SYSTEMS AND METHODS FOR USE IN AUTHENTICATING INDIVIDUALS, IN CONNECTION WITH PROVIDING ACCESS TO THE INDIVIDUALS

CROSS-REFERENCE TO RELATED APPLICATION

This application claims the benefit of, and priority to, U.S. Provisional Application No. 62/190,284 filed on July 9, 2015. The entire disclosure of the above application is incorporated herein by reference.

FIELD

The present disclosure generally relates to systems and methods for use in authenticating individuals (*e.g.*, confirming identities of individuals, etc.), using biometric data for the individuals, in connection with providing access to the individuals, for example, to computing devices, program applications, secure locations, secure documents (broadly, secure items), etc.

BACKGROUND

This section provides background information related to the present disclosure which is not necessarily prior art.

For security reasons, access to various computing devices (including applications available via the computing devices) and/or to various locations is often limited or restricted to particular individuals. That is, to gain access to the computing devices, for example, the individuals must have permission to access the computing devices. It is further known that, to gain access, the individuals must present proper credentials (*e.g.*, proper usernames, passwords, passcodes, pins, tokens, biometrics, combinations thereof, etc.) directly at the computing devices (or applications) or directly at the secure locations to authenticate the individuals. Such computing devices, applications and locations, which require the individuals to have permission and access credentials, are generally referred to as secured.

SUMMARY

According to a first aspect of the present disclosure, there is provided a portable communication device for use in authenticating a user to provide access to the user to multiple secure items including one or more other devices and/or

applications different from the portable communication device, the device comprising a memory configured to store a reference biometric for a user; a biometric reader; and a processor coupled to the memory and to the biometric reader, the processor configured to compare a biometric of the user, captured at the biometric reader, to the reference biometric stored in the memory; and when the captured biometric matches the reference biometric: authenticate the user to the portable communication device; and transmit an authentication signal to the multiple secure items for a duration of a broadcast interval, the authentication signal including an identifier associated with the user, to thereby provide the user with access to the multiple secure items different from the portable communication device without repeated, separate authentication of the user at the multiple secure items.

According to a second aspect of the present disclosure, there is provided a computer-implemented method for authenticating a user to provide access to the user, the computer-implemented method comprising capturing, at a portable communication device, a biometric from a user relating to a desired access; comparing the captured biometric to a reference biometric stored in memory of the portable communication device; and transmitting, by the portable communication device, for a duration of a broadcast interval, an authentication signal to multiple computing devices, the authentication signal including an identifier associated with the user, when the captured biometric matches the reference biometric, to thereby provide the user access to the multiple computing devices without repeated, separate authentication of the user at the multiple computing devices, wherein the multiple computing devices are different than the portable communication device.

According to yet another aspect of the present disclosure, there is provided a non-transitory computer readable storage media comprising computer-executable instructions that, when executed by at least one processor, cause the at least one processor to compare a biometric of a user, received at a portable communication device, to at least one reference biometric; authenticate the user and permit access, for the user, to at least one of the portable communication device and an application at the portable communication device, when the biometric of the user matches the at least one reference biometric; decline access to the user, to at least one of the portable communication device and an application at the portable communication device, when the received biometric does not match the at least one reference biometric; and transmit, from the portable communication device, an

authentication signal during a duration of at least one interval, to multiple different computing devices, whereby the user is able to access the multiple different computing devices receiving the transmitted authentication signal, without repeated, separate authentication of the user at the multiple different computing devices.

DRAWINGS

The drawings described herein are for illustrative purposes only of selected embodiments and not all possible implementations, and are not intended to limit the scope of the present disclosure.

What is claimed is:

1. A portable communication device for use in authenticating a user to provide access to the user to multiple secure items including one or more other devices and/or applications different from the portable communication device, the device comprising:

a memory configured to store a reference biometric for a user;

a biometric reader; and

a processor coupled to the memory and to the biometric reader, the processor configured to:

compare a biometric of the user, captured at the biometric reader, to the reference biometric stored in the memory; and

when the captured biometric matches the reference biometric:

authenticate the user to the portable communication device; and

transmit an authentication signal to the multiple secure items for a duration of a broadcast interval, the authentication signal including an identifier associated with the user, to thereby provide the user with access to the multiple secure items different from the portable communication device without repeated, separate authentication of the user at the multiple secure items.

2. The portable communication device of claim 1, wherein the identifier includes a username for the user and associated with the multiple secure items; and

wherein the authentication signal further includes an authentication code.

3. The portable communication device of claim 1, wherein the biometric reader comprises a fingerprint scanner; and

wherein the memory is configured to store a reference biometric comprising at least one reference fingerprint.

4. The portable communication device of claim 1, wherein the portable communication device includes a smartphone; and

wherein the processor is configured, in order to transmit the authentication signal, to broadcast, via an output device of the smartphone, the authentication signal within a vicinity of the smartphone for the broadcast interval.

5

5. The portable communication device of claim 4, wherein the processor is configured to provide the authentication signal to the multiple secure items associated with the smartphone, whereby the user is permitted one or more rights in each of the multiple secure items without providing a further authentication at the multiple secure items.

6. The portable communication device of claim 4, wherein the processor is further configured, in response to a user command, to pair the smartphone with at least one of the multiple secure items, such that when the authentication signal is broadcast, said signal is recognized by the at least one of the multiple secure items.

7. The portable communication device of claim 4, further comprising a near field communication (NFC) transceiver including the output device; and

wherein the processor is configured to broadcast the authentication signal, by the NFC transceiver.

8. The portable communication device of claim 4, further comprising a Bluetooth® transceiver including the output device; and

wherein the processor is configured to broadcast the authentication signal, by the Bluetooth® transceiver.

9. The portable communication device of claim 4, further comprising a display including the biometric reader.

10. The portable communication device of claim 1, further comprising at least one of the multiple secure items, the at least one of the multiple secure items being configured to impose at least one user specific setting thereto, based on a user profile associated with the user, upon providing access to the user to the at least one of the multiple secure items.

11. A computer-implemented method for authenticating a user to provide access to the user, the computer-implemented method comprising:

capturing, at a portable communication device, a biometric from a user relating to a desired access;

comparing the captured biometric to a reference biometric stored in memory of the portable communication device; and

5

transmitting, by the portable communication device, for a duration of a broadcast interval, an authentication signal to multiple computing devices, the authentication signal including an identifier associated with the user, when the captured biometric matches the reference biometric, to thereby provide the user access to the multiple computing devices without repeated, separate authentication of the user at the multiple computing devices, wherein the multiple computing devices are different than the portable communication device.

12. The computer-implemented method of claim 11, wherein capturing the biometric includes scanning a fingerprint, at the portable communication device, via a fingerprint scanner included in the portable communication device.

13. The computer-implemented method of claim 12, wherein the identifier is recognizable by the multiple computing devices, whereby each of the multiple computing devices becomes accessible.

14. The computer-implemented method of claim 11, wherein transmitting the authentication signal includes at least one of:

wirelessly broadcasting the authentication signal, from the portable communication device, via a network interface of the portable communication device, and

transmitting the authentication signal, via a physical connection, between the portable communication device and the multiple computing devices.

15. The computer-implemented method of claim 14, wherein the network interface includes one of a near field communication (NFC) transceiver and a Bluetooth® transceiver.

16. The computer-implemented method of claim 11, further comprising storing the reference biometric in the memory of the portable communication device.

17. The computer-implemented method of claim 16, further comprising:

setting a biometric status, at the portable communication device, when the captured biometric matches the reference biometric stored in the memory; and

resetting the biometric status after the broadcast interval, the broadcast interval being 30 seconds or more; and

wherein transmitting the authentication signal includes transmitting the authentication signal only during the broadcast interval.

18. A non-transitory computer readable storage media comprising computer-executable instructions that, when executed by at least one processor, cause the at least one processor to:

compare a biometric of a user, received at a portable communication device, to at least one reference biometric;

authenticate the user and permit access, for the user, to at least one of the portable communication device and an application at the portable communication device, when the biometric of the user matches the at least one reference biometric;

decline access to the user, to at least one of the portable communication device and an application at the portable communication device, when the received biometric does not match the at least one reference biometric; and

transmit, from the portable communication device, an authentication signal during a duration of at least one interval, to multiple different computing devices, whereby the user is able to access the multiple different computing devices receiving the transmitted authentication signal, without repeated, separate authentication of the user at the multiple different computing devices.

19. The non-transitory computer readable storage media of claim 18, wherein the authentication signal includes an authentication code associated with the user and recognizable by the multiple different computing devices.

20. The non-transitory computer readable storage media of claim 18, wherein the computer-executable instructions, when executed by the at least one processor, further cause the at least one processor to pair the portable communication device to one of the multiple different computing devices, in response to a user command, such that when the authentication signal is transmitted, said signal is recognized by the one of the multiple different computing devices.