

WHAT IS CLAIMED IS:

1 1. A computer-implemented method comprising:
2 receiving, at a secure remote transaction server from a client device, a
3 request to enroll an account;
4 verifying, by the secure remote transaction server, that the client device
5 has authority to access the account;
6 storing, by the secure remote transaction server, at least a public key of a
7 cryptographic key pair in association with the account, wherein at least a private key of
8 the cryptographic key pair is stored on the client device in association with the account;
9 and
10 generating, by the secure remote transaction server, a token to be
11 associated with the account, the token being stored in association with the account, and
12 wherein the method further comprises
13 receiving, by the secure remote transaction server from an access device,
14 a request to complete a transaction in association with the account, the request
15 including a signed authentication indicator;
16 verifying, by the secure remote transaction server, the signed
17 authentication indicator using the public key stored in association with the account; and
18 upon verifying the authentication indicator, providing the token to the
19 access device.

1 2. The computer-implemented method of claim 1, wherein the signed
2 authentication indicator has been generated by the client device by performing a first
3 cryptographic operation using the private key.

1 3. The computer-implemented method of claim 2, wherein verifying
2 the authentication indicator using the public key comprises performing a second
3 cryptographic operation on the signed authentication indicator using the public key.

1 4. The computer-implemented method of claim 1, wherein verifying
2 that the client device has authority to access the account comprises:
3 identifying, by the secure remote transaction server, an authorization
4 entity associated with the account based on information in the request; and
5 verifying, by the secure remote transaction server, the authenticity of the
6 account with the authorization entity associated with the account.

1 5. The computer-implemented method of claim 4, wherein the
2 authenticity of the account is determined by the authorization entity using a one-time
3 passcode.

1 6. The computer-implemented method of claim 5, wherein the
2 authorization entity transmits the one-time passcode to the client device via a
3 communication channel stored in relation to the account.

1 7. The computer-implemented method of claim 1, wherein the
2 cryptographic key pair is generated on the client device and the public key is received
3 by the secure remote transaction server from the client device.

1 8. The computer-implemented method of claim 1, wherein the
2 cryptographic key pair is generated on the secure remote transaction server and the
3 method further comprises transmitting the private key to the client device.

1 9. The computer-implemented method of claim 1, wherein the public
2 key is forwarded to an authorization entity associated with the account.

1 10. A secure remote transaction server comprising:
2 a processor; and
3 a memory including instructions that, when executed with the processor,
4 cause the secure remote transaction server to, at least:
5 receive, from a client device, a request to enroll an account;
6 verify that the client device has authority to access the account;
7 store at least a public key of a cryptographic key pair in association
8 with the account, wherein at least a private key of the cryptographic key pair is
9 stored on the client device in association with the account; and
10 generate a token to be associated with the account, the token being
11 stored in association with the account,
12 wherein the instructions further cause the secure remote transaction
13 server to:
14 receive, from an access device, a request to complete a transaction
15 in association with the account, the request including a signed authentication
16 indicator;
17 verify the signed authentication indicator using the public key stored
18 in association with the account; and

19 upon verifying the signed authentication indicator, provide the token
20 to the access device.

1 11. The secure remote transaction server of claim 10, wherein verifying
2 the signed authentication indicator using the public key comprises generating an
3 unsigned version of the signed authentication indicator and assessing the unsigned
4 version of the signed authentication indicator and.

1 12. The secure remote transaction server of claim 11, wherein
2 assessing the unsigned version of the signed authentication indicator comprises
3 comparing the unsigned version of the signed authentication indicator to an expected
4 result.

1 13. The secure remote transaction server of claim 11, wherein
2 assessing the unsigned version of the signed authentication indicator comprises
3 determining whether a likelihood value in the unsigned version of the signed
4 authentication indicator exceeds a threshold value.

1 14. The secure remote transaction server of claim 10, wherein the
2 token is subsequently used by the access device to complete the transaction.

1 15. The secure remote transaction server of claim 10, wherein the
2 token is generated as a random string of characters.

1 16. The secure remote transaction server of claim 10, wherein
2 generating the token to be associated with the account comprises receiving the token
3 from an authorization entity associated with the account.

1 17. A computer-implemented method comprising:
2 receiving, by a communication device, a request to register authentication
3 data for an account associated with a service provider;
4 prompting, by the communication device, a user of the account to provide
5 the authentication data;
6 receiving, by the communication device, the authentication data from the
7 user;
8 registering, by the communication device, the authentication data onto the
9 communication device;

10 obtaining, by the communication device, a private key of a cryptographic
11 key pair; and
12 associating, by the communication device, the private key with the
13 account and the authentication data, wherein a secure remote server links a public key
14 of the cryptographic key pair to a token associated with the account.

1 18. The computer-implemented method of claim 17, further comprising:
2 receiving, by the communication device, a request to access the account;
3 prompting, by the communication device, the user to provide the
4 authentication data;
5 receiving, by the communication device, the authentication data from the
6 user;
7 comparing, by the communication device, the received authentication data
8 with the registered authentication data;
9 determining, by the communication device, that the received
10 authentication data matches the registered authentication data;
11 generating, by the communication device, an authentication indicator
12 indicating the match;
13 signing, by the communication device, the authentication indicator using
14 the private key; and
15 sending, by the communication device, the signed authentication indicator
16 to the secure remote server in an access request, wherein the secure remote server
17 releases the token to the service provider to grant the user access to the account in
18 response to verifying the signed authentication indicator using the public key.

1 19. A communication device comprising:
2 a processor; and
3 a computer readable medium, the computer readable medium comprising
4 code, executable by the processor for implementing a method including:
5 receiving a request to register authentication data for an account
6 associated with a service provider;
7 prompting a user to provide the authentication data;
8 receiving the authentication data from the user;
9 registering the authentication data onto the communication device;
10 obtaining a private key of a cryptographic key pair; and

11 associating the private key with the account and the authentication data,
12 wherein a secure remote server links a public key of the cryptographic key pair to a
13 token associated with the account.