

WHAT IS CLAIMED IS:

1                   1.     A method comprising:  
2                   receiving, by a server computer and from a portable communication  
3 device of a user, a base station identifier that uniquely identifies a resource provider  
4 location;  
5                   hashing, by the server computer, at least a first cryptographic pattern and  
6 the base station identifier to form a second cryptographic pattern, wherein the first  
7 cryptographic pattern is formed from hashing at least a credential or a token;  
8                   receiving, by the server computer, from an access device in a transaction,  
9 an authorization request message; and  
10                  analyzing, by the server computer, the authorization request message to  
11 determine that the user of the portable communication device is conducting the  
12 transaction at the access device by determining that the second cryptographic pattern  
13 corresponds to another cryptographic pattern derived from a credential or a token from  
14 a portable transaction device.

1                   2.     The method of claim 1, wherein the method further comprises, prior  
2 to receiving the base station identifier and the first cryptographic pattern from the  
3 portable communication device:  
4                   associating, by the server computer, the credential or the token with  
5 device information within a database, wherein the device information is received from  
6 the portable communication device;  
7                   receiving, by the server computer, the device information from the portable  
8 communication device;  
9                   searching, by the server computer, the database for the credential or the  
10 token associated with the device information;  
11                  hashing, by the server computer, at least the credential or the token to  
12 form the first cryptographic pattern; and  
13                  transmitting, by the server computer, the first cryptographic pattern to the  
14 portable communication device.

1                   3.     The method of claim 1, wherein determining that the second  
2 cryptographic pattern corresponds to the another cryptographic pattern comprises  
3 determining that the authorization request message includes an indicator indicating that  
4 the access device at the resource provider location determined that the second  
5 cryptographic pattern matched the another cryptographic pattern.

1                   4.     The method of claim 1, wherein determining that the second  
2 cryptographic pattern corresponds to the another cryptographic pattern comprises  
3 determining that the authorization request message includes at least a portion of the  
4 another cryptographic pattern and determining that the portion of the another  
5 cryptographic pattern matches the second cryptographic pattern.

1                   5.     The method of claim 1, wherein the portable transaction device is in  
2 the form of a card and the portable communication device is a phone.

1                   6.     The method of claim 1, wherein the portable transaction device  
2 and the portable communication device are the same device.

1                   7.     The method of claim 1, wherein the first cryptographic pattern is  
2 formed from hashing:  
3                   the credential or the token; and  
4                   a nonce.

1                   8.     The method of claim 1, wherein the portable communication device  
2 also forms the second cryptographic pattern by hashing at least the first cryptographic  
3 pattern and the base station identifier.

1                   9.     The method of claim 1, wherein the base station identifier is a  
2 universally unique identifier (UUID) of the base station.

1                   10.    A server computer comprising:  
2                   a processor; and  
3                   a computer readable medium comprising code, executable by the  
4 processor, for implementing a method comprising:

5                   receiving, by a server computer and from a portable communication  
6 device of a user, a base station identifier that uniquely identifies a resource  
7 provider location;

8                   hashing, by the server computer, at least a first cryptographic  
9 pattern and the base station identifier to form a second cryptographic pattern,  
10 wherein the first cryptographic pattern is formed from hashing at least a  
11 credential or a token;

12                  receiving, by the server computer, from an access device in a  
13 transaction, an authorization request message; and

14                  analyzing, by the server computer, the authorization request  
15 message to determine that the user of the portable communication device is  
16 conducting the transaction at the access device by determining that the second  
17 cryptographic pattern corresponds to another cryptographic pattern derived from  
18 a credential or a token from a portable transaction device.

1                  11.    The server computer of claim 10, wherein the method further  
2 comprises, prior to receiving the base station identifier and the first cryptographic  
3 pattern from the portable communication device:

4                  associating, by the server computer, the credential or the token with  
5 device information within a database, wherein the device information is received from  
6 the portable communication device;

7                  receiving, by the server computer, the device information from the portable  
8 communication device;

9                  searching, by the server computer, the database for the credential or the  
10 token associated with the device information;

11                  hashing, by the server computer, at least the credential or the token to  
12 form the first cryptographic pattern; and

13                  transmitting, by the server computer, the first cryptographic pattern to the  
14 portable communication device.

1                  12.    The server computer of claim 10, wherein determining that the  
2 second cryptographic pattern corresponds to the another cryptographic pattern  
3 comprises determining that the authorization request message includes an indicator

4 indicating that the access device at the resource provider location determined that the  
5 second cryptographic pattern matched the another cryptographic pattern.

1           13.    The server computer of claim 10, wherein determining that the  
2 second cryptographic pattern corresponds to the another cryptographic pattern  
3 comprises determining that the authorization request message includes at least a  
4 portion of the another cryptographic pattern and determining that the portion of the  
5 another cryptographic pattern matches the second cryptographic pattern.

1           14.    The server computer of claim 10, wherein the portable transaction  
2 device is in the form of a card and the portable communication device is a phone.

1           15.    The server computer of claim 10, wherein the portable transaction  
2 device and the portable communication device are the same device.

1           16.    The server computer of claim 10, wherein the base station identifier  
2 is a universally unique identifier (UUID) of the base station.

1           17.    A method comprising:  
2           responsive to detecting, at a portable communication device of a user, a  
3 beacon at a resource provider, transmitting device information to a server computer;  
4           receiving, by the portable communication device and from the server  
5 computer, a first cryptographic pattern that is formed from at least a credential or a  
6 token;  
7           receiving, by a portable communication device from a base station at the  
8 resource provider, a base station identifier;  
9           hashing at least the first cryptographic pattern and the base station  
10 identifier to form a second cryptographic pattern; and  
11           electronically providing the second cryptographic pattern to an access  
12 station and/or transmitting at least the base station identifier to the server computer,  
13 wherein when the access station receives the second cryptographic pattern, the access  
14 station:  
15           compares the second cryptographic pattern to another cryptographic  
16 pattern derived from a credential or a token from a portable transaction device; and

17                   if the patterns match, sends an authorization request message that  
18 comprises at least a portion of the another cryptographic pattern to the server computer.

1                   18.    The method of claim 17, wherein the method further comprises,  
2 prior to detecting the beacon, transmitting, by the portable communication device,  
3 device information to the server computer, thereby enabling the server computer to  
4 associate the device information with the credential or the token;

1                   19.    The method of claim 17, wherein the base station identifier is a  
2 universally unique identifier (UUID) of the base station.