



- (51) **International Patent Classification:**  
G07C 9/00 (2006.01) G02B 27/01 (2006.01)
- (21) **International Application Number:**  
PCT/CA20 14/05 1207
- (22) **International Filing Date:**  
12 December 2014 (12.12.2014)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**  
61/915,175 12 December 2013 (12.12.2013) US
- (71) **Applicants:** KABA ILCO INC. [CA/CA]; 7301 boul. Decarie, Montreal, Quebec H4P 2G7 (CA). KABA MAS LLC [US/US]; 749 West Short Street, Lexington, Kentucky 40508 (US).
- (72) **Inventors:** JOHNSON, **Jerrill**; 2813 Michelle Park, Lexington, Kentucky 40511-8644 (US). IACOVINO, **Giovanni**; 319 Newton, Dollard des-Ormeaux, Quebec H9A 3K1 (CA).
- (74) **Agents:** ANGLEHART ET AL. et al; 1939 de Maison-neuve Quest, Montreal, Quebec H3H 1K3 (CA).

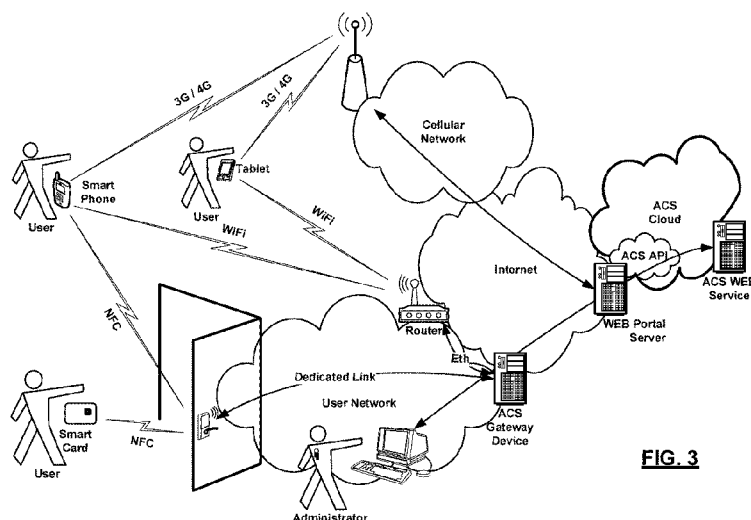
(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,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

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

**Published:**

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

(54) **Title:** AUGMENTED REALITY ADVANCED SECURITY AUTHENTICATION METHODOLOGIES

**FIG. 3**

(57) **Abstract:** Methods and apparatus for actuating a controlled lock to access a facility are described. The apparatus includes an electronic lock enrolled with an access control cloud service. The lock is paired with at least one user also enrolled with the access control cloud service. The methods include sequences of messages and commands for requesting and granting access to the facility.

## AUGMENTED REALITY ADVANCED SECURITY AUTHENTICATION METHODOLOGIES

This application claims priority of U.S. provisional patent application 61/915,175 filed December 12, 2013.

### 5 Technical Field

This invention relates to facility security, and in particular to systems and methods for augmented reality enhanced advanced security authentication.

### Background

10 In the field of facility security management, there is a continuing need for enhancing access security.

With reference to Figures 1A and 1B, current intelligent access control systems are generally composed of door lock hardware and associated personal computer (PC) software. The lock hardware represents physical devices mounted on doors or  
15 other types of access points (such as gates, barriers, lockers, etc.) to limit access to that physical location and/or facility to authorized personnel only. The PC software provides the intelligent interface to the access control system which allows an administrator to input configuration and authorization rights for a population of users. Traditionally, these access control systems also include a "programming"  
20 device, for example a Personal Data Assistant (PDA) or palm computer which ferries physical lock configuration information from the host PC software to battery operated locks and *vice versa*.

In recent years, with reference to Figure 2, advancements in radio-frequency technologies integrated into the lock hardware have made locks more intelligent and  
25 are now communicating wirelessly to the PC software. This has created "Access Control Networks" which now provide real-time features such as remote access, instant revocation and real-time activity notifications.

Software technology has also been evolving and the new concept of "Software as a Service" (SaaS) is taking root in the Access Control field. SaaS in the form of Cloud computing is a shift from the traditional PC installed software, Figures 1A/1B and 2, to software hosted on a remote sever managed by a third party (Figure 3). These  
5 facility security products are now offered as a service versus the traditional shrink-wrapped CD that is sold to a facilities administrator (end user).

### **Summary**

Developments in Access Control Systems (ACS) have now created ACS clouds via  
10 which end users subscribe to their security software and can scale their usage based on evolving requirements for example as illustrated in Figure 3. Along with the ACS Cloud, Figure 3 illustrates components for a full online cloud-based access control system. The main components include:

- Tokens - RFID card, FOB, smartphone, tablet, etc. that are used to  
15 authenticate to the lock hardware on the customers door either directly to the device via Near Field Communications (NFC) or indirectly to the device through the ACS Cloud;
- Wi-Fi / 3G Enabled Device - laptop / smartphone / tablet with web access  
used to administrate the customers locks via the ACS Cloud remotely or via Wi-Fi at  
20 the facility/residence location;
- Router - the customer's premises wireless router;
- Gateway Device - a dedicated device connected to the router which can  
be paired with multiple locks installed in range as well with range extending  
infrastructure;
- 25 • Lock Hardware - lock hardware with a wireless connection back to the  
ACS gateway, NFC/RFID, and key override; and

- ACS Cloud - ACS software which includes the customer-facing web portal, private web service accessed by customer's gateway hardware, and/or a public API to be used for third-party applications or other ACS systems.

5 The ACS cloud is accessible via the Web using any web enabled device with a browser anywhere in the World. It is noted that in this deployment scenario the door lock may not have a physical keypad human-machine interface. The human-machine interface is on the web enabled device, typically via an app.

10 In accordance with the proposed solution, instead of using a company ID card or a PIN code to gain access to a door, an augmented reality device is employed to provide a more natural and secure authentication process. In particular the human-machine interface cannot be snooped as it is only presented to the heads-up display wearer.

15 In accordance with an aspect of the proposed solution there is provided an access control system for granting access to a facility, the system comprising: a controlled lock configured to communicate with a remote access control server via data network infrastructure, said controlled lock providing lock identification information; and a heads-up display device configured to provide a human-machine interface enabling a user to input credentials or authenticate himself by other means to unlock said controlled lock, said heads-up display device being further optionally  
20 configured to communicate wirelessly with said remote access control server via said data network infrastructure, said heads-up display device including a forward facing camera configured to obtain lock identification information from said lock.

25 In accordance with another aspect of the proposed solution there is provided a method for granting access to a facility, the method comprising: identifying a lock by obtaining lock identification information; determining whether said lock is accessible via a particular heads-up display device authenticating a user wearing said heads-up display device with a remote access control system; server executing logic instruction implementing facility access control; requesting opening of said lock; and

informing the user wearing said heads-up display to proceed with actuating a knob of said lock.

### **Brief Description of the Drawings**

- 5 The invention will be better understood by way of the following detailed description of embodiments of the invention with reference to the appended drawings, in which:

Figure 1 is a schematic diagram showing a prior art facilities security deployment;

Figure 2 is another schematic diagram showing a prior art wireless facilities security deployment;

- 10 Figure 3 is a schematic diagram illustrating a cloud based facilities security deployment in accordance with the proposed solution;

Figure 4 is schematic diagram illustrating, in accordance with the proposed solution, trust relationships and communications channels via which the trust relationships are established in providing access control;

- 15 Figure 5 is a schematic message passing diagram illustrating primitives employed in establishing a new access control service in accordance with an embodiment of the proposed solution;

Figure 6 is a schematic diagram illustrating a heads-up display interface for inputting credentials in accordance with the proposed solution;

- 20 Figure 7 is another schematic diagram illustrating a heads up display interface for inputting biometric credentials in accordance with the proposed solution;

Figure 8 is a schematic message passing diagram illustrating a message flow in granting access to a facility to an enrolled user in accordance with the proposed solution;

Figure 9 is a schematic message passing diagram illustrating a message flow for an enrolled user granting access for an unenrolled person to enter a facility in accordance with the proposed solution;

Figure 10 is a schematic diagram illustrating a QR code for conveying enrolled lock  
5 particulars in accordance with the proposed solution;

Figure 11 is a schematic message passing diagram illustrating a message exchange in opening a lock in accordance with a preferred embodiment of the proposed solution; and

Figure 12 is another schematic message passing diagram illustrating another  
10 message exchange in opening a lock in accordance with another preferred embodiment of the proposed solution,

wherein similar features bear similar labels throughout the drawings.

### **Detailed Description**

15 Methods and apparatus for actuating a controlled lock to access a facility are described. The apparatus includes an electronic lock enrolled with an access control cloud service. The lock is associated, in programming, with at least one user also enrolled with the access control cloud service. The methods include sequences of messages and commands for requesting and granting access to the  
20 facility.

Figure 4 schematically illustrates trust relationships and lists possible communications channels via which the trust relationships are established in providing access control in accordance with the proposed solution.

In accordance with the proposed solution, because facilities access control is  
25 provided as a remote service, a number of trust relationships are broadened and a number of new trust relationships are possible.

The core remains the same as in the prior art deployments: Access to a facility such as, but not limited to: restricted grounds, a room, a locker, etc. is controlled through a door/gate having an intelligent lock also referred to as an Electronic Access Point (EAP). The grounds or room have a fixed geographical location  
5 defining inherent trust relationships. However, a locker can change geographical location, for example when implemented in a secure truck or secure container. This new trust relationship is enabled by the cloud based ACS which removes the restriction that the lock be collocated with the ACS Gateway device.

The type of access control is not limited to doors. These methods can further  
10 extend to other lock form factors such as:

- o Padlock form factors for use around the home, garage, fencing, etc.
- o Gun safe locks
- o Kid's room locks
- o Game/entertainment system access control by parents
- 15 o Child safety locks to secure cabinets containing dangerous chemicals

In accordance with the proposed solution, each person actor is equipped with an Artificial Reality (AR) device participating in the ACS deployment. AR devices include, while not being limited to: a wearable Heads-Up Display (HUD), a smartphone, a tablet, a laptop, etc. Examples of wearable heads-up displays  
20 include but are not limited to: Google Glass by Google Inc., Meta Spaceglasses by [www.spaceglasses.com](http://www.spaceglasses.com), etc.

In particular heads-up displays can access the ACS cloud through the customer's associated network-connected device (smartphone, tablet, laptop, etc.) or a network connection internal to the HUD itself. The ACS could authenticate the user and  
25 administrate the customer's system. Voice activated HUDs, such as Google Glass, enable voice operated control of the customers lock's from anywhere in the World. Google Glass allows for different authentication scenarios such as voice entered

PIN codes to grant hands-free access to the lock, image-based authentication, etc. Eventually a Google Glass style headset may be able to allow the user to look at their hand, read gestures or read their fingerprints or other biometric data, such as pulse, vasculature, etc., and grant access

5

#### New Access Control Service Subscription

In accordance with an embodiment of the proposed solution Figure 5 is a schematic message passing diagram illustrating primitives employed in establishing a new access control service.

- 10 Assuming an authentication between the administrator user and an AR device and an authentication between the lock and the cloud-based ACS, registration entails adding a new user of type "administrator". Assuming a single administrator scenario, this message also defines a new configuration. The response to the new user message is a request for credentials.
- 15 Depending on the AR device used, the credential response includes an AR device type and the corresponding credential. For example, if the device is a "smartphone" the credential can be "PIN", Codeword, Un/LockPattern, etc. If the device is a tablet the credential can be "PIN", Codeword, Un/LockPattern, Un/LockGesture, etc.
- 20 Figure 6 is an example of a pin unlock code input screen, whereas Figure 7 is an example of a fingerprint reader input screen such as provided by AIRPrint incorporating the use of the HUD-mounted camera and AR application to get the intuitive biometric input with assistive feedback shown in Figure 7.

- Following the registration procedure, the Admin user logs in by requesting admin
- 25 privileges via the AR device and providing the corresponding credentials. The following description makes an abstraction of other primitives such as are necessary in changing credentials on a particular device, etc.

A logged in admin can enroll a new lock and a new user.



In enrolling a new lock, the Admin user provides an admin credential for the lock via an "Add Lock ()" command. This credential can be different depending on the device employed. In some deployment scenarios, the credential is the admin credential employed by the Admin user to authenticate with the ACS cloud. The

5 ACS cloud responds with requesting "New Lock ()" particulars. The Admin enters the LockID, and the AR device provides the ACS cloud service the entered LockID and the current location of the AR device. The ACS cloud service respond with "Stored ()" message. In this way a number of locks can be enrolled with the ACS cloud service. Enrolling locks can be terminated by a "Logout()" command, for

10 example.

In enrolling a new user, the Admin user provides an admin credential for administering a new user's profile via an "Add User ()" command. This credential can be different depending on the device employed. In some deployment scenarios, the credential is the admin credential employed by the Admin user to

15 authenticate with the ACS cloud. The ACS cloud responds with requesting "New User ()" particulars. The Admin enters the user name and the device the user is allowed to employ to actuate managed locks into the Admin's AR heads-up display device. The AR device provides the ACS cloud service the new user's name and the user's device. The user's device unique device identifier which can be a

20 smartphone IMEI, a Media Access Control (MAC) address, etc. The ACS cloud service contacts the device based on the unique device identifier. Alternately the user could connect to the ACS cloud and enter a code provided by the Administrator if contacting the user's device is not practical or possible. The user's device displays a credential entry screen and user enters the credentials, for

25 example a Codeword or an Un/LockPattern. The ACS cloud service responds to the Admin's AR heads-up device with "Stored ()" message. In this way a number of new users can be enrolled with the ACS cloud service. Enrolling users can be terminated by a "LogoutO" command, for example.

Once at least one lock and at least one user are enrolled with the ACS service,

30 users and locks can be associated thus granting users access to locks and

therefore access to specific facilities. The Admin user provides an admin credential for associating user(s) profiles with LockIDs via an "Add Association ()" command. This credential can be different depending on the device employed; the credential is the admin credential employed by the Admin user to authenticate with the ACS cloud. The ACS cloud responds with requesting "New Pair ()" particulars. The Admin enters the user name and LockID the user is allowed actuate into the Admin's AR heads-up display device. The AR device provides the ACS cloud service the user's name and LockID. The ACS cloud service responds with "Stored ()" message. The ACS cloud service also sends a "Grant ( LockID )" message to the user's device based on the user's profile, and the user's device stores the LockID. In this way a number of users can be associated with locks. Associating users with locks can be terminated by a "Logout()" command, for example. It is noted that compatibility between locks and users' devices is not required as the locks are actuated and authenticated by the ACS cloud service.

15

#### Enrolled User Operating an Enrolled Lock

In accordance with the proposed solution, Figure 8 illustrates a method granting access to a facility.

Accessing a facility may be initiated, for example by a user actuating an EAP of an enrolled lock. The lock can broadcast its LockID only in response to the actuation; this can reduce power requirements for a battery operated lock. However the enrolled lock can periodically emit in-the-blind a signal identifying itself. For example, the lock can blink an LED in an identification pattern. Optionally the lock can inform the ACS cloud service of a tamper incident by providing its LockID and optionally the local time. The time of the tamper incident can also be generated by the ACS cloud service at the time of the receipt of the "Tamper ()" message.

20  
25

The heads-up display AR device of the user reads the LockID, for example via an app executing on the AR device. Alternatively, and without limiting the invention thereto, as illustrated in Figure 10 the LockID can be in the form of a QR-code

which can be read by the AR device via a QR code reader app. While references to QR codes are made throughout this application, it is understood that other marker types can be employed and are more generically referred to as AR markers, bar codes (both 1D and 2D), etc. The AR device performs a lookup based on the LockID to determine whether the LockID corresponds to a known lock thereto. If the LockID is unknown the AR device displays "restricted access" indicia. If the LockID is known, the AR device displays at least open indicia signifying that the lock can be opened for example displays a particular icon. The user interacts with the open indicia to request access. The AR device responds by logging in to the ACS cloud service providing the user name and location. An open request can be implicit or explicit as illustrated providing the LockID broadcast locally by the lock. The ACS cloud service requests the login credentials from the heads-up display AR device and the AR device presents the user with a credential input screen. Once the unlock gesture is input, the AR device provides the ACS cloud service with the credential.

With the removal of the limitation of a fixed controlled facility and collocation between the lock and geographical location, the location becomes an actor. The ACS cloud service performs a lookup based on the LockID provided by the lock and determines if the user location and the location of the lock match. Inside buildings location can be provided by location markers, essentially a sort range broadcasting milestone device. A positive match with respect to the location results in a "Success ()" message being sent to the heads-up display AR device and an "Unlock ()" message being sent to the lock itself. An actuation of the lock EAP results in an open door. While the ACS cloud service clears the tamper indication. In some implementations, the tamper flag is only cleared if the "Success ()" message was generated within a predetermined period of time since the "Tamper ()" message. In other implementations the "Unlock ()" message carries a predetermined period of time within which the lock is to remain in the unlocked state.

### Enrolled User Grants Access to an Enrolled Lock

Along with authentication the person, the person's location can also add to the process with location based services available today on all smartphones. For  
5 example it becomes possible to remotely allow entry to a visiting grandmother. That is the person actuating the lock's EAP need not necessarily be the owner/registered user.

Figure 9 illustrates a message passing diagram implementing remote lock opening by an enrolled user.

10 For example the process can be initiated by an unenrolled person by actuating the EAP of the enrolled lock. In response, the lock emits its LockiD which is received by the unenrolled user's AR device. Alternatively, the lock can emit its LockiD continuously. Yet another way, the lock can bear a unique QR code identifying the lock, QR code which is read by the unenrolled person's AR device via a QR code  
15 reader. (The LockiD can be displayed to the unenrolled person.) Optionally the AR device of the unenrolled person provides the location of the AR device to the ACS cloud service informing the ACS cloud service that the AR device is in front of the door.

With the LockiD, the unenrolled person places a voice call to a user associated with  
20 the lock. The LockiD is provided to either the enrolled user as a voice communication or to the enrolled user's AR device via inter device communications (including an SMS message, an iMessage, a BBM message, etc.) The enrolled user authenticates with his/her heads-up display AR device and provides the LockiD for opening the door. The heads-up display AR device performs a lookup  
25 to determine if the LockiD corresponds to a lock with which it is associated (and/or administers if the enrolled user is the administrator). If the lock is known, then the heads-up display AR device logs in the enrolled user with the ACS cloud service. In response, the ACS cloud service can provide a lock tamper report with a LockiD and the time of the lock's EAP actuation. The head-up display AR device compares

the LockID provided by the user with the LockID from the tamper message and reassures the enrolled user that indeed a person is in front of the door. The time of the tamper incident can provide further reassurance that the voice call and the tamper are happening in real time. Optionally the enrolled user can ask the  
5 unenrolled user to actuate the lock's EAP which results in the ACS cloud service providing another tamper report as a further reassurance to the enrolled user.

When sufficiently reassured that the unenrolled person is in front of the correct door, the enrolled user can chose to unlock the door by interacting with unlock indicia on his heads-up display AR device. An "Open( LockID )" message is send from the  
10 enrolled user's heads-up display AR device to the ACS cloud service, the LockID being provided to ensure that there is no ambiguity as to which lock is being actuated. As a further optional sanity check, the ACS cloud service can compare the location associated with the LockID and the location reported by the unenrolled user are the same before proceeding.

15 Next, the ACS cloud service requests credentials from the enrolled user to unlock the lock. As before, the heads-up display AR device displays a credential input screen, for example but not limited to as shown in Figures 6 or 7. After the enrolled user enters the unlock gesture, the credentials are provided by the heads-up display device to the ACS cloud service which responds with a "Success ()" message.

20 The ACS cloud service also sends an "Unlock ( timeDuration )" command to the lock and clears the tamper condition for the LockID. The timeDuration parameter is optional, the lock can have a present time duration for which it unlocks when instructed to do so.

The success of the remote opening is displayed to the enrolled user via the heads-  
25 up display AR device and the enrolled user can instruct the unenrolled user to try opening the door again. If the actuation of the EAP takes place within the timeDuration of the "UnLock ()" command the door opens.

Having described the above facility access granting processes, a variety of advanced access granting processes are possible. For example:

Advanced Facility Access Granting

Current advances are being made in authentication, for example:

5 \* TouchGo, by Kaba, is a non-invasive wireless technology allowing users to keep a physical token on their person for accessing a door lock. TouchGo uses intra-body low frequency communication to convey authentication information (RFID or Bluetooth 4.0). Such tokens can be in the form of a ring worn on a finger, incorporated into a smart watch, worn as a jewelry pendant.

10 \* Another non-invasive technology is provided by Eye Lock which uses a commodity smart phone/tablet camera and a cloud service to provide iris scanning in providing authentication.

15 \* Electronic tattoos, by The Rogers Research Group at the University of Illinois at Urbana-Champaign, are printed directly on skin and generally include the components of an RFID card and a stretchable battery. Such an electronic tattoo can be employed to authenticate the person wearing it for an extended period of time, about two weeks, it takes for the skin to naturally exfoliate the tattoo.

20 \* Ingestible tokens, by Proteus Digital Health, have been FDA-approved for medical applications to identify a medicine pill type, which when ingested emits an 18-bit signal like an electrocardiogram identifying the medicine pill type. Such technology can be extended to provide a unique signal identifying a particular pill, which can be employed to authenticate the person who swallowed it for an extended period of time it takes for the pill to pass through the digestive tract. The authentication can be activated by touch, since the human body conducts electricity.

25 \* Currently available injectable RFID tokens, typically employed in elder care and assisted living scenarios, can provide surgically removable long term authentication.

In accordance with a preferred embodiment of the proposed solution, the enrolled user's AR device is a heads-up display device configured to detect when the heads-

up display device is taken off and put on. For example, such functionality can be implemented by: detecting electrical continuity through the users' skin between two electrodes, detecting a continuous heart beat in a heads-up display device configured to also measure heart rate, detecting repeated identification beacon  
5 messages from body worn/ingested/tattooed/implanted tokens (mentioned above), etc. In this way an initial authentication between the enrolled user and the heads-up display device can be employed as persistent authentication to automatically authenticate the enrolled user with the ACS cloud service.

Similarly in the preferred embodiment the lock provides information identifying the  
10 lock either: via a repeatedly broadcast blinking pattern, via a Bluetooth beacon message, via a WiFi beacon message, via NFC messaging, etc. Alternatively the lock has displayed thereon a QR-code identifying at least the lock and perhaps the ACS service with which the lock is enrolled and the heads-up display AR device executes a QR code reader app. For certainty, broadcasting LockID information  
15 upon actuating the lock EAP is not excluded.

For example, a modified lock opening procedure is illustrated in Figure 11. A single authentication with the heads-up display device is performed once the heads-up display device is put on. The heads-up display device automatically displays the credential input screen, for example as illustrated in Figures 6 or 7, if a body  
20 worn/ingested/tattooed/implanted tokens (mentioned above), etc. identification beacon message is not detected. One of the advantages of displaying a credential input screen on a heads-up display device is that the credential entry is private. In order for the credential not to be discerned by others from user's gestures, the virtual keypad displayed as illustrated in Figure 6 can be scrambled and/or can be  
25 rescrambled with each combination digit entry.

Referring to the description of the messages exchanged as illustrated in Figure 8, a more automated and expedient unlock method can be achieved by removing the authentication step for the enrolled user to actuate the lock EAP. As well, the unlocked state the lock can be displayed to the enrolled user privately via the  
30 heads-up display device for the predetermined timeDuration.

In accordance with yet another embodiment of the proposed solution, the procedure illustrated in Figure 11 is slightly modified as illustrated in Figure 12.

Namely, the timeDuration the lock is to be unlocked for is set to a very short duration such as a few seconds, for example 2sec at a particular time provided by  
5 the ACS cloud service to both the lock and the heads-up display device. The heads-up display device is then configured to countdown to the unlock time specified.

Customized functionality based of the location of devices linked to your account (i.e. the mother in-law cannot open the front door unless someone is home and then she  
10 can come in on her own, etc.)

While the invention has been shown and described with referenced to preferred embodiments thereof, it will be recognized by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention as defined by the appended claims.

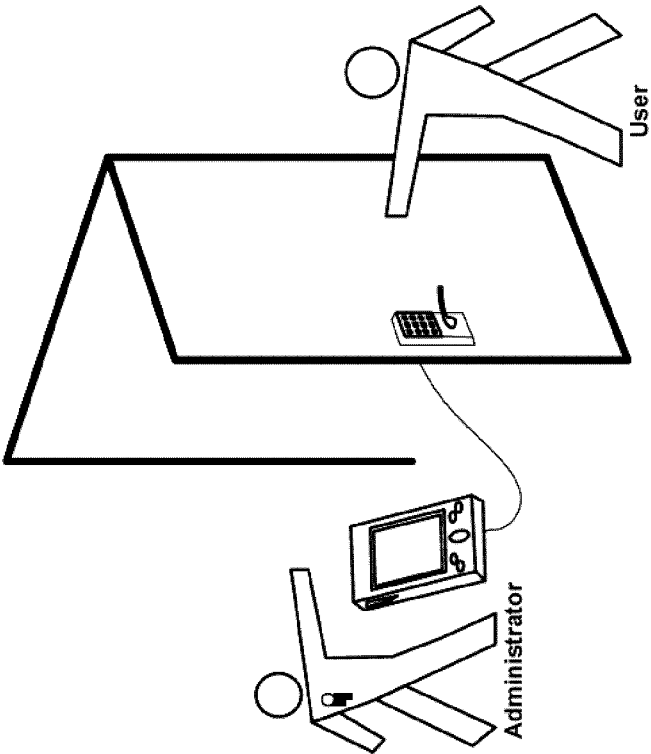


**What is claimed is:**

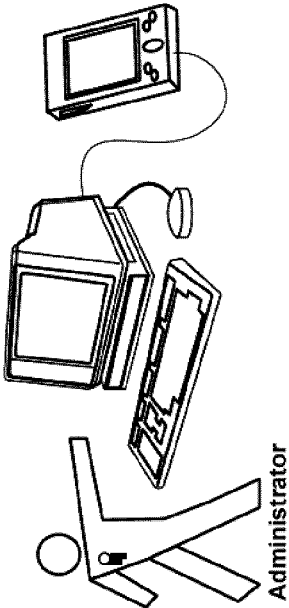
1. An access control system for granting access to a facility for one of physical and logical access control, the system comprising:
  - a. a controlled lock configured to communicate with a remote access control server via data network infrastructure, said controlled lock providing lock identification information; and
  - b. a heads-up display device configured to provide a human-machine interface enabling a user to input credentials to unlock said controlled lock, said heads-up display device being further configured to communicate wirelessly with said remote access control server via said public data network infrastructure, said heads-up display device including a forward facing camera configured to obtain lock identification information from said lock.
2. A system as claimed in claim 1, wherein providing lock identification information said controlled lock comprises displaying a AR code specifying lock identification information, and wherein said heads-up display device includes coded logic instructions executing on a processor implementing a QR code reader to obtain said lock identification information.
3. A system as claimed in claim 1 or 2, wherein providing lock identification information said controlled lock is configured to broadcast said lock identification information.
4. A system as claimed in claim 3, wherein broadcasting said lock identification information said lock is configured to emit an LED blinking pattern specifying said lock identification information.
5. A system as claimed in claim 3, wherein broadcasting said lock identification information said lock is configured to wirelessly transmit a wave train specifying said lock identification information.
6. A system as claimed in any of claims 1 to 5, wherein said heads-up display device further comprises coded logic instructions executing on said processor implementing hand gesture recognition employing said forward facing camera.

7. A system as claimed in any of claims 1 to 6, wherein said heads-up display device further comprises coded logic instructions executing on said processor implementing fingerprint image capture and configured to provide one of fingerprint identification and biometric identification.
8. A method for granting access to a facility, the method comprising:
  - a. identifying a lock by obtaining lock identification information;
  - b. determining whether said lock is associated with a heads-up display device;
  - c. authenticating a user wearing said heads-up display device with a remote access control system server executing logic instruction implementing facility access control;
  - d. requesting opening of said lock; and
  - e. informing the user wearing said heads-up display to proceed with actuating a knob of said lock.
9. A method as claimed in claim 8, wherein obtaining lock identification information the method comprising optically acquiring lock identification information via a forward facing camera mounted on said heads-up display device.
10. A method as claimed in claim 8 or 9, wherein acquiring lock identification information the method comprising recognizing a blinking pattern of an LED of said lock.
11. A method as claimed in claim 8 or 9, wherein acquiring lock identification information the method comprising recognizing a QR code associated with said lock.
12. A method as claimed in claim 8, wherein obtaining lock identification information the method comprising wirelessly acquiring lock identification information via a receiver configured to receive a wave train specifying said lock identification information, wherein said receiver is one of a Bluetooth receiver and a WiFi receiver.

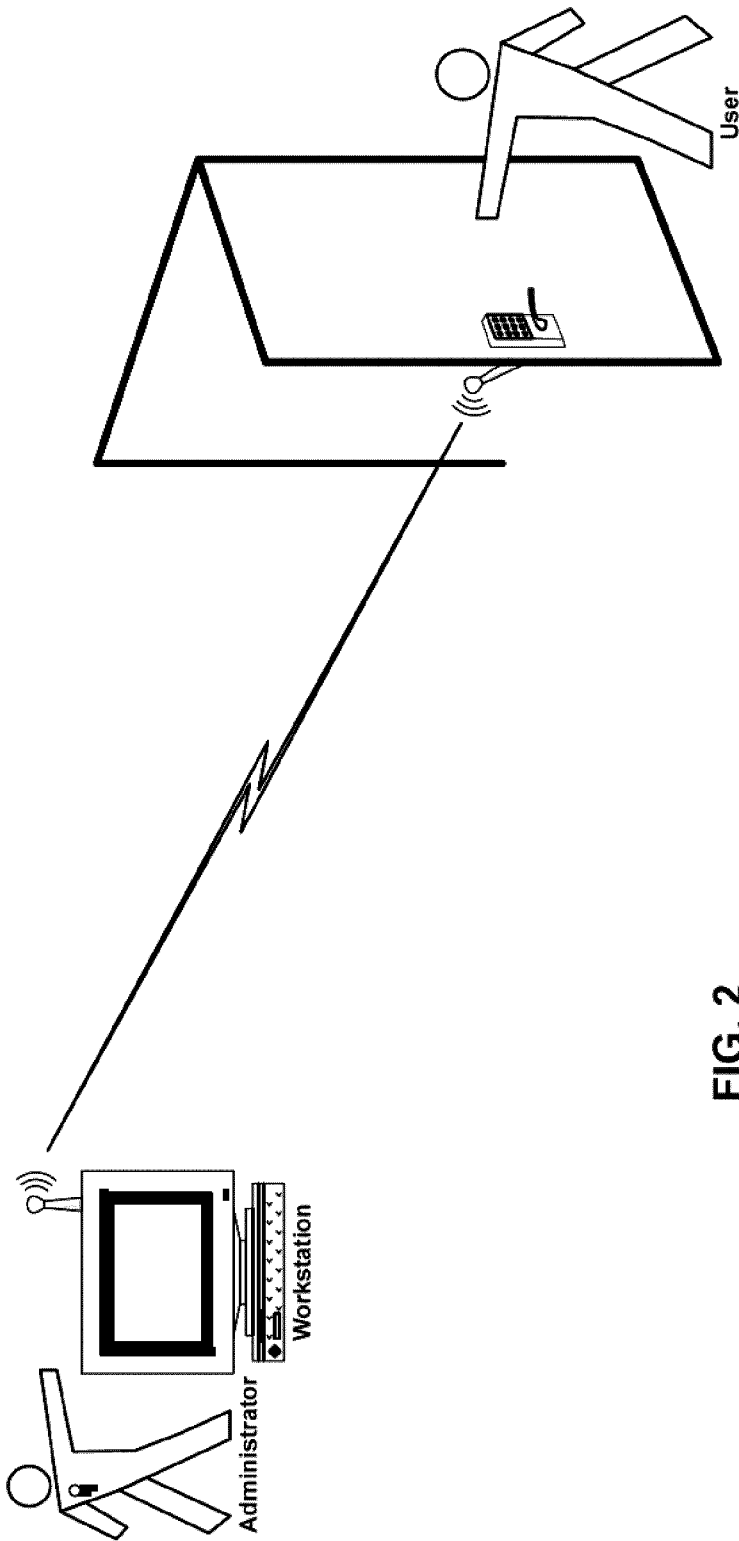
13. A method as claimed in any of claims 8 to 12, wherein authenticating said user the method further comprises obtaining a hand gesture via said forward facing camera of said heads-up display device.
14. A method as claimed in claim 13, wherein obtaining said hand gesture the method comprising executing coded logic instructions on a processor for detecting said hand gesture.
15. A method as claimed in any of claims 8 to 12, wherein authenticating said user the method further comprises obtaining a fingerprint via said forward facing camera of said heads-up display device.
16. A method as claimed in claim 15, wherein obtaining said fingerprint the method comprising executing coded logic instructions on a processor for detecting said fingerprint.



**FIG. 1B**  
**PRIOR ART**

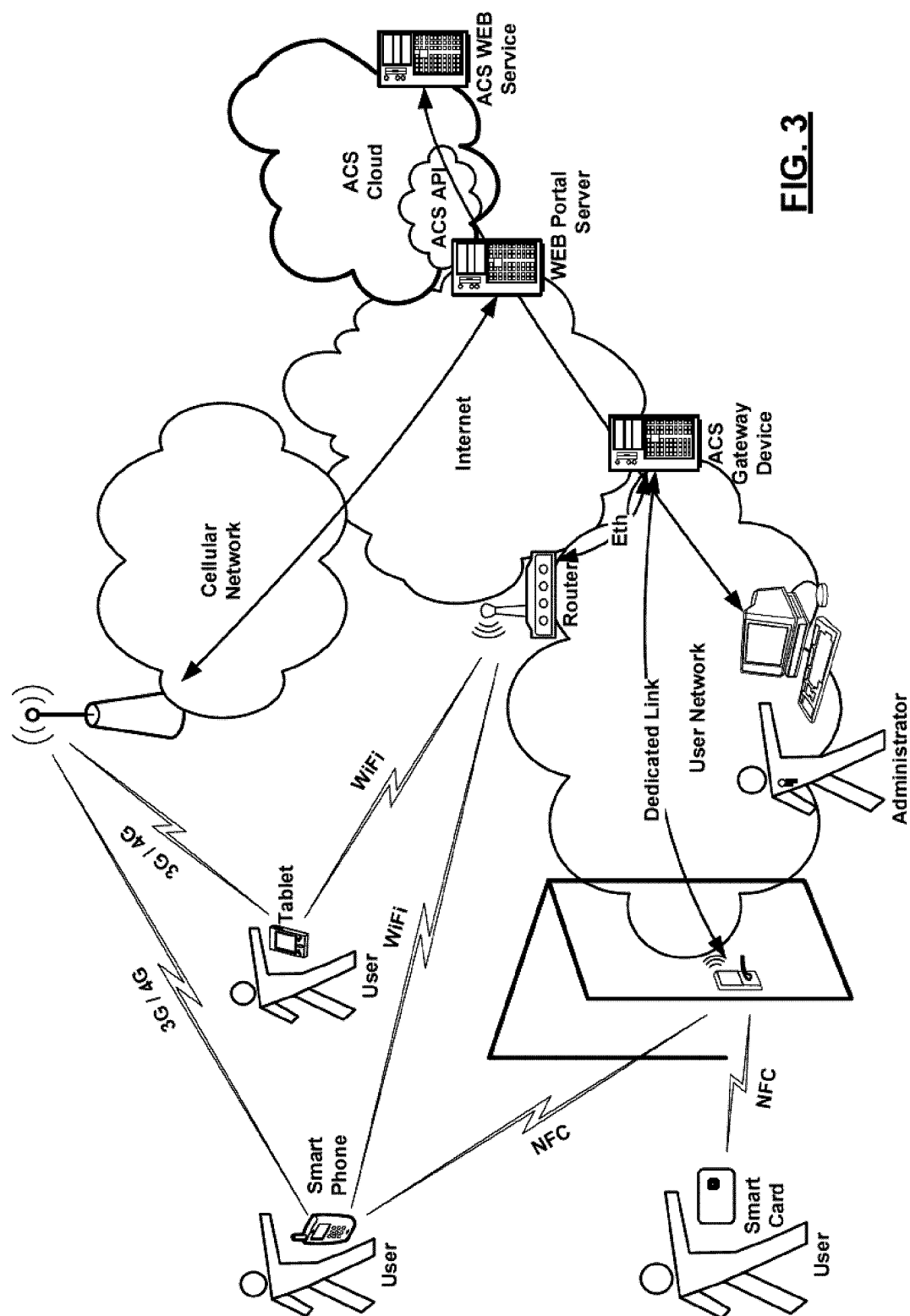


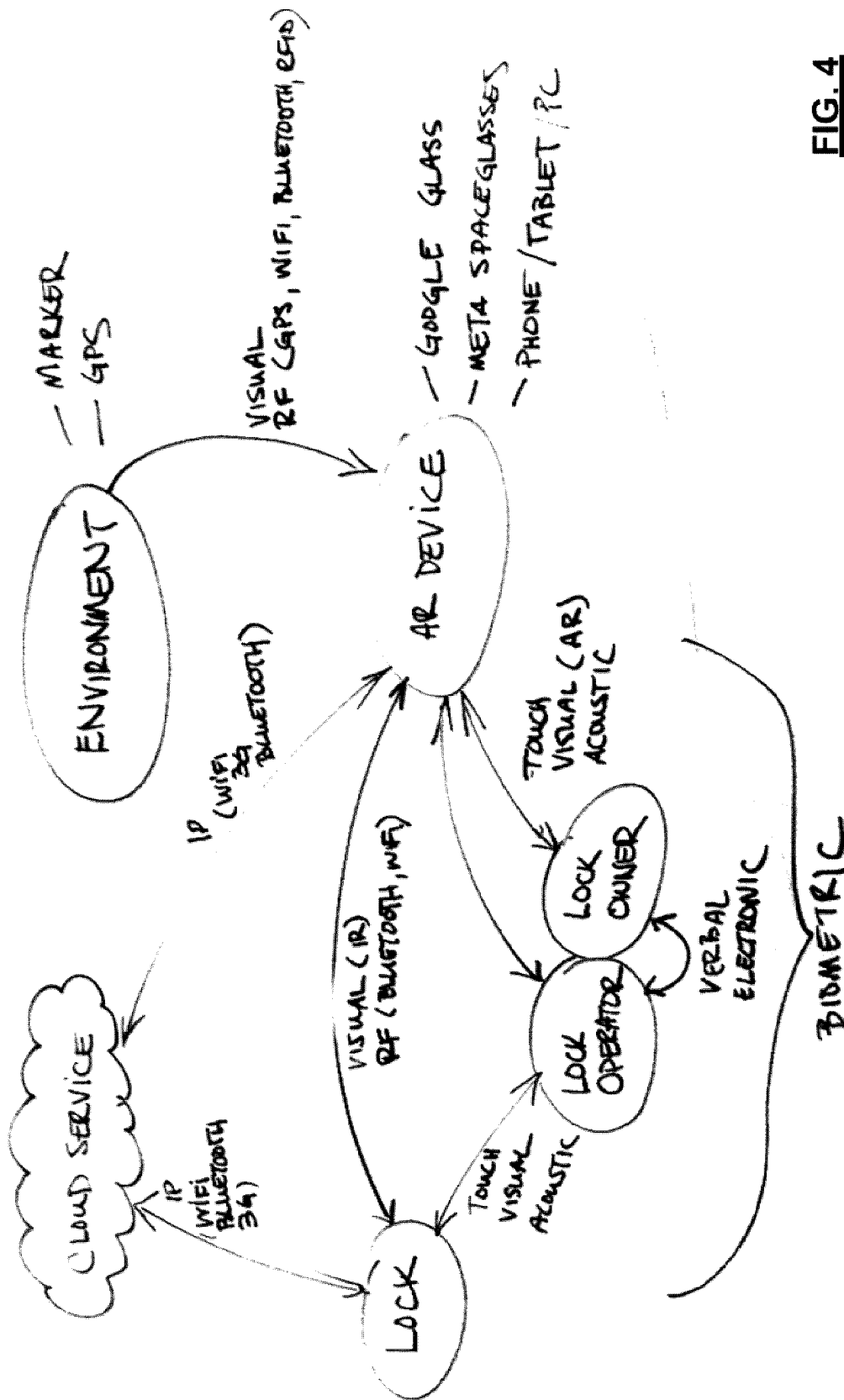
**FIG. 1A**  
**PRIOR ART**



**FIG. 2**  
**PRIOR ART**

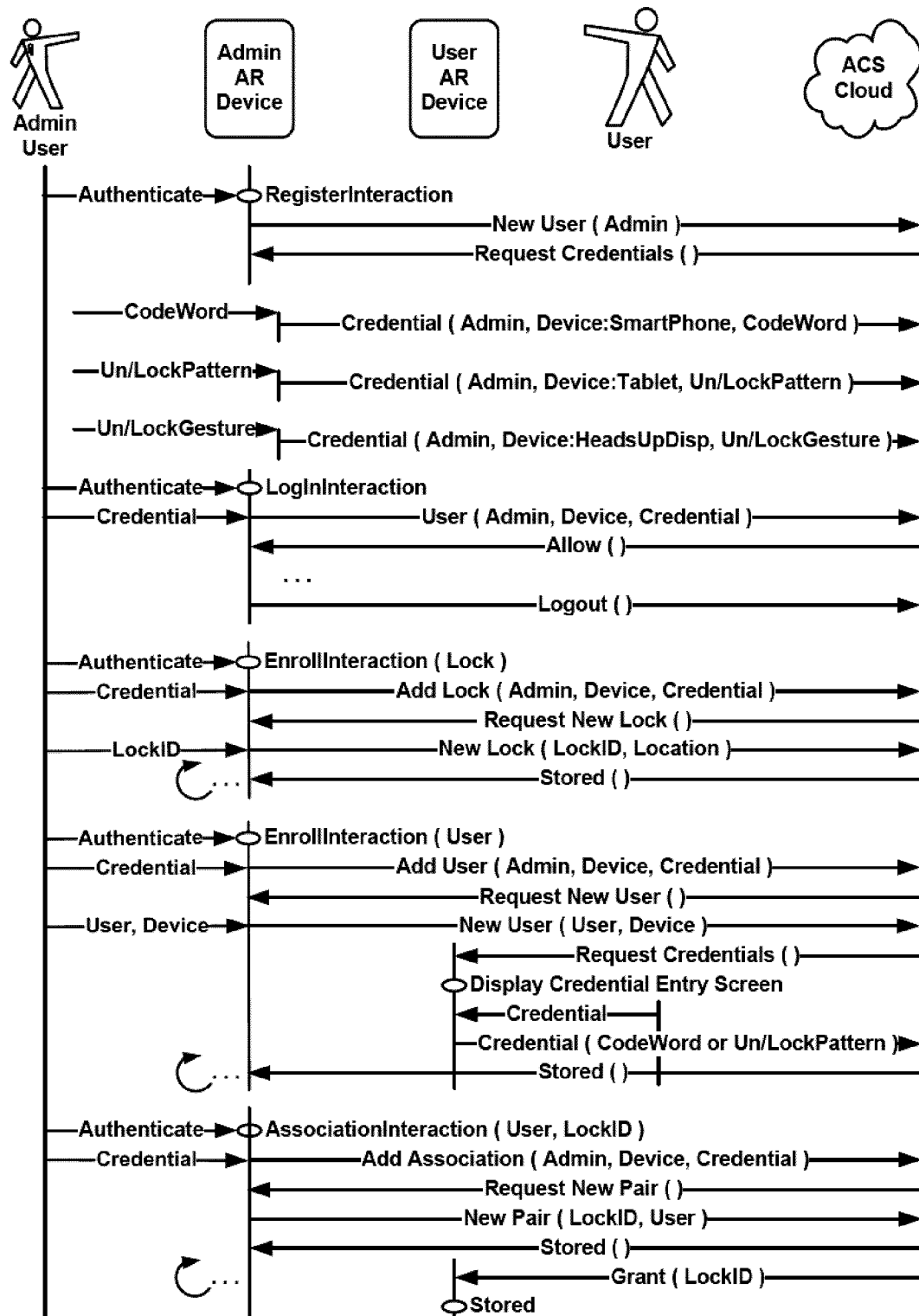
3 / 12

**FIG. 3**



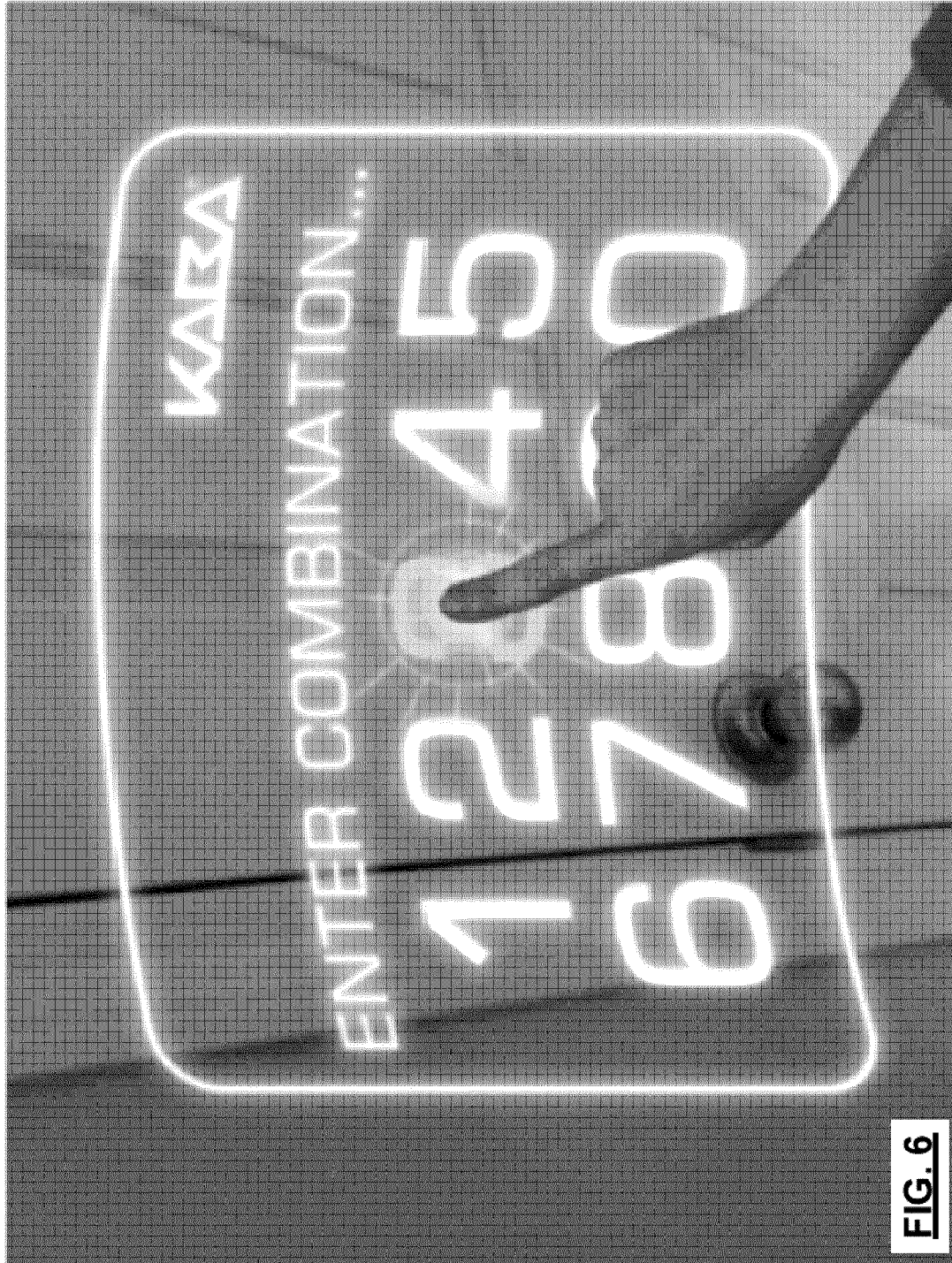
**FIG. 4**

5 / 12

**FIG. 5**

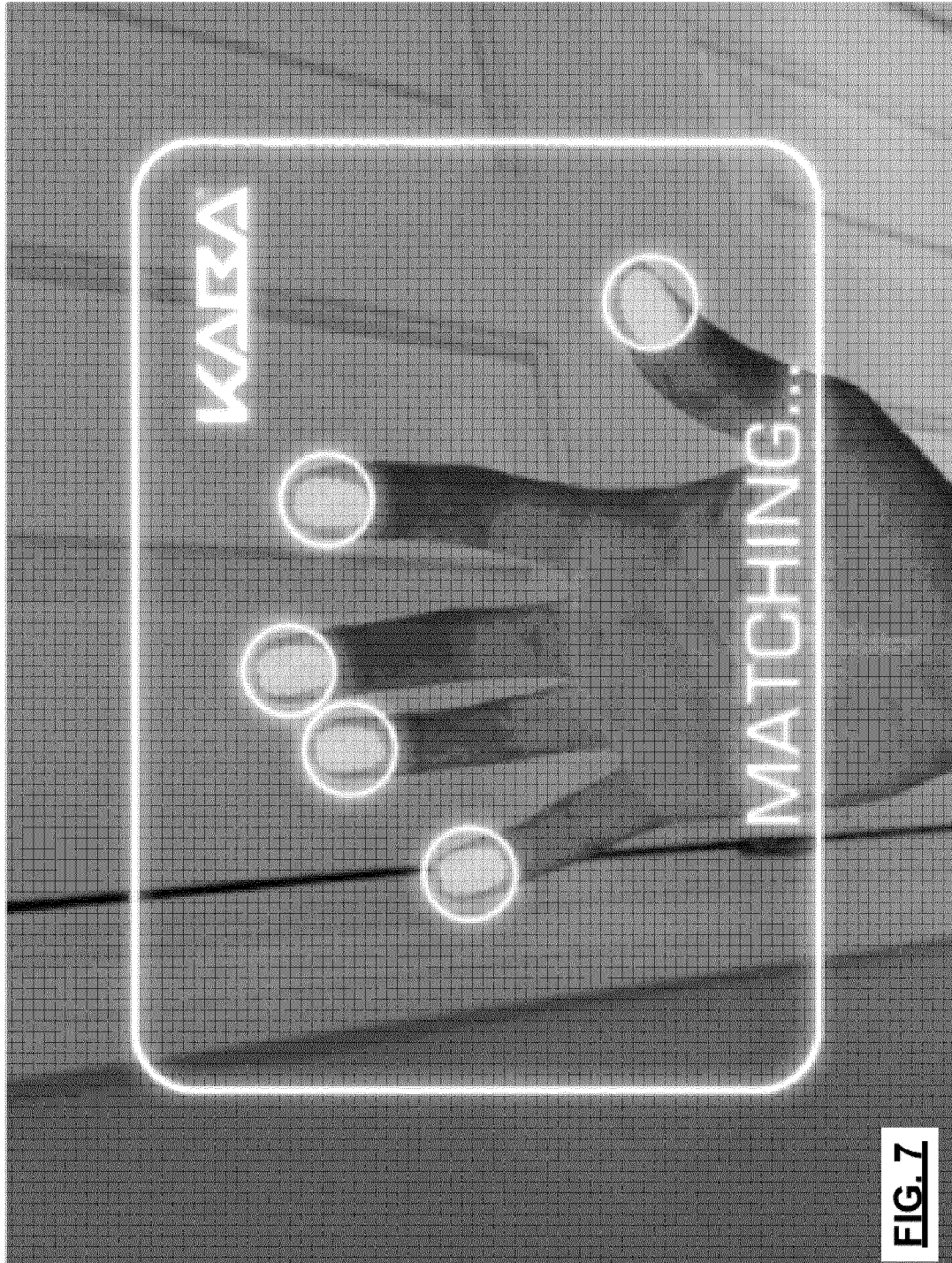


6 / 12



**FIG. 6**

7 / 12



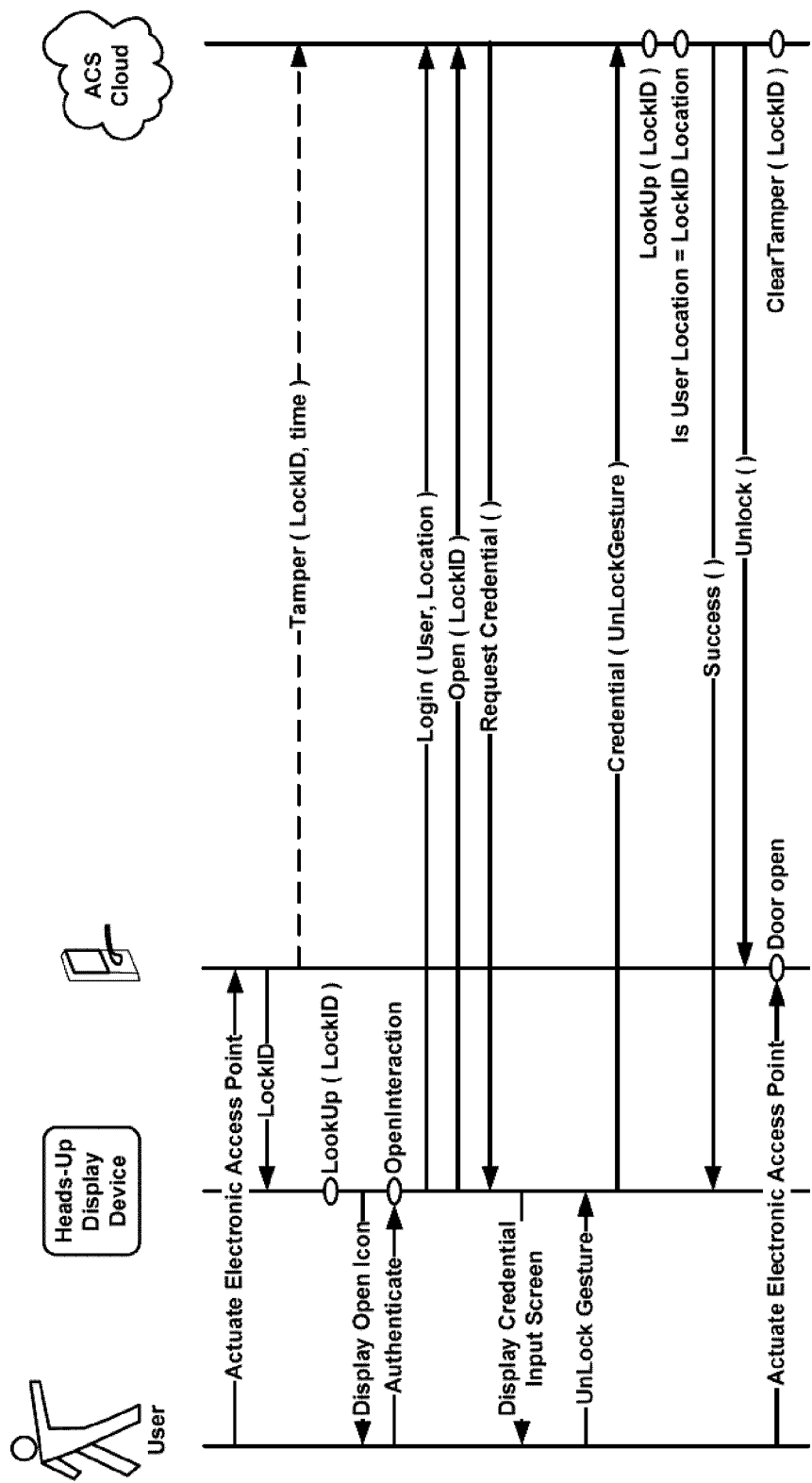
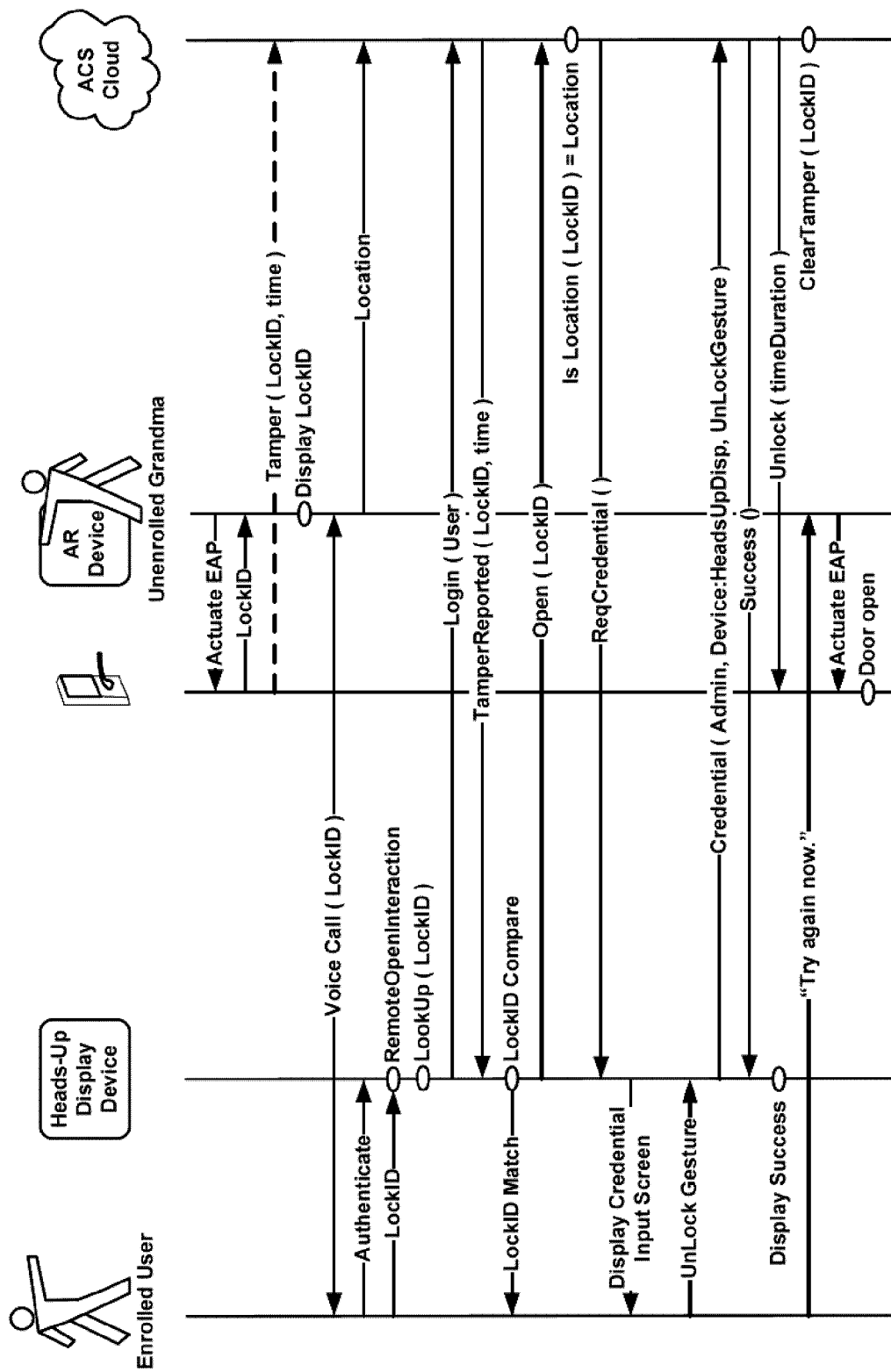


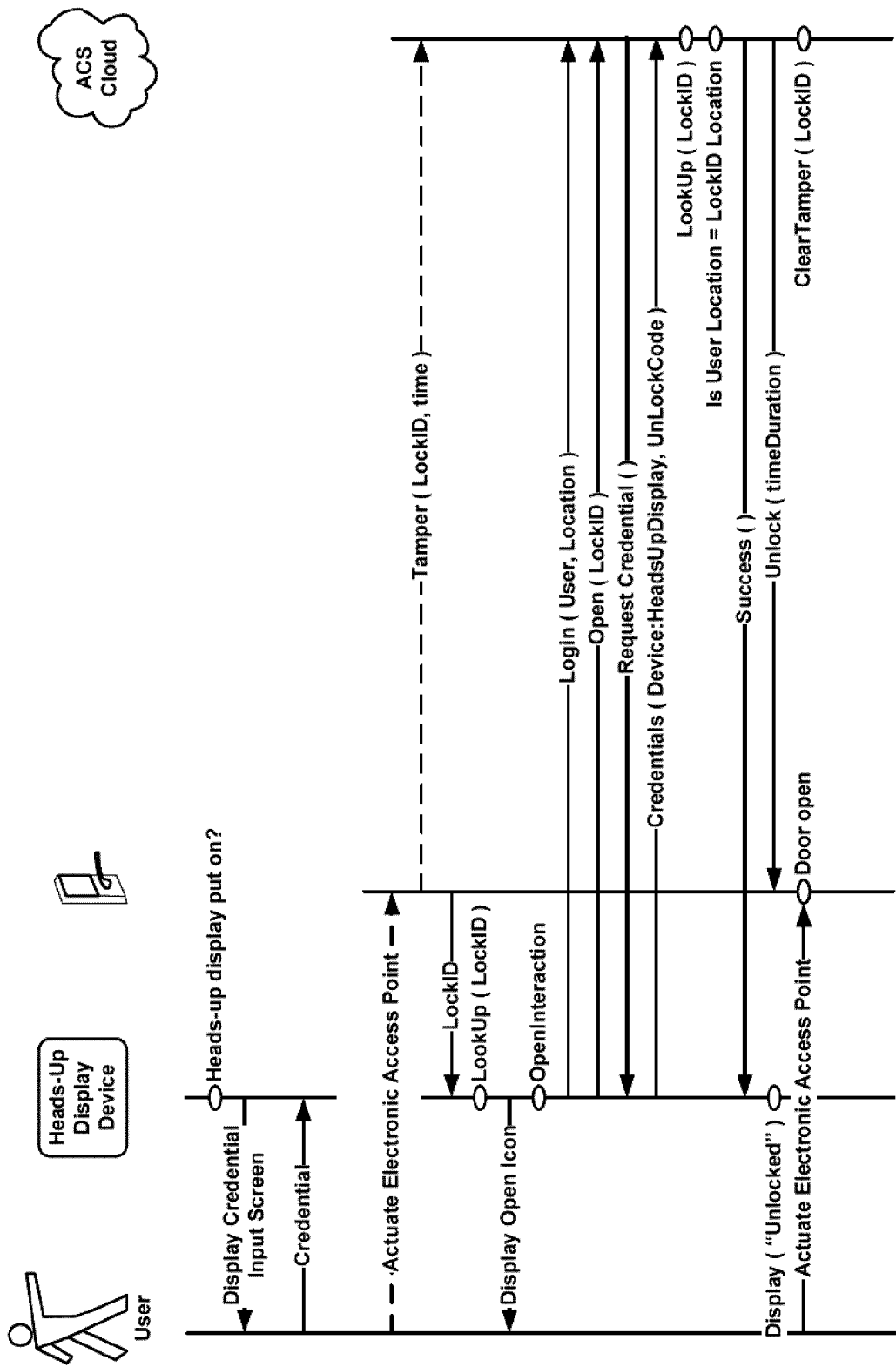
FIG. 8



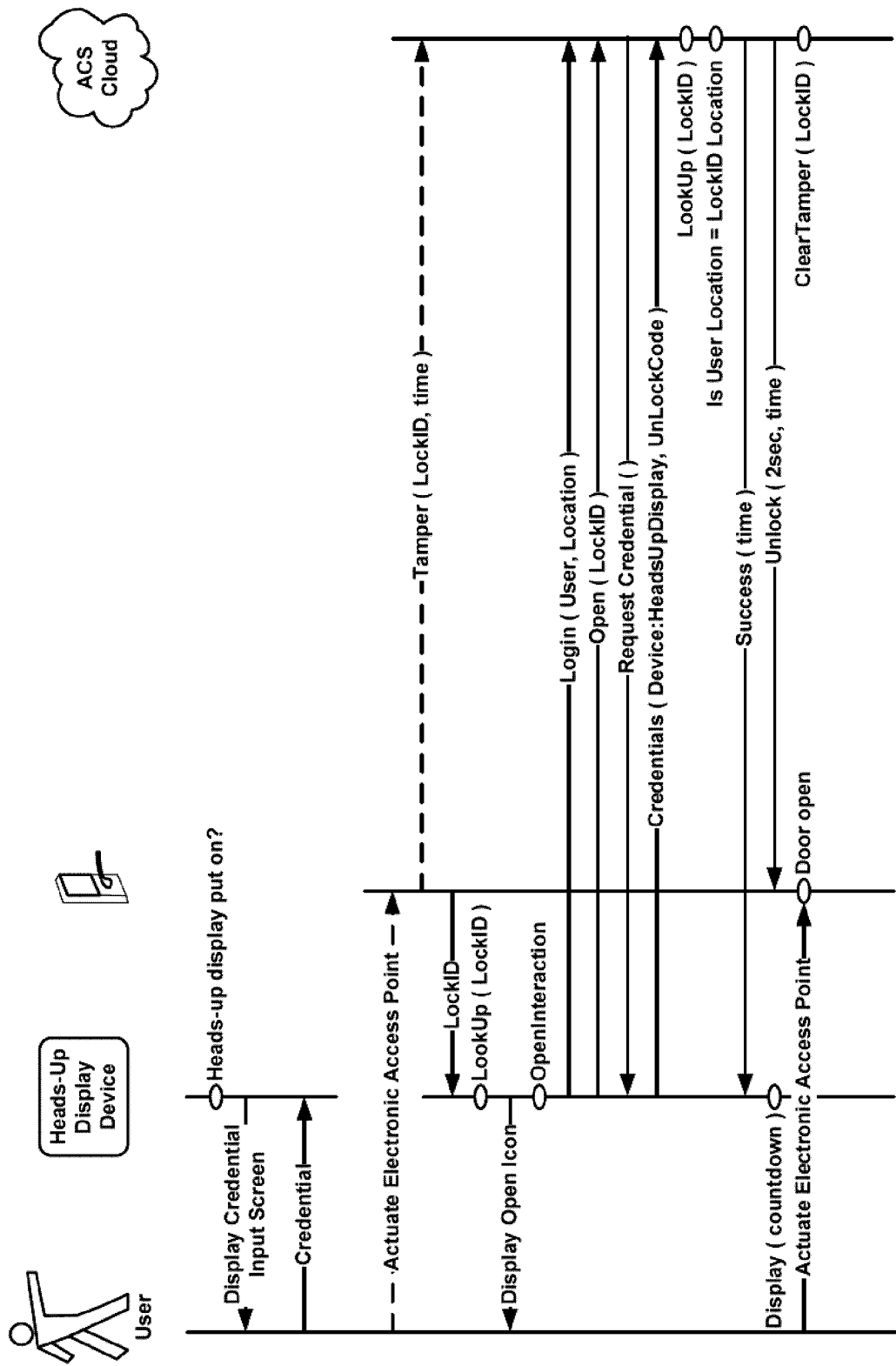
**FIG. 9**



FIG. 10



**FIG. 11**



**FIG. 12**

## INTERNATIONAL SEARCH REPORT

International application No.

**PCT/CA2014/051207**

A. CLASSIFICATION OF SUBJECT MATTER  
IPC: **G07C 9/00** (2006.01) , **G02B 27/01** (2006.01)

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

## B. FIELDS SEARCHED



Minimum documentation searched (classification system followed by classification symbols)  
IPC: G07C 9/00 (2006.01), G02B 27/01 (2006.01)

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)  
Databases: Questel-Orbit (FamPat), Canadian Patent Database, IEEE Xplore. Search terms: grant, provide, control, permit, restrict, access, intelligent, lock, electronic access point, door, gate, entrance, facility, location, site, premises, property, authentication, identification, security, server, remote, wireless, heads-up display, google, HUD, glasses, camera, biometric, gesture, motion, LED, Bluetooth, WiFi, Internet.

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages  | Relevant to claim No. |
|-----------|---|-----------------------|
| X         | US 8,430,310 B1 (Ho et al.) 30 April 2013 (30-04-2013)<br>*entire document*   | 1-16                  |
| A         | US 2013/0221094 A1 (Smith et al.) 29 August 2013 (29-08-2013)<br>*abstract*<br>*paragraphs [0014], [0016], [0018], [0027]-[0035]*<br>*Figures 2, 3* |                       |
| A         | US 2012/0222103 A1 (Bliding et al.) 30 August 2012 (30-08-2012)<br>*paragraphs [0088]-[0098], [0123]-[0147]*<br>*Figures 4, 5*                      |                       |
|           | -/--  |                       |

 Further documents are listed in the continuation of Box C.  See patent family annex.

|                                      |  |                          |  |
|--------------------------------------|--|--------------------------|--|
| *<br>"A"<br>"E"<br>"L"<br>"O"<br>"P" | Special categories of cited documents:<br>document defining the general state of the art which is not considered to be of particular relevance<br>earlier application or patent but published on or after the international filing date<br>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)<br>document referring to an oral disclosure, use, exhibition or other means<br>document published prior to the international filing date but later than the priority date claimed | "T"<br>"X"<br>"Y"<br>"&" | 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<br>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<br>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<br>document member of the same patent family |
|--------------------------------------|--|--------------------------|--|

Date of the actual completion of the international search  
14 January 2015 (14-01-2015)

Date of mailing of the international search report  
09 March 2015 (09-03-2015)

Name and mailing address of the ISA/CA  
Canadian Intellectual Property Office  
Place du Portage I, CI 14 - 1st Floor, Box PCT  
50 Victoria Street  
Gatineau, Quebec K1A 0C9  
Facsimile No.: 001-819-953-2476

Authorized officer  
  
Georges Matar (819) 635-8043



## INTERNATIONAL SEARCH REPORT

International application No.

**PCT/CA2014/051207**

| C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT |  |                       |
|---|--|-----------------------|
| Category*   | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
| A   | US 7,962,369 B2 (Rosenberg) 14 June 2011 (14-06-2011)<br>*column 32, line 49 - column 33, line 14*<br>*column 27, line 28 - column 28, line 22*<br>*claims 25-32*<br>*Figure 20* |                       |
| A   | US 2009/0113543 A1 (Adams et al.) 30 April 2009 (30-04-2009)<br>*column 2, line 58 - column 5, line 38*<br>---   |                       |

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.

**PCT/CA2014/051207**

| Patent Document<br>Cited in Search Report | Publication<br>Date         | Patent Family<br>Member(s)   | Publication<br>Date   |
|---|-----------------------------|--|---|
| US843031 0B1                              | 30 April 2013 (30-04-2013)  | None   |   |
| US201 3221 094A1                          | 29 August 2013 (29-08-2013) | EP281 778A2<br>WO201 3 126675A2  | 31 December 2014 (31-12-2014)<br>29 August 2013 (29-08-2013)  |
| US201 22221 03A1                          | 30 August 2012 (30-08-2012) | EP250481 8A1<br>EP250481 8A4<br>SE0950904A1<br>SE534520C2<br>WO201 1065892A1   | 03 October 2012 (03-10-2012)<br>20 November 2013 (20-11-2013)<br>28 May 2011 (28-05-2011)<br>20 September 2011 (20-09-2011)<br>03 June 2011 (03-06-2011)  |
| US7962369B2                               | 14 June 2011 (14-06-2011)   | US200823861 0A1<br>US201 127651 1A1<br>WO2008042302A2<br>WO2008042302A3  | 02 October 2008 (02-10-2008)<br>10 November 2011 (10-11-2011)<br>10 April 2008 (10-04-2008)<br>10 July 2008 (10-07-2008)  |
| US20091 13543A1                           | 30 April 2009 (30-04-2009)  | CA2641 862A1<br>CA2641 862C<br>CA2703304A1<br>CA2703304C<br>EP2053531A1<br>EP2053531 B1<br>EP2301 186A1<br>EP2301 186A4<br>US20091 44540A1<br>WO2009052637A1 | 25 April 2009 (25-04-2009)<br>04 February 2014 (04-02-2014)<br>30 April 2009 (30-04-2009)<br>20 May 2014 (20-05-2014)<br>29 April 2009 (29-04-2009)<br>30 July 2014 (30-07-2014)<br>30 March 2011 (30-03-2011)<br>31 October 2012 (31-10-2012)<br>04 June 2009 (04-06-2009)<br>30 April 2009 (30-04-2009) |