

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
2 providing, by an access device to a user device associated with a user
3 in a transaction, an initial communication;
4 responsive to providing the initial communication, receiving, by the
5 access device from the user device, a user identifier and an access token;
6 receiving, by the access device, a secret associated with the user;
7 determining, by the access device, using the user identifier and/or the
8 access token, if the transaction is authorized by an authorizing entity computer
9 associated with the access device or by an authorizing entity not associated with the
10 access device;
11 if the transaction is authorized by the authorizing entity computer
12 associated with the access device, then transmitting an authorization request
13 message comprising the user identifier, the secret, and the access token to the
14 authorizing entity computer, wherein the authorizing entity computer validates the
15 secret, retrieves a real credential of the user using the user identifier, and authorizes
16 the transaction; and
17 if the transaction is not associated with the authorizing entity computer,
18 then transmitting the authorization request message comprising the user identifier,
19 the secret, and the access token to a token service computer, wherein the token
20 service computer detokenizes the access token to obtain the real credential replaces
21 the access token with the real credential in the authorization request message to
22 form a modified authorization request message, and forwards the modified
23 authorization request message to another authorizing entity computer for
24 authorization.
- 1 2. The method of claim 1, wherein the method further comprises:
2 receiving, by the access device, the authorization response message
3 comprising at least an indication of whether or not the transaction is authorized from
4 the authorizing entity computer; and

5 displaying, by the access device, the indication of whether or not the
6 transaction is authorized on a display of the access device to the user of the user
7 device.

1 3. The method of claim 1, further comprising:
2 prompting, by the access device, the user to input the secret via one or
3 more input elements on the access device.

1 4. The method of claim 1, wherein if the transaction is authorized
2 by the authorizing entity computer associated with the access device, the authorizing
3 entity computer validates the access token using the real credential.

1 5. The method of claim 1, wherein the user identifier identifies a
2 user information file, wherein the secret is a personal identification number, and
3 wherein the real credential is a primary account number.

1 6. The method of claim 1, wherein the initial communication
2 includes a get processing options command and a read record command.

1 7. The method of claim 6, wherein receiving the user identifier and
2 the access token further comprises:
3 receiving, by the access device, a get processing options response
4 comprising the user identifier in response to the get processing options command;
5 and
6 receiving, by the access device, a read record response comprising the
7 access token in response to the read record command.

1 8. The method of claim 1, wherein if the transaction is authorized
2 by the authorizing entity computer associated with the access device, then
3 transmitting the authorization request message comprising the user identifier, the
4 secret, and the access token to the authorizing entity computer further comprises:
5 transmitting, by the access device, the authorization request message
6 comprising the user identifier, the secret, and the access token to the authorizing
7 entity computer via an access device network.

1 9. The method of claim 1, wherein the token service computer
2 provisions the user device with the access token.

1 10. An access device comprising:
2 a processor; and
3 a computer-readable medium coupled to the processor, the computer-
4 readable medium comprising code executable by the processor for implementing a
5 method comprising:
6 providing, by the access device to a user device associated with
7 a user in a transaction, an initial communication;
8 responsive to providing the initial communication, receiving,
9 from the user device, a user identifier and an access token;
10 receiving a secret associated with the user;
11 determining using the user identifier and/or the access token, if
12 the transaction is authorized by an authorizing entity computer associated
13 with the access device or by an authorizing entity not associated with the
14 access device;
15 if the transaction is authorized by the authorizing entity computer
16 associated with the access device, then transmitting an authorization request
17 message comprising the user identifier, the secret, and the access token to
18 the authorizing entity computer, wherein the authorizing entity computer
19 validates the secret, retrieves a real credential of the user using the user
20 identifier, and authorizes the transaction; and
21 if the transaction is not associated with the authorizing entity
22 computer, then transmitting the authorization request message comprising the
23 user identifier, the secret, and the access token to a token service computer,
24 wherein the token service computer detokenizes the access token to obtain
25 the real credential replaces the access token with the real credential in the
26 authorization request message to form a modified authorization request
27 message, and forwards the modified authorization request message to
28 another authorizing entity computer for authorization.

1 11. The access device of claim 10, wherein if the transaction is not
2 associated with the authorizing entity computer, the token service computer forwards
3 the modified authorization response message to the access device via a transport
4 computer.

1 12. The access device of claim 11, wherein the method further
2 comprises:
3 receiving, by the access device, the authorization response message
4 from the token service computer; and
5 displaying, by the access device, the indication of whether or not the
6 transaction is authorized by the another authorizing entity computer on a display of
7 the access device to the user of the user device.

1 13. The access device of claim 10, wherein if the transaction is
2 authorized by the authorizing entity computer associated with the access device, the
3 method further comprises:
4 transmitting, by the access device, the authorization request message
5 to the token service computer via an access device network.

1 14. The access device of claim 13, wherein the authorizing entity
2 computer generates an authorization response message comprising at least an
3 indication of whether or not the transaction is authorized and the real credential and
4 provides the authorization response message to the token service computer,
5 wherein the token service computer tokenizes the real credential to obtain the
6 access token, replaces the real credential with the access token to form a modified
7 authorization response message, and forwards the modified authorization response
8 message to the access device, wherein the method further comprises:
9 receiving, by the access device, the authorization response message;
10 and
11 displaying, by the access device, the indication of whether or not the
12 transaction is authorized by the authorizing entity computer on a display of the
13 access device to the user of the user device.

1 15. The access device of claim 10, wherein the initial
2 communication is provided to the user device via a short-range communication
3 channel.

1 16. The access device of claim 10, wherein the user device is a first
2 user device, the transaction is a first transaction, the initial communication is a first
3 initial communication, the user identifier is a first user identifier, the access token is a
4 first access token, the memory is a first memory, the secret is a first secret, the
5 authorization request message is a first authorization request message, the modified
6 authorization request message is a first modified authorization request message, the
7 real credential is a first real credential, and wherein the method further comprises:
8 providing, to a second user device associated with a second user in a
9 second transaction, a second initial communication, wherein the second user device
10 then retrieves a second user identifier and a second access token from a second
11 memory in the second user device;
12 receiving, by the access device from the second user device, the
13 second user identifier and the second access token;
14 receiving a second secret associated with the second user;
15 determining using the second user identifier and/or the second access
16 token, if the second transaction is authorized by the authorizing entity computer
17 associated with the access device or by the authorizing entity not associated with the
18 access device;
19 if the second transaction is authorized by the authorizing entity
20 computer associated with the access device, then transmitting a second
21 authorization request message comprising the second user identifier, the second
22 secret, and the second access token to the authorizing entity computer, wherein the
23 authorizing entity computer validates the second secret, retrieves a second real
24 credential of the second user using the second user identifier, and authorizes the
25 second transaction; and
26 if the second transaction is not associated with the authorizing entity
27 computer, then transmitting the second authorization request message comprising
28 the second user identifier, the second secret, and the second access token to the

29 token service computer, wherein the token service computer detokenizes the second
30 access token to obtain the second real credential, replaces the second access token
31 with the second real credential in the second authorization request message to form
32 a second modified authorization request message, and forwards the second
33 modified authorization request message to the another authorizing entity computer
34 for authorization.

1 17. The access device of claim 10, wherein the transaction is a
2 location access transaction, wherein if the location access transaction is authorized,
3 the method further comprises:
4 providing, by the access device, access to a location of the location
5 access transaction to the user.

1 18. The access device of claim 10, wherein the transaction is a data
2 access transaction, wherein if the data access transaction is authorized, the method
3 further comprises:
4 providing, by the access device, data corresponding to the data access
5 transaction to the user device of the user.

1 19. A method comprising:
2 receiving, by an authorizing entity computer, an authorization request
3 message comprising a user identifier, a secret, and an access token from an access
4 device in communication with a user device associated with a user during a
5 transaction, wherein the transaction was determined by the access device to be
6 authorized by the authorizing entity computer associated with the access device,
7 wherein the authorizing entity computer is associated with the access device;
8 validating, by the authorizing entity computer, the secret,
9 retrieving, by the authorizing entity computer, a real credential of the
10 user using the user identifier;
11 authorizing, by the authorizing entity computer, the transaction based
12 on whether or not the secret is validated and/or whether or not the real credential is
13 retrieved;

14 generating, by the authorizing entity computer, an authorization
15 response message including an indication of whether or not the transaction is
16 authorized and the access token; and
17 providing, by the authorizing entity computer, the authorization
18 response message to the access device.

1 20. The method of claim 19, wherein the authorizing entity computer
2 receives the authorization request message from the access device via an access
3 device network, and wherein the authorizing entity computer provides the
4 authorization response message to the access device via the access device
5 network.