



(43) International Publication Date
29 September 2016 (29.09.2016)

(10) International Publication Number
WO 2016/151407 A2

- (51) International Patent Classification: Not classified
- (21) International Application Number: PCT/IB2016/000883
- (22) International Filing Date: 25 March 2016 (25.03.2016)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
62/138,555 26 March 2015 (26.03.2015) US
62/216,039 9 September 2015 (09.09.2015) US
- (71) Applicant: ASSA ABLOY AB [SE/SE]; Klarabergs-
viadukten 90, SE-111 64 Stockholm (SE).
- (72) Inventors: LOVELOCK, Julian, Eric; 3705 Smallwood
Court, Pleasanton, CA 94566 (US). HOYER, Philip; 43
Manor Road, Richmond TW9 1YA (GB).
- (74) Agents: MUIRHEAD, Donald, W. et al.; Muirhead And
Saturnelli, Llc, 200 Friberg Parkway, Suite 1001, Westbor-
ough, MA 01581 (US).
- (81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG,
MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM,
PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC,
SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ,
TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU,
TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE,
DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,
LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished
upon receipt of that report (Rule 48.2(g))

(54) Title: VIRTUALIZED LICENSE DELIVERY

(57) Abstract: Providing virtualized credentials of a license holder includes authorizing a subset of credential data to be sent to a device of a relying party that is different from the license holder, where the subset of credential data depends on a role of the relying party and/or contextual data of the relying party and includes displaying the subset of credential data on a screen of the device of the relying party. The credential data may correspond to a license of the license holder. The license may be a driver's license. The credential data may include insurance information of the license holder. The contextual data may be a geolocation of the relying party. The device of the relying party may be a laptop, a cellphone, or a tablet. The credential data may be provided by a device of the li-
cense holder.



WO 2016/151407 A2

VIRTUALIZED LICENSE DELIVERY

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to U.S. Prov. App. No. 62/138,555, filed March 26, 2015, and entitled "VIRTUALIZED LICENSE DELIVERY" and U.S. Prov. App. No. 62/216,039, filed
5 September 9, 2015, and entitled "VIRTUALIZED LICENSE DELIVERY", both of which are incorporated by reference herein.

TECHNICAL FIELD

This application relates to the field of credentials and more particularly to the field of providing virtualized credentials.

10 BACKGROUND OF THE INVENTION

A license, such as a driver's license, has many uses for its holder that extend beyond the purpose for which the license was issued. For example, a license holder may present their driver's license to service provider to prove the age of the license holder in connection with purchasing liquor even though the purchase of liquor is unrelated to the issuance by a state of
15 the driver's license. Generally, a state issued driver's license is considered proof of identity and/or age in a number of situations unrelated to driving an automobile. The same may be true, perhaps to a lesser extent, to other types of licenses/credentials issued by government or other authorities.

A drawback to using licenses/credentials in this manner is that, in some cases, the
20 recipient receives more information than is needed. In some cases, this may be of no consequence. However, in other cases, the license holder may not want the recipient to have access to the additional/unneeded information. For example, a driver's license holder may present their license to a bartender in connection with purchasing liquor, but the holder may not want the bartender to have access to the home address that is provided on the driver's
25 license. A possible solution is to obtain another type of identification/proof of age credential that does not include a home address. However, this may not be practical for a number of reasons, such as the fact that the license/credential needs to be issued by an authority recognized by a recipient (e.g., the state registry of motor vehicles) and a user may not want to carry multiple licenses/credentials to be presented in different situations.

Accordingly, it is desirable to provide a license/credential that reduces the dissemination of unnecessary information while still being recognized and honored by a recipient.

SUMMARY OF THE INVENTION

5 According to the system described herein, providing virtualized credentials of a license holder includes authorizing a subset of credential data to be sent to a device of a relying party that is different from the license holder, where the subset of credential data depends on a role of the relying party and/or contextual data of the relying party and includes displaying the subset of credential data on a screen of the device of the relying party. The credential data
10 may correspond to a license of the license holder. The license may be a driver's license. The credential data may include insurance information of the license holder. The contextual data may be geolocation of the relying party. The device of the relying party may be a laptop, a cellphone, or a tablet. The credential data may be provided by a device of the license holder. The device of the license holder may communicate directly with the device of the relying party.
15 The credential data may be stored in a cloud and the subset of credential data may be sent from the cloud to the device of the relying party. The relying party may receive a release from the license holder that allows the relying party to view the subset of credential data.

 According further to the system described herein, a non-transitory computer-readable medium contains software that provides virtualized credentials of a license holder. The
20 software includes executable code that authorizes a subset of credential data to be sent to a device of a relying party that is different from the license holder, where the subset of credential data depends on a role of the relying party and/or contextual data of the relying party and includes executable code that causes the subset of credential data to be displayed on a screen of the device of the relying party. The credential data may correspond to a license of
25 the license holder. The license may be a driver's license. The credential data may include insurance information of the license holder. The contextual data may be geolocation of the relying party. The device of the relying party may be a laptop, a cellphone, or a tablet. The credential data may be provided by a device of the license holder. The device of the license holder may communicate directly with the device of the relying party. The credential data may
30 be stored in a cloud and the subset of credential data may be sent from the cloud to the device

of the relying party. The relying party may receive a release from the license holder that allows the relying party to view the subset of credential data.

According further to the system described herein, providing virtualized credentials of a license holder includes authorizing a subset of credential data to be sent to a device of a relying party that is different from the license holder, where the subset of credential data depends on a role of the relying party, selection by the license holder, and/or contextual data of the relying party and includes displaying the subset of credential data on a screen of the device of the relying party. The contextual data may be a privacy level setting and/or a geolocation of the relying party. The role of the relying party may be provided by the relying party. Role information provided by the relying party may be provided in a verifiable format, such as being digitally signed.

According further to the system described herein, a non-transitory computer-readable medium contains software that provides virtualized credentials of a license holder. The software includes executable code that authorizes a subset of credential data to be sent to a device of a relying party that is different from the license holder, where the subset of credential data depends on a role of the relying party, selection by the license holder, and/or contextual data of the relying party and includes executable code that causes the subset of credential data to be displayed on a screen of the device of the relying party. The contextual data may be a privacy level setting and/or a geolocation of the relying party. The role of the relying party may be provided by the relying party. Role information provided by the relying party may be provided in a verifiable format, such as being digitally signed.

User identity information could be anything that has a user's name and address, such as a QC code, image with watermark, etc. that is tied to a license, such as a driver's license, but also other types of licenses, such as a contracting licenses. The licensing information may be tied to insurance associated with that license. The licensing information may be displayed (read via wireless communication or by taking a photo of the information) from a cell phone of the license holder, and delivered to a cell phone (ipad, etc.) of a receiver. The identity of the license holder could optionally come from a web page where a service provided by the license holder is requested, or from an email from the license holder or from a proxy (for example

confirming an appointment for requested service) to allow the receiver to preview credentials of the provider.

The system described herein may use the cloud to translate identity of a user with an associated license. An id may include a virtual identity from a licensing board that also indicates where to retrieve an actual license, and any required access method information. Input of the user optionally includes a release from the providing party to allow the relying party to read the license/insurance data. The id and associated data may include an encrypted dynamic element to prevent a replay attack.

The relying party (possibly a police officer, or service provider such as a rental car agent) may receive on their cell phone (or a local display) a copy of the (drivers/auto) license, and any associated insurance and other data used by the receiver to validate the license holder, such as a biometric reference template. The received data is converted into graphical image(s) of the license which are displayed to a relying party. The graphical image(s) might be abbreviated in the case of poor communication lines or a small display. The format or content of an output may vary based on a wide range of conditions including the device type of the receiver, the role of the receiver and contextual data about the receiver such as geolocation. Optionally, the receiver may present their mobile device (i.e cell phone) for the license holder to enter their fingerprint data for validation.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the system described herein are explained with reference to the several figures of the drawings, which are briefly described as follows.

FIG. 1 is a schematic illustration showing a screen with driver's license information thereon according to an embodiment of the system described herein.

FIG. 2 is a schematic illustration showing a screen with a subset of driver's license information thereon according to an embodiment of the system described herein.

FIG. 3 is a schematic illustration showing a license holder device, a relying party device and a communications/cloud infrastructure according to an embodiment of the system described herein.

FIG 4 is a flow diagram illustrating processing performed by a communications/cloud infrastructure according to an embodiment of the system described herein.

DETAILED DESCRIPTION OF VARIOUS EMBODIMENTS

The system described herein provides a mechanism for selectively providing license information electronically

Referring to FIG. 1, a screen 100 is provided on a device, such as a smartphone, a tablet, etc. The screen 100 provides driver's license information, including date of birth, expiration, name, address, driver's license number, and a photograph of the owner of the driver's license. Any appropriate information/data may be provided as driver's license information, including a QC code, an image with watermark, etc. that is tied to the driver's license. In some cases, automobile insurance information may be associated with the driver's license. The driver's license holder may input some or all of the information and/or another entity/party (e.g. state registry of motor vehicles) may enter some or all of the information. Note also that, although the system described herein is illustrated in connection with a driver's license, other types of licenses may be used instead and, in fact, other types or credentials/documents may be used.

The screen 100 may correspond to a display on a device of the license holder and may be viewed by the license holder either upon request or possibly in connection with the license holder providing a password, fingerprint, and/or some other type of authentication.

Alternatively, the screen 100 may correspond to a screen on a device of a party other than the license holder (e.g., police officer, car rental agent, etc.) and the information provided on the screen 100 may be provided with or without the consent of the license holder, as described in more detail elsewhere herein. In some cases, information provided to a party other than the license holder (relying party) may include an indication of what the license holder used to validate/authorize a particular request.

Referring to FIG. 2, a screen 200 provided on a device is similar to the screen 100, discussed elsewhere herein, except that the screen 200 does not include all of the information provided on the screen 100. In some embodiments, the screen 200 may be presented on a device of the license holder in response to a specific input by the license holder to hide some of the information. For example, if the license holder uses the device/license to purchase liquor, the photograph, date of birth, and driver's license number may be useful, but the home

address of the license holder is not necessary and, in some cases, the license holder may wish to prevent another party, such as a bartender, from seeing home address of the license holder. Note that, instead of data of birth, it may be possible to provide (i.e., by default) just an indicator that the license holder is over 21. The license holder may control which data is presented on an ad hoc basis. For instance, the license holder may make a selection on their device not to display/send a home address when the relying party is, for example, a bartender.

In some cases, the role of the relying party may be provided to the license holder and the information provided to the relying party may depend upon the role of the relying party. For example, if the relying party has a role of "law enforcement", then more information (e.g., home address) may be provided to a relying party than would be provided to a relying party having a role of "bartender". In some cases, the role information may be provided in a format that can be verified (e.g., digitally signed) so that the license holder does not authorize information to be provided to someone fraudulently posing as a member of law enforcement.

It is also possible to provide or not provide specific information based on contextual data, such as geolocation of the license holder and/or relying party, where a photograph of the license holder is not provided in locations where photographs are discouraged for religious reasons. Note that, in some cases a subset of information is provided due to limitations in communication and/or the receiving device. For example, in instances communication bandwidth limitations might cause any provided graphic image to be abbreviated (reduced in size/resolution).

Alternatively, license holder information may be transmitted to a device of a party other than the license holder so that, for example, the screen 200 is provided on a device of a bartender that needs to determine if it is appropriate to serve alcohol to the license holder. The amount and type of information provided to a relying party may be controlled so that different parties receive different information according to the roll of the relying party. For example, a relying party having a role of "law enforcement" may be provided with all of the driver's license information while a relying party having a role "commercial service provider" may be provided with a subset of the information that does not include the home address of the driver's license holder. The license holder may control which data is sent to a recipient on an ad hoc basis. For instance, the license holder may make a selection on their device not to

display/send a home address when the relying party is, for example, a bartender, even if the relying party does not send role information to the device of the license holder. In some instances, the subset information provided may vary according to contextual data corresponding to a privacy level setting so that, for example, in some cases an actual data of birth is provided while in other cases only an indication that the license holder is over 21 is provided.

Referring to FIG. 3, a diagram 300 shows a network/cloud infrastructure 302, a license holder device 304, and a relying party device 306. The infrastructure 302 represents both communication mechanisms between the devices 304, 306, such as a cellular telephone network, and represents storage/processing that may be performed on behalf of the devices 304, 306. For example, information about the license holder may be stored in cloud storage (the infrastructure 302) and then conveyed to the relying party device 306 upon occurrence of a particular event, such as the license holder entering a password, fingerprint (or similar) on the license holder device 304 to authorize transferring information from the cloud to the relying party device. It is also possible for the the event to be simply close proximity of the devices 304, 306. For example, if the relying party is a law enforcement official, then it is possible to have the infrastructure 302 provide information about the license holder to the relying party device 306 in response to the license holder device 304 becoming proximate to the relying party device 306.

In other embodiments, information may be transferred from the license holder device 304 to the relying party device 306 either through the infrastructure 302 or via a more direct link 308 therebetween. Note that the link can be any type of data communication mechanism, such as an Internet connection, WiFi, a Bluetooth connection, etc. In some embodiments, the devices 304, 306 may be connected to each other using a physical wire, such as an electrical wire, a Fiber-optic link, etc. Information may be conveyed between the devices 304, 306 upon occurrence of a particular event, such as the license holder entering a password, fingerprint (or similar) on the license holder device 304 to authorize transferring information from the cloud to the relying party device close proximity of the devices 304, 306, as discussed elsewhere herein.

In some instances, the relying party device 306 may be a laptop or desktop computer (or similar) and information may be provided to the relying party via a Web page (or similar) that the relying party accesses, possibly only after the license holder provides authorization. It is also possible to provide information to the relying party via an email that is sent by the license holder or by a proxy, possibly after authorization of the license holder. Note that, in some cases, it is possible for a relying party to not have a device at all but, instead, to visually inspect the license holder device 304 and/or take a photograph of the screen thereof.

Referring to FIG. 4, a flow diagram 400 illustrates steps performed in connection with the communications/cloud infrastructure 302 providing information to a relying party.

Processing begins at a first step 402 where a request is received. In some embodiments, the relying party requests the information from a license holder so the request received at the step 402 is from the relying party. In other embodiments, the request may be provided by the license holder to send the information to the relying party so that the request received at the step 402 is from the license holder. In either case, the request may include one or more tokens, or similar, that does not directly identify the license holder (and may or may not directly identify the relying party). Following the step 402 is a step 404 where the token(s) are matched by the infrastructure 302 to information for the license holder and/or the relying party. In some cases, the token(s) may indicate where to retrieve the requested license information and possibly required access information (i.e., credentials for remote systems that are accessed). Following the step 404 is a test step 406 where it is determined if the request is authorized. As discussed elsewhere herein, it may be necessary for the license holder to provide authorization in the form of a password, fingerprint, etc. In some cases, the license holder may need to provide a release to authorize the relying party to read the license information, including possibly information about insurance. Note that authorization may include having the relying party (e.g., a police officer) present their device to the license holder who then provides a password, a fingerprint, etc. to the device of the relying party.

If it is determined at the 406 that the request is not authorized, then processing is complete (i.e., no information will be provided). Otherwise, control transfers from the test step 406 to a step 408 where the requested information is encrypted with a dynamic element (to guard against replay attacks). Following the step 408, control transfers to a step 412 where

the requested information is sent to the relying party. Following the step 412, processing is complete.

Various embodiments discussed herein may be combined with each other in appropriate combinations in connection with the system described herein. Additionally, in some instances, the order of steps in the flowcharts or flow diagrams may be modified, where appropriate. Further, various aspects of the system described herein may be implemented using software, hardware, a combination of software and hardware and/or other computer-implemented modules or devices having the described features and performing the described functions. Software implementations of the system described herein may include executable code that is stored in a computer readable storage medium and executed by one or more processors. The computer readable storage medium may include a computer hard drive, ROM, RAM, flash memory, portable computer storage media such as a CD-ROM, a DVD-ROM, a flash drive and/or other drive with, for example, a universal serial bus (USB) interface, and/or any other appropriate tangible storage medium or computer memory on which executable code may be stored and executed by a processor. The system described herein may be used in connection with any appropriate operating system.

Other embodiments of the invention will be apparent to those skilled in the art from a consideration of the specification or practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only.

What is claimed is:

1. A method of providing virtualized credentials of a license holder, comprising:
authorizing a subset of credential data to be sent to a device of a relying party that is
different from the license holder, wherein the subset of credential data depends on at least
5 one of: a role of the relying party and contextual data of the relying party; and
displaying the subset of credential data on a screen of the device of the relying party.
2. A method, according to claim 1, wherein the credential data corresponds to a license of the
license holder.
3. A method, according to claim 2, wherein the license is a driver's license.
- 10 4. A method, according to claim 3, wherein the credential data includes insurance information
of the license holder.
5. A method, according to claim 1, wherein the contextual data is geolocation of the relying
party.
6. A method, according to claim 1, wherein the device of the relying party is one of: a laptop, a
15 cellphone, or a tablet.
7. A method, according to claim 1, wherein the credential data is provided by a device of the
license holder.
8. A method, according to claim 7, wherein the device of the license holder communicates
directly with the device of the relying party.
- 20 9. A method, according to claim 1, wherein the credential data is stored in a cloud and the
subset of credential data is sent from the cloud to the device of the relying party.
10. A method, according to claim 1, wherein the relying party receives a release from the
license holder that allows the relying party to view the subset of credential data.

11. A non-transitory computer-readable medium containing software that provides virtualized credentials of a license holder, the software comprising:

executable code that authorizes a subset of credential data to be sent to a device of a relying party that is different from the license holder, wherein the subset of credential data depends on at least one of: a role of the relying party and contextual data of the relying party;
5 and

executable code that causes the subset of credential data to be displayed on a screen of the device of the relying party.

12. A non-transitory computer-readable medium, according to claim 11, wherein the credential
10 data corresponds to a license of the license holder.

13. A non-transitory computer-readable medium, according to claim 12, wherein the license is a driver's license.

14. A non-transitory computer-readable medium, according to claim 13, wherein the credential data includes insurance information of the license holder.

15. 15. A non-transitory computer-readable medium, according to claim 11, wherein the contextual data is geolocation of the relying party.

16. A non-transitory computer-readable medium, according to claim 11, wherein the device of the relying party is one of: a laptop, a cellphone, or a tablet.

17. A non-transitory computer-readable medium, according to claim 11, wherein the credential
20 data is provided by a device of the license holder.

18. A non-transitory computer-readable medium, according to claim 17, wherein the device of the license holder communicates directly with the device of the relying party.

19. A non-transitory computer-readable medium, according to claim 11, wherein the credential data is stored in a cloud and the subset of credential data is sent from the cloud to the device
25 of the relying party.

20. A non-transitory computer-readable medium, according to claim 11, wherein the relying party receives a release from the license holder that allows the relying party to view the subset of credential data.

21. A method of providing virtualized credentials of a license holder, comprising:

- 5 authorizing a subset of credential data to be sent to a device of a relying party that is different from the license holder, wherein the subset of credential data depends on at least one of: a role of the relying party, selection by the license holder, and contextual data of the relying party; and
- displaying the subset of credential data on a screen of the device of the relying party.

10 22. A method, according to claim 21, wherein the contextual data is at least one of: a privacy level setting and geolocation of the relying party.

23. A method, according to claim 21, wherein the role of the relying party is provided by the relying party.

15 24. A method, according to claim 23, wherein role information provided by the relying party is provided in a verifiable format.

25. A method, according to claim 24, wherein the role information is digitally signed.

26. A non-transitory computer-readable medium containing software that provides virtualized credentials of a license holder, the software comprising:

- 20 executable code that authorizes a subset of credential data to be sent to a device of a relying party that is different from the license holder, wherein the subset of credential data depends on at least one of: a role of the relying party, selection by the license holder, and contextual data of the relying party; and
- executable code that causes the subset of credential data to be displayed on a screen of the device of the relying party.

25 27. A non-transitory computer-readable medium, according to claim 26, wherein the contextual data is at least one of: a privacy level setting and geolocation of the relying party.

28. A non-transitory computer-readable medium, according to claim 26, wherein the role of the relying party is provided by the relying party.

29. A non-transitory computer-readable medium, according to claim 28, wherein role information provided by the relying party is provided in a verifiable format.

- 5 30. A non-transitory computer-readable medium, according to claim 29, wherein the role information is digitally signed.



FIG. 1



FIG. 2

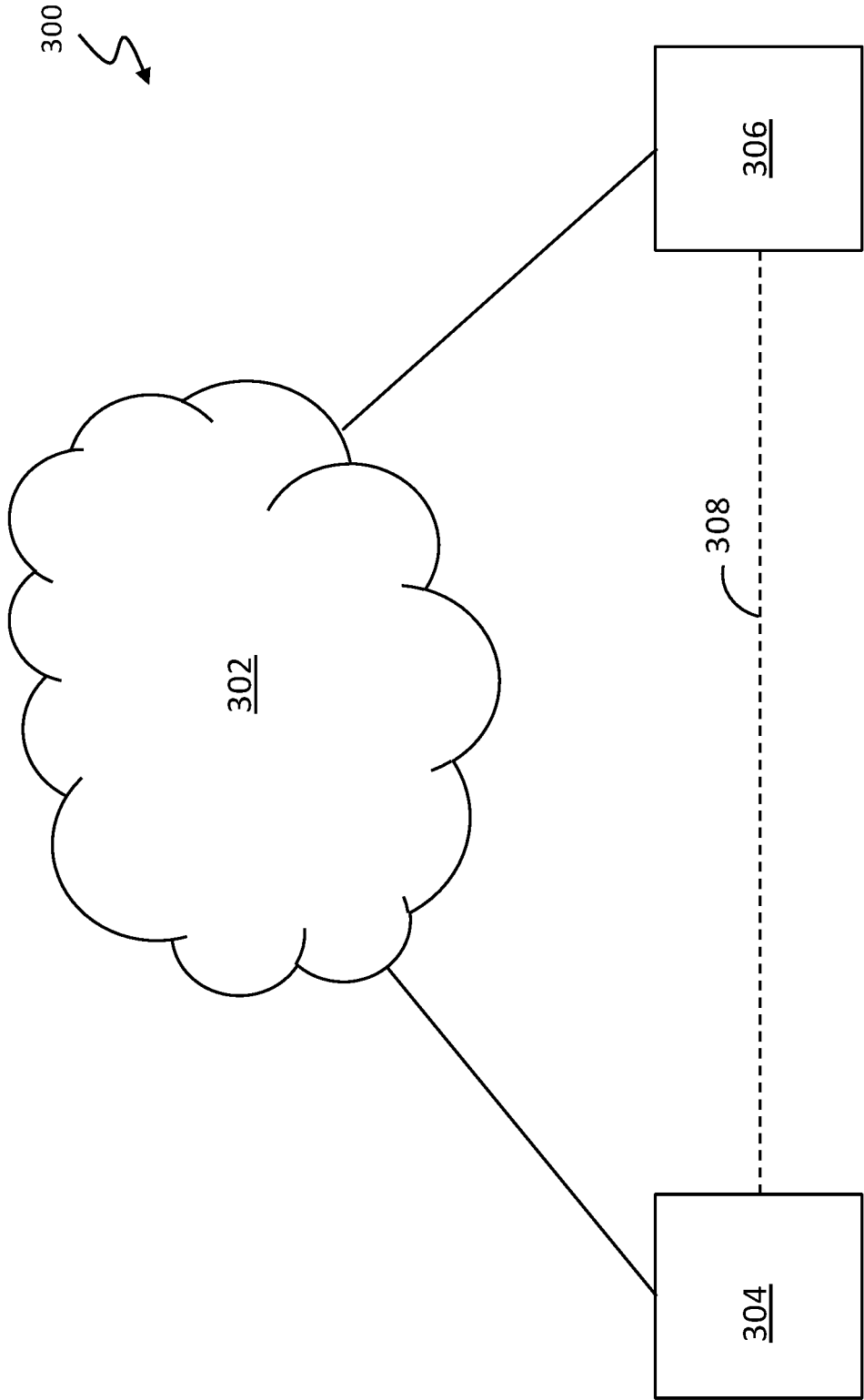


FIG. 3

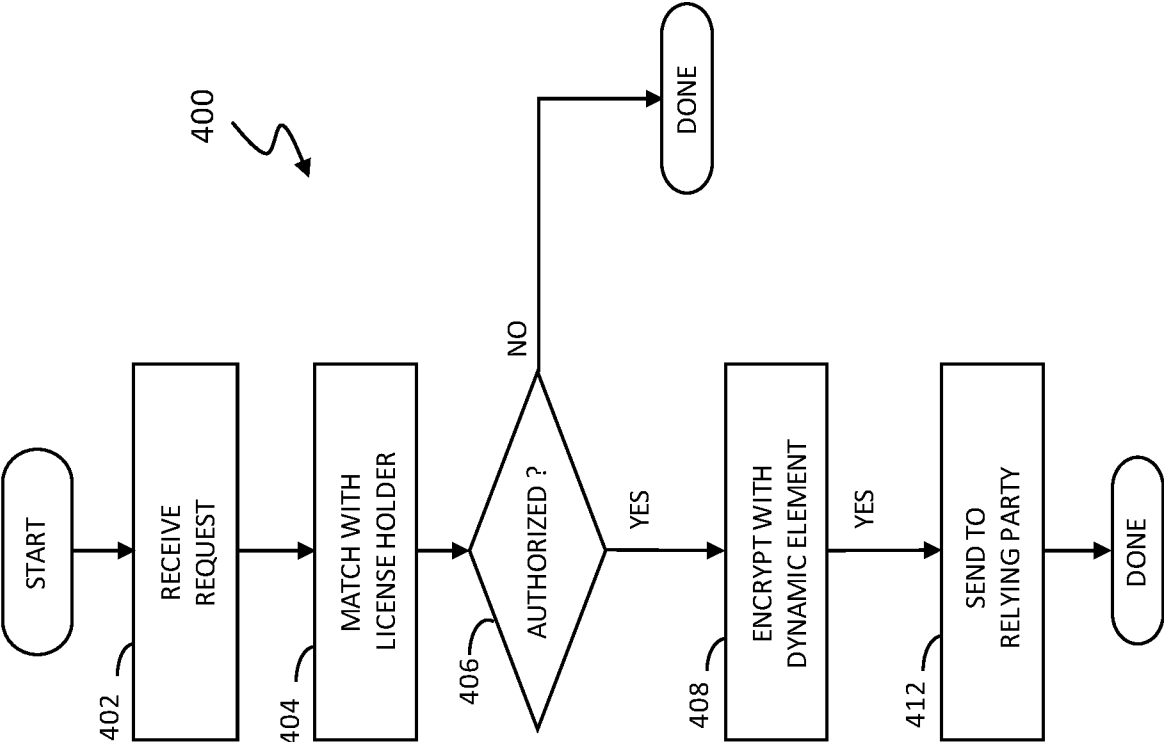


FIG. 4