

U.S. Patent No. 11,916,893

1[pre]: A mobile device for communicating with a wireless network, the mobile device comprising:

1[a]: a first memory configured to store an embedded universal integrated circuit card (eUICC) identity;

1[b]: a random number generator operably connected to a processor connected to a second memory configured to generate a random number for an eUICC private key corresponding to an eUICC public key;

1[c]: a radio including one or more transmit antennas and one or more receiving antennas configured to:

1[c][1]: a. transmit, to a subscription manager, the eUICC identity and the eUICC public key; and

1[c][2]: b. receive, from the subscription manager, i) an eUICC profile comprising network parameters, a key K, and a subscriber identity and ii) a symmetric key; and

1[d]: an eUICC associated with the eUICC identity and configured to

1[d][1]: a. derive a profile key using an elliptic curve Diffie Hellman (ECDH) key exchange with the eUICC private key and a subscription manager public key;

1[d][2]: b. decrypt a first portion of the eUICC profile using the profile key;

1[d][3]: c. receive the symmetric key from a network application operating in the mobile device;

1[d][4]: d. decrypt a second portion of the eUICC profile using the symmetric key, the second portion comprising the key K and the subscriber identity, wherein the first portion and the second portion are distinct; and

1[d][5]: e. generate a response value for authentication of the mobile device with the wireless network using the key K.

2: The mobile device of claim 1, wherein the eUICC is further configured to receive a profile identity for the eUICC profile as a plaintext.

3: The mobile device of claim 1, wherein the eUICC operates within a universal integrated circuit card within the mobile device.

4: The mobile device of claim 1, wherein the random number generator is configured to generate the random number in response to input from at least one of a clock and a sensor.

5: The mobile device of claim 1, wherein the random number generator is configured to generate the random number from a seed value, wherein the seed value comprises data from at least one of a sensor, the radio, a bus, a clock, a physical interface, the memory, and an operating system.

6: The mobile device of claim 1, wherein the network application is configured to communicate with i) the wireless network and ii) the eUICC in the mobile device using a system bus.
7: The mobile device of claim 1, wherein the eUICC comprises computer executable instructions for a processor in the mobile device, and wherein the computer executable instructions are stored within the memory.
8: The mobile device of claim 1, wherein the eUICC comprises a package soldered onto a circuit board of the mobile device.
9: The mobile device of claim 1, further comprising a user interface configured to receive user identification information before the mobile device receives the symmetric key.
10: The mobile device of claim 1, wherein the first portion of the eUICC profile includes the network parameters, the network parameters comprising a list of numbers associated with a mobile network operator.
11: The mobile device of claim 1, wherein the network parameters comprise a mobile country code (MCC) and a mobile network code (MNC) associated with the wireless network.
12: The mobile device of claim 1, wherein the radio is further configured to receive, from the subscription manager, the eUICC profile using transport layer security.
13: The mobile device of claim 1, wherein the subscriber identity comprises an International Mobile Subscriber Identity (IMSI).
14: The mobile device of claim 1, wherein the radio is further configured to receive, from the subscription manager, a ciphertext for the symmetric key, wherein the mobile device is configured to decrypt the ciphertext using at least the eUICC private key.
15: The mobile device of claim 1, wherein the mobile device further comprises at least one of a wireless handset, a cellular phone, a smartphone, a tablet computer, a laptop, a tracking device, and a circuit board with the radio.
16: The mobile device of claim 1, wherein the second memory is the same memory as the first memory.
17: The mobile device of claim 1, wherein the one or more receiving antennas are the one or more transmit antennas.