to support performance of the relevant operations in a "cloud computing" environment or as a "software as a service" (SaaS). For example, at least some of the operations can be performed by a group of computers (as examples of machines 900 including processors 910), with these operations being accessible via a network (e.g., the Internet) and via one or more appropriate interfaces (e.g., an API). In certain embodiments, for example, a client device may relay or operate in communication with cloud computing systems and may access circuit design information in a cloud environment.

[0087] The performance of certain of the operations can be distributed among the processors, not only residing within a single machine 900, but deployed across a number of machines 900. In some example embodiments, the processors 910 or processor-implemented modules are located in a single geographic location (e.g., within a home environment, an office environment, or a server farm). In other example embodiments, the processors or processor-implemented modules are distributed across a number of geographic locations.

EXECUTABLE INSTRUCTIONS AND MACHINE STORAGE MEDIUM

[0088] The various memories (i.e., 930, 932, 934, and/or the memory of the processor(s) 910) and/or the storage unit 936 may store one or more sets of instructions 916 and data structures (e.g., software) embodying or utilized by any one or more of the methodologies or functions described herein. These instructions (e.g., the instructions 916), when executed by the processor(s) 910, cause various operations to implement the disclosed embodiments.

[0089] As used herein, the terms "machine-storage medium," "device-storage medium," and "computer-storage medium" mean the same thing and can be used interchangeably. The terms refer to a single or multiple storage devices and/or media (e.g., a centralized or distributed database, and/or associated caches and servers) that store executable instructions 916 and/or data. The terms shall accordingly be taken to include, but not be limited to, solid-state memories, and optical and magnetic media, including memory internal or external to processors. Specific examples of machine-storage media, computer-storage media and/or device-storage media include non-volatile memory, including by way of example semiconductor memory devices, e.g., erasable programmable read-only memory (EPROM), electrically erasable programmable read-only memory (EEPROM), field-programmable gate array (FPGA), and flash memory devices; magnetic disks such as internal hard disks and removable disks; magneto-optical disks; and CD-ROM and DVD-ROM disks. The terms "machine-storage media," "computer-storage media," and "device-storage media" specifically exclude carrier waves, modulated data signals, and other such media, at least some of which are covered under the term "signal medium" discussed below.

TRANSMISSION MEDIUM

[0090] In various embodiments, one or more portions of the network 980 can be an ad hoc network, an intranet, an extranet, a virtual private network (VPN), a local-area network (LAN), a wireless LAN (WLAN), a wide-area network (WAN), a wireless WAN (WWAN), a metropolitan-area network (MAN), the Internet, a portion of the Internet, a portion of the public switched telephone network (PSTN), a plain old telephone service (POTS) network, a cellular telephone network, a wireless network, a Wi-Fi® network, another type of network, or a combination of two or more such networks. For example, the network 980 or a portion of the network 980 may include a wireless or cellular network, and the coupling 982 can be a Code Division Multiple Access (CDMA) connection, a Global System for Mobile communications (GSM) connection, or another type of cellular or wireless coupling. In this example, the coupling 982 may implement any of a variety of types of data transfer technology, such as Single Carrier Radio Transmission Technology (1xRTT), Evolution-Data Optimized (EVDO) technology, General Packet Radio Service (GPRS) technology, Enhanced Data rates for GSM Evolution (EDGE) technology, third Generation Partnership Project (3GPP) including 3G, fourth generation wireless (4G) networks, Universal Mobile Telecommunications System (UMTS), High-Speed Packet Access (HSPA), Worldwide Interoperability for Microwave Access (WiMAX), Long-Term Evolution (LTE) standard, others defined by various standard-setting organizations, other long-range protocols, or other data transfer technology.

[0091] The instructions can be transmitted or received over the network using a transmission medium via a network interface device (e.g., a network interface component included in the communication components) and utilizing any one of a number of well-known transfer protocols (e.g., hypertext transfer protocol (HTTP)). Similarly, the instructions can be transmitted or received using a transmission medium via the coupling (e.g., a peer-to-peer coupling) to the devices 970. The terms "transmission medium" and "signal medium" mean the same thing and can be used interchangeably in this disclosure. The terms "transmission medium" and "signal medium" shall be taken to include any intangible medium that is capable of storing, encoding, or carrying the instructions for execution by the machine, and include digital or analog communications

signals or other intangible media to facilitate communication of such software. Hence, the terms "transmission medium" and "signal medium" shall be taken to include any form of modulated data signal, carrier wave, and so forth. The term "modulated data signal" means a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal.

COMPUTER-READABLE MEDIUM

[0092] The terms "machine-readable medium," "computer-readable medium," and "device-readable medium" mean the same thing and may be used interchangeably in this disclosure. The terms are defined to include both machine-storage media and transmission media. Thus, the terms include both storage devices/media and carrier waves/modulated data signals.

[0093] Throughout this specification, plural instances may implement resources, components, operations, or structures described as a single instance. Although individual operations of one or more methods are illustrated and described as separate operations, one or more of the individual operations may be performed concurrently, and nothing requires that the operations be performed in the order illustrated. Structures and functionality presented as separate components in example configurations may be implemented as a combined structure or component. Similarly, structures and functionality presented as a single component may be implemented as separate components.

[0094] As used herein, the term "or" may be construed in either an inclusive or exclusive sense. The terms "a" or "an" should be read as meaning "at least one," "one or more," or the like. The presence of broadening words and phrases such as "one or more," "at least," "but not limited to," or other like phrases in some instances shall not be read to mean that the narrower case is intended or required in instances where such broadening phrases may be absent. Additionally, boundaries between various resources, operations, modules, engines, and data stores are somewhat arbitrary, and particular operations are illustrated in a context of specific illustrative configurations. Other allocations of functionality are envisioned and may fall within a scope of various embodiments of the present disclosure. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

[0095] It will be understood that changes and modifications may be made to the disclosed embodiments without departing from the scope of the present disclosure. These and other changes or modifications are intended to be included within the scope of the present disclosure.

CLAIMS

What is claimed is:

1. A method comprising:

configuring, by a hardware processor, access to an external electronic claim verification service;

receiving, from a client device, a request for verifying a set of claims for a user, a claim of the set of claims comprising an asserted data value regarding the user that is to be verified by the external electronic claim verification service;

in response to the request:

causing, based on the configured access to the external electronic claim verification service, the user to be directed to the external electronic claim verification service to verify the set of claims for the user, the external electronic claim verification service causing the user to perform a set of actions to verify the set of claims for the user; and

receiving, from the external electronic claim verification service, a first response relating to verification of the set of claims; and

providing, to the client device, a second response based on the first response.

2. The method of claim 1, wherein the set of actions performed by the user comprises:

causing the user to authenticate with the external electronic claim verification service based on a set of user credentials provided by the user.

3. The method of claim 1, wherein the first response comprises a claim verification value that indicates whether the asserted data value has been verified.

4. The method of claim 3, wherein the asserted data value comprises information associated with identifying the user.

5. The method of claim 1, wherein the first response comprises a claim verification value for at least one claim in the set of claims, and the second response comprises the claim verification value for the at least one claim in the set of claims.

6. The method of claim 1, wherein at least one of the first response or the second response is digitally signed.

7. The method of claim 1, wherein the first response comprises a result of the user authenticating with the external electronic claim verification service.

8. The method of claim 1, wherein the causing the user to be directed to the external electronic claim verification service to verify the set of claims for the user comprises:

using a universal resource locator-based redirection to the external electronic claim verification service.

9. The method of claim 1, wherein the causing the user to be directed to the external electronic claim verification service to verify the set of claims for the user comprises:

providing the external electronic claim verification service with the set of claims to be verified for the user.

10. The method of claim 1, wherein the request from the client device is associated with at least one an electronic signature workflow or a digital certificate workflow for the user to electronically sign a document.

11. The method of claim 1, wherein the first response comprises an authentication token embedded with a claim verification value for at least one claim in the set of claims.

12. The method of claim 1, wherein the second response comprises an authentication token embedded with a claim verification value for at least one claim in the set of claims.

13. The method of claim 12, wherein the authentication token of the second response is configured to authenticate the user at the client device.

14. The method of claim 1, further comprising:

generating a transaction identifier associated with the request; and

logging, in a data structure, information regarding a set of operations performed in response to the request, the logged information comprising the transaction identifier.

15. The method of claim 14, wherein the logged information comprises a requester client identifier associated with the client device and an external claim

verification service identifier associated with the external claim verification service identifier.

16. The method of claim 1, further comprising:

in response to the request:

requesting consent from the user to access the external electronic claim verification service in connection with verifying the set of claims for the user.

17. The method of claim 1, further comprising:

after receiving the first response from the external electronic claim verification service:

determining whether the first response indicates that the user failed to access the external electronic claim verification service;

in response to determining that the first response indicates that the user failed to access the external electronic claim verification service:

determining whether the user transgressed a lockout threshold for accessing the external electronic claim verification service; and

in response to the user transgressing the lockout threshold, enabling a lockout status for the request.

18. The method of claim 17, wherein the lockout threshold is associated with the request or the external electronic claim verification service.

19. A system comprising:

a memory storing instructions;

one or more hardware processors communicatively coupled to the memory and configured by the instructions to perform operations comprising:

configuring access to an external electronic claim verification service;

receiving, at the system, a request from a client device for verifying a set of claims for a user, a claim of the set of claims comprising an asserted data value regarding the user that is to be verified by the external electronic claim verification service;

in response to the request:

causing, based on the configured access to the external electronic claim verification service, the user to be directed to the external electronic claim verification service to verify the set of claims for the user, the external electronic claim verification service causing the user to perform a set of actions to verify the set of claims for the user; and

receiving, from the external electronic claim verification service, a first response relating to verification of the set of claims; and

providing, to the client device, a second response based on the first response.

20. A non-transitory computer-readable medium comprising instructions that, when executed by a hardware processor of a device, cause the device to perform operations comprising:

configuring access to an external electronic claim verification service based on user input data;

receiving, from a client device, a request for verifying a set of claims for a user, a claim of the set of claims comprising an asserted data value regarding the user that is to be verified by the external electronic claim verification service;

in response to the request:

causing, based on the configured access to the external electronic claim verification service, the user to be directed to the external electronic claim verification service to verify the set of claims for the user, the external electronic claim verification service causing the user to perform a set of actions to verify the set of claims for the user; and

receiving, from the external electronic claim verification service, a first response relating to verification of the set of claims; and

providing, to the client device, a second response based on the first response.

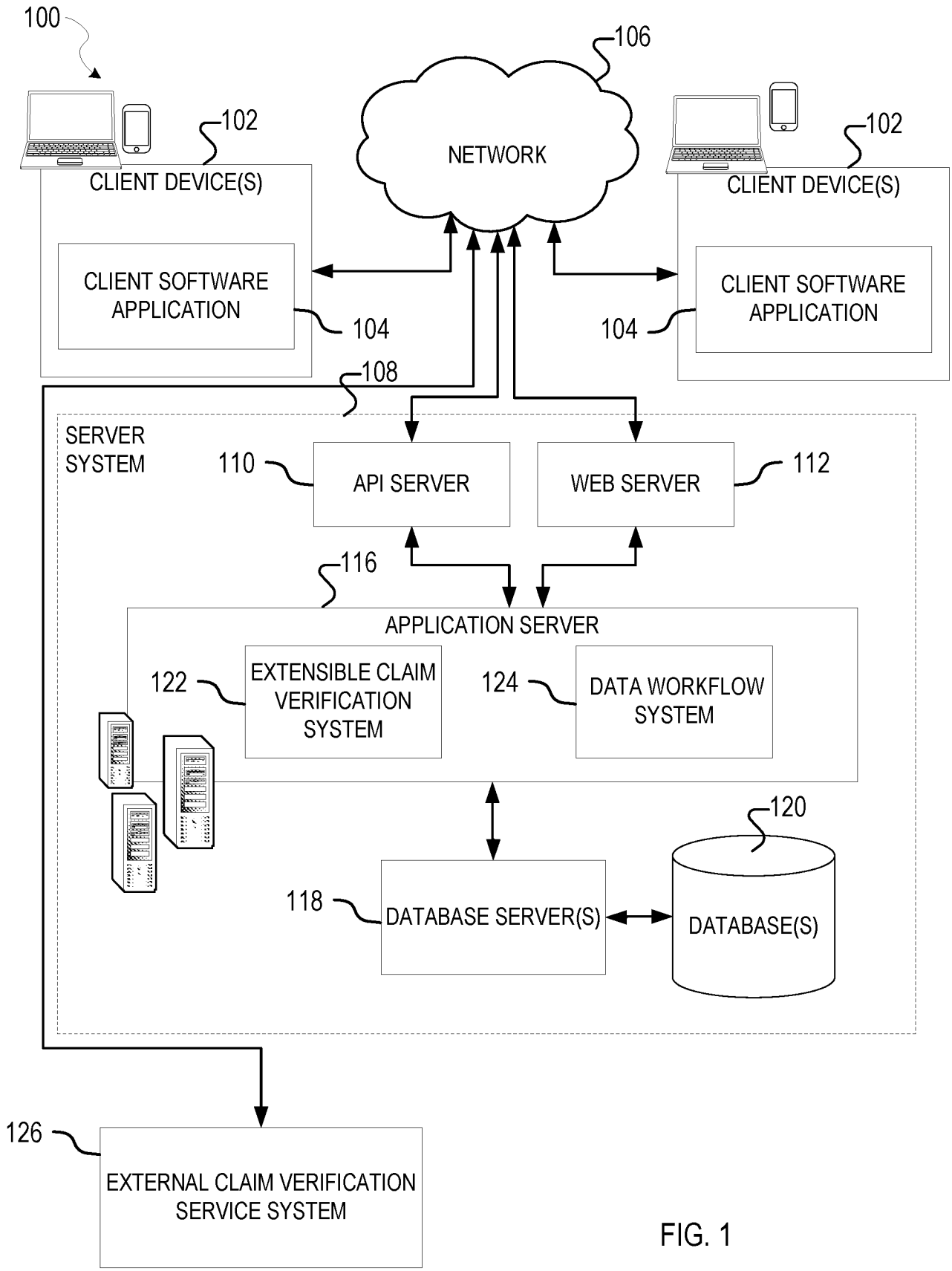

100
106
NETWORK
102
CLIENT DEVICE(S)
CLIENT SOFTWARE APPLICATION
104
102
CLIENT DEVICE(S)
CLIENT SOFTWARE APPLICATION
104
108
SERVER SYSTEM
110
API SERVER
WEB SERVER
112
116
APPLICATION SERVER
122
EXTENSIBLE CLAIM VERIFICATION SYSTEM
124
DATA WORKFLOW SYSTEM
120
118
DATABASE SERVER(S)
DATABASE(S)
126
EXTERNAL CLAIM VERIFICATION SERVICE SYSTEM

FIG. 1

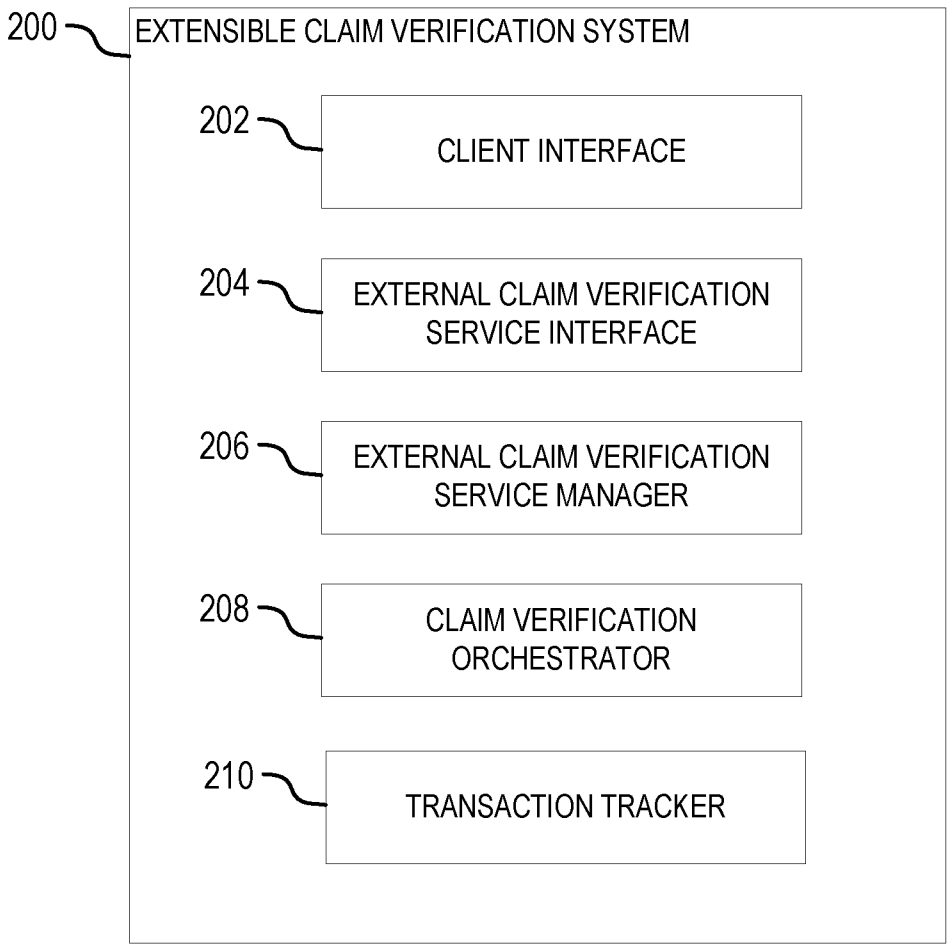

200
EXTENSIBLE CLAIM VERIFICATION SYSTEM
202
CLIENT INTERFACE
204
EXTERNAL CLAIM VERIFICATION SERVICE INTERFACE
206
EXTERNAL CLAIM VERIFICATION SERVICE MANAGER
208
CLAIM VERIFICATION ORCHESTRATOR
210
TRANSACTION TRACKER

FIG. 2

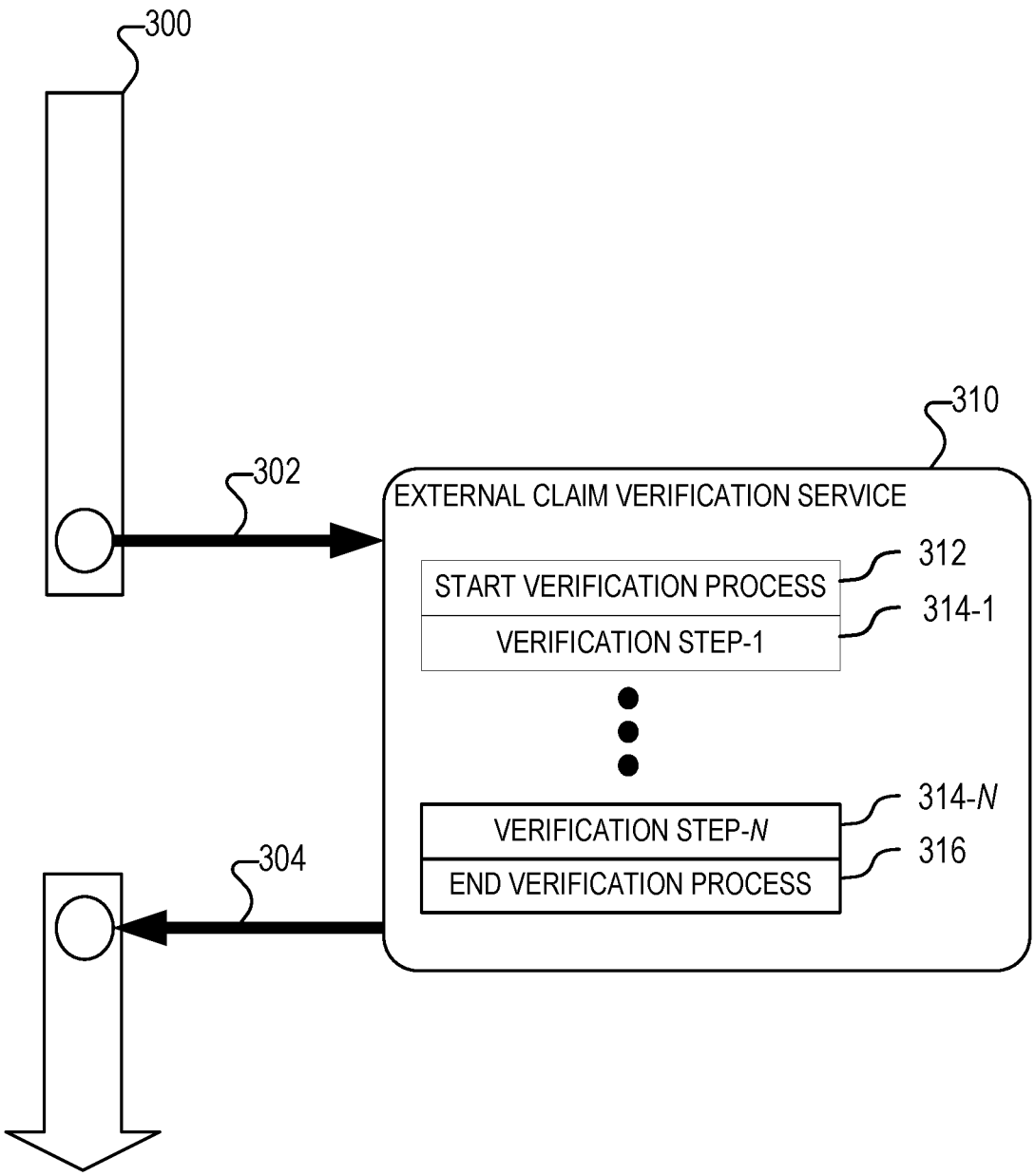

300
302
310
EXTERNAL CLAIM VERIFICATION SERVICE
312
START VERIFICATION PROCESS
314-1
VERIFICATION STEP-1
314-N
VERIFICATION STEP-N
316
END VERIFICATION PROCESS
304

FIG. 3

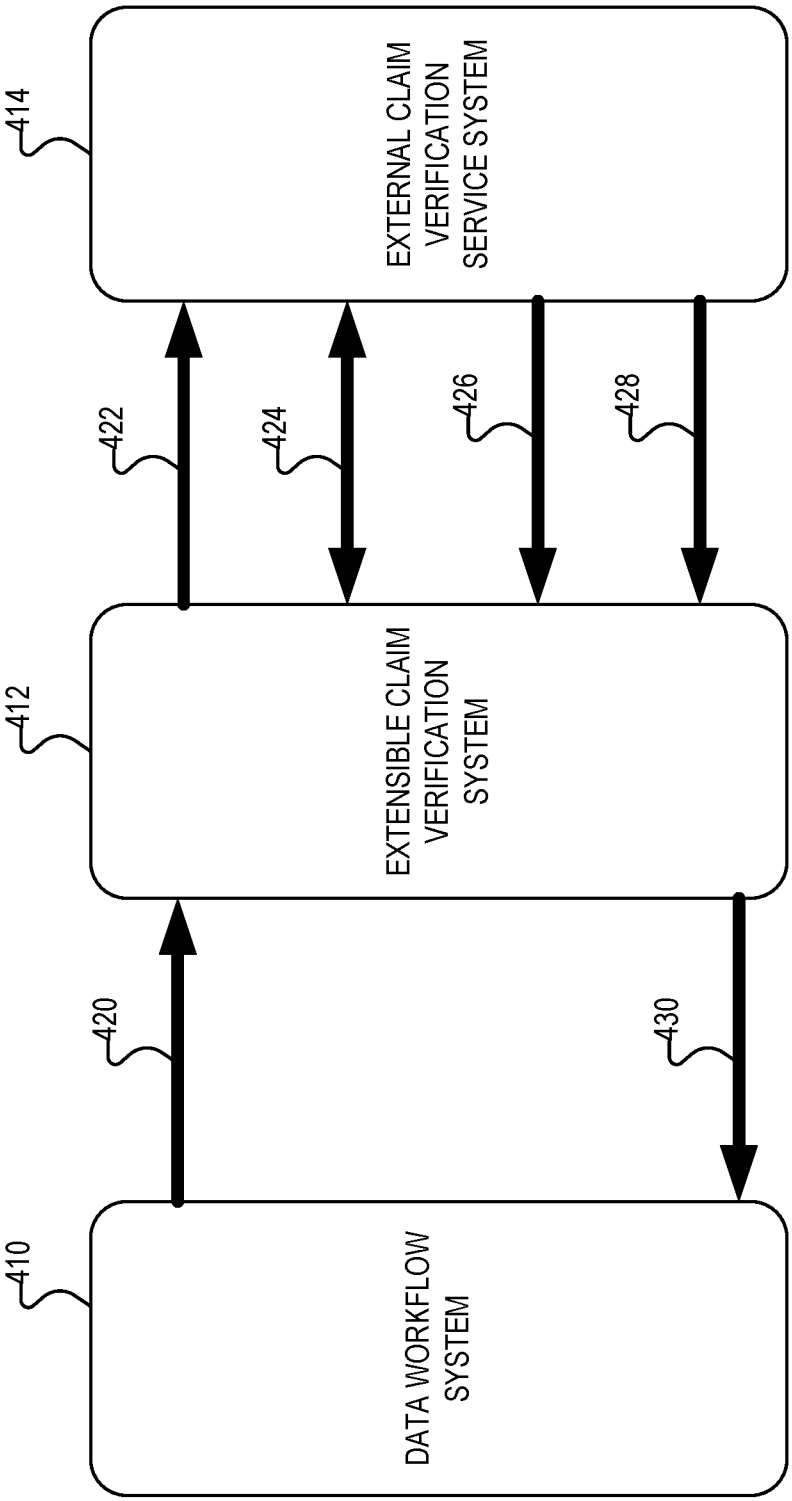

414
EXTERNAL CLAIM VERIFICATION SERVICE SYSTEM
422
424
426
428
412
EXTENSIBLE CLAIM VERIFICATION SYSTEM
420
430
410
DATA WORKFLOW SYSTEM

FIG. 4

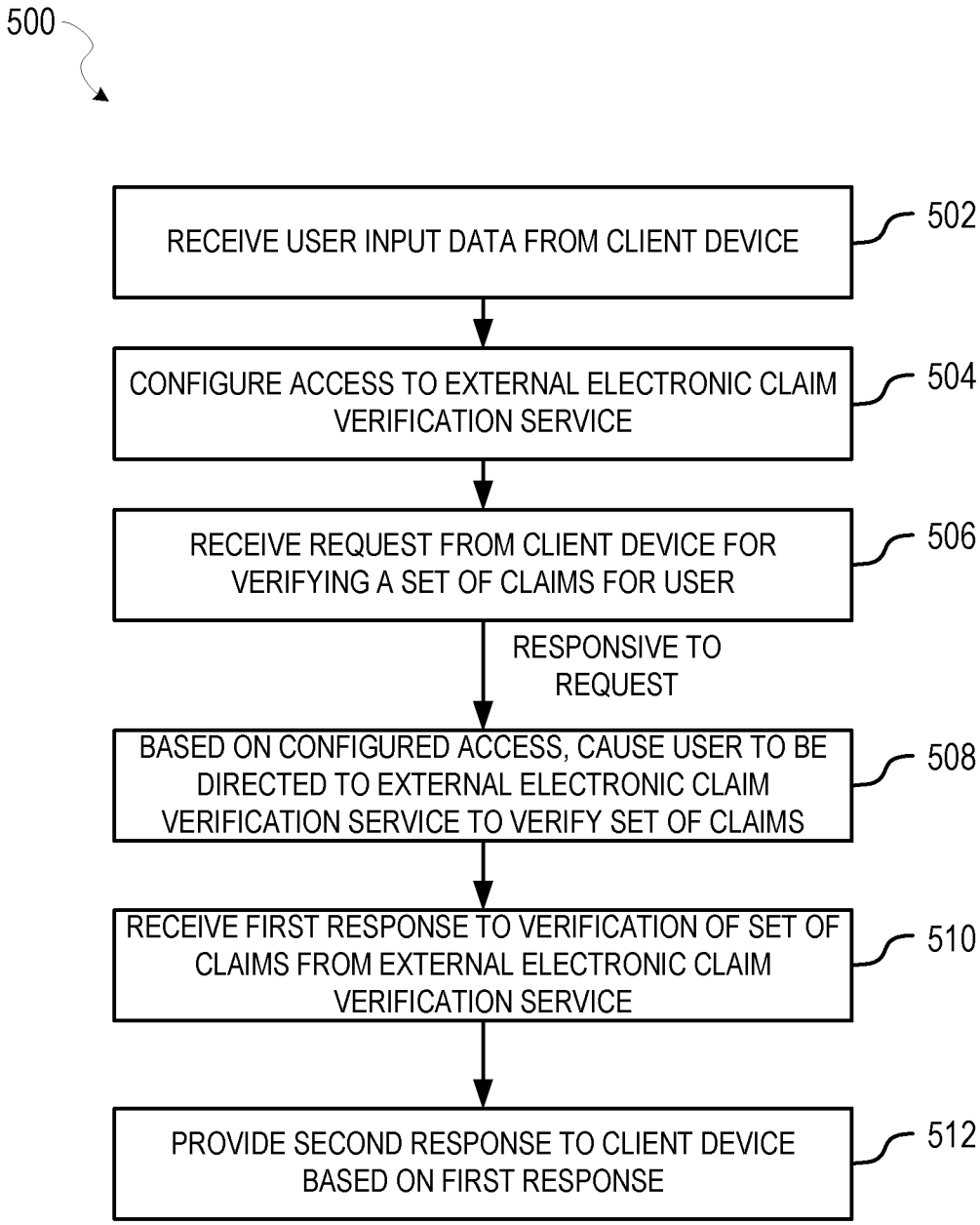

500
RECEIVE USER INPUT DATA FROM CLIENT DEVICE
502
CONFIGURE ACCESS TO EXTERNAL ELECTRONIC CLAIM VERIFICATION SERVICE
504
RECEIVE REQUEST FROM CLIENT DEVICE FOR VERIFYING A SET OF CLAIMS FOR USER
506
RESPONSIVE TO REQUEST
BASED ON CONFIGURED ACCESS, CAUSE USER TO BE DIRECTED TO EXTERNAL ELECTRONIC CLAIM VERIFICATION SERVICE TO VERIFY SET OF CLAIMS
508
RECEIVE FIRST RESPONSE TO VERIFICATION OF SET OF CLAIMS FROM EXTERNAL ELECTRONIC CLAIM VERIFICATION SERVICE
510
PROVIDE SECOND RESPONSE TO CLIENT DEVICE BASED ON FIRST RESPONSE
512

FIG. 5

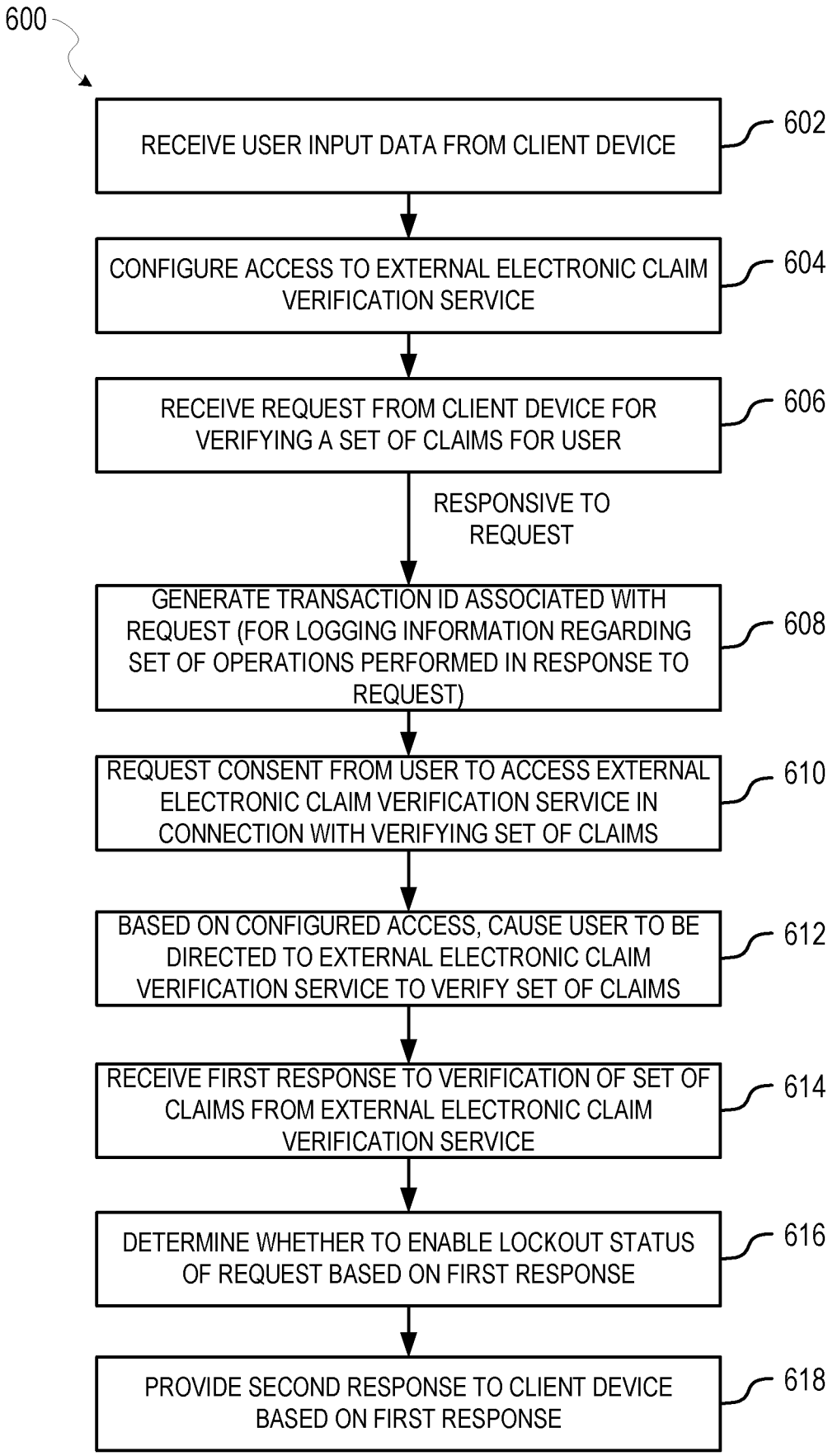

600
RECEIVE USER INPUT DATA FROM CLIENT DEVICE
602
CONFIGURE ACCESS TO EXTERNAL ELECTRONIC CLAIM VERIFICATION SERVICE
604
RECEIVE REQUEST FROM CLIENT DEVICE FOR VERIFYING A SET OF CLAIMS FOR USER
606
RESPONSIVE TO REQUEST
GENERATE TRANSACTION ID ASSOCIATED WITH REQUEST (FOR LOGGING INFORMATION REGARDING SET OF OPERATIONS PERFORMED IN RESPONSE TO REQUEST)
608
REQUEST CONSENT FROM USER TO ACCESS EXTERNAL ELECTRONIC CLAIM VERIFICATION SERVICE IN CONNECTION WITH VERIFYING SET OF CLAIMS
610
BASED ON CONFIGURED ACCESS, CAUSE USER TO BE DIRECTED TO EXTERNAL ELECTRONIC CLAIM VERIFICATION SERVICE TO VERIFY SET OF CLAIMS
612
RECEIVE FIRST RESPONSE TO VERIFICATION OF SET OF CLAIMS FROM EXTERNAL ELECTRONIC CLAIM VERIFICATION SERVICE
614
DETERMINE WHETHER TO ENABLE LOCKOUT STATUS OF REQUEST BASED ON FIRST RESPONSE
616
PROVIDE SECOND RESPONSE TO CLIENT DEVICE BASED ON FIRST RESPONSE
618

FIG. 6

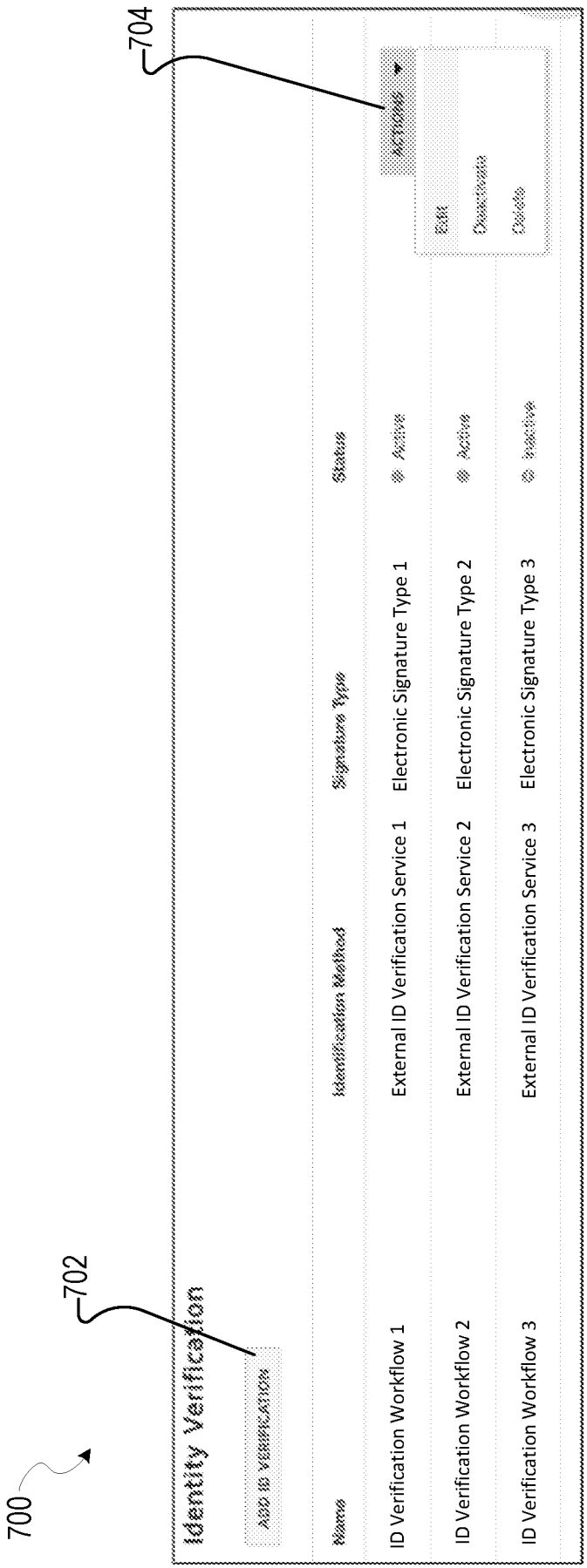

700
702
704
Identity Verification
Add ID Verification
Name
Identification Method
Signature Type
Status
Actions
ID Verification Workflow 1
External ID Verification Service 1
Electronic Signature Type 1
Active
Edit
Deactivate
Delete
ID Verification Workflow 2
External ID Verification Service 2
Electronic Signature Type 2
Active
ID Verification Workflow 3
External ID Verification Service 3
Electronic Signature Type 3
Inactive

FIG. 7

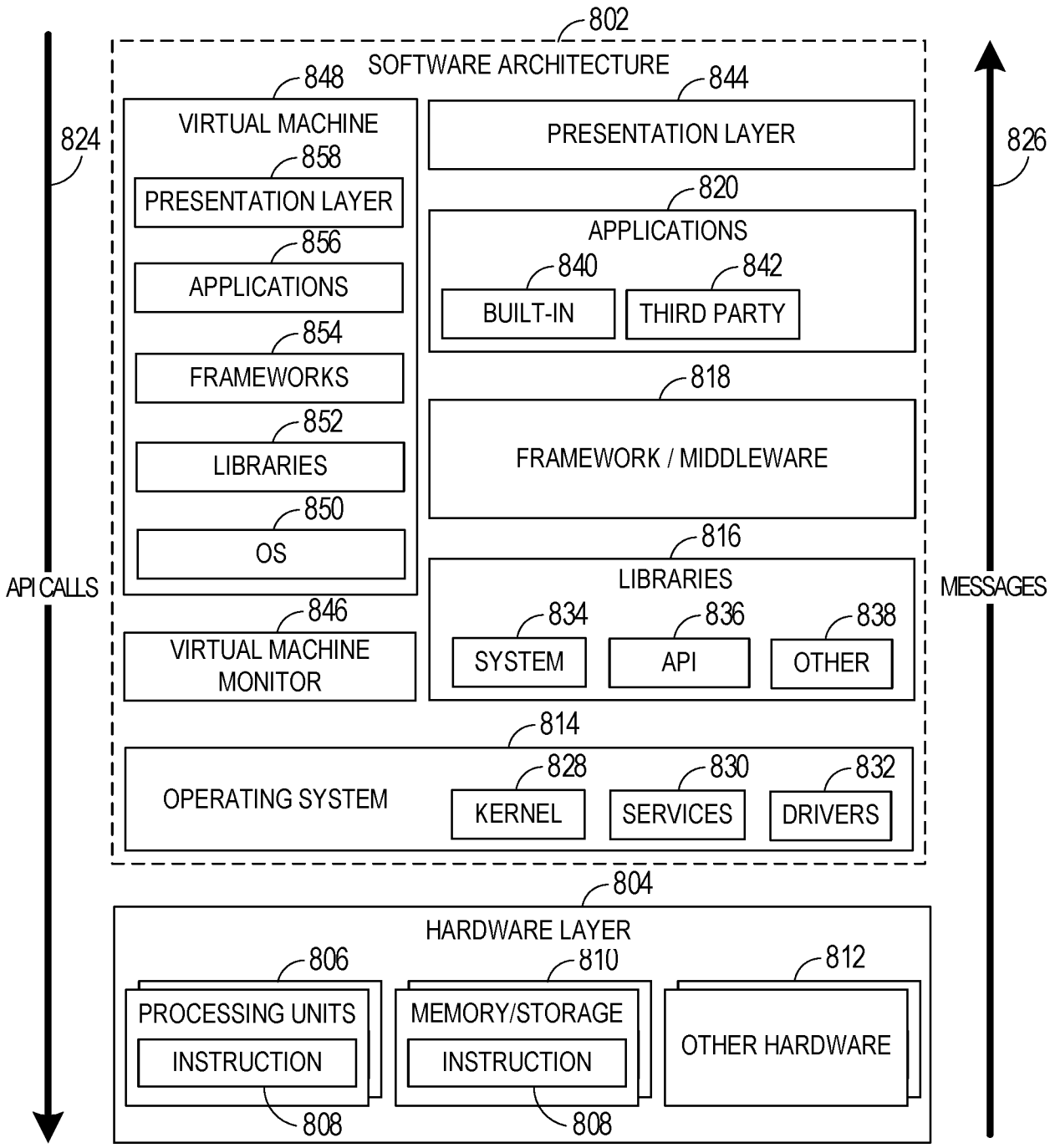

802
SOFTWARE ARCHITECTURE
848
VIRTUAL MACHINE
858
PRESENTATION LAYER
856
APPLICATIONS
854
FRAMEWORKS
852
LIBRARIES
850
OS
846
VIRTUAL MACHINE MONITOR
844
PRESENTATION LAYER
820
APPLICATIONS
840
BUILT-IN
842
THIRD PARTY
818
FRAMEWORK / MIDDLEWARE
816
LIBRARIES
834
SYSTEM
836
API
838
OTHER
814
OPERATING SYSTEM
828
KERNEL
830
SERVICES
832
DRIVERS
824
API CALLS
826
MESSAGES
804
HARDWARE LAYER
806
PROCESSING UNITS
INSTRUCTION
808
810
MEMORY/STORAGE
INSTRUCTION
808
812
OTHER HARDWARE

FIG. 8

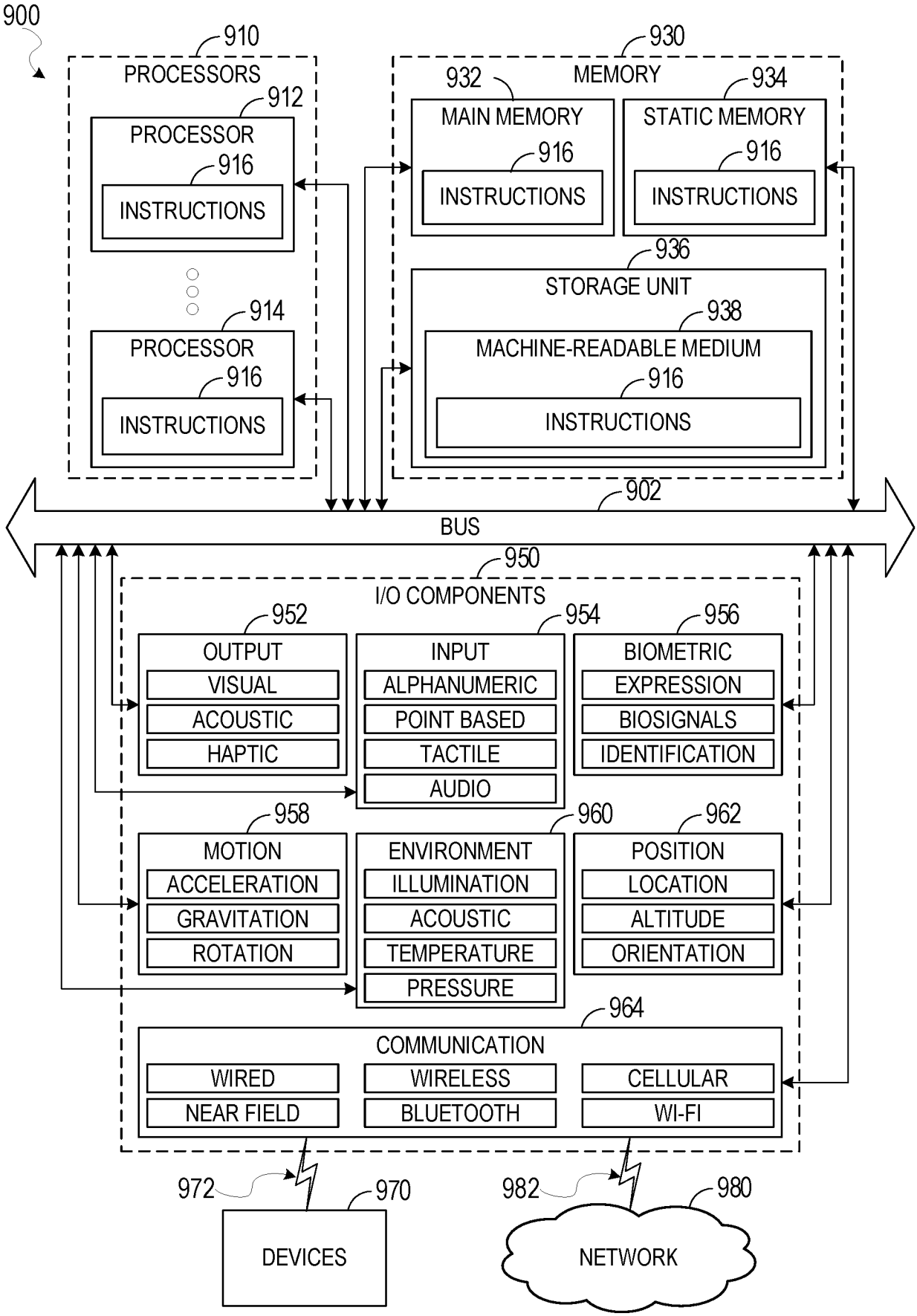

900
910
PROCESSORS
912
PROCESSOR
916
INSTRUCTIONS
914
PROCESSOR
916
INSTRUCTIONS
930
MEMORY
932
MAIN MEMORY
916
INSTRUCTIONS
934
STATIC MEMORY
916
INSTRUCTIONS
936
STORAGE UNIT
938
MACHINE-READABLE MEDIUM
916
INSTRUCTIONS
902
BUS
950
I/O COMPONENTS
952
OUTPUT
VISUAL
ACOUSTIC
HAPTIC
954
INPUT
ALPHANUMERIC
POINT BASED
TACTILE
AUDIO
956
BIOMETRIC
EXPRESSION
BIOSIGNALS
IDENTIFICATION
958
MOTION
ACCELERATION
GRAVITATION
ROTATION
960
ENVIRONMENT
ILLUMINATION
ACOUSTIC
TEMPERATURE
PRESSURE
962
POSITION
LOCATION
ALTITUDE
ORIENTATION
964
COMMUNICATION
WIRED
WIRELESS
CELLULAR
NEAR FIELD
BLUETOOTH
WI-FI
972
970
DEVICES
982
980
NETWORK

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2020/034444

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 21/00; G06Q 20/22; G06Q 99/00; H04L 9/00 (2020.01)
CPC - G06F 21/316; G06F 21/32; G06F 21/33; G06F 21/64; G06F 2221/2103 (2020.05)

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.
A	SILVERMAN. "Identity, Claims, & Tokens – An OpenID Connect Primer, Part 1 of 3." In: okta. 25 July 2017 (25.07.2017) Retrieved on 18 July 2020 (18.07.2020) from <https://developer.okta.com/blog/2017/07/25/oidc-primer-part-1> entire document	1-20
A	US 2008/0175360 A1 (SCHWARZ et al) 24 July 2008 (24.07.2008) entire document	1-20
A	US 8,095,972 B1 (FLOYD et al) 10 January 2012 (10.01.2012) entire document	1-20
A	US 2013/0030989 A1 (GELLER et al) 31 January 2013 (31.01.2013) entire document	1-20
A	US 2013/0019289 A1 (GONSER et al) 17 January 2013 (17.01.2013) entire document	1-20
A	US 2002/0087858 A1 (OLIVER et al) 04 July 2002 (04.07.2002) entire document	1-20

☐ 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
"D" document cited by the applicant in the international application
"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
19 July 2020	28 JUL 2020
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450 Facsimile No. 571-273-8300	Authorized officer Blaine R. Copenheaver Telephone No. PCT Helpdesk: 571-272-4300