

WHAT IS CLAIMED IS:

1 1. A method of processing a transaction comprising:
2 receiving, by a server computer, a thin client identifier from a thin client on
3 a communication device;
4 retrieving, by the server computer, an encrypted first cryptographic key
5 based on the thin client identifier, wherein the encrypted first cryptographic key is a first
6 cryptographic key that is encrypted with a second cryptographic key;
7 initiating, by the server computer, sending of the encrypted first
8 cryptographic key to the thin client; and
9 receiving, by the server computer, an encrypted secret from the thin client,
10 the encrypted secret being a secret encrypted with the first cryptographic key;
11 initiating, by the server computer, a translation of the secret from being
12 encrypted with the first cryptographic key to being encrypted with a third cryptographic
13 key, wherein the third cryptographic key is a transport computer cryptographic key;
14 after initiating the translation of the secret, obtaining, by the server
15 computer, the secret encrypted with the third cryptographic key; and
16 providing, by the server computer, the secret encrypted with the third
17 cryptographic key to a transport computer,
18 wherein the secret encrypted with the third cryptographic key is provided
19 to the transport computer in an authorization request message, and wherein the
20 transport computer decrypts the encrypted secret using the third cryptographic key,
21 encrypts the secret with a fourth cryptographic key, wherein the fourth cryptographic key
22 is an authorizing entity computer cryptographic key, modifies the authorization request
23 message to include the secret encrypted with the fourth cryptographic key and provides
24 the modified authorization request message to an authorizing entity computer, wherein
25 the authorizing entity computer determines whether or not to authorize an interaction
26 associated with the secret, generates an indication of whether or not the interaction is
27 authorized, generates an authorization response message including the indication of
28 whether or not the interaction is authorized, and provides the authorization response
29 message to the server computer via the transport computer, wherein the method further
30 comprises:

31 receiving, by the server computer, the authorization response message;
32 and
33 providing, by the server computer, the authorization response message to
34 the thin client.

1 2. The method of claim 1, wherein the first cryptographic key, the
2 second cryptographic key, and the third cryptographic key are symmetric keys.

1 3. The method of claim 1, wherein the secret is a user's biometric
2 template, a password, a personal identification number, a social security number, or a
3 one-time password.

1 4. The method of claim 1, wherein the thin client receives the
2 encrypted first cryptographic key, decrypts the encrypted first cryptographic key, obtains
3 the secret, encrypts the secret with the first cryptographic key, and provides the secret
4 encrypted with the first cryptographic key to the server computer.

1 5. The method of claim 1, wherein the second cryptographic key is
2 independently derived by the thin client and is used by the thin client to decrypt the
3 encrypted first cryptographic key.

1 6. The method of claim 1, wherein the second cryptographic key is
2 independently derived by the thin client and is used by the thin client to decrypt the
3 encrypted first cryptographic key, wherein the second cryptographic key is
4 independently derived using an initialization vector, a thin client identifier, and a shared
5 secret, the shared secret obtained by the thin client using a Diffie-Hellman Elliptic Curve
6 cryptographic process.

1 7. The method of claim 1 further comprising:
2 receiving, by the server computer, interaction data from the thin client ,
3 during the interaction; and
4 providing, by the server computer, the interaction data to the transport
5 computer.

1 8. A server computer 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 receiving a thin client identifier from a thin client on a
7 communication device;
8 retrieving an encrypted first cryptographic key based on the thin
9 client identifier, wherein the encrypted first cryptographic key is a first
10 cryptographic key that is encrypted with a second cryptographic key;
11 initiating sending of the encrypted first cryptographic key to the thin
12 client;
13 receiving an encrypted secret from the thin client, the encrypted
14 secret being a secret encrypted with the first cryptographic key;
15 decrypting the encrypted secret with the first cryptographic key to
16 obtain the secret;
17 encrypting the secret using a third cryptographic key, wherein the
18 third cryptographic key is a transport computer cryptographic key; and
19 providing the secret encrypted with the third cryptographic key to a
20 transport computer in an authorization request message, and wherein the
21 transport computer decrypts the secret encrypted with the third cryptographic key
22 to obtain the secret, encrypts the secret with an authorizing entity computer
23 cryptographic key, and modifies the authorization request message to include the
24 secret encrypted with the authorizing entity computer cryptographic key and
25 provides the modified authorization request message to an authorizing entity
26 computer, wherein the authorizing entity computer decrypts the secret encrypted
27 with the authorizing entity computer cryptographic key using the authorizing
28 entity computer cryptographic key, determines whether or not to authorize an
29 interaction associated with the secret, generates an indication of whether or not
30 the interaction is authorized, generates an authorization response message
31 including the indication of whether or not the interaction is authorized, and

32 provides the authorization response message to the server computer via the
33 transport computer;
34 receiving the authorization response message; and
35 providing, by the server computer, the authorization response
36 message to the thin client.

1 9. The server computer of claim 8 further comprising:
2 a secret module;
3 an encryption function module;
4 a first hardware security module; and
5 a second hardware security module.

1 10. The server computer of claim 9, wherein the method further
2 comprises:
3 initiating a translation of the secret from being encrypted with the first
4 cryptographic key to being encrypted with a third cryptographic key, wherein initiating
5 the translation of the secret from being encrypted with the first cryptographic key to
6 being encrypted with the third cryptographic key further includes:
7 providing, by the server computer, the secret encrypted with the first
8 cryptographic key and the thin client identifier to the secret module;
9 querying, by the secret module, a database for translation parameters
10 using the thin client identifier;
11 receiving, by the secret module, the translation parameters;
12 providing, by the secret module, the secret encrypted with the first
13 cryptographic key and the translation parameters to the second hardware security
14 module via the encryption function module;
15 decrypting, by the second hardware security module, the secret encrypted
16 with the first cryptographic key using the translation parameters;
17 encrypting, by the second hardware security module, the secret with the
18 third cryptographic key;

19 providing, by the second hardware security module, the secret encrypted
20 with the third cryptographic key to the secret module via the encryption function module;
21 and
22 providing, by the secret module, the secret encrypted with the third
23 cryptographic key to the server computer.

1 11. The server computer of claim 10, wherein the translation
2 parameters include the encrypted first cryptographic key, an initialization vector, a
3 transport computer identifier, the second cryptographic key, a base derivation key
4 identifier, an interaction counter, and a derivation identifier.

1 12. The server computer of claim 10, wherein in the method, after
2 providing, by the second hardware security module, the secret encrypted with the third
3 cryptographic key to the secret module via the encryption function module, the method
4 further comprises:

5 providing, by the secret module, a refresh request message to the first
6 hardware security module via the encryption function module;

7 generating, by the first hardware security module, an updated first
8 cryptographic key;

9 encrypting, by the first hardware security module, the updated first
10 cryptographic key with the second cryptographic key;

11 providing, by the first hardware security module, the encrypted updated
12 first cryptographic key to the secret module via the encryption function module; and

13 storing, by the secret module, the thin client identifier and the encrypted
14 updated first cryptographic key in the database.

1 13. The server computer of claim 8 prior to receiving the thin client
2 identifier from the thin client, the method further comprises:

3 assigning, by the server computer, the thin client identifier to the thin
4 client.

1 14. The server computer of claim 8, wherein in the method, prior to
2 receiving the thin client identifier from the thin client the method further comprises:

3 receiving a public key request from the thin client, wherein the public key
4 request comprises a request for a server computer ephemeral public key;
5 obtaining the server computer ephemeral public key; and
6 providing the server computer ephemeral public key to the thin client,
7 wherein the thin client derives the second cryptographic key from at least the server
8 computer ephemeral public key.