

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
2 receiving, by a server computer, a thin client identifier from a thin client
3 on 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
6 first cryptographic key that is encrypted with a second cryptographic key;
7 initiating, by the server computer, the 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
10 client, the encrypted secret being a secret encrypted with the first cryptographic key.
- 1 2. The method of claim 1, and wherein the method further
2 comprises:
3 initiating, by the server computer, a translation of the secret from being
4 encrypted with the first cryptographic key to being encrypted with a third
5 cryptographic key, wherein the third cryptographic key is a transport computer
6 cryptographic key.
- 1 3. The method of claim 2, wherein the first cryptographic key, the
2 second cryptographic key, and the third cryptographic key are symmetric keys.
- 1 4. 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
3 a one-time password.
- 1 5. The method of claim 1, wherein the thin client receives the
2 encrypted first cryptographic key, decrypts the encrypted first cryptographic key,
3 obtains the secret, encrypts the secret with the first cryptographic key, and provides
4 the secret encrypted with the first cryptographic key to the server computer.
- 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.

1 7. The method of claim 1, and wherein the method further
2 comprises:
3 initiating, by the server computer, a translation of the secret from being
4 encrypted with the first cryptographic key to being encrypted with a third
5 cryptographic key, wherein the third cryptographic key is a transport computer
6 cryptographic key;
7 after initiating the translation of the secret, obtaining, by the server
8 computer, the secret encrypted with the third cryptographic key; and
9 providing, by the server computer, the secret encrypted with the third
10 cryptographic key to a transport computer, wherein the transport computer decrypts
11 the secret encrypted with the third cryptographic key to obtain the secret.

1 8. The method of claim 7, wherein the secret encrypted with the
2 third cryptographic key is provided to the transport computer in an authorization
3 request message, and wherein the transport computer modifies the authorization
4 request message to include the secret and provides the modified authorization
5 request message to an authorizing entity computer, wherein the authorizing entity
6 computer determines whether or not to authorize an interaction associated with the
7 secret, generates an indication of whether or not the interaction is authorized,
8 generates an authorization response message including the indication of whether or
9 not the interaction is authorized, and provides the authorization response message
10 to the server computer via the transport computer, wherein the method further
11 comprises:
12 receiving, by the server computer, the authorization response
13 message; and
14 providing, by the server computer, the authorization response message
15 to the thin client.

1 9. 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

5 shared secret, the shared secret obtained by the thin client using a Diffie-Hellman
6 Elliptic Curve cryptographic process.

1 10. The method of claim 1 further comprising:
2 receiving, by the server computer, interaction data from the thin client ,
3 during an interaction between a user of a portable device and a resource provider of
4 the communication device; and
5 providing, by the server computer, the interaction data and the
6 encrypted secret to a transport computer.

1 11. 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 the sending of the encrypted first cryptographic key to
12 the thin client; and
13 receiving an encrypted secret from the thin client, the encrypted
14 secret being a secret encrypted with the first cryptographic key.

1 12. The server computer of claim 11 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 13. The server computer of claim 12, further comprising;
2 initiating a translation of the secret from being encrypted with the first
3 cryptographic key to being encrypted with a third cryptographic key, wherein initiating

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

1 14. The server computer of claim 13, wherein the translation
2 parameters include the translation parameters including the encrypted first
3 cryptographic key, an initialization vector, a transport computer identifier, the second
4 cryptographic key, a base derivation key identifier, an interaction counter, and a
5 derivation identifier

1 15. The server computer of claim 13, wherein after providing, by the
2 second hardware security module, the secret encrypted with the third cryptographic
3 key to the secret module via the encryption function module, the method further
4 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
14 encrypted updated first cryptographic key in the database.

1 16. The server computer of claim 11 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 17. The server computer of claim 11, wherein prior to receiving the
2 thin client identifier from the thin client the method further comprises:
3 receiving a public key request from the thin client, wherein the public
4 key 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.

1 18. A method comprising:
2 providing, by a thin client on a communication device, a thin client
3 identifier to a server computer during an interaction between the communication
4 device and a portable device;
5 receiving, by the thin client, an encrypted first cryptographic key from
6 the server computer, wherein the encrypted first cryptographic key is a first
7 cryptographic key that is encrypted with a second cryptographic key;
8 decrypting, by the thin client, the encrypted first cryptographic key with
9 the second cryptographic key;
10 receiving, by the thin client, a secret from a user of the portable device;
11 encrypting, by the thin client, the secret with the first cryptographic key;
12 and

13 providing, by the thin client, the secret encrypted to the server
14 computer.

1 19. The method of claim 18 further comprising:
2 receiving, by the thin client, interaction data from the portable device;
3 and
4 providing, by the thin client, the interaction data to the server computer.

1 20. The method of claim 18 further comprising:
2 obtaining, by the thin client, the second cryptographic key from
3 memory; and
4 prompting, by the thin client, the user of the portable device to input the
5 secret.