US009489787B1

(12) **United States Patent**
Ives-Halperin et al.

(10) **Patent No.: US 9,489,787 B1**
(45) **Date of Patent: Nov. 8, 2016**

(54) **SHORT-RANGE DEVICE COMMUNICATIONS FOR SECURED RESOURCE ACCESS**

(71) Applicant: **Live Nation Entertainment, Inc.**, Beverly Hills, CA (US)

(72) Inventors: **Kenneth Ives-Halperin**, Los Angeles, CA (US); **Harry C. Evans, III**, Los Angeles, CA (US)

(73) Assignee: **Live Nation Entertainment, Inc.**, Beverly Hills, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 4 days.

(21) Appl. No.: **14/592,590**

(22) Filed: **Jan. 8, 2015**

Related U.S. Application Data

(60) Provisional application No. 62/095,597, filed on Dec. 22, 2014, provisional application No. 62/035,096, filed on Aug. 8, 2014.

(51) **Int. Cl.**
G07C 9/00 (2006.01)
H04W 4/00 (2009.01)

(52) **U.S. Cl.**
CPC ***G07C 9/00119*** (2013.01); ***H04W 4/008*** (2013.01)

(58) **Field of Classification Search**
CPC G07C 9/00023; G07C 9/00111; G07C 9/00134; G07C 9/0073; H04W 12/06; H04W 4/008; H04W 12/08; H04W 88/08
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,067,532	A	5/2000	Gebb	
7,412,042	B2	8/2008	Henry	
8,869,246	B2 *	10/2014	Kruger et al.	G06F 21/31 726/4
2003/0151493	A1 *	8/2003	Straumann et al.	340/5.25
2004/0153374	A1	8/2004	Nelson et al.	
2008/0007388	A1 *	1/2008	Au et al.	340/5.64
2009/0320538	A1 *	12/2009	Pellaton	70/278.1
2010/0063854	A1	3/2010	Purvis et al.	
2010/0082491	A1 *	4/2010	Rosenblatt et al.	705/65
2010/0201482	A1 *	8/2010	Robertson et al.	340/5.61
2010/0277276	A1 *	11/2010	Bayne et al.	340/5.21
2012/0296828	A1	11/2012	Bergdale et al.	
2012/0323691	A1 *	12/2012	McLaughlin et al.	705/14.58
2013/0017816	A1	1/2013	Talty et al.	
2013/0099891	A1 *	4/2013	Nandakumar	340/5.2
2014/0002236	A1 *	1/2014	Pineau et al.	340/5.6
2014/0375421	A1 *	12/2014	Morrison et al.	340/5.61

FOREIGN PATENT DOCUMENTS

WO	0251180	A1	6/2002

OTHER PUBLICATIONS

International Search Report and Written Opinion of PCT/US2015/042379 mailed Oct. 13, 2015, 14 pages.

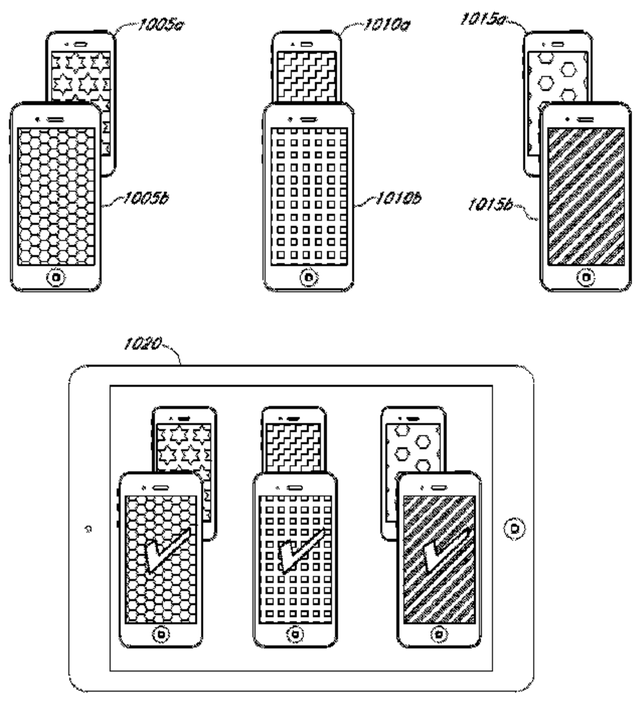
* cited by examiner

Primary Examiner — Benjamin C Lee
Assistant Examiner — Chico A Foxx
(74) *Attorney, Agent, or Firm* — Kilpatrick Townsend & Stockton LLP

(57) **ABSTRACT**

Communications over short-range connections are used to facilitate whether access to resources is to be granted. For example, upon device discovery of one of an electronic user device and an electronic client device by the other device over a Bluetooth Low Energy connection, an access-enabling code associated with a user device or account can be evaluated for validity and applicability with respect to one or more particular resource specifications. An image can be generated to reflect a result of the assessment, so as to enable an image analysis to be performed to decode the assessment result.

19 Claims, 11 Drawing Sheets



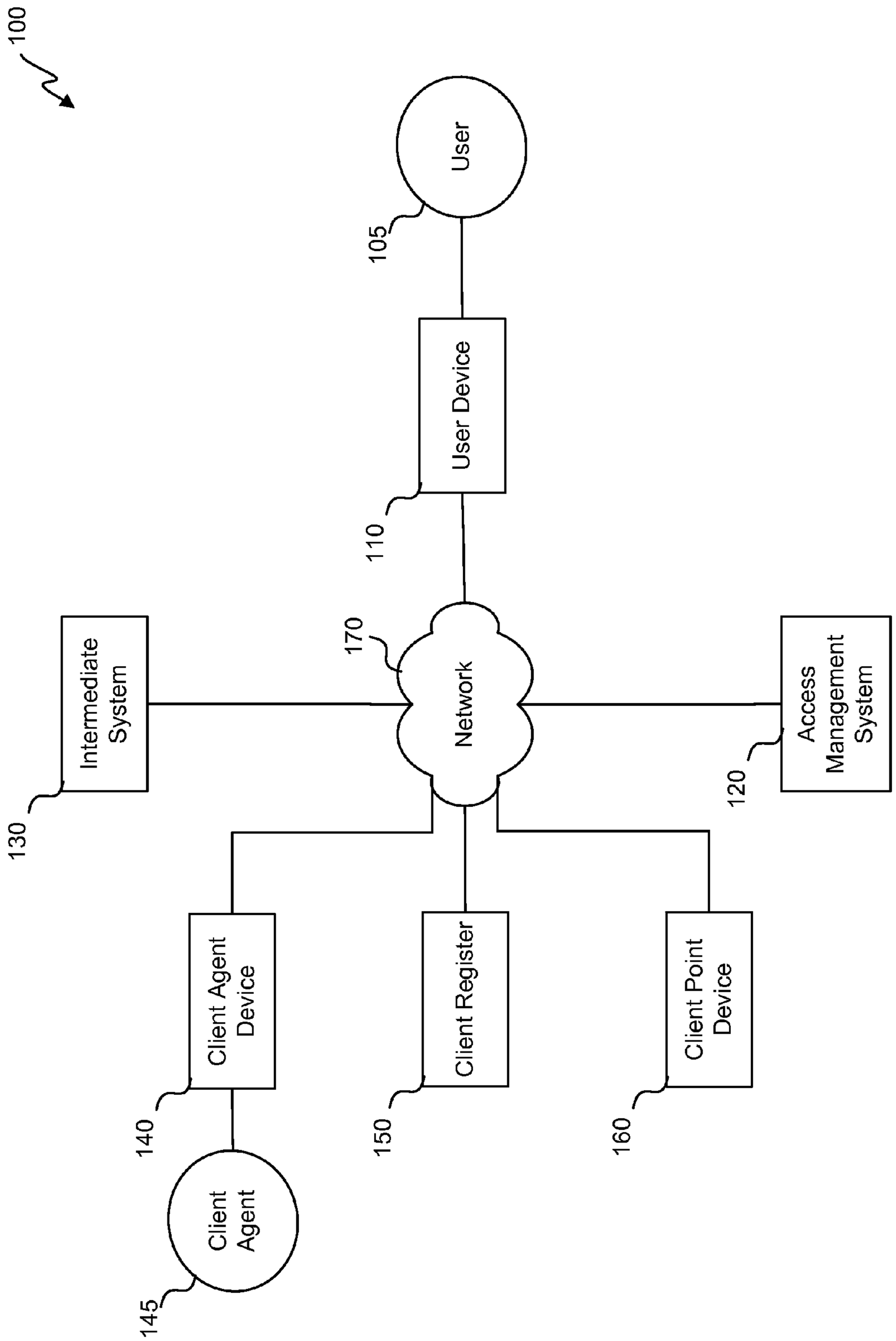

100
User
105
User Device
110
Intermediate System
130
Network
170
Access Management System
120
Client Agent Device
140
Client Register
150
Client Point Device
160
Client Agent
145

FIG. 1

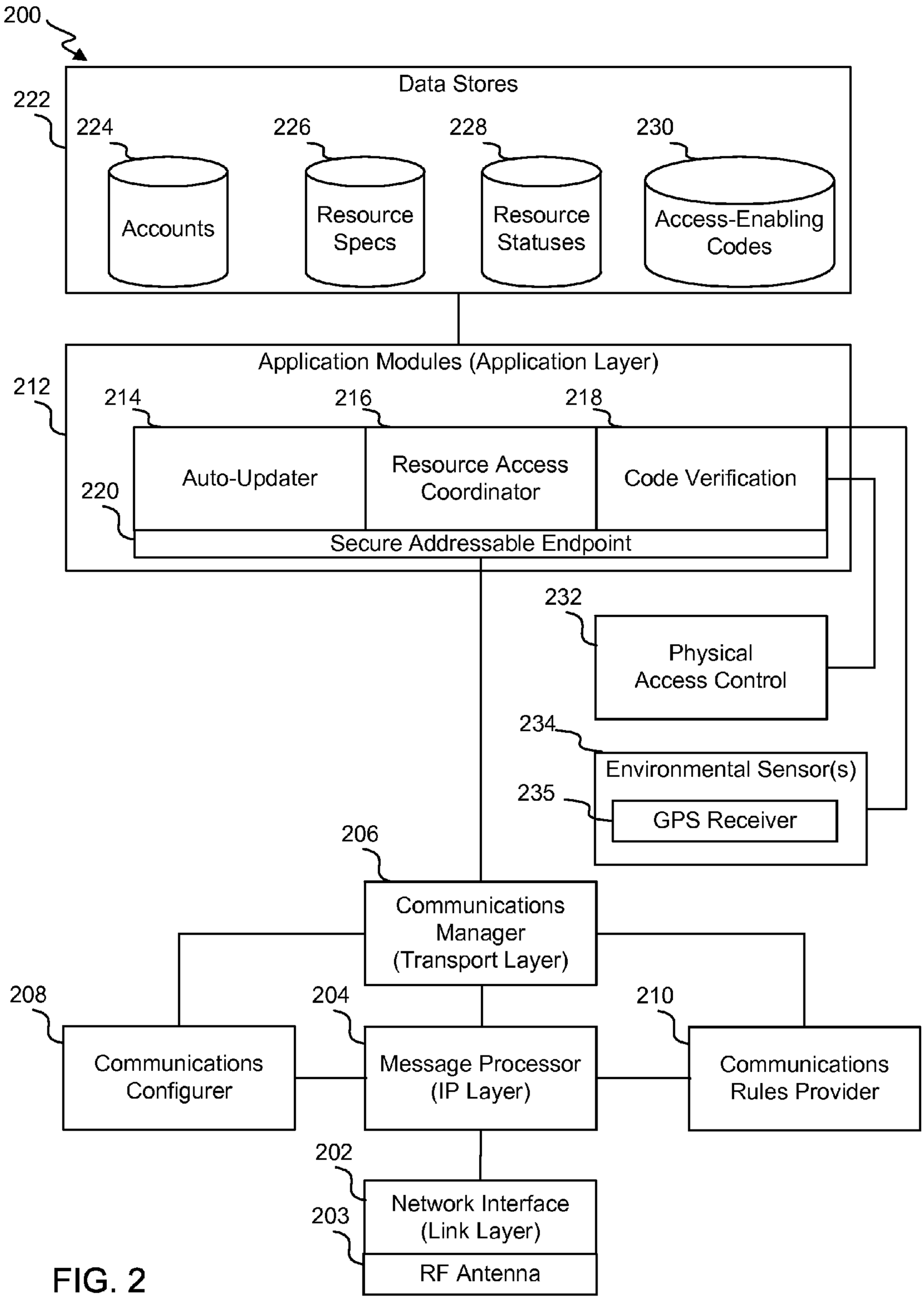

200
Data Stores
222
224
226
228
230
Accounts
Resource Specs
Resource Statuses
Access-Enabling Codes
Application Modules (Application Layer)
212
214
216
218
Auto-Updater
Resource Access Coordinator
Code Verification
220
Secure Addressable Endpoint
232
Physical Access Control
234
Environmental Sensor(s)
235
GPS Receiver
206
Communications Manager (Transport Layer)
208
204
210
Communications Configurer
Message Processor (IP Layer)
Communications Rules Provider
202
Network Interface (Link Layer)
203
RF Antenna

FIG. 2

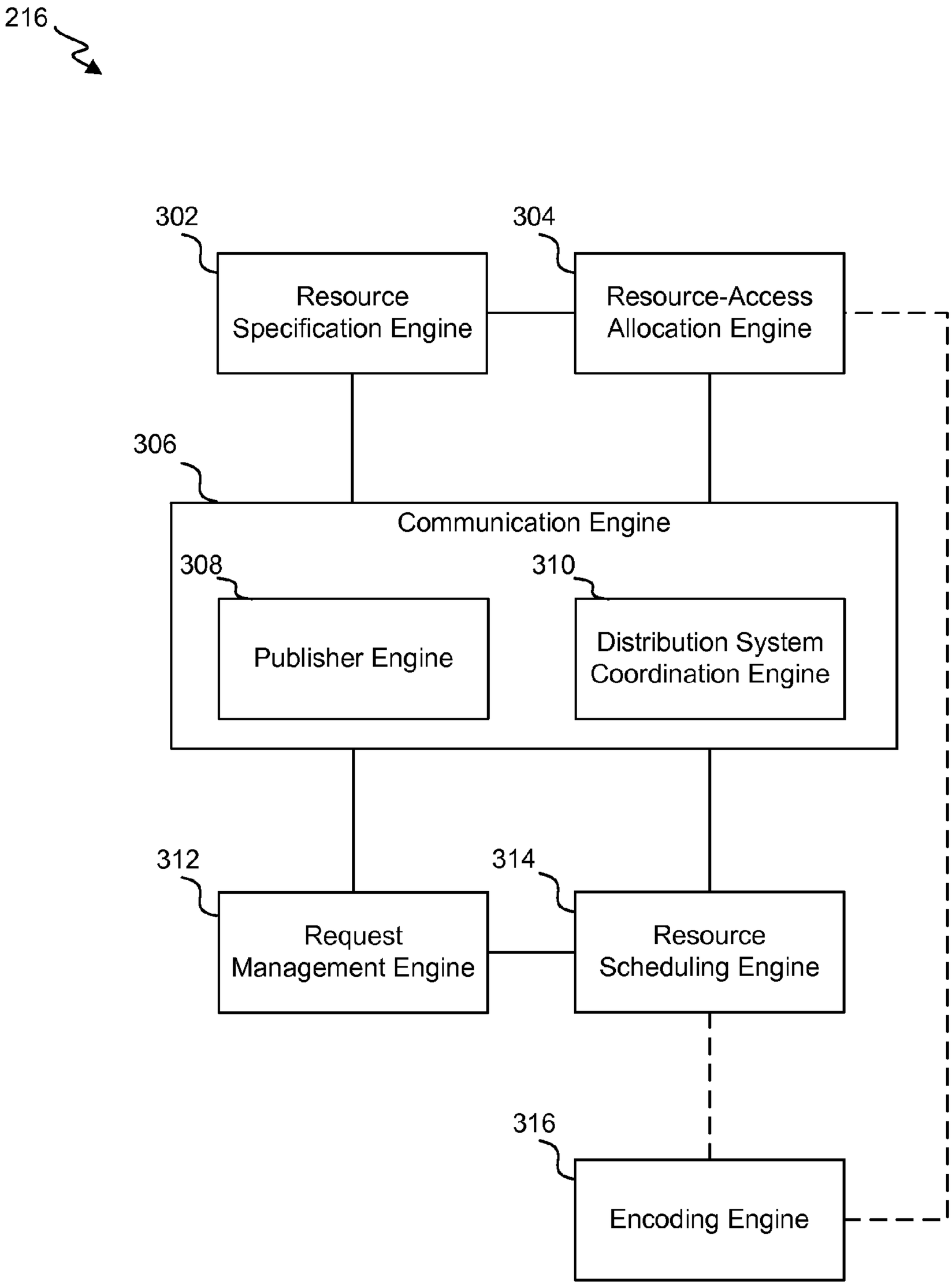

216
302
Resource Specification Engine
304
Resource-Access Allocation Engine
306
Communication Engine
308
Publisher Engine
310
Distribution System Coordination Engine
312
Request Management Engine
314
Resource Scheduling Engine
316
Encoding Engine

FIG. 3

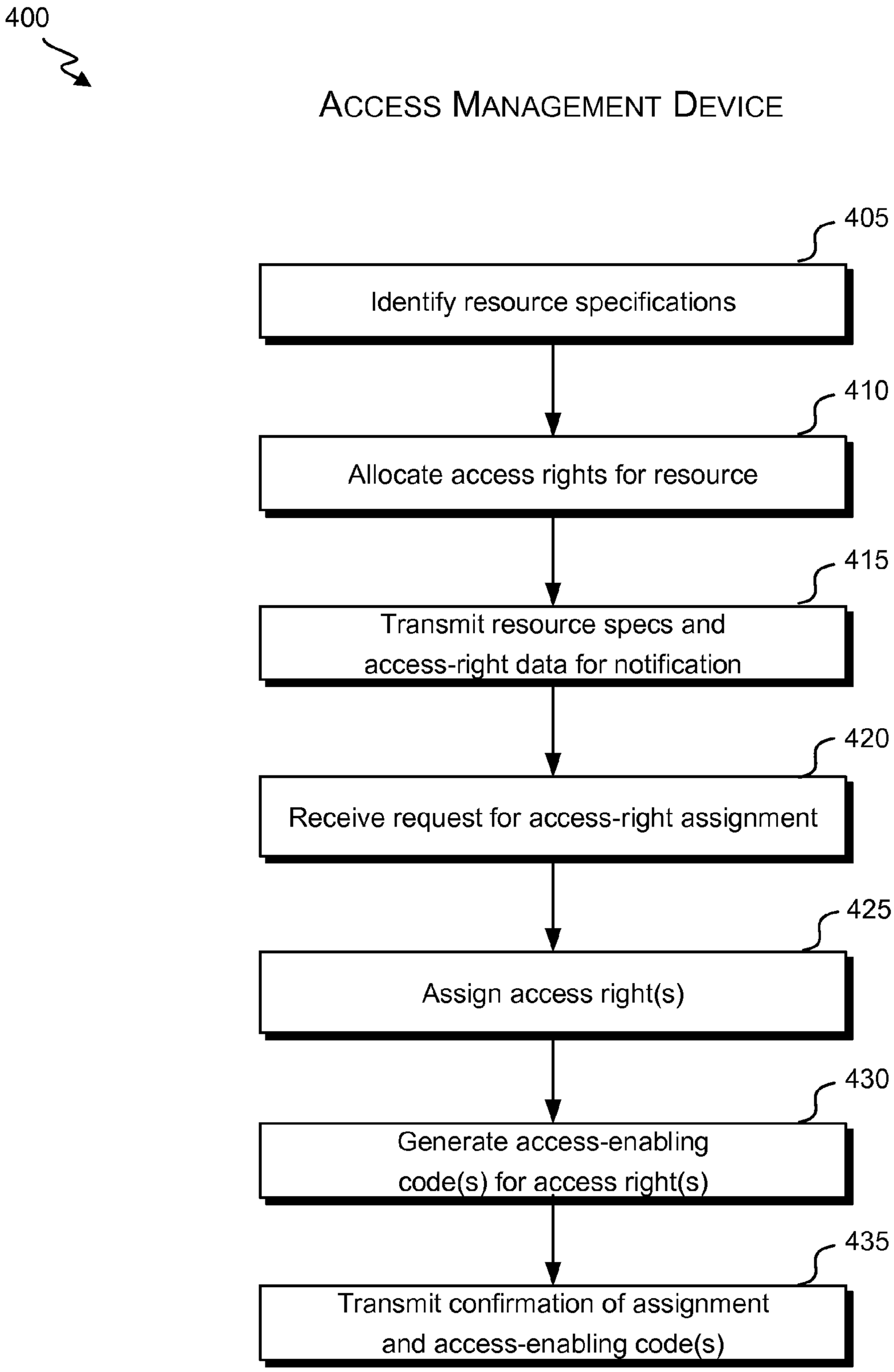

400
ACCESS MANAGEMENT DEVICE
405
Identify resource specifications
410
Allocate access rights for resource
415
Transmit resource specs and access-right data for notification
420
Receive request for access-right assignment
425
Assign access right(s)
430
Generate access-enabling code(s) for access right(s)
435
Transmit confirmation of assignment and access-enabling code(s)

FIG. 4

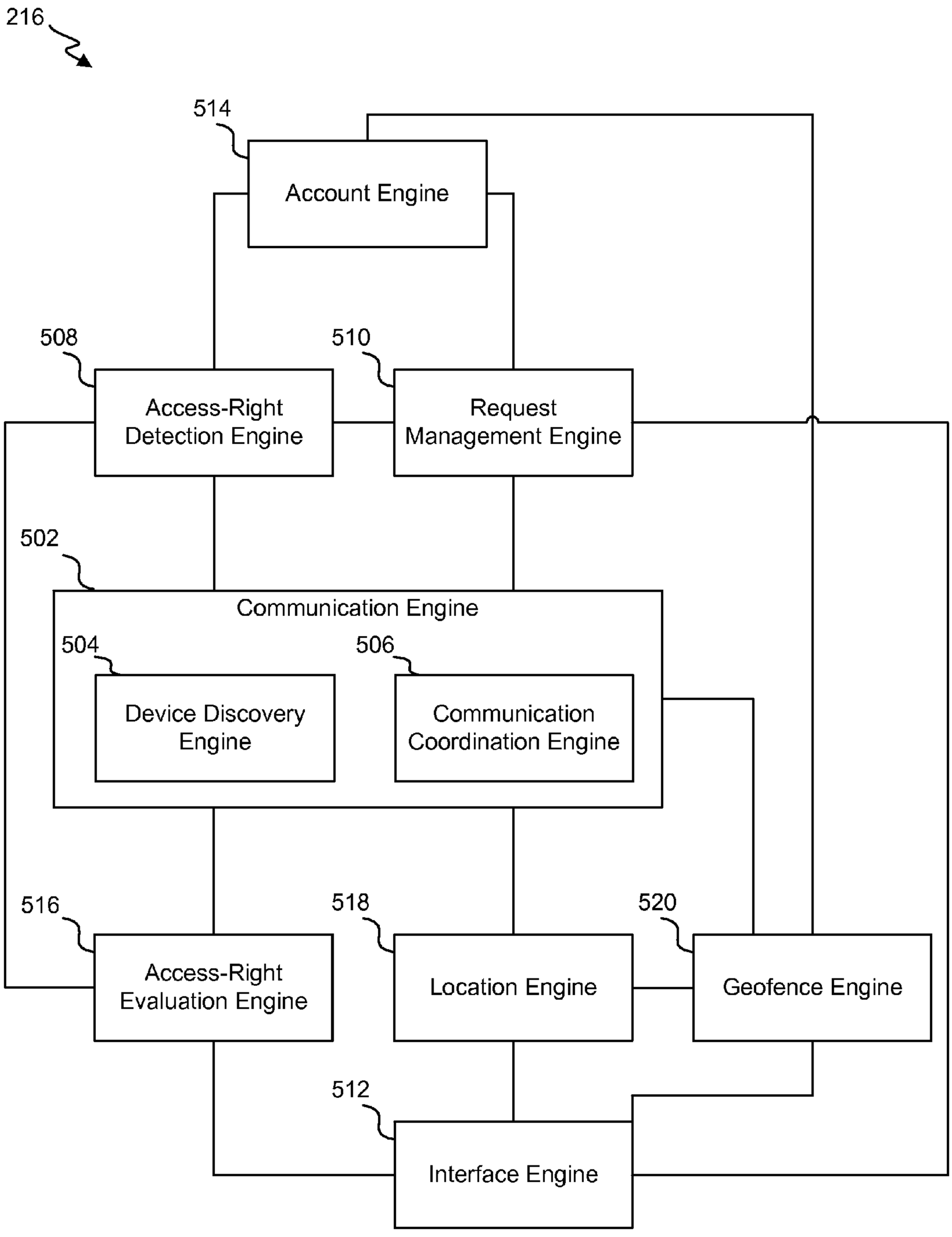

216
514
Account Engine
508
Access-Right Detection Engine
510
Request Management Engine
502
Communication Engine
504
Device Discovery Engine
506
Communication Coordination Engine
516
Access-Right Evaluation Engine
518
Location Engine
520
Geofence Engine
512
Interface Engine

FIG. 5

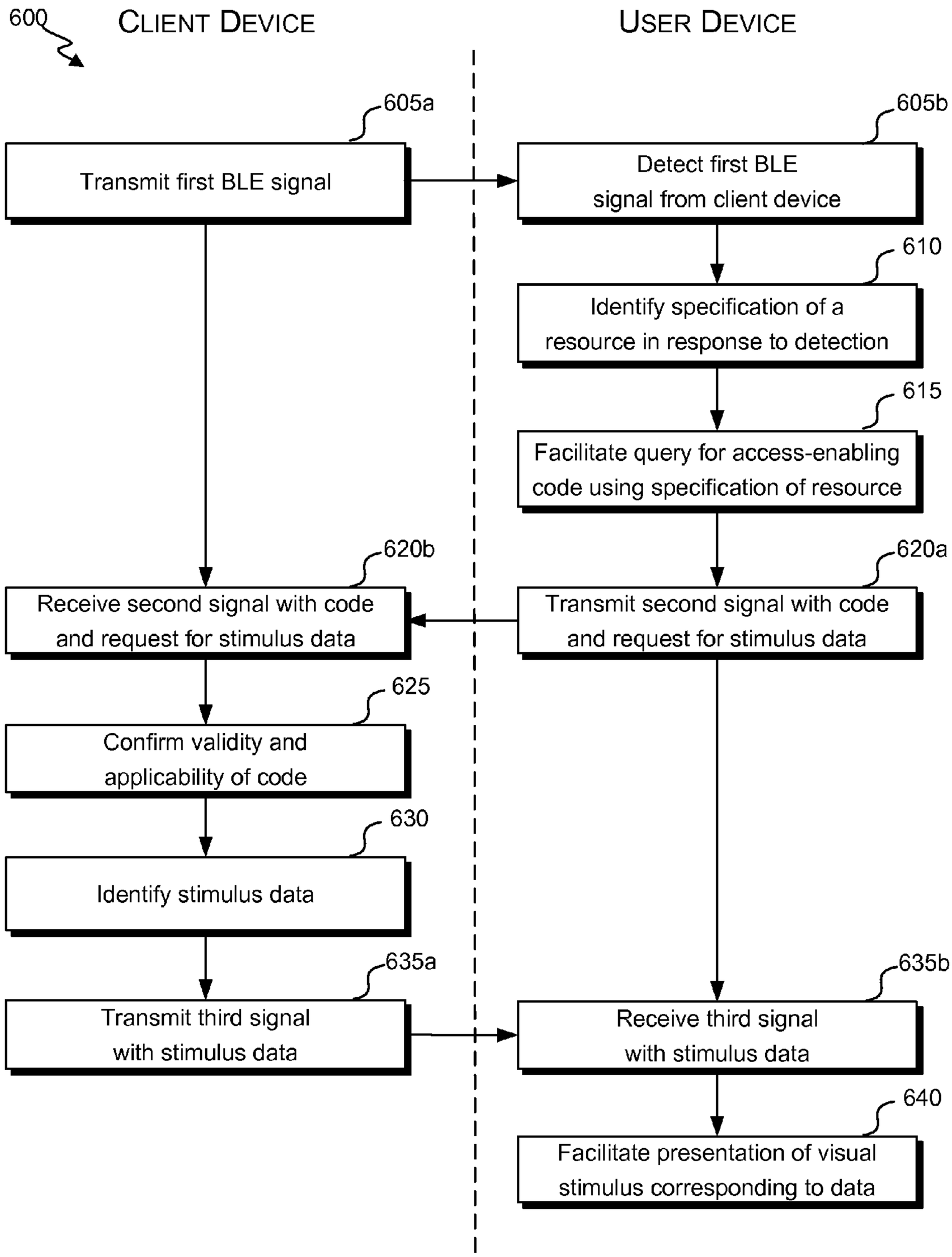

600
CLIENT DEVICE
USER DEVICE
605a
Transmit first BLE signal
605b
Detect first BLE signal from client device
610
Identify specification of a resource in response to detection
615
Facilitate query for access-enabling code using specification of resource
620b
Receive second signal with code and request for stimulus data
620a
Transmit second signal with code and request for stimulus data
625
Confirm validity and applicability of code
630
Identify stimulus data
635a
Transmit third signal with stimulus data
635b
Receive third signal with stimulus data
640
Facilitate presentation of visual stimulus corresponding to data

FIG. 6

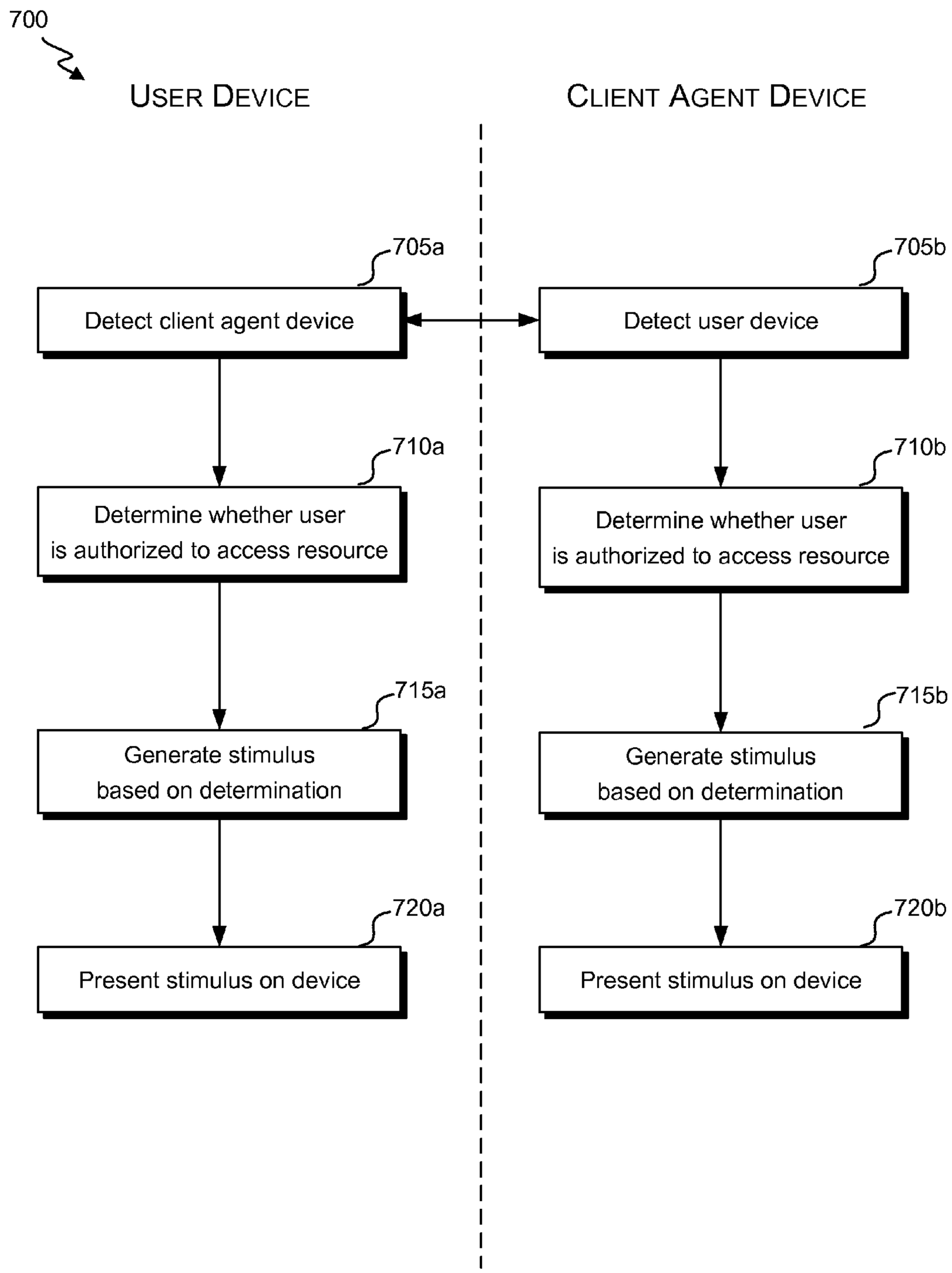

700
USER DEVICE
CLIENT AGENT DEVICE
705a
Detect client agent device
705b
Detect user device
710a
Determine whether user is authorized to access resource
710b
Determine whether user is authorized to access resource
715a
Generate stimulus based on determination
715b
Generate stimulus based on determination
720a
Present stimulus on device
720b
Present stimulus on device

FIG. 7

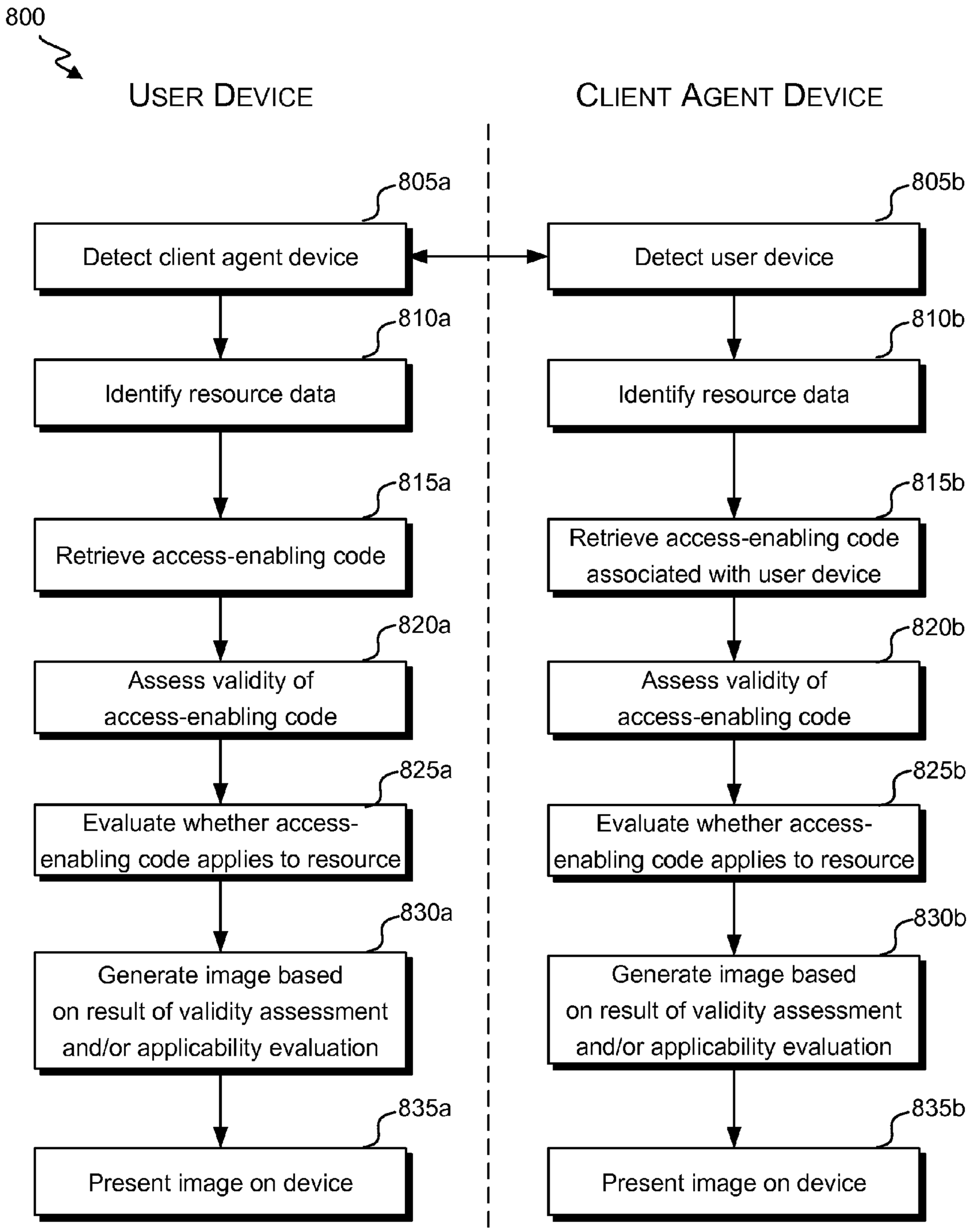

800
USER DEVICE
CLIENT AGENT DEVICE
805a
Detect client agent device
805b
Detect user device
810a
Identify resource data
810b
Identify resource data
815a
Retrieve access-enabling code
815b
Retrieve access-enabling code associated with user device
820a
Assess validity of access-enabling code
820b
Assess validity of access-enabling code
825a
Evaluate whether access-enabling code applies to resource
825b
Evaluate whether access-enabling code applies to resource
830a
Generate image based on result of validity assessment and/or applicability evaluation
830b
Generate image based on result of validity assessment and/or applicability evaluation
835a
Present image on device
835b
Present image on device

FIG. 8

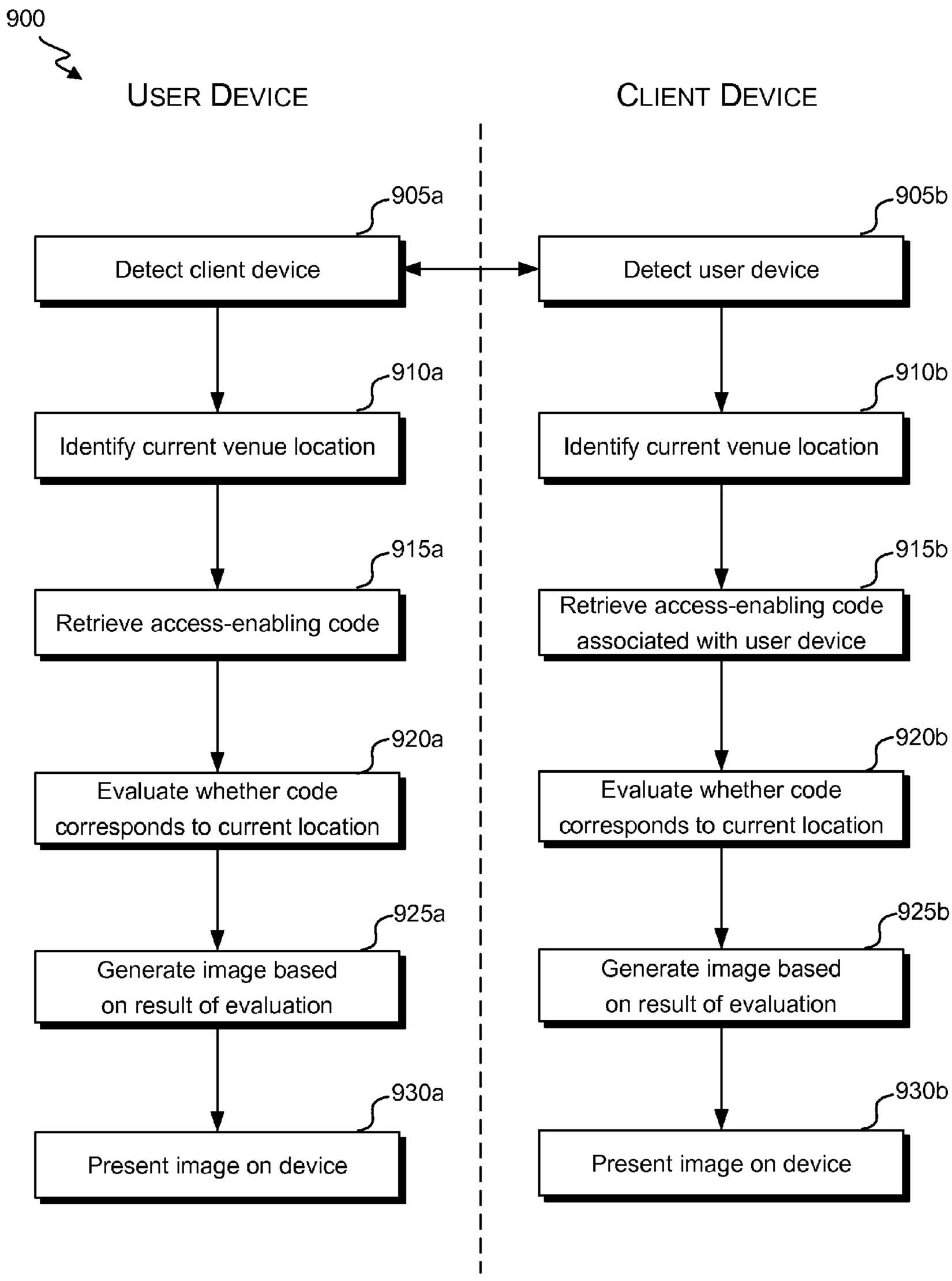

900
USER DEVICE
CLIENT DEVICE
905a
Detect client device
905b
Detect user device
910a
Identify current venue location
910b
Identify current venue location
915a
Retrieve access-enabling code
915b
Retrieve access-enabling code associated with user device
920a
Evaluate whether code corresponds to current location
920b
Evaluate whether code corresponds to current location
925a
Generate image based on result of evaluation
925b
Generate image based on result of evaluation
930a
Present image on device
930b
Present image on device

FIG. 9

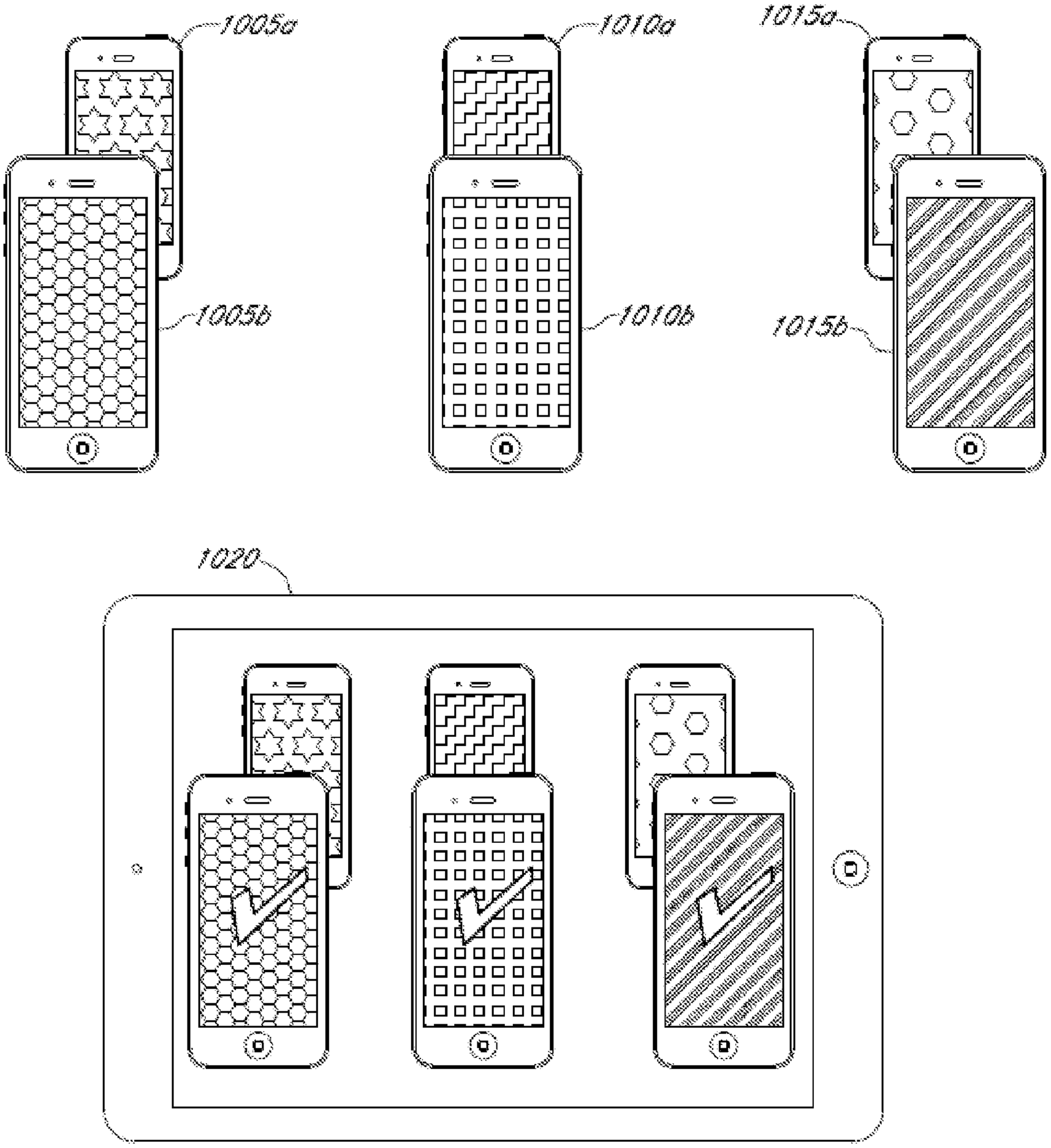


FIG. 10

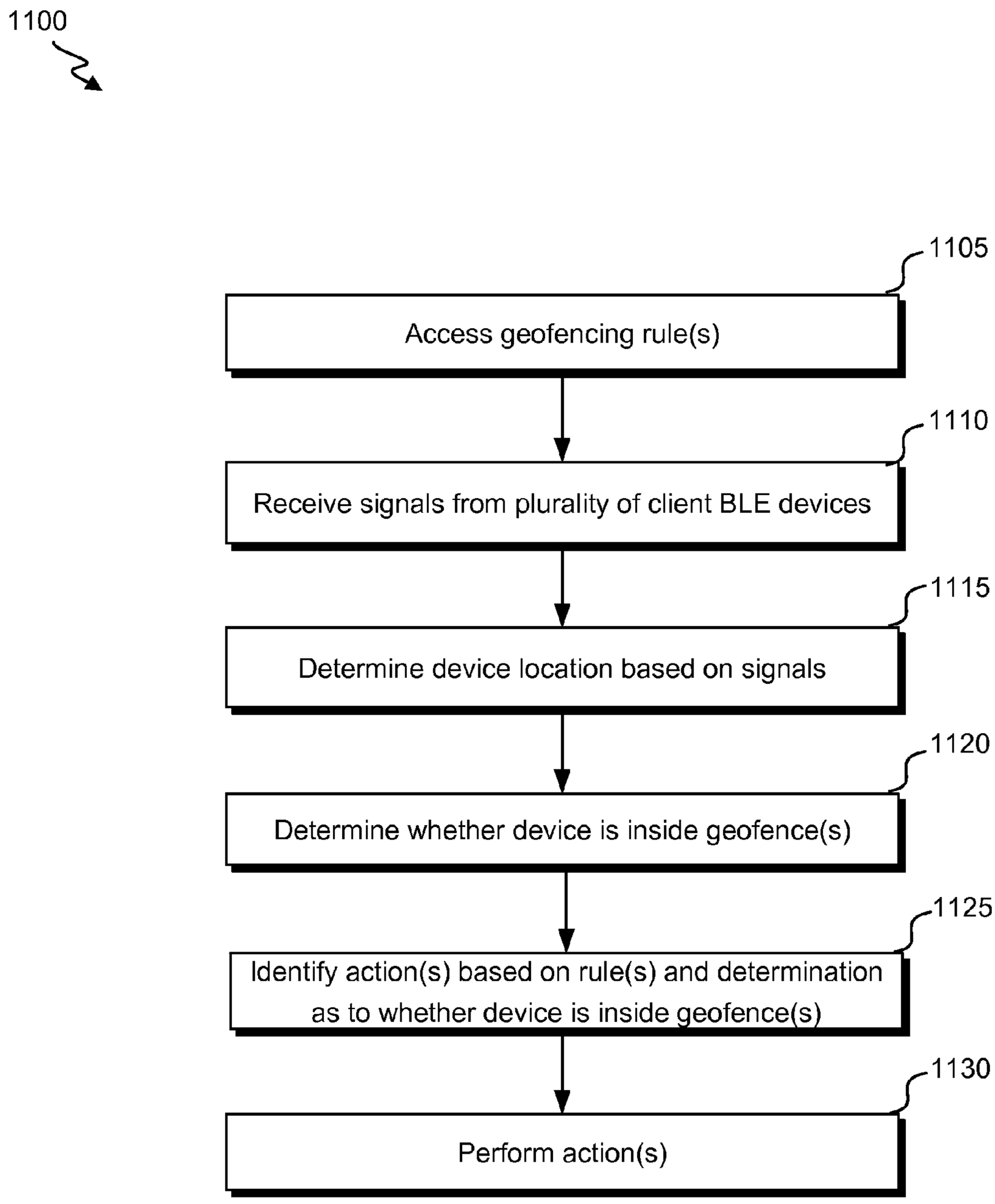

1100
1105
Access geofencing rule(s)
1110
Receive signals from plurality of client BLE devices
1115
Determine device location based on signals
1120
Determine whether device is inside geofence(s)
1125
Identify action(s) based on rule(s) and determination as to whether device is inside geofence(s)
1130
Perform action(s)

FIG. 11

SHORT-RANGE DEVICE COMMUNICATIONS FOR SECURED RESOURCE ACCESS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of and priority to U.S. Provisional Application No. 62/095,597, filed on Dec. 22, 2014 and to U.S. Provisional Application No. 62/035,096, filed on Aug. 8, 2014. Each of these applications is hereby incorporated by reference in its entirety for all purposes.

FIELD OF THE INVENTION

The present disclosure relates to short-range device communications and resource access, and in particular, to methods and systems for using short-range communications to facilitate validation analyses of resource access requests.

BACKGROUND

Electronic devices can communicate with each other using a variety of types of networks. For example, devices can communicate over a cellular network, WiFi or a local area network. One other category of connections is short-range connections. For example, devices can communicate using a Bluetooth or Bluetooth Low Energy connection. Short-range communications can facilitate communications with reduced reliance on external network connections and/or large power supplies. They can further facilitate discovery of nearby devices of interest without relying on previous information about such devices.

SUMMARY

In some embodiments, an electronic user device is provided. The electronic user device can include one or more transceivers for receiving signals. A transceiver of the one or more transceivers can be configured to receive signals transmitted over a short-range connection. The electronic user device can include a communication engine that detects a first wireless signal having been transmitted over a short-range connection by an electronic client device and having been received by the one or more transceivers at the electronic user device. The electronic user device can include an access-right detection engine that, in response to the detection of the first wireless signal having been transmitted over the short-range connection from the electronic client device, identifies a specification of a limited-access resource; and that facilitates a query of a data store using the specification of the limited-access resource for an access-enabling code. The electronic user device can include an access-right evaluation engine that generates a second wireless signal to be transmitted by the one or more transceivers. The second wireless signal can include a request for stimulus data; and the access-enabling code. The electronic user device can include an interface engine that detects that detects the stimulus data having been included in a third wireless signal received by the one or more transceivers; and that facilitates a presentation of a visual stimulus that corresponds to the stimulus data.

In some embodiments, a computer-implemented method for facilitating selective granting of resource access to authorized users based on short-range communication exchanges is provided. A first wireless signal transmitted over a short-range connection from an electronic client device can be detected at an electronic user device. In response to the detecting, a specification of a limited-access resource can be identified. A query of a data store using the specification of the limited-access resource for an access-enabling code can be facilitated. A second wireless signal that includes a request for stimulus data and the access-enabling code can be transmitted by the electronic user device. A third wireless signal can be received at the electronic user device that includes the stimulus data. A presentation of a visual stimulus that corresponds to the stimulus data can be facilitated.

In some embodiments, a computer-implemented method for facilitating selective granting of resource access to authorized users based on short-range communication exchanges can be provided. A first wireless signal can be received at an electronic client device from a first electronic user device. The first wireless signal can include a first request for stimulus data and a first access-enabling code. First stimulus data can be identified. A second wireless signal that includes the first stimulus data can be transmitted from the electronic client device and to the first electronic user device. A first presentation at the electronic client device of a first visual stimulus that corresponds to the first visual stimulus data can be facilitated. A third wireless signal can be received at the electronic client device and from a second electronic user device. The third wireless signal can include a second request for stimulus data and a second access-enabling code. Second stimulus data can be identified. A fourth wireless signal that includes the second stimulus data can be transmitted from the electronic client device and to the second electronic user device. A second presentation at the electronic client device of a second visual stimulus that corresponds to the second visual stimulus data can be facilitated.

BRIEF DESCRIPTION OF THE DRAWINGS

The present disclosure is described in conjunction with the appended figures:

FIG. **1** shows a block diagram of an embodiment of a resource access-facilitating interaction system;

FIG. **2** illustrates example components of a device;

FIG. **3** illustrates example components of resource access coordinator module that may operate, at least in part, at an access management system (e.g., access management system) according to an embodiment of the invention;

FIG. **4** illustrates a flowchart of an embodiment of a process for assigning access rights for resources;

FIG. **5** illustrates example components of resource access coordinator module that may operate, at least in part, at a user device system or client device according to an embodiment of the invention;

FIG. **6** illustrates a flowchart of an embodiment of a process for facilitating selective granting of resource access to authorized users based on short-range communication exchanges;

FIG. **7** illustrates a flowchart of an embodiment of a process for generating and presenting corresponding stimuli on user and client agent device;

FIG. **8** illustrates a flowchart of an embodiment of another process for generating and presenting complementary stimuli on user and client agent devices;

FIG. **9** illustrates a flowchart of an embodiment of another process for generating and presenting corresponding stimuli on user and client agent devices;

FIG. **10** illustrates stimuli that can be generated and presented using a technique described herein according to an embodiment of the invention;

FIG. **11** illustrates a flowchart of an embodiment of a process for using device communication to enforce geofencing rules.

In the appended figures, similar components and/or features can have the same reference label. Further, various components of the same type can 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 description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label.

DETAILED DESCRIPTION

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

Referring first to FIG. **1**, a block diagram of an embodiment of a resource access-facilitating interaction system **100** is shown. A user device **110** (which can be operated by a user **105**) can communicate with an access management system **120** directly or via another system (e.g., via an intermediate system **130**). User device **110** can also communicate with one or more client devices, such as a client agent device **140** operated by a client agent **145**, a client register **150** or a client point device **160**. Each inter-system communication can occur over one or more networks **170** and can facilitate transmission of a variety of types of data. It will be understood that, although only one of various systems, devices, entities and network are shown, interaction system **100** can be extended to include multiple of any given system(s), device(s), entity(ies), and/or networks.

Access management system **120** can be configured to manage a dynamic set of access rights to one or more resources. More specifically, access management system **120** can track which resources are to be made available to users, specifications of the resources and times at which they will be available. Access management system **120** can also allocate access rights for resources and facilitate transmissions of notifications of the available rights to a set of user devices. For example, access management system **120** can alert users of the availability via a website, app page or email. As another example, access management system can transmit data about access rights and resources to one or more intermediate systems **130**, which can facilitate distribution of access-right availability and processing of requests for such rights.

Notifications of available access rights can be accompanied by options to request that one or more access rights be assigned to a user. Therefore, user **105** can provide input to user device **110** via an interface to request such assignment and provide other pertinent information. Intermediate system **130** and/or access management system **120** can process the request to ensure that the requested access right(s) remain available and that all required information has been received and, in some instances, verified. Thereafter, access management system **120** can assign one or more access rights to the user, e.g., matching the access rights requested by the user.

Assigning an access right can include, for example, associating an identifier of the right with an identifier of a user, changing a status of the right from available to assigned, facilitating a cease in notifications that the access right is available, generating an access-enabling code to use such that the corresponding access will be permitted and/or generating a notification to be received at user device **110** confirming the assignment and/or including data required for corresponding access to be permitted.

In some instances, a resource is at least partly controlled, offered or availed by a client. The resource may be offered at a particular location or structure, and a variety of client devices may be present at the location so as to facilitate usage of an access right and other offerings. Exemplary client devices can include client agent device **140**, which can be one operated by a client agent (e.g., a human client agent), a client register **150** (e.g., which can operate independently of an agent and/or can be connected to or include a device that, while in a locked mode, can impede resource access, such as a turnstile) and client point device **160** (e.g., which can operate independently of an agent and/or can be positioned at or around the resource-associated location. For example, in some instances client agent device **140** can be operated by an agent at a location for a resource that is an event ("event resource") taking place at the location. In this example, client agent device **140** is used by an agent that is manning an entrance to the location (e.g., which can include, for example, a location of a structure or a geographic region) or a part thereof; client register **150** can be or can be connected to a turnstile, gate or lockable door that is positioned along a perimeter or entrance to a resource-associated location or part thereof; and client point device **160** can be an electronic device positioned at or within a resource-associated location.

In some instances, user device **105** performs particular functions upon detecting a client device and/or the contrary. For example, user device **110** may locally retrieve or request (e.g., from an external source) an access-enabling code. The access-enabling code can be transmitted to the client device or a remote server (e.g., a server hosting access management system **120**) for evaluation and/or can be locally evaluated. The evaluation can include, for example, confirming that the access-enabling code has a particular characteristic or format (e.g., generally or one characteristic corresponding to a particular resource or type of access), matches one in an access-enabling code data store and/or has not been previously redeemed. A result of the evaluation can be locally displayed at an evaluating device, can control a device component (e.g., a physical access control module), and/or can be transmitted to another device, such as user device **110**.

In some instances, user **105** can use multiple user devices **110** to perform various operations (e.g., using one device to request an access right and another to interact with client devices). Some instances of user device **110**, access management system **120**, intermediate system **130**, client agent device **140**, client register **150** and/or client point device **160** can include a portable electronic device (e.g., a smart phone, tablet, laptop computer or smart wearable device) or a non-portable electronic device (e.g., one or more desktop computers, servers and/or processors).

In exemplary embodiments, access rights can be represented in data maintained at a client device or at access management system **120**. For example, a database or data

store include a list of identifiers for each user or user device having an assigned access right for a resource or associating an identifier for each user or user device with an identifier of a particular access right. In some instances, an indicia can be transmitted to a user device that indicates that an access right is availed. In various instances, it may permitted or prohibited for the indicia to be transferred. The indicia may be provided as part of an electronic or physical object (e.g., a ticket) or independently. The indicia may include an access-enabling code.

In some instances, access management system **120** communicates with one or more intermediate systems **130**, each of which may be controlled by a different entity as compared to an entity controlling access management system **120**. For example, access management system **120** may assign access rights to an intermediate systems **130**. Intermediate system **130** can then collect data pertaining to the assigned access rights and/or a corresponding event, can format and/or edit the data, generate a notification of availability of the access rights that includes the formatted and/or edited data and facilitate presentation of the notification at a user device **110**. When intermediate system **130** receives a communication from a user device **110** indicative of an access-right request, intermediate system **130** can facilitate assignment (or reassignment) of an access right to the user (e.g., by transmitting relevant information to access management system **120** identifying the user and/or user device and/or by transmitting relevant information to user device **110** pertaining to the access right).

A resource can include one managed or provided by a client, such as a performing entity or an entity operating a venue. A user device **110** can transmit data corresponding to the access right (e.g., an access-enabling code) to a client device upon, for example, detecting the client device, detecting that a location of the user device **110** is within a prescribed geographical region, or detecting particular input. The receiving client device may include, for example, a client agent device **145** operated at an entrance of a defined geographical location or a client register **150** that includes or is attached to a locking turnstile. The client device can then analyze the code to confirm its validity and applicability for a particular resource and/or access type, and admittance to the event can be accordingly permitted. For example, a turnstile may change from a locked to an unlocked mode upon confirmation of the code's validity and applicability.

Each of the depicted devices and/or systems may include a software agent or application ("app") that, when executed, performs one or more actions as described herein. In some instances, a software agent or app on one device is, at least in part, complementary to a software agent or app on another device (e.g., such that a software agent or app on user device **110** is, at least in part, complementary to at least part of one on access management system **120** and/or a client device; and/or such that a software agent or app on intermediate system **130** is, at least in part, complementary to at least part of one on access management system **120**).

In some instances, a network in the one or more networks **170** can include an open network, such as the Internet, personal area network, local area network (LAN), campus area network (CAN), metropolitan area network (MAN), wide area network (WAN), wireless local area network (WLAN), a private network, such as an intranet, extranet, or other backbone. In some instances, a network in the one or more networks **170** includes a short-range communication channel, such as Bluetooth or Bluetooth Low Energy channel. Communicating using a short-range communication such as BLE channel can provide advantages such as consuming less power, being able to communicate across moderate distances, being able to detect levels of proximity, achieving high-level security based on encryption and short ranges, and not requiring pairing for inter-device communications.

In one embodiment, communications between two or more systems and/or devices can be achieved by a secure communications protocol, such as secure sockets layer (SSL), transport layer security (TLS). In addition, data and/or transactional details may be encrypted based on any convenient, known, or to be developed manner, such as, but not limited to, DES, Triple DES, RSA, Blowfish, Advanced Encryption Standard (AES), CAST-128, CAST-256, Decorrelated Fast Cipher (DFC), Tiny Encryption Algorithm (TEA), eXtended TEA (XTEA), Corrected Block TEA (XXTEA), and/or RC5, etc.

It will be appreciated that, while a variety of devices and systems are shown in FIG. **1**, in some instances, resource access-facilitating interaction system **100** can include fewer devices and/or systems. Further, some systems and/or devices can be combined. For example, a client agent device **140** may also serve as an access management system **120** or intermediate system **130** so as to as to facilitate assignment of access rights.

As described in further detail herein, an interaction between user device **110** and a client device (e.g., client agent device **140**, client register **150** or client point device **160**) can facilitate, for example, verification that user **105** has a valid and applicable access right, obtaining an assignment of an access right, and/or obtaining an assignment of an upgraded access right.

FIG. **2** illustrates example components of a device **200**, such as a client device (e.g., client agent device **140**, client register **150** and/or client point device **160**), an intermediate system (e.g., intermediate system **130**) and/or an access management system (e.g., access management system **120**) according to an embodiment of the invention.

The components can include one or more modules that can be installed on device **200**. Modules can include some or all of the following: a network interface module **202** (which can operate in a link layer of a protocol stack), a message processor module **204** (which can operate in an IP layer of a protocol stack), a communications manager module **206** (which can operate in a transport layer of a protocol stack), a communications configure module **208** (which can operate in a transport and/or IP layer in a protocol stack), a communications rules provider module **210** (which can operate in a transport and/or IP layer in a protocol stack), application modules **212** (which can operate in an application layer of a protocol stack), a physical access control module **232** and one or more environmental sensors **234**.

Network interface module **202** receives and transmits messages via one or more hardware components that provide a link-layer interconnect. The hardware component(s) can include, for example, RF antenna **203** or a port (e.g., Ethernet port) and supporting circuitry. In some embodiments, network interface module **202** can be configured to support wireless communication, e.g., using Wi Fi (IEEE 802.11 family standards), Bluetooth® (a family of standards promulgated by Bluetooth SIG, Inc.), BLE, or near-field communication (implementing the ISO/IEC 18092 standards or the like).

RF antenna **203** can be configured to convert electric signals into radio and/or magnetic signals (e.g., to radio waves) to transmit to another device and/or to receive radio and/or magnetic signals and convert them to electric signals. RF antenna **203** can be tuned to operate within a particular

frequency band. In some instances, a device includes multiple antennas, and the antennas can be, for example, physically separated. In some instances, antennas differ with respect to radiation patterns, polarizations, take-off angle gain and/or tuning bands. RF interface module **202** can include one or more phase shifters, filters, attenuators, amplifiers, switches and/or other components to demodulate received signals, coordinate signal transmission and/or facilitate high-quality signal transmission and receipt.

In some instances, network interface module **202** includes a virtual network interface, so as to enable the device to utilize an intermediate device for signal transmission or reception. For example, network interface module **202** can include VPN software.

Network interface module **202** and one or more antennas **203** can be configured to transmit and receive signals over one or more connection types. For example, network interface module **202** and one or more antennas **203** can be configured to transmit and receive WiFi signals, cellular signals, Bluetooth signals, Bluetooth Low Energy (BLE) signals, Zigbee signals, or Near-Field Communication (NFC) signals.

Message processor module **204** can coordinate communication with other electronic devices or systems, such as one or more servers or a user device. In one instance, message processor module **204** is able to communicate using a plurality of protocols (e.g., any known, future and/or convenient protocol such as, but not limited to, XML, SMS, MMS, and/or email, etc.). Message processor module **204** may further optionally serialize incoming and/or outgoing messages and facilitate queuing of incoming and outgoing message traffic.

Message processor module **204** can perform functions of an IP layer in a network protocol stack. For example, in some instances, message processor module **204** can format data packets or segments, combine data packet fragments, fragment data packets and/or identify destination applications and/or device addresses. For example, message processor module **204** can defragment and analyze an incoming message to determine whether it is to be forwarded to another device and, if so, can address and fragment the message before sending it to the network interface module **202** to be transmitted. As another example, message processor module **204** can defragment and analyze an incoming message to identify a destination application that is to receive the message and can then direct the message (e.g., via a transport layer) to the application.

Communications manager module **206** can implement transport-layer functions. For example, communications manager module **206** can identify a transport protocol for an outgoing message (e.g., transmission control protocol (TCP) or user diagram protocol (UDP)) and appropriately encapsulate the message into transport protocol data units. Message processor module **204** can initiate establishment of connections between devices, monitor transmissions failures, control data transmission rates and monitoring transmission quality. As another example, communications manager module **206** can read a header of an incoming message to identify an application layer protocol to receive the message's data. The data can be separated from the header and sent to the appropriate application. Message processor module **204** can also monitor the quality of incoming messages and/or detect out of order incoming packets.

In some instances, characteristics of message-receipt or message-transmission quality can be used to identify a health status of an established communications link. In some instances, communications manager module **206** can be configured to detect signals indicating the health status of an established communications link (e.g., a periodic signal from the other device system, which if received without dropouts, indicates a healthy link).

In some instances, a communication configurer module **208** is provided to track attributes of another system so as to facilitate establishment of a communication session. In one embodiment, communication configurer module **208** further ensures that inter-device communications are conducted in accordance with the identified communication attributes and/or rules. Communication configurer module **208** can maintain an updated record of the communication attributes of one or more devices or systems. In one embodiment, communications configurer module **208** ensures that communications manager module **206** can deliver the payload provided by message processor module **204** to the destination (e.g., by ensuring that the correct protocol corresponding to the client system is used).

A communications rules provider module **210** can implement one or more communication rules that relate to details of signal transmissions or receipt. For example, a rule may specify or constrain a protocol to be used, a transmission time, a type of link or connection to be used, a destination device, and/or a number of destination devices. A rule may be generally applicable or conditionally applicable (e.g., only applying for messages corresponding to a particular app, during a particular time of day, while a device is in a particular geographical region, when a usage of a local device resource exceeds a threshold, etc.). For example, a rule can identify a technique for selecting between a set of potential destination devices based on attributes of the set of potential destination devices as tracked by communication configure module **316**. To illustrate, a device having a short response latency may be selected as a destination device. As another example, communications rules provider **210** can maintain associations between various devices or systems and resources. Thus, messages corresponding to particular resources can be selectively transmitted to destinations having access to such resources.

A variety of application modules **212** can be configured to initiate message transmission, process incoming transmissions, facilitate selective granting of resource access, facilitate processing of requests for resource access, and/or performing other functions. In the instance depicted in FIG. **2**, application modules **212** include an auto-updater module **214**, a resource access coordinator module **216**, and/or a code verification module **218**.

Auto-updater module **214** automatically updates stored data and/or agent software based on recent changes to resource utilization, availability or schedules and/or updates to software or protocols. Such updates can be pushed from another device (e.g., upon detecting a change in a resource availability or access permit) or can be received in response to a request sent by device **200**. For example, device **200** can transmit a signal to another device that identifies a particular resource, and a responsive signal can identify availabilities of access to the resource. As another example, device **200** can transmit a signal that includes an access access-enabling code, and a responsive signal can indicate whether the code is applicable for access of a particular resource and/or is valid.

In some instances, auto-updater module **214** is configured to enable the agent software to understand new, messages, commands, and/or protocols, based on a system configuration/change initiated on another device. Auto-updater module **214** may also install new or updated software to provide support and/or enhancements, based on a system configu-

ration change detected on device **200**. System configuration changes that would necessitate changes to the agent software can include, but are not limited to, a software/hardware upgrade, a security upgrade, a router configuration change, a change in security settings, etc. For example, if auto-updater module **214** determines that a communication link with another device has been lost for a pre-determined amount of time, auto-updater module **214** can obtain system configuration information to help re-establish the communication link. Such information may include new settings/configurations on one or more hardware devices or new or upgraded software on or connected to device **200**. Thus, auto-updater module **214** can detect or be informed by other software when there is a new version of agent software with additional functionality and/or deficiency/bug corrections or when there is a change with respect to the software, hardware, communications channel, etc.), and perform updates accordingly.

Based on the newly obtained system configuration for device **200**, auto-updater module **214** can cause a new communication link to be re-established with another device. In one embodiment, upon establishment of the communication link, system configuration information about device **200** can also be provided to another device to facilitate the connection to or downloading of software to device **200**.

In one embodiment, when a poor health signal is detected by another device (e.g., when the health signal is only sporadically received but the communication link is not necessarily lost), the other device can send a command to auto-updater module **214** to instruct auto-updater module **214** to obtain system configuration information about device **200**. The updated system configuration information may be used in an attempt to revive the unhealthy communications link (e.g., by resending a resource request). For example, code can utilize appropriate system calls for the operating system to fix or reestablish communications. By way of example and not limitation, model and driver information is optionally obtained for routers in the system in order querying them. By way of further example, if the code determines that a new brand of router has been installed, it can adapt to that change, or to the change in network configuration, or other changes.

Instead or in addition, the host server (e.g., via communications manager **206**) can send specific instructions to auto-updater module **214** to specify tests or checks to be performed on device **200** to determine the changes to the system configurations (e.g., by automatically performing or requesting an inventory check of system hardware and/or software). For example, the components involved in the chain of hops through a network can be queried and analyzed. Thus, for example, if a new ISP (Internet service provider) is being used and the management system traffic is being filtered, or a new router was installed and the software needs to change its configuration, or if someone made a change to the operating system that affects port the management system is using to communicate, the management system (or operator) can communicate with the ISP, change it back, or choose from a new available port, respectively.

The specific tests may be necessary to help establish the communication link, if, for example, the automatic tests fail to provide sufficient information for the communication link to be re-established, if additional information is needed about a particular configuration change, and/or if the client system is not initially supported by the auto-updater module **214**, etc.

Auto-updater module **214** can also receive signals identifying updates pertaining to current or future availability of resources and/or access permits. Based on the signals, auto-updater module **214** can modify, add to or delete stored data pertaining to resource availabilities, resource schedules and/or valid access permits. For example, upon receiving an update signal, auto-updater **214** can modify data stored in one or more data stores **222**, such as an account data store **224**, resource specification data store **226**, resource status data store **228** and/or access-enabling code data store **230**.

Account data store **224** can store data for entities, such as administrators, intermediate-system agents and/or users. The account data can include technical data, such a particular entity can be associated with one or more device types, IP addresses, browser identifier and/or operating system identifier).

Resource specification data store **226** can store specification data characterizing each of one or more resources. For example, specification data for a resource can include a processing power, available memory, operating system, compatibility, device type, processor usage, power status, device model, number of processor cores, types of memories, date and time of availability, a performing entity, a venue of the event and/or a set of seats (e.g., a chart or list). Specification data can further identify, for example, a cost for each of one or more access rights.

Resource status data store **228** can store status data reflecting which resources are available (or unavailable), thereby indicating which resources have one or more open assignments. In some instances, the status data can include schedule information about when a resource is available. Status data can include information identifying an entity who requested, reserved or was assigned a resource. In some instances, status information can indicate that a resource is being held or reserved and may identify an entity associated with the hold or reserve and/or a time at which the hold or reservation will be released.

Access-enabling code data store **230** can store access-enabling code data that includes one or more codes and/or other information that can be used to indicate that an entity is authorized to use, have or receive a resource. An access-enabling code can include, for example, a numeric string, an alphanumeric string, a text string, a 1-dimensional code, a 2-dimensional code, a barcode, a quick response (QR) code, an image, a static code and/or a temporally dynamic code. An access-enabling code can be, for example, unique across all instances, resource types and/or entities. For example, access-enabling codes provided in association for tickets to a particular event can be unique relative to each other. In some instances, at least part of a code identifies a resource or specification of a resource. For example, for a ticket to a concert, various portions of a code may reflect: a performing entity, resource location, date, section and access-permitted location identifier.

One or more of data stores **224**, **226**, **228**, and **230** can be a relational data store, such that elements in one data store can be referenced within another data store. For example, resource status data store **228** can associate an identifier of a particular access-enabling code with an identifier of a particular entity. Additional information about the entity can then be retrieved by looking up the entity identifier in account data store **224**.

Updates to data stores **224**, **226**, **228**, and **230** facilitated and/or initiated by auto-updater module **214** can improve cross-device data consistency. Resource access coordinator module **216** can coordinate resource access by, for example, generating and distributing identifications of resource avail-

abilities; processing requests for resource access; handling competing requests for resource access; and/or receiving and responding to resource-offering objectives.

FIG. **3** illustrates example components of resource access coordinator module **216** that may operate, at least in part, at an access management system (e.g., access management system) according to an embodiment of the invention. A resource specification engine **302** can identify one or more available resources. For example, resource specification engine **302** can detect input that identifies a current or future availability of a new resource.

Resource specification engine **302** can identify one or more specifications of each of one or more resources. A specification can include an availability time period. For example, resource specification engine **302** can determine that a resource is available, for example, at a particular date and time (e.g., as identified based on input), for a time period (e.g., a start to end time), as identified in the input, and/or from a time of initial identification until another input indicating that the resource is unavailable is detected. A specification can also or alternatively include a location (e.g., a geographic location and/or venue) of the resource. A specification can also or alternatively include one or more parties associated with the resource (e.g., performing acts or teams). Resource specification engine **302** can store the specifications in association with an identifier of the resource in resource specifications data store **226**.

A resource-access allocation engine **304** can allocate access rights for individual resources. An access right can serve to provide an associated entity with the right or a priority to access a resource. Because (for example) association of an access right with an entity can, in some instances, be conditioned on various events, an allocated access right can be initially unassociated with particular entities (e.g., users). For example, an allocated right can correspond to one or more access characteristics, such as an processor identifier, a usage time, a memory allocation, a geographic location (e.g., section or seat identifier), and/or a fee. For an allocated access right, resource-access allocation engine **304** can store an identifier of the right in resource statuses data store **228** in association with an identifier for the resource and an indication that it has not yet been assigned to a particular entity.

A communication engine **306** can facilitate communicating the availability of the resource access rights to users. In some instances, a publisher engine **308** generates a presentation that identifies a resource and indicates that access rights are available. Initially or in response to user interaction with the presentation, the presentation can identify access characteristics about available access rights. The presentation can include, for example, a chart that identifies available access rights for an event and corresponding fees. Publisher engine **308** can distribute the presentation via, for example, a website, app page, email and/or message. The presentation can be further configured to enable a user to request assignments of one or more access rights.

In some instances, an intermediate system coordination engine **310** can facilitate transmission of information about resource availability (e.g., resource specifications and characteristics of resource-access rights) to one or more intermediate systems (e.g., by generating one or more messages that include such information and/or facilitating publishing such information via a website or app page). Each of the one or more intermediate systems can publish information about the resource and receive requests for resource access. In some instances, intermediate system coordination engine **310** identifies different access rights as being available to individual intermediate systems to coordinate assignment. For example, access rights for Section 1 may be provided for a first intermediate system to assign, and access rights for Section 2 may be provided to a second intermediate system to assign.

In some instances, overlapping access rights are made available to multiple intermediate systems to coordinate assignments. For example, some or all of a first set of resource rights (e.g., corresponding to a section) may be provided to first and second intermediate systems. In such instances, intermediate system coordination engine **310** can respond to a communication from a first intermediate system indicating that a request has been received (e.g., and processed) for an access right in the set) by sending a notification to one or more other intermediate systems that indicates that the access right is to be at least temporarily (or entirely) made unavailable.

Intermediate system coordination engine **310** can monitor communication channels with intermediate systems to track the health and security of the channel. For example, a healthy connection can be inferred when scheduled signals are consistently received. Further, intermediate system coordination engine **310** can track configurations of intermediate systems (e.g., via communications generated at the intermediate systems via a software agent that identifies such configurations) so as to influence code generation, communication format, and/or provisions or access rights.

Thus, either via a presentation facilitated by publisher engine **308** (e.g., via a web site or app page) or via communication with an intermediate system, a request for assignment of an access right can be received. A request management engine **312** can process the request. Processing the request can include determining whether all other required information has been received, such as user-identifying information (e.g., name), access-right identifying information (e.g., identifying a resource and/or access-right characteristic) user contact information (e.g., address, phone number, and/or email address), and/or user device information (e.g., type of device, device identifier, and/or IP address).

When all required information has not been received, request management engine **312** can facilitate collection of the information (e.g., via a webpage, app page or communication to an intermediate system). Request management engine **312** can also or alternatively collect and/or process payment-related data.

In some instances, request management engine **312** prioritizes requests, such as requests for overlapping, similar or same access rights (e.g., requests for access rights associated with a same section) received within a defined time period. The prioritization can be based on, for example, times at which requests were received (e.g., prioritizing earlier requests), a request parameter (e.g., prioritizing requests for a higher or lower number of access rights above others), whether requests were received via an intermediate system (e.g., prioritizing such requests lower than others), intermediate systems associated with requests (e.g., based on rankings of the systems), whether requests were associated with users having established accounts, and/or whether requests were associated with inputs indicative of a bot initiating the request (e.g., shorter inter-click intervals or failed CAPTCHA tests).

Upon determining that required information has been received and request-processing conditions have been met, request management engine **312** can forward appropriate request information to a resource scheduling engine **314**. For a request, resource scheduling engine **314** can query

resource status data store **228** to identify access rights matching parameters of the request.

In some instances, the request has an access-right specificity matching a specificity at which access rights are assigned. In some instances, the request is less specific, and resource scheduling engine **314** can then facilitate an identification of particular rights to assign. For example, request management engine **312** can facilitate a communication exchange by which access right characteristics matching the request are identified, and a user is allowed to select particular rights. As another example, request management engine **312** can itself select from amongst matching access rights based on a defined criterion (e.g., best summed or averaged access-right ranking, pseudo-random selection, or a selection technique identified based on user input).

Upon identifying appropriately specific access rights, resource scheduling engine **314** can update resource status data store **228** so as to place the access right(s) on hold and/or to change a status of the access right(s) to indicate that they have been assigned. Such assignment indication may associate information about the user (e.g., user name, device information, phone number and/or email address) and/or assignment process (e.g., identifier of any intermediate system and/or assignment date and time) with an identifier of the access right(s).

For individual assigned access rights, an encoding engine **316** can generate an access-enabling code. The access-enabling code can include, for example, an alphanumeric string, a text string, a number, a graphic, a barcode (e.g., a 1-dimensional or 2-dimensional barcode), a static code, a dynamic code (e.g., with a feature depending on a current time, current location or communication) and/or a technique for generating the code (e.g., whereby part of the code may be static and part of the code may be determined using the technique). The code may be unique across all access rights, all access rights for a given resource, all access rights associated with a given location, all access rights associated with a given time period, all resources and/or all users. In some instances, at least part of the code is determined based on or is thereafter associated with an identifier of a user, user device information, a resource specification and/or an access right characteristic.

In various embodiments, the code may be generated prior to allocating access rights (e.g., such that each of some or all allocated access rights are associated with an access-enabling code), prior to or while assigning one or more access right(s) responsive to a request (e.g., such that each of some or all assigned access rights are associated with an access-enabling code), at a prescribed time, and/or when the device is at a defined location and/or in response to user input. The code may be stored at or availed to a user device. In various instances, at the user device, an access-enabling code may be provided in a manner such that it is visibly available for user inspection or concealed from a user.

Encoding engine **316** can store the access-enabling codes in access-enabling code data store **230**. Encoding engine **316** can also or alternatively store an indication in account data store **224** that the access right(s) have been assigned to the user. It will again be appreciated that data stores **224**, **226**, **228**, and **230** can be relational and/or linked, such that, for example, an identification of an assignment can be used to identify one or more access rights, associated access-enabling code(s) and/or resource specifications.

Resource scheduling engine **314** can facilitate one or more transmissions of data pertaining to one or more assigned access rights to a device of a user associated with the assignment. The data can include an indication that access rights have been assigned and/or details as to which rights have been assigned. The data can also or alternatively include access-enabling codes associated with assigned access rights.

While FIG. **3** depicts components of resource access coordinator module **316** that may be present on an access management system **120**, it will be appreciated that similar or complementary engines may be present on other systems. For example, a communication engine on a user device can be configured to display presentations identifying access right availability, and a request management engine on a user device can be configured to translate inputs into access-right requests to send to an intermediate system or access management system.

Returning to FIG. **2**, code verification module **218** (e.g., at a user device or client device) can analyze data to determine whether an access-enabling code is generally valid and/or valid for a particular circumstance. The access-enabling code can include one that is received at or detected by device **200**. The analysis can include, for example, determining whether all or part of the access-enabling code matches one stored in access-enabling code data store **230** or part thereof, whether the access-enabling code has previously been applied, whether all or part of the access-enabling code is consistent with itself or other information (e.g., one or more particular resource specifications, a current time and/or a detected location) as determined based on a consistency analysis and/or whether all or part of the access-enabling code has an appropriate format.

For example, access-enabling code data store **230** can be organized in a manner such that access-enabling codes for a particular resource, date, resource group, client, etc. can be queried to determine whether any such access-enabling codes correspond to (e.g. match) one being evaluated, which may indicate that the code is verified. Additional information associated with the code may also or alternatively be evaluated. For example, the additional information can indicate whether the code is currently valid or expired (e.g., due to a previous use of the code).

As another example, a portion of an access-enabling code can include an identifier of a user device or user account, and code verification module **218** can determine whether the code-identified device or account matches that detected as part of the evaluation. To illustrate, device **200** can be a client device that electronically receives a communication with an access-enabling code from a user device. The communication can further include a device identifier that identifies, for example, that the user device is a particular type of smartphone. Code verification module **218** can then determine whether device-identifying information in the code is consistent with the identified type of smartphone.

As yet another example, code verification module **218** can identify a code format rule that specifies a format that valid codes are to have. To illustrate, the code format rule may identify a number of elements that are to be included in the code or a pattern that is to be present in the code. Code verification module **218** can then determine that a code is not valid if it does not conform to the format.

Verification of an access-enabling code can indicate that access to a resource is to be granted. Conversely, determining that a code is not verified can indicate that access to a resource is to be limited or prevented. In some instances, a presentation is generated (e.g., and presented) that indicates whether access is to be granted and/or a result of a verification analysis. In some instances, access granting and/or limiting is automatically affected. For example, upon a code verification, a user device and/or user may be automatically

permitted to access a particular resource. Accessing a resource may include, for example, using a computational resource, possessing an item, receiving a service, entering a geographical area, and/or attending an event (e.g., generally or at a particular location).

Verification of an access-enabling code can further trigger a modification to access-enabling code data store **230**. For example, a code that has been verified can be removed from the data store or associated with a new status. This modification may limit attempts to use a same code multiple times for resource access.

A combination of modules **214**, **216**, **218** comprise a secure addressable endpoint agent **220** that acts as an adapter and enables cross-device interfacing in a secure and reliable fashion so as to facilitate allocation of access-enabling codes and coordinate resource access. Secure addressable endpoint agent **220** can further generate a health signal that is transmitted to another device for monitoring of a status of a communication channel. The health signal is optionally a short message of a few bytes or many bytes in length that may be transmitted on a frequent basis (e.g., every few milliseconds or seconds). A communications manager **206** on the receiving device can then monitors the health signal provided by the agent to ensure that the communication link between the host server and device **200** is still operational.

In some instances, device **200** can include (or can be in communication with) a physical access control **232**. Physical access control **232** can include a gating component that can be configured to provide a physical barrier towards accessing a resource. For example, physical access control **232** can include a turnstile or a packaging lock.

Physical access control **232** can be configured such that it can switch between two modes, which differ in terms of a degree to which user access to a resource is permitted. For example, a turnstile may have a locked mode that prevents movement of an arm of the turnstile and an unlocked mode that allows the arm to be rotated. In some instances, a default mode is the mode that is more limiting in terms of access.

Physical access control **232** can switch its mode in response to receiving particular results from code verification module **218**. For example, upon receiving an indication that a code has been verified, physical access control **232** can switch from a locked mode to an unlocked mode. It may remain in the changed state for a defined period of time or until an action or event is detected (e.g., rotation of an arm).

Device **200** can also include one or more environmental sensors **234**. Measurements from the sensor can processed by one or more application modules. Environmental sensor(s) **234** can include a global positioning system (GPS) receiver **235** that can receive signals from one or more GPS satellites. A GPS chipset can use the signals to estimate a location of device **200** (e.g., a longitude and latitude of device **200**). The estimated location can be used to identify a particular resource (e.g., one being provided at or near the location at a current or near-term time). The identification of the particular resource can be used, for example, to identify a corresponding (e.g., user-associated) access-enabling code or to evaluate an access-enabling code (e.g., to determine whether it corresponds to a resource associated with the location).

The estimated location can further or alternatively be used to determine when to perform a particular function. For example, at a user device, detecting that the device is in or has entered a particular geographical region (e.g., is within a threshold distance from a geofence perimeter or entrance gate) can cause the device to retrieve or request an access-enabling code, conduct a verification analysis of the code and/or transmit the code to a client device.

It will be appreciated that environmental sensor(s) **234** can include one or more additional or alternative sensors aside from GPS receiver **235**. For example, a location of device **200** can be estimated based on signals received by another receive from different sources (e.g., base stations, client point devices or Wi Fi access points). As another example, an accelerometer and/or gyroscope can be provided. Data from these sensors can be used to infer when a user is attempting to present an access-enabling code for evaluation.

It will also be appreciated that the components and/or engines depicted in figures herein are illustrative, and a device need not include each depicted component and/or engine and/or can include one or more additional components and/or engines. For example, a device can also include a user interface, which may include a touch sensor, keyboard, display, camera and/or speakers. As another example, a device can include a power component, which can distribute power to components of the device. The power component can include a battery and/or a connection component for connecting to a power source. As yet another example, a module in the application layer can include an operating system. As still another example, an application-layer control processor module can provide message processing for messages received from another device. The message processing can include classifying the message and routing it to the appropriate module. To illustrate, the message can be classified as a request for resource access or for an access-enabling code, an update message or an indication that a code has been redeemed or verified. The message processing module can further convert a message or command into a format that can interoperate with a target module.

It will further be appreciated that the components, modules and/or agents could be implemented in one or more instances of software. The functionalities described herein need not be implemented in separate modules, for example, one or more functions can be implemented in one software instance and/or one software/hardware combination. Other combinations are similarly be contemplated.

Further yet, it will be appreciated that a storage medium (e.g., using magnetic storage media, flash memory, other semiconductor memory (e.g., DRAM, SRAM), or any other non-transitory storage medium, or a combination of media, and can include volatile and/or non-volatile media) can be used to store program code for each of one or more of the components, modules and/or engines depicted in FIGS. **2** and **3** and/or to store any or all data stores depicted in FIG. **2** or described with reference to FIGS. **2** and/or **3**. Any device or system disclosed herein can include a processing subsystem for executing the code. The processing system can be implemented as one or more integrated circuits, e.g., one or more single-core or multi-core microprocessors or microcontrollers, examples of which are known in the art.

FIG. **4** illustrates a flowchart of an embodiment of a process **400** for assigning access rights for resources. Process **400** can be performed by an access management system, such as access management system **120**. Process **400** begins at block **405** where resource specification engine **302** identifies one or more specifications for a resource. The specifications can include, for example, a time at which the resource is to be available, a location of the resource, a capacity of the resources and/or one or more entities (e.g., performing entities) associated with the resource.

At block **410**, resource-access allocation engine **304** allocates a set of access rights for the resource. In some instances, each of at least some of the access rights corresponds to a different access parameter, such as a different location assignment. Upon allocation, each of some or all of the access rights may have a status as available. A subset of the set of access rights can be immediately (or at a defined time) assigned or reserved according to a base assignment or reservation rule (e.g., assigning particular access rights to particular entities, who may be involved in or related to provision of the resource and/or who have requested or been assigned a set of related access rights.

At block **415**, communication engine **306** transmits the resource specifications and data about the access rights. The transmission can occur in one or more transmissions. The transmission can be to, for example, one or more user devices and/or intermediate systems. In some instances, a notification including the specifications and access-right data is transmitted, and in some instances, a notification can be generated at a receiving device based on the specifications and access-right data. The notification can include, for example, a website that identifies a resource (via, at least in part, its specifications) and indicates that access rights for the resource are available for assignment. The notification can include an option to request assignment of one or more access rights.

At block **420**, request management engine **312** receives a request for one or more access rights to be assigned to a user. The request can, for example, identify particular access rights and/or access parameters. The request can include or be accompanied by other information, such as identifying information. In some instances, the access management system can use at least some of such information to determine whether a fee for the access rights has been authorized. In some instances, the request is received via an intermediate system that has already handled such authorization.

At block **425**, resource scheduling engine **314** assigns the requested one or more access rights to the user. The assignment can be conditioned on receipt of all required information, confirmation that the access right(s) have remained available for assignment, determining using data corresponding to the request that a bot-detection condition is not satisfied, fee provision and/or other defined conditions. Assignment of the access right(s) can include associating an identifier of each of the one or more rights with an identifier of a user and/or assignment and/or changing a status of the access right(s) to assigned. Assignment of the access right(s) can result in impeding or preventing other users from requesting the access right(s), being assigned the access right(s) and/or being notified that the access right(s) are available for assignment. Assignment of the access right(s) can, in some instances, trigger transmission of one or more communications to, for example, one or more intermediate systems identifying the access right(s) and indicating that they have been assigned and/or with an instruction to cease offering the access rights.

At block **430**, encoding engine **316** generates an access-enabling code for each of the one or more access rights. The code can be generated, for example, as part of the assignment, as part of the allocation or subsequent to the assignment (e.g., upon detecting that a user is requesting access to the resource). Generating an access-enabling code can include applying a code-generation technique, such on one that generates a code based on a characteristic of a user, user device, current time, access right, resource, intermediate system or other variable. The access-enabling code can include a static code that will not change after it has been initially generated or a dynamic code that changes in time (e.g., such that block **430** can be repeated at various time points).

At block **435**, communication engine **306** transmits a confirmation of the assignment and the access-enabling code(s) in one or more transmissions. The transmission(s) may be sent to one or more devices, such as a user device having initiated the request from block **420**, a remote server or an intermediate system having relayed the request from block **420**.

FIG. **5** illustrates example components of resource access coordinator module **214** that may operate, at least in part, at a user device system or client device according to an embodiment of the invention. In some embodiments, components can be distributed across multiple devices or systems (e.g., a user device and a client device), a part or all of single component can be present at multiple devices or systems, or parts of a single component can be distributed across multiple devices or systems.

A communications engine **502** can facilitate communicating with one or more other devices or systems. Communication engine **502** includes a device discovery engine **504** that can discover other (e.g., nearby) devices. The device discovery can include, for example, detecting devices via BLE communication channels. The discovery can include a passive discovery, whereby device discovery engine **504** monitors received communications (or beacons) and identifies signals having particular characteristics, being received via a particular type of communication protocol (e.g., BLE) and/or being received from a particular type of device (e.g., one indicating that it pertains to a particular resource or is associated with a particular entity). The discovery can also or alternatively include an active discovery, whereby device discovery engine **504** facilitates transmission of periodic (e.g., regular) presence-advertising signals.

Upon discovery or other establishment of a communication channel, a communication coordination engine **506** can facilitate appropriate communication with the device. For example, communication coordination engine **506** can facilitate generation of messages with pertinent content and/or detecting pertinent content from within received communications.

A device discovery, communication receipt or other event (e.g., detection of a time associated with an access right) can trigger an access-right detection engine **508** to identify data pertaining to one or more access rights. In some instances, the one or more access rights include one or more unassigned access rights for a particular resource. For example, a user device can receive a communication from a client device that identifies access rights available to access a resource being availed by a client (e.g., within a defined time period). The data can include access parameters and/or assignment criteria (e.g., fees).

In some instances, the one or more access rights include one or more access rights associated with a particular account or user device. For example, an access-right detection engine **508** on a user device can initiate a query for and/or retrieval of (e.g., from a local or remote data store) data for access rights associated with the device or an account that a user is logged into on the device. The query can further specify or constrain an access parameter (e.g., to correspond to a current time and/or location) and/or resource. To illustrate, access-right detection engine **508** on a user device may detect a signal (e.g., via communication engine **502**) from a client device that identifies a resource, and access-right detection engine **508** can initiate a query for

access rights that are associated with the resource and assigned to one or more particular parties and/or associated with a particular user account. The data can include, for example, one or more parameters associated with the access right(s) and/or an access-enabling code (or code-generating technique).

In some instances, the data pertaining to the one or more access rights includes data received in a communication. For example, access-right detection engine **508** can detect a signal (e.g., via communication coordination engine **506**) from a user device that includes data pertaining to access rights that are being submitted for evaluation and/or redemption. The data can include, for example, one or more access-enabling codes.

A request management engine **510** can facilitate notifying a user of the access right(s). For example, a client device may push data pertaining to one or more unassigned access rights for a resource via a BLE communication channel to a nearby user device, and request management engine **510** at the user device can generate a presentation that includes or represents the data (e.g., identifying locations and prices of the access rights). As another example, request management engine **510** can facilitate dynamic updates to an app interface or web page as a user provides inputs that identifies a resource or constrains a resource identification. Such facilitation can include, for example, translating inputs into selections or constraints, identifying query constraints based on an input, and/or generating a message to send to a remote server (e.g., associated with a website or app) based on inputs that include a request for an updated or new webpage or app page or for access-right data. As yet another example, a client device can send a signal to a user device that identifies a resource. Access-right detection engine **508** can then coordinate transmission of a signal to a remote system (e.g., an access management system) that requests identifications of unassigned access rights for the resource. Request management engine **510** can generate a presentation that includes or represents data received in a responsive communication.

An interface engine **512** can present various notifications and/or presentations, such as those identifying unassigned access rights and/or those generated or requested by request management engine **510**. The notifications and/or presentations can be presented, for example, on a display of a device (e.g., user device). A notification and/or presentation of one or more unassigned access right can be accompanied by one or more options to request access-right assignment (e.g., of one or more particular access rights). For example, an identification or representation of each access right may be accompanied by an option to request assignment of the access right. Interface engine **512** may detect a selection of an option (e.g., via a touch or mouse click) and can convey the selection to request management engine **510**.

Request management engine **510** can collect data and generate a request communication that identifies the requested access right(s) (or requested access-right parameters) and/or other pertinent data (e.g., user identifying information and/or device information). The data can be collected based on input provided at the user device by the user (e.g., and thereby detected by interface engine), automatic detection (e.g., of device specifications and/or configurations), and/or account data.

Thus, in some instances, request management engine **510** can communicate with an account engine **512**, which can determine whether a user device is logged into an account (e.g., based on past provision of a username and password), identify an account, and/or facilitate retrieval (e.g., from a local or remote data store) of account data.

Upon generating the request communication, request management engine **510** can facilitate transmitting the signal to a destination device (e.g., an access management system or client device). In some instances, a responsive communication can indicate that additional information is needed to process the request, and request management engine **510** can coordinate attempts to obtain the requested information and provide such information to the destination device. In some instances, a responsive communication can indicate that one or more access rights have been assigned (e.g., to the user or to another identified party) and may include part or all of an access-enabling code (and/or code-generating technique). Request management engine **510** can then coordinate a presentation of a notification of the assignment and/or local storage of data pertaining to the assignment (e.g., locally storing part or all of an access-enabling code and/or code-generating technique).

Various events can trigger an access-right evaluation, which can be coordinated by an access-right evaluation engine. For example, access-right detection engine **508** may detect a communication from a client device that identifies a resource and requests access-right data and/or an evaluation of access-right data. Access-right detection engine **508** may then query a local or remote data store for access-right data assigned to a particular user, associated with a particular user device and/or pertaining to the identified resource. As another example, access-right evaluation engine may detect a communication from a client device or remote system that requests data identifying a user, person, account, device and/or other variable that may be used to identify select access rights corresponding to a user device. Access-right evaluation engine **516** can then retrieve or identify such information (e.g., by retrieving the information from an account data store, by automatic detection or by prompting a user for input) and can transmit the data to the client device or remote system so as to retrieve and evaluate corresponding access-right data. As yet another example, access-right detection engine **508** can determine that a detected location of a user device and/or current time corresponds to a location and/or time period associated with one or more access rights assigned to a particular user and/or associated with a user device. Access-right detection engine **508** can then retrieve additional access-right data for the access right(s). It will therefore be appreciated that, in various instances, an evaluation of access-right data may be performed by access-right evaluation engine at a user device and/or at another device or system (e.g., client device or access management system).

The access-right data can include part or all of an access-enabling code associating with each of the one or more assigned access rights and/or a code-generating technique. For example, a code-generating technique may indicate that a fixed part of the code is static and is to be combined with another part of the code, which may be dynamic, which may depend on (for example) a current time and/or location of a user device, and/or which may be based on a characteristic of a device performing the technique (e.g., to reflect a device type and/or whether the device matches one corresponding to a party to whom the access right was assigned).

The access-right data can further or alternatively include data reflecting access-right parameters and/or a resource to which the access right(s) apply. For example, access-right data may include a location and/or time corresponding to an access right. The access-right data can also or alternatively include data pertaining to an assignment of the access right(s), such as an identifier of a user (or user account) to

which the right was assigned and/or a device used or identified during the assignment.

Access-right evaluation engine **516** can coordinate an evaluation of an access right. The evaluation can include, for example, determining whether access right parameter(s) pertain to particulars (e.g., a current time, a current location of an evaluating device or of the user device, and/or a particular resource). The evaluation can further or alternatively include determining whether access-right data pertaining to assignment of the access right(s) matches that associated with a user device requesting evaluation and/or redemption of the right(s). For example, it can be determined whether a same account is logged into on an evaluating user device as the one used to request assignment of the access right(s).

The evaluation can include evaluating an access-enabling code, which can include, for example, determining whether part or all of the code matches one in a data store or one independently generated, whether part of the code matches a variable determined based on a current time and/or detected location (e.g., of an evaluating device or user device), whether the code has been previously redeemed, whether part or all of the code corresponds to a particular resource, whether a format of the code is of an approved format, whether the code exhibits an internal defined consistency, whether part or all of the code matches a variable determined based on a characteristic of a user device, and so on.

Based on the evaluation, access-right evaluation engine **516** can generate a stimulus to be presented (e.g., via interface engine **512**) at a user device or client device. In some instances, a same device performs the evaluation, generates the stimulus and presents the stimulus. In some instances, different devices are involved (e.g., and appropriate data is transmitted across devices). The stimulus can include a visual, audio or haptic stimulus. Characteristics of the stimulus can include, for example, one or more spatial or temporal patterns, shapes, colors, images, overlays or dynamic elements (e.g., a degree to which and/or a frequency at which an image or tone changes). Characteristics can be determined based on, for example, a result of the evaluation performed by access-right evaluation engine **516**, one or more access-right parameters, a current time and/or a pseudo-random generator.

For example, at a user device, different stimuli may be generated depending on whether one or more access rights were determined to be valid (e.g., generally, to access a particular resource and/or for a particular type of access). To illustrate, a first pattern may be included in the stimulus upon determining that the user device is not associated with any valid access rights for a resource; a second pattern may be included upon determining that the user device is associated with one or more access rights to access the resource where the access is permitted within a first geographical area; and a third pattern may be included upon determining that the user device is associated with one or more access rights to access the resource where the access is permitted within a second geographical area. As another example, a stimulus characteristic can depend on a quantity of access rights or a priority level of access rights.

In some instances, a stimulus generated for a first holder of a first valid access right (e.g., for a resource and/or associated with an access-right parameter) may be the same or similar as a stimulus generated for a second holder of a second valid access right (e.g., for a same resource and/or associated with a same or similar access-right parameter). This can allow a client agent (e.g., usher) to easily verify the stimulus. However, it can also provide for additional openings for user manipulations (e.g., by copying others' images). Thus, in some instances, a stimulus generated for a first holder of a first valid access right (e.g., for a resource and/or associated with an access-right parameter) differs from a stimulus generated for a second holder of a second valid access right. For example, each generated stimulus can be unique or a stimulus characteristic can depend on a current time or pseudo-random factor.

An additional security feature is that, when a presentation is to be presented on a user device, access-right evaluation engine **516** can delay generation and/or presentation of a stimulus until a user device is near a check point (e.g., such as until it is within a defined distance (e.g., 5, 4, 3, 2 or 1 feet) from another device (e.g., a client device)), until it detects a stimulus-generation signal (e.g., from a client device), until it is within a defined geographical area or crosses a geofence and/or until it detects a particular device motion (e.g., corresponding to a user holding a device up to be shown to another person).

As described in further detail below, in some instances, each of a user device and a client device can include an access-right evaluation engine **516** and interface engine **512** that are each configured to, for example, evaluate an access right associated with the user device (e.g., to determine whether an access right associated with the user device exists, whether any such access right corresponds to a particular resource or access parameter, whether any pertinent access right is valid, etc.) and to generate and present a presentation indicative of a result of the evaluation. In some instances, the devices are sufficiently communicating or drawing from shared data such that the stimulus presented on the user device in part or entirely matches the stimulus presented on the client device. Further, the stimulus can indicate whether and/or to what extent the access right is valid. In some instances, whether and/or a degree to which the stimuli match is indicative of a validity and/or applicability of the access right (e.g., whether it pertains to a particular resource and/or access parameter). Thus, the multi-device stimulus presentations can allow a client agent to easily identify user devices (and associated users) not authorized to be in a particular location, receive a service, etc.

A location engine **518** can determine the current location of a device (e.g., of a user device). The location can be identified, for example, as geographic coordinates, an address, proximity to a device, proximity to a resource location, proximity to a part of a resource location (entrance, exit, gate, etc.), an indication as to whether the device is at a resource location and/or an identification of a part of a resource location that the device is at. The location can be determined by, for example, processing signals received by a receiver (e.g., in a link layer in a protocol stack) to identify which other devices signals are being received, signal strengths of one or more received signals and/or time delays of one or more received signals and to estimate the location based on the identified characteristics. One or more signals can be received by the receiver from, for example, one or more client devices, GPS satellites, or WiFi hot spots.

For example, location engine **518** can triangulate a current position within a stadium based on identified strengths of signals or delays of signals received from multiple client devices having known locations. As another example, location engine **518** at a user device can determine that the user device is near a particular concession stand by determining that the user device can detect a client-device signal (e.g.,

via a device receiver) associated with the stand or that a client-device signal strength associated with the stand is above a threshold.

In some instances, a location is determined based on content of a communication received at a user device from another device. For example, a signal from a client device can identify a particular location. Location engine **518** may determine a user device location to be the same as the location identified in the communication, or a characteristic (e.g., signal strength or latency) of the communication and the identified location can be used to estimate a user-device location (e.g., using a triangulation technique).

In some instances, a location is determined using a dead-reckoning technique. For example, an initial location may be determined based on signals received via a receiver from one or more GPS satellites or client devices, and compass and/or acceleration data (collected by corresponding sensors in the device) can then be tracked to determine a separation distance (e.g., overall or along one or more directions) from the initial location.

In some instances, location engine **518** can use an estimated location and/or other data to provide navigation assistance. Location engine **518** can access map data pertaining to one or more resources' locations, which can include, for example, layout data, such as a map of a resource-associated location and/or locations of particular locations within a resource-associated geographic area. Location engine **518** can, in some instances, generate a modified map of part or all of a resource-associated geographic area that identifies a location of the user device and/or is oriented in a perspective corresponding to a location of the user device. The map may also identify a portion of a geographic area for a resource corresponding to an access right associated with the user device. Because, in some instances, location engine **518** can estimate a user device location based on communications with client devices at a resource location, navigation assistance can be provided even without connectivity to the Internet or to GPS satellites.

Location engine **518** can further or alternatively facilitate or initiate periodic transmission of communications (e.g., to a client device, remote server or other user device) identifying its location. Such transmissions may be initiated, for example, at scheduled times, routine time intervals or upon detecting a threshold movement (e.g., distance or velocity) from a location associated with a last transmission.

In some instances, a device (e.g., a receiving device, client device, remote server or other user device) can use time-lapsed location data from one or more devices or can use location data from multiple devices to identify a congestion variable for a location. The congestion variable can then be transmitted to one or more user devices, such that a user can anticipate a wait time and/or identify a location in view of an anticipated wait or congestion. For example, a client device at a particular restroom location can track, for each of one or more individual user devices, how long the user device is in a communication range. When another user device approaches the restroom's client device, the client device can identify an anticipated wait time based on the collected data.

Communicating system **200** can also include a geofence engine **240**. Geofence engine **240** can manage one or more geofences that indicate when queries for access rights are to be initiated, access-right evaluations are to be initiated, evaluation-influenced stimulus generations are to be initiated, evaluation-influenced stimuli are to be presented and/or particular offers are to be presented. A geofence can depend on a position and/or motion (e.g., a direction of motion). A geofence can be, for example, functional, such as one defined as being within a resource-associated geographic area or structure or having crossed through any gate entrance or absolute location (e.g., defined by geographic coordinates). A geofence can depend on a distance (e.g., within 10 feet from a box office or concession stand) and/or one or more signal properties.

Geofence engine **520** can use a device location estimated by location engine **518** and/or one or more client-device signal properties to determine whether a user device is inside a geofence to determine an action is to be initiated or performed, such as enabling a user device to detect and/or transmit a request for one or more resource access rights or for an upgrade of an access right (e.g., when the user device is inside a resource-associated geographic area). In some instances, the presentation is conditioned on and/or influenced by one or more non-location factors. For example, a presenting providing an opportunity to secure access rights may be presented only upon determining that the user device is not associated with any valid access rights for a resource (or a geofence's threshold separation distance from a client-device location may be larger in such instances).

It will be appreciated that engines depicted in FIG. **5** are illustrative. A device (e.g., user device) need not include all engines depicted in FIG. **5** and/or may include additional engines.

FIG. **6** illustrates a flowchart of an embodiment of a process **600** for facilitating selective granting of resource access to authorized users based on short-range communication exchanges. Process **600** can be performed, at least in part, by a user device (e.g., user device **110**). Process **600** can further be performed, at least in part, by one or more client devices (e.g., client agent device **140**, client register **150** and/or client point device **160**) and/or by one or more remote servers (e.g., access management system **120**).

Process **600** begins at block **605***a*, where a transmitter at a client device transmits a first wireless signal, which is received at a receiver at user device at block **605***b*. The first wireless signal can include one transmitted via BLE, Bluetooth or other short-range connection. The first wireless signal can include, for example, an identifier of the transmitting client device, an identifier of a resource, one or more specifications of a resource, an identifier of a location (e.g., of the client device and/or corresponding to the resource, such as a location of a resource-associated geographic area or structure or section), a request for an access-enabling code for a resource, an identifier of a client associated with the client device and/or resource, and/or a command to be performed at a user device.

At block **610**, access-right detection engine **508** at the user device identifies a specification of a resource in response to the detection. The specification of the resource can include an identifier of the resource (e.g., a name or resource-associated code), a location of the resource (e.g., a venue), a time at which the resource is being made available for access (e.g., an event start time) or a client associated with the resource.

In some instances, the specification of the resource is identified in the first wireless signal, and block **610** includes extracting the specification from the signal. In some instances, block **610** includes using data in the signal to look up or otherwise derive the specification. For example, a first signal may include an identifier of a location, and block **610** may include transmitting a signal to a remote source with the location identifier and current time with a request for an identifier of a resource being offered at the location at the

current time. In some instances, while the detection may trigger the specification identification, the specification identification may be performed independently from data in the first wireless signal. For example, block **610** may include looking up (locally or from a resource data store) an identifier of a resource associated with a current time.

The resource can include a limited-access resource, such that parties cannot indiscriminately access the resource. For example, client agents and/or client devices may selectively permit users to access the resource so long as one or more access conditions are satisfied (e.g., a device of the user transmits a signal and/or presents an indication that includes a valid an applicable code for accessing the resource and/or that indicates that a code associated with the user or device is valid and applicable to a current circumstance).

At block **615**, access-right detection engine **508** at the user device facilitates a query for an access-enabling code using the specification of the resource. For example, block **615** can include querying a local access-enabling code data store using the specification, or block **615** can include transmitting a signal to a remote system that includes the specification (e.g., and other data, such as an identifier of a user, account and/or device) and a request to retrieve an access-enabling code corresponding to the specification (e.g., and other data).

At block **620***a*, a transmitter at the user device transmits a second signal with the access-enabling code and a request for stimulus data, and at block **620***b*, a receiver at the client device receives the second signal. The second signal can include one generated by access-right evaluation engine **516**. The request for stimulus data can include a request for an identification of a characteristic that a visual stimulus is to have that is indicative of a validity and/or applicability of the access-enabling code. In various instances, the second signal may further request an indication as to whether the access-enabling code it determined to be (e.g., by or via the client device) valid and/or applicable. The second signal can include additional data, such as a location of the user device (e.g., as identified by a location engine of the device), a current time, a resource corresponding to the specification, the identified specification of the resource and/or an indicator of a requested type of access (e.g., as identified based on received user input or inferred based on a location).

At block **625**, access-right evaluation engine **516** at the client device confirms that the code is valid and applicable to a particular resource and/or circumstance. A validity can indicate whether, for example, the access-enabling code has an approved format, has not been previously used and/or has a particular consistency (e.g., between elements within the code or between an element in the code and other data, such as a device type or location of the user device and/or current time). An approved format and/or consistency analysis may be general or may differ across, for example, resources, clients, locations, time periods and/or other factors.

An applicability can indicate whether, for example, the access-enabling code is one indicative of an access right having been assigned for a particular resource (e.g., one for which access is being requested), applies to a particular location (e.g., range of geographic coordinates), applies to a current (or particular) time or time period and/or applies to a type of requested access.

Thus, determining that an access-enabling code is applicable can include identifying a particular variable, such as the particular resource, location, time or time period and/or type of requested access (e.g., based on data in the second signal, detecting a location of the client device and/or identifying a current time). In one instance, to determine whether the code is applicable for a particular instance, access-right evaluation engine **516** at the client device may look up a variable associated with the code in a local or remote data store and compare it to the particular variable. For example, a resource associated with an access code may be looked up and compared to a resource identified in the second signal. In one instance, a data store identifying one or more codes associated with a particular variable may be queried to determine whether the access-enabling code is included in the one or more codes. In one instance, a variable for the code can be identified or determined (e.g., using a look-up technique or transformation of all or part of the code) and compared to the particular variable.

At block **630**, access-right evaluation engine **516** at the client device identifies stimulus data. In some instances, the stimulus data is unique across user devices and/or identifying-stimulus-data actions. Thus, the stimulus data identified for a first user device can be different than that for a second user device, even if each user device was associated with a valid and applicable code. The stimulus data may include a stimulus and/or a stimulus characteristic (e.g., color, texture, shape, or movement velocity). The stimulus data may be generated according to an algorithm and/or, by selecting one or more stimulus characteristics or a stimulus from a set of stimulus characteristics or stimuli. For example, a pseudo-random selection technique may be used to select each of: a background color, a background texture, a foreground shape and a foreground color. A higher number of potential characteristics of each type and a higher number of characteristic types that are variable across stimuli can increase the variability across overall stimuli across selections.

In some instances, the stimulus data reflects a validity and/or applicability of the code. For example, stimulus data may be identified to facilitate presentation of a first particular shape, color, pattern and/or image size (e.g., a green circle) when the code is valid and applicable and a second particular shape, color, pattern and/or image size (e.g., red X) otherwise. In some instances, part of the stimulus data reflects a validity and/or applicability of the code and part of the stimulus data is identified according to a technique (e.g., pseudo-random selection and/or generation technique) to promote variation of stimuli across user devices.

At block **635***a*, a transmitter at the client device transmits the stimulus data to the user device, and the receiver at the user device receives the third signal at block **635***b*. In some instances, the third signal includes additional data, such as a command for the user device to execute that causes the user device to generate a visual stimulus with identified characteristic or one that causes the user device to generate a notification that (for example) audibly or visually instructs a user to show a client agent a display of the device.

At block **640***a*, interface engine **512** at the client device facilitates a presentation (at the client device) of a visual stimulus that corresponds to the stimulus data and has the identified characteristic, and at block **640***b*, interface engine **512** at the user device facilitates a presentation (at the user device) of a visual stimulus that corresponds to the stimulus data and has the identified characteristic. In some instances, facilitating the presentation includes generating a presentation with the identified characteristic (e.g., by identifying one or more intensities, such as RGB or CMYK values, for each pixel or point in a presentation).

In some instances, the visual stimulus presented at the client device can be the same as or similar to the visual stimulus presented at the user device, can share a characteristic (e.g., a color, pattern, image and/or texture) with the visual stimulus presented at the user device and/or can

include a characteristic complementary to one of the visual stimulus presented at the user device.

The client device may further presents an indication that the code has been confirmed to be valid and applicable. For example, a check mark can be presented over or near the visual stimulus. A lack of an indication that the code has not been confirmed to be valid and applicable (e.g., a lack of a red X near the stimulus) may also serve to indicate the code's validity and applicability. In various embodiments, an indication (e.g., positive or negative indication reflecting a result of a validity and applicability code analysis) may or may not also be presented at the user device. In some instances, the indication is part of the visual stimulus.

It will be appreciated that process **600** is illustrative and various modifications are contemplated. For example, a presentation facilitated at the client device may not depend on the stimulus data and/or may not reflect whether the code is valid and/or applicable. Rather, the presentation may include one that is indicative of a code being valid and applicable.

As another exemplary modification, process **600** may be modified to include a block **630***b* performed at the user device at which stimulus data is identified. Stimulus data may be identified at each of block **630***a* and block **630***b* based on, for example, a current time, a characteristic of the user device (e.g., which may be identified in the second signal) and/or a characteristic of the code. For example, a number may be calculated based on a current time, a date, an operating system on the user device and a last digit in a numeric access-enabling code, and the number may be used to select each of one or more stimulus characteristics.

As another exemplary modification, process **600** may be modified to facilitate a transmission of another signal from the client device to a remote server that includes the code an identification of a processing that has been performed based on the code and/or a result of such processing. For example, the signal can indicate that the code had been determined to have been valid and/or that a status of the code is to be changed. Generation and/or transmission of such signal may be conditioned upon performance of a defined processing type using the code, detection of a defined processing result (e.g., validity and/or applicability), and/or detection of an input (e.g., indicating that resource access is being granted).

It will be appreciated that the association of particular blocks with the identification of a client or user device is illustrative and that, in some embodiments, particular actions may instead or additionally be performed by another device or system. For example, blocks **620***a*-**635***a* may be performed by a remote access management system. As another example, blocks **625** and **630** may be performed by the user device (e.g., an blocks **620***a*-*b* and **635***a*-*b* may be omitted from process **600**). As another example, block **640** may be performed by the client device (e.g., and blocks **635***a*-*b* may be omitted from process **600**). As yet another example, block **615** may be performed by the client device (e.g., using an identifier of the user device).

It will further be appreciated that a given device (e.g., a user device) can include one or more transmitters, receivers and/or transceivers to transmit and/or receive signals disclosed herein. Use of multiple transmitters, receivers and/or transceivers may, in some instances, facilitate data communication over different types of connections.

FIG. **7** illustrates a flowchart of an embodiment of a process **700** for generating and presenting corresponding stimuli on user and client agent device. Process **700** begins at blocks **705***a* and **705***b*, where a user device and a client agent device detect each other. The devices can detect each other, for example, over a short-range network, such as over a BLE connection. One or both of the user device and client agent device can routinely broadcast transmissions (e.g., BLE transmissions) to alert other devices of its presence and/or other information (e.g., a location of the device).

At block **710***a*, the user device determines whether a user associated with the user device is authorized to access a resource. In some instances, a current location is used to identify a resource to evaluate in the determination. For example, a user device can determine that it is near the entrance to "Section 11" and thereafter determination whether the device is associated with an access-enabling code that authorizes entrance to Section 11. The determination can be based on, for example, determining whether a data store (e.g., a local data store and/or data store associated with a user device or account) includes data identifying a right to access the resource (e.g., whether a local data store includes an access-enabling code corresponding to the resource), such as whether it includes an access-enabling code. The determination can also or alternatively be based on whether data identifying a right to access the resource is valid (e.g., has not yet been use, is not expired, etc.).

At block **710***b*, the client agent device similarly determines whether access the resource is authorized. The determination can be based on determining whether data (e.g., access-right data) exists that associates the user device with an access-enabling code, access right, or other resource-associated data and/or whether such data is valid (e.g., has not been used, includes consistent information and/or has not expired). In some instance, the client agent device queries a different data store than one queried in block **710***a*.

In some instances, a determination made in block **710***a* or **710***b* is based on data in a communication from the other device. For example, the user device can send locally stored data (e.g., access-right data) or data retrieved from a remote source to the client agent device.

At blocks **715***a* and **715***b*, the user device and client agent device generate a stimulus based on the determination. The stimulus can include a visual stimulus, such as an image and/or visual pattern. The stimulus can be indicative of the determination, such that, for example, a stimulus generated at one or both of the user device and client agent device can indicate whether access the resource is authorized or can indicate which resource is authorized for access. In some instances, the stimuli generated at blocks **715***a*-*b* are the same and/or include a similar characteristic. In some instances, the stimuli are the same when it is determined that resource access is authorized.

At blocks **720***a*-*b*, the user device and client agent device present the respective stimuli. The presentation on one or both devices can, in some instances, be delayed until a presentation criterion is satisfied. For example, the presentation can be delayed until the user device is within a threshold distance from the client agent device and/or until the user device is moved in a particular manner or held in a particular orientation (e.g., corresponding to a movement or orientation common to showing another person a screen of a device). Presentation of a particular stimulus on one or both of the user device and the client agent device and/or consistency between the stimuli can indicate that resource access is to be permitted.

The stimulus can include a visual stimulus, such as an image. In some instances, part or all of the stimulus is dynamic. For example, the stimulus can include a movie or a stimulus presented over a dynamic background. A dynamic background can include, for example, a pattern or image that moves along an axis (e.g., a horizontal, vertical or diagonal

axis), that rotates, that jitters or that changes in time. The movement may be continuous (e.g., as in a movie) or can occur via changes happening at defined times (e.g., changing the background every 5 seconds) In one instance, a new stimulus is selected for a background at each of defined times (e.g., every 15 minutes), and between the defined times, the stimulus is moved while serving as a background.

A background stimulus and/or movement of the stimulus may or may not be the same across user devices (e.g., generally or at a given time). For example, a moving background may be indicative of a an access-enabling code's validity and/or it's applicability for a resource being provided at a given location (e.g., corresponding to the device's location as estimated based on BLE signals). A characteristic of the moving background (e.g., a color of a background stimulus) may be indicative of which section the code is valid for.

An overlay stimulus presented over a background stimulus may include, for example, a barcode, access-right characteristic, picture of a user, pseudo-randomly selected image, spatial/colored pattern, etc. The stimulus can include a background that moves in time. If a person attempts to generate a code or copy another valid code, presentation of the mere code would not be associated with the moving background. Meanwhile, by also including a static overlay (or a static portion that is alongside a dynamic portion), a client agent can take time to scan or assess the static portion.

In some instances, the client agent device further transmits a communication (directly or indirectly) to the user device upon determining whether access to the resource is to be permitted and/or upon receiving an indication that access is to be permitted. In some instances, this communication triggers block **720***a* or causes a presented stimulus to change (e.g., which can include generating and/or presenting a new stimulus). For example, a check mark can be overlaid on the stimulus if access is granted and an "x" can be overlaid if access is denied.

It will be appreciated that process **700** (like all processes described herein) can be modified to omit one or more of the depicted blocks and/or to include additional blocks. For example, process **700** can be modified to omit block **710***b*. Rather, the determination as to whether a user is authorized to access a resource can be performed at the user device (e.g., only) and a stimulus can reflect a result of the determination. Meanwhile, a stimulus generated on the client agent device can identify what a correct stimulus is to look like (e.g., and may be constant or depend on parameters such as a location, a time, and/or a pseudo-random generation value). A client agent can then determine whether the user is to be granted access depending on whether the images match.

As another example, one or both of the user device and/or client agent device may communicate with a client-control device. The communication can reflect a result of the determination at block **710***a* and/or **710***b* and/or a control instruction. For example, the client agent device may send an instruction to release a gate turnstile to turn a set number of times upon determining that the user is authorized to be admitted to a section (along with one or more others).

FIG. **8** illustrates a flowchart of an embodiment of another process **800** for generating and presenting corresponding stimuli on user and client agent devices. Blocks **805***a*-**405***b* can correspond to blocks **705***a*-**305***b* in process **700**.

At blocks **810***a*-**810***b*, the user device and the client agent device identify resource data. The resource data can include, for example, an identifier of a particular resource, one or more performing entities, a date and/or time of resource availability and/or a location of a resource. In some instances, the resource data includes an identification of one or more sections or other intra-resource distinctions. Such resource data can be identified by identifying resource data that corresponds to a particular location (e.g., a current location) and/or one or more client devices or client agent devices.

At blocks **815***a*-**815***b*, the user device and client agent device retrieve an access-enabling code associated with the user data. The access-enabling code can include one corresponding to resource data (e.g., for an identified event). One or both devices can retrieve the code from a local or remote data store (e.g., via a communication from another device). In some instances, one of the user device and client agent device retrieves the code and transmits it to the other device. The access-enabling code can include data reflecting or a code based on, e.g., a resource, resource availability date and/or time, resource-involved entity, resource location, user device identifier associated with the code, and/or type of access right.

At blocks **820***a*-**820***b*, the user device and client agent device assess whether the access-enabling code is valid. For example, blocks **820***a* and/or **820***b* can include determining whether a access-enabling code has already been used or whether a first portion of the access-enabling code is consistent with (e.g., the same as, complementary to according to a defined relationship or otherwise related in a defined manner) another portion of the access-enabling code (e.g., a user device identifier).

At blocks **825***a*-**825***b*, the user device and client agent device evaluate whether the access-enabling code matches the resource data. The evaluation can include, for example, determining whether the access-enabling code corresponds to one for a particular resource, resource-availability date, resource location, etc. (as identified in the resource data) or determining whether at least part of the code represents a specification of the resource.

At blocks **830***a*-**830***b*, each of the user device and the client agent device generate an image based on the validity assessment and/or data-match evaluation. In some instances, one or both of the user device and the client agent device are configured to generate a different image when access-enabling code is valid and matches resource data as opposed to otherwise. In some instances, whether images generated by the user device and client agent device match depends on whether the access-enabling code is determined to be valid and/or to match the resource data.

At blocks **835***a*-**835***b*, the images are presented on the respective devices. A client agent can then be poised to review one or both of the presented images to determine whether access is to be granted, for example, enter a geographic area. In some instances, the image is indicative of particular access authorized. For example, the image can indicate a location for which resource access is authorized.

It will be appreciated that, while depicted process **800** includes parallel actions occurring at the user device and client agent device, various other action performances are conceived. For example, one or more of the actions shown as being performed by the client agent device may be performed by another type of client device or remote access management system. As another example, only one of user device and/or client agent device may assess a validity and/or evaluate an applicability of a code and/or generate an image. In some instances, a device performing such action(s) can transmit a communication with one or more assessment results and/or the image to the other device.

FIG. **9** illustrates a flowchart of an embodiment of another process **900** for generating and presenting corresponding stimuli on user and client agent devices. Various blocks in process **900** parallel those in process **800**.

In process **900**, at blocks **910***a* and **910***b*, the user device a client agent device identify a current location. The location can include an intra-venue location and/or functional location

At blocks **920***a*-**920***b*, the devices determine whether an access-enabling code associated with the user device (e.g., and a particular resource) corresponds to the location. For example, it can be determined whether the access-enabling code reflects, includes or is associated with an identifier of a section or zone associated with the location. The images can then be generated based on a result of this evaluation.

FIG. **10** illustrates stimuli that can be generated and presented using a technique described herein according to an embodiment of the invention. In this illustration, each of devices **1005**, **1010** and **1015** is a user device. Each device is associated with an access-enabling code that corresponds to an access right to access a resource at a particular location.

Upon detecting a client agent device **1020**, each user device can transmit information (e.g., an identifier of the device or an access-enabling code) to client agent device **1020**. Client agent device **1020** can then evaluate, based on the information, whether a user associated with the device is to be granted access to a resource. For example, a code can be evaluated for validity and applicability.

One or both of client agent device **1020** can identify stimulus data for the user device that identifies a stimulus or stimulus characteristic for presentation at the user device and/or for presentation at client agent device **1020** (so as to identify the particular user device). In instances where only one device identifies the stimulus or stimulus characteristic, the one device can transmit the stimulus, stimulus characteristic and/or identification thereof to the other device.

Stimulus data may or may not depend on a result of the evaluation of the code. In one instance, the stimulus data may be identified so as to facilitate variability in stimuli across user devices. For example, a pattern in a set of patterns can be pseudo-randomly selected or selected in an ordered manner.

The stimulus can be presented on client agent device **1020** along with an indication as to whether the code was determined to be valid and applicable. For example, a check mark can indicate that the code was determined to be valid and applicable, while an X can indicate that the code was determined to not be valid and applicable.

When an indication represents that a code is valid and applicable to a current circumstance, a client agent can identify a user device presenting a same, similar, corresponding or complementary stimulus and can then grant resource access to the user of the device. When an indication represents not valid and/or not applicable for a current circumstance, a client agent can identify a user device presenting a same, similar, corresponding or complementary stimulus and can then deny resource access to the user of the device.

This illustration exemplifies two security features of embodiments of the invention. First, the stimulus presentation that will ultimately be reviewed by a client agent can be delayed until a user is near the agent. This limits the time that the user may have to manipulate and/or review the stimulus. Second, the stimulus presentation can vary across user devices. Thus, even if a user manipulates her device to present a stimulus corresponding to an authorizing image on a friend's device, the client agent device would not detect the appropriate information from her device to generate the same image, and so a stimulus on the client agent device would not match the one on the user's device.

FIG. **11** illustrates a flowchart of an embodiment of a process **1100** for using device communication to enforce geofencing rules. Process **1100** can be performed in part or in its entirety by a user device.

Process **1100** begins at block **1105**, where one or more geofencing rules are accessed. Each of the one or more geofencing rules can be associated with, for example, a resource, a resource-associated location, a time period and/or a type of resource access. For example, the one or more geofencing rules can include those determined to be applicable to a particular user device given an access-enabling code associated with the device. The geofencing rule(s) can be defined in part or in full, for example, by an entity associated with a resource-associated structure, a performing act, a concession operation and/or a access management system.

Each geofencing rule can define a geofence and can identify an action consequence of being inside the geofence, being outside of the geofence, and/or crossing geofence (generally or in a particular direction). For example, a geofence can be defined as a perimeter, an area, a set of geographic coordinates, a distance from a point location, a functional distance (e.g., being inside the fence so long as the user device can communicate with a particular client device over a certain short-range communication channel, such as BLE or Bluetooth).

At block **1110**, a signal can be received from each of one or more client devices. The one or more client devices can include a device at a fixed location and/or a mobile device. Each of the one or more client devices can each be associated with a known location. For example, a map, table or other data structure identifying a location of each of the one or more client devices can be transmitted to and/or stored on the user device upon (for example) arriving at a resource location, validating an access-enabling code, passing of a time relative to a resource access time, etc. As another example, the signal received from a device of the one or more client devices can identify the location of the client device. Each signal can include a short-range signal such as a BLE signal.

At block **1115**, a location of the user device can be determined based on the signals. For example, the determination can include performing a triangulation technique based on a time delay and/or signal strength of each of the receives one or more signals. As another example, a user device location can be estimated to be a location of a client device of the one or more client devices for which a signal having a defined characteristic was received. To illustrate, a user device may receive signals from three client devices, and a location of the user device may be approximated to be a location of one of the three client devices corresponding to a signal having a shortest latency amongst the received three signals. The position can include estimated geographic coordinates, a section identifier, an intra-venue location or a location relative to one or more client devices or position features (e.g., 10 feet from Concession Stand #5).

At block **1120**, the device location can be used to determine whether the device is inside a geofence (or is outside a geofence or crossed a geofence). At block **1125**, one or more actions can be identified based on the geofencing rule(s) and determination. The action can include presentation of a stimulus, such as a visual stimulus, which can include an offer and/or information. For example, a geofencing rule can indicate that an offer is to be presented when a

user has crossed into a geofence or that navigation assistance is to be offered while a user is inside a geofence. At block **110**, the one or more actions are performed.

It will be appreciated that, as with all depicted and described processes herein, process **1100** is illustrative and modifications including fewer, additional and/or changed actions are contemplated. For example, block **1115** may be omitted from process **1100**, and a determination as to whether a device is within a geofence can be made based on whether the user device can communicate with a particular client device.

Specific details are given in the above description to provide a thorough understanding of the embodiments. However, it is understood that the embodiments can be practiced without these specific details. For example, circuits can be shown in block diagrams in order not to obscure the embodiments in unnecessary detail. In other instances, well-known circuits, processes, algorithms, structures, and techniques can be shown without unnecessary detail in order to avoid obscuring the embodiments.

Implementation of the techniques, blocks, steps and means described above can be done in various ways. For example, these techniques, blocks, steps and means can be implemented in hardware, software, or a combination thereof. For a hardware implementation, the processing units can be implemented within one or more application specific integrated circuits (ASICs), digital signal processors (DSPs), digital signal processing devices (DSPDs), programmable logic devices (PLDs), field programmable gate arrays (FPGAs), processors, controllers, micro-controllers, microprocessors, other electronic units designed to perform the functions described above, and/or a combination thereof.

Also, it is noted that the embodiments can 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 can describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of the operations can be re-arranged. A process is terminated when its operations are completed, but could have additional steps not included in the figure. A process can 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.

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

For a firmware and/or software implementation, the methodologies can be implemented with modules (e.g., procedures, functions, and so on) that perform the functions described herein. Any machine-readable medium tangibly embodying instructions can be used in implementing the methodologies described herein. For example, software codes can be stored in a memory. Memory can be implemented within the processor or external to the processor. As used herein the term "memory" refers to any type of long term, short term, volatile, nonvolatile, or other storage medium and is not to be limited to any particular type of memory or number of memories, or type of media upon which memory is stored.

Moreover, as disclosed herein, the term "storage medium", "storage" or "memory" can represent one or more memories for storing data, including read only memory (ROM), random access memory (RAM), magnetic RAM, core memory, magnetic disk storage mediums, optical storage mediums, flash memory devices and/or other machine readable mediums for storing information. The term "machine-readable medium" includes, but is not limited to portable or fixed storage devices, optical storage devices, wireless channels, and/or various other storage mediums capable of storing that contain or carry instruction(s) and/or data.

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. A system comprising:

an electronic user device comprising:

one or more transceivers for receiving signals, a transceiver of the one or more transceivers being configured to receive signals transmitted over a short-range connection;

a communication engine that detects a first wireless signal having been transmitted over the short-range connection by an electronic client device and having been received by the one or more transceivers at the electronic user device;

an access-right detection engine that:

in response to the detection of the first wireless signal having been transmitted over the short-range connection from the electronic client device, identifies a specification of a limited-access resource, the limited-access resource including an event; and

facilitates a query of a data store using the specification of the limited-access resource for an access-enabling code indicating that a ticket has been acquired to attend the event, the data store being configured to store, for each of one or more events, an access-enabling code indicating that a ticket has been acquired to attend the event;

an access-right evaluation engine that generates a second wireless signal to be transmitted by the one or more transceivers that includes:

a request for stimulus data; and

the access-enabling code; and

an interface engine that:

detects the stimulus data having been included in a third wireless signal received by the one or more transceivers; and

facilitates a presentation of a visual stimulus for visual confirmation of access to the limited-access resource, the visual stimulus:

being one of a set of different visual stimuli indicating that the access to the limited-access resource is to be granted; and

corresponding to the stimulus data; and

the electronic client device comprising:

one or more client-device transceivers that:

transmit the first wireless signal;

receive the second wireless signal that includes the request for stimulus data and the access-enabling code; and

transmit the third wireless signal that includes the stimulus data responsive to the request and to a determination that the received access-enabling code is proper; and

a client-device interface engine that facilitates a client-device presentation of a client-device visual stimulus that corresponds to the stimulus data, so that visual stimulus presented on the electronic user device and the visual stimulus presented on the electronic client device can be matched for confirmation for access of the limited-access resource.

2. The system as recited in claim **1**, wherein the client-device visual stimulus includes a concurrent representation of each of a plurality of visual stimuli, each of the visual stimuli corresponding to stimulus data having been transmitted from the electronic client device to a given user device.

3. The system as recited in claim **1**, wherein the stimulus data includes the visual stimulus.

4. The system as recited in claim **1**, wherein the second signal is transmitted to the electronic client device over the short-range connection and the third signal is signal is received from the electronic client device over the short-range connection.

5. The system as recited in claim **1**, wherein facilitating the presentation of the visual stimulus includes presenting the visual stimulus at the electronic user device.

6. The system as recited in claim **1**, wherein the stimulus data includes a characteristic that the visual stimulus is to have, and wherein each of the visual stimulus and the client-device visual stimulus has the characteristic.

7. The system as recited in claim **1**, wherein the short-range connection includes a Bluetooth Low Energy connection.

8. The system as recited in claim **1**, wherein the determination that the received access-enabling code is proper includes a determination that the access-enabling code is valid and applicable for permitting entry into a live event or a defined geographical region.

9. The system as recited in claim **1**, wherein facilitating the query of the data store using the specification of the limited-access resource includes transmitting a request for the access-enabling code to another device, the request for the access-enabling code including an identifier of the electronic user device, an identifier of a user account or an identifier of a user.

10. The system as recited in claim **1**, wherein the specification of the resource includes an identifier of the resource, an identifier of a client associated with the resource or a location associated with the resource.

11. A computer-implemented method for facilitating selective granting of resource access to authorized users based on short-range communication exchanges, the method comprising:

detecting, at an electronic user device, a first wireless signal transmitted over a short-range connection by an electronic client device;

in response to the detecting, identifying a specification of a limited-access resource, the limited-access resource including an event;

facilitating a query of a data store using the specification of the limited-access resource for an access-enabling code indicating that a ticket has been acquired to attend the event, the data store being configured to store, for each of one or more events, an access-enabling code indicating that a ticket has been acquired to attend the event;

transmitting, from the electronic user device, a second wireless signal that includes:

a request for stimulus data; and

the access-enabling code;

receiving, at the electronic user device, a third wireless signal that includes the stimulus data responsive to the request and to a determination that the received access-enabling code is proper;

facilitating a presentation of a visual stimulus on the electronic user device for visual confirmation of access to the limited-access resource, the visual stimulus:

being one of a set of different visual stimuli indicating that the access to the limited-access resource is to be granted; and

corresponding to the stimulus data; and

facilitating a client-device presentation of a client-device visual stimulus at the electronic client device that corresponds to the stimulus data so that visual stimulus presented on the electronic user device and the visual stimulus presented on the electronic client device can be matched for confirmation for access of the limited-access resource.

12. The computer-implemented method for facilitating selective granting of resource access to authorized users based on short-range communication exchanges as recited in claim **11**, wherein the stimulus data includes the visual stimulus.

13. The computer-implemented method for facilitating selective granting of resource access to authorized users based on short-range communication exchanges as recited in claim **11**, wherein the second signal is transmitted to the electronic client device over the short-range connection and the third signal is received from the electronic client device over the short-range connection.

14. The computer-implemented method for facilitating selective granting of resource access to authorized users based on short-range communication exchanges as recited in claim **11**, wherein the stimulus characteristic includes a background, texture or color that the visual stimulus is to have.

15. The computer-implemented method for facilitating selective granting of resource access to authorized users based on short-range communication exchanges as recited in claim **11**, wherein the short-range connection includes a Bluetooth Low Energy connection.

16. The computer-implemented method for facilitating selective granting of resource access to authorized users based on short-range communication exchanges as recited in claim **11**, wherein the determination that the received access-enabling code is proper includes a determination that the access-enabling code is valid and applicable for permitting entry into a live event or a defined geographical region.

17. The computer-implemented method for facilitating selective granting of resource access to authorized users based on short-range communication exchanges as recited in claim **11**, wherein the visual stimulus includes a dynamic stimulus that changes in time.

18. The computer-implemented method for facilitating selective granting of resource access to authorized users based on short-range communication exchanges as recited in claim **11**, wherein facilitating the query of the data store using the specification of the limited-access resource includes transmitting a request for the access-enabling code to another device, the request for the access-enabling code including an identifier of the electronic user device, an identifier of a user account or an identifier of a user.

19. The computer-implemented method for facilitating selective granting of resource access to authorized users based on short-range communication exchanges as recited in claim **11**, wherein the specification of the resource includes an identifier of the resource, an identifier of a client associated with the resource or a location associated with the resource.

* * * * *