

<b>'893 Patent, Claim 1</b>	<b>'175 Patent (parent), Claim 10</b>
1[pre]: A mobile device for communicating with a wireless network, the mobile device comprising:	10[pre]: A system for supporting authentication, the system comprising:
1[a]: a first memory configured to store an embedded universal integrated circuit card (eUICC) identity;	10[a]: a nonvolatile memory for recording an embedded Universal Integrated Circuit Card (eUICC) identity, an eUICC private key, and an address, wherein the eUICC private key is associated with an eUICC public key;
	10[b]: a first server device for encrypting (i) a profile using a profile key, and (ii) the profile key using the eUICC public key, wherein the first server device is associated with an eUICC subscription manager;
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	10[c][i]: a network interface for sending the eUICC identity to the address,
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	10[c][ii]: a network interface ... for receiving, from the eUICC subscription manager, the encrypted profile and the encrypted profile key after sending the eUICC identity,  10[f][ii]: a network application ... for receiving the encrypted symmetric key;
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;	10[c][iii]: wherein the encrypted profile key is decrypted with an asymmetric ciphering algorithm and the eUICC private key, wherein a first portion of the encrypted profile is decrypted with the decrypted profile key, and wherein the decrypted first portion includes a first key K1;
	10[d]: a memory for recording the first key K1;
1[d][3]: c. receive the symmetric key from a network application operating in the mobile device;	

'893 Patent, Claim 1	'175 Patent (parent), Claim 10
	10[e]: a second server device for encrypting a symmetric key, wherein the second server device is associated with a mobile network operator, wherein the mobile network operator is configured to send the first portion of the profile and a second portion of the profile to the eUICC subscription manager before the eUICC identity is sent from the network interface to the address;
	10[f][i]: a network application for authenticating with a wireless network using the first key K1,
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	10[g]: a hardware processor for decrypting the second portion of the profile with the symmetric key, wherein the decrypted portion includes a second key K2; and
1[d][5]: e. generate a response value for authentication of the mobile device with the wireless network using the key K.	10[h]: an eUICC for receiving a pseudo-random number (RAND), for calculating a response value (RES) using the RAND and the second key K2, and for sending the RES.