

U.S. Patent No. 12,166,869

1[pre]: A method for a mobile device with an embedded universal integrated circuit card (eUICC) to securely communicate with a wireless network, the method performed by the mobile device, the method comprising:

1(a): storing, in the eUICC, a first module private key, a corresponding first module public key, and a network public key;

1(b) receiving, from a first server associated with the wireless network, an encrypted profile for the eUICC comprising cryptographic parameters, a module identity, and a key K;

1(c): generating a shared secret key using a first elliptic curve Diffie-Hellman (ECDH) key exchange with the first module private key and the network public key;

1(d): decrypting, with the shared secret key, at least a portion of the encrypted profile for the eUICC;

1(e): generating, by the eUICC, a second module public key and a corresponding second module private key;

1(f): sending, to a second server associated with the wireless network, the second module public key;

1(g): generating a symmetric key using a second ECDH key exchange with the second module private key and the cryptographic parameters;

1(h): generating, with the symmetric key, module encrypted data, the module encrypted data comprising the module identity; and

1(i): sending, to the second server, the module encrypted data.

2: The method of claim 1, wherein the module identity comprises an international mobile subscriber identity (IMSI).

3: The method of claim 1, wherein the module identity comprises a permanent identifier for the mobile device.

4: The method of claim 1, wherein the cryptographic parameters comprise an identifier for a set of cryptographic parameters.

5: The method of claim 1, further comprising in step c) deriving the shared secret key using an American National Standards Institute (ANSI) standard X-9.63 key derivation function.

6: The method of claim 1, further comprising in step g) deriving the symmetric key using an ANSI standard X-9.63 key derivation function.

7: The method of claim 1, wherein the first server mutually derives the shared secret key using the first ECDH key exchange with the first module public key and a network private key corresponding to the network public key.

8: The method of claim 1, further comprising in step e), generating, by the eUICC, the second module public key and the second module private key using a random number generator and input from a sensor.
9: The method of claim 1, further comprising in step h) generating, with the symmetric key and an Advanced Encryption Standard (AES), the module encrypted data.
10: The method of claim 1, wherein steps g) and h) occur before step f).
11: The method of claim 1, wherein the network public key is associated with an eUICC subscription manager.
12: The method of claim 11, wherein the eUICC subscription manager comprises the first server.
13: The method of claim 1, further comprising: j) receiving, from the wireless network, a random number (RAND) and generating a response (RES) using the RAND and the key K.
14: The method of claim 1, further comprising before step b), authenticating the first server by (i) receiving a server digital signature and (ii) verifying the server digital signature with a server public key.
15: The method of claim 1, further comprising (i) in step a), storing a server name for the first server and a port number in a nonvolatile memory of the eUICC, and (ii) before step b) sending the first module public key to the first server.
16: The method of claim 1, wherein the first server, the second server, and the wireless network are associated with a mobile network operator.
17: The method of claim 1, wherein the eUICC comprises a processor, firmware, and protected memory.
18: The method of claim 1, wherein the cryptographic parameters include a base point G for an elliptic curve.
19: The method of claim 1, wherein the mobile device comprises a wireless device with a radio for communicating with a plurality of base stations for the wireless network.
20: The method of claim 1, wherein the eUICC comprises a package soldered to a circuit board of the mobile device.