(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
01 October 2020 (01.10.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/193577 A1

(51) International Patent Classification:
G01S 1/00 (2006.01) *G07C 9/28* (2020.01)
G01S 13/76 (2006.01) *G07C 9/29* (2020.01)
G07C 9/00 (2020.01) *H04W 12/06* (2009.01)
G07C 9/22 (2020.01) *H04W 4/02* (2018.01)

(21) International Application Number:
PCT/EP2020/058216

(22) International Filing Date:
24 March 2020 (24.03.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/823,341 25 March 2019 (25.03.2019) US

(71) Applicant: **ASSA ABLOY AB** [SE/SE]; Box 70340, 107 23 Stockholm (SE).

(72) Inventors: **FRANK, Hans Gunnar**; Lundagårdsvägen 20, 163 51 Spånga (SE). **STEFFL, Jan**; Na Stráni, 27301 Senomaty (CZ). **PREVOST, Sylvain Jacques**; 9808 Faith and Trust Cv, Austin, Texas 78717 (US). **JONSSON, Tomas Lars**; Fiskaruddsvägen 35, 144 62 Rönninge (SE). **EINBERG, Fredrik Carl Stefan**; Klyftvägen 8, 141 41 Huddinge (SE). **PIRCH, Hans-Juergen**; Dr. Blaasweg 15, 9560 Feldkirchen (AT).

(74) Agent: **SCHWEGMAN LUNDBERG WOESSNER LIMITED**; Hillington Park Innovation Centre, 1 Ainslie Road, Glasgow Strathclyde G52 4RU (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,

(54) Title: PHYSICAL ACCESS CONTROL SYSTEMS WITH LOCALIZATION-BASED INTENT DETECTION

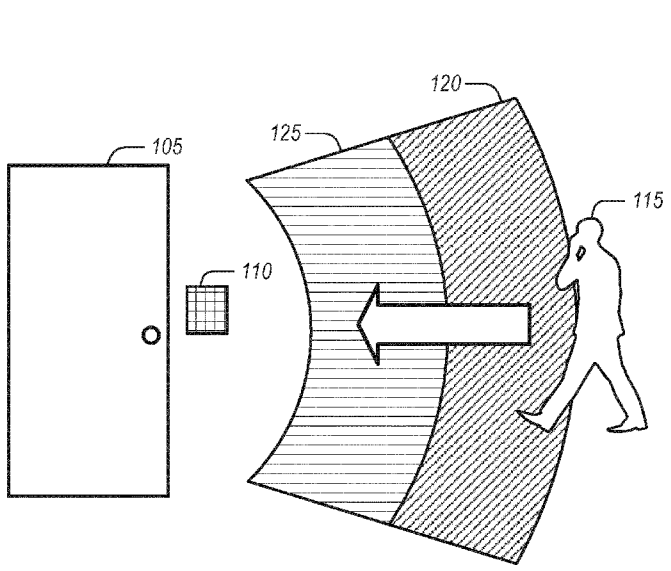

FIG. 1

(57) Abstract: Systems and techniques for a physical access control systems with localization-based intent detection are described herein. In an example, an access control system may regulate access to an asset. The access control system is adapted to receive a credential from a key device associated with a user using a first wireless connection. The access control system may be further adapted to verify the credential with a preliminary authentication for the asset. The access control system may be further adapted to establish a second wireless connection with the key device in response to verifying the credential with the preliminary authentication. The access control system may be adapted to determine an intent of the user to access the asset. The access control system may identify the credential includes a pattern in the preliminary authentication. The access control system may be further adapted to provide a command to grant access to the asset.

WO 2020/193577 A1

[Continued on next page]

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

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

Published:

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

PHYSICAL ACCESS CONTROL SYSTEMS WITH LOCALIZATION-BASED INTENT DETECTION

TECHNICAL FIELD

[0001] Embodiments described herein generally relate to physical access control systems and more specifically to physical access control systems having credential location detection capabilities.

BACKGROUND

[0002] Physical access to an area, such as through a doorway, may be controlled by an electronic physical access control system (PACS). A person may have a keycard or mobile device to provide their credentials to the PACS. The environment for the PACS may vary with the number of people that may be provided access and the number of entry points. For example, a building for a company may have a single point of entry which provides entry access for all employees. Within that building, there may be multiple offices and private meeting rooms which provide entry access for select employees. Another example may be a hotel which has many entry points for each room, but each room may only be accessed by a select individual.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] In the drawings, which are not necessarily drawn to scale, like numerals may describe similar components in different views. Like numerals having different letter suffixes may represent different instances of similar components. The drawings illustrate generally, by way of example, but not by way of limitation, various embodiments discussed in the present document.

[0004] FIG. 1 illustrates an example of a user interacting with a PACS, in accordance with some embodiments.

[0005] FIGS. 2A–2D illustrate an example for key devices interacting with the PACS, in accordance with some embodiments.

[0006] FIG. 3 illustrates an example of a person directly approaching three doorways, in accordance with some embodiments.

[0007] FIG. 4 illustrates an example of a person approaching three doorways, in accordance with some embodiments.

[0008] FIG. 5 illustrates a flowchart showing a technique for regulating access to an asset, in accordance with some embodiments.

[0009] FIG. 6 illustrates a flowchart showing a technique for regulating access to an asset using a key-device, in accordance with some embodiments.

[0010] FIG. 7 illustrates a flowchart showing a technique for regulating access to an asset, in accordance with some embodiments.

[0011] FIG. 8 illustrates a flowchart showing a technique for regulating access to an asset, in accordance with some embodiments.

[0012] FIG. 9 illustrates a flowchart showing a technique for regulating access to an asset, in accordance with some embodiments.

[0013] FIG. 10 illustrates a flowchart showing a technique for regulating access to an asset, in accordance with some embodiments.

[0014] FIG. 11 is a block diagram illustrating an example of a machine upon which one or more embodiments may be implemented.

DETAILED DESCRIPTION

[0015] When attempting to enter a secured area, a person may become frustrated by a delayed response between their approach to the entry point and the unlocking of the secure entry mechanism (e.g., an electronically controlled door lock). For example, an employee may pass through an entry point for a secure area multiple times a day. Additionally, in some conventional PACS, users may be required to physically present their credential (e.g., card/badge, or mobile device) to a reader located on the wall, which in some circumstances can inconvenience users or cause further unwanted delays, such as if the user's hands are full. As such, a PACS that is able to more easily and seamlessly identify the user (e.g., authenticate a user's permissions to end the secured area) can yield a more user-friendly and preferred experience. Further, users of an entry with a PACS may find benefit in a PACS that determines the intent of a user such that the PACS may perform preemptive

credential verification such that the secure entry mechanism may be unlocked as the user approaches the entry point.

[0016] In some cases, the systems and methods described herein can permit a seamless experience by obtaining or receiving a credential from the user without requiring the user to actively present the device containing the credential (e.g., card or mobile device). That is, in some cases, the systems and methods described herein can include the credential being automatically sent (e.g., without active input from the user) to the reader when the user approaches the reader.

[0017] In some cases, the systems and methods described herein can implement various approaches to detect intent of the user such that the entry point will open not only when the user with a proper credential is in a defined vicinity of the entry point, but also once it is adequately determined that the authenticated user intend to cross through the entry point. A challenge with performing preemptive credential verification may be identifying false positives which would result in releasing the secure entry mechanism when it should not be unlocked (e.g., false intent detection). This is potentially problematic as an unauthorized person may gain access to the entry. For example, an authorized person may be walking down a hallway and pass by a secure entry point. If the PACS were to mis-identify the person's approach to the secure entry point, the PACS may unlock the secure entry mechanism. The person may pass by the door while another person may enter through the secure entry point while the secure entry mechanism is unlocked.

[0018] Wireless PACS may have generally used wireless communication technologies such as near field communications (NFC) such as radio-frequency identification (RFID) and personal area network (PAN) technologies, such as the IEEE 802.15.1 and Bluetooth Low Energy (BLE). These technologies may have drawbacks for a seamless user experience and entry. For example, the range of NFC is limited, such that a credential exchange typically does not occur until the user attempts to gain access (e.g., standing in front of the door, holding a keycard against the reader). The credential transfer to the reader and response by the host server may take several seconds, which results in a frustrating user experience. Further, the user generally may be required to remove the keycard or access device

from their pocket, for example, and place it on or very near the reader for the process to begin.

[0019] BLE devices have a range of tens of meters (e.g., ten to twenty meters). Thus, credential exchange may be performed as the user approaches the reader. PAN standards may feature secure handshaking, encryption, and favorable energy profiles for discovery and data transmission. However, PAN standards do not offer accurate physical tracking of devices (e.g., ranging, positioning). Thus, it may be difficult for the reader to determine whether the inter of the user is to actually gain access to the secure area without any additional evidence of intent. Additional evidence of intent may include touching a door handle and gesturing with the key-device. However, this may still be a less than ideal user experience compared to a user simply walking up to the reader and gaining access to the secured area.

[0020] Ultra-wideband (UWB) wireless communication protocols may be used for communication by encoding data via time modulation (e.g., pulse-position encoding). With UWB, symbols are specified by pulses on a subset of time units out of a set of available time units. Other examples of UWB encodings may include amplitude modulation and polarity modulation. The wide band transmission tends to be more robust to multipath fading than carrier-based transmission techniques. Further, the lower power of pulses at any given frequency tend to reduce interference with carrier-based communication techniques.

[0021] UWB may be used in radar operations and provide localization accuracies on a scale of tens of centimeters. Due to the possibility of variable absorption and reflection of different frequencies in a pulse, both surface and obstructed (e.g., covered) features of an object may be detected. In some cases, the localization may provide an angle of incidence, in addition to providing a range or distance.

[0022] Physical access control may include a range of systems and methods for governing access, for example by people, to secure areas. Physical access control may include identification of authorized users or devices (e.g., vehicles, drones) and actuation of a gate, door, or other facility used to secure an area. PACS may include a reader (e.g., an online or offline reader) that holds authorization data and may be capable of determining whether the credentials provided are authorized for an

actuator (e.g., door lock, door opener, turning off an alarm). An online reader or system may include a system which is connected to a network or the Internet for determining authorization. An offline reader or system may be a self-contained system which does not connect to any outside resources. For example, a PACS for a residential home may be offline.

[0023] PACS may include a host server to which readers and actuators (e.g., via a controller) are connected in a centrally managed configuration. In centrally managed configurations, readers may obtain credentials from key devices (e.g., a radio frequency identification (RFID) chip in a card, a fob, or a personal electronic device such as a mobile phone) and pass those credentials to the PACS host server. The host server may determine whether the credentials authorize access to the secure area and commands the actuator accordingly.

[0024] To address the issues with identifying intent, localization techniques (e.g., using secure UWB ranging) may be combined with PAN discovery and the key exchange. The key-device and the reader may coordinate secure ranging using a PAN technology. This may include the reader providing a secret (e.g., a scrambled time stamp (STS)) that is used to mark ranging messages to prevent spoofing. The key-device may provide the credentials during same PAN session in which the secret was shared. The reader may decrypt or otherwise prepare the credentials as it would normally do except that the credentials are cached until an intent trigger occurs.

[0025] The reader may use UWB to physically locate the key-device. In some examples, the UWB is activated after the secret is shared to conserve energy, which may be useful for battery powered readers or key-devices.

[0026] Identifying a physical location of a key-device with UWB may be more accurate than other techniques and may be accurate to the tens of centimeters, providing both range and direction to the reader. This accuracy surpasses the roughly ten-meter accuracy of PAN when readers are not coordinated. The precision of UWB accuracy may provide details needed for user intent determinations. For example, several zones may be defined, such as different ranges of distance from the reader, to provide different contexts for understanding

user intent. Moreover, the accuracy of the tracking enables an accurate model of user motion from which intent may be discerned. Thus, the reader may categorize user motion as likely approaching the reader, or simply walking past.

[0027] An intent threshold or intent trigger may be in place, where once the likelihood of the intent exceeds the intent threshold, the intent trigger may activate a series of events, such as having the reader act on the cached credentials. For an offline reader, the reader may control the actuator (e.g., a lock on a disconnected door lock). In a centrally managed PACS, the reader may forward the credentials to the host server to act upon (e.g., sending credentials to a controller to make a determination and further actuate a door lock, as appropriate).

[0028] The systems and methods described herein may be implemented so that a first transmission or exchange with a key-device via a communication protocol with longer range capabilities, or in some cases with less accuracy (e.g., BLE, Wi-Fi), may be used to provide a user's credentials to a reader. Those credentials may be stored in a cached location within the reader until and unless, in a second transmission or exchange with the key-device via a communication protocol with increased accuracy and precision (e.g., UWB), it is determined that the user indeed intends to enter the secured area (e.g., open the door at which the reader is installed). Once the user's intent is determined, the reader may then release the credential (sometimes referred to as PACS bits) for processing, such as sending the credential to a controller to determine the user's access permissions, or to directly unlock the door (e.g., in an offline reader). This two-step authentication sequence may reduce computational time that may lead to delays in the door opening for a user (also referred to as latency). With this approach, the authentication and communication between the reader and the key device is effectively already performed by the time the system has determined that the user does intend to enter the door and the user reaches the door.

[0029] In some embodiments, if the intent trigger does not occur within a time-period, or an anti-intent trigger occurs—such as moving away from the reader—the cached credentials may be cleared. This may be performed as many credentials may be cached in the reader, but potentially a smaller subset of the cached credentials

may actually be used in an authentication process (e.g., based on later predicted intent).

[0030] In some embodiments, if the reader has identified whether or not the credentials provide access to the secured area, such as with an offline reader, the credentials are not cached if it is determined the credentials do not provide access to the secured area. Additionally, the UWB localization may not be activated.

[0031] In some embodiments, the reader may include persistent authentication of the credential. The persistency may be based on a timeout value. The amount of time the credential is stored, or its persistency, is dependent on the timeout value. If the timeout is quite long, the need for re-exchanging PAN credentials is reduced.

[0032] For example, a key device is within PAN range to the reader. The reader may cache the PACS ID (e.g., 26bit PACS for legacy systems) read from the credential provided by the key device. A seed to a time-based one-time password (TOTP) technique is generated by the reader and shared via PAN to the key device. The UWB ranging received from the key device comprises a TOPT that the reader verifies. If UWB ranges the key device close enough (within some meters) to the reader or other target (e.g., center of a door), the reader transmits the cached PACS ID to the host server. The host server triggers the door opening. The reader may then delete the cached PACS ID. Instead, if the UWB does not range the key device after some timeout (e.g., 5 min), the TOTP is invalid. The key device then has to connect to the reader to get a new TOTP. Additionally, after some authentication timeout (e.g., some hours), the PAN authentication may expire.

[0033] When using secure UWB localization, in order to effectively function in the system, any reader involved may require a seed or secret for secure ranging, such as STS. For example, if several readers may be connected (e.g., via BLE, a mesh network, etc.) to distribute the same secret across all participating readers. This potentially reduces the need for exchanging STS between each reader and key device. Further, this shared exchange may exchange the cached PACS IDs to all readers—e.g., from the one initial reader to which the key device connected. By doing so, one credential and STS exchange is needed for each key device.

[0034] A coordinated PACS may use a gateway device to coordinate several readers within a PACS, whether it is centrally managed or offline. The readers may operate as remote radio heads to the gateway, with the gateway performing the credential caching, intent determination, and credential forwarding to the host server or commanding the actuator to operate. A coordinated PACS facilitates UWB positioning of key devices with one or more of the connected readers. In some examples, the gateway may load balance UWB localization responsibilities. This may be helpful in dense key device scenarios, such as at ticketing speed-gates.

[0035] In some embodiments, the credentials being sent to a reader may include encoded or cryptographic information, such as SEOS® credentials by HID Global, MIFARE® DESFire® credentials by NXP, or FeliCa™ credentials by Sony stored in or on the key-device. The reader may decrypt or obtain various information from the credential received from the key-device and provide that information to the access server (e.g., controller) to determine permissions for the user, such as access permissions. In some cases, a reader may decrypt a credential and obtain access control identification information about the user (e.g., PACS bits), and send those to the controller to determine if the user has permission to access the controlled area or system for which they are attempting to gain access.

[0036] FIG. 1 illustrates an example 100 of a user interacting with a PACS, in accordance with some embodiments. A doorway 105 may be secured with an electronic lock that is controlled through a PACS. The PACS uses a reader 110 for receiving credentials from a user 115 that desires to enter the doorway 105.

[0037] As the user 115 approaches the doorway 105 and reader 110, a first wireless communication 120 communicates with a key device of the user 115. The first wireless communication 120 may be a low power communication such as BLE. The first wireless communication 120 may have capabilities to communicate with a key device at a greater distance, but may not be able to perform localization and ranging of the key device. Using the first wireless communication 120, the reader 110 may receive credentials and other identifying information from the key device. The reader 110 may cache the credentials or may transmit the credentials to a

verification system of the PACS that may determine if the user 115 may enter the doorway 105.

[0038] As the user 115 continues to approach the doorway 105 and reader 110, a second wireless communication 125 begins communicating with the key device of the user 115. The second wireless communication 125 may be a higher power and advanced communication, such as UWB. The second wireless communication 125 may include localization and ranging to track the movement of the user 115. The second wireless communication 125 may track the user 115 and use factors such as the speed the user 115 is moving to determine if the intent of the user 115 is to enter the doorway 105. For example, if a user 115 is not intending to enter the doorway 115, then their speed may remain constant. Conversely, if the intent of the user 115 is the enter the doorway 105, then the user 115 may slow their pace as they approach the doorway 105 and reach for the door handle.

[0039] The PACS may use the data received from the reader 110 using the second wireless communication 125 to determine the likelihood or probability the user 115 is intending to pass through the doorway 105. The determination may be a calculation using the received data or the received data may be provided to a fixed or evolutive model. If the determined probability of intent exceeds a predetermined threshold, then the PACS may unlock the door such that the user 115 may seamlessly enter the doorway 105. The threshold may vary depending on how precise the probability determination is and how secure the doorway 105 may need to be. For example, a meeting room may have a threshold of 50% intent probability as there is no risk if it is unlocked for a false positive. However, a door for a laboratory for new product development may have a threshold of 90% for intent probability. Furthermore, using the system available user credential to associate additional information, such as but not limited to, access rights and access history, the threshold could be modulated per user.

[0040] FIGS. 2A–2D illustrate an example 200 for key devices interacting with the PACS, in accordance with some embodiments. The example 200 of the PACS includes a doorway 205 that is secured with a reader 210 and a lock 215. The reader includes a cache 220 for storing credentials and other data received from key

devices. The reader 210 communicates with access control 225. Access control 225 may be a server that is connected to a local internal network. Access control 225 may be remote systems connected through the internet for governing access to multiple locations.

[0041] In FIG. 2A, key device A 230, key device B 235, and key device C 240 come within a BLE range (as an example of a low energy wireless communication) of the reader 210. In establishing the connection with the reader 210, each of key device A 230, key device B 235, and key device C 240 provide a credential to the reader 210.

[0042] In FIG. 2B, the reader 210 may perform preliminary authentication of the credentials. For example, the reader 210 may include a blacklist or a white list to make an immediate decision about tracking a key device. Using UWB for ranging and localization provides additional information about the movement of the key device, but also is requires more energy. Thus, it is advantageous if a determination may be made if a key device should be tracked or not. In the example 200 of FIG. 2B, the reader 210 determines that key device B 235 does not have the credentials to access doorway 205. Thus, the reader 210 does not range key device B 235 with UWB as key device B 235 would not be permitted to access doorway 205.

[0043] In some embodiments, the reader 210 may transmit the credential to the access control 225 for authorization. If the access control 225 determines that the credential associated with a key device is authorized for entry to the doorway 205 associated with reader 210, access control 225 may provide a token to the reader 210 for that credential. The reader 210 may store each token with their respective credential. Similarly, in this embodiment, if the reader 210 does not receive a token, then the credential is removed and the key device, such as key device B 235, is not tracked.

[0044] In some embodiments, the reader 210 may cache the credential when first received through BLE. The reader 210 may hold the credential in the cache until ranging occurs using UWB. Once the key device is within a certain range, the reader 210 may release the credential for authentication by access control 225 or an authentication server.

[0045] In FIG. 2C, key device A 230 and key device C 240 have moved closer to the reader 210 and UWB may be used for communication. With UWB, localization or ranging is possible. Location information for key device A 230 and key device C 240 is provided to reader 210. The location information may be used determine the intent of the person with each respective key device. The location information may be derived from UWB, such as by performing range detection.

[0046] In FIG. 2D, key device A 230 and key device C 240 continue to move and the location information of their respective movement is provided to the reader 210 through the UWB communication. Key device C 240 moves away from the reader 210, and thus the determined intent of key device C 240 entering the doorway 205 is low. The reader 210 may continue tracking key device C 240 until it is out of range. The reader 210 may be battery conscious and hardware conscious to monitor the how power and processing is used. This may include discarding credentials from the cache as soon as it is determined the credential is no longer needed, such as if the intent drops below a threshold value. Managing the credentials stored in the cache based on a confidence or intent for the person accessing the entry point may be essential for a PACS that manages a set of entry gates, such as a bank of turnstiles. This type of entry point may receive a large number of credentials at certain times, such as the entry for a subway or sporting arena.

[0047] Key device A 230 continues to approach the doorway 205, and thus the intent is high that key device A 230 will access the doorway 205. The reader 210 may release the token for key device A 230 to the access control 225. When access control 225 receives the token, access control 225 may transmit a command to the door lock 215 to unlock so that the person holding key device A 230 may enter doorway 205 with ease and no delay. If a token has not been provided, the reader may send the credential for key device A 230 to access control 225 to unlock the door lock 215. For an offline system, reader 210 may have direct control of door lock 215 and send the command directly to door lock 215 to unlock.

[0048] Many factors may be used to determine when the reader 210 should transmit the release, such as transmitting the token, to access control 225. If the doorway 205 is for a secure area, then the determined intent, or probability for

accessing the doorway 205, may need to be very high, and thus have a high threshold, so that the doorway 205 is not inadvertently opened. Other factors, such as a frequency with which the person accesses the doorway 205 or known contextual data, such as a meeting that is about to start in the room of the doorway 205 may contribute to determining the threshold for intent.

[0049] For security, the reader 210 may generate session keys for communication with a key device, such as key device A 230. Each side, such as the reader 210 and key device A 230 may have a counter. This counter may be hashed as part of the session key. To track the movement of key device A 230, the reader 210 is continually communicating with the key device A 230 to determine the distance. With each communication, the reader 210 or key device A 230 may respectively increase the count for the hashed counter. The session key is then changed with each communication to prevent malicious attacks while the reader 210 and key device A 230 may continually communicate as each is aware of what the count should be and can decipher the hash.

[0050] Identifying the intent of entering a doorway by a person may be used to expedite the process of authenticating credentials and unlocking the doorway such that the person is not hindered by the process and is presented with what appears to be a seamless transition. The previous discussions have focused on identifying an intent for a single doorway. Challenges arise for identifying the intent when multiple doorways and multiple readers are present, as found in the examples of FIGS. 3 and 4.

[0051] FIG. 3 illustrates an example 300 of a person 335 directly approaching three doorways, in accordance with some embodiments. A person 335 may approach a set of doorways that are directly in front of them. For each of doorway 305, doorway 315, and doorway 325 it may be difficult for the respective reader 310, reader 320, and reader 330 to identify which doorway the person 335 is intending to enter. For example, if reader 310, reader 320, and reader 330 are using ranging alone, the person 335 would be within relatively the same range of reach reader. Identifying the location of the person 335 and performing continuous localization of the person 335 (through their key device), may provide a direction

the person 335 is moving. Using the determined direction, the readers may identify an angle of arrival 340. The angle of arrival 340 may be used to determine which doorway of multiple doorways that the person 335 is intending to enter.

[0052] FIG. 4 illustrates an example 400 of a person 435 approaching three doorways, in accordance with some embodiments. A person 435 may approach a set of doorways that may be to a side of the person 435, such as if the person 435 were walking down a hallway in an office building. For each of doorway 405, doorway 415, and doorway 425 it may be difficult for the respective reader 410, reader 420, and reader 430 to identify which doorway the person 335 is intending to enter. While the person 435 is at different distances from each of reader 410, reader 420, and reader 430, the person 435 could stop at anyone of the doorways.

[0053] As the person 435 moves down the hallway and passes a reader, such as passing reader 430 in example 400, then doorway 425 may be immediately removed from the possible doorways of intent. This may free the cache for reader 430 and change the probability for the person 435 intending to enter doorway 405 or doorway 415.

[0054] The PACS may attempt to monitor the speed with which person 435 is moving. The speed with which a person moves in such a scenario may be relatively constant until just before the person reaches their intended doorway, at which time their pace slows. This type of movement information may be used to identify the intended doorway. A neural network may be trained with movement data of how people move down a hallway and how their movement changes in relation to the doorway they enter. The neural network may be used with the PACS and the location data provided by the readers through UWB to identify the intended doorway.

[0055] In example 400, the PACS may use contextual data to identify the intended doorway. For example, the PACS may have access to the calendar system of a company. The PACS may identify a meeting is about to begin in the room corresponding to doorway 415. Thus, while the intended doorway of person 435 is indeterminable by movement alone, using the calendar, the PACS may determine the intent of person 435 is to enter doorway 415. The accuracy of the intent may be

further improved if the PACS has access to the individuals that are invited to the meeting and then cross references the identification of person 435 (from their key device) with the list of invitees.

[0056] Another scenario of this example may be if doorway 405, doorway 415, and doorway 425 with reader 410, reader 420, and reader 430 were a hallway of a hotel. Identifying the intent of a guest may be less trivial as the guest would have credentials which only correspond to one doorway. Thus, as the guest walked down the hotel hallway the PACS of the hotel may anticipate the intent of the guest even before the guest is within range of the reader for their room, as the PACS may identify that there is only one doorway/room for which the guest has credentials to access.

[0057] The PACS may access communication systems such as email, instant messaging, and short message service (SMS) that may provide information used to determine the doorway a person intends to enter. For example, if John sends Bob an instant message asking Bob to meet John in Laboratory B, then when Bob approaches the doorways for the laboratories, the PACS may recognize that Bob intends to enter Laboratory B based on the request from John.

[0058] Different types of doorways or entry points may alter how the intent is utilized and when the readers transmits the release to the access control system. For example, the entry point may be a turnstile and if there is a large bank of turnstiles, then identifying the intended turnstile may not occur until the person has stepped into the turnstile. Types of doorways or entry points may include a manual lock, an automated lock, a manual door, an automated door, a turnstile, a transit speedgate, a parking gate, or an elevator.

[0059] The timing of the release of credentials and unlocking of the doorway may be determined by the data received through the ranging and localization performed through UWB. The intent may be altered by radii of distance from the reader. Different entry environments may alter this timing. For example, an open area of an office with multiple secured doorways may result in waiting until the key device is at a particular doorway before the release occurs as a high enough probability of intent is not able to be determined because of the multiple secured doorways.

Conversely, the front door lock of a home may be released well before a person the front door reaches it as there would be no other door that person has access.

[0060] The key device may be a mobile device, such as a smart phone or tablet. Devices such as a smart phone include different types of sensors that may provide information to the PACS. As the key device communicates with the reader and the PACS through the BLE and UWB wireless connections, data collected from the sensors on the key device may be transmitted to the reader and PACS. The key device may include sensors such as a gyroscope, accelerometer, barometer, global positioning system (GPS), microphone, and camera. The key device may collect information from communication protocols such as Wi-Fi and BLE. Data provided from these sensors and communication protocols may be used to determine the relative location, motion, and speed of the key device.

[0061] The sensor data may provide information for determining the intent of the person with the key device. For example, the PACS may determine that the key device is approaching a doorway quickly. Using the data provided from the gyroscope and accelerometer, the PACS may identify that the person is running. Based on the determination the person is running, different actions may be taken. In one scenario, if there is only one doorway that the person has credentials to access, then the PACS may unlock the door sooner as the person will reach the door faster than if they were walking. In another scenario, if the person has credentials for multiple meeting rooms, but using the calendar system the PACS identifies that a meeting started 10 minutes ago in one of the meeting rooms, the PACS may determine that meeting room is the intended destination based on the person running.

[0062] Data stored in the mobile device and data of the current functioning of the mobile device may be communicated to the PACS and used to determine intent. If the PACS is not connected to a calendar system, then the mobile device may provide information from the calendar or reminders in the mobile device. For example, a person that lives in an apartment building may share childcare responsibilities with another tenant and each has access to the other's apartment. The person may have a reminder to pick up the other tenant's child for school,

which is used to identify the intent that the person will enter the other tenant's apartment.

[0063] The current functioning of the mobile device may be communicated to the PACS, such as if the person is talking on the mobile device or playing a game. For example, if a person is walking down a hallway while playing a game on their mobile device, it may be determined that an intent to enter a meeting room is low.

[0064] Cameras, noise sensors (microphones), and environmental sensors such as thermometers and barometers may be used to provide information for the PACS to identify intent. For example, a camera may be used to assist in identifying which turnstile a user intends to enter. The temperature outside may affect the paths or habits of users. For example, if two doorways are near each other, but one leads outside, the PACS may determine the outside doorway is likely to be the intended doorway if it is currently freezing outside.

[0065] The PACS may be connected to additional systems that may not require a key device to access but provide indications of actions by a person that may subsequently be attempting to gain entry to a doorway controlled by PACS. This may include Internet-of-Things (IoT) devices. Examples of devices and systems that a person may interact with which could provide intent indications and behavior patters to the PACS may include garage door opener, thermostat, smart lighting, television, and appliances.

[0066] The PACS may use a neural network that is trained with user habits to anticipate and identify the intent of a user accessing a doorway. This may include identifying different actions or connections a user may be performing, such as with their mobile device. For example, an office may have a gym for people to use. Tara may walk by the door and reader to the gym multiple times a day as part of her normal workday. However, when Tara does use the gym, she usually is listening to music with her Bluetooth ear buds. The PACS neural network may use this data to identify that Tara typically intends to enter the gym when she is using her ear buds, but otherwise the intent to enter is very low.

[0067] The PACS neural network may be trained with the habits of each user to identify common user actions and sequences of actions that may be used to identify

intended doorways and points of entry. For example, a typical day for a person may include entering a building access point, entering an access point for their floor, and then accessing a secure room. Some of these access point may have multiple options, such as the floor may have different doors for different tenants. The habit data may include other data to identify changes to the habit. For example, the previously described habit may be for when the person reaches the office in the morning. However, at lunch time, the person may return with lunch and go to the lunch room which is through a different doorway on the floor.

[0068] The trained neural network may be used to identify the intent of unknown or new users. For example, a new employee may begin working and thus specific habit data does not exist for the employee. The PACS neural network identifies that the employee works in accounting and thus uses the trained data for other accounting employees to identify the intent of the new employee.

[0069] The PACS may receive data about other applications and functions the user performs with their mobile device. For example, the user may have Wi-Fi connected lights in an office or meeting room. The user may turn the lights on with their mobile device before they reach the doorway to such a room. The PACS may use this action data to identify that the user intends to enter the room.

[0070] The PACS neural network may combine multiple factors to identify the intent of a person to enter a doorway and the timing with which to release the credentials for entering a doorway. For example, determining that a user's normal routine may be affected by the temperature.

[0071] The reader may perform a preliminary authentication when the credential is received by BLE to identify if the credential provided by the key device should be authenticated and if any further communication should occur with the key device, such as ranging with UWB. If the reader is able to determine with a broad verification that the credential provided will not authenticate, then the power and processing cost of using UWB to range the key device is eliminated.

[0072] The preliminary authentication may be performed using blacklists or whitelists. The blacklists and whitelists may have conditional factors, such as a time condition. For example, a building may restrict access during the night and

thus from 8:00 PM to 6:00 AM a whitelist is used that only includes security and maintenance.

[0073] The preliminary authentication may be performed through regular expression matching and similar pattern identification. The reader may receive a credential through the BLE communication with a key device. The reader, using a regular expression for the format sequence of a credential which is accepted at that reader for entry, may identify if the received credential is of the correct format sequence. If not, then the reader may discard the credential and cease communication with the key device. As an example, the credentials accepted by the reader for entry may be of a format sequence of the letter "K" followed by six numeric digits. If the credential provided is of a format sequence of the letters "WX" followed by seven numeric digits then the reader may dismiss the credential and not cache or authenticate it, including ceasing any communication or ranging to save power and processing.

[0074] The PACS may initiate additional precautions for accessing a secure doorway based on the people near the person attempting access to the doorway, such as to prevent tailgaters (e.g., a person that attempts to gain access by following an authorized person). If the PACS identifies unauthorized key devices near an authorized key device, this may increase the threshold for identifying intent, as well as only unlocking the doorway when the authorized key device is very close to the doorway. The same may be applied if a camera were used with the PACS and there are persons without key devices near a person with an authorized key device.

[0075] FIG. 5 illustrates a flowchart showing a technique 500 for regulating access to an asset, in accordance with some embodiments. The technique 500 may be used to regulate access to an asset where the asset is a physical location, such as a room, a building, or a home. The technique 500 may be used to regulate access to an asset where the asset is an electronic device, such as a computer, a computer network, a smartphone, or a specific device such as an automatic teller machine.

[0076] The technique 500 includes an operation 502 to establish a first connection with a key-device, such as a connection between the key-device and a reader. The first connection may be an NFC such as RFID or PAN technologies,

such as the IEEE 802.15.1, Wi-Fi, or BLE. The key-device may a physical card with an integrated circuit which stores information such as credentials and information about the holder of the key-device. The key-device may be a mobile device, such as a smartphone. The mobile device may include an application for interfacing with the reader or include secure elements.

[0077] The technique 500 includes an operation 504 to receive a credential for a user over the first connection. Upon establishing the first connection between the reader and the key-device, the key device may transmit a credential, such as a credential for a user, to the reader. The technique 500 may include an operation to store the credential in cache memory of the reader. The credential may be stored in other memory or transmitted to another computer system for storage in the respective memory of the system.

[0078] The technique 500 includes an operation 506 to establish a second connection with the key-device. The second connection may be UWB. The technique 500 may include an operation to maintain a location or position of the key-device using the second connection. The location or position may be determined using range detection. The operation of establishing the second connection with key-device may occur based on the interaction of the key-device using the first connection.

[0079] The technique 500 may include an operation to authenticate the credential for the user associated with the credential to access the asset. Authenticating may include transmitting the credential to authentication authority. The technique 500 may include an operation to receive a validation indication from the authentication service and thus permit access to the asset.

[0080] The technique 500 includes an operation 508 to provide the credential to an access controller. Providing the credential to the access controller may include an operation to transfer the credential from the cache memory. Providing the credential to the access controller may be based on determining the user intends to access the asset. The access controller may include a physical access control system controller.

[0081] The technique 500 may, in determining the user intends to access the asset, include an operation to determine a set of location points of the key-device using the second connection. The location points may be locations, positions, or ranges from the reader detected through UWB. The technique 500 may include an operation to calculate a probability the user will access the asset using the set of location points. The technique 500 may include an operation to determine the probability exceeds a predetermined threshold. Depending on the asset and the type of security access, the threshold may be adjusted, thus a high probability threshold may be in place for more secure assets and a low probability threshold may be in place for less secure assets.

[0082] The technique 500 may include an operation to receive a validation indication from the access controller and permit access to the asset. For example, the credential may be validated that the user may access the asset. The asset may be doorway or secure entry point, or the asset may be an electronic device.

[0083] The technique 500 may include an operation to remove the credential from the cache memory. Removing the credential from the cache memory may be based on receiving an indication the user is not permitted to access the asset. For example, the credential may not be validated, and the reader may receive an indication that the user may not access the asset. Removing the credential from the cache memory may be based on losing the second connection with the key-device. For example, if the key-device moves out of range of the second connection, this may indicate that the key-device (and the user) are no longer near the reader and thus the intent to access the asset is low and thus the credential is removed from the cache memory. Removing the credential from the cache memory may be based on an elapsing of a predetermined time. For example, from the time the second connection is established, if the key-device is not used to access the asset within a predetermined time period, then the credential may be removed from the cache memory. This may be performed to save memory and resources. The user may be required to perform an action, such as placing the key-device on the reader, to transfer the credential again and attempt to access the asset.

[0084] FIG. 6 illustrates a flowchart showing a technique 600 for regulating access to an asset using a key-device, in accordance with some embodiments. The technique 600 may be used to regulate access to an asset where the asset is a physical location, such as a room, a building, or a home. The technique 600 may be used to regulate access to an asset where the asset is an electronic device, such as a computer, a computer network, or a smartphone.

[0085] The technique 600 includes, upon the key-device entering a first connection range, an operation 502 to establish a first connection between the key-device and a reader. The first connection may be a PAN such as through BLE. The technique 600 includes an operation 604 to provide, from the key-device, a credential associated with a user to the reader using the first connection.

[0086] The technique 600 includes an operation 606 to establish a second connection between the key-device and the reader. The second connection may be UWB. The second connection is based on the key-device entering a second connection range. For example, UWB does not have as large a range as BLE. The key-device may first establish a connection with the reader through BLE. As the key-device moves closer to the reader and is within UWB range, the key-device and the reader may establish a second connection over UWB. Through UWB, the range or location of the key-device may be determined.

[0087] The technique 600 includes an operation 608 to provide, from the reader, the credential to an authorization service. The reader may transmit the credential to receive authorization for the user of the key-device to access the asset. The technique 600 includes an operation 610 to receive, at the reader, validation of the credential from the authorization service. If the credential does not have permission to access the asset, the reader may receive a denial from the authorization service.

[0088] The technique 600 includes an operation 612 to transmit, from the reader, a command, to an access controller, to grant access to the asset. This may be a command to unlock a doorway or a command to unlock an electronic device for use. Providing the credential to the access controller may be based on determining the user intends to access the asset. The technique 600 may include, in determining the user intends to access the asset, an operation to determine, at the reader, a set of

location points of the key-device using the second connection. This may be performed through range detection using UWB. The technique 600 may include an operation to calculate a probability the user will access the asset using the set of location points and determine the probability exceeds a predetermined threshold.

[0089] Determining the user intends to access the asset may be based in part on sensor data collected from a sensor of the key-device. For example, a GPS of the key-device may provide location information or an accelerometer of the key-device may provide movement information, such as that the user is running.

[0090] FIG. 7 illustrates a flowchart showing a technique 700 for regulating access to an asset, in accordance with some embodiments. The technique 700 includes an operation 702 to receive a first message from a wireless key device associated with a user using a first wireless connection. The PACS may receive the first message at a reader for a secure entry point. The first message may include a user credential. The first wireless connection may be an NFC such as RFID or PAN technologies, such as the IEEE 802.15.1 and BLE.

[0091] The technique 700 includes an operation 704 to receive a set of messages from the wireless key device using a second wireless connection. The second wireless connection may be UWB. The set of messages may be a series of communications back and forth between the reader and the key device. The communications may include a seed or hashed counter to provide security and prevent spoofing of the key device.

[0092] The technique 700 includes an operation 706 to identify a set of location points of the wireless key device for the set of messages using the second wireless connection. Using a communication technology such as UWB, the PACS may identify locations of the key device or ranges of the key device to the reader or a plurality of readers.

[0093] The technique 700 includes an operation 708 to determine the user intends to physically access a secure entry point based on the set of location points. The secure entry point may be one of a plurality of secure entry points within range of the second wireless connection. The technique 700 includes a further operation to determine the user intends to physically access the secure entry point from the

plurality of secure entry points based on calculating a trajectory from the set of location points.

[0094] The technique 700 includes a further operation to calculate a probability the user will physically access the secure entry point using the set of location points and determine the probability exceeds a predetermined threshold. For example, the reader may identify multiple radii of ranges from the reader. For each progressively closer range the key device is determined to be within, the probability may increase. If the key device is determined to stop within one of the ranges or if the key device returns to a further range, then the probability may decrease. A predetermined threshold may be used to identify when the probability, or intent, is high enough that the secure entry point should be released. The threshold may be dependent on factors such as the level of security for the area being accessed (i.e., meeting room or development laboratory), the number of other entry points nearby, and frequency of the particular key device accessing the secure entry point.

[0095] The technique 700 includes an operation 710 to transmit a command to unlock the secure entry point. There are many types of secure entry points, such as doorways, turnstiles, pass through gates, elevators, and parking arms. To unlock the secure entry point includes any applicable method for the type of secure entry point which would provide for the restricted access to become unrestricted to the holder of the key device.

[0096] The technique 700 includes a further operation to transmit the credential to an authorization service. The authorization service may be local to the reader, such as in a residential home. The authorization service may be connected to the reader through a network or the Internet to provide credential authorization to multiple locations or entry points. The authorization service may be integrated into the reader. The technique 700 includes a further operation to receive an indication the user is authorized to access the secure entry point from the authorization service. The authorization service may validate the credential and return an indication to the reader that the holder of the credential is authorized or not authorized to enter the secure entry point.

[0097] FIG. 8 illustrates a flowchart showing a technique 800 for regulating access to an asset, in accordance with some embodiments. The technique 800 includes an operation 802 to receive a credential from a key device associated with a user using a first wireless connection. The first wireless connection may be an NFC such as RFID or PAN technologies, such as the IEEE 802.15.1 and BLE.

[0098] The technique 800 includes an operation 804 to verify the credential with a preliminary authentication for the asset. The preliminary authentication may take place at the reader or device local to the reader. The preliminary authentication may include identifying that the credential includes a pattern using pattern matching. The pattern may be defined using a regular expression. The technique 800 includes an operation to verify the credential with the preliminary authentication by comparing the credential to a whitelist of credentials. The whitelist may be applied in the preliminary authentication based on time of day. For example, the whitelist may identify a group of people which are permitted to enter an office building at night and on the weekend.

[0099] The technique 800 includes, in response to verifying the credential with the preliminary authentication, an operation 806 to establish a second wireless connection with the key device. The second wireless connection may be UWB. Using a communication technology such as UWB, the PACS may identify locations of the key device or ranges of the key device to the reader or a plurality of readers.

[0100] The technique 800 includes operations to transmit the credential to an authorization service and to receive an indication the user is authorized to access the asset from the authorization service. The preliminary authorization is performed to help eliminate any credentials that would automatically be rejected by the authorization service as they may not fit the correct format or pattern. This may eliminate the time and processing of transmitting and authenticating these credentials. The technique 800 includes an operation 808 to provide a command to grant access to the asset.

[0101] FIG. 9 illustrates a flowchart showing a technique 900 for regulating access to an asset, in accordance with some embodiments. The technique 900 includes an operation 902 to receive a credential for an asset from a key device

associated with a user using a first wireless connection. The first wireless connection may be an NFC such as RFID or PAN technologies, such as the IEEE 802.15.1 and BLE.

[0102] The technique 900 includes an operation 904 to store the credential in a cache of the memory. The PACS may cache the credential in memory, such as memory of the reader, for future authentication when the intent of the user to enter the asset. The intent threshold to authenticate the credential may be lower than the intent threshold to unlock access to the asset. For example, as a user moves toward a doorway, the PACS may determine a 60% probability the user is intending to enter the doorway and transmits the credential to the authentication service. As the user continues toward the door, the probability may change to 90% and the reader then transmits the command to unlock the doorway.

[0103] The technique 900 includes an operation 906 to establish a second wireless connection with the key device. The second wireless connection may be UWB. Using a communication technology such as UWB, the PACS may identify locations of the key device or ranges of the key device to the reader or a plurality of readers.

[0104] The technique 900 includes, in response to establishing the second wireless connection with the key device, an operation 908 to request a validation of the credential from an authorization service. The authorization service may be local to the reader, such as in a residential home. The authorization service may be connected to the reader through a network or the Internet to provide credential authorization to multiple locations or entry points. The authorization service may be integrated into the reader.

[0105] The technique 900 includes an operation 910 to receive a validation token from the authorization service. The validation token may be used to transmit to the authorization service or an access control service to indicate the provided credential has been validated. The technique 900 includes an operation 912 to store the validation token in the cache.

[0106] The technique 900 may further include an operation to determine the key device is within a first range radius of a plurality of range radii using the second wireless connection, wherein the plurality of range radii extend from a wireless key

device reader. The PACS may identify distance ranges from the reader. For example, the PACS may designate three ranges, the first is within a five foot radius of the reader, the second is within a five to ten foot radius of the reader, and the third is within a ten to fifteen foot radius of the reader.

[0107] The technique 900 may further include an operation to determine the key device is within a second range radius of a plurality of range radii using the second wireless connection, wherein the second range radius is closer to the wireless key device reader than the first range radius. From the previous example of the three ranges, the PACS may determine, using UWB, that the key device was originally within the third range and has moved into the second range.

[0108] The technique 900 may further include an operation to calculate a probability the user intends physically access the asset based on determining the wireless key device is within the second range radius. From the previous example, the key device has moved from a further distance range to a closer distance range, thus increasing the probability the user is moving toward the reader.

[0109] The technique 900 may further include an operation to determine the probability exceeds a predetermined threshold. The technique 900 may further include an operation to transmit the validation token to an access control service. Based on the probability exceeding a threshold, the PACS may transmit the validations toke to the access control service to indicate the asset should be unlocked. The technique 900 may further include an operation to receive a command to grant access to the asset. The authorization service and the access control service may be integrated into the PACS, may be networked to the PACS, or may be separate services to the PACS.

[0110] The technique 900 may further include an operation to determine the key device is within a second range radius of a plurality of range radii using the second wireless connection, wherein the second range radius is further from the wireless key device reader than the first range radius. From the previous example of the three ranges, the PACS may determine, using UWB, that the key device was originally within the second range and has moved further away into the third range.

[0111] The technique 900 may further include an operation to remove the validation token and credential from the cache. From the previous example, the key device has moved from a closer distance range to a further distance range, thus increasing the probability the user is not intending to access the asset, and thus the stored information, such as the credential and validation token, are removed from the cache.

[0112] The technique 900 may further include an operation to determine a response from the key device has not been received within a predetermined time period. When the PACS sends the message, it may start a timer. When the PACS receives a response from the wireless key device, the timer may be canceled. If the timer times out, based on a determined timeout time, then the PACS may determine that the wireless key device is no longer within range and thus the probability the user intends to access the asset is very low. The technique 900 may further include an operation to remove the validation token and credential from the cache based on them no longer being needed.

[0113] FIG. 10 illustrates a flowchart showing a technique 1000 for regulating access to an asset, in accordance with some embodiments. The technique 1000 includes an operation 1002 to receive a credential of a user from a key device associated with the user using a first wireless connection. The first wireless connection may be an NFC such as RFID or PAN technologies, such as the IEEE 802.15.1 and BLE.

[0114] The technique 1000 includes an operation 1004 to establish a second wireless connection with the key device. The second wireless connection may be UWB. Using a communication technology such as UWB, the PACS may identify locations of the key device or ranges of the key device to the reader or a plurality of readers.

[0115] The technique 1000 includes an operation 1006 to determine the user intends to access the asset based on a data set generated derived from the second wireless connection. The PACS may determine location information from the second wireless connection by using UWB. The second wireless connection may include information from the key device, such as sensor data from sensors of the

key device. The data set may include data both provided from the key device and derived from the second wireless connection that may be used to determine the intent of the user.

[0116] The technique 1000 may, in determining the user intends to access the asset, include an operation to determine a probability the user intends to access the asset using the data set and a trained machine learning model. The trained machine learning model is trained with data sets collected from a plurality of users. The data sets may include movement data for the plurality of users within a range of the asset. The data sets may include movement data from the plurality of users. The information received from the wireless key device may include movement data of the user collected from an accelerometer of the wireless key device.

[0117] For example, for a particular asset or secure entry point, location and movement data for how different people approach and move toward the secure entry point when entering the secure entry point and data for when people do not enter the secure entry point may be used to train the machine learning model. This training may provide for the machine learning model to recognize how people may move and angles of their approach, when their intent is to enter the secure entry point. The data sets may include a time of day timestamp and the data set of the user may be timestamped. Including the time in the training of the machine learning model may indicate different patterns and actions based on the time of day. For example, people may be less likely to access the secure entry point at lunch time.

[0118] The determination that the user intends to access an asset may include using data received from a calendar system. The technique 1000 may further include an operation to identify an event in the calendar system associated with the asset. For example, the calendar system may indicate that a meeting is occurring in the room attached to the secure entry point. The technique 1000 may further include an operation to identify an indication of attendance to the event by the user. The calendar system may provide a list of attendees to the meeting and the PACS may identify that the user is one of those attendees, which may increase the probability the user intends to enter the secure entry point. The technique 1000 includes an operation 1008 to transmit a command to grant access to the asset.

[0119] FIG. 11 illustrates a block diagram of an example machine 1100 upon which any one or more of the techniques (e.g., methodologies) discussed herein may perform. In alternative embodiments, the machine 1100 may operate as a standalone device or may be connected (e.g., networked) to other machines. In a networked deployment, the machine 1100 may operate in the capacity of a server machine, a client machine, or both in server-client network environments. In an example, the machine 1100 may act as a peer machine in peer-to-peer (P2P) (or other distributed) network environment. The machine 1100 may be a personal computer (PC), a tablet PC, a set-top box (STB), a personal digital assistant (PDA), a mobile telephone, a web appliance, a network router, switch or bridge, or any machine capable of executing instructions (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein, such as cloud computing, software as a service (SaaS), other computer cluster configurations.

[0120] Examples, as described herein, may include, or may operate by, logic or a number of components, or mechanisms. Circuit sets are a collection of circuits implemented in tangible entities that include hardware (e.g., simple circuits, gates, logic, etc.). Circuit set membership may be flexible over time and underlying hardware variability. Circuit sets include members that may, alone or in combination, perform specified operations when operating. In an example, hardware of the circuit set may be immutably designed to carry out a specific operation (e.g., hardwired). In an example, the hardware of the circuit set may include variably connected physical components (e.g., execution units, transistors, simple circuits, etc.) including a computer readable medium physically modified (e.g., magnetically, electrically, moveable placement of invariant massed particles, etc.) to encode instructions of the specific operation. In connecting the physical components, the underlying electrical properties of a hardware constituent are changed, for example, from an insulator to a conductor or vice versa. The instructions enable embedded hardware (e.g., the execution units or a loading mechanism) to create members of

the circuit set in hardware via the variable connections to carry out portions of the specific operation when in operation. Accordingly, the computer readable medium is communicatively coupled to the other components of the circuit set member when the device is operating. In an example, any of the physical components may be used in more than one member of more than one circuit set. For example, under operation, execution units may be used in a first circuit of a first circuit set at one point in time and reused by a second circuit in the first circuit set, or by a third circuit in a second circuit set at a different time.

[0121] Machine (e.g., computer system) 1100 may include a hardware processor 1102 (e.g., a central processing unit (CPU), a graphics processing unit (GPU), a hardware processor core, field programmable gate array (FPGA), or any combination thereof), a main memory 1104 and a static memory 1106, some or all of which may communicate with each other via an interlink (e.g., bus) 1108. The machine 1100 may further include a display unit 1110, an alphanumeric input device 1112 (e.g., a keyboard), and a user interface (UI) navigation device 1114 (e.g., a mouse). In an example, the display unit 1110, input device 1112 and UI navigation device 1114 may be a touch screen display. The machine 1100 may additionally include a storage device (e.g., drive unit) 1116, a signal generation device 1118 (e.g., a speaker), a network interface device 1120, and one or more sensors 1121, such as a global positioning system (GPS) sensor, compass, accelerometer, or other sensor. The machine 1100 may include an output controller 1128, such as a serial (e.g., universal serial bus (USB), parallel, or other wired or wireless (e.g., infrared (IR), near field communication (NFC), etc.) connection to communicate or control one or more peripheral devices (e.g., a printer, card reader, etc.).

[0122] The storage device 1116 may include a machine readable medium 1122 on which is stored one or more sets of data structures or instructions 1124 (e.g., software) embodying or used by any one or more of the techniques or functions described herein. The instructions 1124 may also reside, completely or at least partially, within the main memory 1104, within static memory 1106, or within the hardware processor 1102 during execution thereof by the machine 1100. In an

example, one or any combination of the hardware processor 1102, the main memory 1104, the static memory 1106, or the storage device 1116 may constitute machine readable media.

[0123] While the machine readable medium 1122 is illustrated as a single medium, the term "machine readable medium" may include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) configured to store the one or more instructions 1124.

[0124] The term “machine readable medium” may include any medium that is capable of storing, encoding, or carrying instructions for execution by the machine 1100 and that cause the machine 1100 to perform any one or more of the techniques of the present disclosure, or that is capable of storing, encoding or carrying data structures used by or associated with such instructions. Non-limiting machine readable medium examples may include solid-state memories, and optical and magnetic media. In an example, a massed machine readable medium comprises a machine readable medium with a plurality of particles having invariant (e.g., rest) mass. Accordingly, massed machine-readable media are not transitory propagating signals. Specific examples of massed machine readable media may include: non-volatile memory, such as semiconductor memory devices (e.g., Electrically Programmable Read-Only Memory (EPROM), Electrically Erasable Programmable Read-Only Memory (EEPROM)) and flash memory devices; magnetic disks, such as internal hard disks and removable disks; magneto-optical disks; and CD-ROM and DVD-ROM disks.

[0125] The instructions 1124 may further be transmitted or received over a communications network 1126 using a transmission medium via the network interface device 1120 utilizing any one of a number of transfer protocols (e.g., frame relay, internet protocol (IP), transmission control protocol (TCP), user datagram protocol (UDP), hypertext transfer protocol (HTTP), etc.). Example communication networks may include a local area network (LAN), a wide area network (WAN), a packet data network (e.g., the Internet), mobile telephone networks (e.g., cellular networks), Plain Old Telephone (POTS) networks, and wireless data networks (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.11 family of standards

known as Wi-Fi®, IEEE 802.16 family of standards known as WiMax®), IEEE 802.15.4 family of standards, peer-to-peer (P2P) networks, among others. In an example, the network interface device 1120 may include one or more physical jacks (e.g., Ethernet, coaxial, or phone jacks) or one or more antennas to connect to the communications network 1126. In an example, the network interface device 1120 may include a plurality of antennas to wirelessly communicate using at least one of single-input multiple-output (SIMO), multiple-input multiple-output (MIMO), or multiple-input single-output (MISO) techniques. The term "transmission medium" shall be taken to include any intangible medium that is capable of storing, encoding or carrying instructions for execution by the machine 1100, and includes digital or analog communications signals or other intangible medium to facilitate communication of such software.

[0126] The above detailed description includes references to the accompanying drawings, which form a part of the detailed description. The drawings show, by way of illustration, specific embodiments that may be practiced. These embodiments are also referred to herein as "examples." Such examples may include elements in addition to those shown or described. However, the present inventors also contemplate examples in which only those elements shown or described are provided. Moreover, the present inventors also contemplate examples using any combination or permutation of those elements shown or described (or one or more aspects thereof), either with respect to a particular example (or one or more aspects thereof), or with respect to other examples (or one or more aspects thereof) shown or described herein.

[0127] All publications, patents, and patent documents referred to in this document are incorporated by reference herein in their entirety, as though individually incorporated by reference. In the event of inconsistent usages between this document and those documents so incorporated by reference, the usage in the incorporated reference(s) should be considered supplementary to that of this document; for irreconcilable inconsistencies, the usage in this document controls.

[0128] In this document, the terms "a" or "an" are used, as is common in patent documents, to include one or more than one, independent of any other instances or

usages of "at least one" or "one or more." In this document, the term "or" is used to refer to a nonexclusive or, such that "A or B" includes "A but not B," "B but not A," and "A and B," unless otherwise indicated. In the appended claims, the terms "including" and "in which" are used as the plain-English equivalents of the respective terms "comprising" and "wherein." Also, in the following claims, the terms "including" and "comprising" are open-ended, that is, a system, device, article, or process that includes elements in addition to those listed after such a term in a claim are still deemed to fall within the scope of that claim. Moreover, in the following claims, the terms "first," "second," and "third," etc. are used merely as labels, and are not intended to impose numerical requirements on their objects.

[0129] The above description is intended to be illustrative, and not restrictive. For example, the above-described examples (or one or more aspects thereof) may be used in combination with each other. Other embodiments may be used, such as by one of ordinary skill in the art upon reviewing the above description. The Abstract is to allow the reader to quickly ascertain the nature of the technical disclosure and is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. Also, in the above Detailed Description, various features may be grouped together to streamline the disclosure. This should not be interpreted as intending that an unclaimed disclosed feature is essential to any claim. Rather, inventive subject matter may lie in less than all features of a particular disclosed embodiment. Thus, the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separate embodiment. The scope of the embodiments should be determined with reference to the appended claims, along with the full scope of equivalents to which such claims are entitled.

CLAIMS

WHAT IS CLAIMED IS:

1. A method for regulating access to an asset, comprising:

receiving a credential from a key device associated with a user using a first wireless connection;

verifying the credential with a preliminary authentication for the asset;

in response to verifying the credential with the preliminary authentication, establishing a second wireless connection with the key device; and

providing a command to grant access to the asset.

2. The method of claim 1, wherein the first wireless connection is Bluetooth Low Energy and the second wireless connection is Ultra-Wideband.

3. The method of claim 1 or 2, further comprising:

transmitting the credential to an authorization service; and

receiving an indication the user is authorized to access the asset from the authorization service.

4. The method of claim 1, 2 or 3, wherein the preliminary authentication includes identifying the credential includes a pattern using pattern matching.

5. The method of claim 4, wherein the pattern is defined using a regular expression.

6. The method of any preceding claim, wherein verifying the credential with the preliminary authentication comprises comparing the credential to a whitelist of credentials.

7. The method of claim 6, wherein the whitelist is applied in the preliminary authentication based on time of day.

8. The method of any preceding claim, wherein the asset is a physical location.

9. The method of any preceding claim, wherein the asset is an electronic device.

10. The method of any preceding claim, wherein providing the command to grant access to the asset is based on determining the user intends to access the asset.

11. A system for regulating access to an asset, comprising:

at least one processor; and

memory including instructions that, when executed by the at least one processor, cause the at least one processor to:

receive a credential from a key device associated with a user using a first wireless connection;

verify the credential with a preliminary authentication for the asset;

in response to verifying the credential with the preliminary authentication, establish a second wireless connection with the key device; and

provide a command to grant access to the asset.

12. The system of claim 11, wherein the first wireless connection is Bluetooth Low Energy and the second wireless connection is Ultra-Wideband.

13. The system of claim 11 or 12, further comprising instructions to:

transmit the credential to an authorization service; and

receive an indication the user is authorized to access the asset from the authorization service.

14. The system of claim 11, 12 or 13, wherein the preliminary authentication includes identifying the credential includes a pattern using pattern matching.

15. The system of claim 14, wherein the pattern is defined using a regular expression.

16. The system of any of claims 11 to 15, wherein verifying the credential with the preliminary authentication comprises instructions to compare the credential to a whitelist of credentials.

17. The system of claim 16, wherein the whitelist is applied in the preliminary authentication based on time of day.

18. The system of any of claims 11 to 17, wherein the asset is a physical location.

19. The system of any of claims 11 to 18, wherein the asset is an electronic device.

20. The system of any of claims 11 to 19, wherein providing the command to grant access to the asset is based on determining the user intends to access the asset.

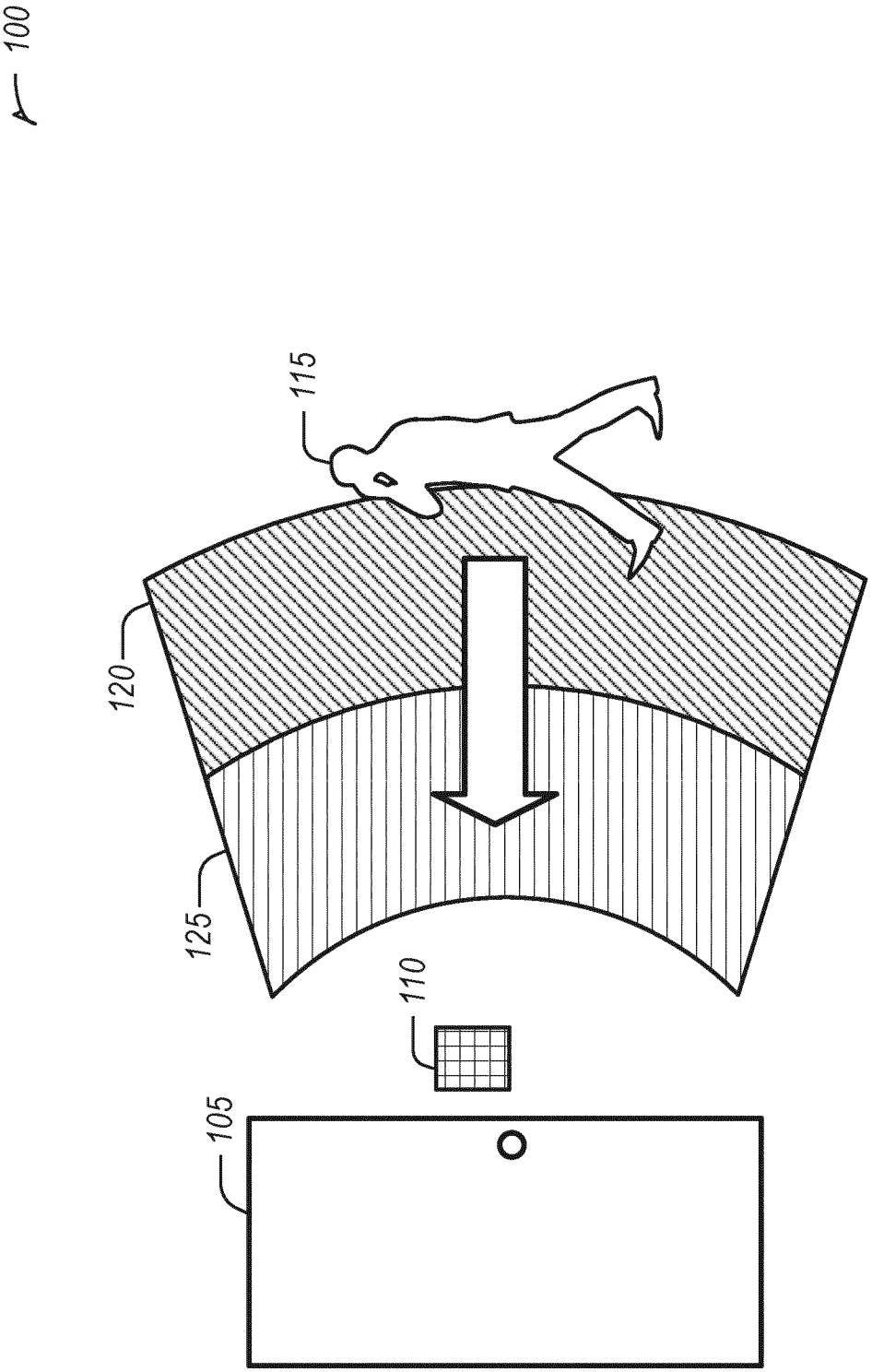

FIG. 1

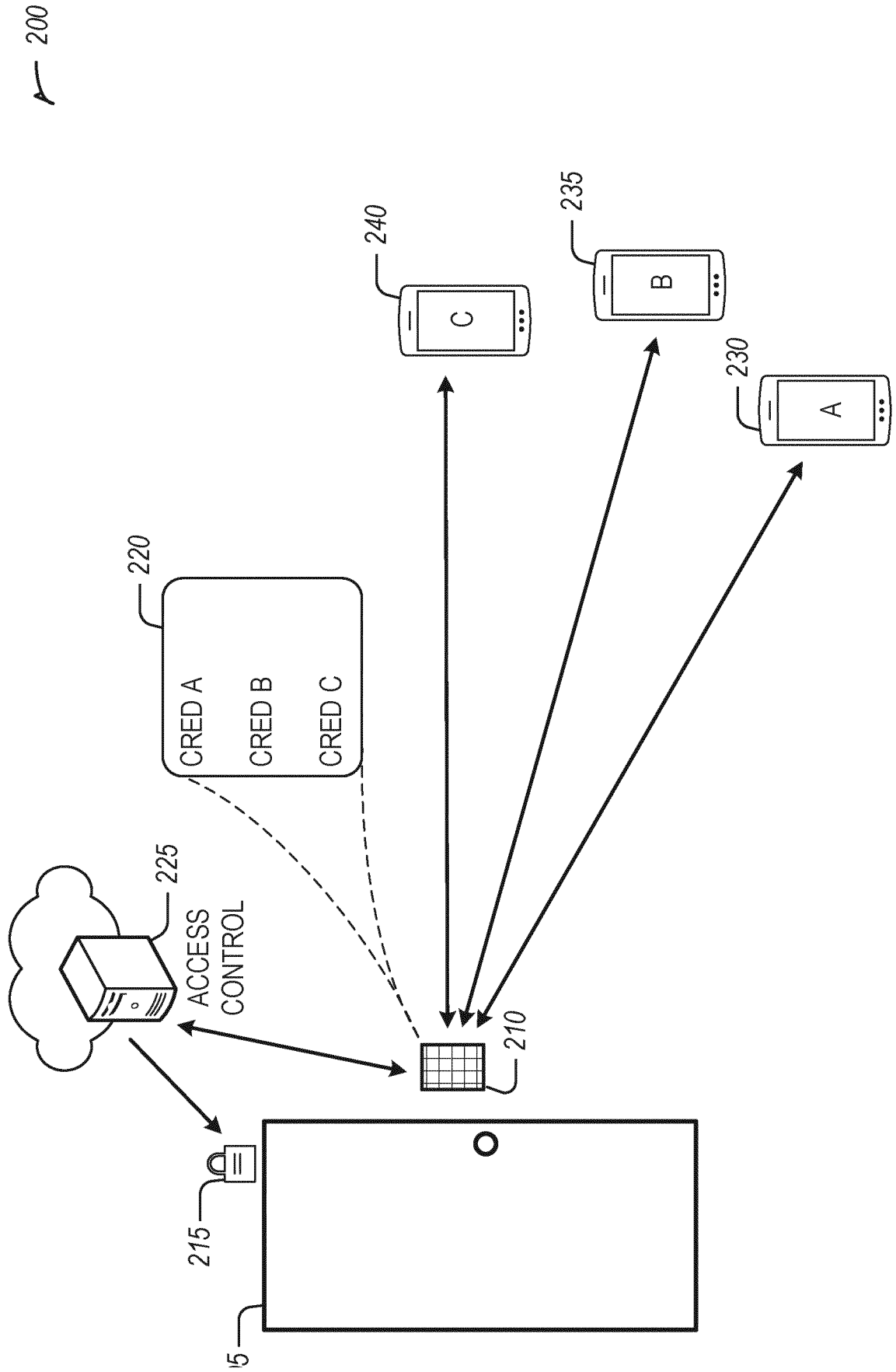
200
240
C
235
B
230
A
220
CRED A
CRED B
CRED C
225
ACCESS CONTROL
210
215
5

FIG. 2A

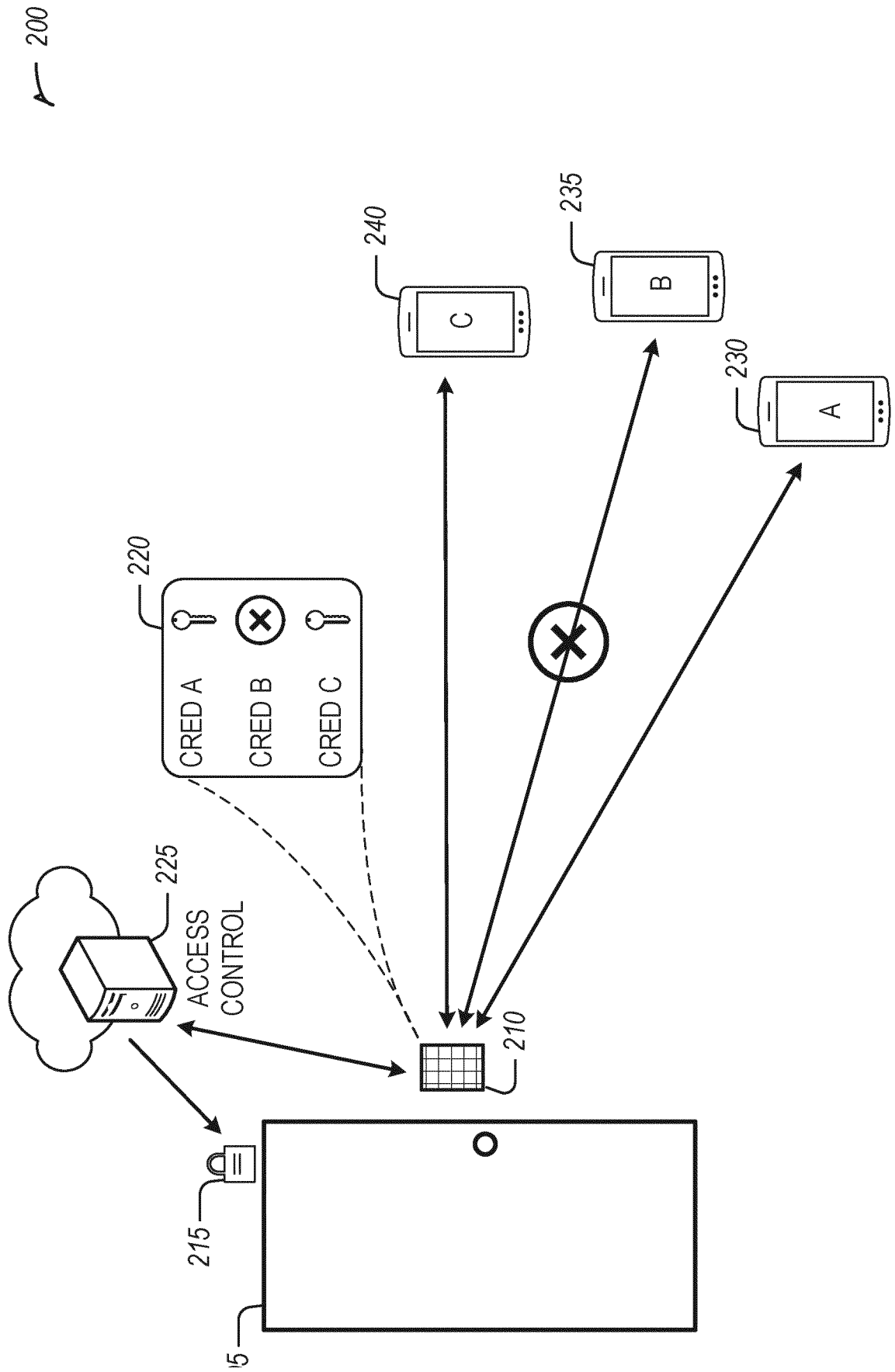
200
240
C
235
B
230
A
220
CRED A
CRED B
CRED C
225
ACCESS CONTROL
210
215
5

FIG. 2B

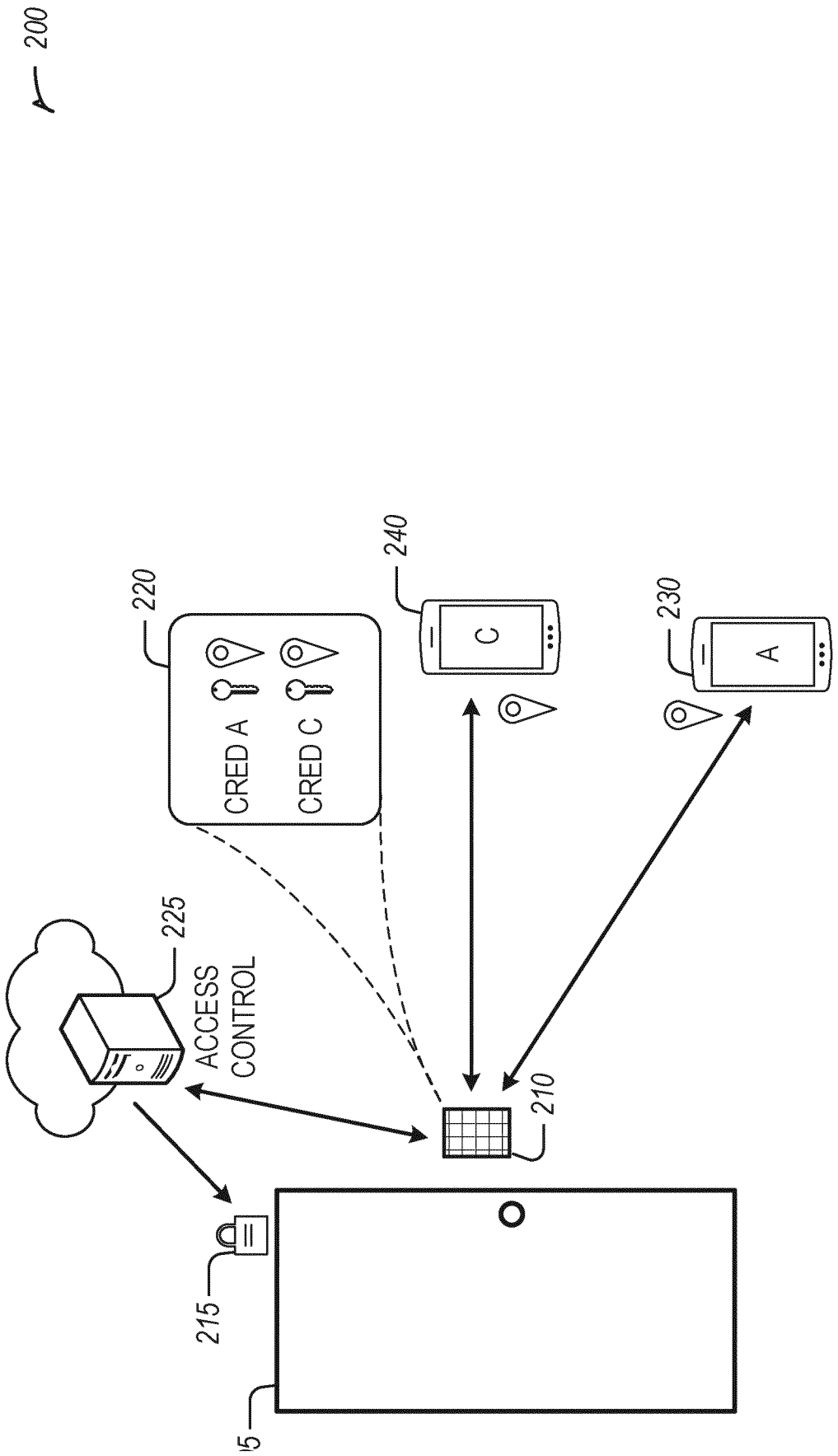

FIG. 2C

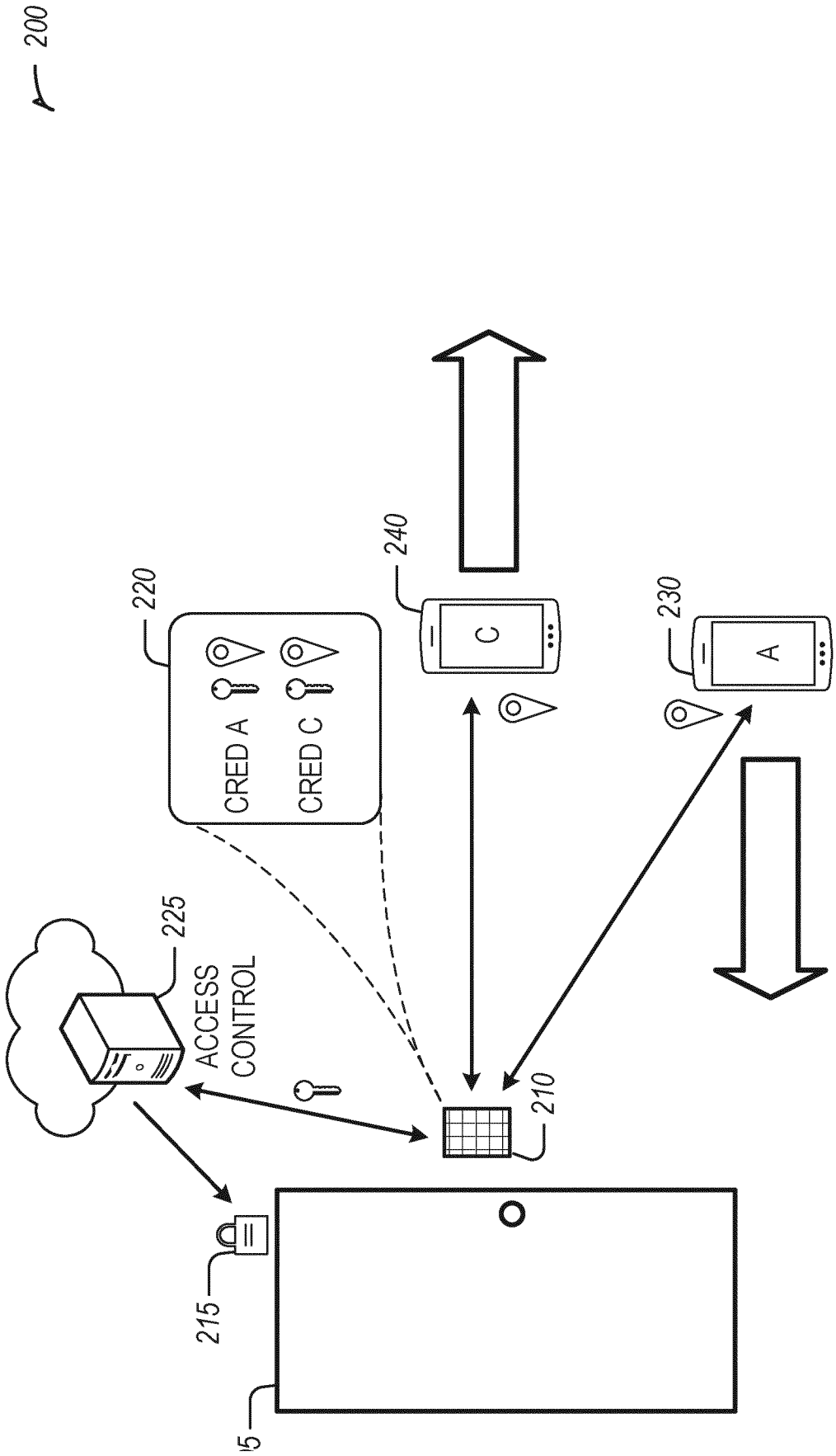

FIG. 2D

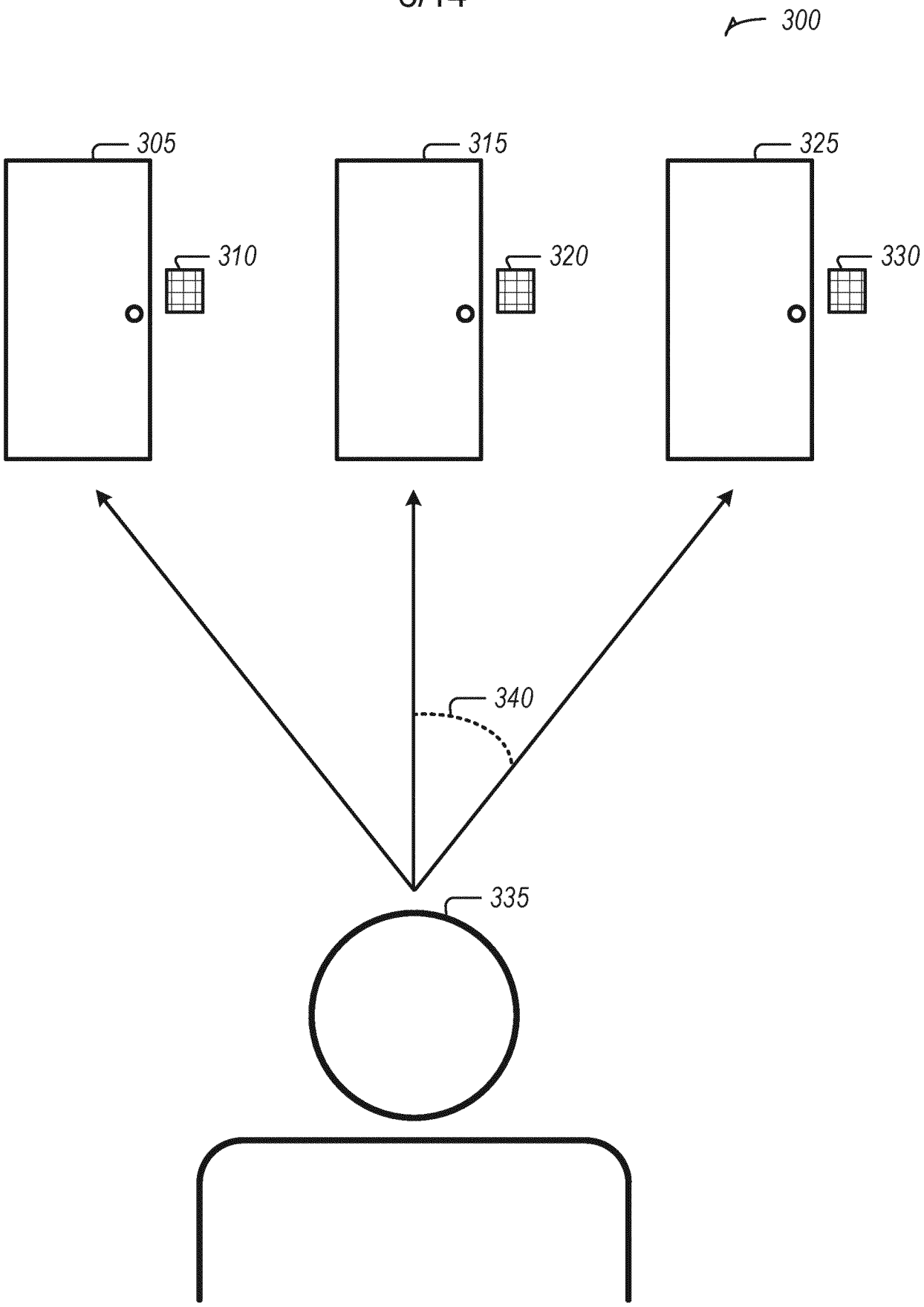

FIG. 3

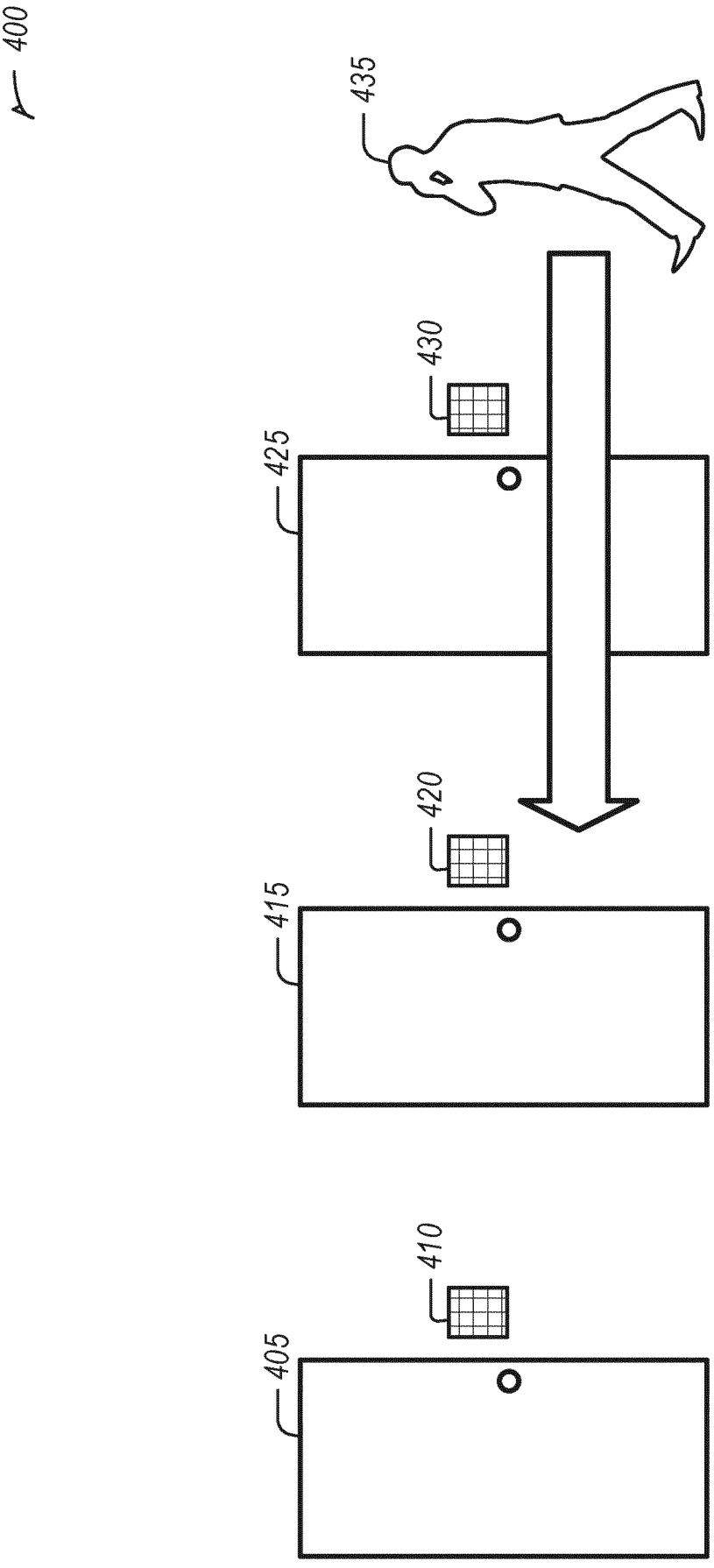

FIG. 4

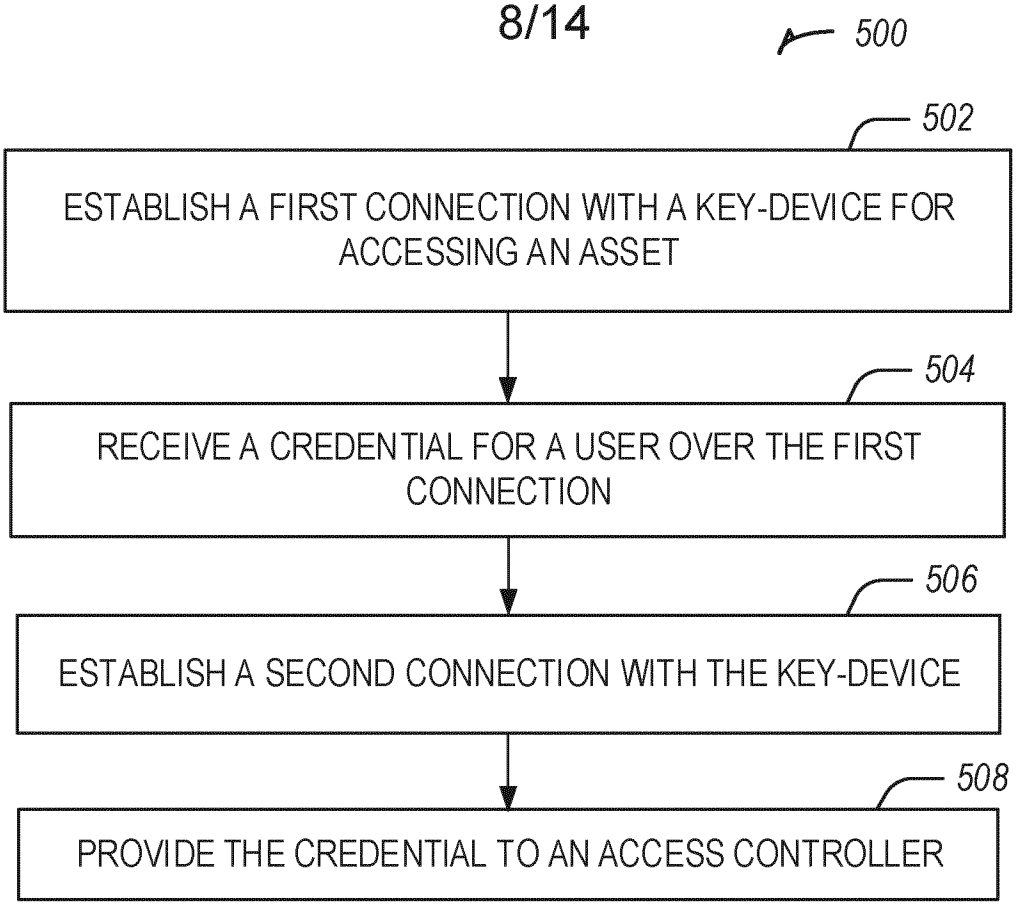
500
502
ESTABLISH A FIRST CONNECTION WITH A KEY-DEVICE FOR ACCESSING AN ASSET
504
RECEIVE A CREDENTIAL FOR A USER OVER THE FIRST CONNECTION
506
ESTABLISH A SECOND CONNECTION WITH THE KEY-DEVICE
508
PROVIDE THE CREDENTIAL TO AN ACCESS CONTROLLER

FIG. 5

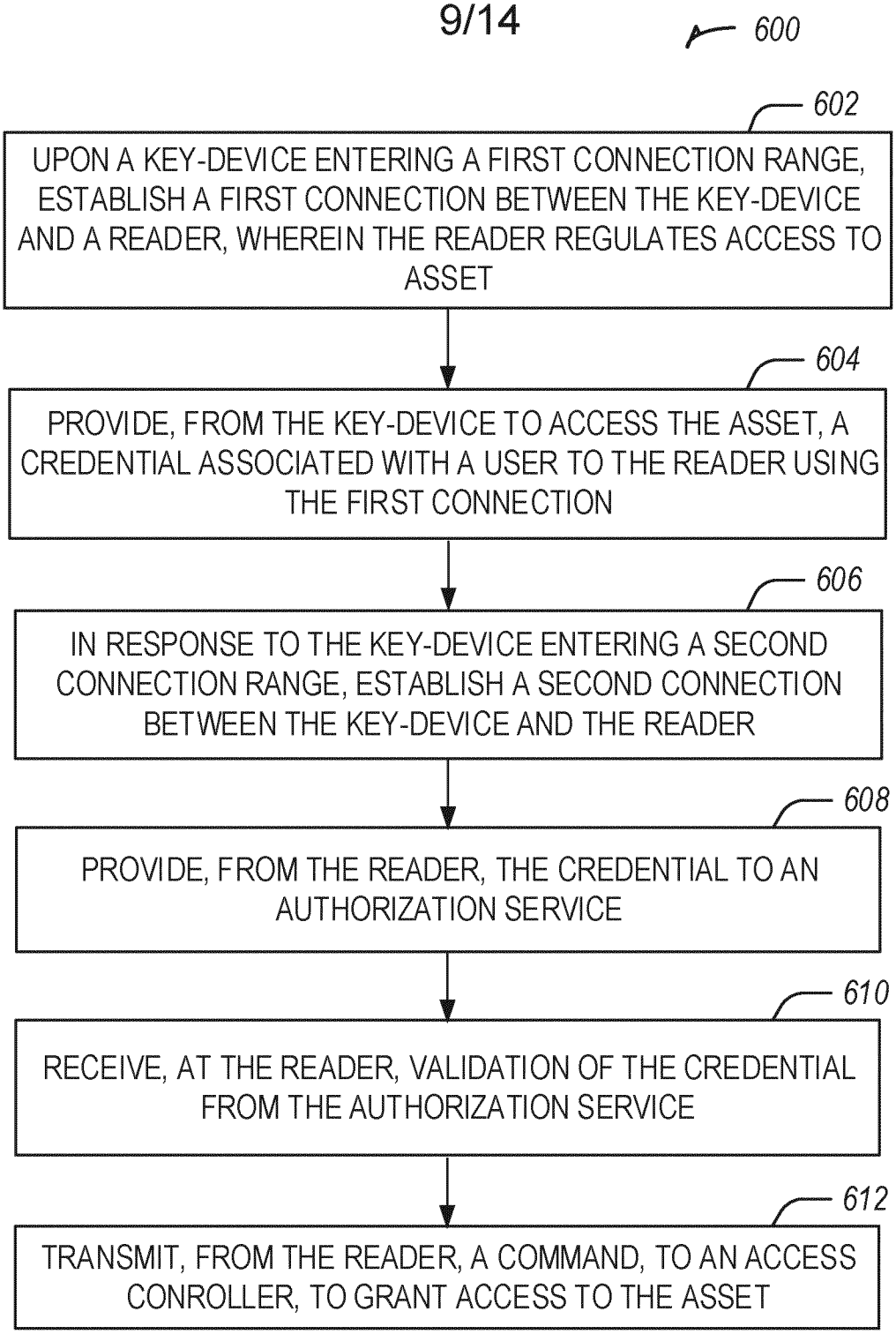
600
602
UPON A KEY-DEVICE ENTERING A FIRST CONNECTION RANGE, ESTABLISH A FIRST CONNECTION BETWEEN THE KEY-DEVICE AND A READER, WHEREIN THE READER REGULATES ACCESS TO ASSET
604
PROVIDE, FROM THE KEY-DEVICE TO ACCESS THE ASSET, A CREDENTIAL ASSOCIATED WITH A USER TO THE READER USING THE FIRST CONNECTION
606
IN RESPONSE TO THE KEY-DEVICE ENTERING A SECOND CONNECTION RANGE, ESTABLISH A SECOND CONNECTION BETWEEN THE KEY-DEVICE AND THE READER
608
PROVIDE, FROM THE READER, THE CREDENTIAL TO AN AUTHORIZATION SERVICE
610
RECEIVE, AT THE READER, VALIDATION OF THE CREDENTIAL FROM THE AUTHORIZATION SERVICE
612
TRANSMIT, FROM THE READER, A COMMAND, TO AN ACCESS CONROLLER, TO GRANT ACCESS TO THE ASSET

FIG. 6

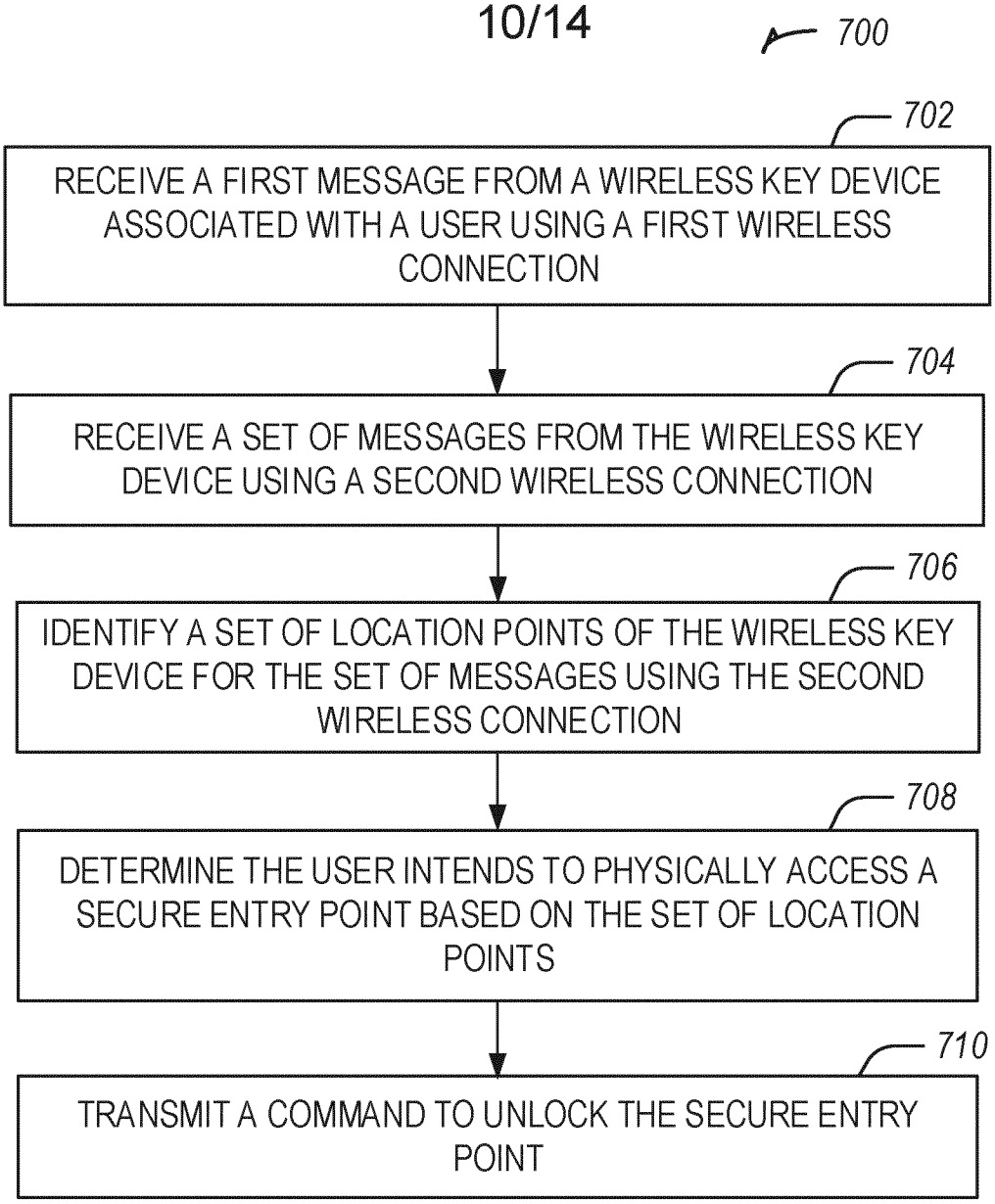
700
702
RECEIVE A FIRST MESSAGE FROM A WIRELESS KEY DEVICE ASSOCIATED WITH A USER USING A FIRST WIRELESS CONNECTION
704
RECEIVE A SET OF MESSAGES FROM THE WIRELESS KEY DEVICE USING A SECOND WIRELESS CONNECTION
706
IDENTIFY A SET OF LOCATION POINTS OF THE WIRELESS KEY DEVICE FOR THE SET OF MESSAGES USING THE SECOND WIRELESS CONNECTION
708
DETERMINE THE USER INTENDS TO PHYSICALLY ACCESS A SECURE ENTRY POINT BASED ON THE SET OF LOCATION POINTS
710
TRANSMIT A COMMAND TO UNLOCK THE SECURE ENTRY POINT

FIG. 7

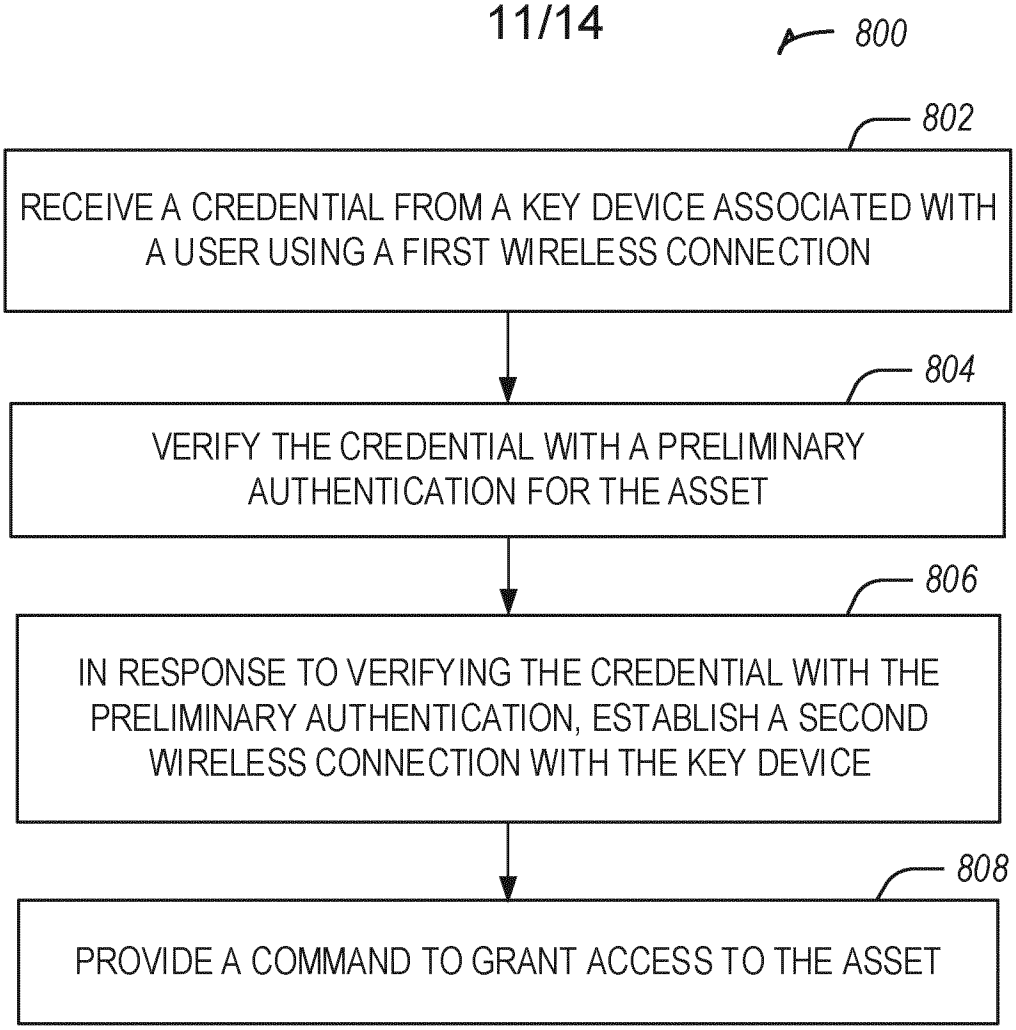
800
802
RECEIVE A CREDENTIAL FROM A KEY DEVICE ASSOCIATED WITH A USER USING A FIRST WIRELESS CONNECTION
804
VERIFY THE CREDENTIAL WITH A PRELIMINARY AUTHENTICATION FOR THE ASSET
806
IN RESPONSE TO VERIFYING THE CREDENTIAL WITH THE PRELIMINARY AUTHENTICATION, ESTABLISH A SECOND WIRELESS CONNECTION WITH THE KEY DEVICE
808
PROVIDE A COMMAND TO GRANT ACCESS TO THE ASSET

FIG. 8

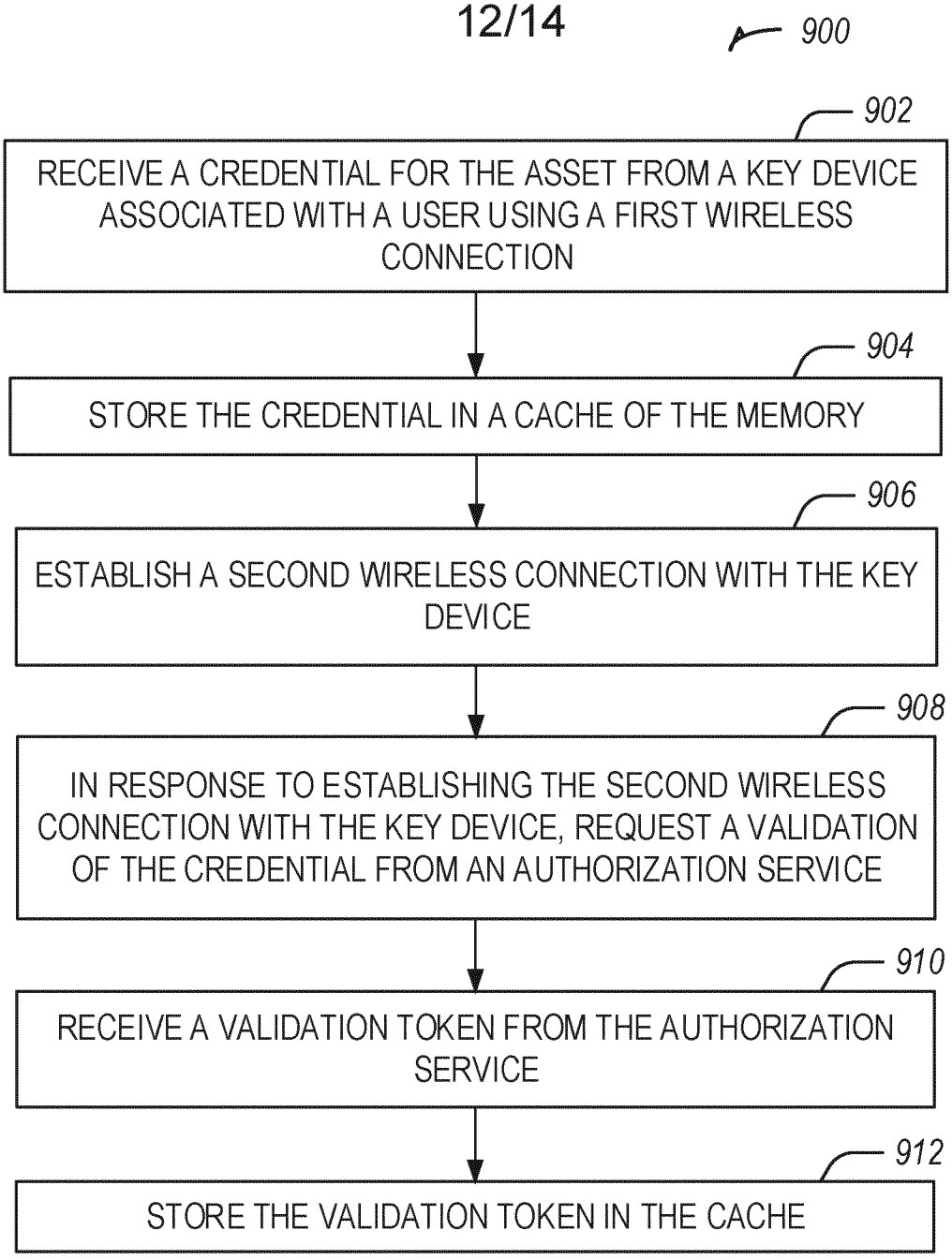
900
902
RECEIVE A CREDENTIAL FOR THE ASSET FROM A KEY DEVICE ASSOCIATED WITH A USER USING A FIRST WIRELESS CONNECTION
904
STORE THE CREDENTIAL IN A CACHE OF THE MEMORY
906
ESTABLISH A SECOND WIRELESS CONNECTION WITH THE KEY DEVICE
908
IN RESPONSE TO ESTABLISHING THE SECOND WIRELESS CONNECTION WITH THE KEY DEVICE, REQUEST A VALIDATION OF THE CREDENTIAL FROM AN AUTHORIZATION SERVICE
910
RECEIVE A VALIDATION TOKEN FROM THE AUTHORIZATION SERVICE
912
STORE THE VALIDATION TOKEN IN THE CACHE

FIG. 9

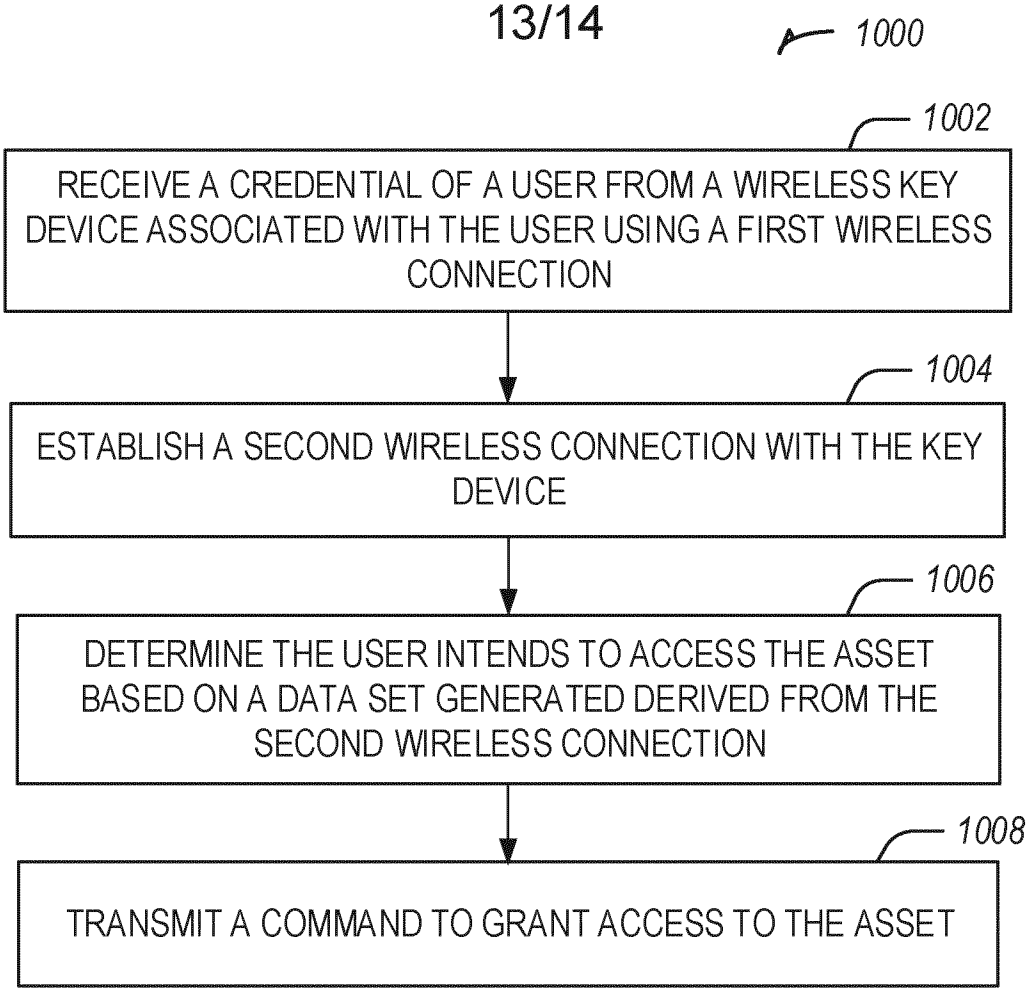
1000
1002
RECEIVE A CREDENTIAL OF A USER FROM A WIRELESS KEY DEVICE ASSOCIATED WITH THE USER USING A FIRST WIRELESS CONNECTION
1004
ESTABLISH A SECOND WIRELESS CONNECTION WITH THE KEY DEVICE
1006
DETERMINE THE USER INTENDS TO ACCESS THE ASSET BASED ON A DATA SET GENERATED DERIVED FROM THE SECOND WIRELESS CONNECTION
1008
TRANSMIT A COMMAND TO GRANT ACCESS TO THE ASSET

FIG. 10

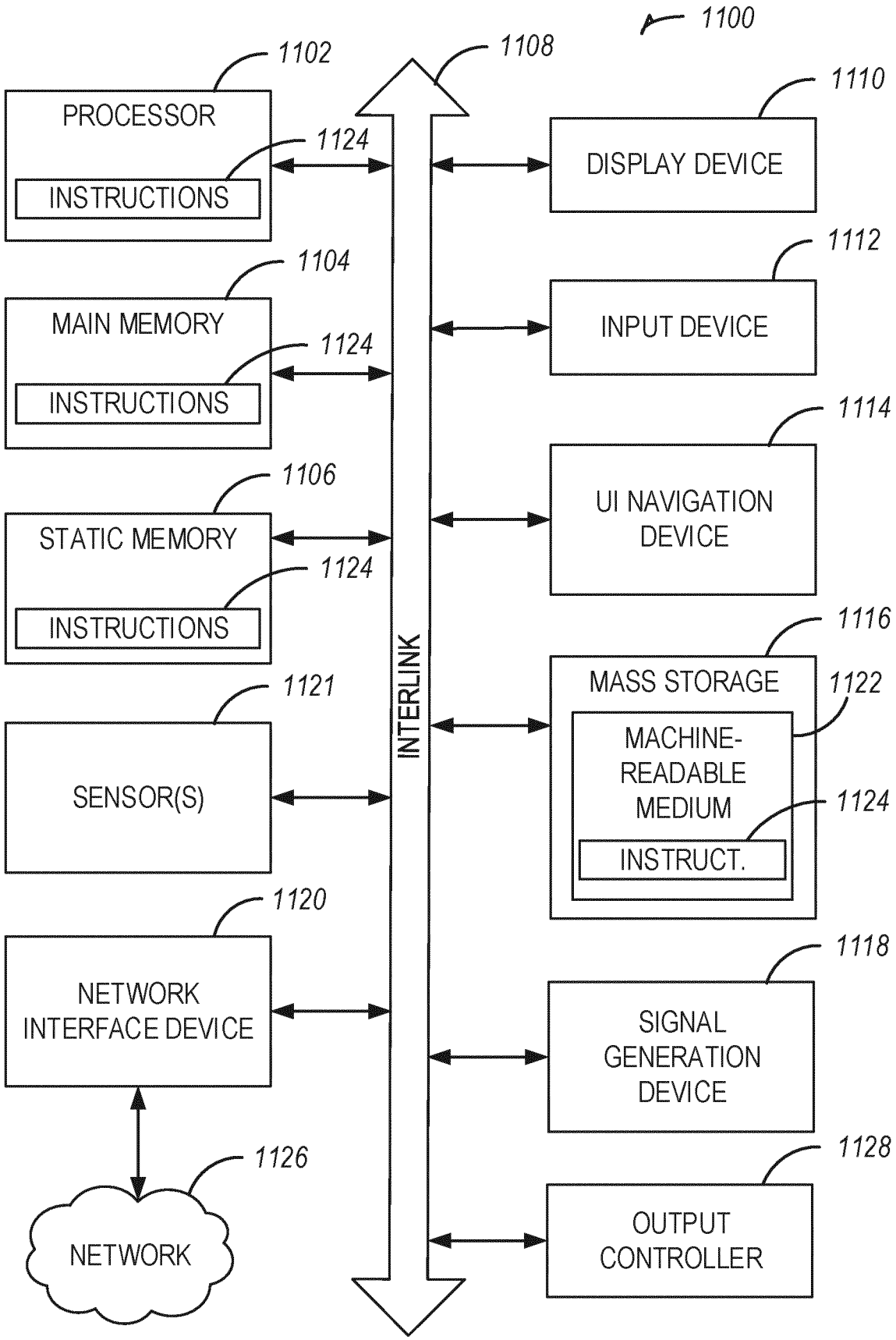
1100
1102
PROCESSOR
1124
INSTRUCTIONS
1104
MAIN MEMORY
1124
INSTRUCTIONS
1106
STATIC MEMORY
1124
INSTRUCTIONS
1121
SENSOR(S)
1120
NETWORK INTERFACE DEVICE
1126
NETWORK
1108
INTERLINK
1110
DISPLAY DEVICE
1112
INPUT DEVICE
1114
UI NAVIGATION DEVICE
1116
MASS STORAGE
1122
MACHINE-READABLE MEDIUM
1124
INSTRUCT.
1118
SIGNAL GENERATION DEVICE
1128
OUTPUT CONTROLLER

FIG. 11

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2020/058216

A. CLASSIFICATION OF SUBJECT MATTER
INV. G01S1/00 G01S13/76 G07C9/00 G07C9/22 G07C9/28
G07C9/29 H04W12/06
ADD. H04W4/02
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
B60R G01S G06N G07C H04W

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2018/234797 A1 (LEDVINA BRENT M [US] ET AL) 16 August 2018 (2018-08-16) paragraph [0005] - paragraph [0008] paragraph [0040] - paragraph [0050] paragraph [0070] paragraph [0126] - paragraph [0130] -----	1-7, 9-17,19, 20
X	WO 2016/089837 A1 (CARRIER CORP [US]) 9 June 2016 (2016-06-09) paragraph [0058] - paragraph [0062] paragraph [0073] - paragraph [0078] -----	1,3-11, 13-20
X	WO 2017/181132 A2 (APPLE INC [US]) 19 October 2017 (2017-10-19) paragraph [0003] - paragraph [0005] paragraph [0023] - paragraph [0028] paragraph [0040] -----	1-9, 11-19

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 June 2020	26/06/2020

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Mechenbier, Bernd

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Google: "core/java/android/companion/BluetoothLeDeviceFilter.java - platform/frameworks/base - Git at Google", Android Core Code, Bluetooth Companion, 1 January 2017 (2017-01-01), XP055704592, Retrieved from the Internet: URL:https://android.googlesource.com/platform/frameworks/base/+/master/core/java/android/companion/BluetoothLeDeviceFilter.java [retrieved on 2020-06-12] line 47 line 308 - line 317 -----	4,5,14, 15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2020/058216

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2018234797 A1	16-08-2018	CN 110312644 A	08-10-2019
		DE 112018000346 T5	19-09-2019
		JP 2020510567 A	09-04-2020
		KR 20190105049 A	11-09-2019
		US 2018234797 A1	16-08-2018
		US 2019297457 A1	26-09-2019
		WO 2018148687 A1	16-08-2018
WO 2016089837 A1	09-06-2016	CA 2968521 A1	09-06-2016
		CN 107005798 A	01-08-2017
		EP 3228098 A1	11-10-2017
		US 2017330226 A1	16-11-2017
		WO 2016089837 A1	09-06-2016
WO 2017181132 A2	19-10-2017	AU 2017250352 A1	11-10-2018
		CN 109076487 A	21-12-2018
		EP 3417663 A2	26-12-2018
		KR 20180123091 A	14-11-2018
		WO 2017181132 A2	19-10-2017