

WHAT IS CLAIMED IS:

1. A method comprising:
receiving, by an access device from a portable communication device, a second cryptographic pattern that is derived from a base station identifier and a credential or a token, wherein the access device receives the second cryptographic pattern from the portable communication device via a base station associated with the base station identifier;
during a transaction that is conducted at the access device, receiving the credential or the token from a portable transaction device, wherein the credential is a primary account number and the token is a payment token;
generating another cryptographic pattern that is derived from at least the base station identifier and the received credential or token;
comparing the second cryptographic pattern the another cryptographic pattern; and
if the patterns match, sending an authorization request message to a server computer.
2. The method of claim 1, wherein the portable transaction device is a payment card.
3. The method of claim 1, wherein the base station identifier is a UUID.
4. The method of claim 1, wherein the second cryptographic pattern is also derived from a nonce, and the another cryptographic pattern is also derived from the nonce.
5. The method of claim 4, wherein the access device receives the nonce along with the second cryptographic pattern from the portable communication device.
6. The method of claim 1, wherein the access device comprises a point of sale device.
7. The method of claim 1, wherein the second cryptographic pattern is stored at the base station in a list with other cryptographic patterns.
8. The method of claim 1, wherein the authorization request message comprises at least a portion of the another cryptographic pattern, and wherein the server computer compares the at least the portion of the another cryptographic pattern to a first cryptographic pattern at the server computer, the server computer deriving the first cryptographic pattern from the base station identifier and the credential or the token.
9. The method of claim 1, wherein the second cryptographic pattern is derived from the token.
10. The method of claim 1, wherein the portable communication device and the access device communicate via BLE (Bluetooth Low Energy).
11. An access device comprising:
a processor; and
a computer readable medium, the computer readable medium coupled to the processor and comprising code, executable by the processor for implementing operations comprising:
receiving, from a portable communication device, a second cryptographic pattern that is derived from a base station identifier and a credential or a token, wherein the access device

receives the second cryptographic pattern from the portable communication device via a base station associated with the base station identifier;

during a transaction that is conducted at the access device, receiving the credential or the token from a portable transaction device, wherein the credential is a primary account number and the token is a payment token;

generating another cryptographic pattern that is derived from at least the base station identifier and the received credential or token;

comparing the second cryptographic pattern the another cryptographic pattern; and
if the patterns match, sending an authorization request message to a server computer.

12. The access device of claim 11, wherein the base station identifier is a UUID.

13. The access device of claim 11, wherein the access device is a point of sale terminal.

14. The access device of claim 11, wherein the portable communication device and the access device communicate via BLE (Bluetooth Low Energy).

15. The access device of claim 11, wherein the second cryptographic pattern is derived from the token.

16. The access device of claim 11, wherein the access device receives a nonce along with the second cryptographic pattern from the portable communication device.

17. The access device of claim 11, wherein the second cryptographic pattern is also derived from a nonce, and the another cryptographic pattern is also derived from the nonce.

18. The access device of claim 11, wherein the second cryptographic pattern is derived from the credential.