

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
11 June 2009 (11.06.2009)

PCT

(10) International Publication Number
WO 2009/073207 A1

(51) International Patent Classification:
G06F 7/04 (2006.01)

(21) International Application Number:
PCT/US2008/013398

(22) International Filing Date:
5 December 2008 (05.12.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/951,425 6 December 2007 (06.12.2007) US

(71) Applicant (for all designated States except US): **FIRST DATA CORPORATION** [US/US]; 6200 S. Quebec St., Suite 270, Greenwood Village, CO 80111 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **GEPPERT, Mike** [US/US]; 2240 N. 161st St., Omaha, NE 68116 (US).

(74) Agents: **GIBBY, Darin, J.** et al.; Townsend and Townsend and Crew LLP, 1200 17th Street, Suite 2700, Denver, CO 80202 (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, BR, BW, BY, BZ, CA, CH, 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, KM, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

(54) Title: MULTI-MODULE AUTHENTICATION PLATFORM

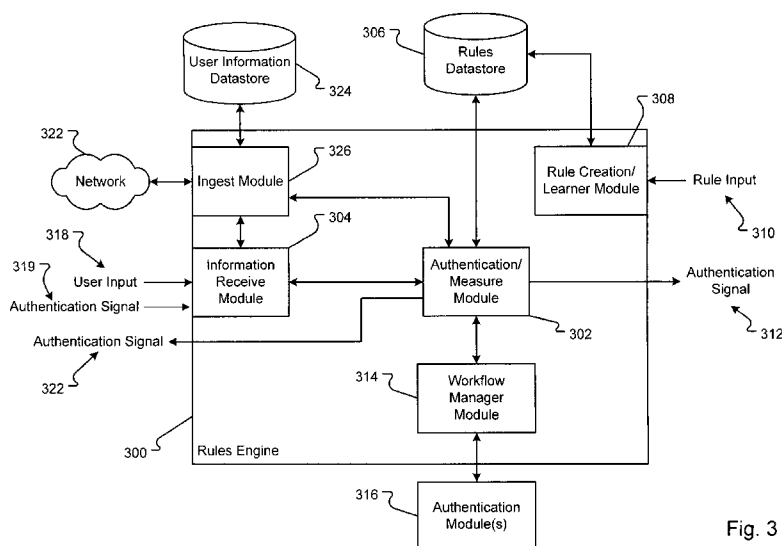


Fig. 3

(57) **Abstract:** Embodiments of the disclosure generally relate to systems and methods for authenticating users of an entity system. In embodiments, an authentication platform receives a request for authentication. The authentication platform interacts with one of several authentication modules to authenticate the user. Each authentication module may use different information or procedures to authenticate the user. If authenticated, the user is allowed access to the system. Having access to two or more authentication modules allows the authentication platform to provide automatically a more robust authentication and alleviates the entity system from needing to integrate the several authentication modules.

WO 2009/073207 A1

MULTI-MODULE AUTHENTICATION PLATFORM

BACKGROUND

[0001] This disclosure relates, in general, to authentication of users and, more specifically,
5 but not by way of limitation, to authentication of customers attempting to create or access an account at a financial institution.

[0002] Identity theft and fraud have caused great losses for financial institutions and consumers alike. To combat the illegal or unauthorized use of a consumer's account, financial institutions generally require the consumer to authenticate themselves. For
10 example, the consumer uses a password to enter his or her account.

[0003] Unfortunately, the people committing the fraud or stealing identities are continually becoming more sophisticated. The methods used to enter illegitimately another person's account generally requires an ever-increasing need for preventative measures. In some cases, financial institutions are trying to use two or more preventative measures to authenticate
15 users. However, using several preventative measures becomes increasingly hard to integrate into the financial institution's system and hard to maintain the preventative measures.

[0004] It is in view of these and other considerations not mentioned herein that the embodiments of the present disclosure were envisioned.

BRIEF DESCRIPTION OF THE DRAWINGS

20 [0005] The present disclosure is described in conjunction with the appended figures:

[0006] Fig. 1 is a block diagram of an embodiment of a system operable to authenticate a user desiring access to an entity system;

[0007] Fig. 2 is a hardware and/or software block diagram of an embodiment of a authentication platform for use in a system for authenticating users;

25 [0008] Fig. 3 is a block diagram of an embodiment of a rules engine for use in an authentication platform for authenticating users;

[0009] Figs. 4A-B are block diagrams of embodiments of one or more data structures for storing authentication rules in an authentication platform;

[0010] Fig. 5 is a flow diagram of an embodiment of a process for creating an authentication rule executed at an authentication platform;

[0011] Fig. 6 is a flow diagram of an embodiment of a process for creating an authentication rule executed at an entity system;

5 [0012] Figs. 7A-B are flow diagrams of an embodiment of a process for authenticating a user executed at an authentication platform;

[0013] Fig. 8 is a flow diagram of an embodiment of a process for authenticating a user executed at a user computer;

10 [0014] Fig. 9 is a block diagram of an embodiment of a computer system for use in the system for authenticating a user.

[0015] In the appended figures, similar components and/or features may have the same reference label. Further, various components of the same type may be distinguished by following the reference label by a dash and a second label that distinguishes among the similar components. If only the first reference label is used in the specification, the
15 description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label.

DETAILED DESCRIPTION

[0016] The ensuing description provides exemplary embodiment(s) only and is not intended to limit the scope, applicability or configuration of the possible embodiments.
20 Rather, the ensuing description of the exemplary embodiment(s) will provide those skilled in the art with an enabling description for implementing an exemplary embodiment. It being understood that various changes may be made in the function and arrangement of elements without departing from the spirit and scope of the possible embodiments as set forth in the appended claims.

25 [0017] Embodiments of the disclosure generally relate to systems and methods for authenticating users of a system. In embodiments, an authentication platform receives a request for authentication. The authentication platform interacts with at least one of several authentication modules to authenticate the user. Each authentication module may use different information or procedures to authenticate the user. If authenticated, the user is
30 allowed access to the system. Having access to two or more authentication modules allows the authentication platform to provide automatically a more robust authentication and

alleviates the entity from needing to integrate the several authentication modules into the entity's system.

[0018] Before describing several embodiments, an example of how the systems and methods may work may be useful. A new customer of a bank contacts the bank's website with the customer's computer. The customer requests to open a new account. The bank transfers the customer to an authentication service to verify the identity of the customer.

[0019] The authentication service has communicated with the bank to establish rules for how new or existing customers will have their identities verified. The new customer sent to the authentication service tests the new customer as to their identity. For example, the new customer enters identifying information such as his or her social security number, address, phone number, name, etc. These items of information may be checked for correlation. According to the rules the bank created, the authentication service may also ask an "out-of-pocket" question that can be verified with public records, such as, "what car did you drive in 1999?" After the identity of the new customer is verified to the liking of the bank, the authentication service may ask the new customer other questions to establish a security profile. For example, the new customer establishes a user name and password. How the password is entered, that is how the new customer hits each key on the keyboard, may be recorded. After the new customer has completed the information, he or she may be redirected back to the bank to open the account as a verified user.

[0020] When the customer returns to logon to the account that he or she created, the bank may again redirect the returning customer to the authentication service. The authentication service can test the authenticity of the returning customer according to a different set of rules established by the bank. For example, the returning customer may enter his or her user name and password. How the password is entered may be checked against stored information at the authentication service. The returning customer may be sent a one-time password to an email address the returning customer previously provided. The returning customer can enter the one-time password. After the returning customer has completed enough tests according to the rules established by the bank, the authentication service can redirect the customer back to the bank to access their existing account.

[0021] The example above will help understand the embodiments of systems and methods that follow. The above example also highlights the advantages of the embodiments described herein. Notably, the authentication service may employ several different types of tests to

verify the customer. Further, the bank may establish rules with the authentication service to customize authentication procedures. Still further, how the customers are authenticated may change making it more difficult for a fraudster to impersonate the customer.

[0022] While various aspects of embodiments of the disclosure have been summarized

5 above, the following detailed description illustrates exemplary embodiments in further detail to enable one of skill in the art to practice the disclosure. In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present disclosure. It will be apparent, however, to one skilled in the art that the present disclosure may be practiced without some of these specific details. In other
10 instances, well-known structures and devices are shown in block diagram form. Several embodiments of the disclosure are described below, and while various features are ascribed to different embodiments, it should be appreciated that the features described with respect to one embodiment may be incorporated with another embodiment as well. By the same token, however, no single feature or features of any described embodiment should be considered
15 essential to the disclosure, as other embodiments of the disclosure may omit such features.

[0023] Specific details are given in the following description to provide a thorough understanding of the embodiments. However, it will be understood by one of ordinary skill in the art that the embodiments may be practiced without these specific details. For example, circuits may be shown in block diagrams in order not to obscure the embodiments in
20 unnecessary detail. In other instances, well-known circuits, processes, algorithms, structures, and techniques may be shown without unnecessary detail in order to avoid obscuring the embodiments. A computing system may be used to execute any of the tasks or operations described herein. In embodiments, a computing system includes memory and a processor and is operable to execute computer-executable instructions stored on a computer readable
25 medium that define processes or operations described herein.

[0024] Also, it is noted that the embodiments may be described as a process which is depicted as a flowchart, a flow diagram, a data flow diagram, a structure diagram, or a block diagram. Although a flowchart may describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of the
30 operations may be re-arranged. A process is terminated when its operations are completed, but could have additional steps not included in the figure. A process may correspond to a method, a function, a procedure, a subroutine, a subprogram, etc. When a process

corresponds to a function, its termination corresponds to a return of the function to the calling function or the main function.

[0025] Furthermore, embodiments may be implemented by hardware, software, firmware, middleware, microcode, hardware description languages, or any combination thereof. When implemented in software, firmware, middleware or microcode, the program code or code segments to perform the necessary tasks may be stored in a machine-readable medium such as a storage medium. A processor(s) may perform the necessary tasks. A code segment may represent a procedure, a function, a subprogram, a program, a routine, a subroutine, a module, an object, a software package, a class, or any combination of instructions, data structures, or program statements. A code segment may be coupled to another code segment or a hardware circuit by passing and/or receiving information, data, arguments, parameters, or memory contents. Information, arguments, parameters, data, etc., may be passed, forwarded, or transmitted via any suitable means including memory sharing, message passing, token passing, network transmission, etc.

[0026] An embodiment of a system 100 for authenticating a user or consumer 106 for access to an entity's systems 102 is shown in Fig. 1. A user 106 is the person desiring access to the entity's system 102 and any associated system, computer, or other hardware and/or software being used by the user 106 to access the entity's system 102. The entity system 102 is the entity, for example, a financial institution, a bank, a healthcare provider, etc., and any associated system, computer, or other hardware and/or software being used by the entity 102 to transact business, store data, sell services or products, etc. In embodiments, the system 100 comprises a consumer 106 in communication with an authentication platform 104 via a network 108, the authentication platform 104 also in communication with the entity system 102. The components of the system 100 may be located together at one location or may be distributed over a LAN, WAN, the Internet, or other network in physically different locations.

[0027] In embodiments, the consumer 106 desires access to the entity system 102 and sends a request for access to the entity system 102. The entity system 102, in embodiments, generates an authentication request and sends the authentication request to the authentication platform 104. The authentication platform may then evaluate the authentication request and respond back to the entity system 102 as to whether the consumer 106 is authenticated. The various components of the system 100 are described hereinafter.

[0028] A first communications channel 122 allows communication between the authentication platform 104 and the entity system 102, which may be in a distant location or located locally with or substantially near the authentication platform 104. The first communications channel 122 may be any type of communications system including wireless, wired, or other communication system. In one embodiment, the first communications channel 122 is a local area network (LAN), wide area network (WAN), or Internet connection. If a wireless communication channel, the first communication channel can be Bluetooth[®], 802.11g, cellular, or other wireless system.

[0029] In embodiments, the system 100 includes a network 108. The network 108 provides a second communications channel. The second communications channel 126 allows the authentication platform 104 to communicate with a user 106, who may be located in a distant location. For example, the authentication platform 104 communicates with the user 106, who is located in another state or country. The network 108 may be a cellular network, a wireless LAN or WAN, the Internet, or other communication system.

[0030] The authentication platform 104, in embodiments, is a system, module, and/or device comprised of hardware and/or software that authenticates the user 106 before the user 106 can access the entity system 102 or create a new relationship, e.g., new account, new membership, etc., with the entity system 102. In embodiments, the authentication platform 104 is a hosted system through which the initial communications between the user 106 and the entity system 102 are routed. The authentication platform 104 is operable to receive communications from and send communications to the entity system 102. Further, the authentication platform 104 is operable to communicate with the network 108 to receive communications from and send communications to the user 106.

[0031] The authentication platform 104, in embodiments, comprises a decision engine 110 and two or more authentication modules 112, 114, 116, 118, and 120. In embodiments, the authentication platform 104 comprises fewer authentication modules than those shown in Fig. 1. In other embodiments, the authentication platform 104 comprises more authentication modules than those shown in Fig. 1, as represented by ellipses 124. In embodiments, an authentication module 112, 114, 116, 118, or 120 performs a type of authentication. For example, authentication module #1 112 authenticates a user 106 using keyboard dynamics, authentication module #2 114 authenticates a user 106 using a one-time password, authentication module #3 116 authenticates a user 106 using a computer fingerprint,

authentication module #4 118 authenticates a user 106 using one or more out-of-wallet questions, authentication module #5 120 authenticates a user 106 using a voice print, etc. The computer fingerprint, one-time password, voice print, and/or keyboard dynamics may be compared against associated data stored at the authentication platform 104. Keyboard
5 dynamics relates to the unique way (the speed at which the key is typed, the length a user 106 holds down a key, the duration between keystrokes, etc.) the user 106 types in a word or phrase, such as a password. A one-time password is a password that is sent to a user's known email account, cell phone, other device, or account that allows the user 106 to retrieve and use the password. A computer fingerprint is an item of information stored on the user's
10 computer or generated from the unique characteristics of the user's computer, such as the type of computer, the date, the processor used, the amount of computer memory, the time, etc. An out-of-wallet question is a question directed to the user 106 that only the user 106 is likely to know, such as "What car did you drive in 1998?". A voice print is the unique characteristics of a person's voice based on frequency, amplitude, etc. when the user 106 says a
15 predetermined phrase or word. One skilled in the art will recognize that other types of authentication processes or methods are possible and contemplated as being used in the system 100.

[0032] The decision engine 110, in embodiments, is hardware, software, or hardware and software that controls the authentication of the user 106. In embodiments, the decision
20 engine 110 receives requests for authentication and one or more items of information from the user 106. Further, the decision engine 110 can store authentication rules created by the entity that controls the flow of authentication for the users 106 of the entity system 102. In embodiments, the one or more rules determine which authentication modules 112, 114, 116, 118, or 120 to use for authentication, the intensity of the authentication, the response to
25 authentication failures, etc. The decision engine 110 may respond to the request for authentication, then read and respond to the rules to authenticate the user 106.

[0033] In operation, an entity may use the entity system 102 to create one or more authentication rules used by the decision engine 110 to authenticate one or more users 106. The decision engine 110 stores the rules. A user 106, in embodiments, requests access to or
30 desires to establish a new relationship with the entity. The entity system 102 creates an authentication request and sends the authentication request to the authentication platform 104 to authenticate the user before he or she accesses the entity system 102. The decision engine 110 receives the request, which may include an identifier for the entity system 102 that the

decision engine 110 can use to retrieve the one or more authentication rules associated with the entity system 102. The decision engine 110, in embodiments, retrieves the first rule to which to respond. The decision engine 110 can retrieve authentication information from the authentication request or can request authentication information from the user 106. In
5 embodiments, the decision engine 110 provides the authentication information to at least one of the authentication modules 112, 114, 116, 118, or 120. The authentication module 112, 114, 116, 118, or 120 may determine if the user 106 is authenticated or may conduct a measurement or test of the authentication information and can return a response to the decision engine 110.

10 **[0034]** The decision engine 110, in embodiments, determines if the user 106 is authenticated from the return from the authentication module 112, 114, 116, 118, or 120. In other embodiments, the decision engine 110 responds to the return of authentication success or failure from the authentication module 112, 114, 116, 118, or 120. In embodiments, the decision engine 110 responds to or determines authentication success and sends a response to
15 the entity system 102 to allow the user 106 to access the entity system 102. In alternative embodiments, the decision engine 110 determines or receives indication of authentication failure. The decision engine 110 may then retrieve another rule in response to the failure and can send information to another authentication module 112, 114, 116, 118, or 120. In other embodiments, the decision engine 110 sends a response to the entity system to prevent access
20 of the user 106 to the entity system 102.

[0035] In an alternative embodiment, the decision engine 110 sends information to two or more authentication modules 112, 114, 116, 118, or 120 at substantially the same time and evaluates together the returns from the two or more authentication modules 112, 114, 116, 118, or 120 to determine if the user is authenticated. In other words, if the entity desires that
25 two or more authentication modules 112, 114, 116, 118, or 120 be used, the decision engine 110 need not interact with the two or more authentication modules 112, 114, 116, 118, or 120 serially but may have the two or more authentication modules 112, 114, 116, 118, or 120 process the authentication tests in parallel.

[0036] In embodiments, the entity is a financial institution and the entity system 102 is a
30 financial institution system. Hereinafter, embodiments may be described using the example of the financial institution, but this exemplary description is not meant to limit the embodiments to the financial institution. Other embodiments may include other systems that

use the authentication platform 104 to authenticate users, for example, healthcare institutions, schools, etc.

[0037] An embodiment of the decision engine 200 is shown in Fig. 2. In embodiments, the authentication decision engine 200 is the same or similar to the decision engine 110 (Fig. 1).

5 The decision engine 200, in embodiments, comprises a user interface 208, an institution interface 204, a rules engine 202, a rules datastore 206, and/or an authentication module interface 210. The user interface 208 interacts with a user 106 (Fig. 1) to receive user input 214 or send communication to the user 106 (Fig. 1). User input 214 may be a request for authentication or one or more items of authentication information provided to the rules
10 engine 202 or one or more authentication modules 212 to authenticate the user 106 (Fig. 1). The user interface 208, in embodiments, is hardware, software, or hardware and software for communicating with the user 106 (Fig. 1) and the user's system. The user interface 208 may be a communication systems for communicating over a LAN, WAN, the Internet, a wireless LAN, etc. The user interface 208 may also provide output to display on a system of the user
15 106 (Fig. 1). For example, the user interface 208 generates a web page that is shown on a display device of the user 106 (Fig. 1).

[0038] The institution interface 204 is similar to the user interface 208 in that the institution interface 204 receives inputs from an entity system 102 (Fig. 1) and outputs one of more displays or other information to the entity system 102 (Fig. 1). One of the inputs from the
20 entity system 102 (Fig. 1) may be one or more authentication rules 216. The institution interface 204, in embodiments, is hardware, software, or hardware and software for communicating with the entity system 102 (Fig. 1). The institution interface 204 may be a communication systems for communicating over a LAN, WAN, the Internet, a wireless LAN, etc.

25 [0039] The authentication module interface 210 is also similar to the user interface 208 and the institution interface 204 in that the authentication module interface 210 communicates with the authentication modules 212. The authentication modules 212 may be the same or similar to the authentication modules 112 (Fig. 1), 114 (Fig. 1), 116 (Fig. 1), 118 (Fig. 1), or 120 (Fig. 1). The authentication module interface 210 can send authentication information to
30 the authentication modules 212 and receive replies or returns from the authentication modules 212. The authentication module interface 210, in embodiments, is hardware, software, or hardware and software for communicating with the authentication modules 212. The

authentication module interface 210 may be communication systems for communicating over a LAN, WAN, the Internet, a wireless LAN, etc. In alternative embodiments, the authentication module interface 210 is a translator or an API that changes the common requests, commands, and/or replies of the rules engine 202 into program specific requests, commands, and/or replies of the one or more authentication modules 212. In embodiments, each authentication module 212 may have a different protocol, format, or method of communication to which the authentication module interface 210 adjusts. As such, the authentication platform 104 (Fig. 1) may integrate authentication modules 212 from different vendors and still provide a common interface to the user 106 (Fig. 1) and the entity system 102 (Fig. 1).

[0040] In embodiments, the rules datastore 206 stores information about one or more rules 216 received from the financial institution. The rules datastore 206 may be hardware, software, or hardware and software for storing data. In embodiments, the rules datastore 206 is memory or a storage device operable to store data. For example, the rules datastore 206 is random access memory (RAM), read only memory (ROM), an optical storage device, magnetic media, etc., either integrated with the authentication decision engine 200 or configured as a separate device. Further, the rules datastore 206 may be software to control the storage of data, for example, a file system or other software. The authentication rules 216 may be stored in the rules datastore 206 in a relational database or other manner. Further description of the rules datastore 206 is provided in conjunction with Figs. 4A-B.

[0041] The rules engine 202, in embodiments, is hardware, software, or hardware and software for executing authentication rules, stored in the rules datastore 206, in response to authentication requests 214. The rules engine 202 may be a software program executed in a processor or may be separate hardware and/or software for completing the functions described herein. In embodiments, the rules engine 202 receives authentication rules 216 or assists the financial institution in generating the authentication rules 216. The rules engine 202 can store the created rules in the rules datastore 206. The rules engine 202 executes one or more authentication rules 216 in response to user input 214, such as an authentication request 214. The authentication rule 216 executed by the rules engine 202, in embodiments, requires the rules engine 202 to send authentication information, through the authentication module interface 210, to one of the authentication modules 212. The authentication module 212 may determine from the user input 214 if the user is authenticated or conduct a

measurement or test of the authentication information and can return a response to an authentication module interface 210 for the rules engine 202.

[0042] The rules engine 202, in embodiments, determines if the user is authenticated from the return from the authentication module 212. In other embodiments, the rules engine 202 responds to the return of authentication success and allows the user 106 (Fig. 1) to access the entity system 102 (Fig. 1). In alternative embodiments, the rules engine 202 determines or receives indication of authentication failure and, in response, may then retrieve another rule from the rules datastore 206 and can send information to another authentication module 212. In other embodiments, the rules engine 202 prevents access of the user to the institution.

[0043] An embodiment of a rules engine 300 is shown in Fig. 3. The rules engine 300 may be hardware, software, or hardware and software operable to complete the functions described herein. In an embodiment, the rules engine 300 comprises one or more software modules that have one or more computer-executable instructions for completing the operations described herein. The rules engine 300, in embodiments, comprises an information receive module 304, an authentication/measure module 302, a workflow manager module 314, an ingest module 326, and/or a rule creation/learner module 308.

[0044] In embodiments, the information receive module 304 receives user input 318. The information receive module 304 can receive authentication information in one or more transmissions of user input 318. The information receive module 304 may extract authentication information, for example, passwords, voice prints, computer signatures, etc., from the user input 318 and provide the information to the authentication/measure module 302. In alternative embodiments, the information receive module 304 receives requests 319 for authentication that initiates an authentication. The information receive module 304 can pass the authentication request 319 to the authentication/measure module 302 to begin the authentication.

[0045] In embodiments, the information receive module 304 also provides the one or more items of authentication information to an ingest module 326. The ingest module 326, in embodiments, can store the one or more items of authentication information into a user information datastore 324 for later retrieval. For example, the ingest module 326 stores the computer fingerprint for a user and can provide the stored computer fingerprint to the authentication/measure module 302 for later comparison.

[0046] In alternative embodiments, the ingest module 326 retrieves public or other information from outside sources through a network 322. For example, the ingest module 326 retrieves information from a department of motor vehicle, health insurance provider, the Social Security Administration, etc. The information retrieved may be forwarded to the authentication/measure module 302 for use in authentication.

[0047] In other alternative embodiments, the information receive module 304 requests additional information from the user. For example, the information receive module 304 requests the user 106 (Fig. 1) to enter a one-time password or a voice print by saying a phrase or word into a microphone and sending the audio data to the information receive module 304. The information receive module 304 can send information, e.g., the one-time password, to the user 106 (Fig. 1) by requesting the email address of the user 106 (Fig. 1) from the ingest module 326, which retrieves the email address from the user information datastore 324.

[0048] The rule creation/learner module 308 receives rule inputs 310 from a financial institution or other entity to create the one or more authentication rules. In embodiments, the rule creation/learner module 308 provides an interface to the entity for authentication rule creation. The interface may be a display with one or more questions or other requests for information that allow the rule creation/learner module 308 to formulate an authentication rule. For example, the rule creation/learner module 308 may determine if the entity desires to use a keyboard dynamics for authentication. The questions may also ask at what confidence level or other measure should be considered successful authentication. For example, authentication is successful if the keyboard dynamics comparison is 80% correct or higher. The rule creation/learner module 308, in embodiments, also helps form a part of the authentication rule directed to the reaction to an authentication success or failure. The one or more determinations are rule input 310 that the rule creation/learner module 308 can use to formulate authentication rules and store the authentication rules into the rules datastore 306. The rules data store 306 may be the same or similar to the rules datastore 206 (Fig. 2). The rules may be created contemporaneously with the authentication of a user or, in embodiments, the rules are created one time by the entity, stored, and automatically read and used by the authentication/measure module 302 as authentication requests are received.

[0049] The workflow manager module 314 determines with which authentication modules 316 to communicate and how to communicate with the authentication modules 316. The authentication/measure module 302, in embodiments, provides the authentication information

needed for a predetermined authentication and requests authentication from one or more authentication modules 316. The workflow manager module 314 can reformat the request and authentication information into a form understandable by the authentication modules 316 and forward the request to the authentication modules 316. The workflow manager module 314, in embodiments, receives the reply from the authentication modules 316 and returns the response to the authentication/measure module 302 in a form understandable by the authentication/measure module 302. The workflow manager module 314 may be modified to accommodate different communications with new authentication modules 316 when the new authentication modules 316 are added. As such, while the workflow manager module may change, the interfaces to the authentication/measure module 302, the user 106 (Fig. 1), or the entities remains unchanged during these upgrades. Thus, the workflow manager module 314 allows the authentication platform to be easily upgradeable.

[0050] The authentication/measure module 302, in embodiments, completes the authentications for users 106 (Fig. 1). As such, the authentication/measure module 302 receives user input 318 from the information receive module 304, including requests 319 for authentication. Based on the authentication information within the user input 318, the authentication/measure module 302 can determine which entity's rules to use and retrieves the first rule associated with authentication for the entity from the rules datastore 306. The rule stored in the rules datastore 306 may then determine which of the authentication modules 316 to use for the authentication.

[0051] The authentication/measure module 302, in embodiments, forwards the request for authentication using the predetermined authentication modules 316, with the required information, to the workflow manager module 314. The information sent to the workflow manager module 314 may include authentication information received in the initial user input 318. In alternative embodiments, the authentication/measure module 302 may request additional information from the user 106 (Fig. 1) in which the information receive module 304 forwards the request to the user 106 (Fig. 1). For example, the information receive module 304 sends a display to the user's computer asking a question or requesting the user to enter some form of information, e.g., a voice print, fingerprint, one-time password, etc. In alternative embodiments, the authentication/measure module 302 also sends other stored data or data from public or other sources to the workflow manager module 314. For example, the authentication/measure module 302 requests, from the ingest module 326, the user's 106 (Fig. 1) previous voice print(s) stored in the user information datastore 324. The previous

voice print(s) may then be forwarded to the workflow manager module 314 with the user's current voice print received from the information receive module 304.

[0052] The authentication/measure module 302, in embodiments, also receives the result from the authentication modules 316 and responds to the result. In embodiments, one or more authentication modules 316 returns a binary result, that is, the user is authenticated or is not authenticated. In other embodiments, one or more authentication modules 316 returns a measurement. For example, the voice print authentication module 316 returns a likeness score, that is, the received voice print is some percentage like the stored voice print(s). The authentication/measure module 302 can compare the score received from the one or more authentication modules 316 and compare the received score to the threshold established in the authentication rule. If the received score is above the threshold, the user is authenticated. In alternative embodiments, if the received score is substantially near but not over the threshold, the authentication/measure module 302 attempts to conduct further authentication using one or more other authentication modules 316. In still other embodiments, the authentication/measure module 302 conducts authentication with two or more authentication modules 316 substantially simultaneously and uses the results from the two or more authentication modules 316 to determine authentication success.

[0053] If authentication is successful, the authentication/measure module 302 can send an authentication signal 322 to the user 106 (Fig. 1) verifying successful authentication. The authentication signal 322 may also grant access to the entity system 102 (Fig. 1). In alternative embodiments, the authentication/measure module 302 also sends an authentication signal 312 to the entity verifying successful authentication. The authentication signal 312 may also request the entity to grant access for the user to the entity system 102 (Fig. 1). If authentication fails, the authentication/measure module 302 may send a failure signal (not shown) to the user 106 (Fig. 1) or request the user 106 (Fig. 1) to complete other actions, for example, call the entity's customer service, inform a security entity of possible fraud, etc.

[0054] In an alternative embodiment, an authentication score model is used. The authentication/measure module 302, in embodiments, compares the authentication result from one or more authentication modules 316 to a score set in a rule. The score is a relative number that may be a percentage, a number, or other threshold. Each authentication module 316 may return a score of how well the user's input matched information stored earlier for the user. For example, the returned score is a percentage that may be compared to an

authentication percentage threshold in a rule. For example, authentication fails if the returned percentage of 65% is lesser than the threshold of 85%. In further embodiments, the returned percentage from two or more authentication modules 316 may be combined to determine the returned percentage. For example, a returned percentage of 95% is averaged with the
5 returned percentage of 85% to produce a percentage of 90%. The 90% returned percentage may then be compared to the threshold. Authentication scores above the threshold mean the user is authenticated

[0055] An embodiment of an authentication rule data structure 400 for storing one or more rules in a rules datastore is shown in Figs. 4A and 4B. The authentication rule data structure
10 400, in embodiments, is stored in a rules datastore similar or the same as rules datastore 306 (Fig. 3) and/or rules datastore 206 (Fig. 2). The rules datastore may include one or more authentication rules data structures 400 as evidenced by the ellipses 414. Embodiments of the authentication rule data structure 400 includes one or more fields, which may include, but are not limited to, an institution identifier field 402, a transaction type field 404, and/or one or
15 more authentication rules 406. The authentication rule data structure 400 may include fewer or more fields than those shown in Fig. 4 as represented by the ellipses 416. In embodiments, two or more authentication rules data structures 400 may apply to the same entity identified in the institution identifier field 402 or the same type of transaction identified in the transaction type field 404.

[0056] The institution identifier field 402 includes an identifier for the financial institution or other entity that created the authentication rule for use with the entity's customers. The institution identifier field 402 may include an entity name, a globally unique identifier (GUID), or other identifier that allows the authentication platform 200 (Fig. 2) and the entity system 202 (Fig. 2) to recognize which authentication rules apply to the user requesting the
25 authentication. For example, the user input 318 (Fig. 3) sent by a user 106 (Fig. 1) can include the institution identifier that the authentication/measure module 302 (Fig. 3) can match to the institution identifier in the institution identifier field 402 to determine which authentication rules to use for the user 106 (Fig. 1).

[0057] The transaction type field 404 includes information for the authentication platform
30 200 (Fig. 2B) that allows the authentication platform 200 (Fig. 2B) to respond to a certain type of request from the user 106 (Fig. 1). For example, a user 106 (Fig. 1) may be attempting to create an account with the financial institution. This type of transaction may

require different authentication rules because there is as yet no information stored in the user information datastore 324 (Fig. 3) for the user 106 (Fig. 1). In another example, the user 106 (Fig. 1) may be requesting access to an existing account which can require still different authentication rules. There may be other types of transactions not mentioned herein that one skilled in the art will recognize are contemplated as possible embodiments. In embodiments, the transaction type field 404 includes an identifier or other information that can be used to match the request received in the user input 318 (Fig. 3) with the authentication rules for that type of transaction. The transaction type field 404, in embodiments, includes the name of the transaction, e.g., access, account creation, etc., or an understood identifier for the transaction.

[0058] In embodiments, the authentication rules 406 includes the one or more authentication rules used for the institution identified in the institution identifier field 402 and for the transaction identifier in the transaction type field 404. An embodiment of an authentication rule 406 is shown in Fig. 4B. In embodiments, a transaction type may require authentication using two or more authentication methods executed by two or more authentication modules 316 (Fig. 3), as represented by the ellipses 420. Further, in embodiments, each authentication rule 406 may include fewer or more fields than those shown in Fig. 4B, as represented by the ellipses 418. In embodiments, the authentication rules 406 are comprised of a module identifier field 408, an information required field 409, a success threshold field 410, and/or a reaction field 412.

[0059] In embodiments, the module identifier field 408 identifies which of the authentication modules 316 (Fig. 3) should be used for the user authentication associated with the institution identified in the institution identifier field 402 and for the transaction identified in the transaction type field 404. The module identifier field 408 may include, a module name, a GUID, or other identifier that allows the rules engine 202 (Fig. 2) to determine which of the authentication modules 316 (Fig. 3) to use.

[0060] The information required field 409, in embodiments, includes the one or more items of information the authentication module 316 (Fig. 3) will need to complete the authentication. The information in the information required field 409 may include information from the user input 318 (Fig. 3) and/or information retrieved from the user information datastore 324 (Fig. 3), or information from another source and provided by the ingest module 326 (Fig. 3). The authentication/measure module 302 (Fig. 3), in embodiments, reads the information required field 409 and obtains the information listed to

provide to the workflow manager module 314 (Fig. 3) to send to the authentication module 316 (Fig. 3).

[0061] The success threshold field 410 can include the measure or the indicator used by the authentication/measure module 302 (Fig. 3) to determine if authentication is successful. In some embodiments, the success threshold field 410 includes no information or an indication that the authentication module 316 (Fig. 3) returns an indication of authentication success or failure. In alternative embodiments, the success threshold field 410 includes a score, for example, 80%, with which the authentication/measure module 302 (Fig. 3) compares to the score returned by the authentication module 316 (Fig. 3). If the returned score is higher than the score provided in the success threshold field 410, the authentication/measure module 302 (Fig. 3) can indicate authentication success. In alternative embodiments, the success threshold field 410 may include two or more thresholds with each threshold having a separate associated reaction. For example, if the score returned by the authentication module 316 (Fig. 3) is higher than a first threshold, the authentication/measure module 302 (Fig. 3) can indicate authentication success. However, if the score returned by the authentication module 316 (Fig. 3) is lower than a first threshold but higher than a second threshold listed in the success threshold field 410, the authentication/measure module 302 (Fig. 3) can attempt another type of authentication with a different authentication module 316 (Fig. 3). If the score is below both thresholds, the authentication/measure module may indicate authentication failure.

[0062] The reaction field 412, in embodiments, includes the response for the authentication/measure module 302 (Fig. 3) associated with authentication successful and/or failure. For example, the reaction field 412 contains the rule that the authentication/measure module 302 (Fig. 3) should attempt another type of authentication with a different authentication module 316 (Fig. 3) if the score returned by the authentication module 316 (Fig. 3) is lower than a first threshold but higher than a second threshold listed in the success threshold field 410. In alternative embodiments, the reaction field 412 provides an instruction to the authentication/measure module 302 (Fig. 3) to allow access and/or to send the authentication signal 322 (Fig. 3) and/or authentication signal 312 (Fig. 3) if authentication is successful. Further, the reaction field 412 may include instructions for the authentication/measure module 302 (Fig. 3) if authentication is a failure. For example, the rule in the reaction field 412 for authentication failure may be to try another authentication rule with a different identifier in the module identifier field 408. In another example, the instruction in the reaction field 412 may be to deny access and/or request the user 106 (Fig. 1)

contact customer service. In still another example, the instruction in the reaction field 412 may be to alert a security entity of a possible fraud and/or collect information on the fraudster.

5 [0063] An embodiment of a method 500 executed at an authentication platform 200 (Fig. 2) for creating an authentication rule is shown in Fig. 5. In embodiments, the method 500 generally begins with a START operation 502 and terminates with an END operation 516. The steps shown in the method 500 may be executed in a computer system as a set of computer-executable instructions. While a logical order is shown in Fig. 5, the steps shown or described can, in some circumstances, be executed in a different order than presented
10 herein.

[0064] Receive operation 504 receives institution information. In embodiments, an entity operating an entity system 102 (Fig. 1) initiates the rule creation method 500. The entity may interact with a rule creation/learner module 308 (Fig. 3) to initiate the method 500. The entity operating an entity system 102 (Fig. 1), in embodiments, sends rules information 216
15 (Fig. 2) to the authentication platform 200 (Fig. 2). In embodiments, the rule creation/learner module 308 (Fig. 3) receives the rule input 310 (Fig. 3) through interactions with the entity through a web service or other system or process allowing for communication between an administrator or other user at the entity and the authentication platform 200 (Fig. 2). A rule creation/learner module 308 (Fig. 3), in embodiments, receives the rule input 310 (Fig. 3).
20 The rule input 310 (Fig. 3) can comprise an identifier for the entity. The identifier may be a name, a GUID, or other identifier for the entity. In embodiments, the rule creation/learner module 308 (Fig. 3) creates an authentication rule data structure 400 (Fig. 4) for the new rule. The identifier received from the entity may be stored in the institution identifier field 402 of the rule data structure 400 (Fig. 4).

25 [0065] Receive operation 506 receives transaction type information. In embodiments, the entity operating the entity system 102 (Fig. 1), in embodiments, sends more rules information 216 (Fig. 2) to the authentication platform 200 (Fig. 2). The rule creation/learner module 308 (Fig. 3), in embodiments, receives the additional rule input 310 (Fig. 3), which may comprise transaction type information. The transaction type information may be an identifier or name
30 for a transaction type, for example, new account creation, user access, etc. In embodiments, the rule creation/learner module 308 (Fig. 3) creates a transaction type field 404 (Fig. 4A) for the transaction type information in the authentication rules data structure 400 (Fig. 4). The

transaction type information received from the entity may be stored in the transaction type field 404 (Fig. 4A) of the authentication rules data structure 400 (Fig. 4).

[0066] Receive operation 508 receives an authentication module choice for the transaction type. In embodiments, the entity operating the entity system 102 (Fig. 1) sends more rules information 216 (Fig. 2) to the authentication platform 200 (Fig. 2). The rule creation/learner module 308 (Fig. 3), in embodiments, receives the additional rule input 310 (Fig. 3), which comprises a selection of one or more authentication modules 316 (Fig. 3) for the type of transaction. The selection of one or more authentication modules 316 (Fig. 3) may be an input of an identifier for the one or more authentication modules 316 (Fig. 3) or a selection of the one or more authentication modules 316 (Fig. 3) from a user display, for example, a drop down menu in a web page. In embodiments, the rule creation/learner module 308 (Fig. 3) creates an authentication rules field 406 (Fig. 4A) including a module identifier field 408 (Fig. 4B) for the selection of one or more authentication modules 316 (Fig. 3). The selection of one or more authentication modules 316 (Fig. 3) received from the entity may be stored in the module identifier field 408 (Fig. 4B) of the authentication rules field 406 (Fig. 4A). Different rules may apply to different transactions. For example, if a user is desiring to create a new relationship with the entity, a set of rules for authentication of a new user are used. If the user is returning to access an existing account, a different set of rules may be used.

[0067] Determine operation 509 determines the information required for the one or more authentication modules 316 (Fig. 3). In embodiments, the rule creation/learner module 308 (Fig. 3) reads information about the one or more authentication modules 316 (Fig. 3) from the authentication rule datastore 306 (Fig. 3). The information includes one or more items of information needed by the one or more authentication modules 316 (Fig. 3) to attempt an authentication. The rule creation/learner module 308 (Fig. 3) can create an information required field 409 (Fig. 4B) in the authentication rules field 406 (Fig. 4A). The one or more items of information required by the one or more authentication modules 316 (Fig. 3), as determined by the rule creation/learner module 308 (Fig. 3), may be stored in the information required field 409 (Fig. 4B) of the authentication rules field 406 (Fig. 4A).

[0068] Receive operation 510 receives the success criteria for the authentication. The entity operating an entity system 102 (Fig. 1), in embodiments, sends more rules information 216 (Fig. 2) to the authentication platform 200 (Fig. 2), which comprises the success threshold for the authentication using the one or more authentication modules 316 (Fig. 3).

The rule creation/learner module 308 (Fig. 3), in embodiments, receives the additional rule input 310 (Fig. 3). The success threshold information may be a score to compare to a return from the one or more authentication modules 316 (Fig. 3) or may be a simple success or failure indicator for the return by the one or more authentication modules 316 (Fig. 3). In alternative embodiments, no success threshold is provided as the one or more authentication modules 316 (Fig. 3) provide the authentication success indication. In embodiments, the rule creation/learner module 308 (Fig. 3) creates a success threshold field 410 (Fig. 4B). The success threshold received from the entity may be stored in the success threshold field 410 (Fig. 4B) of the authentication rules field 406 (Fig. 4A).

[0069] Receive operation 512 receives the reaction information. In embodiments, the entity operating an entity system 102 (Fig. 1) sends more rules information 216 (Fig. 2) to the authentication platform 200 (Fig. 2), which comprises the reaction information for the authentication using the one or more authentication modules 316 (Fig. 3). The rule creation/learner module 308 (Fig. 3), in embodiments, receives the additional rule input 310 (Fig. 3). The reaction information may be one or more instructions on how to react to the success or failure of an authentication. For example, if authentication fails using one of the one or more authentication modules 316 (Fig. 3), another of the one or more authentication modules 316 (Fig. 3) may then be used to complete the authentication. In embodiments, the rule creation/learner module 308 (Fig. 3) creates a reaction field 412 (Fig. 4B). The reaction instructions received from the entity may be stored in the reaction field 412 (Fig. 4B) of the authentication rules field 406 (Fig. 4A).

[0070] Store operation 514 stores the received information. In embodiments, the rule creation/learner module 308 (Fig. 3) stores the information received from the entity or determined for the authentication rule into the one or more fields of the authentication rules data structure 400 (Fig. 4). The information may be stored as received or the entire authentication rules data structure 400 (Fig. 4) may be written into the rules datastore 306 (Fig. 3) after all of the information is received. After storing the authentication rules data structure 400 (Fig. 4), the rule creation/learner module 308 (Fig. 3) may receive information to create a new rule for the entity.

[0071] An embodiment of a method 600 executed at an entity operating an entity system 102 (Fig. 1) for creating an authentication rule is shown in Fig. 6. In embodiments, the method 600 generally begins with a START operation 602 and terminates with an END

operation 616. The steps shown in the method 600 may be executed in a computer system as a set of computer-executable instructions. While a logical order is shown in Fig. 6, the steps shown or described can, in some circumstances, be executed in a different order than presented herein.

5 [0072] Send operation 604 sends institution information. In embodiments, an entity operating an entity system 102 (Fig. 1) initiates the rule creation method 600. The entity may interact with a rule creation/learner module 308 (Fig. 3) to initiate the method 600. The entity operating an entity system 102 (Fig. 1), in embodiments, sends rules information 216 (Fig. 2) to the authentication platform 200 (Fig. 2). In embodiments, the entity system 102 (Fig. 1) sends rule input 310 (Fig. 3) to a creation/learner module 308 (Fig. 3) through
10 interactions with a web service or other system or process allowing for communication between an administrator or other user at the entity and the authentication platform 200 (Fig. 2). A rule creation/learner module 308 (Fig. 3), in embodiments, receives the rule input 310 (Fig. 3). The rule input 310 (Fig. 3) can comprise an identifier for the entity. The
15 identifier may be a name, a GUID, or other identifier for the entity.

[0073] Send operation 606 sends transaction type information. The entity operating the entity system 102 (Fig. 1), in embodiments, sends more rules information 216 (Fig. 2) to the authentication platform 200 (Fig. 2), which may comprise transaction type information. The transaction type information may be an identifier or name for a transaction type, for example,
20 new account creation, user access, etc. Different rules may apply to different transactions. For example, if a user is desiring to create a new relationship with the entity, a set of rules for authentication of a new user are used. If the user is returning to access an existing account, a different set of rules may be used.

[0074] Send operation 608 sends a choice of an authentication module for authentication
25 associated with the transaction type. In embodiments, the entity operating the entity system 102 (Fig. 1) sends more rules information 216 (Fig. 2) to the authentication platform 200 (Fig. 2), which comprises a selection of one or more authentication modules 316 (Fig. 3) for the type of transaction. The selection of one or more authentication modules 316 (Fig. 3) may be an input of an identifier for the one or more authentication modules 316 (Fig. 3) or a
30 selection of the one or more authentication modules 316 (Fig. 3) from a user display, for example, a drop down menu in a web page.

[0075] Send operation 610 sends the success criteria for the authentication. In embodiments, the entity operating an entity system 102 (Fig. 1) sends more rules information 216 (Fig. 2) to the authentication platform 200 (Fig. 2), which comprises the success threshold for the authentication using the one or more authentication modules 316 (Fig. 3).

5 The rule creation/learner module 308 (Fig. 3), in embodiments, receives the additional rule input 310 (Fig. 3). The success threshold information may be a score to compare to a return from the one or more authentication modules 316 (Fig. 3) or may be a simple success or failure indicator for the return by the one or more authentication modules 316 (Fig. 3). In alternative embodiments, no success threshold is provided as the one or more authentication
10 modules 316 (Fig. 3) provide the authentication success indication.

[0076] Send operation 612 sends the reaction information. In embodiments, the entity operating an entity system 102 (Fig. 1) sends more rules information 216 (Fig. 2) to the authentication platform 200 (Fig. 2), which comprises the reaction information for the authentication using the one or more authentication modules 316 (Fig. 3). The rule
15 creation/learner module 308 (Fig. 3), in embodiments, receives the additional rule input 310 (Fig. 3). The reaction information may be one or more instructions on how to react to the success or failure of an authentication. For example, if authentication fails using one of the one or more authentication modules 316 (Fig. 3), another of the one or more authentication modules 316 (Fig. 3) may then be used to complete the authentication.

20 [0077] Receive operation 614 receives an indication that the authentication rule was created. In embodiments, the rule creation/learner module 308 (Fig. 3) stores the information received from the entity or determined for the rule into the one or more fields of the authentication rules data structure 400 (Fig. 4). In response to storing the authentication rules data structure 400 (Fig. 4), the rule creation/learner module 308 (Fig. 3) may then send an
25 indication to the entity system 102 (Fig. 1) that the rule was created. The indication may be a message stating that rule creation was necessary. In another embodiment, the indication is a request from the rule creation/learner module 308 (Fig. 3) to the entity system 102 (Fig. 1) to create another rule. After receiving the indication, the entity system 102 (Fig. 1) may send more information to create a new rule for the entity.

30 [0078] An embodiment of a method 700 executed at an authentication platform 200 (Fig. 2) for authenticating a user 106 (Fig. 1) of an entity system 102 (Fig. 1) is shown in Figs. 7A and 7B. In embodiments, the method 700 generally begins with a START operation 702 and

terminates with an END operation 728. The steps shown in the method 700 may be executed in a computer system as a set of computer-executable instructions. While a logical order is shown in Figs. 7A and 7B, the steps shown or described can, in some circumstances, be executed in a different order than presented herein. Page connector A 714 and connector B

5 716 continue the flow of the method 700 between Fig. 7A and Fig. 7B.

[0079] Receive operation 704 receives a request for authentication. In embodiments, a user 106 (Fig. 1) initiates an authentication request 319 (Fig. 3). The authentication request 319 (Fig. 3) may include the user requesting a web page from an entity system 102 (Fig. 1), the user requesting a new account or relationship with the entity system 102 (Fig. 1), or the user attempting to access an existing account. The entity system 102 (Fig. 1) can require the user 106 (Fig. 1) to log-in to the entity system 102 (Fig. 1). The entity system 102 (Fig. 1) may then have the user 106 (Fig. 1) request authentication from the authentication platform 200 (Fig. 2) or may forward the authentication request to the authentication platform 200 (Fig. 2). In embodiments, the user interface 208 (Fig. 2) receives the request. In further embodiments, 15 the information receive module 304 (Fig. 3) of the rules engine 300 (Fig. 3) receives the request 319 (Fig. 3).

[0080] Extract operation 706 extracts authentication information from the authentication request 319 (Fig. 3) or user input 318 (Fig. 3). In embodiments, the information receive module 304 (Fig. 3) extracts one or more items of information. For example, the information 20 receive module 304 (Fig. 3) extracts the entity identifier and the type of transaction from the authentication request 319 (Fig. 3) or user input 318 (Fig. 3) to send to the authentication/measure module 302 (Fig. 3). In embodiments, the information receive module 304 (Fig. 3) provides the extracted information to the authentication/measure module 302 (Fig. 3).

25 [0081] Determine operation 708 determines the authentication module to use for the authentication. In embodiments, the authentication/measure module 302 (Fig. 3) accesses the rules datastore 306 (Fig. 3) to locate the rule data structure 400 (Fig. 4) associated with the entity identifier, type of transaction, and other information provided by the information receive module 304 (Fig. 3). The authentication/measure module 302 (Fig. 3) may read the 30 institution identifier field 402 (Fig. 4A) for one or more authentication rule data structures 400 (Fig. 4) and compare the institution identifier received from the information receive module 304 (Fig. 3) to the institution identifier in the institution identifier field 402 (Fig. 4A).

Upon finding a match, the authentication/measure module 302 (Fig. 3) may compare the information in the type of transaction field 404 (Fig. 4A) with the type of transaction information received from the information receive module 304 (Fig. 3). The type of transaction may be the establishment of a new account or the access of an existing account.

5 The comparisons may continue until the authentication/measure module 302 (Fig. 3) determines the one or more authentication modules, listed in the authentication module identifier field 408 (Fig. 4B), to use for authentication.

[0082] Send operation 710 sends information to the determined authentication module. In embodiments, the authentication/measure module 302 (Fig. 3) collects one or more items of
10 information for the identified authentication module 316 (Fig. 3). For example, the authentication/measure module 302 (Fig. 3) sends one or more other items extracted from the authentication request by the information receive module 304 (Fig. 3). In other embodiments, the authentication/measure module 302 (Fig. 3) requests the ingest module 326 (Fig. 3) to provide one or more items of information. In one embodiment, the ingest module
15 326 (Fig. 3) accesses the user information datastore 324 (Fig. 3) to obtain known information, for example, a computer fingerprint, a voice print, keyboard dynamics, etc., about the user 106 (Fig. 1). This known information may have been compiled from one or more previous authentications. The known information may have been used to authenticate the user previously. Known information may not be available for new users asking for an account
20 creation.

[0083] In other embodiments, the ingest module 326 (Fig. 3) accesses information from one or more other sources via a network 322 (Fig. 3). For example, if the user 106 (Fig. 1) is requesting the creation of an account, no known information may be stored in the user information datastore 324 (Fig. 3). As such, the ingest module 326 (Fig. 3) may retrieve
25 information from other sources. For example, an out-of-wallet authentication module 118 (Fig. 1) can authenticate a user 106 (Fig. 1) having the user 106 (Fig. 1) answer questions about a previous car the user 106 (Fig. 1) may have owned. The information about the car may be retrieved from the Department of Motor Vehicles by the ingest module 326 (Fig. 3). This retrieved information may be provided to the authentication/measure module 302
30 (Fig. 3) to send to the authentication module 316 (Fig. 3). In embodiments, the authentication/measure module 302 (Fig. 3) provides the request and information to the workflow manager 314 (Fig. 3) to send in the proper format to the authentication module 316 (Fig. 3).

[0084] Further communications between the authentication/measure module 302 (Fig. 3), the authentication module 316 (Fig. 3), and/or the information receive module 304 (Fig. 3) are possible to request and provide further information. For example, a one-time password authentication module 114 (Fig. 1) may request the authentication/measure module 302 (Fig. 3) to send a one-time password to the user. The authentication/measure module 302 (Fig. 3) may request the email address from the ingest module 326 (Fig. 3), which reads the email address from the user information datastore 324 (Fig. 3) and provides the email address to the authentication/measure module 302 (Fig. 3). The authentication/measure module 302 (Fig. 3) can have the information receive module 304 (Fig. 3) send an email to the user 106 (Fig. 1) with the one-time password. The information receive module 304 (Fig. 3) may then send the received password back to the authentication module 316 (Fig. 3) after the password is received from the user 106 (Fig. 1). As such, the send operation 710 continues until the authentication module 316 (Fig. 3) has the information for the authentication.

[0085] Receive operation 712 receives a return. In embodiments, the workflow manager 314 (Fig. 3) receives the return from the authentication module 316 (Fig. 3). The workflow manager 314 (Fig. 3) may translate the return for the authentication/measure module 302 (Fig. 3). The method 700 then flows through page connector A 714 to determine operation 718.

[0086] Determine operation 718 determines if the user 106 (Fig. 1) was authenticated by the authentication module 316 (Fig. 3). In embodiments, the authentication module 316 (Fig. 3) provides an indication of authentication success or failure. For example, a one-time password authentication module 114 (Fig. 1) may return an indication that the password was correct. In other embodiments, the authentication/measure module 302 (Fig. 3) determines authentication success or failure by comparing a return to a success threshold stored in a success threshold field 410 (Fig. 4B) in a rule data structure 400 (Fig. 4). The authentication/measure module 302 (Fig. 3) may retrieve the rule data structure 400 (Fig. 4) from the rules datastore 306 (Fig. 3). Then, the authentication/measure module 302 (Fig. 3) can read the success threshold from the success threshold field 410 (Fig. 4B). In embodiments, the return is then compared to the success threshold. If the return betters the threshold, the authentication/measure module 302 (Fig. 3) can indicate authentication success.

[0087] For example, a keyboard dynamics authentication module 112 (Fig. 1) may return a score of 82% as a match of the user's method for entering a word or phrase with a known method. The success threshold stored in the success threshold field 410 (Fig. 4B) may be 80%, wherein returned scores greater than 80% represent a successful authentication. The authentication/measure module 302 (Fig. 3) may compare the returned score of 82% with the threshold of 80% and indicate successful authentication.

[0088] In further embodiments, the authentication/measure module 302 (Fig. 3) may interact with two or more authentication modules 316 (Fig. 3) and require success from each of the authentication modules 316 (Fig. 3). If authentication is successful, the method 700 flows YES to allow operation 720. If the user 106 (Fig. 1) fails the authentication, the method 700 flows NO to read operation 722.

[0089] Allow operation 720 allows access. In embodiments, the authentication/measure module 302 (Fig. 3) allows the user 106 (Fig. 1) to access the entity system 102 (Fig. 1) after successful authentication. The authentication/measure module 302 (Fig. 3) may send an authentication signal 322 (Fig. 3) to the user 106 (Fig. 1) to indicate successful authentication and may send authentication signal 312 (Fig. 3) to the entity system 102 (Fig. 1) to instruct the entity that the user 106 (Fig. 1) is authenticated and should be allowed access.

[0090] Read operation 722 reads a next rule. After authentication failure, the authentication/measure module 302 (Fig. 3) determines what to do next. In embodiments, the authentication/measure module 302 (Fig. 3) reads the reaction field 412 (Fig. 4B) to retrieve instructions for how to respond to the authentication failure. The information in the reaction field 412 (Fig. 4B) may represent the rule read by the authentication/measure module 302 (Fig. 3). In another embodiment, the reaction field 412 (Fig. 4B) instructs the authentication/measure module 302 (Fig. 3) to access a different rule data structure 400 (Fig. 4) stored in the rules datastore 306 (Fig. 3). For example, the reaction field 412 (Fig. 4B) contains another set of authentication module identifier 408 (Fig. 4B) or other information with an instruction to authenticate using the different authentication module 316 (Fig. 3). This separate authentication rule may represent the rule read by the authentication/measure module 302 (Fig. 3).

[0091] Determine operation 724 determines if a next authentication module is to be used. If the reaction field 412 (Fig. 4B) has information to use another authentication module, the authentication/measure module 302 (Fig. 3) determines that another authentication module is

to be used, and the method 700 flows YES through page connector B 716 back to receive operation 704. In embodiments, the authentication/measure module 302 (Fig. 3) collects more information for the next-used authentication module 316 (Fig. 3). In an alternative embodiment, all needed information was already collected and the method flows YES to
5 determine operation 708. If the reaction field 412 (Fig. 4B) does not require the use of another authentication module, the authentication/measure module 302 (Fig. 3) determines that another authentication module is not to be used, and the method flows NO to react operation 726.

[0092] React operation 726 responds to authentication failure. In embodiments, the
10 reaction field 412 (Fig. 4B) contains instructions for a failure to authenticate. The authentication/measure module 302 (Fig. 3) can read the instructions from the reaction field 412 (Fig. 4B) and execute the instructions. In one embodiment, the authentication/measure module 302 (Fig. 3) denies the user 106 (Fig. 1) access by informing the entity system 102 (Fig. 1) not to allow access. In another embodiment, the authentication/measure module 302
15 (Fig. 3) sends a message to the user 106 (Fig. 1) to contact customer service personnel. In still another embodiment, the authentication/measure module 302 (Fig. 3) informs a security entity for the entity system 102 (Fig. 1) that the user may be a potential fraudster and action is required to protect the entity system 102 (Fig. 1).

[0093] In an alternative embodiment, the authentication/measure module 302 (Fig. 3) sends
20 information to two or more authentication modules during the send operation 710. The two or more returns are received in the receive operation 712. The authentication/measure module 302 (Fig. 3) can then use the combined returns to determine if the user is authenticated in determine operation 718.

[0094] An embodiment of a method 800 executed by a user 106 (Fig. 1) for authenticating
25 the user 106 (Fig. 1) of an entity system 102 (Fig. 1) is shown in Fig. 8. In embodiments, the method 800 generally begins with a START operation 802 and terminates with an END operation 814. The steps shown in the method 800 may be executed in a computer system as a set of computer-executable instructions. While a logical order is shown in Fig. 8, the steps shown or described can, in some circumstances, be executed in a different order than
30 presented herein.

[0095] Send operation 804 sends a request for authentication and/or authentication information. In embodiments, the user 106 (Fig. 1) initiates an authentication request. The

authentication request 319 (Fig. 3) may include the user 106 (Fig. 1) requesting a web page from an entity system 102 (Fig. 1), the user requesting a new account or relationship with the entity system 102 (Fig. 1), or the user attempting to access an existing account. The entity system 102 (Fig. 1) may require the user 106 (Fig. 1) to log-in to the entity system 102 (Fig. 1). The entity system 102 (Fig. 1) may then have the user 106 (Fig. 1) request authentication from the authentication platform 200 (Fig. 2) or may forward the authentication request to the authentication platform 200 (Fig. 2). In embodiments, the user interface 208 (Fig. 2) receives the request 319 (Fig. 3). In further embodiments, the information receive module 304 (Fig. 3) of the rules engine 300 (Fig. 3) receives the request 319 (Fig. 3).

[0096] In embodiments, the user 106 (Fig. 1) may also send one or more items of authentication information 318 (Fig. 3) requested by identified authentication module 316 (Fig. 3). For example, the authentication/measure module 302 (Fig. 3) requests one or more other items of information 318 (Fig. 3) from the user 106 (Fig. 1). In other embodiments, the authentication/measure module 302 (Fig. 3) requests the ingest module 326 (Fig. 3) to provide one or more items of information. For example, a one-time password authentication module 114 (Fig. 1) may request the authentication/measure module 302 (Fig. 3) to send a one-time password to the user 106 (Fig. 1). The authentication/measure module 302 (Fig. 3) may request the email address from the ingest module 326 (Fig. 3), which reads the email from the user information datastore 324 (Fig. 3) and provides the email address to the authentication/measure module 302 (Fig. 3). The authentication/measure module 302 (Fig. 3) can have the information receive module 304 (Fig. 3) send an email to the user 106 (Fig. 1) with the one-time password. The user 106 (Fig. 1) may access his or her email account to retrieve the one-time password. The one-time password may then be sent to the authentication platform 200 (Fig. 2). As such, the send operation 804 continues until the authentication module 316 (Fig. 3) has the information for the authentication.

[0097] Determine operation 806 determines if the user 106 (Fig. 1) was authenticated. In embodiments, the authentication/measure module 302 (Fig. 3) allows the user 106 (Fig. 1) to access the entity system 102 (Fig. 1) after successful authentication. The authentication/measure module 302 (Fig. 3) may send an authentication signal 322 (Fig. 3) to the user 106 (Fig. 1) to indicate successful authentication and may send authentication signal 312 (Fig. 3) to the entity system 102 (Fig. 1) to instruct the entity that the user 106 (Fig. 1) is authenticated and should be allowed access. If the user 106 (Fig. 1) receives the

authentication signal 322 (Fig. 3), the user 106 (Fig. 1) determines that he or she has been authenticated, and the method flows YES to receive operation 808. If the user 106 (Fig. 1) does not receive the authentication signal 322 (Fig. 3), the user 106 (Fig. 1) determines that he or she has not been authenticated, and the method flows NO to determine operation 810.

5 [0098] Receive operation 808 receives user access. In embodiments, the user 106 (Fig. 1) gains access to the entity system 102 (Fig. 1) after receiving authentication signal 322 (Fig. 3) allows the user 106 (Fig. 1). The user 106 (Fig. 1) can then begin to use the entity system 102 (Fig. 1).

[0099] Determine operation 810 determines if more information is required. In
10 embodiments, the reaction field 412 (Fig. 4B) instructs the authentication/measure module 302 (Fig. 3) to access a different authentication rule data structure 400 (Fig. 4) stored in the rules datastore 306 (Fig. 3). For example, the reaction field 412 (Fig. 4B) contains another set of authentication module identifier 408 (Fig. 4B) or other information with an instruction to authenticate using the different authentication module 316 (Fig. 3). In embodiments, the
15 authentication/measure module 302 (Fig. 3) collects more information for the next-used authentication module 316 (Fig. 3). If more information is required, the method 800 flows YES back to send operation 804. In embodiments, the user 106 (Fig. 1) provides the additional information required by sending the information to the authentication platform 100 (Fig. 1). If no more information is required, the method 800 flows NO to fail operation 812.
20 Fail operation 812 fails to provide access. In embodiments, the user 106 (Fig. 1) receives an indication that authentication failed and he or she will not be given access. The user 106 (Fig. 1) may then attempt another authentication.

[0100] Embodiments of the different systems represented in this disclosure, which may include the user system 106 (Fig. 1), the authentication platform 100 (Fig. 1), and/or the
25 entity system 102 (Fig. 1), may be a computer system, such as computer system 900 shown in Fig. 9. A basic computer system is shown as one skilled in the art will recognize the technical changes and modifications that may be required to make the systems described herein operable. The computer system 900 comprises a processor 902, which completes the operations described in conjunction with Figs. 5 through 8 or makes the systems operable
30 described in conjunction with Figs. 1 through 3. The processor 902 may be any type of processor operable to complete the operations or implement the systems described herein.

For example, the processor 902 may be an Intel Pentium processor, an application specific integrated circuit (ASIC), a field programmable gate array (FPGA), or other device.

[0101] The computer system 900 also comprises memory 904 to hold data or code being executed by processor 902. The memory 904 may permanently or temporarily store the instructions described in conjunction with Figs. 5 through 8 or the data elements described in conjunction with Figs. 4A and 4B. Memory may be classified as computer readable medium, for example, RAM, ROM, magnetic media, optical media, etc.

[0102] The computer system 900 also can comprise software elements, including an operating system and/or other code, such as one or more application programs for creating an authentication rule at the authentication platform 100 (Fig. 1) with interaction with entity system 102 (Fig. 1) or authenticating a user with the authentication platform 100 (Fig. 1) with interactions with a user 106 (Fig. 1). The application programs may comprise computer programs described herein, and/or may be designed to implement methods described herein and/or configure systems described herein. Merely by way of example, one or more procedures described with respect to the method(s) discussed in conjunction with Figs. 5 through 8 might be implemented as code and/or instructions executable by the computer system 900 (and/or the processor 902 within the computer 900).

[0103] A set of these instructions and/or code might be stored on a computer readable storage medium, such as the storage device(s) 908 or memory 904. In some cases, the storage medium might be incorporated within a computer system. In other embodiments, the storage medium might be separate from a computer system (i.e., a removable medium, such as a compact disc, etc.), and/or provided in an installation package, such that the storage medium can be used to program a general purpose computer with the instructions/code stored thereon. These instructions might take the form of executable code, which is executable by the computer system 900 and/or might take the form of source and/or installable code, which, upon compilation and/or installation on the computer system 900 (e.g., using any of a variety of generally available compilers, installation programs, compression/decompression utilities, etc.) then takes the form of executable code.

[0104] Further embodiments of the computer system 900 comprises input/output (I/O) modules of systems 906. I/O systems 906 may include displays such as LCDs, plasma screen, cathode ray tubes, etc. The I/O systems 906 can provide a visual representation of data to a user 106 (Fig. 1) or the entity system 102 (Fig. 1). I/O system 906 may also include

input devices such as mice, keyboards, touch screens, etc. Input devices or the communications interfaces with other systems allow the user 106 (Fig. 1) or entity system 102 (Fig. 1) to input information into the authentication platform 100 (Fig. 1). I/O systems 906 may also comprise communication systems such as wired, wireless, or other communication systems. Further, communication systems may communicate with peripheral devices, such as printers, modems, or other devices.

[0105] In light of the above description, a number of advantages of the present disclosure are readily apparent. For example, the systems described herein allow entities, such as banks, or other institutions, to authenticate a user using one or many authentication processes. The institutions can customize how to authenticate users using different authentication methods, can customize the different intensities of authentication (e.g., how high to set success thresholds), and can customize the responses to authentication failures. Further, the authentication platform 100 (Fig. 1) can easily integrate or remove authentication modules without changing the interfaces for the user or the entity. Thus, the authentication systems are easily upgraded as new types of authentication are introduced in the market. The easy upgrading of the authentication platform 100 (Fig. 1) ensures the authentication platform 100 (Fig. 1) can adapt to meet ever-changing security needs of the different entities.

[0106] A number of variations and modifications of the disclosure can also be used. For example, the entity system may integrate the authentication platform 100 (Fig. 1) into the entity system 102 (Fig. 1). In other embodiments, the authentication platform 100 (Fig. 1) can be a hosted platform contacted by two or more entities. As such, the authentication platform 100 (Fig. 1) can meet the authentication needs of two or more entities using the same system. The authentication platform 100 (Fig. 1) would create different authentication rules for the different entities and store the authentication rules in the rules datastore 306 (Fig. 3).

[0107] It will be apparent to those skilled in the art that substantial variations may be made in accordance with specific requirements. For example, customized hardware might also be used, and/or particular elements might be implemented in hardware, software (including portable software, such as applets, etc.), or both. Further, connection to other computing devices such as network input/output devices may be employed.

[0108] While the principles of the disclosure have been described above in connection with specific apparatuses and methods, it is to be clearly understood that this description is made only by way of example and not as limitation on the scope of the disclosure.

WHAT IS CLAIMED IS:

1 1. An authentication platform for authenticating a user desiring access to
2 an entity system, the authentication platform comprising:
3 two or more authentication modules, each authentication module operable to
4 authenticate the user using a different authentication method;
5 a decision engine in communication with the two or more authentication
6 modules, the decision engine operable to receive an authentication request from the user, the
7 decision engine operable to send one or more items of authentication information to a first
8 authentication module to authenticate the user, the decision engine operable to receive a
9 return from the first authentication module, the decision engine operable to determine if the
10 user has been authenticated by the first authentication module, the decision engine operable
11 to inform the user that the user has been authenticated.

1 2. The authentication platform as defined in claim 1, wherein the decision
2 engine is operable to send one or more items of information to a second authentication
3 module to authenticate the user if the first authentication module failed to authenticate the
4 user, the decision engine operable to receive a return from the second authentication module,
5 the decision engine operable to determine if the user has been authenticated by the second
6 authentication module, the decision engine operable to inform the user that the user has been
7 authenticated.

1 3. The authentication platform as defined in claim 1, further comprising:
2 a user system in communication with the decision engine; and
3 an entity system in communication with the decision engine.

1 4. The authentication platform as defined in claim 1, wherein the decision
2 engine comprises:
3 a user interface, the user interface operable to receive the authentication
4 request, the user interface operable to receive one or more items of the authentication
5 information from the user;
6 an institution interface, the institution interface operable to receive one or
7 more authentication rules from one or more entities;
8 an authentication module interface, the authentication module interface
9 operable to send information to one of the two or more authentication modules for

10 authentication, the authentication module interface operable to receive the return from one of
11 the two or more authentication modules for authentication;
12 a rules datastore, the rules datastore operable to store one or more
13 authentication rules; and
14 a rules engine in communication with the user interface, the institution
15 interface, the authentication module interface, and the rules datastore, the rules engine
16 operable to store one or more authentication rules received from the institution interface into
17 the rules datastore, the rules engine operable to receive an authentication request and the one
18 or more items of authentication information from the user interface, the rules engine operable
19 to read a rule from the rules datastore associated with the authentication request, the rules
20 engine operable to send the authentication information to the authentication module interface
21 for the first authentication module identified in the rule, the rules engine operable to receive a
22 return from the first authentication module, the rules engine operable to determine if the user
23 has been authenticated by the first authentication module, and the rules engine operable to
24 inform the user that the user has been authenticated by sending a message through the user
25 interface.

1 5. The authentication platform as defined in claim 4, wherein the rules
2 engine comprises:
3 a rule creation/learner module, the rule creation/learner module operable to
4 receive the one or more authentication rules from the institution interface, the rule
5 creation/learner module operable to store the one or more authentication rules in the rules
6 datastore.

1 6. The authentication platform as defined in claim 4, wherein the rules
2 engine comprises:
3 an information receive module, the information receive module operable to
4 receive the authentication request and the one or more items of authentication information
5 from the user, the information receive module operable to extract the one or more items of
6 authentication information, the information receive module operable to request one or more
7 other items of authentication information from the user; the information receive module
8 operable to receive the one or more other items of authentication information from the user.

1 7. The authentication platform as defined in claim 6, wherein the rules
2 engine comprises:

3 an ingest module, the ingest module operable to store one or more items of
4 authentication information received from the user in a user information datastore, the ingest
5 module operable to provide the one or more items of authentication information from the user
6 information datastore, and the ingest module operable to retrieve one or more items of
7 authentication information from one or more other sources accessed through a network.

1 8. The authentication platform as defined in claim 4, wherein the rules
2 engine comprises:

3 a workflow manager module, the workflow manager module operable to send
4 the one or more items of authentication information to one or more authentication modules,
5 the workflow manager module operable to receive a return from the one or more
6 authentication modules.

1 9. The authentication platform as defined in claim 4, wherein the rules
2 engine comprises:

3 an authentication/measure module, the authentication/measure module
4 operable to receive an authentication request and the one or more items of authentication
5 information from an information receive module, the authentication/measure module
6 operable to read a rule from the rules datastore associated with the authentication request, the
7 authentication/measure module operable to send the authentication information to a workflow
8 manager module for the first authentication module identified in the rule, the
9 authentication/measure module operable to receive a return from the workflow manager
10 module, the authentication/measure module operable to determine if the user has been
11 authenticated by the first authentication module, and the authentication/measure module
12 operable to inform the user that the user has been authenticated by sending an authentication
13 signal to the user.

1 10. The authentication platform as defined in claim 9, wherein the
2 authentication/measure module is operable to determine that more authentication information
3 is needed from the user, the authentication/measure module operable to request the
4 information receive module to provide the more authentication information, and the
5 information receive module operable to request the more authentication information.

1 11. A method for authenticating a user of an entity system using an
2 authentication platform, the method comprising:
3 receiving an authentication request from the user;
4 extracting one or more items of authentication information;
5 determining a first authentication module to use for the authentication;
6 sending at least one of the one or more items of extracted authentication
7 information to a first authentication module;
8 receiving a return from the first authentication module;
9 determining if the user has been authenticated by the first authentication
10 module;
11 if the user has been authenticated, allowing the user access to the entity
12 system; and
13 if the user has not been authenticated, denying the user access to the entity
14 system.

1 12. The method as defined in claim 11, further comprising:
2 if the user has not been authenticated, sending at least one of the one or more
3 items of extracted authentication information to a second authentication module;
4 receiving a return from the second authentication module;
5 determining if the user has been authenticated by the second authentication
6 module;
7 if the user has been authenticated, allowing the user access to the entity
8 system; and
9 if the user has not been authenticated, denying the user access to the entity
10 system.

1 13. The method as defined in claim 11, wherein determining a first
2 authentication module to use for the authentication comprises:
3 reading an authentication rule from a rules datastore; and
4 reading an authentication module identifier for the authentication rule.

1 14. The method as defined in claim 13, further comprising:
2 receiving institution information from the entity system;
3 receiving transaction type information from the entity system;

4 receiving a choice of one or more authentication modules from the entity
5 system;
6 determining authentication information required for the chosen one or more
7 authentication modules;
8 receiving success criteria from the entity system;
9 receiving reaction information from the entity system; and
10 storing the institution information, the transaction type information, the choice
11 of one or more authentication modules, the authentication information required, the success
12 criteria, and the reaction information into an authentication rule data structure.

1 15. The method as defined in claim 11, wherein determining if the user has
2 been authenticated by the first authentication module comprises:
3 reading the score from a success threshold field of an authentication rule
4 stored in a rules datastore;
5 comparing a returned score returned by the first authentication module with
6 the score stored in the authentication rule; and
7 determining if the returned score betters the score stored in the authentication
8 rule.

1 16. The method as defined in claim 11, further comprising:
2 requesting further authentication information from the user;
3 receiving the further authentication information from the user; and
4 sending at least a portion of the further authentication information to the first
5 authentication module.

1 17. A computer program stored on a computer readable medium, the
2 computer program embodied in one or more instructions for authenticating a user of an entity
3 system, the computer program comprising:

4 instructions to receive an authentication request;

5 instructions to determine the entity system associated with the authentication
6 request;

7 instructions to determine a type of transaction associated with the
8 authentication request;

9 instructions to locate an authentication rule associated with the entity system
10 and the type of transaction;

11 instructions to read the authentication rule;

12 instructions to determine the authentication module associated with the
13 authentication rule;

14 instructions to provide one or more items of authentication information to the
15 authentication module;

16 instructions to receive a return from the authentication module; and

17 instructions to determine if the user is authenticated according to the return.

1 18. The computer program as defined in claim 17, further comprising:

2 instructions to receive institution information from the entity system;

3 instructions to receive transaction type information from the entity system;

4 instructions to receive a choice of one or more authentication modules from
5 the entity system;

6 instructions to determine authentication information required for the chosen
7 one or more authentication modules;

8 instructions to receive success criteria from the entity system;

9 instructions to receive reaction information from the entity system;

10 instructions to create the authentication rule; and

11 instructions to store the institution information, the transaction type
12 information, the choice of one or more authentication modules, the authentication
13 information required, the success criteria, and the reaction information into the authentication
14 rule.

1 19. The computer program as defined in claim 18, wherein the institution
2 information is stored in an institution information field, the transaction type information is
3 stored in a transaction type field, the choice of one or more authentication modules is stored
4 in an authentication module identifier field, the authentication information required is stored
5 in an information required field, the success criteria is stored in a success threshold field, and
6 the reaction information is stored in a reaction field.

1 20. The computer program as defined in claim 17, further comprising
2 instructions to send an authentication signal to the user indicating the user has been
3 authenticated.

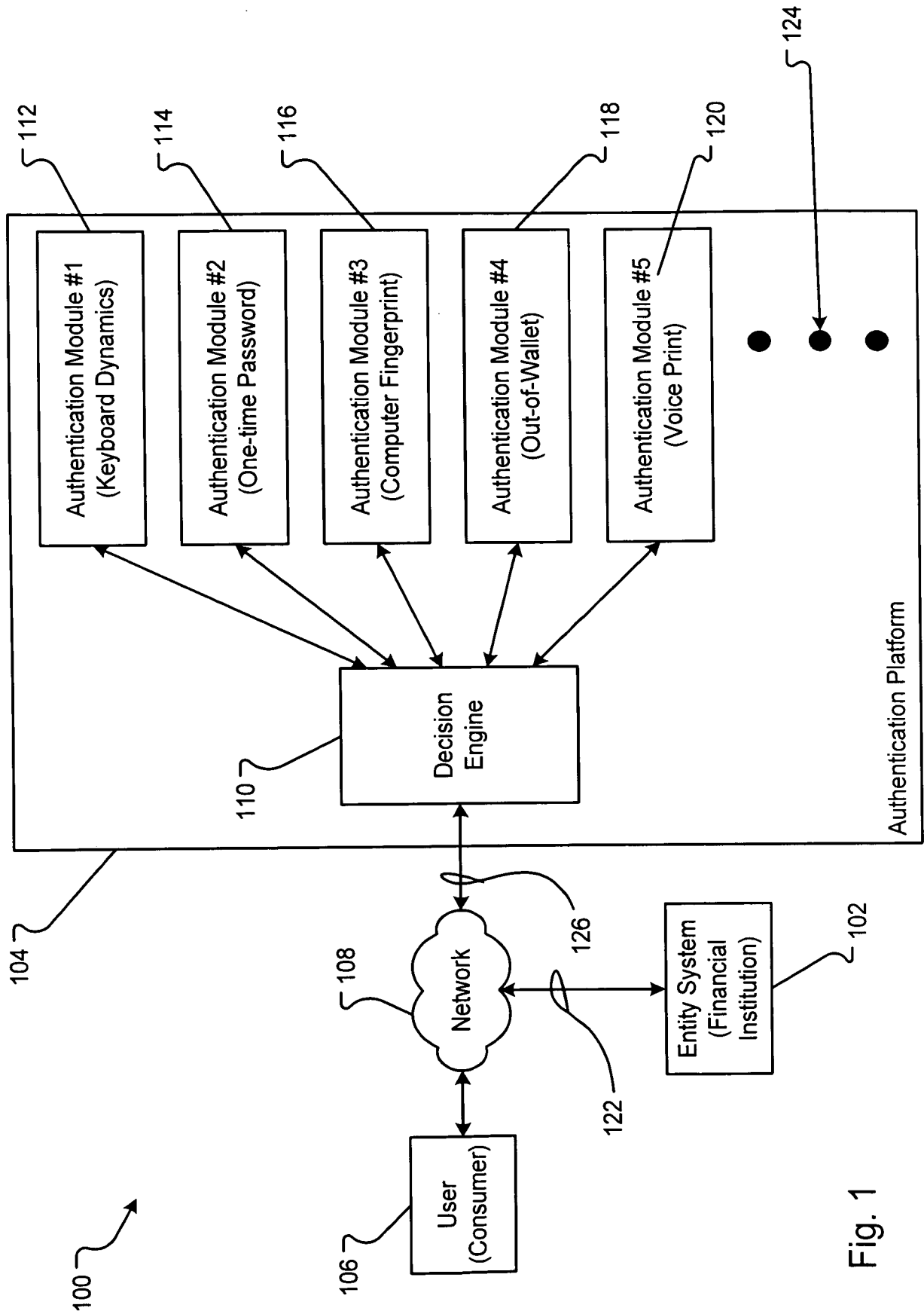


Fig. 1

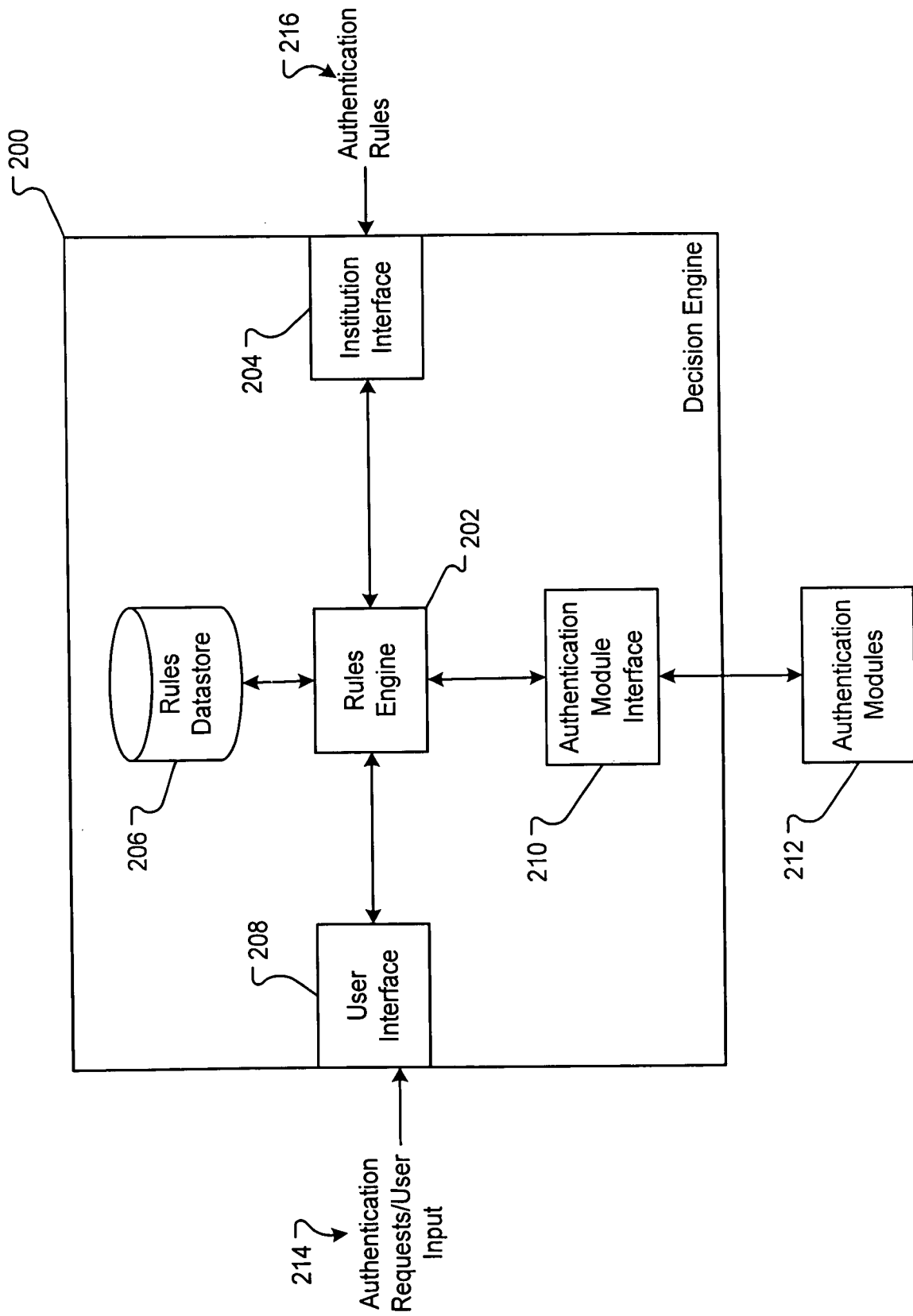


Fig. 2

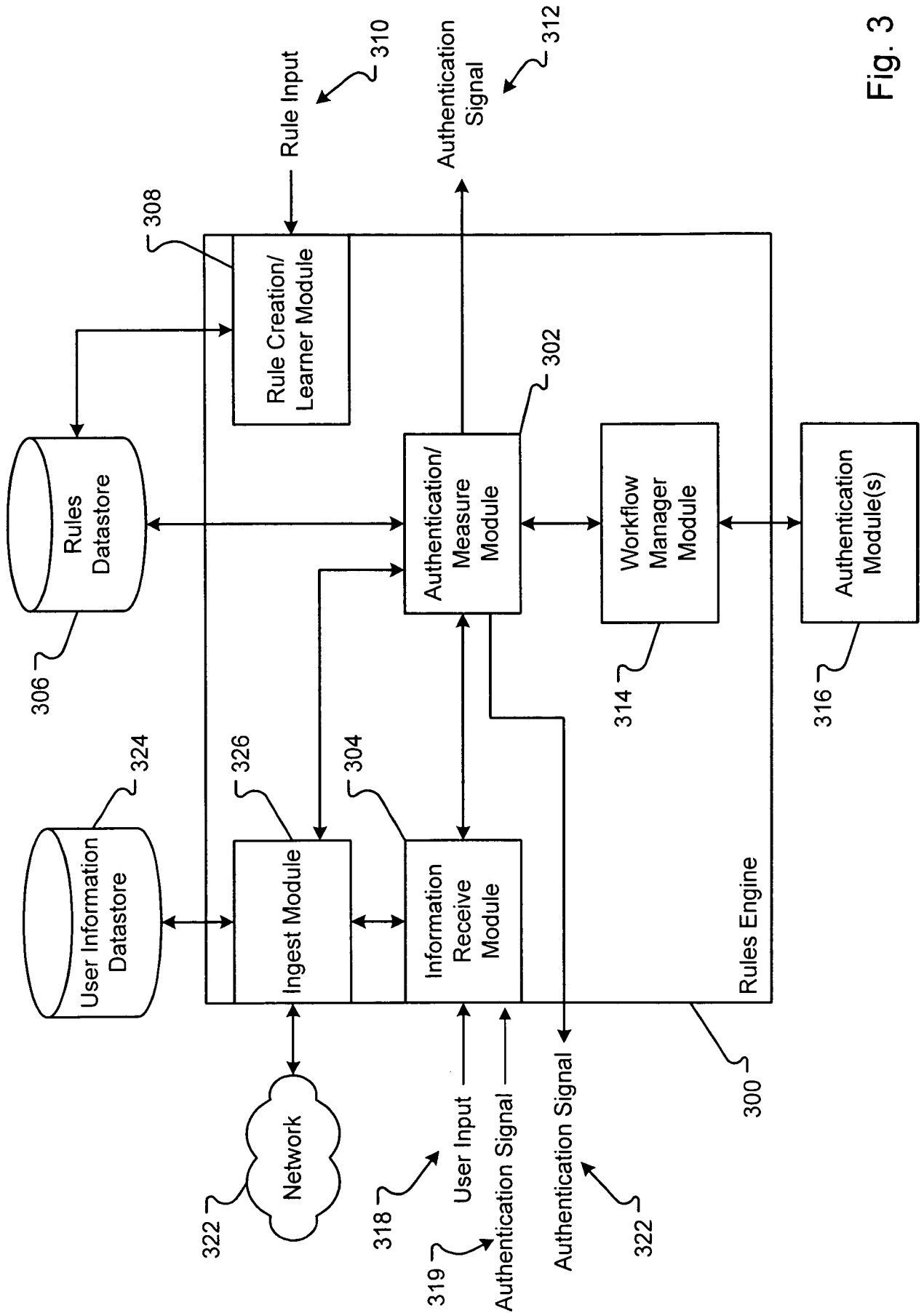


Fig. 3

Fig. 4A

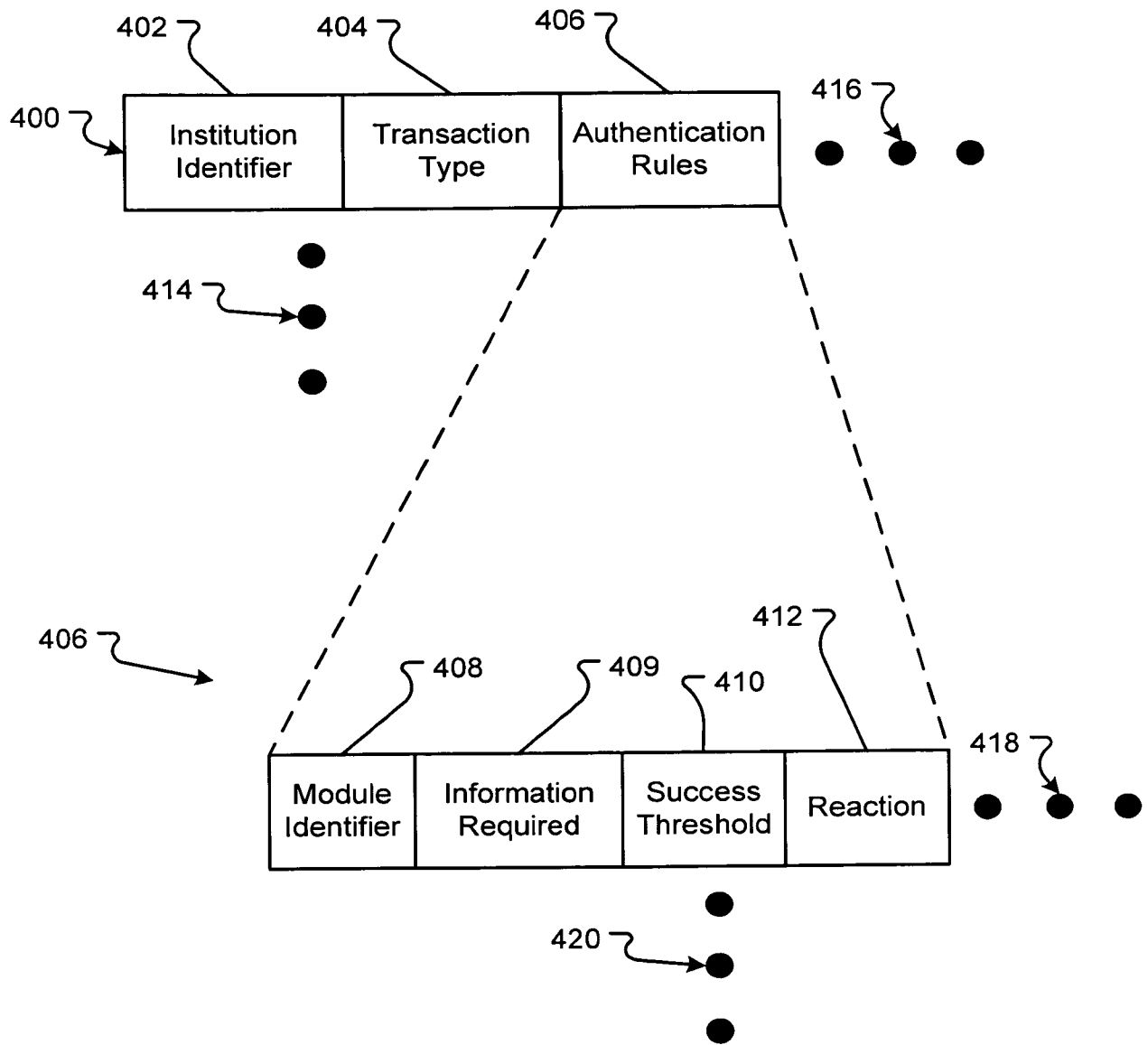


Fig. 4B

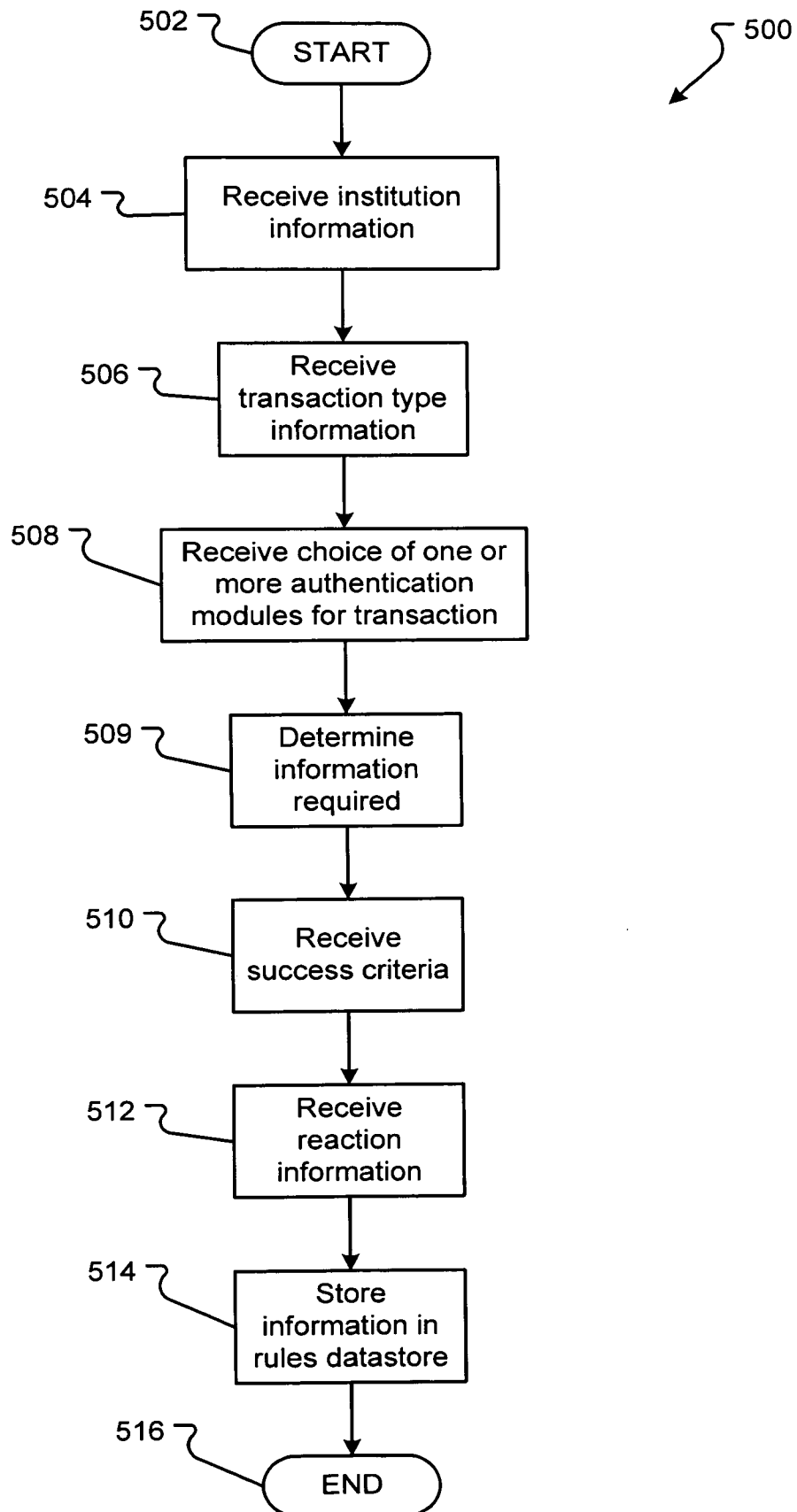


Fig. 5

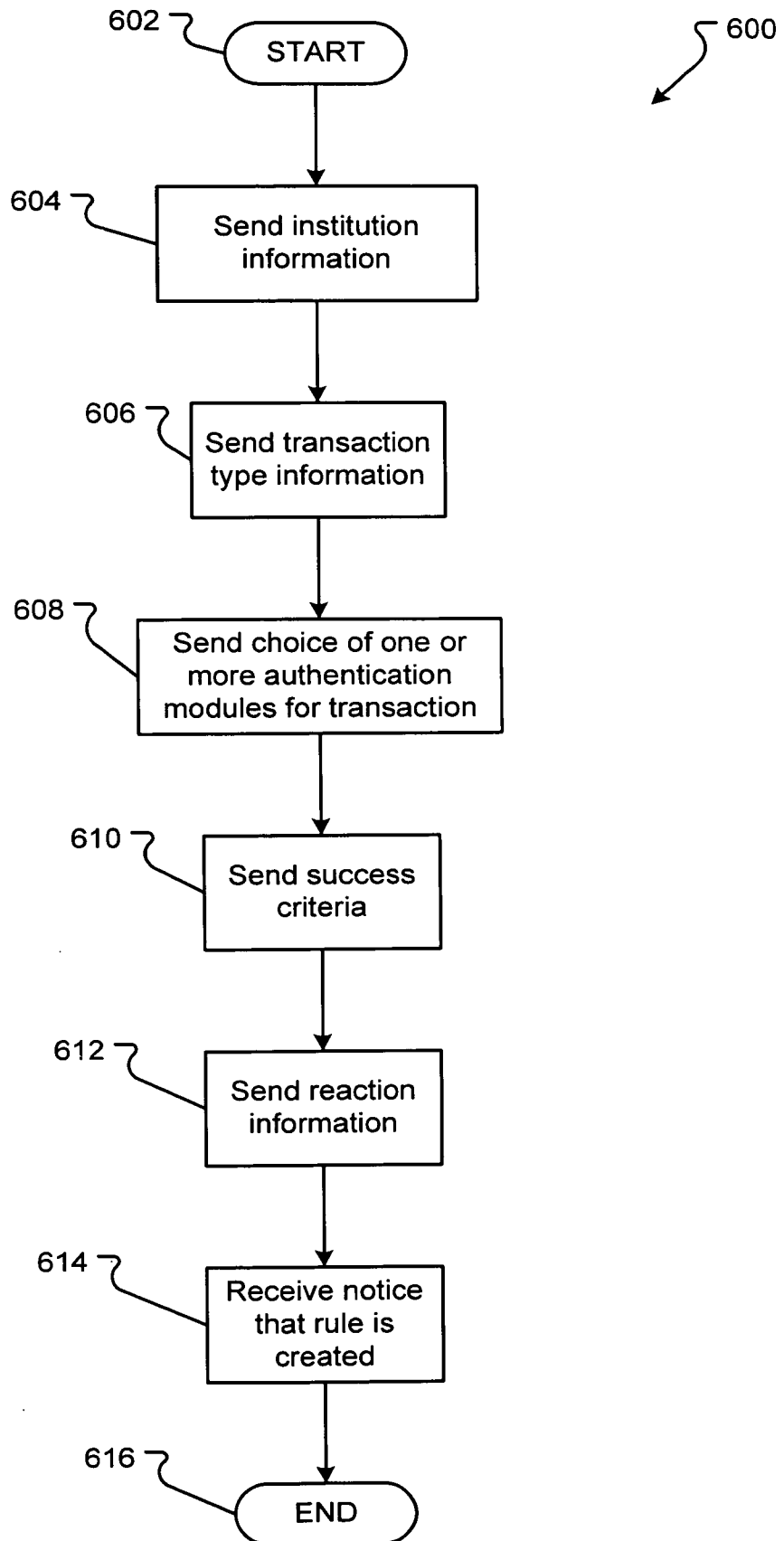


Fig. 6

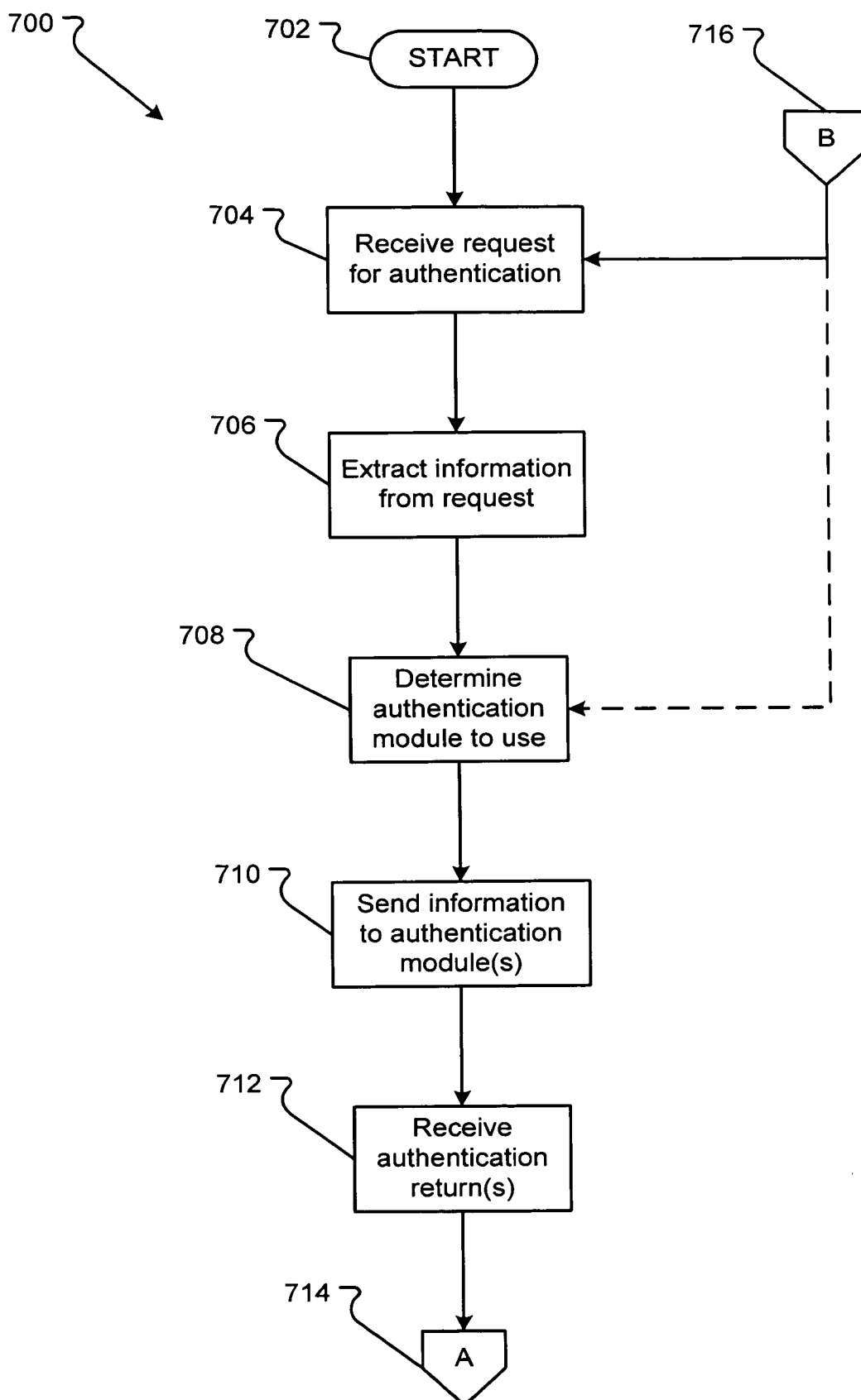


Fig. 7A

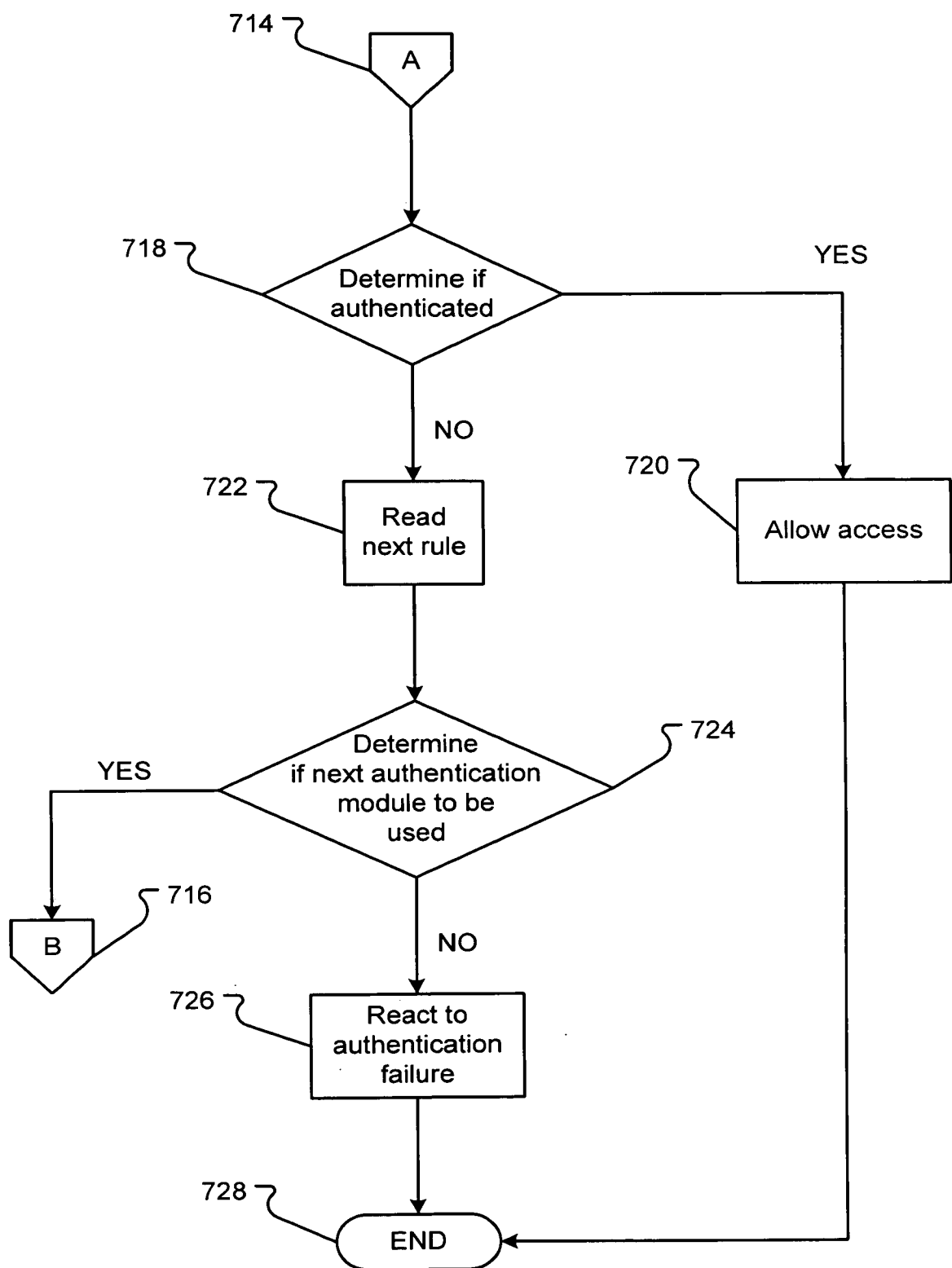


Fig. 7B

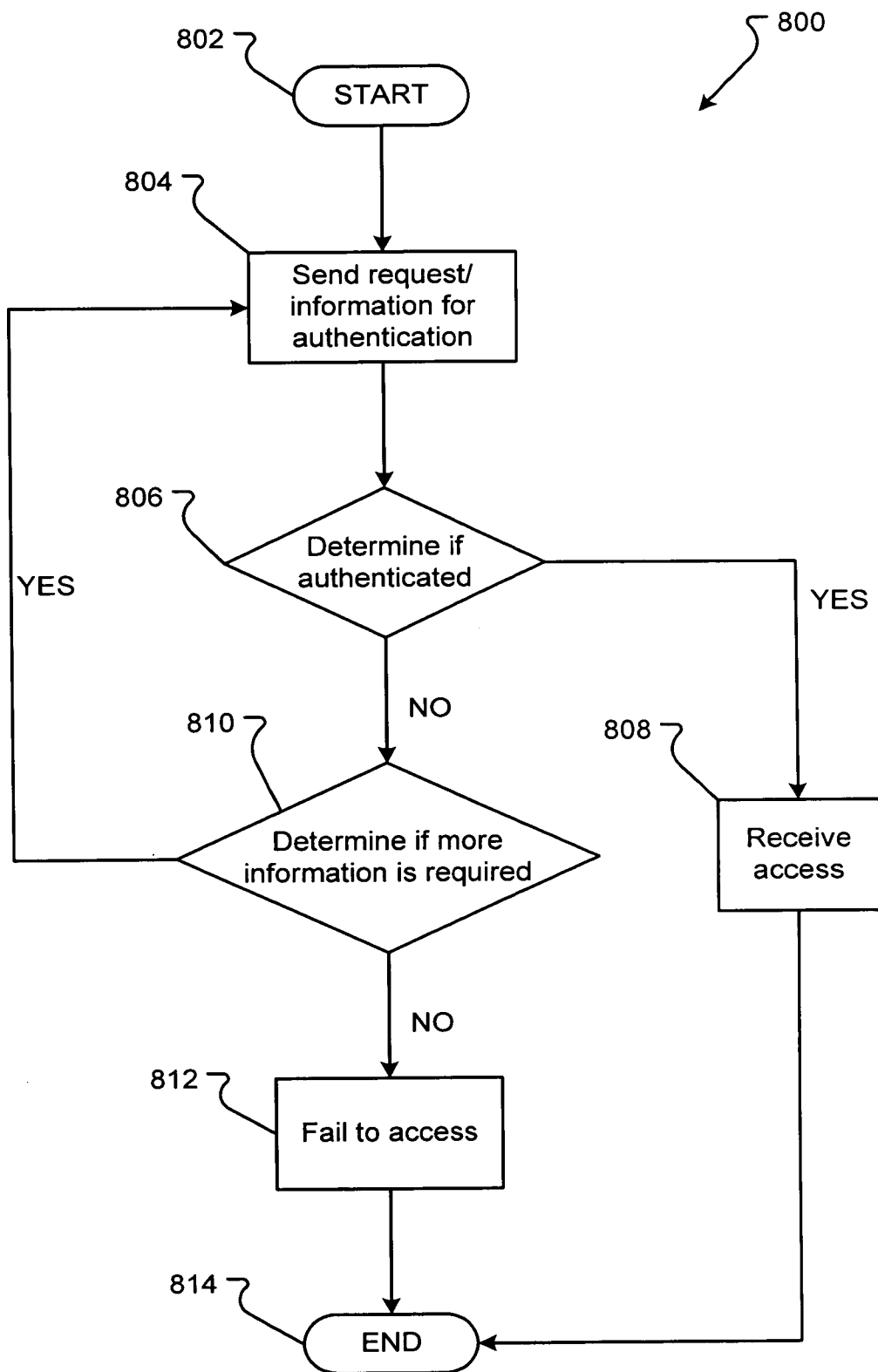


Fig. 8

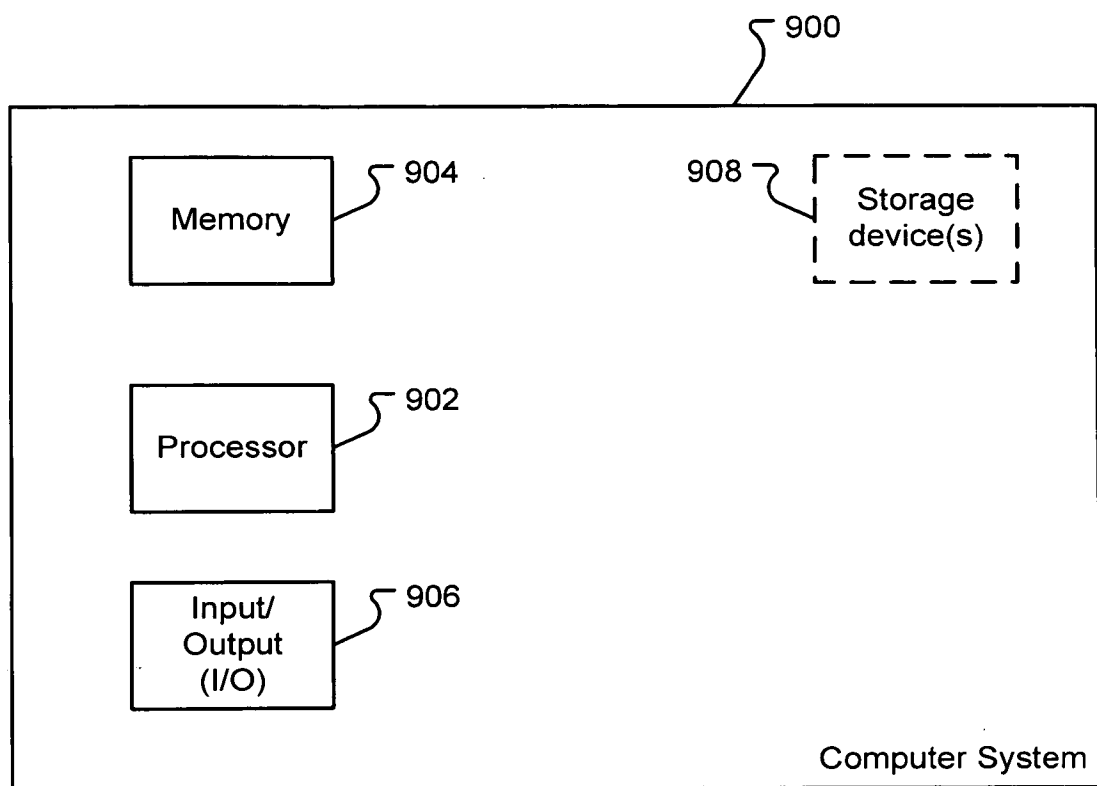


Fig. 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 08/13398

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 7/04 (2009.01)

USPC - 726/4

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)

USPC: 726/4

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 705/67, 76; 726/2, 3, 5, 28 (text search-see terms below)

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

PubWEST (USPT, PGPB, EPAB, JPAB); DialogPRO; Google

Authentication, authenticate, module, platform, user, entity, system, method, procedure, interact, request, inform, compare, receive, retrieve, request, extract, ingest, allow, permit, access, deny, success, fail, score, criteria, type, first, second, redundant, redundancy

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2003/0074580 A1 (KNOUSE et al.) 17 April 2003 (17.04.2003), FIG. 1, 2, 3, 15, 16, 17, 18, 19, 20, 21, 22, 23, 25, 26A, 28, and 29, para [0019]-[0020], [0094], [0096], [0104]-[0105], [0110], [0132], [0134]-[0140], [0143]-[0145], [0149]-[0151], [0153]-[0158], [0165], [0199], [0205], and [0209]	1-3, 11-13, 15-17, 20 --- 4-10, 14, 18-19
Y	US 2007/0180493 A1 (CROFT et al.) 02 August 2007 (02.08.2007), FIG. 2C, 3A, 3B, 7A, 7B, 8, 9, 10, 17, 85, and 86, para [0195]-[0196], [0198]-[0200], [0263]-[0266], [0270]-[0271], [0274], [0278], [0280], [0314], [0318]-[0319], [0323], [0630]-[0631], [0636], [0642], [0643], and [1176]-[1177]	4-10, 14
Y	US 2007/0245403 A1 (GINTER et al.) 18 October 2007 (18.10.2007), FIG. 1, 2, 3, 5A, 30, 31, 32, and 33, para [0390]-[0391], [0400]-[0409], [0411]-[0412], [0423], [1214]-[1223], [1231]-[1232], [1234], and [1241]	18-19

☐ Further documents are listed in the continuation of Box C.

* 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

22 January 2009 (22.01.2009)

Date of mailing of the international search report

03 FEB 2009

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774