Claims

1. A computerized method implemented on a mobile device of a user for controlling access to a facility, the method comprising:

communicating access details of the facility from the mobile device to the facility for a first authentication process, the mobile device located in front of the facility initially in a secured state for preventing access thereto, the access details being embedded in a quick response (QR) code displayed by the mobile device at a time when the mobile device is located in front of the facility, the QR code being refreshed at a defined frequency by a client server, wherein a host server is configured to authenticate the access details in a first authentication process by comparing the received QR code with a current version of the QR code from the client server;

receiving a request notification on the mobile device in response to positive authentication of the access details from the first authentication process, the request notification comprising a request for biometric data of the user, the positive authentication comprising confirming that the mobile device is in front of the facility;

receiving an input of the biometric data on the mobile device; and

communicating the biometric data from the mobile device to the host server for a second authentication process,

wherein the facility is configured to change from the secured state to an unsecured state in response to positive authentication, by the host server, of the biometric data from the second authentication process, thereby providing, to the user, access to the facility.

2. The method according to claim 1, wherein the facility comprises an electronic device for maintaining the facility in the secured state and the access details are communicated from the mobile device to the electronic device of the facility based on the mobile device being located in front of the electronic device and the facility reverts from the unsecured state to a secured state after a set period of time.

3. The method according to claim 1, wherein the access details comprise a dynamic identifier generated at a time of reservation of the facility for the user, the dynamic identifier including a timestamp generated at a time of confirmation of the reservation of the facility.

4. The method according to claim 1, further comprising performing a registration process prior to communication of the access details to the facility.

5. The method according to claim 4, the registration process comprising:

generating identifier data associated with a user account of the user, the identifier data including a media access control (MAC) address of the mobile device;

receiving an input of reference biometric data associated with the user account on the mobile device; and

communicating the reference biometric data from the mobile device to the host server for the second authentication process.

6. The method according to claim 1, wherein the positive authentication of the biometric data from the second authentication process comprises matching the biometric data with stored reference data based on a set of conditions defined by the host server and stringency of the matching is adjusted by the host server based on characteristics of the facility.

7. The method according to claim 1, wherein the QR code is refreshed by synchronizing the QR code between the host server and the client server.

8. The method according to claim 1, wherein the access details are matched with stored records in the first authentication process.

9. The method according to claim 1, further comprising receiving, on the mobile device, a confirmation notification in response to the facility successfully changing from the secured state to the unsecured state.

10. A system for controlling access to a facility, the system comprising:

a host server comprising a processor and a memory configured to store computer-readable instructions, wherein when the instructions are executed, the processor is caused to:

receive access details of the facility from the facility, the access details communicated from a mobile device of a user located in front of the facility in a secured state for preventing access thereto, the access details being embedded in a quick response (QR) code displayed by the mobile device at a time when the mobile device is located in front of the facility, the QR code being refreshed at a defined frequency by a client server associated with the facility;

authenticate the access details in a first authentication process by comparing the received QR code with a current version of the QR code from the client server;

communicate a request notification to the mobile device in response to positive authentication of the access details from the first authentication process, the positive authentication comprising confirming that the mobile device is in front of the facility, the request notification comprising a request for biometric data of the user;

receive the biometric data inputted via the mobile device;

authenticate, by the host server, the biometric data in a second authentication process; and

change the facility from the secured state to an unsecured state in response to positive authentication of the biometric data from the second authentication process, thereby providing, to the user, access to the facility.

11. The system according to claim 10, wherein the facility comprises an electronic device for maintaining the facility in the secured state and the access details are communicated from the mobile device to the electronic device of the facility based on the mobile device being located in front of the electronic device and the facility reverts to a secured state after a set period of time.

12. The system according to claim 10, wherein the access details comprise a dynamic identifier generated at a time of reservation of the facility for the user, the dynamic identifier including a timestamp generated at a time of confirmation of the reservation of the facility.

13. The system according to claim 10, wherein when the instructions are executed, the processor is further caused to authenticate the access details received from the facility against an access records database during the first authentication process.

14. The system according to claim 10, wherein when the instructions are executed, the processor is further caused to authenticate the biometric data received from the mobile device against a biometric database during the second authentication process.

15. The system according to claim 10, wherein the OR code is refreshed by synchronizing the QR code between the host server and the client server.

16. The system according to claim 10, further comprising performing a registration process prior to receiving the access details from the facility.

17. The system according to claim 16, the registration process comprising:

generating identifier data associated with a user account of the user, the identifier data including a media access control (MAC) address of the mobile device; and

receiving reference biometric data from the mobile device for the second authentication process, the reference biometric data associated with the user account.

18. The system according to claim 10, wherein authenticating the biometric data in the second authentication process comprises matching the biometric data with stored reference data based on a set of conditions defined by the host server and a

stringency of the matching is adjusted by the host server based on characteristics of the facility.

19. The system according to claim 10, wherein when the instructions are executed, the processor is further caused to perform a reservation process to book the facility.

20. A non-transitory computer-readable medium storing computer-readable instructions that, when executed, cause a processor of a host server to:

receive access details of a facility from the facility, the access details provided by a mobile device of a user, the mobile device located in front of the facility in a secured state, the access details being embedded in a quick response (QR) code displayed by the mobile device at a time when the mobile device is located in front of the facility, the QR code being refreshed at a defined frequency by a client server associated with the facility;

authenticate the access details in a first authentication process by comparing the received QR code with a current version of the QR code from the client server;

communicate a request notification to the mobile device in response to positive authentication of the access details from the first authentication process, the positive authentication comprising confirming that the mobile device is in front of the facility, the request notification comprising a request for biometric data of the user;

receive the biometric data inputted via the mobile device;

authenticate, by the host server, the biometric data in a second authentication process; and

change the facility from the secured state to an unsecured state in response to positive authentication of the biometric data from the second authentication process, thereby providing, to the user, access to the facility.