CLAIMS

1. A computer-implemented method for access control identification, the method comprising the steps of:

selecting, by a selection module of a mobile device, an identifier prestored in a memory device of the mobile device (501);

retrieving, by a scanning module of the mobile device, a biometric data from a user (502);

determining, by a matching module of the mobile device, a match between the retrieved biometric data and a biometric data of an authorized user that is prestored in a memory device of the mobile device (503);

encrypting, by an encryption module of the mobile device, a selected identifier using an encryption key and mobile device's time stamp information (505);

converting, by a conversion module of the mobile device, the selected identifier into a displayable access code carrying a time stamp to indicate its expiry time (506);

generating, by the conversion module of the mobile device, a new access code encrypted using an updated time stamp comprising the selected identifier to replace an expired access code (507);

displaying, by a display of the mobile device, an updated access code to an access point (508); and

scanning, by the access point, the updated access code to provide access to the user upon validation of the updated access code (509);

wherein the access point is in communication with a computing device which connects to a same server with the mobile device, such that the access point synchronises its clock with the mobile device through communication with the computing device at a predetermined time;

wherein the access point communicates with a code reader, in which the code reader decrypts the access code using an encryption key obtained from the computing

device and a time stamp of the code reader, to obtain the selected identifier, for the selected identifier to be compared with a reference identifier stored in a controller that is in communication with the code reader; and

wherein the access point shall deny access to the user when the code reader fails to decrypt the access code using the time stamp of the code reader, when the selected identifier fails to match with the reference identifier, or when the code reader determines that the time stamps of the mobile device and the code reader fail to fall within an expiry threshold.

2. The method according to claim 1, wherein the biometric data comprises fingerprints, hand characteristics, eye characteristics, facial characteristics, voice characteristics or in any combination thereof.

3. The method according to claim 1, wherein the identifier comprises user credentials and a unique identifier retrieved from the mobile device.

4. The method according to claim 1 further comprising the steps of:

scanning, by the scanning module of the mobile device, the biometric data of the user for registration of the authorised user (201); and

storing the registered biometric data of the authorised user in the memory device.

5. The method according to claim 1, wherein the server is connected to Network Time Protocol (NTP) for clock synchronization.

6. The method according to claim 1 further comprising the step of converting, by the conversion module, the encrypted identifier from raw string data into two-dimensional barcode (603) that corresponds to the access code.

7. The method according to claim 1 further comprising the step of transmitting entry records from the controller to the computing device (507).

8. The method according to claim 1 further comprising the steps of:

transmitting, by the code reader, the decrypted access code to a controller;

determining, by the controller, validity of the access code and transmit a signal to an actuator upon validation of the access code (509); and

determining, by the controller, an operative mode of the actuator in response to the transmitted signal (510).

9. An access control identification system comprising:

a mobile device (101) comprising:

a scanning module (102) for retrieving a biometric data from a user;

a matching module (103) for determining a match between the retrieved biometric data and a biometric data of an authorized user that is prestored in a memory device (110) of the mobile device (101);

a selection module (104) for selecting an identifier associated with the matched biometric data from a plurality of identifiers prestored in the memory device (101);

an integrity module (117) for securing integrity of the selected identifier;

an encryption module (116) for encrypting the selected identifier using an encryption key and time stamp information;

a conversion module (105) for converting the selected identifier into a displayable access code carrying a time stamp to indicate its expiry time and generating a new access code carrying an updated time stamp using the selected identifier to replace an expired access code;

a display (106) for displaying an updated access code;

an access point (107) for scanning the updated access code to provide access to the user upon validation of the updated access code;

a computing device (108) in communication with the access point (107); and

a server (109) for connecting to the computing device (108) and to the mobile device (101) such that the access point (107) synchronises its clock with the mobile device (101) through communication with the computing device (108) at a predetermined time;

wherein the access point (107) communicates with a code reader (111), in which the code reader (111) decrypts the access code using an encryption key obtained from the computing device (108) and a time stamp of the code reader (111), to obtain the selected identifier, for the selected identifier to be compared with a reference identifier stored in a controller (112) that is in communication with the code reader (111); and

wherein the access point (107) shall deny access to the user when the code reader (111) fails to decrypt the access code using the time stamp of the code reader (111), when the selected identifier fails to match with the reference identifier, or when the code reader (111) determines that the time stamps of the mobile device (101) and the code reader (111) fail to fall within an expiry threshold.