

'780 Patent, Claim 1	'175 Patent (parent), Claim 10
1[pre]: An embedded universal integrated circuit card (eUICC) comprising:	10[pre]: A system for supporting authentication, the system comprising:
1[a]: one or more processors; and	
1[b]: a non-transitory computer-readable memory operatively connected to the one or more processors, the non-transitory computer-readable memory having stored thereon machine readable instructions that, when executed by the one or more processors cause the one or more processors to perform steps of:	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[c][1]: (a) generating a first message comprising:	
1[c][1][i]: (1) an identity of the embedded universal integrated circuit card;	
1[c][1][ii]: (2) a nonce; and	
1[c][1][iii]: (3) a first digital signature, generated using a first eUICC private key, wherein the first eUICC private key corresponds to a first eUICC public key;	
1[c][2]: (b) sending the first message via a network application to a subscription manager system;	10[c][i]: a network interface for sending the eUICC identity to the address,
1[c][3]: (c) deriving a second eUICC private key and a corresponding second eUICC public key using a first random number generator and a first set of cryptographic algorithms;	
1[c][4]: (d) storing a subscription manager public key which corresponds to a subscription manager private key;	
1[c][5][i]: (e) deriving a profile key using a key exchange algorithm based on at least: (i) the second eUICC private key, and (ii) the stored subscription manager public key,	
1[c][5][ii]: wherein the profile key can also be derived at the subscription manager system based at least on: (iii) the second eUICC public key, and (iv) the subscription manager private key;	

'780 Patent, Claim 1	'175 Patent (parent), Claim 10
1[c][6]: (f) receiving from the subscription manager system, an encrypted profile comprising a ciphertext including a key K encrypted with a symmetric key;	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,
1[c][7]: (g) receiving the symmetric key;	10[f][ii]: a network application ... for receiving the encrypted symmetric key;
1[c][8]: (h) decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted 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;
	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[c][9]: (i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key; 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[c][10]: (j) storing at least the key K in the embedded universal integrated circuit card for use in future communications.	
	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.