

U.S. Patent No. 12,207,094
Element 1[pre]: A method comprising:
Element 1[a][1]: (a) generating a first message comprising
Element 1[a][2][i]: (1) an identity of an embedded universal integrated circuit card (eUICC);
Element 1[a][2][ii]: (2) a nonce; and
Element 1[a][2][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;
Element 1[b]: (b) sending the first message via a network application to a subscription manager system;
Element 1[c]: (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;
Element 1[d]: (d) storing a subscription manager public key which corresponds to a subscription manager private key;
Element 1[e][1]: (e) deriving a profile key using a key exchange algorithm based on at least:
Element 1[e][2]: wherein the profile key can also be derived at the subscription manager system based at least on: the second eUICC public key, and the subscription manager private key;
Element 1[f]: (f) receiving from the subscription manager system, an encrypted profile comprising a ciphertext including a key K encrypted with a symmetric key;
Element 1[g]: (g) receiving the symmetric key;
Element 1[h]: (h) decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key;
Element 1[i]: (i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key; and
Element 1[j]: (j) storing at least the key K in the embedded universal integrated circuit card for use in future communications.
2: The method of claim 1, wherein the subscription manager public key is downloaded via the network application.
3: The method of claim 1, wherein the step of storing the subscription manager public key occurs at the time of manufacture of the embedded universal integrated circuit card.
4: The method of claim 1, wherein the key exchange algorithm is a Diffie-Hellman key exchange.

6: The method of claim 1, wherein the encrypted profile is encrypted in a manner so that intermediate nodes on an IP network would not be able to read data within the profile in an unencrypted form.
7: The method of claim 1, wherein subscription manager system stores the ciphertext and the symmetric key before step (a).
8: The method of claim 1, wherein after the step (b), the embedded universal integrated circuit card is authenticated by the subscription manager system using at least the identity of the embedded universal integrated circuit card included in the first message.
10: The method of claim 1, wherein the decrypted ciphertext is stored in nonvolatile memory of the embedded universal integrated circuit card.
11: The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module and wherein the module is a machine-to-machine module.
12: The method of claim 11, wherein the module comprises a module of a type selected from the group consisting of: vending machine, automobile, alarm system, tracking device, monitoring device, security system and remote control device.
13: The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module and wherein the module is a wireless module.
15: The method of claim 13, wherein the module comprises a module of a type selected from the group consisting of the following: wireless handset, cellular phone, smartphone, laptop computer, tracking device, computer with a radio, circuit board with a radio, hand-held device, netbook, portable computer, multiprocessor system, microprocessor based consumer electronic, programmable consumer electronic, network personal computer, minicomputer, mainframe computer and smartcard.
16: The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module, wherein the module is a wired module.
18: The method of claim 16, wherein the module comprises a module of a type selected from the group consisting of: computer, security camera, security monitoring device and networked controller.
19: The method of claim 1, wherein the deriving step (c) is performed prior to the generating step (a).
20: The method of claim 1, wherein the generating step (a) is performed before the deriving step (c).
21: The method of claim 1, wherein the embedded integrated circuit card is operably connected to a module and a user accesses a user interface of the

module to enter authentication information before the module receives the symmetric key

22: The method of claim 1, wherein the subscription manager receives the ciphertext from a mobile network operator before the network application sends the first message