

'869 Patent, Claim 1	'223 Patent (parent), Claim 1
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[pre]. A method for a module using an embedded universal integrated circuit card (eUICC) to derive a first shared secret key and a second shared secret key, the method comprising the module:
1(a): storing, in the eUICC, a first module private key, a corresponding first module public key, and a network public key;	1(a): storing a network public key and a module identity in the eUICC, wherein the module uses the network public key to authenticate an eUICC subscription manager;
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(b): receiving a token for a key derivation function from the authenticated eUICC subscription manager;
	1(c): deriving a module private key and a module public key, wherein the module sends the derived module public key and the module identity to the eUICC subscription manager;
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): deriving the first shared secret key using the key derivation function and a set of cryptographic parameters, wherein the key derivation function uses as input at least (i) the derived module private key, (ii) the set of cryptographic parameters, and (iii) the received token;
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.	

'869 Patent, Claim 1	'223 Patent (parent), Claim 1
	1(e): deriving the second shared secret key using (i) a shared secret algorithm and (ii) the derived first shared secret key as a random number for the shared secret algorithm, wherein the shared secret algorithm uses a secure hash algorithm; and
	1(f): receiving an eUICC profile, wherein the eUICC uses the derived second shared secret key to decrypt the eUICC profile.