

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
 - 2 receiving, by an access operator computer from an access device of an
 - 3 access provider, a first transaction request for a first transaction, the first transaction
 - 4 request comprising a credential, the first transaction request associated with a first
 - 5 transaction amount;
 - 6 identifying, by the access operator computer, a token, based upon the
 - 7 credential;
 - 8 transmitting, by the access operator computer to an authorizing
 - 9 computer, a pre-authorization request message comprising the credential and a pre-
 - 10 authorization amount;
 - 11 receiving, by the access operator computer, a pre-authorization
 - 12 response message from the authorizing computer;
 - 13 receiving, by the access operator computer from the access device or
 - 14 another access device, a second transaction request for a second transaction, the
 - 15 second transaction request comprising the credential, the second transaction
 - 16 request associated with a second transaction amount;
 - 17 identifying, by the access operator computer, the token from the
 - 18 credential;
 - 19 determining, by the access operator computer, that the token has been
 - 20 used at the access provider;
 - 21 forming a total amount by aggregating, by the access operator
 - 22 computer, at least the first transaction amount and the second transaction amount;
 - 23 and
 - 24 initiating transmitting a clearing message including the total amount.
- 1 2. The method of claim 1, wherein the pre-authorization response
- 2 message is a decline and wherein the method further comprises:
 - 3 transmitting, by the access operator computer, the pre-authorization
 - 4 response message to the access device.
- 1 3. The method of claim 2, further comprising:
 - 2 adding, by the access operator computer, the token to a blacklist; and

3 sending, by the access operator computer, the blacklist to the access
4 device.

1 4. The method of claim 3, further comprising:
2 receiving, by the access operator computer, an approval response; and
3 removing, by the access operator computer, the token from the
4 blacklist.

1 5. The method of claim 3, further comprising:
2 receiving, by the access operator computer from a site, a debt recovery
3 message including the credential;
4 retrieving, by the access operator computer, the total amount,
5 transmitting, by the access operator computer to the site, the total
6 amount, wherein the site generates a debt recovery request comprising the
7 credential and the total amount;
8 receiving, by the access operator computer from the site, a debt
9 recovery response; and
10 removing, by the access operator computer, the token from the
11 blacklist.

1 6. The method of claim 1, wherein the first transaction request
2 comprises the token and wherein identifying the token comprises extracting the
3 token from the first transaction request.

1 7. The method of claim 1, wherein the pre-authorization request
2 message comprises a pre-authorization identifier, wherein the clearing message also
3 includes the pre-authorization identifier, and wherein the authorizing computer uses
4 the pre-authorization identifier to retrieve the credential.

1 8. The method of claim 1, further comprising:
2 periodically sending, by the access operator computer, an updated
3 blacklist to a plurality of access devices including the access device.

1 9. The method of claim 1, further comprising:
2 periodically sending, by the access operator computer, a clearing
3 message for each token on a blacklist.

1 10. The method of claim 9, wherein the clearing message is a
2 recurring transaction.

1 11. A server computer comprising:
2 a processor; and
3 a computer readable medium comprising code, executable by
4 the processor, for performing a method comprising:
5 receiving, from an access device of an access provider, a first
6 transaction request for a first transaction, the first transaction request comprising a
7 credential, the first transaction request associated with a first transaction amount,
8 identifying a token, based upon the credential,
9 transmitting, to an authorizing computer, a pre-authorization request
10 message comprising the credential and a pre-authorization amount,
11 receiving a pre-authorization response message from the authorizing
12 computer,
13 receiving, from the access device or another access device, a second
14 transaction request for a second transaction, the second transaction request
15 comprising the credential, the second transaction request associated with a second
16 transaction amount,
17 identifying the token from the credential,
18 determining that the token has been used at the access provider,
19 forming a total amount by aggregating at least the first transaction
20 amount and the second transaction amount, and
21 initiating transmitting a clearing message including the total amount.

1 12. The server computer of claim 11, wherein the method further
2 comprises:
3 storing the first transaction request without the credential in a
4 transaction log.

1 13. The server computer of claim 12, wherein the method further
2 comprises:
3 updating the first transaction request in the transaction log with the
4 second transaction request.

1 14. The server computer of claim 12, wherein determining that the
2 token has been used at the access provider comprises querying the transaction log
3 with the credential.

1 15. The server computer of claim 11, wherein identifying the token
2 comprises retrieving the token from a token storage.

1 16. The server computer of claim 11, wherein the first transaction
2 request and/or the second transaction request comprises the token and wherein
3 identifying the token comprises identifying the token in the first transaction request
4 and/or the second transaction request.

1 17. The server computer of claim 11 wherein identifying the token
2 comprises applying a cryptographic function to the credential.

1 18. The server computer of claim 11, wherein the token is valid for
2 one day.

1 19. The server computer of claim 11, wherein the pre-authorization
2 amount is less than the first transaction amount.

1 20. The method of claim 1, wherein the credential is encrypted.

1 21. A method comprising:
2 receiving, by an access device, a credential from a portable device;
3 identifying, by the access device, a token based upon the credential;
4 determining, by the access device, that the token is not on a blacklist;
5 admitting, by the access device, a user associated with the portable
6 device; and
7 transmitting, by the access device to an access operator computer, a
8 transaction request comprising the credential, the transaction request associated
9 with a transaction amount.

1 22. The method of claim 21, wherein the credential is a first
2 credential, the portable device is a first portable device, the token is a first token, and
3 the user is a first user and wherein the method further comprises:

4 receiving, by the access device, a second credential from a second
5 portable device associated with a second user;
6 identifying, by the access device, a second token based upon the
7 second credential;
8 determining, by access device, that the second token is on the
9 blacklist; and
10 denying access, by the access device, to the second user associated
11 with the second portable device.

1 23. The method of claim 21, wherein the method further comprises:
2 receiving, by the access device from the access operator computer, a
3 pre-authorization response message, wherein the pre-authorization response
4 message is a decline; and
5 adding, by the access device, the token to the blacklist.

1 24. The method of claim 21, wherein identifying the token comprises
2 generating the token with a cryptographic function.

1 25. The method of claim 21, further comprising:
2 receiving, from the access operator computer, an updated blacklist.

1 26. An access device comprising:
2 a processor; and
3 a computer readable medium comprising code, executable by the
4 processor, for performing a method comprising:
5 receiving a credential from a portable device,
6 identifying a token based upon the credential,
7 determining that the token is not on a blacklist,
8 admitting a user associated with the portable device, and
9 transmitting, to an access operator computer, a transaction
10 request comprising the credential, the transaction request associated with a
11 transaction amount.

1 27. The access device of claim 26, wherein the access device
2 further comprises a secure element and wherein the secure element stores a
3 cryptographic key.

1 28. The access device of claim 27, wherein the method further
2 comprises encrypting the credential with the cryptographic key to form an encrypted
3 credential and wherein the transaction request includes the encrypted credential.

1 29. The access device of claim 26, wherein determining the token is
2 not on a blacklist comprises determining that the credential is not on the blacklist.

1 30. The access device of claim 26, wherein the portable device is a
2 smartphone or a payment card.