

'869 Patent, Claim 1	'206 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 securely distributing a profile from a subscription manager system to a module comprising the steps of:
	1(a): recording, in memory operatively connected to the subscription manager system, a digital signature algorithm comprising an elliptic curve digital signature algorithm;
1(a): storing, in the eUICC, a first module private key, a corresponding first module public key, and a network public key;	1(b): recording, by the memory operatively connected to the subscription manager system, a server private key and a corresponding server public key, wherein the server public key and the server private key use elliptic curve cryptography;
	1(c): recording, by the memory operatively connected to the subscription manager system, a symmetric ciphering algorithm, wherein the symmetric ciphering algorithm comprises an Advanced Encryption Standard with a 128 bit key length;
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(d): receiving, by the subscription manager system, a certificate associated with the module from a module provider system associated with a module provider, wherein the certificate includes a module public key;
	1(e): receiving, by the subscription manager system, a challenge from the module;
	1(f): generating, by the subscription manager system, a network private key and a corresponding network public key, using a key pair generation algorithm;
	1(g): sending the generated network public key to the module; and
	1(h): sending a digital signature and the challenge to the module, wherein the digital signature is generated using the server private key and the digital signature algorithm;

'869 Patent, Claim 1	'206 Patent (parent), Claim 1
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(i): generating, by the subscription manager system, a mutually derived shared key using Elliptic Curve Diffie-Hellman based on at least: (1) the module public key, and (2) the network private key; wherein the mutually derived shared key is derived by the module based on at least: (i) a module private key associated with the module public key, and (ii) the network public key;
	1(j): encrypting, by the subscription manager system, the profile using: (1) the symmetric ciphering algorithm, and (2) the mutually derived shared key;
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.	1(k): sending, from the subscription manager system to the module, the encrypted profile, wherein the profile includes network access credentials for a wireless network.