



(51) International Patent Classification:

G06F 21/62 (2013.01) G06F 21/42 (2013.01)

G06F 21/64 (2013.01)

(21) International Application Number:

PCT/US2020/034597

(22) International Filing Date:

26 May 2020 (26.05.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

16/445,103 18 June 2019 (18.06.2019) US

(71) Applicant: MICROSOFT TECHNOLOGY LICENSING, LLC [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventors: MURDOCH, Brandon; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). MORTON, Sydney; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). STROCKIS, Daniel Luke; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). PATTEL, Ankur; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US).

(74) Agent: SWAIN, Cassandra T. et al.; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (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,

(54) Title: VALIDATION DATA STRUCTURE FOR DECENTRALIZED IDENTITY CLAIM

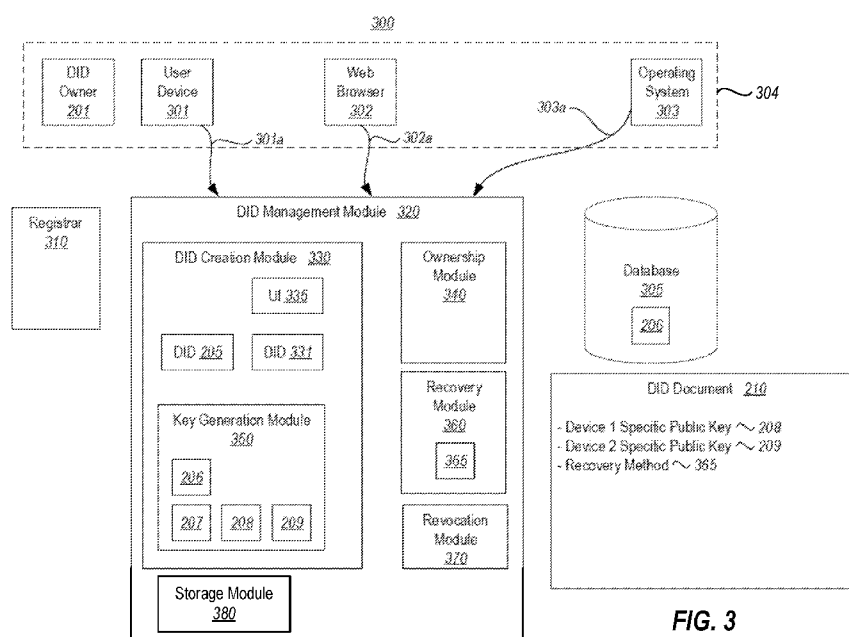


FIG. 3

(57) Abstract: Use of a validation data structure in order to securely communicate an encrypted claim that has a decentralized identifier as a subject. The sending system generates the validation data structure and presents the validation data structure to a user that owns the decentralized identifier. The sending system encrypts the claim using at least the validation data structure, and constructs a message that includes the encrypted claim, but which does not include the validation data structure. The relying party receives the message. However, without separately receiving the validation data structure from the user, the relying party computing system cannot decrypt the encrypted claim. If the user wishes the relying party computing system to have access to the claim, the user may communicate the validation data structure to the relying party computing system.

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, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

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

Published:

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

VALIDATION DATA STRUCTURE FOR DECENTRALIZED IDENTITY CLAIM**BACKGROUND**

[0001] Most currently used documents or records that prove identity are issued by
5 centralized organizations, such as governments, schools, employers, or other service centers
or regulatory organizations. These organizations often maintain every member's identity in
a centralized identity management system. A centralized identity management system is a
centralized information system used for organizations to manage the issued identities, their
authentication, authorization, roles and privileges. Centralized identity management
10 systems have been deemed as secure since they often use professionally maintained
hardware and software. Typically, the identity issuing organization sets the terms and
requirements for registering people with the organization. When a party needs to verify
another party's identity, the verifying party often needs to go through the centralized identity
management system to obtain information verifying and/or authenticating the other party's
15 identity.

[0002] Decentralized Identifiers (DIDs) are a new type of identifier, which are
independent from any centralized registry, identity provider, or certificate authority.
Distributed ledger technology (such as blockchain) provides the opportunity for using fully
decentralized identifiers. Distributed ledger technology uses globally distributed ledgers to
20 record transactions between two or more parties in a verifiable way. Once a transaction is
recorded, the data in the section of ledger cannot be altered retroactively without the
alteration of all subsequent sections of ledger, which provides a fairly secure platform. Since
a DID is generally not controlled by a centralized management system but rather is owned
by an owner of the DID, DIDs are sometimes referred to as identities without authority.

25 [0003] The subject matter claimed herein is not limited to embodiments that solve any
disadvantages or that operate only in environments such as those described above. Rather,
this background is only provided to illustrate one exemplary technology area where some
embodiments describe herein may be practiced.

SUMMARY

30 [0004] Embodiments disclosed herein relate to the use of a validation data structure in
order to securely communicate an encrypted claim that has a decentralized identifier as a
subject. Some embodiments may be performed on the sending side of the communication
that includes the encrypted claim. Other embodiments may be performed on the receiving
side of the communication, at a relying party computing system that relies upon the claim.

[0005] On the sending side, the sending computing system generates the validation data structure (such as a validation code) and presents the validation data structure to a user that owns the decentralized identifier. For instance, a user agent (e.g., a wallet) of the decentralized identifier may generate the validation data structure. The sending computing system encrypts the claim using at least the validation data structure. The sending computing system constructs a message that includes the encrypted claim, but which does not include the validation data structure. The sending computing system then sends the message to the computing system that will rely upon the claim.

[0006] On the receiving side, the relying party computing system receives the message. However, without separately receiving the validation data structure from the user, the relying party computing system cannot decrypt the encrypted claim. If the user wishes the relying party computing system to have access to the claim, the user may communicate the validation data structure to the relying party computing system. Accordingly, the user retains control over access to the claim.

[0007] In some embodiments, the communication of the message may be on a different communication channel than was used to communicate the validation data structure. Thus, even if there was an unintended party that was able to inappropriately access the message, that party cannot decrypt the claim without the validation code. This reduces the risk of claims being accessed via phishing attacks. Furthermore, this mechanism allows the user to securely communicate using multiple devices, and not just the computing system that contains the user agent for the user. Instead, the user may present the validation code from any computing system in the control of the user.

[0008] Additional features and advantages will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by the practice of the teachings herein. Features and advantages of the invention may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. Features of the present invention will become more fully apparent from the following description and appended claims, or may be learned by the practice of the invention as set forth hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] In order to describe the manner in which the above-recited and other advantages and features can be obtained, a more particular description of the subject matter briefly described above will be rendered by reference to specific embodiments which are illustrated in the appended drawings. Understanding that these drawings depict only typical

embodiments and are not therefore to be considered to be limiting in scope, embodiments will be described and explained with additional specificity and details through the use of the accompanying drawings in which:

5 [0010] Figure 1 illustrates an example computing system in which the principles described herein may be employed;

[0011] Figure 2 illustrates an example environment for creating a decentralized identification (DID);

[0012] Figure 3 illustrates an example environment for various DID management operations and services;

10 [0013] Figure 4 illustrates an example decentralized storage device or identity hubs;

[0014] Figure 5 illustrates an environment that includes a user, a sending computing system and a receiving computing system;

[0015] Figure 6 illustrates a flowchart of a method for communicating a message that includes an encrypted claim about a decentralized identity;

15 [0016] Figure 7 illustrates an example encryption environment, in which the encryption process receives the claim to be encrypted; and

[0017] Figure 8 illustrates the decryption environment, which includes a decryption process that receives the encrypted claim and recovers the claim in decrypted form.

DETAILED DESCRIPTION

20 [0018] Embodiments disclosed herein relate to the use of a validation data structure in order to securely communicate an encrypted claim that has a decentralized identifier as a subject. Some embodiments may be performed on the sending side of the communication that includes the encrypted claim. Other embodiments may be performed on the receiving side of the communication, at a relying party computing system that relies upon the claim.

25 [0019] On the sending side, the sending computing system generates the validation data structure (such as a validation code) and presents the validation data structure to a user that owns the decentralized identifier. For instance, a user agent (e.g., a wallet) of the decentralized identifier may generate the validation data structure. The sending computing system encrypts the claim using at least the validation data structure. The sending
30 computing system constructs a message that includes the encrypted claim, but which does not include the validation data structure. The sending computing system then sends the message to the computing system that will rely upon the claim.

[0020] On the receiving side, the relying party computing system receives the message. However, without separately receiving the validation data structure from the user, the

relying party computing system cannot decrypt the encrypted claim. If the user wishes the relying party computing system to have access to the claim, the user may communicate the validation data structure to the relying party computing system. Accordingly, the user retains control over access to the claim.

5 **[0021]** In some embodiments, the communication of the message may be on a different communication channel than was used to communicate the validation data structure. Thus, even if there was an unintended party that was able to inappropriately access the message, that party cannot decrypt the claim without the validation code. This reduces the risk of claims being accessed via phishing attacks. Furthermore, this mechanism allows the user
10 to securely communicate using multiple devices, and not just the computing system that contains the user agent for the user. Instead, the user may present the validation code from any computing system in the control of the user.

[0022] Because the principles described herein may be performed in the context of a computing system, some introductory discussion of a computing system will be described
15 with respect to Figure 1. Then, this description will return to the principles of a decentralized identifier (DID) platform with respect to the remaining figures.

[0023] Computing systems are now increasingly taking a wide variety of forms. Computing systems may, for example, be handheld devices, appliances, laptop computers, desktop computers, mainframes, distributed computing systems, data centers, or even
20 devices that have not conventionally been considered a computing system, such as wearables (e.g., glasses). In this description and in the claims, the term “computing system” is defined broadly as including any device or system (or a combination thereof) that includes at least one physical and tangible processor, and a physical and tangible memory capable of having thereon computer-executable instructions that may be executed by a processor. The
25 memory may take any form and may depend on the nature and form of the computing system. A computing system may be distributed over a network environment and may include multiple constituent computing systems.

[0024] As illustrated in Figure 1, in its most basic configuration, a computing system
100 typically includes at least one hardware processing unit 102 and memory 104. The
30 processing unit 102 may include a general-purpose processor and may also include a field programmable gate array (FPGA), an application specific integrated circuit (ASIC), or any other specialized circuit. The memory 104 may be physical system memory, which may be volatile, non-volatile, or some combination of the two. The term “memory” may also be used herein to refer to non-volatile mass storage such as physical storage media. If the

computing system is distributed, the processing, memory and/or storage capability may be distributed as well.

[0025] The computing system 100 also has thereon multiple structures often referred to as an “executable component”. For instance, the memory 104 of the computing system 100 is illustrated as including executable component 106. The term “executable component” is the name for a structure that is well understood to one of ordinary skill in the art in the field of computing as being a structure that can be software, hardware, or a combination thereof. For instance, when implemented in software, one of ordinary skill in the art would understand that the structure of an executable component may include software objects, routines, methods, and so forth, that may be executed on the computing system, whether such an executable component exists in the heap of a computing system, or whether the executable component exists on computer-readable storage media.

[0026] In such a case, one of ordinary skill in the art will recognize that the structure of the executable component exists on a computer-readable medium such that, when interpreted by one or more processors of a computing system (e.g., by a processor thread), the computing system is caused to perform a function. Such structure may be computer readable directly by the processors (as is the case if the executable component were binary). Alternatively, the structure may be structured to be interpretable and/or compiled (whether in a single stage or in multiple stages) so as to generate such binary that is directly interpretable by the processors. Such an understanding of example structures of an executable component is well within the understanding of one of ordinary skill in the art of computing when using the term “executable component”.

[0027] The term “executable component” is also well understood by one of ordinary skill as including structures, such as hard coded or hard wired logic gates, that are implemented exclusively or near-exclusively in hardware, such as within a field programmable gate array (FPGA), an application specific integrated circuit (ASIC), or any other specialized circuit. Accordingly, the term “executable component” is a term for a structure that is well understood by those of ordinary skill in the art of computing, whether implemented in software, hardware, or a combination. In this description, the terms “component”, “agent”, “manager”, “service”, “engine”, “module”, “virtual machine” or the like may also be used. As used in this description and in the case, these terms (whether expressed with or without a modifying clause) are also intended to be synonymous with the term “executable component”, and thus also have a structure that is well understood by those of ordinary skill in the art of computing.

[0028] In the description that follows, embodiments are described with reference to acts that are performed by one or more computing systems. If such acts are implemented in software, one or more processors (of the associated computing system that performs the act) direct the operation of the computing system in response to having executed computer-executable instructions that constitute an executable component. For example, such computer-executable instructions may be embodied on one or more computer-readable media that form a computer program product. An example of such an operation involves the manipulation of data. If such acts are implemented exclusively or near-exclusively in hardware, such as within a FPGA or an ASIC, the computer-executable instructions may be hard-coded or hard-wired logic gates. The computer-executable instructions (and the manipulated data) may be stored in the memory 104 of the computing system 100. Computing system 100 may also contain communication channels 108 that allow the computing system 100 to communicate with other computing systems over, for example, network 110.

[0029] While not all computing systems require a user interface, in some embodiments, the computing system 100 includes a user interface system 112 for use in interfacing with a user. The user interface system 112 may include output mechanisms 112A as well as input mechanisms 112B. The principles described herein are not limited to the precise output mechanisms 112A or input mechanisms 112B as such will depend on the nature of the device. However, output mechanisms 112A might include, for instance, speakers, displays, tactile output, virtual or augmented reality, holograms and so forth. Examples of input mechanisms 112B might include, for instance, microphones, touchscreens, virtual or augmented reality, holograms, cameras, keyboards, mouse or other pointer input, sensors of any type, and so forth.

[0030] Embodiments described herein may comprise or utilize a special-purpose or general-purpose computing system including computer hardware, such as, for example, one or more processors and system memory, as discussed in greater detail below. Embodiments described herein also include physical and other computer-readable media for carrying or storing computer-executable instructions and/or data structures. Such computer-readable media can be any available media that can be accessed by a general-purpose or special-purpose computing system. Computer-readable media that store computer-executable instructions are physical storage media. Computer-readable media that carry computer-executable instructions are transmission media. Thus, by way of example, and not limitation, embodiments of the invention can comprise at least two distinctly different kinds of

computer-readable media: storage media and transmission media.

[0031] Computer-readable storage media includes RAM, ROM, EEPROM, CD-ROM, or other optical disk storage, magnetic disk storage, or other magnetic storage devices, or any other physical and tangible storage medium which can be used to store desired program code means in the form of computer-executable instructions or data structures and which can be accessed by a general-purpose or special-purpose computing system.

[0032] A “network” is defined as one or more data links that enable the transport of electronic data between computing systems and/or modules and/or other electronic devices. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a computing system, the computing system properly views the connection as a transmission medium. Transmission media can include a network and/or data links which can be used to carry desired program code means in the form of computer-executable instructions or data structures and which can be accessed by a general-purpose or special-purpose computing system. Combinations of the above should also be included within the scope of computer-readable media.

[0033] Further, upon reaching various computing system components, program code means in the form of computer-executable instructions or data structures can be transferred automatically from transmission media to storage media (or vice versa). For example, computer-executable instructions or data structures received over a network or data link can be buffered in RAM within a network interface module (e.g., a “NIC”), and then be eventually transferred to computing system RAM and/or to less volatile storage media at a computing system. Thus, it should be understood that storage media can be included in computing system components that also (or even primarily) utilize transmission media.

[0034] Computer-executable instructions comprise, for example, instructions and data which, when executed at a processor, cause a general-purpose computing system, special-purpose computing system, or special-purpose processing device to perform a certain function or group of functions. Alternatively, or in addition, the computer-executable instructions may configure the computing system to perform a certain function or group of functions. The computer executable instructions may be, for example, binaries or even instructions that undergo some translation (such as compilation) before direct execution by the processors, such as intermediate format instructions such as assembly language, or even source code.

[0035] Although the subject matter has been described in language specific to structural

features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the described features or acts described above. Rather, the described features and acts are disclosed as example forms of implementing the claims.

5 **[0036]** Those skilled in the art will appreciate that the invention may be practiced in network computing environments with many types of computing system configurations, including, personal computers, desktop computers, laptop computers, message processors, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, mobile
10 telephones, PDAs, pagers, routers, switches, datacenters, wearables (such as glasses) and the like. The invention may also be practiced in distributed system environments where local and remote computing system, which are linked (either by hardwired data links, wireless data links, or by a combination of hardwired and wireless data links) through a network, both perform tasks. In a distributed system environment, program modules may be located
15 in both local and remote memory storage devices.

[0037] Those skilled in the art will also appreciate that the invention may be practiced in a cloud computing environment. Cloud computing environments may be distributed, although this is not required. When distributed, cloud computing environments may be distributed internationally within an organization and/or have components possessed across
20 multiple organizations. In this description and the following claims, “cloud computing” is defined as a model for enabling on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). The definition of “cloud computing” is not limited to any of the other numerous advantages that can be obtained from such a model when properly deployed.

25 **[0038]** The remaining figures may discuss various computing system which may correspond to the computing system 100 previously described. The computing systems of the remaining figures include various components or functional blocks that may implement the various embodiments disclosed herein as will be explained. The various components or functional blocks may be implemented on a local computing system or may be implemented
30 on a distributed computing system that includes elements resident in the cloud or that implement aspects of cloud computing. The various components or functional blocks may be implemented as software, hardware, or a combination of software and hardware. The computing systems of the remaining figures may include more or less than the components illustrated in the figures and some of the components may be combined as circumstances

warrant.

[0039] Some introductory discussion of a decentralized identifier (DID) and the environment in which they are created and reside will now be given with respect to Figure 2. As illustrated in Figure 2, a DID owner 201 may own or control a DID 205 that represents an identity of the DID owner 201. The DID owner 201 may register a DID using a creation and registration service, which will be explained in more detail below.

[0040] The DID owner 201 may be any entity that could benefit from a DID. For example, the DID owner 201 may be a human being or an organization of human beings. Such organizations might include a company, department, government, agency, or any other organization or group of organizations. Each individual human being might have a DID while the organization(s) to which each belongs might likewise have a DID.

[0041] The DID owner 201 may alternatively be a machine, system, or device, or a collection of machine(s), device(s) and/or system(s). In still other embodiments, the DID owner 201 may be a subpart of a machine, system or device. For instance, a device could be a printed circuit board, where the subpart of that circuit board are individual components of the circuit board. In such embodiments, the machine or device may have a DID and each subpart may also have a DID. A DID owner might also be a software component such as the executable component 106 described above with respect to Figure 1. An example of a complex executable component 106 might be an artificial intelligence. Accordingly, an artificial intelligence may also own a DID.

[0042] Thus, the DID owner 201 may be any entity, human or non-human, that is capable of creating the DID 205 or at least having the DID 205 created for and/or associated with them. Although the DID owner 201 is shown as having a single DID 205, this need not be the case as there may be any number of DIDs associated with the DID owner 201 as circumstances warrant.

[0043] As mentioned, the DID owner 201 may create and register the DID 205. The DID 205 may be any identifier that may be associated with the DID owner 201. Preferably, that identifier is unique to that DID owner 201, at least within a scope in which the DID is anticipated to be in use. As an example, the identifier may be a locally unique identifier, and perhaps more desirably a globally unique identifier for identity systems anticipated to operate globally. In some embodiments, the DID 205 may be a Uniform Resource identifier (URI) (such as a Uniform Resource Locator (URL)) or other pointer that relates the DID owner 201 to mechanisms to engage in trustable interactions with the DID owner 201.

[0044] The DID 205 is “decentralized” because it does not require a centralized, third

party management system for generation, management, or use. Accordingly, the DID 205 remains under the control of the DID owner 201. This is different from conventional centralized IDs which base trust on centralized authorities and that remain under control of corporate directory services, certificate authorities, domain name registries, or other centralized authority (referred to collectively as “centralized authorities” herein). Accordingly, the DID 205 may be any identifier that is under the control of the DID owner 201 and that is independent of any centralized authority.

[0045] In some embodiments, the structure of the DID 205 may be as simple as a user name or some other human-understandable term. However, in other embodiments, for increased security, the DID 205 may preferably be a random string of numbers and letters. In one embodiment, the DID 205 may be a string of 128 numbers and letters. Accordingly, the embodiments disclosed herein are not dependent on any specific implementation of the DID 205. In a very simple example, the DID 205 is shown within the figures as “123ABC”.

[0046] As also shown in Figure 2, the DID owner 201 has control of a private key 206 and public key 207 pair that is associated with the DID 205. Because the DID 205 is independent of any centralized authority, the private key 206 should at all times be fully in control of the DID owner 201. That is, the private and public keys should be generated in a decentralized manner that ensures that they remain under the control of the DID owner 201.

[0047] As will be described in more detail to follow, the private key 206 and public key 207 pair may be generated on a device controlled by the DID owner 201. The private key 206 and public key 207 pair should not be generated on a server controlled by any centralized authority as this may cause the private key 206 and public key 207 pair to not be fully under the control of the DID owner 201 at all times. Although figure 2 and this description have described a private and public key pair, it will also be noted that other types of reasonable cryptographic information and/or mechanisms may also be used as circumstances warrant.

[0048] Figure 2 also illustrates a DID document 210 that is associated with the DID 205. As will be explained in more detail to follow, the DID document 210 may be generated at the time that the DID 205 is created. In its simplest form, the DID document 210 describes how to use the DID 205. Accordingly, the DID document 210 includes a reference to the DID 205, which is the DID that is described by the DID document 210. In some embodiments, the DID document 210 may be implemented according to methods specified by a distributed ledger 220 (such as blockchain) that will be used to store a representation of the DID 205 as will be explained in more detail to follow. Thus, the DID document 210

may have different methods depending on the specific distributed ledger.

[0049] The DID document 210 also includes the public key 207 created by the DID owner 201 or some other equivalent cryptographic information. The public key 207 may be used by third party entities that are given permission by the DID owner 201 to access
5 information and data owned by the DID owner 201. The public key 207 may also be used to verify that the DID owner 201 in fact owns or controls the DID 205.

[0050] The DID document 210 may also include authentication information 211. The authentication information 211 may specify one or more mechanisms by which the DID owner 201 is able to prove that the DID owner 201 owns the DID 205. In other words, the
10 mechanisms of the authentication information 211 may show proof of a binding between the DID 205 (and thus its DID owner 201) and the DID document 210. In one embodiment, the authentication information 211 may specify that the public key 207 be used in a signature operation to prove the ownership of the DID 205. Alternatively, or in addition, the authentication information 211 may specify that the public key 207 be used in a biometric
15 operation to prove ownership of the DID 205. Accordingly, the authentication information 211 may include any number of mechanisms by which the DID owner 201 is able to prove that the DID owner 201 owns the DID 205.

[0051] The DID document 210 may also include authorization information 212. The authorization information 212 may allow the DID owner 201 to authorize third party entities
20 the rights to modify the DID document 210 or some part of the document without giving the third party the right to prove ownership of the DID 205. For example, the authorization information 212 may allow the third party to update any designated set of one or more fields in the DID document 210 using any designated update mechanism. Alternatively, the authorization information may allow the third party to limit the usages of DID 205 by the
25 DID owner 201 for a specified time period. This may be useful when the DID owner 201 is a minor child and the third party is a parent or guardian of the child. The authorization information 212 may allow the parent or guardian to limit use of the DID owner 201 until such time as the child is no longer a minor.

[0052] The authorization information 212 may also specify one or more mechanisms
30 that the third party will need to follow to prove they are authorized to modify the DID document 210. In some embodiments, these mechanisms may be similar to those discussed previously with respect to the authentication information 211.

[0053] The DID document 210 may also include one or more service endpoints 213. A service endpoint may include a network address at which a service operates on behalf of the

DID owner 201. Examples of specific services include discovery services, social networks, file storage services such as identity servers or hubs, and verifiable claim repository services. Accordingly, the service endpoints 213 operate as pointers for the services that operate on behalf of the DID owner 201. These pointers may be used by the DID owner 201 or by third party entities to access the services that operate on behalf of the DID owner 201. Specific examples of service endpoints 213 will be explained in more detail to follow.

[0054] The DID document 210 may further include identification information 214. The identification information 214 may include personally identifiable information such as the name, address, occupation, family members, age, hobbies, interests, or the like of DID owner 201. Accordingly, the identification information 214 listed in the DID document 210 may represent a different persona of the DID owner 201 for different purposes.

[0055] A persona may be pseudo anonymous. As an example, the DID owner 201 may include a pen name in the DID document when identifying him or her as a writer posting articles on a blog. A persona may be fully anonymous. As an example, the DID owner 201 may only want to disclose his or her job title or other background data (e.g., a school teacher, an FBI agent, an adult older than 21 years old, etc.) but not his or her name in the DID document. As yet another example, a persona may be specific to who the DID owner 201 is as an individual. As an example, the DID owner 201 may include information identifying him or her as a volunteer for a particular charity organization, an employee of a particular corporation, an award winner of a particular award, and so forth.

[0056] The DID document 210 may also include credential information 215, which may also be referred to herein as an attestation. The credential information 215 may be any information that is associated with the DID owner 201's background. For instance, the credential information 215 may be (but not limited to) a qualification, an achievement, a government ID, a government right such as a passport or a driver's license, a payment provider or bank account, a university degree or other educational history, employment status and history, or any other information about the DID owner 201's background.

[0057] The DID document 210 may also include various other information 216. In some embodiments, the other information 216 may include metadata specifying when the DID document 210 was created and/or when it was last modified. In other embodiments, the other information 216 may include cryptographic proofs of the integrity of the DID document 210. In still further embodiments, the other information 216 may include additional information that is either specified by the specific method implementing the DID document or desired by the DID owner 201.

[0058] Figure 2 also illustrates a distributed ledger 220. The distributed ledger 220 may be any decentralized, distributed network that includes various computing systems that are in communication with each other. For example, the distributed ledger 220 may include a first distributed computing system 230, a second distributed computing system 240, a third distributed computing system 250, and any number of additional distributed computing systems as illustrated by the ellipses 260. The distributed ledger 220 may operate according to any known standards or methods for distributed ledgers. Examples of conventional distributed ledgers that may correspond to the distributed ledger 220 include, but are not limited to, Bitcoin [BTC], Ethereum, and Litecoin.

[0059] In the context of DID 205, the distributed ledger or blockchain 220 is used to store a representation of the DID 205 that points to the DID document 210. In some embodiments, the DID document 210 may be stored on the actual distributed ledger. Alternatively, in other embodiments the DID document 210 may be stored in a data storage (not illustrated) that is associated with the distributed ledger 220.

[0060] As mentioned, a representation of the DID 205 is stored on each distributed computing system of the distributed ledger 220. For example, in Figure 2 this is shown as DID hash 231, DID hash 241, and DID hash 251, which are ideally identical hashed copies of the same DID. The DID hash 231, DID hash 241, and DID hash 251 may then point to the location of the DID document 210. The distributed ledger or blockchain 220 may also store numerous other representations of other DIDs as illustrated by references 232, 233, 234, 242, 243, 244, 252, 253, and 254.

[0061] In one embodiment, when the DID owner 201 creates the DID 205 and the associated DID document 210, the DID hash 231, DID hash 241, and DID hash 251 are written to the distributed ledger 220. The distributed ledger 220 thus records that the DID 205 now exists. Since the distributed ledger 220 is decentralized, the DID 205 is not under the control of any entity outside of the DID owner 201. DID hash 231, DID hash 241, and DID hash 251 may each include, in addition to the pointer to the DID document 210, a record or time stamp that specifies when the DID 205 was created. At a later date, when modifications are made to the DID document 210, each modification (and potentially also a timestamp of the modification) may also be recorded in DID hash 231, DID hash 241, and DID hash 251. DID hash 231, DID hash 241, and DID hash 251 may further include a copy of the public key 207 so that the DID 205 is cryptographically bound to the DID document 210.

[0062] Having described DIDs and how they operate generally with reference to Figure

2, specific embodiments of DID environments will now be explained. Turning to Figure 3, an environment 300 that may be used to perform various DID management operations and services will now be explained. It will be appreciated that the environment of Figure 3 may reference elements from Figure 2 as needed for ease of explanation.

5 [0063] As shown in Figure 3, the environment 300 may include various devices and computing systems that may be owned or otherwise under the control of the DID owner 201. These may include a user device 301. The user device 301 may be, but is not limited to, a mobile device such as a smart phone, a computing device such as a laptop computer, or any device such as a car or an appliance that includes computing abilities. The device 301
10 may include a web browser 302 operating on the device and an operating system 303 operating the device. More broadly speaking, the dashed line 304 represents that all of these devices may be owned or otherwise under the control of the DID owner 201.

[0064] The environment 300 also includes a DID management module 320. It will be noted that in operation, the DID management module 320 may reside on and be executed
15 by one or more of user device 301, web browser 302, and the operating system 303 as illustrated by respective lines 301a, 302a, and 303a. Accordingly, the DID management module 320 is shown as being separate for ease of explanation. The DID management module 320 may be also described as a “wallet” in that it can hold various claims related to a particular DID. The DID management module 320 may also be described as a “user
20 agent”.

[0065] As shown in Figure 3, the DID management module 320 includes a DID creation module 330. The DID creation module 330 may be used by the DID owner 201 to create the DID 205 or any number of additional DIDs, such as DID 331. In one embodiment, the DID creation module may include or otherwise have access to a User Interface (UI) element
25 335 that may guide the DID owner 201 in creating the DID 205. The DID creation module 330 may have one or more drivers that are configured to work with specific distributed ledgers such as distributed ledger 220 so that the DID 205 complies with the underlying methods of that distributed ledger.

[0066] A specific embodiment will now be described. For example, the UI 335 may
30 provide a prompt for the user to enter a user name or some other human recognizable name. This name may be used as a display name for the DID 205 that will be generated. As previously described, the DID 205 may be a long string of random numbers and letters and so having a human-recognizable name for a display name may be advantageous. The DID creation module 330 may then generate the DID 205. In the embodiments having the UI

335, the DID 205 may be shown in a listing of identities and may be associated with the human-recognizable name.

[0067] The DID creation module 330 may also include a key generation module 350. The key generation module may generate the private key 206 and public key 207 pair
5 previously described. The DID creation module 330 may then use the DID 205 and the private and public key pair to generate the DID document 210.

[0068] In operation, the DID creation module 330 accesses a registrar 310 that is configured to the specific distributed ledger that will be recording the transactions related to the DID 205. The DID creation module 330 uses the registrar 310 to record DID hash
10 231, DID hash 241, and DID hash 251 in the distributed ledger in the manner previously described, and to store the DID document 210 in the manner previously described. This process may use the public key 207 in the hash generation.

[0069] In some embodiments, the DID management module 320 may include an ownership module 340. The ownership module 340 may provide mechanisms that ensure
15 that the DID owner 201 is in sole control of the DID 205. In this way, the provider of the DID management module 320 is able to ensure that the provider does not control the DID 205, but is only providing the management services.

[0070] As previously discussed, the key generation module 350 generates the private key 206 and public key 207 pair and the public key 207 is then recorded in the DID
20 document 210. Accordingly, the public key 207 may be used by all devices associated with the DID owner 201 and all third parties that desire to provide services to the DID owner 201. Accordingly, when the DID owner 201 desires to associate a new device with the DID 205, the DID owner 201 may execute the DID creation module 330 on the new device. The DID creation module 330 may then use the registrar 310 to update the DID document 210
25 to reflect that the new device is now associated with the DID 205, which update would be reflected in a transaction on the distributed ledger 220, as previously described.

[0071] In some embodiments, however, it may be advantageous to have a public key per device 301 owned by the DID owner 201 as this may allow the DID owner 201 to sign with the device-specific public key without having to access a general public key. In other
30 words, since the DID owner 201 will use different devices at different times (for example using a mobile phone in one instance and then using a laptop computer in another instance), it is advantageous to have a key associated with each device to provide efficiencies in signing using the keys. Accordingly, in such embodiments the key generation module 350 may generate additional public keys 208 and 209 when the additional devices execute the

DID creation module 330. These additional public keys may be associated with the private key 206 or in some instances may be paired with a new private key.

[0072] In those embodiments where the additional public keys 208 and 209 are associated with different devices, the additional public keys 208 and 209 may be recorded
5 in the DID document 210 as being associated with those devices. This is shown in Figure 3. It will be appreciated that the DID document 210 may include the information (information 205, 207 and 211 through 216) previously described in relation to Figure 2 in addition to the information (information 208, 209 and 365) shown in Figure 3. If the DID document 210 existed prior to the device-specific public keys being generated, then the DID document
10 210 would be updated by the creation module 330 via the registrar 310 and this would be reflected in an updated transaction on the distributed ledger 220.

[0073] In some embodiments, the DID owner 201 may desire to keep secret the association of a device with a public key or the association of a device with the DID 205. Accordingly, the DID creation module 330 may cause that such data be secretly shown in
15 the DID document 210.

[0074] As described thus far, the DID 205 has been associated with all the devices under the control of the DID owner 201, even when the devices have their own public keys. However, in some embodiments it may be useful for each device or some subset of devices under the control of the DID owner 201 to each have their own DID. Thus, in some
20 embodiments the DID creation module 330 may generate an additional DID, for example DID 331, for each device. The DID creation module 330 would then generate private and public key pairs and DID documents for each of the devices and have them recorded on the distributed ledger 220 in the manner previously described. Such embodiments may be advantageous for devices that may change ownership as it may be possible to associate the
25 device-specific DID to the new owner of the device by granting the new owner authorization rights in the DID document and revoking such rights from the old owner.

[0075] As mentioned, to ensure that the private key 206 is totally in the control of the DID owner 201, the private key 206 is created on the user device 301, browser 302, or operating system 303 that is owned or controlled by the DID owner 201 that executed the
30 DID management module 320. In this way, there is little chance that a third party (and most consequentially, the provider of the DID management module 320) may gain control of the private key 206.

[0076] However, there is a chance that the device storing the private key 206 may be lost by the DID owner 201, which may cause the DID owner 201 to lose access to the DID

205. Accordingly, in some embodiments, the UI 335 may include the option to allow the DID owner 201 to export the private key 206 to an off device secured database 305 that is under the control of the DID owner 201. As an example, the database 305 may be one of the identity hubs 410 described below with respect to Figure 4. A storage module 380 is configured to store data (such as the private key 206 or attestations made by or about the DID owner 201) off device in the database 305 or identity hubs 410. In some embodiments, the private key 206 may be stored as a QR code that may be scanned by the DID owner 201.

[0077] In other embodiments, the DID management module 320 may include a recovery module 360 that may be used to recover a lost private key 206. In operation, the recovery module 360 allows the DID owner 201 to select one or more recovery mechanisms 365 at the time the DID 205 is created that may later be used to recover the lost private key. In those embodiments having the UI 335, the UI 335 may allow the DID owner 201 to provide information that will be used by the one or more recovery mechanisms 365 during recovery. The recovery module 360 may then be run on any device associated with the DID 205.

[0078] The DID management module 320 may also include a revocation module 370 that is used to revoke or sever a device from the DID 205. In operation, the revocation module may use the UI element 335, which may allow the DID owner 201 to indicate a desire to remove a device from being associated with the DID 205. In one embodiment, the revocation module 370 may access the DID document 210 and may cause that all references to the device be removed from the DID document 210. Alternatively, the public key for the device may be removed. This change in the DID document 210 may then be reflected as an updated transaction on the distributed ledger 220 as previously described.

[0079] Figure 4 illustrates an embodiment of an environment 400 in which a DID such as DID 205 may be utilized. Specifically, the environment 400 will be used to describe the use of the DID 205 in relation to one or more decentralized stores or identity hubs 410 that are each under the control of the DID owner 201 to store data belonging to or regarding the DID owner 201. For instance, data may be stored within the identity hubs using the storage module 380 of Figure 3. It will be noted that Figure 4 may include references to elements first discussed in relation to figures 2 or 3 and thus use the same reference numeral for ease of explanation.

[0080] In one embodiment, the identity hubs 410 may be multiple instances of the same identity hub. This is represented by the line 410A. Thus, the various identity hubs 410 may include at least some of the same data and services. Accordingly, if a change is made to part of at least some of the data (and potentially any part of any of the data) in one of the

identity hubs 410, the change may be reflected in one or more of (and perhaps all of) the remaining identity hubs.

[0081] The identity hubs 410 may be any data store that may be in the exclusive control of the DID owner 201. As an example only, the first identity hub 411 and second identity
5 hub 412 are implemented in cloud storage (perhaps within the same cloud, or even on different clouds managed by different cloud providers) and thus may be able to hold a large amount of data. Accordingly, a full set of the data may be stored in these identity hubs.

[0082] However, the identity hubs 413 and 414 may have less memory space. Accordingly, in these identity hubs a descriptor of the data stored in the first and second
10 identity hubs may be included. Alternatively, a record of changes made to the data in other identity hubs may be included. Thus, changes in one of the identity hubs 410 are either fully replicated in the other identity hubs or at least a record or descriptor of that data is recorded in the other identity hubs.

[0083] Because the identity hubs may be multiple instances of the same identity hub,
15 only a full description of the first identity hub 411 will be provided as this description may also apply to the identity hubs 412 through 414. As illustrated, identity hub 411 may include data storage 420. The data storage 420 may be used to store any type of data that is associated with the DID owner 201. In one embodiment the data may be a collection 422 of a specific type of data corresponding to a specific protocol. For example, the collection 422
20 may be medical records data that corresponds to a specific protocol for medical data. The collection 422 may include any other type of data, such as attestations made by or about the DID owner 201.

[0084] In one embodiment, the stored data may have different authentication and privacy settings 421 associated with the stored data. For example, a first subset of the data
25 may have a setting 421 that allows the data to be publicly exposed, but that does not include any authentication to the DID owner 201. This type of data may be for relatively unimportant data such as color schemes and the like. A second subset of the data may have a setting 421 that allows the data to be publicly exposed and that includes authentication to the DID owner 201. A third subset of the data may have a setting 421 that encrypts the
30 subset of data with the private key 206 and public key 207 pair (or some other key pair) associated with the DID owner 201. This type of data will require a party to have access to the public key 207 (or to some other associated public key) in order to decrypt the data. This process may also include authentication to the DID owner 201. A fourth subset of the data may have a setting 421 that restricts this data to a subset of third parties. This may require

that public keys associated with the subset of third parties be used to decrypt the data. For example, the DID owner 201 may cause the setting 421 to specify that only public keys associated with friends of the DID owner 201 may decrypt this data. With respect to data stored by the storage module 380, these settings 411 may be at least partially composed by the storage module 380 of Figure 3.

[0085] In some embodiments, the identity hub 411 may have a permissions module 430 that allows the DID owner 201 to set specific authorization or permissions for third parties such as third parties 401 and 402 to access the identity hub. For example, the DID owner 201 may provide access permission to his or her spouse to all the data 420. Alternatively, the DID owner 201 may allow access to his or her doctor for any medical records. It will be appreciated that the DID owner 201 may give permission to any number of third parties to access a subset of the data 420. This will be explained in more detail to follow. With respect to data stored by the storage module 380, these access permissions 430 may be at least partially composed by the storage module 380 of Figure 3.

[0086] The identity hub 411 may also have a messaging module 440. In operation, the messaging module allows the identity hub to receive messages such as requests from parties such as third parties 401 and 402 to access the data and services of the identity hub. In addition, the messaging module 440 allows the identity hub 411 to respond to the messages from the third parties and to also communicate with a DID resolver 450. This will be explained in more detail to follow. The ellipsis 416 represents that the identity hub 411 may have additional services as circumstances warrant.

[0087] In one embodiment, the DID owner 201 may wish to authenticate a new device 301 with the identity hub 411 that is already associated with the DID 205 in the manner previously described. Accordingly, the DID owner 201 may utilize the DID management module 320 associated with the new user device 301 to send a message to the identity hub 411 asserting that the new user device is associated with the DID 205 of the DID owner 201.

[0088] However, the identity hub 411 may not initially recognize the new device as being owned by the DID owner 201. Accordingly, the identity hub 411 may use the messaging module 440 to contact the DID resolver 450. The message sent to the DID resolver 450 may include the DID 205.

[0089] The DID resolver 450 may be a service, application, or module that is configured in operation to search the distributed ledger 220 for DID documents associated with DIDs. Accordingly, in the embodiment the DID resolver 450 may search the distributed ledger 220 using the DID 205, which may result in the DID resolver 450 finding the DID document

210. The DID document 210 may then be provided to the identity hub 411.

[0090] As discussed previously, the DID document 210 may include a public key 208 or 209 that is associated with the new user device 301. To verify that the new user device is owned by the DID owner 201, the identity hub 411 may provide a cryptographic challenge
5 to the new user device 301 using the messaging module 440. This cryptographic challenge will be structured such that only a device having access to the private key 206 will be able to successfully answer the challenge.

[0091] In this embodiment, since the new user device is owned by DID owner 201 and thus has access to the private key 206, the challenge may be successfully answered. The
10 identity hub 411 may then record in the permissions 430 that the new user device 301 is able to access the data and services of the identity hub 411 and also the rest of the identity hubs 410.

[0092] It will be noted that this process of authenticating the new user device 301 was performed without the need for the DID owner 201 to provide any username, password or
15 the like to the provider of the identity hub 411 (i.e., the first cloud storage provider) before the identity hub 411 could be accessed. Rather, the access was determined in a decentralized manner based on the DID 205, the DID document 210, and the associated public and private keys. Since these were at all times in the control of the DID owner 201, the provider of the identity hub 411 was not involved and thus has no knowledge of the transaction or of any
20 personal information of the DID owner 201.

[0093] In another example embodiment, the DID owner 201 may provide the DID 205 to the third-party entity 401 so that the third party may access data or services stored on the identity hub 411. For example, the DID owner 201 may be a human who is at a scientific conference who desires to allow the third party 401, who is also a human, access to his or
25 her research data. Accordingly, the DID owner 201 may provide the DID 205 to the third party 401.

[0094] Once the third party 401 has access to the DID 205, he or she may access the DID resolver 450 to access the DID document 210. As previously discussed, the DID document 210 may include an end point 213 that is an address or pointer to services
30 associated with the decentralized identity.

[0095] Completing the research data example, the third party 401 may send a message to the messaging module 440 asking for permission to access the research data. The messaging module 440 may then send a message to the DID owner 201 asking if the third party 401 should be given access to the research data. Because the DID owner desires to

provide access to this data, the DID owner 201 may allow permission to the third party 401 and this permission may be recorded in the permissions 430.

[0096] The messaging module 440 may then message the third party 401 informing the third party that he or she is able to access the research data. The identity hub 411 and the third party 401 may then directly communicate so that the third party may access the data. It will be noted that in many cases, it will actually be an identity hub associated with the third party 401 that communicates with the identity hub 411. However, it may be a device of the third party 401 that does the communication.

[0097] Advantageously, the above described process allows the identity hub 411 and the third party 401 to communicate and to share the data without the need for the third party to access the identity hub 411 in the conventional manner. Rather, the communication is provisioned in the decentralized manner using the DID 205 and the DID document 210. This advantageously allows the DID owner to be in full control of the process.

[0098] As shown in Figure 4, the third party 402 may also request permission for access to the identity hub 411 using the DID 205 and the DID document 210. Accordingly, the embodiments disclosed herein allow access to any number of third parties to the identity hubs 410.

[0099] Having described an example context in which the principles described herein might be employed, the principles of communicating encrypted claims using a validation data structure will now be described with respect to Figures 5 through 9.

[00100] Figure 5 illustrates an environment 500 that includes a user 501, a sending computing system 510 and a receiving computing system 520. As represented by line 502, the sending computing system 510 is in the control of a user 501. As represented by ellipsis 511, the user 501 may also have control of other computing systems. As an example, the computing systems 510, 511 and 520 may each be structured as described above for the computing system 100 of Figure 1. The computing systems may be any form of computing system including, but not limited to, wearables, devices, desktops, tablet PCs, desktop PCs, or any other computing system.

[00101] The sending computing system 510 sends (as represented by arrow 515) an encrypted claim about the user 501 to the receiving computing system 520. Specifically, the user 501 is represented as a decentralized identifier (or “DID” as the acronym is widely used above). The claim may be accessed by a user agent 530 running on the sending computing system 510. As an example, the user agent 530 may be the management module 320 of Figure 3, which has access to a number of claims about the decentralized identifier.

The user agent 530 may also be considered as a digital wallet that stores claims about the decentralized identifier. Because the receiving computing system 520 receives and relies upon the claim, the receiving computing system 520 may also be referred to herein as a “relying party” computing system.

5 **[00102]** Figure 6 illustrates a flowchart of a method 600 for communicating a message that includes an encrypted claim about a decentralized identity. As an example, the method 600 may be performed in the environment 500 of Figure 5. Some of the acts of the method 600 may be performed by a user (e.g., user 501 of Figure 5), and thus are listed under the left column of Figure 6 under the heading “User”. Others of the acts of the method 600 may be performed by a computing system that sends an encrypted claim (e.g., the sending computing system 510 of Figure 5), and thus are listed in the middle column of Figure 6 under the heading “Sending C.S.” Others of the acts of the method 600 may be performed by a relying party computing system that receives and relies upon the encrypted claim (e.g., the receiving computing system 520 of Figure 5), and are thus listed in the right column of Figure 6 under the heading “Relying Party C.S.”.

[00103] As illustrated, the method 600 begins at the sending computing system (e.g., the computing system 510). The sending computing system generates a validation data structure (act 611). That validation data structure is “associated” with the decentralized identifier in that the relying party computing system will need access to that validation data structure in order to be able to interpret an encrypted claim about the decentralized identity. As an example, the user agent 530 may generate the validation data structure.

[00104] The validation data structure might be any arrangement of data. For instance, the validation data structure might be a file, or perhaps a code. The validation code might be, for instance, a sequence of characters such as a Personal Identification Number (PIN). The validation code might also be a visual code, such as a barcode (e.g., a linear barcode or a matrix barcode, such as a QR code) The code might also be an audio code, such as an audio signature. The validation data structure could also be any combination of these.

[00105] The sending computing system then causes the validation data structure to be presented to a user that owns the decentralized identifier (act 612). The user then receives that validation data structure (act 601). This presentation is sufficient that the user may later present the validation data structure to the relying party computing system.

[00106] For instance, if the validation data structure were a file, the user may access that file so as to be able to upload that file to the relying party computing system. If the validation data structure were a sequence of characters, the user may be shown that sequence

of characters, so that the user can enter that sequence of characters remotely into the relying party computing system. If the validation data structure were an image, such as a barcode, the user would be presented with that image, so that the user can present that image to a camera, for digital transport to the relying party computing system. If the validation data structure were an audio signature, the user may be given access to play that audio signature, so that the user can sound that signature into a speaker, for digitally transmitting that signature to the relying party computing system.

[00107] The sending computing system also uses the validation data structure to encrypt a claim that has the decentralized identifier as a subject (act 613). Figure 7 illustrates an example encryption environment 700, in which the encryption process 710 receives the claim 701 to be encrypted. The encryption process 710 uses an encryption algorithm 711, the validation data structure 712, and the public key 713 of the relying party associated with the relying party computing system in order to generate the encrypted claim 721. The sending computing system generates a message that includes the encrypted claim, but which does not include the validation data structure (act 614). In one embodiment, the encryption process 710 generates a JSON Web Encryption (JWE) object, where the validation data structure is an initialization vector.

[00108] The sending computing system then transmits the message to the relying party computing system that will rely upon the claim (act 615), whereupon the relying party computing system receives that message (act 621). Since the relying party computing system needs the validation data structure in order to decrypt the encrypted claim, if the user wishes the relying party computing system to rely on the claim, the user must provide the validation data structure to the relying party (act 602), whereupon the relying party computing system receives the validation data structure (act 622). There is no requirement as to whether the relying party computing system receives the message (act 621) or the validation data structure (act 622) first.

[00109] The relying party computing system then uses the validation data structure to decrypt the encrypted claim (act 623). Figure 8 illustrates the decryption environment 800, which includes a decryption process 810 that receives the encrypted claim 721, and recovers the claim 701 in decrypted form. The decryption process 810 receives the decryption algorithm identification 811, the validation data structure 712, and the private key 713 of the relying party computing system, in order to perform that decryption.

[00110] In one embodiment, the communication channel used to receive validation data structure is different than the communication channel used to received the message that

included the decrypted claim. That way, even if an intermediary was improperly intercepting traffic on the communication channel used to communicate the message, that intermediary would not be able to access the claim, since the intermediary does not also have the validation data structure communicated over a different communication channel.

5 Thus, privacy of the user associated with the decentralized identifier is preserved. Furthermore, the user retains strict control over access to their claims.

[00111] This process also allows for the user to operate securely across multiple devices, even though only one of those devices operates a user agent. That is because the user proves that they are the decentralized identity by providing the validation data structure on
10 whatever other device is in possession and control of the user. Thus, the relying party can safely interface with the user on whatever device provided the validation data structure, with high confidence that device is in the control of the user associated with the decentralized identity.

[00112] For the processes and methods disclosed herein, the operations performed in the
15 processes and methods may be implemented in differing order. Furthermore, the outlined operations are only provided as examples, and some of the operations may be optional, combined into fewer steps and operations, supplemented with further operations, or expanded into additional operations without detracting from the essence of the disclosed embodiments.

20 [00113] The present invention may be embodied in other specific forms without departing from its spirit or characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within
25 their scope.

CLAIMS

1. A method for sending a message that includes an encrypted claim about a decentralized identity to a relying party computing system such that the encrypted claim cannot be decrypted without a user associated with the decentralized identifier providing a validation code to the relying party computing system, the method comprising:

generating a validation data structure associated with a decentralized identifier;

causing the validation data structure to be presented to a user that owns the decentralized identifier;

encrypting a claim that has the decentralized identifier as a subject, the encryption using the validation data structure associated with the decentralized identifier such that decryption of the claim requires the validation data structure;

generating a message that includes the encrypted claim, but which does not include the validation data structure;

causing the message to be transmitted to a relying party computing system that will rely on the claim, wherein the relying party computing system cannot decrypt the claim until the user provides the validation data structure to the relying party computing system.

2. The method in accordance with Claim 1, the validation data structure comprising a validation code.

3. The method in accordance with Claim 2, the validation code being pseudo-randomly generated.

4. The method in accordance with Claim 2, the validation code comprising a sequence of characters.

5. The method in accordance with Claim 2, the validation code comprising a barcode.

6. The method in accordance with Claim 2, the validation code comprising an audio signature.

7. The method in accordance with Claim 1, the encryption also using a public key of a relying party associated with the relying party computing system.

8. The method in accordance with Claim 1, the method being performed by a user agent running on a computing system in possession of the user.

9. The method in accordance with Claim 1, the method further comprising:

communicating, by the user, the validation data structure to the relying party computing system using a different communication channel that is used to communicate the message.

10. A computing system comprising:

one or more processors; and

one or more computer-readable media having thereon computer-executable instructions that are structured such that, when executed by the one or more processors, cause the computing system to perform a method for sending a message that includes an encrypted claim about a decentralized identity to a relying party computing system such that the encrypted claim cannot be decrypted without a user associated with the decentralized identifier providing a validation code to the relying party computing system, the method comprising:

generating a validation data structure associated with a decentralized identifier;

causing the validation data structure to be presented to a user that owns the decentralized identifier;

encrypting a claim that has the decentralized identifier as a subject, the encryption using the validation data structure associated with the decentralized identifier such that decryption of the claim requires the validation data structure;

generating a message that includes the encrypted claim, but which does not include the validation data structure;

causing the message to be transmitted to a relying party computing system that will rely on the claim, wherein the relying party computing system cannot decrypt the claim until the user provides the validation data structure to the relying party computing system.

Computing System
100

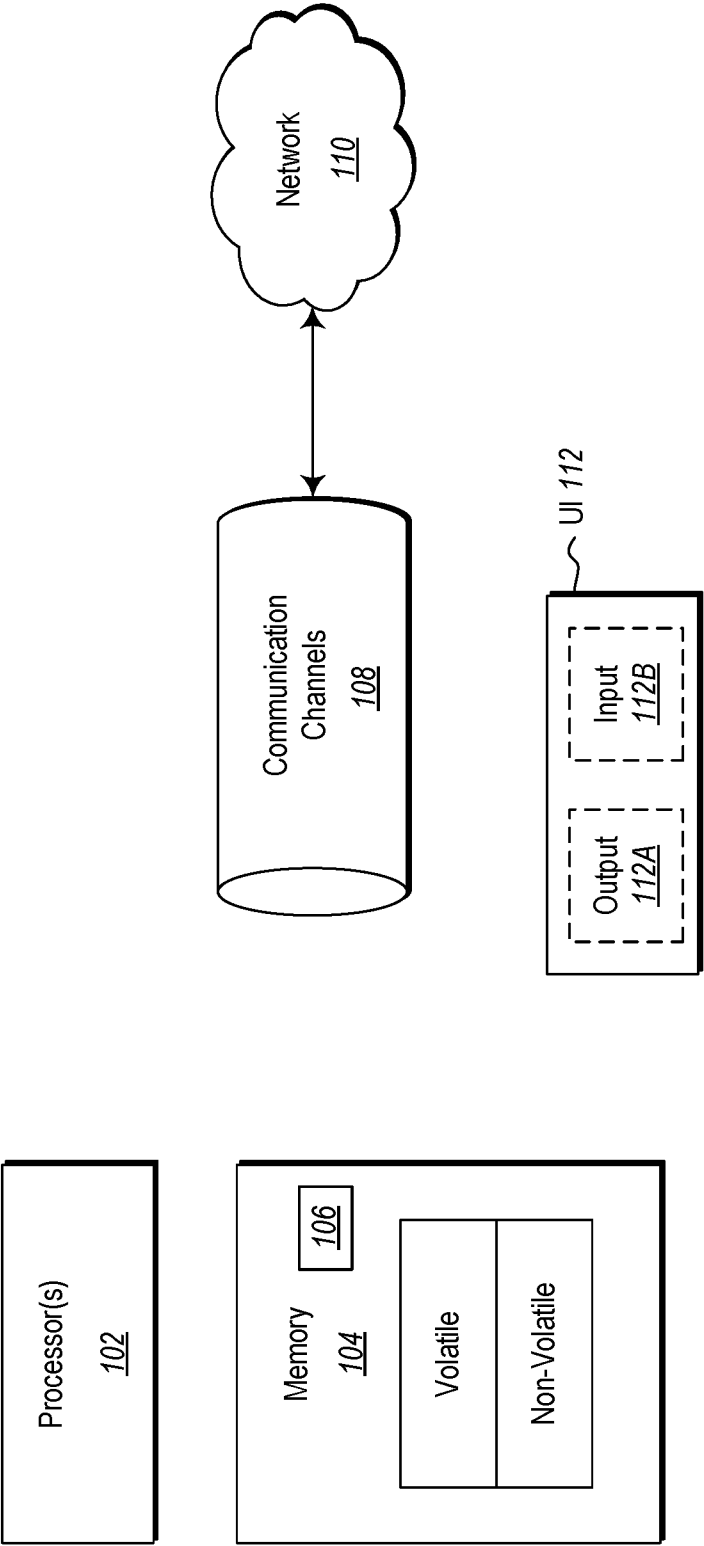


FIG. 1

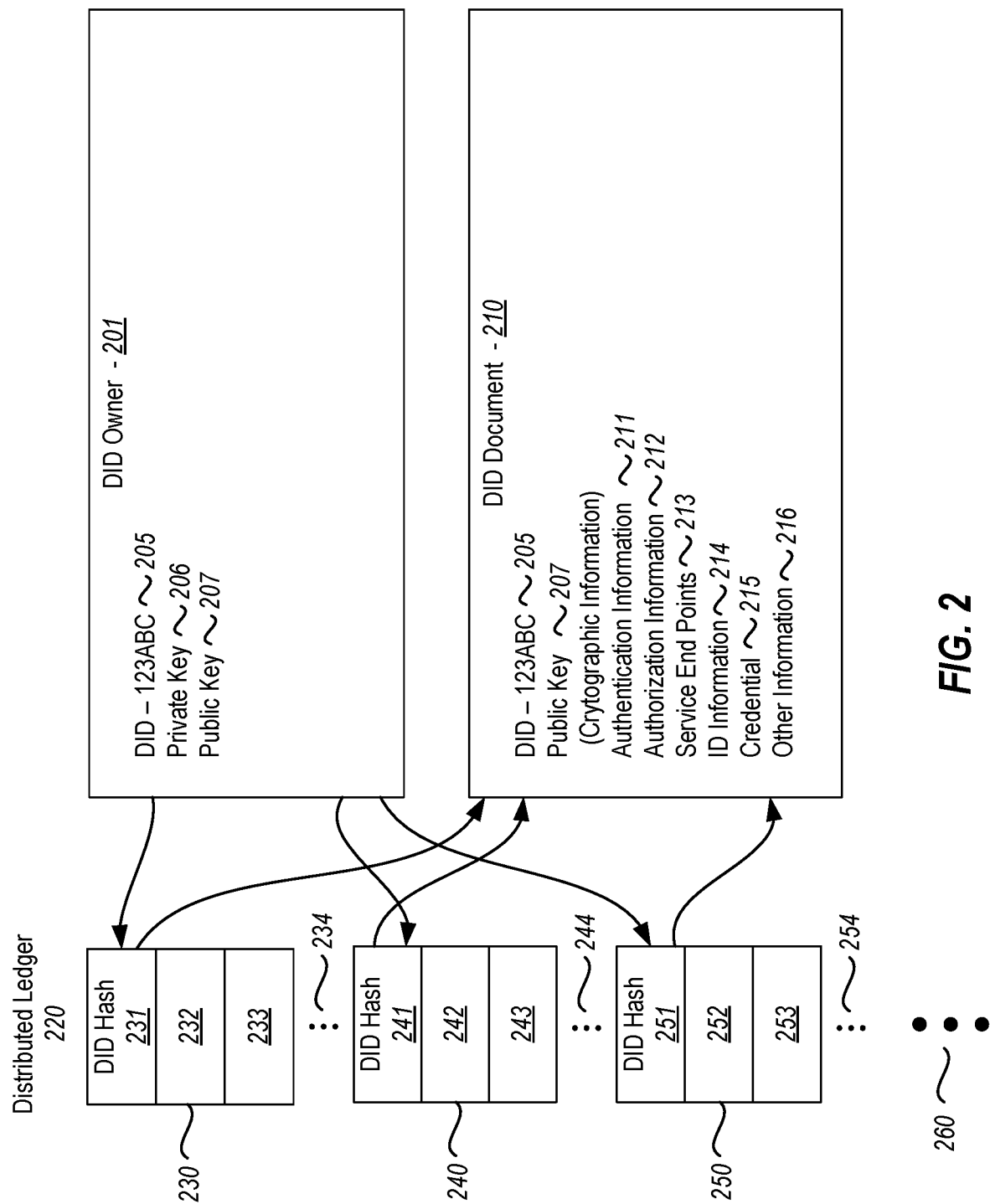


FIG. 2

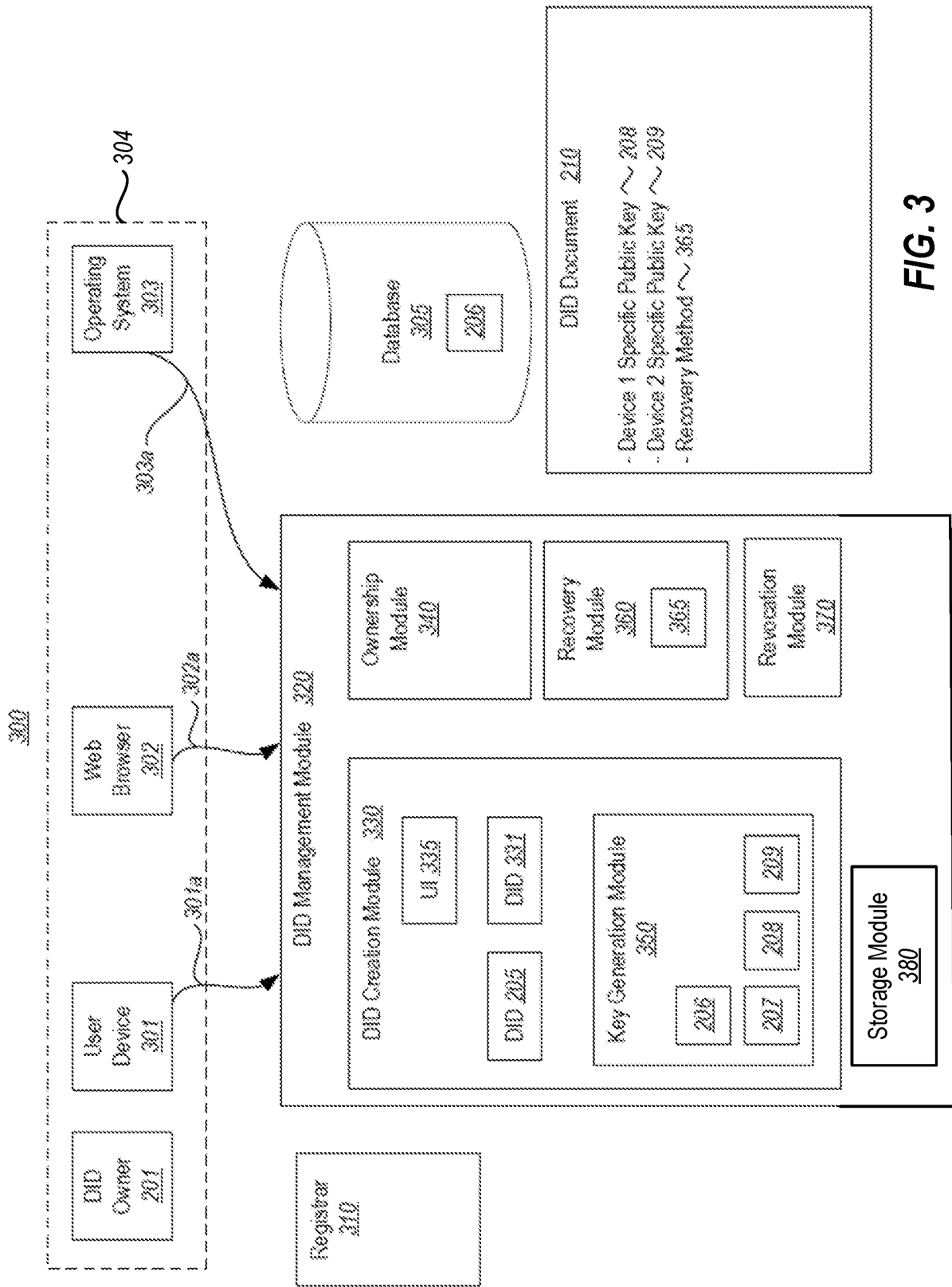


FIG. 3

4/7

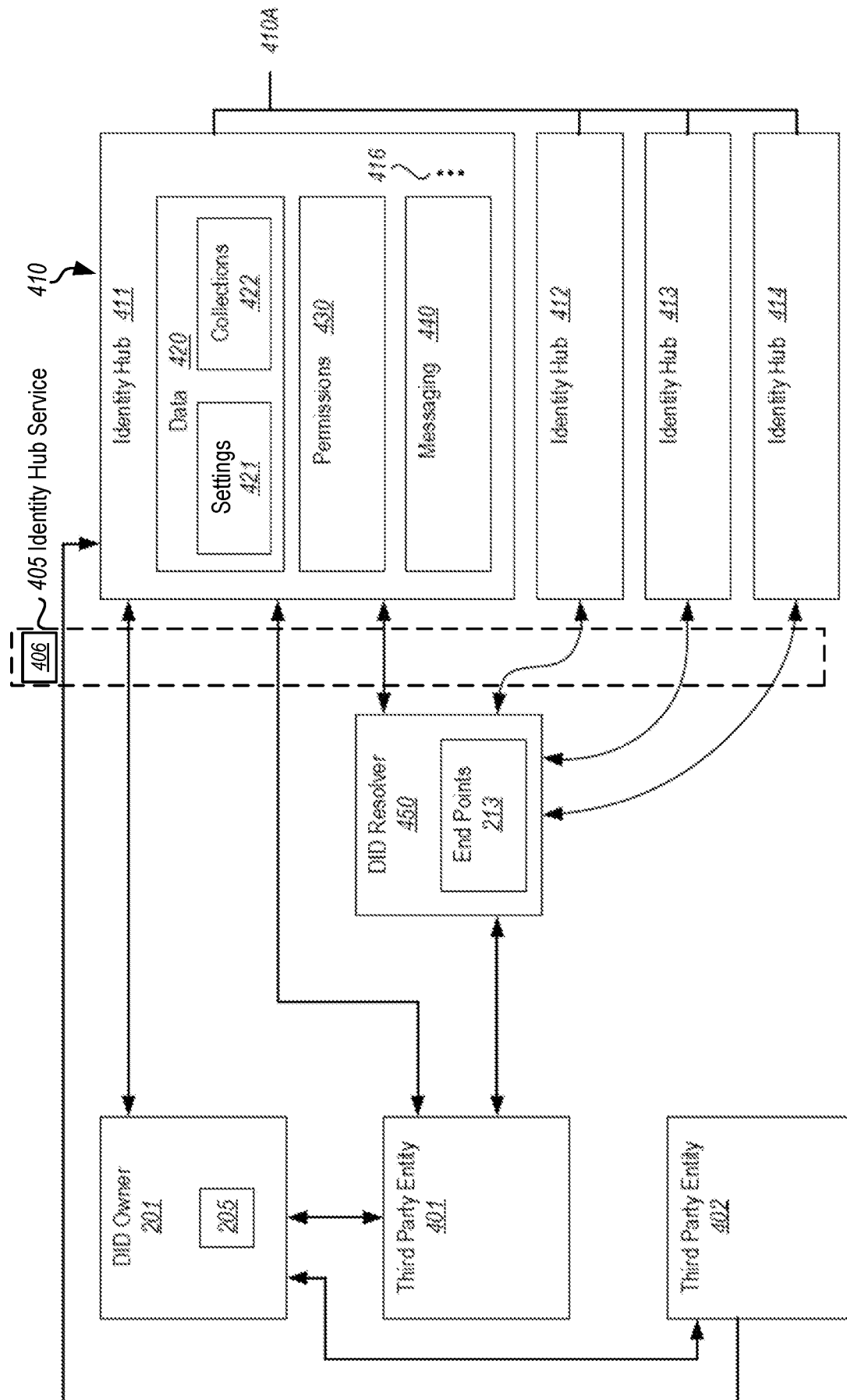


FIG. 4

500

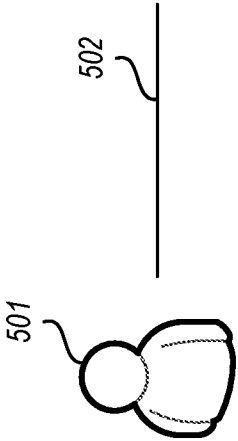
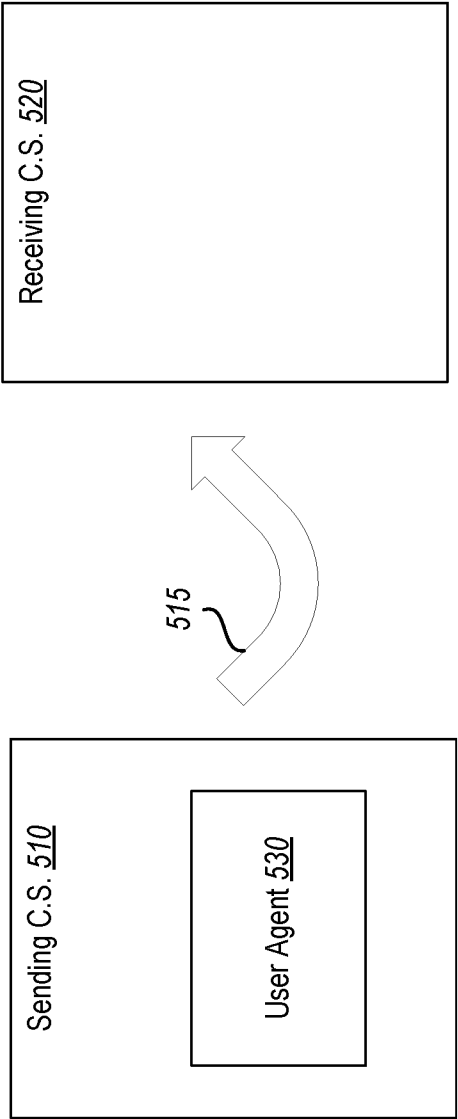


FIG. 5

600

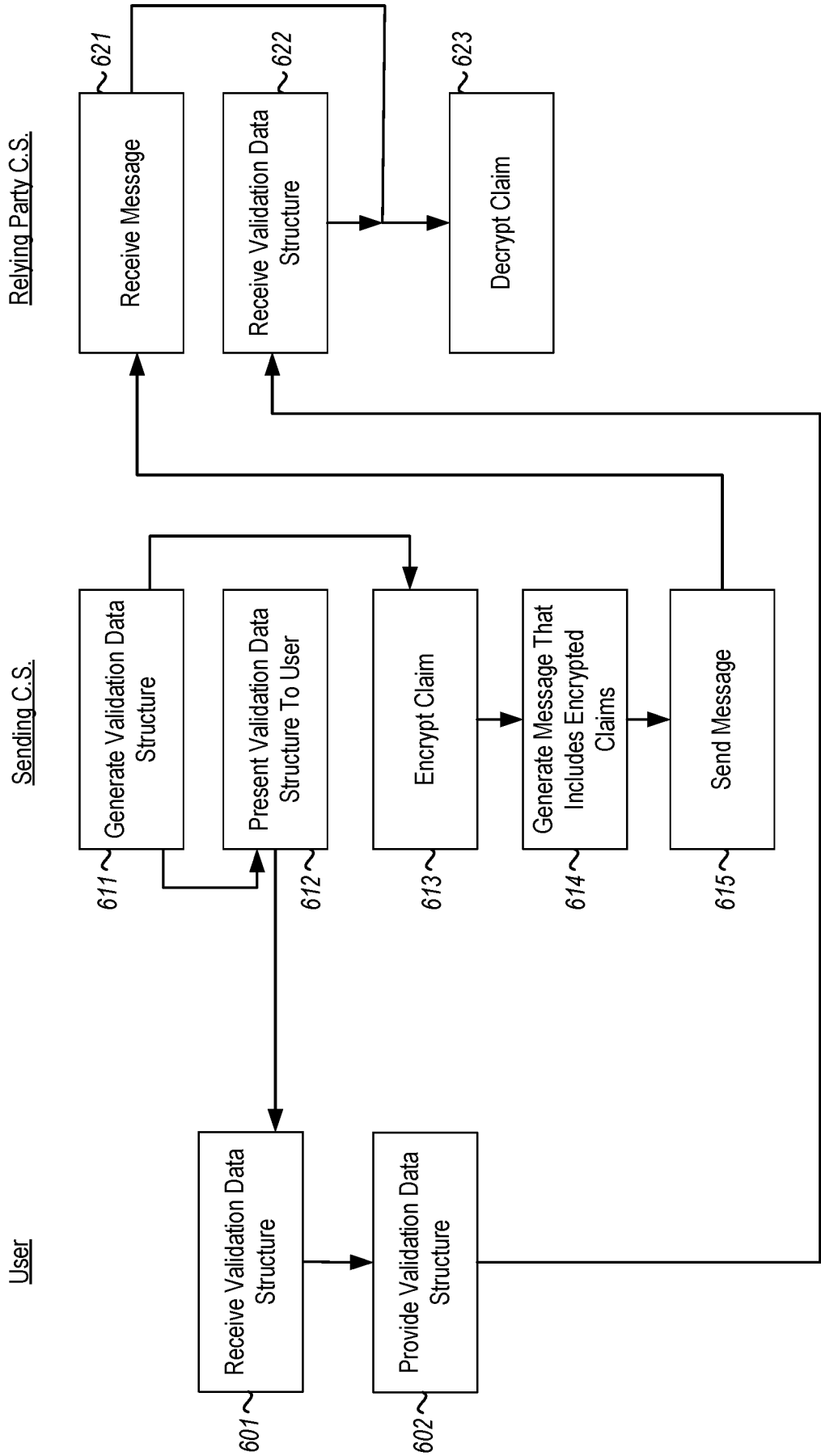
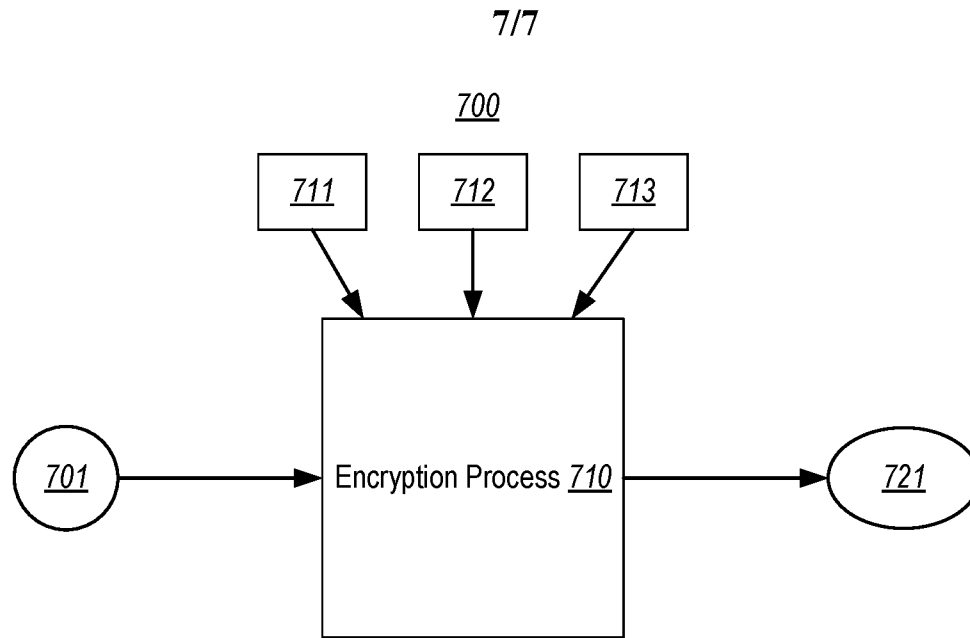
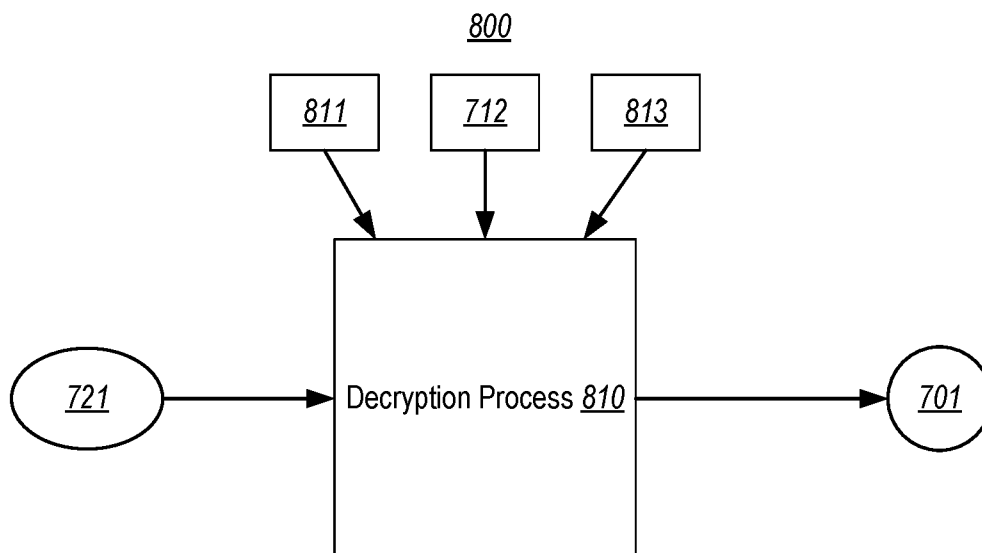


FIG. 6

**FIG. 7****FIG. 8**

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2020/034597

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/62 G06F21/64
ADD. G06F21/42

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)
G06F H04L

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	TAKEMIYA MAKOTO ET AL: "Sora Identity: Secure, Digital Identity on the Blockchain", 2017 IEEE 41ST ANNUAL COMPUTER SOFTWARE AND APPLICATIONS CONFERENCE (COMPSAC), IEEE, vol. 2, 23 July 2018 (2018-07-23), pages 582-587, XP033409765, ISSN: 0730-3157, DOI: 10.1109/COMPSAC.2018.10299 ISBN: 978-1-5386-2667-2 [retrieved on 2018-06-08]	1,10
Y	Abstract, Sections I-IV -----	2-9
Y	US 2019/097812 A1 (TOTH KALMAN CSABA [US]) 28 March 2019 (2019-03-28) paragraph [0015] - paragraph [0027] paragraph [0532] - paragraph [0566] ----- -/-	2-9



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

20 August 2020

Date of mailing of the international search report

28/08/2020

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Ghani, Hamza

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2020/034597

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Andrew Tobin ET AL: "Sovrin: What Goes on the Ledger? A white paper from Evernym in cooperation with the Sovrin Foundation. An overview of what's on the Sovrin distributed ledger and why", 31 October 2018 (2018-10-31), XP055723746, Retrieved from the Internet: URL:https://sovrin.org/wp-content/uploads/2018/10/What-Goes-On-The-Ledger.pdf [retrieved on 2020-08-19] the whole document -----	1,10
A	US 2018/117447 A1 (TRAN BAO [US] ET AL) 3 May 2018 (2018-05-03) paragraph [0296] - paragraph [0301] -----	1,10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2020/034597

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2019097812	A1	28-03-2019	NONE

US 2018117447	A1	03-05-2018	NONE
