'864 Patent, Claim 1	'740 Patent (Parent), Claim 1
1[pre]: A method comprising:	1[pre]: A method for supporting machine-to-machine communications, the method performed by a server, the method comprising:
1(a)(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 a mobile device and the cryptographic algorithms includes a symmetric ciphering algorithm;	1(a): authenticating a first message, wherein the first message includes (i) a first module public key with a first module public key identity, (ii) a module identity that comprises a first string, and (iii) a first source Internet protocol address and port (IP:port) number; receiving a module instruction and the module identity from an application server;
1(a)(2): deriving a module private key and a corresponding module public key associated with the mobile device using the cryptographic algorithms;	
1(a)(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(a)(4): generating module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity;	1(b): receiving a second message, wherein the second message includes a module encrypted data, the module identity, and a second source IP:port number, wherein the first source IP:port number and the second source IP:port number differ from one another, wherein the module identity in the second message includes a second string, and wherein the first string and the second string are associated with a serial number of a module;
1(a)(5): sending a message to a server for a wireless network, the message comprising the module encrypted data and the corresponding 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	

‘864 Patent, Claim 1	‘740 Patent (Parent), Claim 1
1(a)(6): authenticating the mobile device with the wireless network using a message digest with the pre-shared secret key.	
	1(c): sending a first response to the second source IP:port number after receiving the second message, wherein the server receives the second message after receiving the module instruction, wherein the first response includes a server encrypted data, wherein the server encrypted data is ciphered using the first module public key, and wherein the server encrypted data includes the module instruction and a security token;
	1(d): sending a second response, wherein the second response includes (i) a key generation command for generating a public key infrastructure (PKI) key pair and (ii) a set of cryptographic parameters, and wherein the generated PKI key pair is used for authentication;
	1(e): using the first module public key to authenticate a third message after sending the second response, wherein the third message includes a second module public key with a second module public key identity and the module identity; and,
	1(f): authenticating a fourth message, wherein the fourth message includes the module identity, the second module public key identity, a third source IP:port number, and a module digital signature, wherein the server authenticates the module digital signature using the authenticated second module public key, and wherein the third source IP:port number and the second source IP:port number differ from one another.