WHAT IS CLAIMED

1. A method comprising:

generating, by a portable communication device comprising a data processor and a memory storing a personal token, a first random code, the portable communication device being used by a user;

transmitting, by the portable communication device, the first random code to an access device, wherein the access device receives the first random code, generates a second random code, receives the personal token from a user of the portable communication device, and hashes the first random code, the second random code, and the personal token to form a first hash output;

receiving, from the access device, the first hash output and the second random code;

hashing the first random code, the stored personal token, and the second random code to form a second hash output;

determining, by the portable communication device, if the first hash output and the second hash output are equal; and

forming a secure communication channel between the portable communication device and the access device when the first hash output and the second hash output are equal.

2. The method of claim 1, wherein the access device comprises input elements, a data processor, and a memory, wherein the user enters the personal token into the access device via the input elements and the memory is configured to store the personal token and subsequently delete the personal token.

3. The method of claim 1, wherein the secure communication channel is not formed between the access device and the portable communciation device if the first hash output and the second hash output are not equal.

4. The method of claim 1, wherein the secure communication channel utilizes Bluetooth.

5. The method of claim 1, wherein the portable communication device is a mobile phone.

6. The method of claim 1, wherein the method further comprises, after forming the secure communication channel:

transmitting access data from the portable communication device to the access device.

7. The method of claim 6, wherein the access data includes an access token.

8. A portable communication device comprising:

a processor; and

a computer readable medium coupled to the processor, comprising code executable by the processor for implementing a method comprising

generating, by a portable communication device comprising a data processor and a memory storing a personal token, a first random code, the portable communication device being used by a user,

transmitting, by the portable communication device, the first random code to an access device, wherein the access device receives the first random code, generates a second random code, receives the personal token from a user of the portable communication device, and hashes the first random code, the second random code, and the personal token to form a first hash output,

receiving, from the access device, the first hash output and the second random code,

hashing the first random code, the stored personal token, and the second random code to form a second hash output,

~~determining, by the portable communication device, if the first hash output and the second hash output are equal, and~~

~~forming a secure communication channel between the portable communication device and the access device when the first hash output and the second hash output are equal.~~

~~9. The portable communication device of claim 8, wherein the secure communication channel is a secure wireless communication channel.~~

~~10. The portable communication device of claim 9, wherein the secure wireless communication channel utilizes Bluetooth.~~

~~11. The portable communication device of claim 8, wherein the portable communication device is a mobile phone.~~

~~12. The portable communication device of claim 8, wherein the method further comprises, after forming the secure communication channel:~~

~~transmitting access data from the portable communication device to the access device.~~

~~13. The portable communication device of claim 12, wherein the access data is an access token.~~

~~14. A method comprising:~~

~~receiving, by an access device, a personal token from a user;~~

~~receiving, by the access device, a first random code from a portable communication device;~~

~~generating, by the access device, a second random code;~~

~~generating, by the access device, a first hash output of the first random code, the second random code, the personal token;~~

transmitting, by the access device, the second random code and the first hash output to a portable communication device within a vicinity of the access device, wherein the portable communication device generates a second hash output from the personal token, the first random code, and the second random code, and determines if the first hash output and the second hash output are equal; and

forming a secure communication channel between the access device and the portable communication device when the first hash output and the second hash output are the same.

15. The method of claim 14, wherein the portable communication device is a mobile phone.

16. The method of claim 14, wherein the method further comprises, after forming the secure communication channel:

receiving, from the portable communication device, access data;

generating, an authorization request message including the access data; and

transmitting the authorization request message to an authorizing computer.

17. The method of claim 14, wherein the access device allows or does not allow access to a secure location.

18. The method of claim 14, further comprising:

transmitting, by the access device, the at least the second random code to a plurality of additional portable communication devices that do not store the personal token, and that do not form a secure communication channel with the access device.

19. An access device comprising:

a data processor; and

~~a computer readable medium, the computer readable medium comprising code, executable by the processor, for performing a method according to any of claims 14-18.~~

~~20. A system comprising the access device of claim 19, and the portable communication device.~~

WHAT IS CLAIMED

1. A method comprising:

generating, by a portable communication device comprising a data processor and a memory storing a personal token, a first random code, the portable communication device being used by a user;

transmitting, by the portable communication device, the first random code to an access device within a vicinity of the portable communication device, wherein the access device receives the first random code, generates a second random code, receives the personal token from the user of the portable communication device, and hashes the first random code, the second random code, and the personal token to form a first hash output;

receiving, from the access device, the first hash output and the second random code;

hashing the first random code, the stored personal token, and the second random code to form a second hash output;

determining, by the portable communication device, if the first hash output and the second hash output are equal; and

forming a secure communication channel between the portable communication device and the access device when the first hash output and the second hash output are equal.

2. The method of claim 1, wherein the data processor is a first data processor and the memory is a first memory, and wherein the access device comprises input elements, a second data processor, and a second memory, wherein the user enters the personal token into the access device via the input elements and the second memory is configured to store the personal token and subsequently delete the personal token.

3. The method of claim 1, wherein the secure communication channel is not formed between the access device and the portable communication device if the first hash output and the second hash output are not equal.

4. The method of claim 1, wherein the secure communication channel utilizes a short-range communication protocol.

5. The method of claim 1, wherein the portable communication device is a mobile phone.

6. The method of claim 1, wherein the method further comprises, after forming the secure communication channel:

transmitting access data from the portable communication device to the access device.

7. The method of claim 6, wherein the access data includes an access token.

8. The method of claim 1, wherein the portable communication device is a mobile phone and the access device is a point of sale terminal.

9. A portable communication device comprising:

a processor; and

a non-transitory computer readable medium coupled to the processor, comprising code executable by the processor for implementing a method comprising:

generating, by the portable communication device comprising a data processor and a memory storing a personal token, a first random code, the portable communication device being used by a user,

transmitting, by the portable communication device, the first random code to an access device in a vicinity of the portable communication device, wherein the access device receives the first random code, generates a second random code, receives the personal token from the user of the portable communication device, and hashes the first random code, the second random code, and the personal token to form a first hash output,

receiving, from the access device, the first hash output and the second random code,

hashing the first random code, the stored personal token, and the second random code to form a second hash output,

determining, by the portable communication device, if the first hash output and the second hash output are equal, and

forming a secure communication channel between the portable communication device and the access device when the first hash output and the second hash output are equal.

10. The portable communication device of claim 9, wherein the secure communication channel is a secure wireless communication channel.

11. The portable communication device of claim 10, wherein the secure wireless communication channel utilizes a medium range communication protocol.

12. The portable communication device of claim 9, wherein the portable communication device is a mobile phone.

13. The portable communication device of claim 9, wherein the method further comprises, after forming the secure communication channel:

transmitting access data from the portable communication device to the access device.

14. The portable communication device of claim 13, wherein the access data is an access token, wherein the access token is a payment token.

15. A method comprising:

receiving, by an access device, a personal token from a user;

receiving, by the access device, a first random code from a portable communication device;

generating, by the access device, a second random code;

generating, by the access device, a first hash output of the first random code, the second random code, and the personal token;

transmitting, by the access device, the second random code and the first hash output to the portable communication device within a vicinity of the access device, wherein the portable communication device generates a second hash output by

hashing the personal token, the first random code, and the second random code, and determines if the first hash output and the second hash output are equal; and

forming a secure communication channel between the access device and the portable communication device when the first hash output and the second hash output are the same.

16. The method of claim 15, wherein the portable communication device is a mobile phone.

17. The method of claim 15, wherein the method further comprises, after forming the secure communication channel:

receiving, from the portable communication device, access data;

generating, an authorization request message including the access data; and

transmitting the authorization request message to an authorizing computer.

18. The method of claim 15, wherein the access device allows or does not allow access to a secure location.

19. The method of claim 15, further comprising:

transmitting, by the access device, at least the second random code to a plurality of additional portable communication devices that do not store the personal token, and that do not form a secure communication channel with the access device.

20. The method of claim 15, wherein the portable communication device is a mobile phone and the access device is a point of sale terminal.