



- (51) **International Patent Classification:**
G06F 15/16 (2006.01) *H04L 9/32* (2006.01)
- (21) **International Application Number:**
PCT/SE2013/050813
- (22) **International Filing Date:**
28 June 2013 (28.06.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant:** TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) [SE/SE]; SE-164 83 Stockholm (SE).
- (72) **Inventors:** JOKELA, Petri; Kukkaromäki 6G14, FI-02770 Espoo (FI). AHMED, Abu Shohel; Lintukorventie 2F 71, FI-02660 Espoo (FI).
- (74) **Agent:** EGRELIUS, Fredrik; Ericsson AB, Patent Unit Kista DSM, SE-16480 Stockholm (SE).
- (81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,

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

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

Published:

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

(54) **Title:** IDENTITY MANAGEMENT SYSTEM

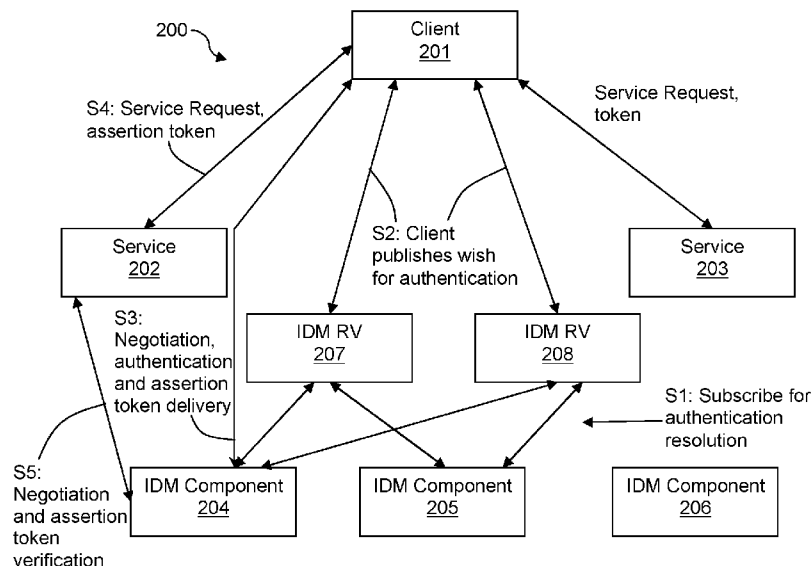


Figure 2

(57) **Abstract:** There is described a system for authenticating a client device in a network having a plurality of IDM components. One or more of the IDM components subscribes (using the publish-subscribe message pattern) to authentication requests published by client devices. The client device publishes an authentication

[Continued on next page]

request into the network. The most appropriate IDM component to process the published authentication request is selected, and the authentication request forwarded to the selected IDM component. The selected IDM component is then operated to negotiate with and authenticate the client device.

IDENTITY MANAGEMENT SYSTEM

Technical Field

- 5 The present invention relates to an identity management system. In particular, the invention relates to a scalable identity management system usable in distributed systems.

Background

10

Identity and access management (IDM) is an important component of computing based systems and networks. The purpose of an IDM is to allow legitimate users to access resources. IDM systems have evolved over the years, from centralised to distributed access control, from multiple logons to a single sign-on mechanism, from backend
15 federation to frontend federation, and so on. The appropriate nature of IDM depends on the nature of the whole system.

The introduction of distributed systems such as Cloud brings new features and challenges for IDM systems. Cloud provides an abstraction of unlimited resources to
20 consumers. The resources of a cloud are shared among the consumers (tenants) using a concept called multi-tenancy. This allows multiple tenants to share (use) the same physical resource on a pay per use basis. One of the main characteristics of the cloud system is scalability and elasticity. Scalability ensures that the cloud abstracted resources increase or decrease (horizontally scale) their capacity based on the load of
25 the system. To ensure this, cloud based services are designed in a modular fashion so that each service can be scaled by adding or deleting an instance of that service. This also applies to the identity and access management system.

In the cloud, the cloud service provider (CSP) will require an easy way to control
30 access to resources in the system. One way of addressing this requirement is with a centralised IDM solution. One possible approach for centralised access control is illustrated in Figure 1, which is a schematic diagram of elements of a network 100 including a client 101, identity server 102, and two service providers 103, 104. If the client 101 wishes to access a service provided by one of the service providers 103, it

authenticates itself with the identity server 102. As a result of authentication process an assertion token is returned to the client 101. This token is subsequently used by the client 101 to provide proof of identity (and/or of authorisation to use the requested service) to the service provider 103, which can be thought of as an identity consumer.

5 It may be that the client is able to access a different service, for example from another service provider 104, without first having to obtain a specific assertion token.

This approach is widely used by many computer systems. A typical network authentication protocol provides mutual authentication in a client-server fashion (*i.e.*,
10 the client and the server authenticate each other). One possible approach involves the client authenticating with the Authentication server to receive a 'Ticket' for a particular service. The 'Ticket' is further used to access the desired service. The drawback of this approach is the centralised authentication server, which represents a single point of failure.

15 In contrast, distributed authentication mechanisms generally allow users, and parties that rely on proof of identity (identity consumers), to choose an identity provider for authentication from a set of identity providers. This eliminates the need to have a single identity provider for user authentication. The problem with this approach is the
20 establishment of a trust anchor – *i.e.*, to establish trust of an identity provider by the identity consumers.

Centralised identity systems provide easy maintenance and control over the system. However, centralisation is not a good choice for the cloud and distributed systems due
25 to the problem of a single point of failure. In a cloud ready system (application), all components should be elastic and horizontally scalable. Currently available centralised identity management systems do not achieve this property. It would therefore be desirable to achieve both the control flexibility of a centralised identity system and the scalability of a distributed system

30

Summary

In accordance with one aspect of the present invention there is provided a client device in a network having a plurality of IDM components. The client device comprises a

- processor and a memory. The memory contains instructions executable by said processor to cause the processor to generate a request for authentication and publish the authentication request into the network *via* an input/output unit operably connected to the processor. The authentication request is published using a publish-subscribe message pattern. The instructions further cause the processor to receive an authentication initiation message from one of the IDM components in the network, and negotiate the receipt of authentication information from the IDM component. Each IDM component may have its own set of capabilities regarding the authentication process.
- 5
- 10 The instructions may be configured to cause the processor to request a service from a service provider in the network and to send the authentication information to the service provider. The authentication information may include an assertion token, which is optionally service-specific.
- 15 The authentication initiation message from the IDM component may include a certificate of the IDM component, and the instructions may be configured to cause the processor to verify the certificate. The negotiation may include the establishment of a secure session with the IDM component.
- 20 The authentication request may include an operational parameter of the client device. This may include a capability of the client device (*e.g.*, the client device is mobile or supports particular authentication protocols) or a preference (*e.g.*, IDM components should be located in a particular region, IDM components should supports two factor authentication mechanism).
- 25
- In accordance with another aspect of the present invention there is provided an IDM component in a network having a plurality of IDM components. The IDM component comprises a processor and a memory. The memory contains instructions executable by said processor to cause the processor to subscribe, *via* an input/output unit, to authentication requests published in the network. The instructions further cause the processor to receive an authentication request published by a client device, initiate a negotiation with the client device, and authenticate the client device or a user of the client device.
- 30

The authentication of the client device may include sending an assertion token to the client device.

5 The instructions may be configured to cause the processor to receive a verification request from a service provider in the network, the verification request including an identifier of the client device or user or the assertion token, and verify the authentication of the client device or user or assertion token to the service provider. The IDM component may obtain the verification request by subscribing to verification requests published in the network, so that the verification request received from the
10 service provider is a verification request published by the service provider using a publish-subscribe message pattern.

The subscription to the authentication request (and/or verification request) may be at a broker in the network. The published authentication request and/or verification request
15 may be received from said broker. The subscription may include details of the capabilities of the IDM component, such as a region of the IDM component, authentication protocols available to the IDM component, availability of IDM component, number of authentications currently being handled by IDM component.

20 The authentication negotiation may include sending a certificate to the client device. The certificate may be obtained from a certification authority in a trusted domain. The instructions may be configured to cause the processor to share authentication states with other IDM components in the network. In other words each IDM component can work independently, needing to share only the authentication states with other such
25 IDM components.

Thus a certification authority can effectively “delegate” authentication to distributed IDM components. The IDM components can be trusted by the client because of the certificate from a trusted domain, However the client does not need to know which IDM
30 component to contact, and need only publish an authentication request, which is forwarded (optionally by a broker) and allows the selection of the most appropriate IDM node. One IDM component can thus be selected from a plurality of IDM components with varying capability without the client needing to make this selection. The IDM components can share authentication states. This removes binding between the client

and the IDM component by decoupling the authentication process: assertion generation and verification steps may be carried out by different components. Furthermore, the IDM component may subscribe to specific formatted authentication requests, e.g. those in which the client specifies operational preferences and its
5 identity, which facilitates the later stage for the IDM component to start negotiation with the client.

In accordance with another aspect of the present invention there is provided a service provider in a network having distributed IDM components. The service provider
10 comprises a processor and a memory. The memory contains instructions executable by said processor to cause the processor to receive, *via* an input/output device, a service request from a client device in the network, said service request including an authentication of the client and/or an assertion token and an identification of one of the IDM components in the network. The instructions are further configured to cause the
15 processor to send a verification request to the IDM component, receive a verification from the IDM component of the client authentication and/or assertion token, and deliver the requested service to the client device.

Alternatively, the service provider may request verification by publishing a verification
20 request rather than contacting the IDM component directly. Accordingly, in accordance with another aspect of the present invention there is provided a service provider in a network having distributed IDM components. The service provider comprises a processor and a memory. The memory contains instructions executable by said processor to cause the processor to receive, *via* an input/output device, a
25 service request from a client device in the network, said service request including an authentication of the client and/or an assertion token. The instructions are further configured to cause the processor to publish a verification request into the network, receive a verification, from one of the IDM components in the network, of the client authentication and/or assertion token, and deliver the requested service to the client
30 device.

In accordance with another aspect of the present invention there is provided a rendezvous (RV) node or broker in a network having distributed IDM components. The broker comprises a processor and a memory. The memory contains instructions

executable by said processor to cause the processor to receive, from at least one of the IDM components *via* an input/output device, a subscription to authentication requests (813). The instructions are further configured to cause the processor to receive an authentication request published by a client device in the network,
5 determine if the subscription matches the published authentication request, and forward the authentication request to one of the at least one IDM components.

The instructions may be configured to cause the processor to determine if capabilities of the IDM component included in the subscription are suitable for the authentication
10 request.

The instructions may be configured to cause the processor to receive, from the IDM component or another IDM component in the network, a subscription to verification requests, to receive a verification request published by a service provider in the
15 network, to determine if the subscription matches the published verification request, and to forward the verification request to the IDM component.

In accordance with another aspect of the present invention there is provided a method of authenticating a client device in a network having a plurality of IDM components.
20 The method comprises, at the client device, publishing an authentication request using a publish-subscribe message pattern into the network. The client device receives an authentication initiation message from one of the IDM components in the network, and negotiates receipt of authentication information, optionally including an assertion token, from the IDM component. The client device may request a service from a service
25 provider in the network and send the assertion token to the service provider to provide authorisation (proof of claim) for service delivery.

In accordance with another aspect of the present invention there is provided a method of authenticating a client device in a network having a plurality of IDM components.
30 The method comprises, at one of the IDM components, subscribing to authentication requests in the network. The IDM component receives an authentication request published by a client device, initiates a negotiation with the client device, and authenticates the client device, optionally sending an assertion token to the client device following the negotiation.

The IDM component may receive a verification request from a service provider (202) in the network, the verification request including an identifier of the client device or the assertion token, and verifying the authentication of the client device or assertion token
5 to the service provider. The verification request may be received as a result of subscribing to verification requests published in the network, in which case the verification request received from the service provider is a verification request published by the service provider.

10 The method may include the IDM component subscribing to authentication requests at a broker in the network, and receiving the published authentication request from said broker.

The method may include distributing information between IDM components in the
15 network.

In accordance with another aspect of the present invention there is provided a method of providing a service in a network having a plurality of IDM components. The method comprises, at a service provider, receiving a service request from a client device in the
20 network, said service request including an authentication of the client and/or an assertion token and an identification of one of the IDM components in the network. The service provider sends a verification request to the IDM component, receives a verification from the IDM component of the client authentication and/or assertion token, and delivers the requested service to the client device.

25

In accordance with another aspect of the present invention there is provided a method of providing a service in a network having a plurality of IDM components. The method comprises, at a service provider, receiving a service request from a client device in the network, said service request including an authentication of the client and/or an
30 assertion token. The service provider publishes a verification request into the network, receives a verification from one of the IDM components of the client authentication and/or assertion token, and delivers the requested service to the client device.

In accordance with another aspect of the present invention there is provided a method of brokering an authentication request in a network with distributed IDM components. The method comprises receiving, at a broker, from an IDM component in the network, a subscription to authentication requests. The broker further receives an authentication request published by a client device in the network, determines if the subscription matches the published authentication request, and forwards the authentication request to the IDM component. The method may further include the IDM component matching received authentication requests to capabilities of IDM components subscribed.

10 In accordance with another aspect of the present invention there is provided a method of authenticating a client device in a network having a plurality of IDM components. The method comprises one or more of the IDM components subscribing to authentication requests published by client devices, and the client device publishing an authentication request into the network. The method further comprises the network or
15 a broker selecting the most appropriate IDM component to process the published authentication request and forwarding the authentication request to the selected IDM component, and operating the selected IDM component to negotiate with and authenticate the client device.

20 The steps of selecting (404) the most appropriate IDM component to process the published authentication request and forwarding the authentication request to the selected IDM component may be carried out at a broker in the network. The one or more IDM components may subscribe to authentication requests at said broker. The broker may match received authentication requests to capabilities of subscribed IDM
25 components.

The network may include a plurality of brokers, and the method may further comprise monitoring traffic through all of the brokers and/or IDM components, identifying when traffic to one or more IDM components exceeds a predetermined threshold, and
30 provisioning additional IDM components.

The authentication of the client device may include sending an assertion token from the IDM component to the client device. The method may further comprise the client device requesting a service (409) from a service provider (202) in the network and

sending the assertion token to the service provider to provide authorisation for service delivery.

5 The service provider may publish a verification request into the network. One or more IDM components may subscribe to verification requests. The most appropriate IDM component to process the verification request may be selected, the verification request forwarded to the selected IDM component; and the selected IDM component operated to negotiate with and verify the assertion token to the service provider.

10 The invention also provides a computer program comprising computer readable code which, when run on a device, causes it to behave as the device described above.

15 The invention also provides a computer program comprising computer readable code which, when run on a device, causes the device to execute the method described above.

The invention also provides a memory comprising a computer program as described above and a computer readable means on which the computer program is stored. The memory may be arranged in the form of a computer program product.

20

The invention also provides a vessel or vehicle comprising the client device described above.

Brief Description of the Drawings

25

Some preferred embodiments of the invention will now be described by way of example only and with reference to the accompanying drawings, in which:

30 Figure 1 is a schematic drawing of a elements of a network having a centralised identity management provider;

Figure 2 is a schematic diagram of elements of a network having a distributed IDM system;

Figure 3 is a schematic diagram of elements of a network similar to Figure 2 having an alternative verification pathway;

Figure 4 is a signalling diagram showing an exemplary workflow for the implementation
5 of service provision in the network of Figure 3;

Figures 5A and 5B are schematic diagrams illustrating alternative implementations of a client device;

10 Figures 6A and 6B are schematic diagrams illustrating alternative implementations of an IDM component;

Figures 7A and 7B are schematic diagrams illustrating alternative implementations of a service provider;
15

Figures 8A and 8B are schematic diagrams illustrating alternative implementations of a rendezvous (RV) point; and

Figure 9 is a schematic diagram illustrating a vehicle including a client device.
20

Detailed Description

Figure 2 is a schematic diagram of elements of a network 200 having a distributed Identity Management (IDM) system. The distributed IDM system makes use of
25 message-oriented architecture, such as a publish-subscribe pattern. Publish/subscribe is a message pattern consisting of publishers (senders) and subscribers (receivers). A publisher publishes messages (information) without the knowledge of who is going to consume the message: the messages are not sent to specific recipients. Subscribers consume messages based on specific topics or interests. Many publish/subscribe
30 paradigms include a broker in between the publisher and subscriber to perform filtering of messages. The subscriber registers with the broker, commonly known as a Rendezvous (RV) point.

The network 200 of Figure 2 includes a client 201 and one or more service providers 202, 203. In addition the network includes a plurality of IDM components 204, 205, 206, and one or more RV points (brokers) 207, 208.

- 5 The IDM components 204-206 collectively represent a distributed authentication provider. Individual IDM components 204, 205 may subscribe S1 to one or more of the RV points 207, 208 to confirm that those IDM components are available to provide authentication for some or all users. For example, one IDM component 204 may be available to authenticate users in a particular region, or users operating a particular authentication protocol, or even a number of users up to a predefined maximum. The
10 subscription sent to the RV points 207, 208 includes may include details of any such restrictions.

- When a user wishes to access a service, the client 201 publishes a request for authentication S2. The request may include the identity of the client and/or user, and
15 may also include an indication of the service for which authentication is required. The published request is received by at least one RV point (broker) 207, which registers the request. It will be appreciated that the authentication can be applied to anything related to the device that can be authenticated: examples include a SIM (in any form),
20 a subscription, or an individual person or object, but is not limited to such entities.

- The RV 207 maintains subscriptions from one or more IDM components, and searches for a match between the requirements of the subscriptions (e.g. region in which the user is located) and the details of the authentication request. When a match is found,
25 the RV 207 delegates the client's wish request to one of the IDM components 204. The IDM component 204 communicates directly with the client 201 and performs a negotiation and authentication operation S3, resulting (if successful) in delivery of an assertion token to the client 201. It will be appreciated that there may be one or many potential IDM components 204, 205 all capable of resolving the same authentication
30 request. This ensures high availability of identity operation. If necessary, the RV 207 chooses one IDM component (among many registered subscribers) for a particular client request. In situations where more than one IDM RV receive the same publication of an authentication request, they may negotiate among themselves to select an IDM component.

After completion of the authentication process, the client 201 receives some form of authentication information, which may include an assertion token. The client makes a service request S4 to one of the service providers (identity consumers) 202, using the
5 assertion token as proof of identity. The service, in turn, verifies the assertion S5. In the implementation shown in Figure 2, this verification is implemented by the service provider communicating directly with the IDM component 204. This requires the IDM component 204 to include its own identity to the client during the authentication process, so that the client can pass this identity on to the service provider 202, and
10 then the service provider can contact the same IDM component 204 to verify the assertion token.

An alternative implementation for the service provider to verify the assertion token is illustrated in Figure 3. Steps S1 to S4 are identical to those shown in Figure 2, but in
15 this implementation the service provider 202 and IDM component 204 again use the publish/subscribe message pattern to assist with the verification process. Once the service provider 202 has received the service request and assertion token S4, it publishes a request S6 for assertion token verification. The IDM components 204-206 are subscribed to the RV points (brokers) 207, 208 for verification as well as for
20 authentication, and one of the RV points 207 selects a suitable IDM component 204 subscribed to it for solving the assertion verification wish. The selected IDM component 204 then contacts the service provider 201 in step S7 to verify that the assertion token is legitimate.

25 It will be appreciated that the IDM components 204-206 may share authentication states with each other, so it could be another IDM component that is selected by the RV 207 to contact the service provider 202 and verify the assertion token. The IDM components need not maintain state – in one implementation they store every successful assertion token along with the token policy to a shared database (not shown
30 in Figure 3). The IDM component will access the shared database to find the current state of an assertion token. This has the additional advantage that no IDM component 204 is a single point of failure, even between completion of authentication and verification of the assertion token: another IDM component can complete the verification process if necessary. This approach also makes it possible to use

whichever IDM component which is most appropriate in view of the resources available.

Figure 4 is a signalling diagram including an exemplary workflow for the implementation shown in Figure 3, showing the process between the client 201, service provider 202, RV point (broker) 207, and two IDM components 204, 205. For the purposes of this discussion it can be assumed that the client device has a mechanism, either pre-installed or through some trusted means, to verify the certificate of IDM components: this is discussed in more detail below. Each IDM component 204, 205 may have a public/private key pair signed by a trusted certificate authority. In the context of a cloud system, it could be the certification authority of the Cloud provider.

- 401,402. IDM components 203, 205 subscribe to the RV point 207 for authentication requests and verification requests.
- 403. Client 201 publishes authentication request which is received by the RV point 207.
- 404. The RV point 207 performs a matching and filtering operation to choose the IDM component most appropriate to satisfy the authentication request.
- 405. The RV point 207 forwards the authentication request to an appropriate IDM component 204.
- 406. IDM component 204 starts authentication negotiation with the client. For example, the IDM component 204 sends a negotiation initiation message, including its certificate, to the client 201. The client 201 verifies the certificate. The client establishes a secure session with the IDM component 204. The client 201 proves its user claim by, for example, presenting username and password pair.
- 407. The IDM component 204 verifies the user claim and generates an assertion token for a valid user claim.
- 408. The IDM component 204 sends the assertion token to the client 201.
- 409. The client 201 forwards the service request along with the assertion token to the intended service provider (identity consumer) 202.
- 410. The service provider 202 publishes a verification request which is received by the RV point 207.

- 5 411. The RV point 207 performs a matching and filtering operation to choose the most appropriate IDM component 204 to address the verification request. This may be the same IDM component 204 as that used for the original authentication process, or may be a different one. In this example it is shown as being the same one.
412. The RV point 207 forwards the verification wish request to the chosen IDM component 204.
- 10 413. Both the IDM component 204 (for verification) and the service provider 202 should establish trust, for example through a pre-shared certificate, before exchanging the assertion token. The IDM component 204 verifies the assertion token against the policy of the assertion token. If valid, it sends a positive reply to the service.
414. At this stage, the service provider 202 has proved the identity of the user and proceeds to fulfil the user request.

15

Filtering operations which may be carried out in steps 404 and 411 include (but are not limited to):

1. If all IDM components 204-206 are busy, RV 207 queues the message.
- 20 2. If RV 207 can identify that the user belongs to a particular region, it can forward the request to IDM components 204 in that region.
3. If the user request contains a particular filtering criteria, RV 207 can fulfil this during the forwarding step.
4. RV 207 can forward the message to IDM components which handle protocol specific authentication: for example, one IDM component may be responsible
25 for username/password authentication, and another IDM component may be responsible for PKI based authentication.
5. RV 207 may start another IDM component to handle system load, or may contact another entity to enable this other entity to do so.

30 Figure 5A is a schematic diagram illustrating some of the structure of one implementation of a client device 201. The client device 201 includes a processor 510, memory 511 and input/output unit 512 for communicating with other elements in the network. The memory 511 includes instructions executable by the processor 510 to operate the input/output unit 512, and further includes an authentication request

generation module 513 having instructions causing the processor to generate an authentication request, and an authentication request publication module 514 to cause the processor to publish that request. The memory also includes an authentication negotiation module 515 including instructions for the processor to negotiate receipt of authentication information such as an assertion token from an IDM component, and a service request module 516 including instructions for the processor to issue a service request to a service provider including the authentication information. The instructions 513-516 may be in the form of software introduced into the memory from a software product 517 such as a CD, DVD or disk.

Figure 5B illustrates an alternative implementation of the client device 201, in which the software modules described above have been replaced by hardware modules 513B, 514B, 515B, 516B.

Figure 6A is a schematic diagram illustrating some of the structure of one implementation of an IDM component 204. The IDM component includes a processor 610, memory 611 and input/output unit 612 for communicating with other elements in the network. The memory 611 includes instructions executable by the processor 610 to operate the input/output unit 612, and further includes a subscription module 613 having instructions causing the processor to subscribe to an authentication or verification request at one or more brokers, and an authentication request receipt module 614 to cause the processor to receive a request from a broker. The memory also includes an negotiation initiation module 615 including instructions for the processor to send a negotiation initiation message, possibly including a certificate, to a client device following receipt of the authentication request, and an authentication module 616 including instructions for the processor to authenticate the client device. A similar set of modules may also be used for a request for verification from a service provider. The instructions 613-616 may be in the form of software introduced into the memory from a software product 617 such as a CD, DVD or disk.

Figure 6B illustrates an alternative implementation of the IDM component 204, in which the software modules described above have been replaced by hardware modules 613B, 614B, 615B, 616B.

Figure 7A is a schematic diagram illustrating some of the structure of one implementation of a service provider 202. The service provider 202 includes a processor 710, memory 711 and input/output unit 712 for communicating with other elements in the network. The memory 711 includes instructions executable by the processor 710 to operate the input/output unit 712, and further includes a service request receipt module 713 having instructions causing the processor to receive a service request (including an assertion token or other authorisation) from a client device, and a send/publish verification request module 714 to cause the processor to send a verification request to a specified IDM module (in the implementation of Figure 2) or publish a verification request (in the implementation of Figure 3). The memory also includes an verification receipt module 715 including instructions for the processor to receive verification from an IDM component, and a service delivery module 716 including instructions for the processor to provide the requested service to the client device. The instructions 713-716 may be in the form of software introduced into the memory from a software product 717 such as a CD, DVD or disk.

Figure 7B illustrates an alternative implementation of the service provider 202, in which the software modules described above have been replaced by hardware modules 713B, 714B, 715B, 716B.

Figure 8A is a schematic diagram illustrating some of the structure of one implementation of a broker such as a RV point 207. The broker 207 includes a processor 810, memory 811 and input/output unit 812 for communicating with other elements in the network. The memory 811 includes instructions executable by the processor 810 to operate the input/output unit 812, and further includes a subscription receiver module 813 having instructions causing the processor to receive subscriptions from IDM components in the network, and an authentication request receiver module 814 to cause the processor to receive published authentication requests and/or verification request from client devices and service providers. The memory also includes a publication/subscription matching module 815 including instructions for the processor to match the published authentication or verification requests to the subscriptions held and assign an IDM component to each authentication or verification request, and an authentication request forwarding module 816 including instructions for the processor to forward each authentication or verification request to a corresponding

selected IDM component. The instructions 813-816 may be in the form of software introduced into the memory from a software product 817 such as a CD, DVD or disk.

Figure 8B illustrates an alternative implementation of the RV point 207, in which the software modules described above have been replaced by hardware modules 813B, 814B, 815B, 816B.

Figure 9 is a schematic diagram illustrating a vehicle 901 including a client device 201.

10 In order for the system described above to operate effectively, it is important that service providers can trust the authentication provided by the IDM components. A trusted system is easy to achieve in a controlled domain. However, in a typical case a distributed system includes both trusted and un-trusted components. One possible trust model that addresses this problem is described below.

15 The user accesses the services and is in possession of authentication credentials.

The client device 201 is used by the user to access services. It can be assumed the client device is trusted.

20 The service provider 202, 203 does not trust the user and the user cannot trust the service provider before verifying the authenticity of the service provider. There can be malicious services, which reuse the assertion tokens, pretending to be a user towards another service.

25 The IDM components 204, 205, 206 perform users' authentication, generate authentication assertions, and perform assertion verification. These are trusted entities. However, there could be malicious components so component identity must be verified before communication.

30 The RV points (brokers) 207, 208 act as message matching and filtering points. They are un-trusted actors in this model. They can be considered as active network adversaries that overhear, intercept and synthesise messages.

All other components, including the network between the mentioned entities, are not trusted.

5 The process described above does not require a new authentication protocol, but enables scalability using existing authentication mechanisms.

10 Once subscriptions have been set up, the first message towards an RV (message 403 in Figure 4) is an authentication request from the client 201. An active attacker (malicious RV) could alter the client's request message or redirect the user to a malicious IDM component.

15 The IDM component 204 establishes a session with the client 201 during authentication (step 406 in Figure 4). During this process the client 201 makes sure that it is communicating with an authentic IDM component. One approach to establish authenticity of the IDM component is to verify its certificate by the client. Given that there are many IDM components, and the number may change dynamically, this can present a problem. One solution to this problem is that all IDM components have certificates from a trusted domain (by a trusted CA) and the client can verify the certificate of the IDM components using a pre-downloaded (or pre-installed) certificate
20 of the same trusted domain.

25 In message 409 of Figure 4, the client 201 delivers the assertion token to a service provider (identity consumer) 202 as a proof of claim. The client 201 needs to ensure that it is delivering the assertion token to the user-intended service provider *e.g.*, by verifying a service certificate. This will prevent the delivery of the assertion token to an un-trusted party. Other mechanisms can also be employed on the assertion token. For example, the assertion token may have a time limit, and the client must deliver it to the service provider before it expires. The assertion token may also be service specific - *i.e.*, only valid for a particular service.

30

The assertion token verification (message 410, Figure 4) from a service provider (identity consumer) to the RV 207 can be a publish request, indicating that it wants to verify some identity assertion. The RV 207 forwards the request to a subscriber (IDM component). Each service provider should set up necessary mechanisms to verify the

authenticity of the IDM components, e.g., mutual authentication, between the service provider and the IDM component. In one implementation, it may be that, the user assertion token itself is transferred from the service provider 202 to the IDM component 204 for verification.

5

The scalability of the approach described above lends itself to dynamic control of the number of IDM components. An orchestration entity or server (not shown) may monitor the traffic through all the RV points 207, 208, and identify when traffic to a particular IDM component exceeds a threshold, or when all traffic to IDM components exceeds a
10 threshold, at which point it may provision one or more additional IDM components to cope with the additional load. Similarly, if the traffic to one or more existing IDM components falls below a threshold they may be decommissioned if necessary. Similarly, if one IDM component fails the orchestration server can provision a replacement.

15

Thus the systems described above provide multiple workers (components) for identity and access control resolution - both for user authentication (assertion generation) and assertion verification for identity consumers (e.g. service providers). This provides scalability and elasticity for an identity system. Existing authentication protocols can be
20 integrated within the system.

It will be appreciated that variations from the examples provided above may still fall within the scope of the invention. For example, although the RV points or brokers are useful for the intelligent filtering that they can provide, it is possible to implement the
25 system without them. The IDM components can subscribe to messages published by client devices and/or service providers and act on these messages without the filtering provided by RV points or brokers.

CLAIMS:

1. A client device (201) in a network (200) having a plurality of identity management, IDM, components (204, 205, 206), the client device comprising:
 - 5 a processor (510) and a memory (511), said memory containing instructions executable by said processor to cause the processor to:
 - generate a request for authentication (513);
 - publish the authentication request (514) using a publish-subscribe message pattern into the network *via* an input/output unit (512) operably connected to the
 - 10 processor;
 - receive an authentication initiation message from one of the IDM components (204) in the network; and
 - negotiate the receipt of authentication information (515) from the IDM component.
- 15 2. The client device of claim 1, wherein the instructions are configured to cause the processor to request a service (516) from a service provider (202) in the network and to send the authentication information to the service provider.
- 20 3. The client device of claim 1 or 2, wherein the authentication information includes an assertion token.
4. The client device of claim 3, wherein the assertion token is service-specific.
- 25 5. The client device of any preceding claim, wherein the authentication initiation message from the IDM component (204) includes a certificate of the IDM component, and the instructions are configured to cause the processor to verify the certificate.
6. The client device of any preceding claim, wherein the instructions are
- 30 configured so that the negotiation (515) includes the establishment of a secure session with the IDM component.
7. The client device of any preceding claim, wherein the authentication request includes an operational parameter of the client device.

8. An identity management, IDM, component (204) in a network (200) having a plurality of IDM components, the IDM component comprising:
a processor (610) and a memory (611), said memory containing instructions
5 executable by said processor to cause the processor to:
subscribe (613), *via* an input/output unit (612), to authentication requests
published in the network;
receive an authentication request (614) published by a client device (201);
initiate a negotiation (615) with the client device; and
10 authenticate (616) the client device or a user of the client device.
9. The IDM component of claim 8, wherein the authentication of the client device includes sending an assertion token to the client device.
- 15 10. the IDM component of claim 8 or 9, wherein the instructions are configured to cause the processor to:
receive a verification request from a service provider (202) in the network, the verification request including an identifier of the client device or user or the assertion token; and
20 verify the authentication of the client device or user or assertion token to the service provider.
11. The IDM component of claim 10, wherein the instructions are configured to cause the processor to subscribe to verification requests published in the network, and
25 wherein the verification request received from the service provider is a verification request published by the service provider.
12. The IDM component of any of claims 8 to 11, wherein the instructions are configured to cause the processor to subscribe to the authentication request and/or
30 verification request at a broker (207) in the network, and receive the published authentication request and/or verification request from said broker.
13. The IDM component of claim 12, wherein the subscription includes details of the capabilities of the IDM component.

14. The IDM component of claim 13, wherein the capabilities include one or more selected from a region of the IDM component, authentication protocols available to the IDM component, availability of IDM component, number of authentications currently
5 being handled by IDM component.

15. The IDM component of any of claims 8 to 14, wherein the authentication negotiation includes sending a certificate to the client device.

10 16. The IDM component of claim 15, wherein the instructions are configured to cause the processor to obtain the certificate from a certification authority in a trusted domain.

15 17. The IDM component of any of claims 8 to 15, wherein the instructions are configured to cause the processor to share authentication states with other IDM components in the network.

18. A service provider (202) in a network (200) having distributed identity management, IDM, components (204, 205, 206), the service provider comprising:

20 a processor (710) and a memory (711), said memory containing instructions executable by said processor to cause the processor to:

receive, *via* an input/output device (712), a service request (713) from a client device (201) in the network, said service request including an authentication of the client and/or an assertion token and an identification of one of the IDM components
25 (204) in the network;

send a verification request (714) to the IDM component;

receive a verification (715) from the IDM component of the client authentication and/or assertion token; and

deliver the requested service (716) to the client device.

30

19. A service provider (202) in a network (200) having distributed identity management, IDM, components (204, 205, 206), the service provider comprising:

a processor (710) and a memory (711), said memory containing instructions executable by said processor to cause the processor to:

receive, *via* an input/output device (712), a service request (713) from a client device (201) in the network, said service request including an authentication of the client and/or an assertion token;

publish a verification request (714) into the network;

5 receive a verification (715), from one of the IDM components (204) in the network, of the client authentication and/or assertion token; and

deliver the requested service (716) to the client device.

20. A broker (207) in a network (200) having distributed identity management, IDM,
10 components (204, 205, 206), the broker comprising:

a processor (810) and a memory (811), said memory containing instructions executable by said processor to cause the processor to:

receive, from at least one of the IDM components (204) *via* an input/output device (812), a subscription to authentication requests (813);

15 receive an authentication request (814) published by a client device (201) in the network;

determine if the subscription matches the published authentication request (815); and

20 forward the authentication request (816) to one of the at least one IDM components.

21. The broker of claim 20, wherein the instructions are configured to cause the processor to determine if capabilities of the IDM component, included in the subscription, are suitable for the authentication request.

25

22. The broker of claim 20 or 21, wherein the instructions are configured to cause the processor to:

receive, from the IDM component or another IDM component in the network, a subscription to verification requests;

30 receive a verification request published by a service provider in the network; determine if the subscription matches the published verification request; and

forward the verification request to one of the subscribed IDM components.

23. A method of authenticating a client device (201) in a network (200) having a plurality of identity management, IDM, components (204, 205, 206), the method comprising, at the client device:

publishing an authentication request (403) using a publish-subscribe message
5 pattern into the network;

receiving an authentication initiation message from one of the IDM components in the network; and

negotiating receipt of authentication information (406) from the IDM component.

10 24. The method of claim 23, further comprising receiving an assertion token (408) from the IDM component as a result of the negotiation.

25. The method of claim 24, further comprising requesting a service (409) from a service provider (202) in the network and sending the assertion token to the service
15 provider to provide authorisation for service delivery.

26. A method of authenticating a client device (201) in a network (200) having a plurality of identity management, IDM, components (204), the method comprising, at one of the IDM components:

20 subscribing (401) to authentication requests in the network;
receiving (405) an authentication request published by a client device;
initiating a negotiation (406) with the client device; and
authenticating (408) the client device.

25 27. The method of claim 26, further comprising sending an assertion token (408) to the client device following the negotiation.

28. The method of claim 26 or 27, further comprising receiving a verification request (412) from a service provider (202) in the network, the verification request including an
30 identifier of the client device or the assertion token, and verifying the authentication of the client device or assertion token to the service provider (413).

29. The method of claim 28, further comprising subscribing to verification requests published in the network, wherein the verification request received from the service provider is a verification request published (410) by the service provider.

5 30. The method of any of claims 26 to 29, further comprising subscribing to the authentication request (401) at a broker (207) in the network, and receiving the published authentication request (405) from said broker.

10 31. The method of any of claims 26 to 30, further comprising sharing authentication states among IDM components in the network.

32. A method of providing a service in a network (200) having a plurality of identity management, IDM, components (204), comprising, at a service provider (202):
receiving a service request (409) from a client device (201) in the network, said
15 service request including an authentication of the client and/or an assertion token and an identification of one of the IDM components (204) in the network;
sending a verification request to the IDM component;
receiving a verification (413) from the IDM component of the client authentication and/or assertion token; and
20 delivering the requested service (414) to the client device.

33. A method of providing a service in a network having a plurality of identity management, IDM, components (204), comprising, at a service provider:
receiving a service request (409) from a client device (201) in the network, said
25 service request including an authentication of the client and/or an assertion token;
publishing a verification request (410) into the network;
receiving a verification (413) from one of the IDM components (204) of the client authentication and/or assertion token; and
delivering the requested service (414) to the client device.

30

34. A method of brokering an authentication request in a network (200) with distributed identity management, IDM, components (204, 205, 206), the method comprising, at a broker (207):

receiving, from an IDM component (204) in the network, a subscription to authentication requests (401);

receiving an authentication request (403) published by a client device (201) in the network;

5 determining if the subscription matches the published authentication request (404); and

forwarding the authentication request (405) to the IDM component.

35. The method of claim 34, further comprising matching received authentication requests to capabilities of IDM components subscribed (404).

36. The method of claim 35, wherein the capabilities of the IDM component include one or more of: a region of the IDM component, authentication protocols available to the IDM component, availability of the IDM component, and number of authentications currently being handled by the IDM component.

37. A method of authenticating a client device (201) in a network (200) having a plurality of identity management , IDM, components (204, 205, 206), the method, comprising:

20 one or more of the IDM components (204), subscribing (401) to authentication requests published by client devices;

publishing an authentication request (403) into the network from the client device;

at a broker, selecting (404) the most appropriate IDM component to process the published authentication request;

forwarding (405) the authentication request from the broker to the selected IDM component; and

at the selected IDM component, negotiating with (406) and authenticating the client device.

30

38. The method of claim 37, wherein the one or more IDM components subscribe to authentication requests at said broker.

39. The method of claim 38, wherein the broker matches received authentication requests to capabilities of IDM components subscribed (404).

40. The method of claim 38 or 39, wherein the network includes a plurality of
5 brokers, the method further comprising:

at an orchestration entity, monitoring traffic through all of the brokers and/or IDM components;

identifying when traffic to one or more IDM components exceeds a predetermined threshold; and

10 provisioning additional IDM components.

41. The method of any of claims 37 to 40, wherein the authentication of the client device includes sending an assertion token (408) from the IDM component to the client device.

15

42. The method of claim 41, further comprising the client device requesting a service (409) from a service provider (202) in the network and sending the assertion token to the service provider to provide authorisation for service delivery.

20 43. The method of claim 42, further comprising:

the service provider publishing a verification request (410) into the network;

one or more IDM components subscribing to verification requests;

at a broker, selecting the most appropriate IDM component to process the verification request (411);

25 forwarding the verification request (412) from the broker to the selected IDM component; and

at the selected IDM component, negotiating with and verifying (413) the assertion token to the service provider.

30 44. A computer program comprising computer readable code which, when run on a device, causes it to behave as a device according to any of claims 1 to 22.

45. A computer program comprising computer readable code which, when run on a device, causes the device to execute the method according to any of claims 23 to 36.

46. A memory comprising a computer program according to claim 44 or 45 and a computer readable means on which the computer program is stored.

5 47. The memory according to claim 46, wherein the memory is arranged in the form of a computer program product.

48. A vessel or vehicle (901) comprising the client device (201) of any of claims 1 to 7.

1/8

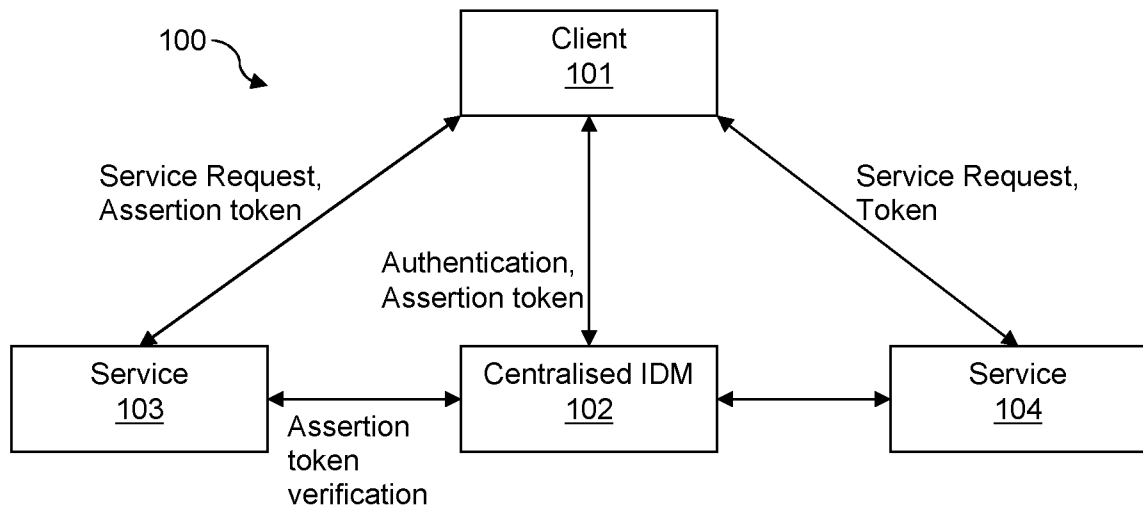


Figure 1

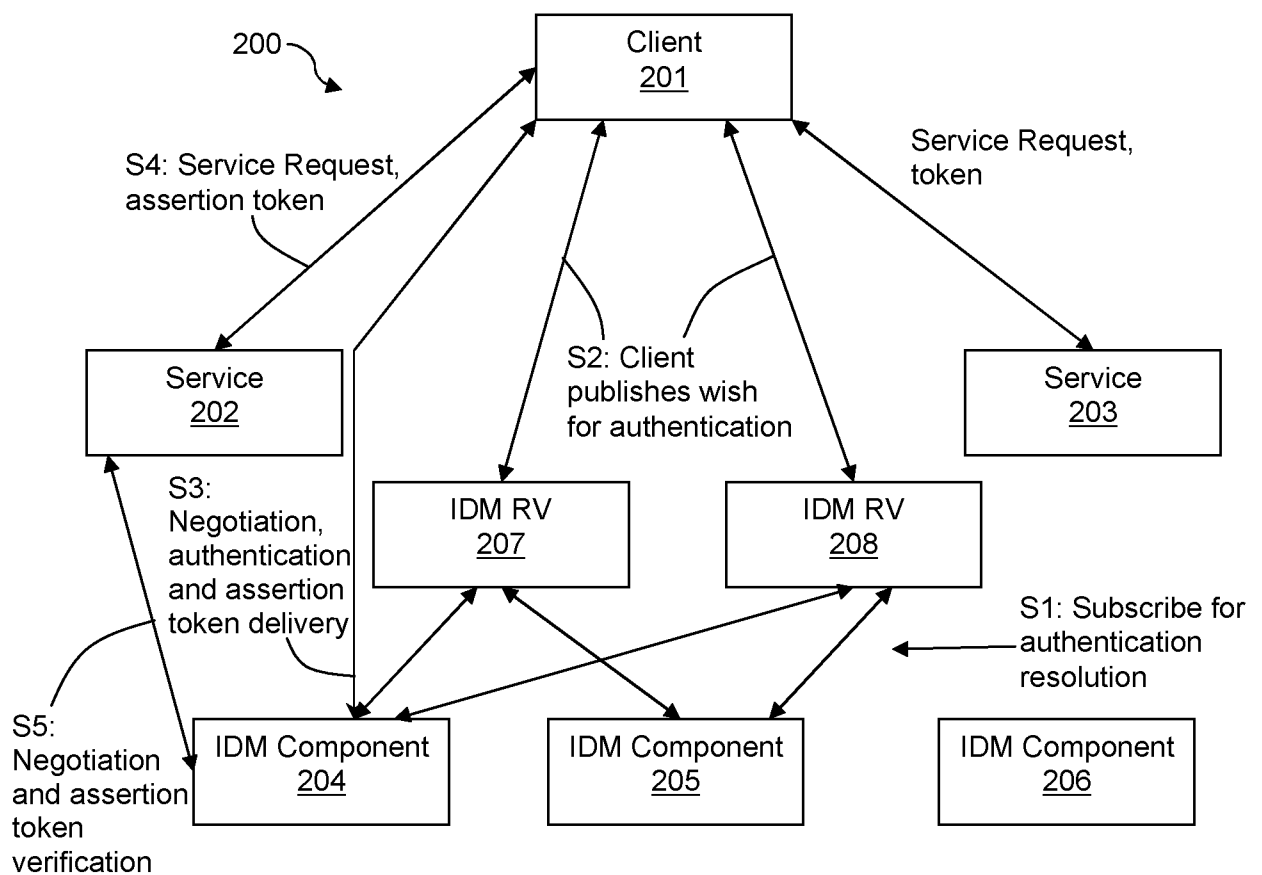


Figure 2

2/8

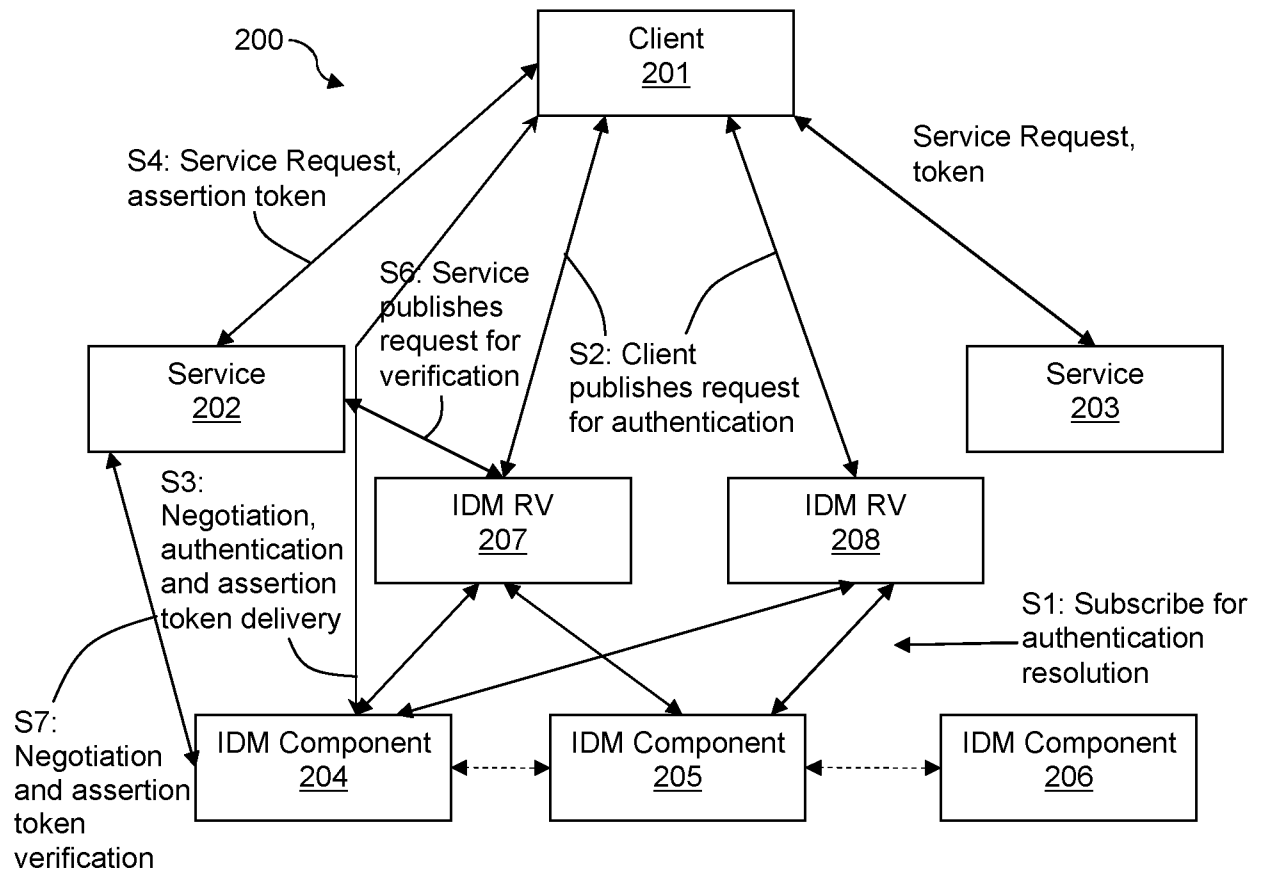


Figure 3

3/8

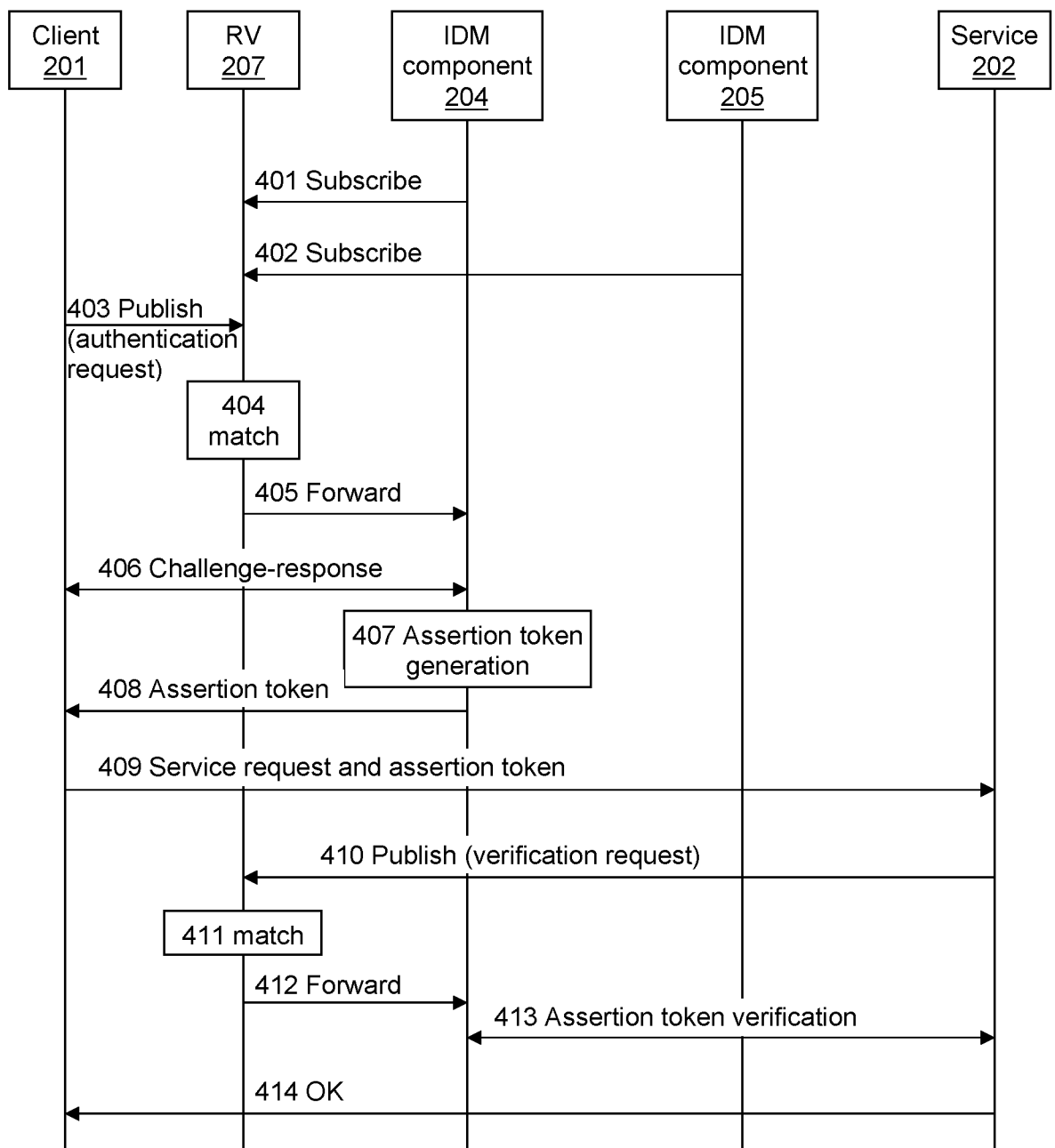


Figure 4

4/8

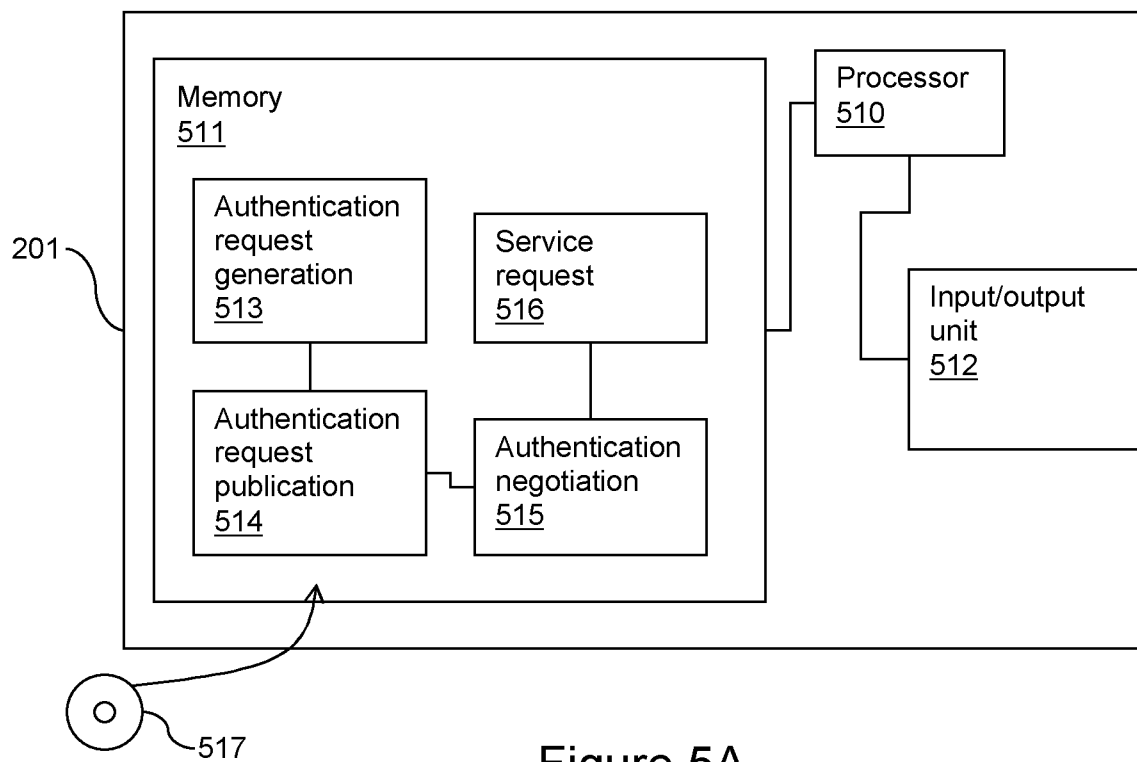


Figure 5A

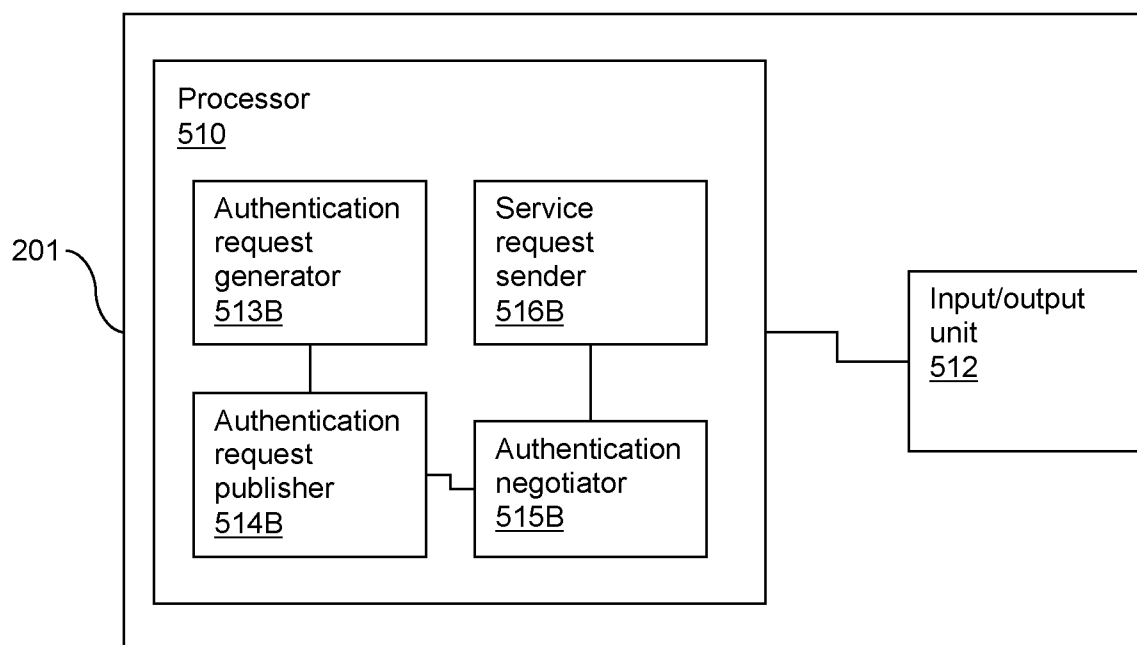


Figure 5B

5/8

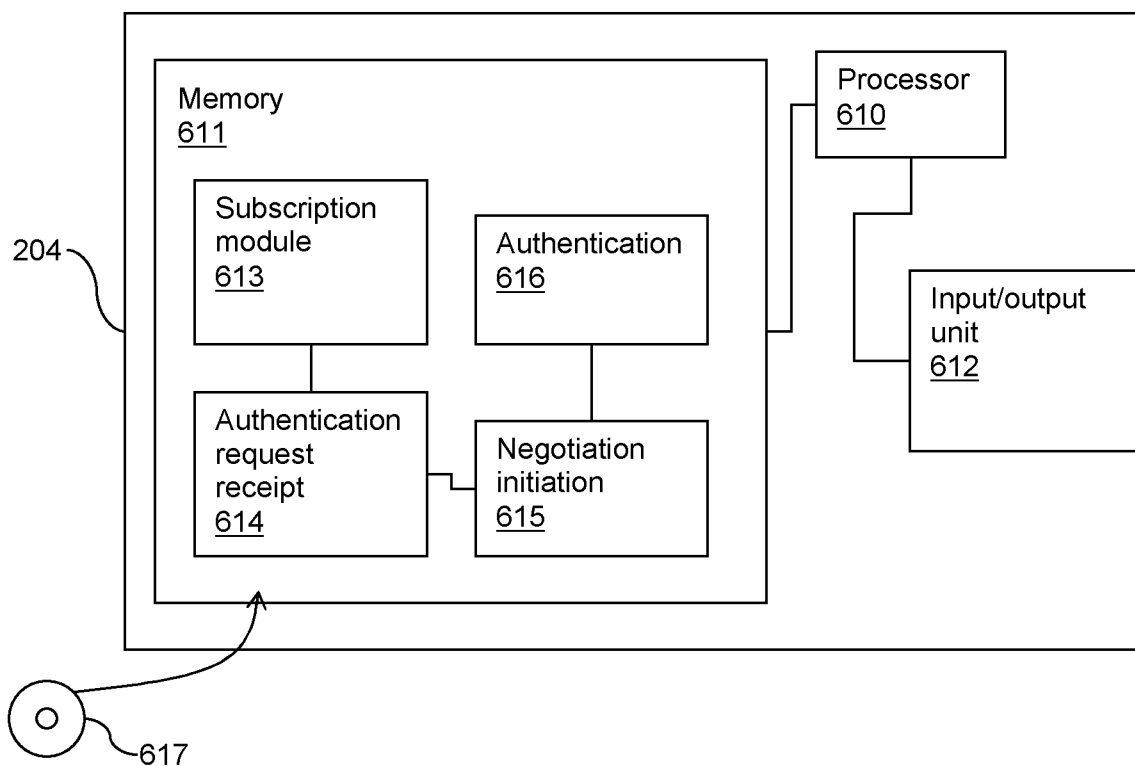


Figure 6A

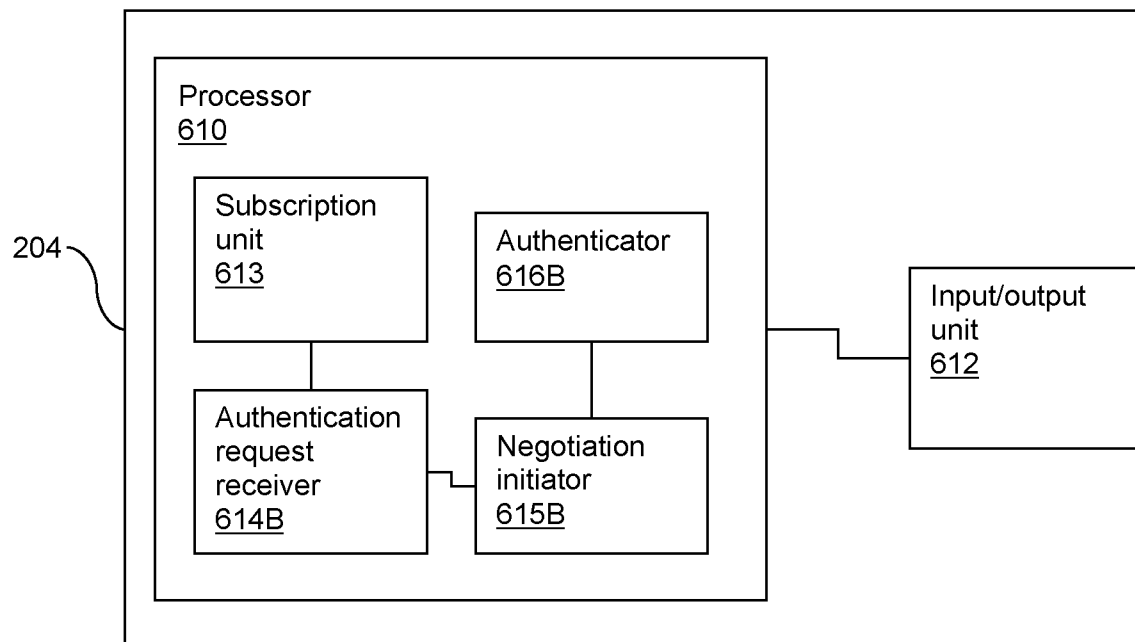


Figure 6B

6/8

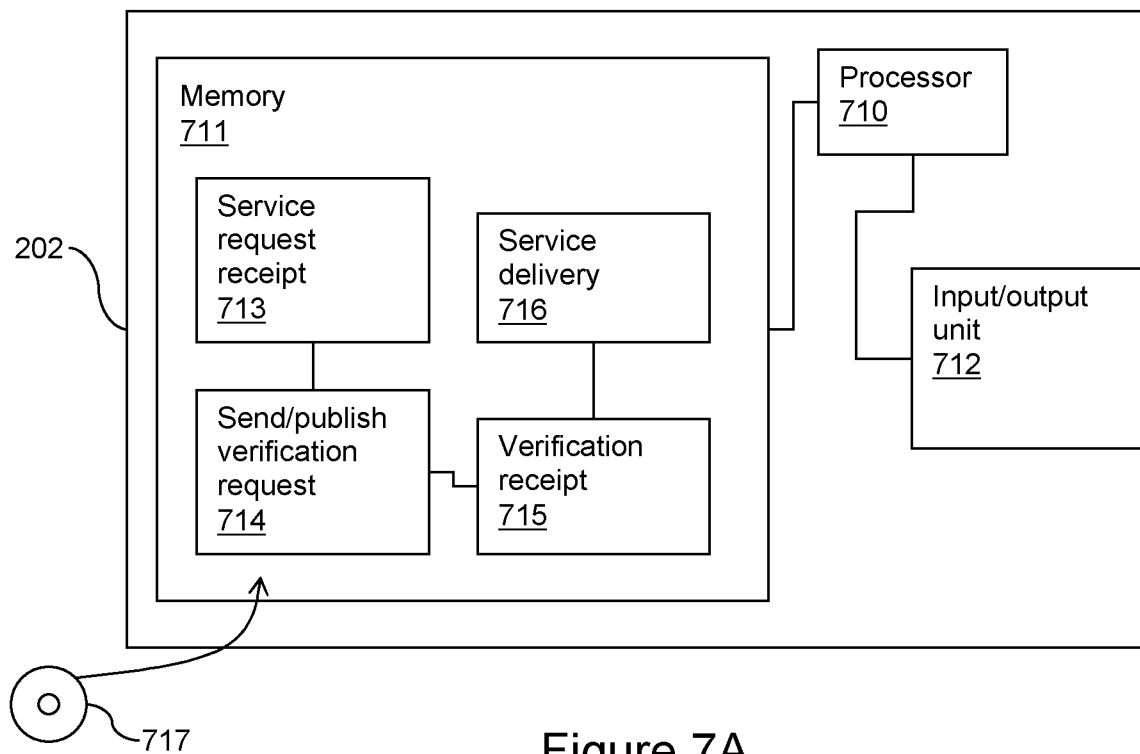


Figure 7A

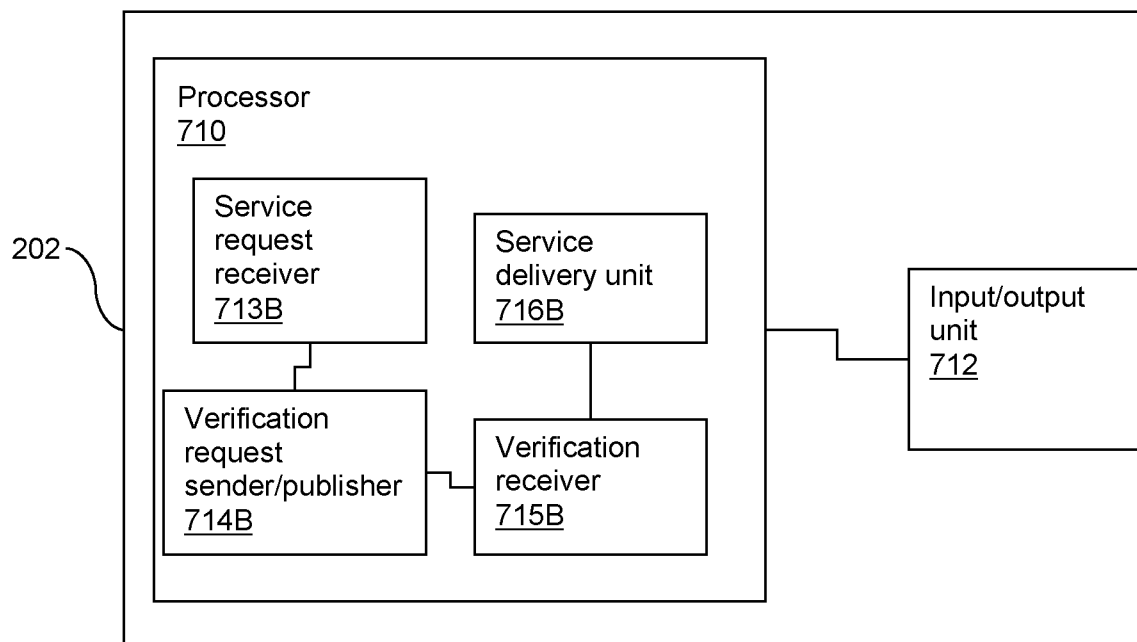


Figure 7B

7/8

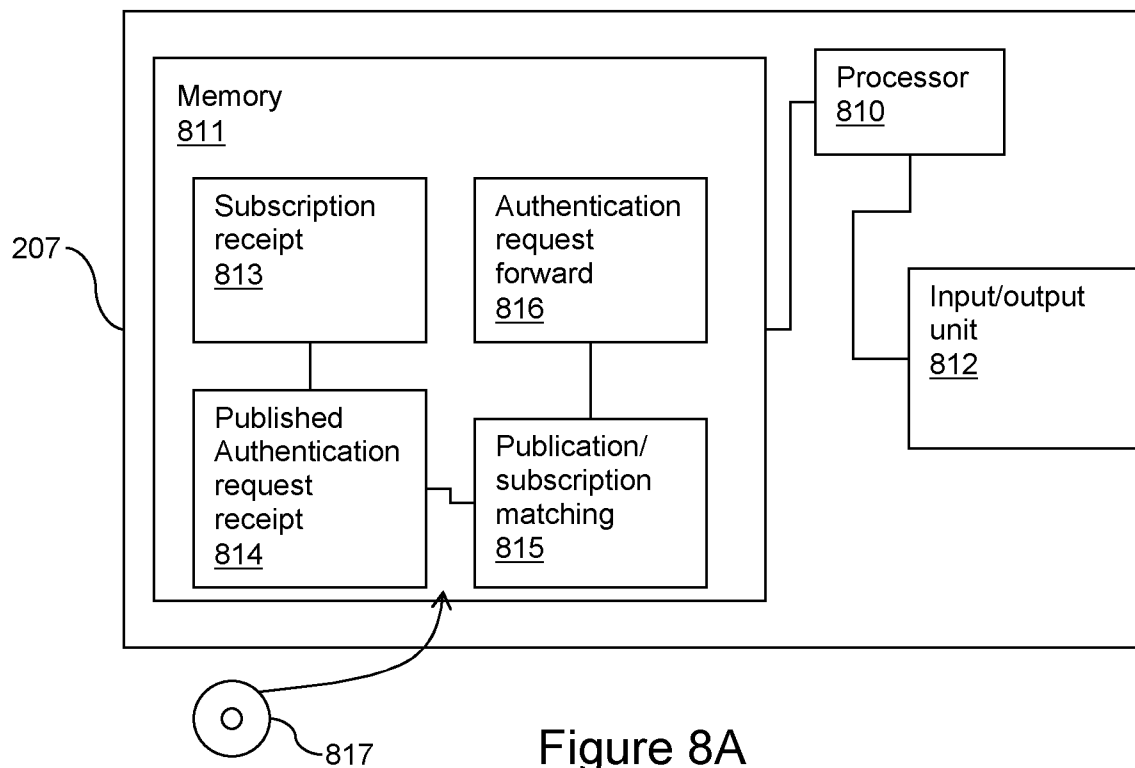


Figure 8A

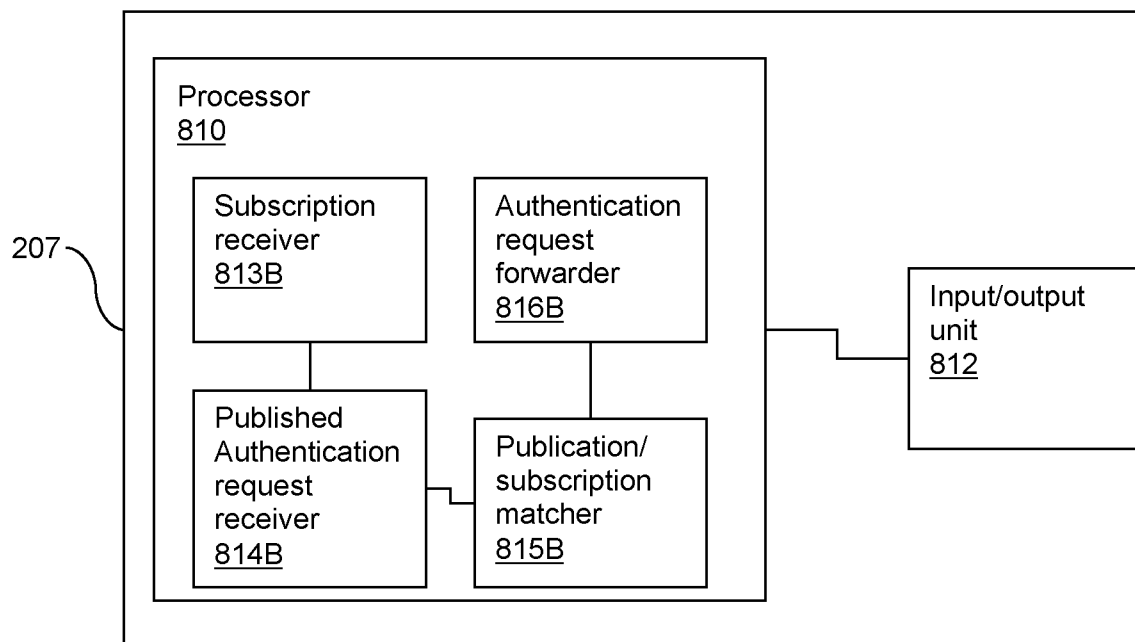


Figure 8B

8/8

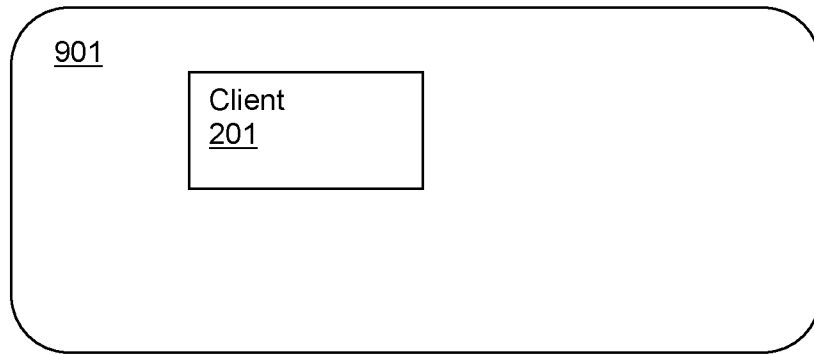


Figure 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2013/050813

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F, H04L

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

SE, DK, FI, NO classes as above

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

EPO-Internal, PAJ, WPI data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 20120023556 A1 (SCHULTZ PAUL T ET AL), 26 January 2012 (2012-01-26); abstract; paragraph [0013]; figure 5	18, 32
A	--	1-17, 19-31, 33-48
Y	Jun Chen et al: "A decentralised approach for implementing identity management in cloud computing", IEEE, 2012 Second International Conference on Cloud and Green Computing, 2012-11-01.; abstract; Section III	18, 32
A	--	1-17, 19-31, 33-48

☒ 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

01-04-2014

Date of mailing of the international search report

01-04-2014

Name and mailing address of the ISA/SE

Patent- och registreringsverket
Box 5055
S-102 42 STOCKHOLM
Facsimile No. + 46 8 666 02 85

Authorized officer

Ralf Boström

Telephone No. + 46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2013/050813

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2012174210 A2 (ZTE CORP ET AL), 20 December 2012 (2012-12-20); abstract; paragraph [0011] --	1-48
A	US 20110184860 A1 (BISHOP FRED), 28 July 2011 (2011-07-28); abstract --	1-48
A	US 20090300152 A1 (FERRIS JAMES MICHAEL), 3 December 2009 (2009-12-03); abstract -- -----	1-48

Continuation of: second sheet**International Patent Classification (IPC)*****G06F 15/16*** (2006.01)***H04L 9/32*** (2006.01)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SE2013/050813

US	20120023556 A1	26/01/2012	US	8474017 B2	25/06/2013
WO	2012174210 A2	20/12/2012	NONE		
US	20110184860 A1	28/07/2011	US	20110202565 A1	18/08/2011
			US	20110184988 A1	28/07/2011
			US	20110184987 A1	28/07/2011
			US	20110184986 A1	28/07/2011
			US	20110184985 A1	28/07/2011
			US	20110184861 A1	28/07/2011
US	20090300152 A1	03/12/2009	US	7886038 B2	08/02/2011