

U.S. Patent No. 11,606,204	
1[pre]: A mobile device comprising:	
1(a): at least one processor; and	
1(b): at least one computer-readable medium operatively connected to the at least one processor and having stored thereon instructions that, when executed by the at least one processor, cause the mobile device to perform a method of authentication with a wireless network, the method comprising:	
1(b)(1): storing a server public key, a module identity, cryptographic algorithms, and a pre-shared secret key, wherein the module identity comprises a permanent identifier for the mobile device and the cryptographic algorithms includes a symmetric ciphering algorithm;	
1(b)(2): deriving a module private key and a corresponding module public key using the cryptographic algorithms;	
1(b)(3): deriving a symmetric ciphering key using (i) an elliptic curve integrated encryption scheme with the server public key and the module private key and (ii) an American National Standards Institute standard X-9.63 key derivation function;	
1(b)(4): generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity;	
1(b)(5): sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity; and	
1(b)(6): authenticating with the wireless network using a message digest with the pre-shared secret key.	
2: The mobile device of claim 1, wherein the message further comprises a module identity string, the module identity string comprising a temporary identification for the mobile device.	
3: The mobile device of claim 1, wherein the pre-shared secret key comprises a key K, wherein the mobile device and the wireless network mutually derive a response from (i) a random value and (ii) the key K, and wherein the mobile device receives the random value from the wireless network.	
4: The mobile device of claim 1, wherein, in step (1), the pre-shared secret key is stored within a subscriber identity module card, the pre-shared secret key comprising a key K.	

5: The mobile device of claim 1, wherein, in step (1), the pre-shared secret key is stored before the mobile device communicates with the wireless network.
6: The mobile device of claim 1, further comprising, in step (1), storing parameters for the cryptographic algorithms, the parameters comprising a standard curve for elliptic curve cryptography, and wherein, in step (2), the module public key and the module private key are derived using the standard curve.
7: The mobile device of claim 6, wherein, in step (5), the message further comprises the parameters for the cryptographic algorithms, and wherein the server mutually derives the symmetric ciphering key using at least the module public key and the parameters for the cryptographic algorithms.
8: The mobile device of claim 1, wherein the mobile device receives the pre-shared secret key via a wireless 802.11 connection to a web portal after a user for the mobile device submits a pre-shared secret key code for the mobile device to the web portal.
9: The mobile device of claim 1, further comprising, in step (2), deriving (i) the module private key from a random number generator and (ii) the module public key from a key pair generation algorithm, wherein the module private key comprises a random number.
10: The mobile device of claim 9, wherein the random number generator is configured to generate the random number from a seed value, and wherein the seed value comprises data from at least one of a sensor and a radio for the mobile device.
11: The mobile device of claim 1, wherein, in step (1), the server public key is stored in a nonvolatile memory of the mobile device.
12: The mobile device of claim 1, wherein the server comprises a plurality of computers, wherein the plurality includes at least one sub-server and at least one database.
13: The mobile device of claim 1, wherein the server comprises at least one virtualized server operating on at least one computer.
14: The mobile device of claim 1, wherein the wireless network includes the server.
15: The mobile device of claim 1, wherein, in step (1), the module identity is stored in a read-only nonvolatile memory address, wherein the mobile device designates the read-only nonvolatile memory address as read-only for a time interval.
16: The mobile device of claim 1, wherein the wireless network comprises at least one base station communicating with a 3 GPP wireless technology.

17: The mobile device of claim 1, wherein the message comprises a single user datagram protocol packet.
18: The mobile device of claim 1, wherein the symmetric ciphering algorithm comprises an Advanced Encryption Standard algorithm and has a length of 128 bits.
19: The mobile device of claim 1, wherein the module identity comprises a number for an international mobile subscriber identity number.
20: The mobile device of claim 1, wherein the mobile device comprises a smartphone.