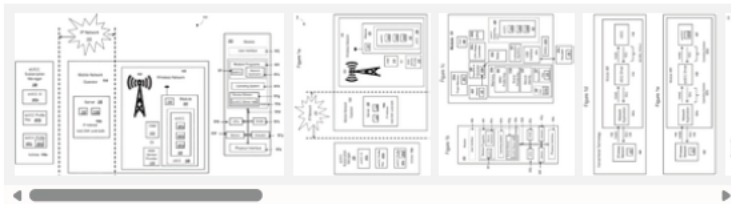


Embedded universal integrated circuit card supporting two-factor authentication

Abstract

A module with an embedded universal integrated circuit card (eUICC) can include a profile for the eUICC. The profile can include a first and second shared secret key K for authenticating with a wireless network. The first shared secret key K can be encrypted with a first key, and the second shared secret key K can be encrypted with a second key. The module can (i) receive the first key, (ii) decrypt the first shared secret key K with the first key, and (iii) subsequently authenticate with the wireless network using the plaintext first shared secret key K. The wireless network can authenticate the user of the module using a second factor. The module can then (i) receive the second key, (ii) decrypt the second shared secret key K, and (iii) authenticate with the wireless network using the second shared secret key K. The module can comprise a mobile phone.

Images (13)



Classifications

■ **H04W12/35** Protecting application or service provisioning, e.g. securing SIM application provisioning

[View 17 more classifications](#)

Landscapes

Engineering & Computer Science

Computer Security & Cryptography

[Show more](#)

Claims (20)

[Hide Dependent](#)

What is claimed is:

1. An embedded universal integrated circuit card (eUICC) comprising:

one or more processors; and

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:

(a) generating a first message comprising:

(1) an identity of the embedded universal integrated circuit card;

(2) a nonce; and

(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;

US11233780B2

United States

[Download PDF](#) [Find Prior Art](#) [Similar](#)

Inventor: John A. Nix

Current Assignee: Network 1 Technologies Inc, M2M and IoT Technologies LLC

Worldwide applications

2013 • [US](#) [US](#) 2014 • [EP](#) [EP](#) [WO](#) [EP](#) [EP](#) [CA](#) 2015 • [US](#)
2016 • [US](#) 2018 • [US](#) [US](#) 2019 • [US](#) [US](#) 2021 • [US](#)
2024 • [US](#) [US](#) [US](#) [US](#)

Application US16/453,682 events

• PTAB case IPR2026-00114 filed (Pending)

2019-06-26 • Application filed by Network 1 Technologies Inc

2019-06-26 • Priority to US16/453,682

2019-10-17 • Publication of US20190319937A1

2022-01-25 • Publication of US11233780B2

2022-01-25 • Application granted

Status • Active

2034-01-04 • Adjusted expiration

[Show all events](#)

Info: [Patent citations \(250\)](#) [Non-patent citations \(120\)](#), [Cited by \(164\)](#), [Legal events](#), [Similar documents](#), [Priority and Related Applications](#)

External links: [USPTO](#), [USPTO PatentCenter](#), [USPTO Assignment](#), [Espacenet](#), [Global Dossier](#), [Discuss](#)

- (b) sending the first message via a network application to a subscription manager system;
 - (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;
 - (d) storing a subscription manager public key which corresponds to a subscription manager private key;
 - (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,
 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;
 - (f) receiving from the subscription manager system, an encrypted profile comprising a ciphertext including a key K encrypted with a symmetric key;
 - (g) receiving the symmetric key;
 - (h) decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key;
 - (i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key; and
 - (j) storing at least the key K in the embedded universal integrated circuit card for use in future communications.
2. The embedded universal integrated circuit card of claim 1, wherein the subscription manager public key is downloaded via the network application.
 3. The embedded universal integrated circuit card 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 embedded universal integrated circuit card of claim 1, wherein the key exchange algorithm is a Diffie-Hellman key exchange.
 5. The embedded universal integrated circuit card of claim 1, wherein the key exchange algorithm is an Elliptic Curve Diffie-Hellman key exchange.
 6. The embedded universal integrated circuit card 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 embedded universal integrated circuit card of claim 1, wherein subscription manager system stores the ciphertext and the symmetric key before step a).
 8. The embedded universal integrated circuit card of claim 1, wherein after the step 1(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.
 9. The embedded universal integrated circuit card of claim 1, wherein after the step 1(b), the eUICC is authenticated by the subscription manager system using at least the digital signature included in the first message.
 10. The embedded universal integrated circuit card of claim 1, wherein the decrypted ciphertext is stored in nonvolatile memory of the embedded universal integrated circuit card.
 11. The embedded universal integrated circuit card of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module includes the eUICC and wherein the module is a machine-to-machine module.
 12. The embedded universal integrated circuit card 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 embedded universal integrated circuit card of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module, includes the eUICC and wherein the module is a wireless module.
 14. The embedded universal integrated circuit card 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.
 15. The embedded universal integrated circuit card of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module, wherein the module is a wired module.
 16. The embedded universal integrated circuit card of claim 15, wherein the module comprises a module of a type selected from the group consisting of: computer, security camera, security monitoring device and networked controller.

17. The embedded universal integrated circuit card of claim 1, wherein the one or more processors perform the deriving step (c) prior to the generating step (a).
18. The embedded universal integrated circuit card of claim 1, wherein the one or more processors perform the generating step (a) before the deriving step (c).
19. The embedded universal integrated circuit card 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.
20. The embedded universal integrated circuit card of claim 1, wherein the subscription manager receives the ciphertext from a mobile network operator before the network application sends the first message.

Description

CROSS-REFERENCE TO RELATED APPLICATIONS

This is a continuation of U.S. patent application Ser. No. 16/110,804, filed Aug. 23, 2018, entitled "Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication," which is a continuation of U.S. patent application Ser. No. 15/928,848, filed Mar. 22, 2018, entitled "EMBEDDED UNIVERSAL INTEGRATED CIRCUIT CARD SUPPORTING TWO-FACTOR AUTHENTICATION," which is a continuation of U.S. patent application Ser. No. 14/751,119, filed Jun. 25, 2015, entitled "An Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication", now U.S. Pat. No. 9,961,060, which is a continuation of U.S. patent application Ser. No. 14/099,329, filed Dec. 6, 2013, entitled "An Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication," now U.S. Pat. No. 9,100,175, the contents of all of which are incorporated herein by reference in their entirety.

The subject matter of this application is related to the subject matter of U.S. patent application Ser. No. 14/084,141, filed Nov. 19, 2013 in the name of John Nix, entitled "Key Derivation for a Module using an Embedded Universal Integrated Circuit Card," now U.S. Pat. No. 9,319,223, which is hereby incorporated by reference in its entirety.

BACKGROUND

Technical Field

The present methods and systems relate to communications for a module, and more particularly, to methods and systems for using an embedded universal integrated circuit card (eUICC), where the methods and systems also support the authentication of a user associated with the eUICC.

Description of Related Art

The combination of "machine-to-machine" (M2M) communications and using low-cost sensors, Internet connections, and processors is a promising and growing field. Among many potential benefits, M2M technologies allow the remote monitoring and/or control of people, assets, or a location where manual monitoring is not economic, or costs can be significantly reduced by using automated monitoring as opposed to manual techniques. Prominent examples today include vending machines, automobiles, alarm systems, and remote sensors. Fast growing markets for M2M applications today include tracking devices for shipping containers or pallets, health applications such as, but not limited to, the remote monitoring of a person's glucose levels or heartbeat, monitoring of industrial equipment deployed in the field, and security systems. Many M2M applications leverage either wired Internet connections or wireless connections, and both types of connections continue to grow rapidly. M2M applications may also be referred to as "the Internet of things".

M2M communications can provide remote control over actuators that may be connected to a M2M device, such as, but not limited to, turning on or off a power switch, locking or unlocking a door, adjusting a speed of a motor, or similar remote control. A decision to change or adjust an actuator associated with an M2M device can utilize one or a series of sensor measurements. An M2M device may also be referred to as a "wireless module" or also simply a module. As one example, if a building or room is too cold, then temperature can be reported to a central server by an M2M device and the server can instruct the M2M device to turn on a switch that activates heat or adjusts a thermostat. As the costs for computer and networking hardware continue to decline, together with the growing ease of obtaining either wired or wireless Internet access for small form-factor devices, the number of economically favorable applications for M2M communications grows.

Many M2M applications can leverage wireless networking technologies. Wireless technologies such as, but not limited to, wireless local area networks and wireless wide area networks have proliferated around the world over the past 15 years, and usage of these wireless networks is also expected to continue to grow. Wireless local area network (LAN) technologies include WiFi and wireless wide area network (WAN) technologies include 3rd Generation Partnership Project's (3GPP) 3rd Generation (3G) Universal Mobile Telecommunications System (UMTS) and 4th Generation (4G) Long-term Evolution (LTE), LTE Advanced, and the Institute of Electrical and Electronics Engineers' (IEEE) 802.16 standard, also known as WiMax. The use of wireless technologies with M2M communications creates new opportunities for the deployment of M2M modules in locations less suitable for fixed-wire Internet access, but also creates a significant new class of problems that need to be solved.

One class of problems for using M2M modules with traditional wireless networks results from basic design considerations for the wireless networks, where many wireless wide-area networking standards were designed and optimized for mobile phones, including smart phones. A core element of traditional wireless WAN technologies such as 3GPP and ETSI standards over the past 20 years has included the use of a subscriber identity module (SIM) card within 2G networks and a related universal integrated circuit card (UICC) for 3G and 4G networks, including LTE networks. ETSI standards for a physical UICC as of 2013 include ETSI TR 102 216. Traditionally, these cards have been supplied by a mobile network operator (MNO) and contain a pre-shared secret key K in addition to a set of parameters for a mobile phone or user equipment to connect with the wireless network operated by the MNO. The parameters could include (i) an identity such as an IMSI, (ii) a set of frequencies for a mobile phone to scan in order to locate a beacon signal from the MNO, (iii) a preferred access list of other MNOs in order to support roaming in locations where the MNI associated with the IMSI is not available, and (iv) many other related parameters as well. The physical media and cards in the form of a UICC can be appropriate or suitable for a mobile phone or mobile

handset, where an end user can readily replace or “swap out” the physical card as the mobile phone changes geographical locations or due to other preferences for the subscriber or end-user. Distributors of either mobile handsets or mobile phone service can physically insert or change an appropriate UICC for the mobile phones as well.

However, the rapid growth for “machine-to-machine” applications has created significant challenges to the traditional model of utilizing physical media such as a UICC in order to provide data and parameters for a module's connectivity to a MNO. Exemplary reasons for potential difficulties with physical media such as a UICC in M2M applications include (i) the modules may be installed in remote locations that are difficult or expensive to reach after installation, such as, but not limited to, tracking devices on shipping containers that can move globally, (ii) a manufacturer or service provider may prefer for the module to be hermetically sealed for business or technical reasons, including the physical UICC may not be easily tampered with, and (iii) a module (such as a tracking device on a 40 foot shipping container) may move between several different countries, and the lowest costs for Internet or data connectivity through the wireless WAN may be through utilizing different UICC cards from different operators, but the cost of swapping the UICC card could be prohibitive.

Other needs for changing a preferred network or network credentials without physically changing a UICC exist as well. These needs have been one motivation for the industry, including ETSI and 3GPP standards bodies, to consider an embedded UICC, also known as an “eUICC”. With an eUICC, the operation of a UICC can be essentially “virtualized”, such that the data and algorithms within a UICC can be processed in software and distributed through electronic media (such as, but not limited to, a file transfer or file download). Exemplary benefits and technical considerations for using an eUICC in M2M applications as of November 2013 is outlined in ETS TS 103 383 v12.1, entitled “Smart Cards; Embedded UICC; Requirements Specification,” which is herein incorporated by reference in its entirety. Note that this published standard from June 2013, and the standard is primarily in the requirements definition phase, and many of the technical specifications for implementation and operation of an eUICC will be defined in the future.

Although the use of an embedded eUICC can solve many of the issues for distributing and managing physical media such as a UICC, many additional challenges remain. Many open and remaining challenges for a eUICC pertain to securely and electronically transferring a new set of MNO network access credentials (such as an IMSI and network key K) to a module in a secure and efficient manner. A need exists in the art for a module to securely obtain network access credentials. Another need exists in the art for the obtained credentials in a eUICC to be fully compatible with the significant installed and legacy base of networks that use a pre-shared secret key K, where the key K serves as the foundation for authentication and ciphering of data for a mobile phone or user equipment, including modules using conventional technology. A successful solution to these needs for M2M applications in the form of an eUICC can also provide a working solution of the needs for regular mobile phones as well, such that a consumer mobile phone or smartphone could implement and utilize an eUICC in order to eliminate the costs and complexity of dealing with a physical UICC.

A need exists in the art for module and a mobile network operator to securely share a pre-shared secret key K without depending on physical distribution of the key K or electronic distribution of the key K through 3rd parties, even in an encrypted form. A need exists in the art for the decryption of data within an eUICC profile to be under the control of the mobile network operator, because the mobile network operator may not control the distribution or release of profiles from an eUICC subscription manager to a module with an eUICC. As currently contemplated in November of 2013 by eUICC standards discussed above, a pre-shared secret key K and related network access credentials are transmitted to a module from an eUICC subscription manager. The pre-shared secret key K is also known as key K in 4G LTE and related networks and key Ki in 3G networks. The resulting security for the electronically transferred, pre-shared secret key K is no stronger than (i) the encryption on the channel used to transfer key K, and (ii) the security and chain of control for keys used to encrypt the communications channel transferring key K to a module or a mobile phone. A module and mobile network operator (MNO) using an electronically transferred key K for network access credentials is dependent on the communications channel for transferring key K, even though that communications channel may be outside the control of the MNO (such as at a time when key K is transferred using another MNO or a different network). Therefore, a need exists in the art for the MNO to securely and efficiently control the use of an electronically transferred key K within a profile for an eUICC, even though copying and distributing the profile may be outside the control of the MNO.

In addition, over an extended period of time such as several years, a mobile network operator could prefer for the key K to periodically rotate or change for an individual module or mobile phone in order to increase security. The continued and extended use of a single key K for all communications with a module or mobile phone can be a security risk, especially with a large volume of data transferred that could be subject to analysis for cryptographic weaknesses by potential attackers. Additionally, in the future a standard key length for key K may increase from today's current 128 bits to a longer key length such as an exemplary 256 bits. With conventional technology where key K is recorded in physical media such as a UICC, the only feasible way to change key K for a module or mobile phone is to physically distribute a new UICC card, with resulting costs and business complexities. A need exists in the art for a module, including a mobile phone, and a MNO to securely and efficiently support a change in network access credentials, including a key K for the module connecting to the MNO, without requiring a physical replacement of a UICC or equivalent physical media recording a key K.

And other needs exist in the art as well, as the list recited above is not meant to be exhaustive but rather illustrative.

SUMMARY

Methods and systems are provided for secure and efficient communication using a module to communicate with a server and a mobile operator network. The module can support “Machine to Machine” (M2M) communications, also known as “the Internet of things”. The methods and systems contemplated herein can also support other applications as well, including mobile phone handsets connecting to a wireless network, where the wireless network can be associated with or the radio access portion of a mobile network operator. A module in the present invention can comprise a mobile phone such as a smartphone, and may also be referred to as a mobile device, mobile station, or user equipment. An objective of the invention is to address the challenges noted above for securing the deployment of modules that can utilize an embedded universal integrated circuit card (eUICC) and/or also PKI algorithms and keys.

The methods and systems contemplated herein can reduce the need for manual intervention with a module in order to automatically and remotely change network access credentials in order for the module to utilize new or different keys in order to connect and authenticate with a wireless network. By using an eUICC, where the eUICC can support both (i) the authentication of a user by the MNO, and (ii) the secure decryption or derivation of the key K under control of the MNO, the value and usefulness of modules can be increased for a user and a mobile operator network. An eUICC can also comprise

software and/or firmware components to "virtualize" the operation of a physical UICC, such that (i) the data normally recorded in a physical UICC can be recorded in a file with encryption, and (ii) the steps for using the data in the file can be processed by an eUICC.

In a first embodiment, a mobile network operator can process a set of data for inclusion in a profile for an eUICC. Data within the profile can be equivalent or similar to the data recorded in a physical UICC, including a set of network parameters, a module network identity, and a first key K. The mobile network operator can send the data for a profile to an eUICC subscription manager. A module can include an embedded universal integrated circuit card (eUICC). The eUICC can be processed by an operating system on the module and can be recorded in a nonvolatile memory, such that the eUICC is available after a powered off state. The eUICC can include data such as an eUICC identity, an eUICC profile key, and a symmetric ciphering algorithm. A manufacturer or distributor could record the data for the eUICC before the module is received by a user. The eUICC can communicate in the module with a network application. The network application can communicate with the mobile network operator using a wireless network and a radio within the module. The module can connect with a first network, send the eUICC identity and receive an encrypted profile, and the module can record the encrypted profile in a nonvolatile memory associated with the eUICC. The first network can be a network different than the wireless network for the profile, and the first network could comprise a WiFi network, a LAN connection using a USB interface to the module, or a public land mobile network.

Continuing with this first embodiment, the encrypted profile as received by the module can include a first portion of ciphertext and a second portion of ciphertext. The module using the eUICC can decrypt the first portion of ciphertext using the eUICC profile key and the symmetric ciphering algorithm. The resulting plaintext from the decrypted first portion of ciphertext can include the set of network parameters, the first network module identity, and the first key K. The module using the eUICC can select and activate the profile in order to connect with the wireless network associated with the mobile network operator. The module can conduct a first authentication with the mobile network operator using the first network module identity and the first key K. The module can send an attach request message, including an exemplary radio resource request message with the first network module identity, and the module can receive a random number in the form of a first RAND value.

Continuing with this first embodiment, the module can forward the RAND to the eUICC with the activated profile. The eUICC can input the first RAND and the first key K into a cryptographic algorithm in order to output a response RES value. The eUICC can return the RES value to the module, and the module could forward the RES to the wireless network. The wireless network can compare the received RES with a stored, expected RES (previously calculated using the same first RAND and first key K), and if the two RES values match then the module with the eUICC and profile can be authenticated by the network. The network and the module can take additional steps for the module to have at least limited access to an IP network. With access to the IP network for the module, a user associated with the module can conduct an authentication with the mobile network operator (whereas the mobile network operator may not have control over distribution of the profile with the network access credentials including the first key K up to this point).

Continuing with this first embodiment, the mobile network operator can authenticate or verify a user or M2M service provider associated with the module. The authentication or verification could comprise steps to verify a user, including the user entering information in a web page through the IP connection established with the network in the paragraph above using the first key K. Or the user could place a telephone call to a call center, and the user could verbally confirm identification information or enter DTMF digits. Or, the MNO could authenticate or verify the identity of a user associated with the module by a representative of the MNO visually viewing physical identification of the user such as a drivers license or a passport. If the module is associated with or operated by an M2M service provider, then the MNO could exchange data with the M2M service provider in order to confirm the module with the first key K is authenticated. In either case, where the module is associated with a user or an M2M service provider, the MNO could take steps to authenticate with a second factor, where authentication with the first factor comprised receiving the RES. After successful authentication with the second factor, the MNO can confirm the identity of an entity associated with the module, whereas that identity may not be known before the authentication with the second factor since the distribution of the eUICC profile may be outside the control of the mobile network operator.

Continuing with this first embodiment, after successful authentication with the second factor, the mobile network operator can send a symmetric key to the module. The symmetric key can be encrypted with a key ciphering algorithm. Or, the symmetric key can be (i) plaintext at the application layer, and (ii) encrypted at the data-link layer using the encryption between the module and wireless network after the first authentication above with the first key K. The module can receive the symmetric key (and decrypt the symmetric key if encrypted), and subsequently decrypt the second portion of ciphertext in the eUICC profile. The second portion of ciphertext can include a second network module identity and a second key K. The module can convert the second portion of ciphertext into plaintext using the symmetric ciphering algorithm and the received symmetric key. Note that the decryption of the second portion of ciphertext in the profile without the symmetric key is not feasible, and thus the mobile network operator can retain control over the use of the second key K in the profile for the eUICC, such as not releasing the symmetric key until after a user has successfully completed authentication with the mobile network operator as contemplated in the paragraph above.

After decrypting the second portion of ciphertext, the module with the eUICC can read a plaintext second network module identity and second key K. The second key K can be recorded in a protected, nonvolatile memory. The module can disconnect from the wireless network (where the first session used the first key K), and reconnect with the wireless network using the second network module identity and the second key K. The module with the eUICC can conduct a second authentication using the second key K, including sending the second network module identity, receiving a second RAND value, calculating a second RES value using the second RAND and the second key K, and sending the second RES value. After a successful second authentication, the module can access the IP network and the public Internet through the wireless network, and subsequent authentications with the wireless network can continue to use the second network module identity and the second key K. For embodiments where the module comprises a mobile phone and the user is an individual subscribing to mobile phone services from the mobile network operator, the user can be associated with a telephone number and place/receive phone calls after a successful second authentication.

In another embodiment, the eUICC profile key, associated with decrypting the profile from the eUICC subscription manager, may not be recorded in the eUICC before the eUICC sends an eUICC identity to the module, where the module sends the eUICC identity to the eUICC subscription manager through a first network. The eUICC can record an eUICC private key and the eUICC subscription manager could record an eUICC public key. The eUICC subscription manager can (i) encrypt the profile with the eUICC profile key, and then (ii) encrypt the eUICC profile key with an asymmetric ciphering algorithm and the eUICC public key, where the output is an encrypted eUICC profile key. The eUICC can receive the encrypted eUICC profile key from the eUICC subscription manager and decrypt the encrypted eUICC key using the asymmetric ciphering algorithm and the eUICC private key. After reading the plaintext eUICC

profile key, the eUICC can decrypt the encrypted profile using the plaintext eUICC profile key, in order to read a plaintext first key K and first network module identity.

In an exemplary embodiment, the first key K is a null value for a profile recorded in the eUICC in a module. The use of a null value or the number zero for a shared secret key K is contemplated in wireless WAN standards and supported by commercial wireless networks in order to support emergency services for a module without a valid UICC. With a null value for the first key K, the MNO and wireless network can provide limited access to the IP network, such that a user of the module with a null or zero value for the first key K could perform steps to authenticate or verify the user with the MNO through the IP network accesses with the first key K as a null value. The data-link layer may not be effectively ciphered due to the use of a null value for the first key K, but the application or transport layer could secure communication from a web browser on the module to a web server for the user to authenticate with the MNO. The secure communication between the web browser and web server can utilize transport layer security (TLS) or similar standards for security at the transport or application layer, even though the data-link or network layer may not be encrypted. After successful authentication via the web browser, the MNO can take steps (discussed in other embodiments) allowing the module with the eUICC to access and use a second key K and a second network module identity for subsequent secured communication between the module and the MNO.

In another embodiment, the second key K can be derived using by both the mobile network operator and the module with the eUICC using a key derivation algorithm. The eUICC could include an eUICC key exchange algorithm and the mobile network operator could include a MNO key exchange algorithm, and the key exchange algorithms can include a key derivation algorithm that accepts input of a token value, a private key, and a public key for the other node. The mobile network operator and the module with the eUICC could communicate the token value used for the key derivation algorithm (including using the connectivity through the wireless network after using the first key K in the profile). The module can record an eUICC private key, and the MNO can have access to the eUICC public key. The key derivation algorithm in the eUICC key exchange algorithm can output a second key K using the token. The MNO can obtain the same value for the second key K. In this manner, both node can derive the same second key K without electronically transferring the second key K, even in encrypted form and thereby increasing the security of a systems with an eUICC.

In an exemplary embodiment can support a module changing a key K used to (i) authenticate with a wireless network and (i) cipher/decipher data with a wireless network. The module can change key K without requiring the manual exchange of a UICC or other physical intervention. The module can use an eUICC profile and change key K while using the same eUICC profile. The module, could also comprise a mobile phone such as, but not limited to, a smart phone. After connecting with a first network, which could comprise a first wireless WAN, wireless LAN, or wired connection, the module can receive a eUICC profile for an eUICC in the module, where the eUICC profile includes a first network module identity and a first key K. The first key K can be a standards-based key K used with wireless networks, and be equivalent to a pre-shared secret key K recorded in physical UICCs for LTE networks.

After authenticating with the wireless network using the first key K, the module and MNO can share a token. The module and MNO can mutually derive a second key K using the token and a key derivation algorithm. The module can disconnect from the wireless network after attaching using the first key K, and then reconnect using the second key K which has now been mutually derived by both the module and the mobile network operator. The module or MNO could determine or evaluate if the use of a new key K is required or preferred, and share a new token for input into the key derivation algorithms to derive a mutually shared new key K. In this manner, a module can change the key K used to authenticate and cipher/decipher data with a wireless network from a first key K to a second key K. This can increase flexibility of the system and reduce costs of physically distributing a new UICC to the module (or electronically sending new eUICC profiles) in order to change a key K.

These as well as other aspects and advantages will become apparent to those of ordinary skill in the art by reading the following detailed description, with reference where appropriate to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Various exemplary embodiments are described herein with reference to the following drawings, wherein like numerals denote like entities.

FIG. 1a is a graphical illustration of an exemplary system that includes a module and a mobile network operator, in accordance with exemplary embodiments;

FIG. 1b is a graphical illustration of hardware, firmware, and software components for a module, in accordance with exemplary embodiments;

FIG. 1c is a graphical illustration of components within a module, in accordance with exemplary embodiments;

FIG. 1d is a graphical illustration for authenticating with a wireless network using a physical UICC, in accordance with conventional technology;

FIG. 1e is a graphical illustration for authenticating with a wireless network using an eUICC, in accordance with exemplary embodiments;

FIG. 1f is a graphical illustration of an exemplary system that includes a module, a mobile network operator, and an eUICC in accordance with exemplary embodiments;

FIG. 2a is a graphical illustration of an exemplary profile for an eUICC, including encrypted data, decryption steps, and decrypted data for the profile, in accordance with exemplary embodiments;

FIG. 2b is a graphical illustration for ciphering and deciphering a profile using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments;

FIG. 2c is a graphical illustration for ciphering and deciphering a key K using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments;

FIG. 2d is a graphical illustration of a public key and a private key for an eUICC, in accordance with exemplary embodiments;

FIG. 2e is a graphical illustration for ciphering and deciphering a key for an eUICC using an asymmetric ciphering algorithm using a PKI key pair, in accordance with exemplary embodiments;

FIG. 3 is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments;

FIG. 4 is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments;

FIG. 5a is a graphical illustration of a public keys, private keys, and a key derivation algorithm, in accordance with exemplary embodiments;

FIG. 5b is a graphical illustration of deriving a second key K using public keys, private keys, and a key derivation algorithm, in accordance with exemplary embodiments;

FIG. 5c is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments; and,

FIG. 6 is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS OF THE INVENTION

FIG. 1a

FIG. 1a is a graphical illustration of an exemplary system that includes a module and a mobile network operator, in accordance with exemplary embodiments. The system 100 includes a module 101 operating within a wireless network 102. System 100 can also include a mobile network operator 104, an IP Network 111, and an eUICC subscription manager 109. Mobile network operator (MNO) 104 can include a server 105. For embodiments where the MNO 104 uses 4G LTE and LTE Advanced networks server 105 could comprise a home subscriber server (HSS) and/or a mobility management entity (MME). Server 105 could be a server with related functionality as a HSS or MME for a MNO 104 that uses different wireless network standards than those based on 4G LTE. Although not illustrated in FIG. 1a, an eUICC subscription manager 109 may also include one or more servers 105, such that a first server 105 could function as an HSS in 4G LTE and LTE Advanced networks and a second server 105 could function as a MME in 4G LTE and LTE Advanced networks.

System 100 is illustrated without specific packet transmissions between module 101 and mobile network operator 104 and eUICC subscription manager 109. Examples of the communications and messages pertaining to the present invention will be illustrated in later Figures. As contemplated herein, machine-to-machine communications may comprise communication between a module 101 and a server 105, such that data can be transferred between the two with minimal manual intervention, although manual intervention can be required to set up system 100 and any occasional manual maintenance required. As contemplated herein, machine-to-machine communications may also be referred to as "the Internet of things" (IoT). Also note that module 101 may comprise a wireless module, such that module 101 can communicate with wireless network 102 using a radio and an antenna. A wireless or a wired configuration for module 101 can be utilized in the present invention.

If module 101 operates as a wireless module, module 101 and wireless network 102 can communicate using a base station 103. Module 101 and wireless network 102 can utilize a variety of wireless technologies to communicate, including WiFi, WiMax, a 2nd generation wireless wide area network (WAN) technology such as, but not limited to, General Packet Radio Services (GPRS) or Enhanced Data rates for GSM Evolution (EDGE), 3rd Generation Partnership Project (3GPP) technology such as, but not limited to, 3G, 4G LTE, or 4G LTE Advanced, and other examples exist as well including wireless networks based on WiMAX standards. A wired module 101 can connect to the IP Network 111 via a wired connection such as, but not limited to, an Ethernet, a fiber optic, or a Universal Serial Bus (USB) connection (not shown).

Generally, the communication techniques described herein can be independent of the network technologies utilized at the physical and data-link layers, so long as the underlying network provides access to the IP Network 111 and supports Internet Protocols (IP). The IP Network 111 can be an IPv4 or an IPv6 packet-switched based network that utilizes standards derived from the Internet Engineering Task Force, such as, but not limited to, RFC 786 (User Datagram Protocol), RFC 793 (Transmission Control Protocol), and related protocols. The IP Network 111 can be the public Internet comprising globally routable IP addresses, or a private network that utilizes private IP addresses. IP Network 111 as illustrated in FIG. 1a could comprise the globally routable public Internet, or IP Network 111 could also be a private Internet that is (i) not globally routable and (ii) only accessible to authorized modules and servers. As one example of a private IP Network 111, IP Network 111 could use private IP addresses for nodes on the network, and in this case IP Network 107 could be referred to as an intranet or private network. Alternatively, IP Network 111 could be a private network layered on top of the publicly routable Internet via secured and encrypted connections. The specific numbers for IP addresses and port numbers shown in FIG. 1a and other figures are illustrative and any valid IP address or port number can be used, including an IPv4 and an IPv6 address. Server 105 within mobile network operator 104 can communicate with the module 101 using IP network 111, where IP network 111 can comprise a private network that utilizes Internet Protocol standards. Module 101 can access the public Internet after authenticating with the server 105 associated with the MNO 104.

When operating in a wireless network configuration module 101 can access the IP Network 111 via the wireless network 102. In the wireless network configuration, module 101 can be a wireless handset, a cellular phone, a smartphone, a tablet computer, a laptop, a computer with a radio, a tracking device, or a circuit board with a radio that accesses wireless network 102. Examples of wireless modules that utilize a wireless WAN such as, but not limited to, 2G and 3G networking technologies include the Motorola® G24-1 and Huawei® MC323. Example manufacturers of wireless modules in 2012 include Sierra Wireless® and Telit®. Example leading manufacturers of mobile phones in 2013 include Apple® and Samsung®. In a wired configuration (not shown), module 101 can be a computer, security camera, security monitoring device, networked controller, etc. Module 101 can include a module identity 110, which can comprise a serial number or identity code in order to identify an individual, specific module 101 among a plurality of modules 101. A more detailed depiction of exemplary components of a module 101 is included in FIG. 1b and FIG. 1c below. Module 101 could also operate as a "smartcard" such that an end user presents module 101 to merchants for payments.

Wireless network 102 may comprise either a wireless local area network (LAN) or a wireless WAN such as a public land mobile network (PLMN). Examples for technologies used in wireless LANs include an 802.11 WLAN, Bluetooth, or Zigbee among other possibilities. Module 101 operating in wireless mode could communicate with a base station 103 of a wireless network 102 using a radio and an antenna. Wireless network 102 could operate

as a Mode II device according to FCC Memorandum Opinion and Order (FC-12-36) and related white space regulation documents. If module **101** supports IEEE 802.15.4, then wireless network **102** could be a Zigbee network, an ISA100.11a standards-based network, or a 6LoWPAN network as described by IETF RFC 4944. Other possibilities exist as well for the wireless technology utilized by a wireless network **102** and module **101**, operating in a wireless mode, without departing from the scope of the present invention.

System **100** can include an eUICC subscription manager **109**, where an eUICC subscription manager **109** can manage the recording and secure distribution of eUICC profiles **107 c** to a module **101**. Example entities that could operate or control an eUICC subscription manager **109** include a manufacturer of module **101**, an M2M service provider that manages the operation of module **101**, or possibly a mobile network operator **104** could operate the eUICC subscription manager **109**. Other entities could operate as an eUICC subscription manager **109** as well. An exemplary eUICC subscription manager **109** is described in ETSI TS 103 383 v12.1, entitled "Smart Cards; Embedded UICC; Requirements Specification," which is herein incorporated by reference in its entirety. An eUICC subscription manager **109** can also use a server **105** and record private keys and public keys for the server/subscription manager operation (including exemplary keys depicted and described in connection with FIG. 2d below).

In exemplary embodiments, eUICC subscription manager **109** can use an eUICC profile key **107 b** to cipher portions of an eUICC profile **107 c**, such that only module **101** with the same eUICC profile key **107 b** could reasonably decipher the portions of the eUICC profile **107 c**. In this manner, the eUICC profile **107 c** can remain reasonably secured. The eUICC subscription manager **109** can share the eUICC profile key **107 b** in several different ways, including (i) pre-sharing the eUICC profile key **107 b**, or (ii) the eUICC subscription manager **109** sending the eUICC profile key **107 b** to the eUICC **107** using an asymmetric ciphering algorithm **219** as depicted and described in connection with FIG. 2e below. An eUICC profile **107 c** can include an eUICC profile identity **107 e** in order to identify a profile among a plurality of eUICC profiles **107 c**. An eUICC subscription manager **109** can include an address **109 a**. The address **109 a** could comprise a domain name, such that a domain name system (DNS) or secure DNS (DNSSEC) query could resolve the name into an IP address in order for module **101** to communicate with the eUICC subscription manager **109**. Or the address **109 a** could comprise an Internet Protocol (IP) address, and the address **109 a** could include or be associated with a port number, such as port number **443** for data that utilizes transport layer security.

An eUICC **107** within module **101** can comprise an embedded universal integrated circuit card (eUICC) **107**. An eUICC **107** can provide the equivalent functionality as a physical UICC, where definitions for a physical UICC are included in ETSI TR 102 216 and ETSI TS 102 221 V11.0.0, and other examples for the use of a physical UICC in mobile phones and M2M modules exist as well. An eUICC **107** in FIG. 1a can support exemplary requirements for an eUICC outlined in ETSI TS 103 383 v12.1, entitled "Smart Cards; Embedded UICC; Requirements Specification," which is herein incorporated by reference in its entirety. In other words, an eUICC **107** can operate as a "virtualized" UICC, such that data operations and input/output to a physical UICC can be provided by an eUICC **107**. Exemplary details of a conventional, physical UICC for authenticating a module **101** (which can be "virtualized" in an eUICC **107**) are depicted and described in connection with FIG. 1d below. An eUICC **107** can include an eUICC identity **107 a**, such that an eUICC subscription manager **109** can select and identify the eUICC **107** among a plurality of eUICCs **107**. The eUICC **107** can also record an eUICC profile key **107 b** and an eUICC profile **107 d**. Profile **107 d** can represent a profile that is partially decrypted using the eUICC profile key **107 b**, as depicted and described in connection with FIG. 2a below. Additional exemplary details for the operation of an eUICC **107** within module **101** are also provided in FIG. 1b, FIG. 1c, FIG. 1e, and FIG. 1f below.

According to an exemplary embodiment, an eUICC **107** can be recorded and operate within a "eUICC supporting" physical universal integrated circuit card (UICC) **108** within module **101**. This "eUICC supporting", physical UICC **108** can include a processing unit, RAM memory, ROM memory, EEPROM memory, a bus, and a physical interface (not shown in FIG. 1a, but described in FIG. 1b). An exemplary processing unit, RAM memory, ROM memory, EEPROM memory, and bus are depicted and described in connection with FIG. 1b below. The physical interface for an UICC **108** is depicted and described in connection with FIG. 1d below. The "eUICC supporting" physically UICC **108** can perform all of the functions of an eUICC **107**, including (i) receiving and recording profiles **107 d**, (ii) receiving and recording eUICC profile keys **107 b**, (iii) recording an eUICC identity **107 a**, (iv) decrypting an eUICC profile **107 c** into an eUICC profile **107 d** as depicted and described in connection with FIG. 2a below, (v) recording a set of network parameters **201** (in FIG. 2a below) for module **101** to connect with wireless network **102**, and (vi) recording keys such as a key K for conducting a message digest authentication with wireless network as depicted and described in FIG. 1d, FIG. 1e, and FIG. 3 below. An "eUICC supporting" physical UICC **108** can include a physical electrical interface of ISO/IEC 7816-3 in order to support existing physical slots for UICCs. The use of an "eUICC supporting" physical UICC **108** is optional, and can be omitted. In this case (where "eUICC supporting" physical UICC **108** is omitted), the eUICC **107** can operate as a program within module **101** as depicted and described in connection with FIG. 1b below, and the eUICC **107** would not reside within the "eUICC supporting" physical UICC **108**.

The physical form-factor for an "eUICC supporting" UICC **108** could be identical to a UICC, and a difference between the two may not even be apparent upon visual inspection without special markings on the card. The physical form-factor for an "eUICC supporting" UICC **108** could comprise a "micro-SIM" or a "nano-SIM" as defined in ETSI TS 102 221 V11.0.0, which is herein incorporated by reference. When the module **101** detects a "eUICC supporting" UICC **107**, the module **101** could send received eUICC profiles **107 c** to the "eUICC supporting" UICC **107**, and also select, deselect, activate, and deactivate the different received eUICC profiles **107 d** recorded in the "eUICC supporting" UICC **108**. When a module **101** detects that a regular UICC (i.e. not an "eUICC supporting" UICC **108**) has been loaded into a slot for UICCs within the module, the module **101** could access the UICC in a regular manner implemented by mobile phones and modules for connecting to existing wireless networks in 2013, such as LTE or 3G networks. This use of conventional technology for a physical UICC is depicted and described in connection with FIG. 1d below.

A module **101** can be associated with a user **113** or an M2M service provider **115**. A user **113** could be a subscriber to mobile phone services provided by the mobile network operator **104**. In this case, the user could be an individual and the module **101** could comprise a mobile phone with a telephone number, an email client, and a web browser (in addition to other, standard functionality for a mobile phone). The user **113** could periodically charge the module **101** (which can comprise a mobile phone), such as typically at night and carry the module **101** during the day in order to place calls and send/receive data. Thus, the user **113** may typically be physically close to a mobile phone as module **101**, but an M2M service provider **115** can be associated with module **101** but may not be physically close to module **101**. For embodiments where module **101** is associated with M2M communications, such as including a sensor to collect data regarding a monitored unit, the module **101** can be associated with an M2M service provider **115**. In this case, the M2M service provider **115** can be a company or a division or department within a larger company that is associated with a plurality of modules **101** for collecting data using sensors and sending the data to a server similar to server **105**. The M2M service provider **115** may operate the

server similar to server 105 in order to automatically collect data from the plurality of modules 101. The server for the M2M service provider 115 could communicate with module 101 using the IP network 111 and the wireless network 102 when module 101 is connected to the wireless network 102.

Other configurations besides the one illustrated in FIG. 1a are possible as well. In many common commercial relationships for the operation of mobile phone service in the United States in 2013, wireless network 102 could represent a portion of the radio access network used by a mobile network operator 104. MNO 104 could outsource portions of the operation and maintenance of a radio access network, such as a wireless network 102, to 3rd parties. In this configuration, wireless network 102 could represent a network operated by a first company specializing in the operation of radio towers and BTS equipment. This first company could be contracted with the mobile network operator 104 in order to support mobile phone service or data services to modules 101.

In addition, server 105 could reside within wireless network 102 in a data center managed by wireless network 102. Wireless network 102 could also operate as an eUICC subscription manager 109. Although a single module 101, server 105, wireless network 102, and mobile network operator 104 are illustrated in FIG. 1a, system 100 could comprise a plurality of each of these elements. Module 101 could also record sensor data pertaining to a monitored unit (not shown). Module 101 could be mobile, such as physically attached to a truck or a pallet, and module 101 could connect to a series of different wireless networks 102 or base stations 103 as module 101 moves geographically. Other configurations are possible as well for the elements illustrated in FIG. 1a without departing from the scope of the present invention.

FIG. 1b

FIG. 1b is a graphical illustration of hardware, firmware, and software components for a module, in accordance with exemplary embodiments. FIG. 1b is illustrated to include many components that can be common within a module 101, and module 101 may also operate in a wireless configuration in order to connect with a wireless network 102. In a wireless configuration, the physical interface 101 a of module 101 may support radio-frequency (RF) communications with networks including a wireless network 102 via standards such as, but not limited to, GSM, UMTS, mobile WiMax, CDMA, LTE, LTE Advanced, and/or other mobile-network technologies. In a wireless configuration, the physical interface 101 a may also provide connectivity to local networks such as, but not limited to, 802.11 WLAN, Bluetooth, or Zigbee among other possibilities. In a wireless configuration, module 101 could use a physical interface 101 a to be connected with both a wireless WAN and wireless LAN simultaneously. In a wired configuration, the physical interface 101 a can provide connectivity to a wired network such as, but not limited to, through an Ethernet connection or USB connection. As contemplated herein, a physical interface 101 a can include a network interface (such as a radio or an Ethernet port), such that module 101 can use the network interface in order to connect with a network and communicate with the network. A network interface can also comprise a physical interface 101 a as contemplated herein.

The physical interface 101 a can include associated hardware to provide the connections such as, but not limited to, radio-frequency (RF) chipsets, a power amplifier, an antenna, cable connectors, etc., and additional exemplary details regarding these components are described below in FIG. 1c. Device driver 101 g can communicate with the physical interfaces 101 a, providing hardware access to higher-level functions on module 101. Device drivers 101 g may also be embedded into hardware or combined with the physical interfaces 101 a. Module 101 may preferably include an operating system 101 h to manage device drivers 101 g and hardware resources within module 101. The operating systems described herein can also manage other resources such as, but not limited to, memory and may support multiple software programs operating on module 101 at the same time.

The operating system 101 h can include Internet protocol stacks such as, but not limited to, a User Datagram Protocol (UDP) stack, Transmission Control Protocol (TCP) stack, a domain name system (DNS) stack, etc., and the operating system 101 h may include timers and schedulers for managing the access of software to hardware resources. The operating system shown of 101 h can be appropriate for a low-power device with limited memory and CPU resources (compared to a server 105). An example operating system 101 h for module 101 includes Linux, Android® from Google®, Windows® Mobile, or Open AT® from Sierra Wireless®. Additional example operating systems 101 h for module 101 include eCos, uC/OS, LiteOs, and Contiki, and other possibilities exist as well without departing from the scope of the present invention.

A module program 101 i may be an application programmed in a language such as, but not limited to, C, C++, Java, and/or Python, and could provide functionality to support regular mobile phone functionality. The module program 101 i could include a network application 101 x, where network application 101 x comprises the user equipment protocol for accessing and communicating with the wireless network 102. For embodiments where module 101 connects with a wireless network 102 comprising an LTE network, the network application 101 x can receive, process, and send signals with the wireless network 102 for user equipment messages in ETSI TS 136 331 v.10.7 entitled "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification", which is herein incorporated by reference. In other words, network application 101 x can comprise software for accessing and communicating with the wireless network 102. Although network application 101 x is depicted in FIG. 1b as operating as software within RAM memory 101 e, the network application 101 x could be included in firmware or a processor or application associated with a radio 101 z (described in FIG. 1c). Exemplary messages sent and received by a network application 101 x are also depicted and described in connection with FIG. 3 below.

A module program 101 i could also include software for M2M applications such as, but not limited to, remote monitoring of sensors and remote activation of actuators. Module program 101 i could also include a software routine, subroutine, linked library, or software module, according to one preferred embodiment. As contemplated herein, a module program 101 i can include an application operating within a smartphone, such as, but not limited to, an iPhone® or Android®-based smartphone, and in this case module 101 could comprise a smartphone. The application functioning as a module program 101 i could be downloaded from an "app store" associated with the smartphone. A set of device drivers 101 g could include an eUICC driver 129, such that a network application 101 x or other software or firmware within module 101 communicating with the eUICC 107 could send and receive data with the eUICC driver 129. Additional details regarding an exemplary eUICC driver 129 are depicted and described in connection with FIG. 1e below.

Many of the logical steps for operation of module 101 or eUICC 107 can be performed in software and hardware by various combinations of physical interface 101 a, device driver 101 g, operating system 101 h, and a module program 101 i. As depicted in FIG. 1b, module program 101 i can include an eUICC 107 and a network application 101 x. When module 101 or eUICC 107 is described herein as performing various actions such as acquiring an IP address, connecting to the wireless network, monitoring a port, transmitting a packet, sending a message, receiving a response, or encrypting or signing data, specifying herein that module 101 or eUICC 107 performs an action can refer to software, hardware, and/or firmware operating within module 101 illustrated in FIG. 1b or FIG. 1c performing the action.

Note that module 101 may also optionally include user interface 101 j which may include one or more devices for receiving inputs and/or one or more devices for conveying outputs. User interfaces are known in the art and thus user interfaces are not described in detail here. User interface 101 j could comprise a touch screen if module 101 operates as a smartphone or mobile phone. For embodiments where module 101 comprises a module for M2M applications and is associated with an M2M service provider 115, then module 101 can optionally omit a user interface 101 j, since no local user 113 input may be required for many M2M applications, although a user interface 101 j could be included with module 101. For embodiments where module 101 comprises a mobile phone and is associated with a user 113, the user interface 101 j could comprise a touch screen on the front of a mobile phone.

Module 101 may be a computing device that includes computer components for the purposes of collecting data from a sensor 101 f or triggering an action by an actuator 101 y. Module 101 may include a central processing unit (CPU) 101 b, a random access memory (RAM) 101 e, and a system bus 101 d that couples various system components including the random access memory 101 e to the processing unit 101 b. The system bus 101 d may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures including a data bus. Note that the computer components illustrated for the module 101 in FIG. 1b may be selected in order to minimize power consumption and thereby maximize battery life, if module 101 includes a battery and is not attached to external power. In addition, the computer components illustrated for the module 101 in FIG. 1b may also be selected in order to optimize the system for both long periods of sleep or idle states relative to active communications and also may be optimized for predominantly uplink (i.e. device to network) communications with small packets or messages. The computer components illustrated for the module 101 in FIG. 1b may also be general-purpose computing components, and specialized components may not be required in order to utilize many of the embodiments contemplated herein.

Module 101 may include a read-only memory (ROM) 101 c which can contain a boot loader program. Although ROM 101 c is illustrated as "read-only memory", ROM 101 c could comprise long-term memory storage chipsets or physical units that are designed for writing once and reading many times. As contemplated within the present invention, a read-only address could comprise a ROM 101 c memory address or another hardware address for read-only operations accessible via bus 101 d. Changing data recorded in a ROM 101 c can require a technician have physical access to module 101, such as, but not limited to, removing a cover or part of an enclosure, where the technician can subsequently connect equipment to a circuit board in module 101, including replacing ROM 101 c. ROM 101 c could also comprise a nonvolatile memory, such that data is stored within ROM 101 c even if no electrical power is provided to ROM 101 c. Although not illustrated in FIG. 1b, but illustrated in FIG. 1c below, module 101 could also include a flash memory 101 w. Module program 101 i, network application 101 x, operating system 101 h, eUICC 107, or device drivers 101 g could be stored in flash memory 101 w within module 101 when the module is powered off. These components and/or instructions could be moved from a flash memory 101 w (not shown in FIG. 1b but shown in FIG. 1c) into RAM 101 e when the module is powered on by a bootloader program recorded in the ROM 101 c. Note that ROM 101 c could be optionally omitted or included in a memory unit within CPU 101 b (not shown).

Although the exemplary environment described herein employs ROM 101 c and RAM 101 e, it should be appreciated by those skilled in the art that other types of computer readable media which can store data that is accessible by a module 101, such as, but not limited to, memory cards, subscriber identity module (SIM) cards, local miniaturized hard disks, and the like, may also be used in the exemplary operating environment without departing from the scope of the invention. The memory and associated hardware illustrated in FIG. 1b provide nonvolatile storage of computer-executable instructions, data structures, program modules, module program 101 i, and other data for computer or module 101. Note the module 101 may include a physical data connection at the physical interface 101 a such as, but not limited to, a miniaturized universal serial bus adapter 101 v (illustrated in FIG. 1c), firewire, optical, or other another port.

The computer executable instructions such as, but not limited to, module program 101 i, network application 101 x, eUICC 107, operating system 101 h, or device driver 101 g can be initially loaded into memory such as, but not limited to, ROM 101 c or RAM 101 e through the physical interface 101 a before module 101 is given to an end user, shipped by a manufacturer to a distribution channel, or installed by a technician. In addition, the computer executable instructions such as, but not limited to, module program 101 i, network application 101 x, operating system 101 h or device driver 101 g could be transferred wirelessly to module 101. In either case (wired or wireless transfer of computer executable instructions), the computer executable instructions such as module program 101 i, network application 101 x, operating system 101 h, or device driver 101 g could be stored remotely on a disk drive, solid state drive, or optical disk (external drives not shown).

A number of program modules may be stored in RAM 101 e, ROM 101 c, or possibly within CPU 101 b, including an operating system 101 h, device driver 101 g, an http client (not shown), a DNS client, and related software. Further, the module program 101 i and/or network application 101 x can perform the various actions described in the present invention for the module 101 through instructions the module program 101 i and/or network application 101 x provide to the CPU 101 b. A user may enter commands and information into module 101 through an optional user interface 101 j, such as a keypad, keyboard (possibly miniaturized for a mobile phone form-factor), and a pointing device. Pointing devices may include a trackball, an electronic pen, or a touch screen.

The module 101, comprising a computer, may operate in a networked environment using logical connections to one or more remote computers, such as the server 105 illustrated in FIG. 1a. Server 105 can also function as a general purpose server to provide files, programs, disk storage, remote memory, and other resources to module 101 usually through a networked connection. Additional remote computers with which module 101 communicates may include another module 101 or mobile device, an M2M node within a capillary network, a personal computer, other servers, a client, a router, a network PC, a peer device, a base station 103, or other common network node. It will be appreciated that the network connections shown throughout the present invention are exemplary and other means of establishing a wireless or wired communications link may be used between mobile devices, computers, servers, corresponding nodes, and similar computers. Although a single module program 101 i is depicted in FIG. 1b, module 101 could include a plurality of module programs 101 i.

The module program 101 i, eUICC 107, and network application 101 x operating within module 101 illustrated in FIG. 1b can provide computer executable instructions to hardware such as CPU 101 b through a system bus 101 d in order for a module 101 to (i) connect with a wireless network 102, (ii) authenticate with a mobile network operator 104 associated with the wireless network 102, and (iii) send or receive packets with a server 105 or a server associated with an eUICC subscription manager 109. The module program 101 i and/or network application 101 x can enable the module 101 or eUICC 107 to transmit or send data from the eUICC 107 or module 101. The eUICC 107 or module 101 can send data by recording data in memory such as RAM 101 e, where the data can include cryptographic data such as a RAND and RES values, a destination IP:port number, a packet or packet header value, an

encryption or ciphering algorithm and key, a digital signature algorithm and key, etc. The data recorded in RAM 101 e can be subsequently read by the operating system 101 h or the device driver 101 g. The operating system 101 h or the device driver 101 g can write the data to a physical interface 101 a using a system bus 101 d in order to use a physical interface 101 a to send data to the wireless network 102 and IP network 111 using a radio 101 z (shown in FIG. 1c). Alternatively, the module program 101 i and/or network application 101 x can write the data directly to the physical interface 101 a using the system bus 101 d.

The module program 101 i, eUICC 107, network application 101 x, and/or operating system 101 h can include steps to process the data recorded in memory such as, but not limited to, encrypting data, selecting a destination address, or decrypting ciphertext data. The data recorded in memory could also include an eUICC profile 107 c or eUICC profile 107 d, as described in FIG. 1a above and FIG. 2a below. The eUICC profiles 107 d can include instructions and data for connecting with wireless network 102, including network parameters and network access credentials. The module 101 can use the physical interface 101 a such as, but not limited to, a radio to transmit or send the data associated with a profile 107 d to a base station 103. For those skilled in the art, other steps are possible as well for a module program 101 i or operating system 101 h to communicate with a wireless network 102 using data associated with an UICC (where an eUICC 107 records data normally associated with a physical UICC) without departing from the scope of the present invention.

Conversely, in order for module 101, network application 101 x, or eUICC 107 to receive a packet or message from MNO 104 or wireless network 102, the physical interface 101 a can use a radio to receive data from a base station 103. The received data can include information from MNO 104 and may comprise a datagram, a source IP:port number, a packet or header value, an instruction for module 101, an acknowledgement to a packet that module 101 sent, a digital signature, and/or encrypted data. The received data can also include radio resource control (RRC) messages, and related layer 1 and layer 2 access and control messages for module 101 to access the wireless network 102. The operating system 101 h or device driver 101 g can use a system bus 101 d and CPU 101 b to record the received data in memory such as RAM 101 e, and the module program 101 i or operating system 101 h may access the memory in order to process the received data and determine the next step for the module 101 after receiving the data. The steps within this paragraph may also describe the steps a module program 101 i, eUICC 107, or network application 101 x can perform in order to receive a message from wireless network 102 that includes a RAND value. For those skilled in the art, other steps are possible as well for a module program 101 i, network application 101 x, module 101, and/or eUICC 107 to receive a message from a mobile network operator 104 or wireless network 102 within the scope of the present invention.

Module program 101 i can include an eUICC 107, which can provide the functionality or CPU 101 b instructions for module 101 to access data normally within a physical UICC, such as network parameters and network access credentials. An eUICC 107 as illustrated in FIG. 1a and FIG. 1b can be implemented within module 101 in several different ways, including (i) as depicted in FIG. 1b a module program 101 i stored in RAM 101 e during operation, but also recorded in a nonvolatile memory, such as, but not limited to, either flash memory 101 w (described in FIG. 1c) or ROM 101 c at other times than normal operation (such as during periods of power off), (ii) firmware within CPU 101 b or another specialized processing unit within module 101, (iii) an "eUICC supporting" physical UICC 108 within module 101 that contains the eUICC 107, or (iv) a specialized circuit within a surface mount package that is soldered directly onto a circuit board of the module 101, including an 8-lead small outline non-leaded (SON-8) package. For the embodiment where an eUICC 107 comprises a module program 101 i, the eUICC 107 could be loaded and installed within nonvolatile memory 101 w in module 101 using the steps and procedures described for a module program 101 i in FIG. 1b. Other possibilities exist as well for the physical implementation of an eUICC 107 within a module 101 without departing from the scope of the present invention. An eUICC 107 may also be referred to as an "electronic UICC", an "electronic SIM" (eSIM), or an "embedded SIM" (also eSIM).

For embodiments where an eUICC 107 can be loaded into a RAM 101 e or flash 101 w memory, a CPU 101 b could designate the RAM 101 e or flash 101 w memory containing the instructions or data for an eUICC 107 to be a protected memory. When (i) loaded with appropriate data (such as, but not limited to a eUICC profile 107 d described in FIG. 2a below), and (ii) a profile for a MNO 104 is selected and activated, then an eUICC 107 can provide the equivalent functionality of a physical UICC. The eUICC 107, using an activated eUICC profile 107 d, can provide the module 101 with (i) network access credentials 202 and 203, and (ii) network parameters 201 in order to connect with wireless network 102. The eUICC 107, using an activated eUICC profile 107 d, can record a first key K 203 (described in FIGS. 2a and 3 below) and also a first network module identity 202. The eUICC 107 can support standard steps by module 101 for network authentication contemplated in 3GPP TS 33.401 V12.9.0 and related standards, including inputting a RAND value into the eUICC 107 and outputting a RES value.

Moreover, those skilled in the art will appreciate that the present invention may be implemented in other computer system configurations, including handheld devices, netbooks, portable computers, multiprocessor systems, microprocessor based or programmable consumer electronics, network personal computers, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments, where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices. In addition, the terms "mobile node", "mobile station", "mobile device", "M2M module", "M2M device", "networked sensor", "industrial controller", or "user equipment" can also refer to module 101 or its functional capabilities. Other possibilities exist as well for the configuration or combination of components illustrated in FIG. 1b without departing from the scope of the present invention.

FIG. 1c

FIG. 1c is a graphical illustration of components within a module, in accordance with exemplary embodiments. FIG. 1c is illustrated to show a combination of components useful for leveraging the efficient and secure communication techniques described in the present invention. In addition to the components illustrated in FIG. 1b above, module 101 can include a eUICC 107, a battery 101 k, a MNO public key 502, a wireless module private key 112 a, a connection to an actuator 101 y, a USB interface 101 v, a CPU wake controller 101 u, a flash memory 101 w, a symmetric key 127, a random number generator 128, cryptographic algorithms 141, a radio 101 z, and other components illustrated in FIG. 1c. Not all of the components illustrated in FIG. 1c are required for many exemplary embodiments, and some of the components illustrated in FIG. 1c may also be optionally omitted in some exemplary embodiments.

The CPU 101 b can comprise a general purpose processor appropriate for the low power consumption requirements of a module 101, and may also function as a microcontroller. CPU 101 b could be a processor with an ARM® core, or possibly an ATOM® core or processors, and other possibilities exist

as well. The CPU 101 b can include registers, a cache memory, and arithmetic logic units. Clock 160 can comprise a crystal oscillator generating sine or square wave outputs at a frequency to drive a system bus 101 d, CPU 101 b, and RAM 101 e, in addition to other functionality. In exemplary embodiments, clock 160 can comprise a temperature-compensated crystal oscillator (TCXO), a voltage-controlled crystal oscillator (VCXO), or a voltage-controlled temperature-compensated crystal oscillator (VCTCXO), and other possibilities exist as well. Clock 160 could include circuits and logic to keep time while module 101 is both in an active state and a dormant state.

Sensor 101 f could be a device to collect environmental data or data regarding (i) a monitored unit for M2M applications or (ii) user 113 for applications where module 101 comprises a mobile phone and user 113 is an individual person such as a mobile phone subscriber. Sensor 101 f could collect data such as, but not limited to, temperature, humidity, pressure, visible light levels, radiation, shock and/or vibration, voltage, current, weight, pH levels, orientation/motion, or the presence of specific chemicals. Sensor 101 f could also be a microphone. Sensor 101 f could be a magnetic strip reader for credit cards and similar cards, or an antenna for either near-field RF communications, such as, but not limited to, reading an RF identity tag. An antenna for a sensor 101 f could also collect longer-range RF signals, such as, but not limited to, reading long-range radio frequency identity tags. Sensor 101 f could also collect biometric data such as, but not limited to, heart rate, glucose levels, body temperature, or other health measurements for a user 113. The sensor 101 f can provide data to the CPU 101 b in the form of analog or digital data, which can be communicated via a system bus 101 d or physical interface 101 a and other electrical interfaces are possible as well. A sensor measurement can comprise the analog or digital data collected by CPU 101 b from sensor 101 f.

A sensor measurement from sensor 101 f can include processing of the analog or digital data input CPU 101 b by sensor 101 f, such as, but not limited to, averaging over time, using mathematic formulas to convert the raw data from sensor 101 f into a usable form. Module 101 may also collect sensor data or sensor values using a sensor 101 f and CPU 101 b, where the data or values are derived from electrical signals output by a sensor 101 f. A sensor measurement can comprise the sensor data or sensor values. If module 101 comprises a "point of presence" payment terminal, then a sensor measurement could comprise data read from a payment card. As contemplated herein, the terms "sensor measurement" and "sensor data" can be used interchangeably, and can also be considered functionally equivalent. Although a single sensor 101 f is shown in FIG. 1c, a module 101 could include multiple sensors. Each of the multiple sensors 101 f could include a sensor identity 151, which could comprise a number or string to identify the sensor 101 f. A sensor 101 f could be external to module 101, and also a plurality of sensors 101 f may be used and they also can connect to module 101 when module 101 uses radio 101 z as a base station for a WiFi network.

Actuator 101 y could be a device to control a parameter or state for a monitored unit in M2M applications for module 101, such as, but not limited to, changing a voltage or current, activating a switch or relay, turning on or off a microphone or speaker, activating or deactivating a light, and other examples are well known in the art. Actuator 101 y could also be a speaker. Actuator 101 y could be controlled by module 101 via a digital or analog output from CPU 101 b, which could also be transmitted or sent via system bus 101 d or a physical interface 101 a. Although actuator 101 y is illustrated as external to wireless module 101 in FIG. 1c, actuator 101 y could also be internal to module 101, and module 101 could include multiple actuators 101 y. A module 101 could include multiple actuators 101 y each with an actuator identity 152. Sensors and actuators are well known to those of ordinary skill in the art, and thus are not described in additional detail herein.

Module 101 can include a Universal Serial Bus (USB) interface 101 v. In accordance with an exemplary embodiment module 101 can comprise a wireless module and include a radio 101 z. Note that the use of a radio 101 z is not required for module 101, which could also obtain a connection to the IP Network 111 via a wired line such as Ethernet. Although not illustrated, radio 101 z could include antennas for reception and transmission of RF signals, and even multiple antennas could be used. Although a single radio 101 z is illustrated in module 101, module 101 could also contain multiple radios 101 z. Radio 101 z can support wireless LAN standards such as, but not limited to, WiFi, Bluetooth, and Zigbee, or similar wireless LAN standards. Note that module 101 may also operate as a base station in a wireless LAN, such as, but not limited to, an 802.11 base station. When module 101 operates a wireless LAN, radio 101 z can function as either a client/node and/or a base station 103 to support communication from other wireless nodes in physical proximity, such as, but not limited to, other nodes within an exemplary 50 meters. The other wireless nodes could comprise a sensor 101 f and/or actuator 101 y, and in this case a sensor could be referred to as a "networked sensor" and an actuator could be referred to as a "networked actuator".

In accordance with exemplary embodiments module 101 can store module private key 112 a, MNO public key 502, and module identity 110, and a symmetric key 127 in memory/RAM 101 e during operation, such as when CPU 101 b is active and the module 101 is connected to a network such as a wireless network 102 during data transmissions. Module private key 112 a preferably is recorded in nonvolatile memory such as, but not limited to, flash memory 101 w, so that module 101 has access to its private key 112 a after the private key has been derived or loaded, including times when a battery 101 k has been fully drained or removed from module 101 (if module 101 does not utilize a persistent power source such as land-line power). Symmetric key 127 can be a secure, shared private key for use with symmetric encryption or symmetric ciphering algorithms 211 (in FIG. 2c below). Symmetric key 127 may also include an expiration time 133, such that symmetric key 127 may only be used by module 101 and/or eUICC 107 during a limited period of time, such as symmetric key 127 remaining only valid for a day, or a week, or during a session (where the session comprises multiple messages and/or responses between a module 101 and a wireless network 102), etc.

Module identity 110 is preferably a unique identifier of module 101, and could comprise a number or string such as, but not limited to, a serial number, an international mobile subscriber identity number (IMSI), international mobile equipment identity (IMEI), or an Ethernet media access control (MAC) address. According to an exemplary embodiment, module identity 110 can also comprise a serial number or string that is written into hardware of module 101 upon manufacturing or distribution of module 101 (also depicted and described in connection with a step 511 in FIG. 5b below). In this case, module identity 110 could be recorded in a read only memory 101 c, where read only memory 101 c could not be easily erased or otherwise tampered with. Read only memory 101 c could also comprise a protected memory and the address for accessing the module identity 101 within the ROM 101 c could comprise a protected address.

A protected address can comprise an address accessible to a CPU 101 b and readable by CPU 101 b where the data within the protected address is not modified, changed, or updated by a CPU 101 b under normal operating conditions. Also note that the protected address can comprise one form of a nonvolatile memory, where a memory records data. In exemplary embodiments module identity 110 may preferably be permanently or persistently associated with the physical hardware of module 101, which can be helpful for the security procedures contemplated herein. Module identity 110 can function as a basic identifier for services from mobile network operator 104, eUICC subscription manager 109, wireless network 102, M2M service

provider **115**, or server **105** in order to properly identify module **101** among a plurality of modules. Module private key **112 a** and an associated module public key **112 b** could be unique to module **101** and uniquely associated with module identity **110**, according to a preferred embodiment.

MNO public key **502** in module **101** could be obtained from downloading the key over the IP Network **111**, or optionally also written into nonvolatile memory of module **101** upon manufacture or distribution. MNO public key **502** could be obtained using a domain name or Internet address that is recorded in nonvolatile memory upon the configuration of module **101**, such as, but not limited to, during installation or distribution, and module **101** could fetch the MNO public key **502** upon connecting to a wireless network **102** or other connection to the IP Network **111**. Additional elements besides those depicted in FIG. 1c could also be recorded in volatile memory **101 e**, which could comprise a RAM **101 e**. For example, cryptographic algorithms **141** could also be recorded in RAM **101 e** as well. Note that values and related data can also be recorded in both RAM **101 e** and nonvolatile memory **101 w** at the same time, such that data in nonvolatile memory **101 w** allows module **101** to access the data after a shutdown state, but moving the same data into RAM **101 e** during an active state allows module **101** to more quickly perform operations using a CPU **101 b**. Other possibilities exist as well for the storage location of various values and data elements illustrated in FIG. 1c without departing from the scope of the present invention.

Module **101** may also contain cryptographic algorithms **141**, which may comprise a suite of algorithms or subroutines that can be utilized for (i) deriving a pair of keys comprising a public key and a private key, (ii) encrypting data using public keys, (iii) decrypting data using private keys, (iv) processing secure hash signatures using private keys, and (v) verifying secure hash signatures using public keys, and related software, firmware, or subroutines for implementing a cryptographic system, including symmetric ciphering algorithms. Cryptographic algorithms **141** could utilize publicly available software libraries within tools such as, but not limited to, OpenSSL maintained by The OpenSSL Project (<http://www.openssl.org/>), libgcrypt maintained by The Free Software Foundation (<http://www.gnu.org/software/libgcrypt/>), and similar libraries such as, but not limited to, libmccrypt and Crypto++. Note that cryptographic algorithms **141** could also use proprietary cryptographic libraries as well. In addition to implementing asymmetric encryption/ciphering, such as, but not limited to, used with RSA and ECC cryptography, cryptographic algorithms **141** can provide symmetric ciphering where a shared private key is utilized to both encrypt and decrypt, such as, but not limited to, with the Advanced Encryption Standard (AES) cipher suite.

As illustrated in FIG. 1c, module **101** may also contain a random number generator **128**. Random number generator **128** may contain a seed **128 b**. The creation of random numbers with a high degree of entropy may be important the use of cryptographic algorithms **141**. A plurality of the data as a source for a random number seed **128 b** could be appended together into a "module random seed file" with a combined series or list of states (i.e. a plurality of sensor **101 f** measurements, radio **101 z** measurements, clock **160** times or values, memory **101 e** or memory **101 w** states, operating system **101 h** states, actuator **101 y** states, and/or hardware **101 a** or **101 d** states). Note that values or data for each of the elements listed in the previous sentence could be utilized in a "module random seed file" instead of or in addition to a state. The use of a "module random seed file" with a random number generator **128** is also depicted and described in connection with FIG. 1d of U.S. patent application Ser. No. 14/084,141, filed Nov. 19, 2013 in the name of John Nix, which is hereby incorporated by reference in its entirety.

FIG. 1d

FIG. 1d is a graphical illustration for authenticating with a wireless network using a physical UICC, in accordance with conventional technology. FIG. 1d illustrates the components and interfaces for using a physical UICC in order to a module **101** conduct an authentication with a wireless network **102** according to wireless WAN standards which use a pre-shared secret key K recorded in the physical UICC **116**. The wireless network could be an LTE, LTE Advanced, or a 3G network, and also based on related standards. With a 3G network, the pre-shared secret key K is also known as "Ki". The module **101** can include a network application **101 x**, a UICC driver **114**, and a physical interface supporting the ISO/IEC 7816-3 electrical standards, such as the third edition published on Nov. 1, 2006. The physical UICC **116** can be a smart card in the form factor of a mini-SIM, micro-SIM, or nano-SIM, connected to the physical interface such as ISO/IEC 7816-3 and related electrical standards. The physical interface can include six electrical contacts known as C1 through C6, where C1 provides a power supply to the physical UICC **116**, C2 provides a reset signal input, C3 provides a clock signal input, etc. The network application **101 x** can comprise software or firmware for the module **101** to communicate with the wireless network **102** using the standards that include layer 2 messages between module **101** and wireless network **102** such as, but not limited to, radio resource control (RRC) messages, security mode commands, ciphering, and authentication. The network application **101 x** can communicate with a radio **101 z** (described in FIG. 1c) using the system bus **101 d**.

A network application **101 x** in a FIG. 1d can be similar or equivalent to a network application **101 x** depicted and described in connection with FIG. 1b. The UICC driver **114** can comprise a driver within a set of drivers **101 g** within module **101**, where drivers **101 g** are also depicted and described in connection with FIG. 1b. A physical UICC **116** can support other and additional functionality for a module **101** than the authentication functionality depicted in FIG. 1b, such as, but not limited to, (i) recording a set of network parameters equivalent to a set of network parameters **201** in FIG. 2a below in order to module **101** to identify and select a wireless network **102**, (ii) recording an address book with a list of phone numbers for user **113**, (iii) recording a list of recent SMS messages and telephone numbers dialed, and/or (iv) recording and implementing a personal identification number (PIN) in order for a user **113** to authenticate and access the module **101** with the UICC **116**, and other functionality of a physical UICC **116** is possible as well. The physical UICC **116** can also include (i) an IP Multimedia Services Identity Module (ISIM) application and data and/or a (ii) Universal Subscriber Identity Module (USIM) application for the module **101** to utilize when communicating with the wireless network **102**.

After power-up of the module **101** from a powered off state, the module **101** can use the UICC driver **114** to read data from the physical UICC **116** such as a set of network parameters **203** (depicted in FIG. 2a below) as well as an IMSI or equivalent value as a network module identity. The set of network parameters **203** or IMSI in a physical UICC **116** may not be encrypted (or associated with an eUICC profile **107 d**) and the set of network parameters can be directly read by the UICC driver **114**. The module **101** can use the set of network parameters to tune a radio **101 z** to particular frequencies for the wireless network **102** and search for a beacon signal from a base station **103**. The beacon signal can include codes such as a mobile country code (MCC) and mobile network code (MNC) that can match values in either the network parameters or IMSI. Upon finding and selecting base station **103**, the module **101** can send a random access channel (RACH) message and subsequently an identity value recorded in the physical UICC **116** such as an IMSI, temporary mobile subscriber identity (TMSI), a globally unique temporary identity (GTUI), or a similar value to identify the module **101** using the physical UICC **116** with the wireless network **102**.

In order to authenticate a module **101** with the wireless network **102**, the wireless network **102** can record a set of authentication tokens or vectors associated with a network identity sent by the module **101**, such as a GTUI value. An authentication vector **117** for the module's **101** network identity can

comprise a vector or set of values that includes a random number (RAND) 118, response (RES) 119, a network authentication token (AUTN), and a sequence number. The value AUTN and sequence number is not shown in FIG. 1d and subsequent figures such as FIG. 1e and FIG. 3, but the value AUTN and sequence number can be used by module 101 with a physical UICC 116 or eUICC 107 in order to authenticate the wireless network 102. The sequence number can prevent replay attacks and the AUTN value can comprise a digital signature or message digest value the physical UICC 116 or eUICC 107 can also calculate using the RAND 118 value in order for the module 101 to authenticate the wireless network 102. The values for the authentication vector 117 that includes a RAND 118 and a RES 119 can be calculated by a home subscriber server (HSS) for the mobile network operator 104 associated with the wireless network 102 and provided by the mobile network operator 104 to servers associated with the wireless network 102. An exemplary format for the use of a RAND 118 with a response RES 119 is described in ETSI standard TR 131 900 v.10.0.0 and related documents. Other possibilities exist as well for the format, structure, and data elements within an authentication vector 117 without departing from the scope of the present invention.

In order to conduct an authentication of module 101, after receiving a RACH message and the network module identity such as an IMSI, TMSI, or GTUI value, the wireless network 102 can send a RAND 118 from the authentication vector 117. The module 101 can receive the RAND 118 value using the network application 101 x and the radio 101 z. The network application 101 x can send the RAND 118 value to the UICC driver 114, and the UICC driver 114 can send the RAND 118 value through the physical interface such as ISO/IEC 7816-3 to the physical UICC 116. After receiving the exemplary RAND 118 message, in order to conduct an authentication, module 101 using a physical UICC 116 could take steps to demonstrate to a wireless network 102 that the physical UICC 106 records the same pre-shared secret key K for the network module identity as recorded by a mobile network operator 104 associated with the wireless network 102. Physical UICC 116 can properly respond to the RAND 118 using message digest algorithms by calculating a secure hash value RES 119 using the RAND 118 and the recorded secret key K. The physical UICC 116 could use algorithms specified in ETSI TS 135 205-209, as well as subsequent and related standards, in order for the physical UICC 116 to calculate a secure hash value such as a RES 119. The calculation and processing of a RES 119 using a RAND 118 and a secret key K is also depicted and described in connection with steps 306 and 311 of FIG. 3. Other possibilities exist as well for a physical UICC 116 or an eUICC 107 to calculate a RES 119 value using a RAND 118 and a secret key K without departing from the scope of the present invention.

After the calculation of a RES 119 value in response to the RAND 118, the physical UICC 116 can send the RES 119 to the UICC driver 114 through the physical interface such as ISO/IEC 7816-3. The device driver 114 can send the RES 119 value to the network application 101 x and the network application 101 x can send the RES 119 value to the wireless network 102 using a radio 101 z and the base station 103. The wireless network 102 can take steps to compare the received RES 119 with a recorded RES 119 value in the authentication vector 117. If the received RES 119 matches the recorded RES 119 in the authentication vector 117 then the module 101 with the physical UICC 116 can be considered authenticated. The authentication of module 101 by wireless network 102 is also depicted and described in connection with a step 308 a of FIG. 3. After successful authentication, the module 101 and wireless network 102 can then take subsequent steps for a module 101 to have access to the IP network 111 including the public Internet, as well as configuring services such as voice and SMS.

FIG. 1e

FIG. 1e is a graphical illustration for authenticating with a wireless network using an eUICC, in accordance with exemplary embodiments. A module 101 with an eUICC 107 can perform the equivalent steps for authentication with a wireless network 102, such that a module 101 can use an eUICC 107 instead of a physical UICC 116. The wireless network 102 can perform the same steps as (i) recording an authentication vector 117 from a mobile network operator 104 associated with the wireless network 102, (ii) receiving a RACH message and a network module identity such as a GTUI or TMSI from the module 101, (iii) sending values from the authentication vector 117 including a RAND 118, and (iv) receiving a RES 119 and comparing the received RES 119 with a recorded RES 119 in the authentication vector 117 in order to authenticate the module 101 using an eUICC 107 instead of a physical UICC 116. In other words, the use of an eUICC 107 by module 101 can be transparent to a wireless network 102, such that a module 101 with an eUICC 107 instead of a physical UICC 116 can be fully "backward compatible" with standards, software, and infrastructure deployed on a wireless network 102.

A module 101 in FIG. 1e can include a network application 101 x, an eUICC driver 129, an eUICC 107, and an operating system 101 h. The network application 101 x can be equivalent or similar to a network application 101 x depicted and described in connection with FIG. 1d and FIG. 1b above. The use of an eUICC 107 instead of a physical UICC 116 within module 101 can also be transparent to network application 101 x, via the use of eUICC driver 129. In other words, in exemplary embodiments, the same or equivalent network application 101 x can be used for either (i) a module 101 with a physical UICC 116 or (ii) a module 101 with an eUICC 107, since the eUICC driver 129 can perform the identical input and output functions as a UICC driver 114 when communicating with the network application 101 x. The use of an eUICC driver 129 is also depicted and described in connection with FIG. 1b above. The eUICC driver 129 can communicate with the network application 101 x using the operating system 101 h. The internal communication between network application 101 x and eUICC driver 129 using an operating system 101 h could comprise sharing memory 101 e, such that network application 101 x writes messages such as, but not limited to, an exemplary RAND 118 value into the shared memory 101 e and eUICC driver 129 reads the values from the shared memory 101 e. In another embodiment, the internal communication between network application 101 x and eUICC driver 129 using an operating system 101 h could comprise using loopback UDP ports within operating system 101 h, such that network application 101 x sends a UDP datagram with the RAND 118 value using a first UDP loopback port, and the eUICC driver 129 receives the UDP datagram with the RAND 118 value using a second UDP loopback port. Similar steps could be taken as well for an eUICC driver 129 to send data such as a RES 119 to the network application 101 x using the operating system 101 h.

As illustrated in FIG. 1e, eUICC driver 129 can also communicate with the eUICC 107 using the operating system 101 h. Two differences between conventional technology illustrated in FIG. 1d and the exemplary embodiment illustrated in FIG. 1e include (i) the eUICC driver 129 communicates with the eUICC 107 using operating system 101 h instead of a physical interface such as ISO/IEC 7816-3 and related electrical standards, and (ii) the eUICC 107 can operate as a separate program or application within memory 101 e or memory 101 w instead of a physically separate application operating on a physical UICC 116. The eUICC driver 129 can communicate with the eUICC 107 using the equivalent steps and procedures for a network application 101 x to communicate with an eUICC driver 129 described in the paragraph above, including using shared memory or sending UDP loopback messages on internal UDP loopback ports. Other possibilities for the communication between eUICC driver 129 and eUICC 107 exist as well without departing from the scope of the present invention. In addition, although eUICC driver 129 and eUICC 107 are depicted in FIG. 1e and FIG. 1b as separate elements, programs,

and/or processes for a module **101**, the eUICC driver **129** could be optionally combined with an eUICC **107** such that the network application **101 x** can communicate directly with the eUICC **107** using the operating system **101 h**.

The eUICC **107** can include an eUICC profile **107 d** which can contain the same information used by a physical UICC **116** in FIG. 1d above, including a set of network parameters, a network module identity, and a key K. In other words, the data recorded in a eUICC **107** in the form of a profile **107 d** can allow and support the eUICC **107** in FIG. 1e to operate in an equivalent manner as a physical UICC in FIG. 1d for the authentication steps illustrated in FIG. 1d and FIG. 1e. Although not illustrated in FIG. 1e, the eUICC **107** could also perform the similar or equivalent functions of a physical UICC including (i) recording a set of network parameters equivalent to a set of network parameters **201** in FIG. 2a below in order to module **101** to identify and select a wireless network **102**, (ii) recording an address book with a list of phone numbers for user **113**, (iii) recording a list of recent SMS messages and telephone numbers dialed, and/or (iv) recording and implementing a personal identification number (PIN) in order for a user **113** to authenticate and access the module **101** with the eUICC **107**. Other functionality of an eUICC **107** for a module **101** is possible as well without departing from the scope of the present invention.

As illustrated in FIG. 1e, the network application **101 x** in module **101** can receive a RAND **118** value from wireless network **102** in order to authenticate the module **101**. The network application **101 x** can send the RAND **118** value to the eUICC driver **129**. The eUICC **107** can read a RAND **118** value from the network application **101 x** using the eUICC driver **129**. After receiving the exemplary RAND **118** message, in order to conduct an authentication, module **101** using an eUICC **107** could take steps to demonstrate to a wireless network **102** that the module **101** records the same pre-shared secret key K for the network module identity as recorded by a mobile network operator **104** associated with the wireless network **102**. eUICC **107** can properly respond to the RAND **118** using message digest algorithms by calculating a secure hash value RES **119** using the RAND **118** and the recorded secret key K from the profile **107 d**. The eUICC **107** could use algorithms specified in ETSI TS 135 205-209, as well as subsequent and related standards, in order for the eUICC **107** to calculate a secure hash value such as a RES **119**. The calculation and processing of a RES **119** using a RAND **118** and a secret key K for an eUICC **107** is also depicted and described in connection with steps **306** and **311** of FIG. 3. Other possibilities exist as well for an eUICC **107** to calculate a RES **119** value using a RAND **118** and a secret key K, without departing from the scope of the present invention. As illustrated in FIG. 1e, the eUICC **107** can send the RES **119** to the eUICC driver **129**, and the eUICC driver **129** can send the RES **119** to the network application **101 x**. The network application **101 x** can then send the RES **119** to the wireless network **102**, and the wireless network **102** could perform a step **308 a** as depicted and described in connection with FIG. 3 in order to authenticate the module **101** using the eUICC **107** and profile **107 d**.

FIG. 1f

FIG. 1f is a graphical illustration of an exemplary system that includes a module, a mobile network operator, and an eUICC in accordance with exemplary embodiments. System **199** in FIG. 1f can include a mobile network operator **104** and a module **101**. The mobile network operator **104** can communicate with the module **101** using a wireless network **102**, and the wireless network **102** could comprise the radio access portion of the mobile network operator **104**, such as a collection of base stations **103** using licensed radio spectrum such as, but not limited to, the 700 Mhz band for LTE, and other possibilities exist as well for the wireless network **102**. The mobile network operator **104** can include a server **105** with an IP address **106 a**. The server **105** with MNO **104** in FIG. 1f can comprise a Mobility Management Entity (MME) in LTE networks, or equivalent functionality to receive authentication requests from modules **101** with other wireless wide-area networking technology. The MME can support radio bearer activation/deactivation processes for the module **101** and authenticating the module **101** by recording an authentication vector **117**, where the authentication vector **117** can be received from an HSS.

The server **105** can comprise a server as depicted and described in connection with server **105** in FIG. 1k and FIG. 1m of U.S. patent application Ser. No. 14/084,141, filed Nov. 19, 2013 in the name of John Nix, which is hereby incorporated by reference in its entirety. The IP address **106 a** can include a subnet prefix **106 d** and an interface identifier **106 e**. The IP address **106 a** can comprise an IPv6 address, where the subnet prefix **106 d** comprises the first 64 bits of a 128 bit IPv6 address, and the interface identifier **106 e** can comprise the last 64 bits of a 128 bit IPv6 address as shown in FIG. 1f. Other nodes connected to the wireless network **102** can also include IPv6 addresses with different values for the subnet prefix **106 d** and the interface identifier **106 e**. A module **101** can include both a network application **101 x** and an eUICC **107**, where a network application **101 x** is depicted and described in connection with FIG. 1b and an eUICC **107** is depicted and described in connection with FIG. 1a, FIG. 1b, FIG. 1c, and FIG. 1e.

In an exemplary embodiment, different elements within module **101** can be associated with different IP addresses. The network application **101 x** can be associated with an IP address **106 b** and the eUICC **107** can be associated with an IP address **106 c**. The wireless network **102** could assign the module **101** the subnet prefix **106 d** used by module **101** with wireless network **102**, and an operating system **101 h** could assign the interface identifier **106 e** used by the network application **101 x** and the eUICC **107**. Other possibilities exist as well for the source of IP addresses in a system **199**, but an end result can comprise the eUICC **107** having a unique IPv6 address **106 c** such that a server **105** such as an MME can communicate with the eUICC **107** directly by sending a packet with a RAND **118** value from server **105** address **106 a** to eUICC **107** address **106 c**.

Although not illustrated in FIG. 1f, the exemplary IP addresses for server **105** and eUICC **107** can be associated with port numbers, such that server **105** can use a first port number with the IP address **106 a** when sending a RAND **118**, and eUICC **107** could use a second port number with the IP address **106 c** when receiving the RAND **118**. Server **105** can use a third port number when receiving a RES **119**, and eUICC **107** could use a fourth port number when sending the RES **119**. The first and third port numbers could be the same value or number, and the second and fourth port numbers could be the same value or number. In an exemplary embodiment, the RAND **118** and RES **119** in system **199** can be formatted according to the UDP Lite protocol, as specified in IETF RFC 3828, which is also incorporated by reference herein. The term "UDP Lite" described in the present invention may also refer to any connectionless protocol supported on IP Network **111** and wireless network **102** where checksums may be partially disabled, thereby supporting the transfer of bit errors within a datagram.

As illustrated in FIG. 1f, an eUICC **107** operating in module **101** could be an application with a unique IPv6 address **106 c**, and the network application **101 x** utilize a different IPv6 address **106 b**. The two IP addresses could be on the same subnet **106 d** used by a module **101**, and the network application **101 x** could communicate with the eUICC **107** locally within module **101** using the two different IPv6 addresses **106 b** and **106 c**. The network application **101 x** could communicate with the eUICC **107** locally for exemplary "other data" depicted in FIG. 1f, which could comprise the storing of an address book in the eUICC **107**, reading a set of network parameters by the network application **101 x** from the eUICC **107** with the eUICC profile **107 d**, etc. In an exemplary embodiment, the eUICC **107** could communicate with the mobile network operator **104** for authentication, thus potentially bypassing the network application **101 x** for separate handling of RAND **118** and RES **119** values depicted in FIG. 1e above. The authentication messages comprising a

RAND 118 and a RES 119 could be communicated between the eUICC 107 with IP address 106 c to the mobile network operator 104 with IP address 106 a without the use of a network application 101 x.

The eUICC 107, with an associated IP address 106 c could also communicate with the eUICC subscription manager 109 by sending a packet from IP address 106 c to an IP address of a server associated with the eUICC subscription manager, such as the exemplary data for a step 205 depicted and described in connection with FIG. 2a and FIG. 3 below. Note that the eUICC 107 with the IP address 106 c can communicate with the eUICC subscription manager 109 without the wireless network 102, but rather through an IP network 111. The connectivity for the IP network 111 could be provided by a different wireless network 102 than the wireless network 102 associated with the MNO 104. Although the use of a specific, unique IP address 106 c for eUICC 107 is illustrated in FIG. 1f, an eUICC 107 does not require a separate IP address 106 c in other embodiments, and the eUICC 107 could share an IP address 106 b with a network application 101 x or other processes or elements within module 101.

FIG. 2a

FIG. 2a is a graphical illustration of an exemplary profile for an eUICC, including encrypted data, decryption steps, and decrypted data for the profile, in accordance with exemplary embodiments. Two exemplary forms of an eUICC profile are illustrated in FIG. 2a: an encrypted eUICC profile 107 c and an eUICC profile 107 d. As contemplated herein, an eUICC profile, such as the exemplary eUICC profile 107 c and 107 d, can be similar to profiles for an eUICC contemplated in ETSI specification TS 103 383 v12.2.0 and related standards, but with differences to the currently published standards, as described below. An eUICC profile 107 d can comprise the data from an encrypted eUICC profile 107 c, where (i) a first portion of the data, comprising ciphertext 208 a, has been decrypted, and (ii) a second portion of the encrypted eUICC profile 107 c, comprising ciphertext 208 b remains encrypted. Thus, an encrypted eUICC profile 107 c can include a first portion, or ciphertext 208 a and a second portion, or ciphertext 208 b as depicted in FIG. 2a. As contemplated herein, an encrypted eUICC profile 107 c can be referred to as "profile 107 c", and the eUICC profile 107 d can be referred to as "profile 107 d". Both profile 107 c and profile 107 d can include a profile identity 107 e. Profile identity 107 e can comprise a number or string such that various elements illustrated in FIG. 1a can properly refer to, select, and/or identify a profile 107 c or profile 107 d, including elements such as a mobile network operator 104, eUICC subscription manager 109, module 101, and/or an eUICC 107.

A profile 107 c or profile 107 d in exemplary systems herein, including systems 100, 300, and 500 can comprise several different possible embodiments. The profiles could be recorded in a file or data set, and stored in nonvolatile memory associated with an eUICC 107, such as, but not limited to, a flash memory 101 w. As transferred across a wireless network 102 and/or IP network 111, the encrypted eUICC profile 107 c can be segmented into separate datagrams and transferred using a transport layer protocol such as TCP. An application layer protocol such as transport layer security (TLS) and additional ciphering at the data-link layer could be utilized as well, in addition to sending and receiving the data for a profile 107 c as ciphertext 208 a and 208 b. The exemplary forms for a profile 107 c and 107 d in FIG. 2a can represent data for a file recorded in a module, such as, but not limited to, (i) storing in a volatile memory 101 e when the profiles 107 c or 107 d are being processed or accessed by a CPU 101 b, or (ii) storing in a nonvolatile memory such as flash memory 101 w when the profile 107 c and 107 d are stored long term, including times when a battery 101 k may be removed from module 101.

Note that profile 107 c with at least two distinct portions, comprising ciphertext 208 a and ciphertext 208 b, could be recorded in separate segments or in distinct location within module 101 or with an eUICC subscription manager 109, and the two or multiple portions together can comprise a profile 107 c. In other words, the portions of ciphertext 208 a and 208 b (and other data in a profile 107 c or profile 107 d) can be recorded in different locations while comprising a profile 107 c. Other possibilities exist as well for the structure and recording of the exemplary data for a profile 107 c and 107 d without departing from the scope of the present invention. Although the label "Stored w/Subscription Manager 109" is depicted with an encrypted eUICC profile 107 c, the encrypted eUICC profile 107 c can also be stored as the format depicted in FIG. 2a within a module 101 or an eUICC 107, until at least a step 206 is performed to decrypt the first ciphertext 208 a, as described in this FIG. 2a and FIG. 3 below.

A first portion of profile 107 c can include ciphertext 208 a, where ciphertext 208 a can include a set of network parameters 201, a first network module identity 202, and a first key K 203. Ciphertext 208 a can include these elements in a ciphered string or file, such that a third party would not feasibly be able to read the plaintext within ciphertext 208 a without a key such as eUICC profile key 107 b. Ciphertext 208 a can comprise the set of network parameters 201, the first network module identity 202, and the first key K 203 as plaintext ciphered with a eUICC profile key 107 b, as depicted and described in connection with FIG. 2b below. The set of network parameters 201 could comprise a list of values and settings for a module 101 to utilize in connecting with a mobile network operator 104. The set of network parameters 201 could include a list of numbers or strings for values such as (i) allowed frequencies or frequency bands to scan, (ii) preferred access lists for roaming onto other wireless networks, (iii) criteria for a module 101 to select base stations 103 in idle mode, (iv) support for emergency services, (v) supported languages or character encoding, (vi) codes to search for in beacons broadcast by a wireless network 102, (vii) parameters for a radio 101 z to use when connecting to a wireless network 102, (viii) names or addresses for a server 105 associated with a MNO 104 in order for a module 101 to send data, etc.

A first network module identity 202 within a ciphertext 208 a in profile 107 c can comprise a subscriber identity or related identifier of module 101 when connected to a MNO 104 through a wireless network 102. In an exemplary embodiment, the first network module identity 202 can comprise an international mobile subscriber identity (IMSI), a globally unique temporary identity (GTUI), a media access control (MAC) address, a temporary mobile subscriber identity (TMSI) or a similar number or string to identify a module 101 with wireless network 102. Note that a network module identity such as the first network module identity 202 can be different than a module identity 110, such that a network module identity can be assigned by a mobile network operator 104, while a module identity 110 can be assigned by manufacturer. In other words, a network module identity such as the first network module identity 202 can change over time for a module 101, while the module identity 110 can remain the same. The eUICC identity 107 a can also remain the same value or number while a network module identity changes.

A first key K 203 within a ciphertext 208 a in profile 107 c can comprise a standards-based shared secret key K for use in wireless WAN networks based on ETSI, 3GPP, and related standards. As currently specified in ETSI/3GPP standards for LTE and LTE Advanced networks, the shared secret key K, (i) recorded in a SIM or UICC, and a MNO 104 HSS, and (ii) described in 3GPP TS 33.401 V12.9.0 and related standards, comprises a pseudo-random number with a length of 128 bits. The length of key K for standards-based wireless networks 102 may be extended in the future. The use of shared secret key K for authentication of a module 101, and also for ciphering and data integrity, with a wireless network 102 that implements ETSI and/or 3GPP standards is also defined in the specifications ETSI TS 135 205-209 and related standards. Both the first key K 203 and the second key K 204 can comprise a shared secret key K as described in 3GPP TS 33.401 V12.9.0 FIG. 6.2-1 and related standards. A mobile network operator 104 using the function of an

authentication center, possibly within a home subscriber server (HSS) can generate or process authentication vectors 117 comprising an random number (RAND), an authentication token (AUTN), a response (RES), and a sequence number using the first key K 203 recorded in a eUICC profile 107 c or 107 d for the first network module identity 202. Likewise, authentication vectors 117 can be generated by a HSS and sent to a MME for the second network module identity 209 a with the second key K 204.

In exemplary embodiments, the first key K 203 depicted in FIG. 2a is also depicted and described as operating as a standards-based shared secret key K in FIG. 3 below at a step 306. Using the properties of a standards-based key K, a module 101 or an eUICC 107 can use the first key K 203 and a first random number RAND 118 received to process or calculate a first response RES 119. Step 306 with a first key K 203 can comprise an authentication for a module 101 (comprising a "mobile phone", "mobile station", or "user equipment") within standards such as 3GPP TS 33.401 V12.9.0 and related standards using a shared secret key K. As contemplated herein, the use of the term "random number" can comprise a pseudo-random number with a high degree of information entropy that may not be purely mathematically random, but can be considered a random number and referred to as a random number for the purposes herein.

In an exemplary embodiment, as described in FIG. 2e and step 302 a of FIG. 3 below, the first key K 203 can be optionally recorded in ciphertext 208 a with an additional layer of encryption, such that the first key K 203 is recorded as a ciphertext 208 c within ciphertext 208 a. In other words, upon conversion of ciphertext 208 a into plaintext using a profile deciphering algorithm 206, the first key K 203 can retain an additional layer of encryption as ciphertext 208 c with other data in a profile 107 d that may be plaintext. This optional additional layer of encryption for the first key K 203 is also depicted within the profile 107 d, where ciphertext 208 c optionally remains in profile 107 d after the conversion of ciphertext 208 a into plaintext using a step 206. As described below, the optionally additional layer of encryption for ciphertext 208 c with the first key K 203 can be (i) processed into plaintext first key K 203 (ii) after a subsequent deciphering with an asymmetric ciphering algorithm 219 as illustrated in FIG. 2 e.

Note that the additional layer of encryption for the first key K 203, in the form of using a ciphertext 208 c, can be optionally omitted and the first key K 203 could be plaintext after the conversion of the first portion of profile 107 c as ciphertext 208 a into plaintext in a profile 107 d using a step 206. Thus, the dashed lines around the first key K 203 as a ciphertext 208 c indicate the use of ciphertext 208 c is optional, depending on the security requirements for an MNO 104 when distributing electronically the first key K 203. In another embodiment as described in FIG. 3, the first key K 203 can comprise a null value, such as the value for a key K in order to support emergency services if module 101 has no valid UICC, and in this case the use of additional encryption via ciphertext 208 c can be omitted for a first key K 203. In a related embodiment, the first key K 203 can be omitted entirely from a profile 107 c and profile 107 d, and the eUICC 107 can subsequently use a null value for the first key K 203.

A second portion of profile 107 c can include ciphertext 208 b, where ciphertext 208 b can include a second key K 204 a and a second network module identity 209 a. Ciphertext 208 b can be ciphered with a symmetric key 127, where the ciphering and deciphering of a portion of ciphertext 208 b is depicted and described in connection with FIG. 2c below. In an exemplary embodiment, the second network module identity 209 a can comprise an international mobile subscriber identity (IMSI), a globally unique temporary identity (GTUI), a media access control (MAC) address, or similar number or string to identify a module 101. In exemplary embodiments, the second network module identity 209 a can be a different number or value than the first network module identity 202. Although the second network module identity 209 a is illustrated in FIG. 2a as internal to ciphertext 208 b, the second network module identity 209 a could be external to ciphertext 208 b, such as, but not limited to, the second network module identity 209 a being within a profile 107 c or profile 107 d and external to ciphertext 208 b. In other words, in exemplary embodiments, the second network module identity 209 a may optionally not be ciphered with the symmetric key 127, while the second key K 204 a can be ciphered with the symmetric key 127. As contemplated herein, the term second network identity 209 a comprises an encrypted second network identity 209 a, where the second network identity 209 is the plaintext version of the encrypted second network identity 209 a. Likewise, the term second key K 204 a comprises an encrypted second key K 204 a, where the second key K 204 is the plaintext version of the encrypted second key K 204 a.

In another exemplary embodiment, the second network module identity 209 can comprise the same number or value as the first network module identity 202, or the second network module identity 209 can be optionally omitted. In this case, if (A) the second network module identity 209 comprises the same number or value as the first network module identity 202, or the second network module identity 209 is optionally omitted, then (B) the mobile network operator 104 can preferably support the use of two different shared secret keys K (i.e. first key K 203 and second key K 204) for the same network module identity 202. However, given the current functionality of an HSS and related infrastructure for wireless networks 102, the use of two different network module identities (i.e. the first network module identity 202 and the second network module identity 209) with two different shared secret keys K (i.e. first key K 203 and second key K 204, respectively) may be more compatible or suitable for deployed and operational HSS infrastructure.

A second key K 204 a (as an encrypted form of plaintext second key K 204) within a ciphertext 208 b in profile 107 c can comprise a standards-based shared secret key K for use in wireless WAN networks based on ETSI, 3GPP, and related standards. The use of a second key K 204 a (in an unencrypted form of second key K 204) can be equivalent to a first key k 203, but comprise a different random number. The second key K 204 can comprise a random number that is 128 bits in length in order to support 4G networks such as LTE that are widely deployed in 2013, although the length of either first key K 203 or second key K 204 may be a longer number in the future, such an exemplary 256 bits and other possibilities exist as well for the key length. A second key K 204 can also be used with standards-based authentication with a wireless network 102, where the second key K 204 in FIG. 2a is also depicted and described as operating as a standards-based shared secret key K in FIG. 3 below at a step 311.

The list of exemplary data for encrypted eUICC profile 107 c and an eUICC profile 107 d comprises an exemplary set, and the profiles could also include additional data to the exemplary data illustrated in FIG. 2a. The additional data for a profile 107 c or 107 d could include (i) a set of cryptographic parameters for eUICC 107, (ii) a set of cryptographic algorithms, such as the exemplary cryptographic algorithms described within ETSI TS 135 205-209 and related standards, (iii) a name or address for an eUICC subscription manager 109 associated with the profile 107 c, (iv) a name or address for a server 105 associated with a mobile network operator 104, (v) a digital signature of the profile 107 d processed with a private key from either eUICC subscription manager 109 or MNO 104, (vi) a date or timestamp for processing the profile 107 c or 107 d, (vii) and similar or related values for a module 101 and/or eUICC 107 to utilize the profiles. This exemplary additional data which is not depicted in FIG. 2a could be included within or external to any of ciphertext 208 a and ciphertext 208 b.

Note that the profile identity 107 e may preferably be external to ciphertext 208 a and ciphertext 208 b, in order that module 101 and/or eUICC 107 can take steps to identify a profile 107 c or 107 d. In addition, although a single profile 107 c and profile 107 d are illustrated in FIG. 2a, a module 101 and/or

an eUICC 107 could include a plurality of profiles 107 c and/or 107 d, where each of the plurality of profiles could comprise different data associated with different wireless networks 102. In an exemplary embodiment, more than one profile 107 c or profile 107 d could be associated with the same wireless network 102, such that a mobile network operator 104 can prefer for the same module 101 to utilize different network access credentials over time, such that the same module 101 could use a different key K and a different network module identity with the same wireless network 102 or mobile network operator 104 over time. Different profiles 107 c or 107 d can also be identified by the use of a different profile identity 107 e. Each profile 107 c can be associated with an eUICC profile key 107 b as an encryption key (shown in FIG. 2b below), although multiple profiles 107 c could also share the same eUICC profile key 107 b.

A module 101 can receive a profile 107 c using a step 205. A profile 107 c can be recorded with an eUICC subscription manager 109 before being received by a module 101. As depicted in FIG. 2a, a module 101 can receive the profile 107 c at a step 205 using the IP network 111. The use of a step 205 by a module 101 is depicted and described in connection with FIG. 3 below. The module 101 can receive the profile 107 c using a network that is different than wireless network 102 associated with the network access credentials comprising the first key K 203 and the first network module identity 202. In an exemplary embodiment, module 101 can receive the profile 107 c in a step 205 using an initial wireless network 102, where module 101 connects with and authenticates with the initial wireless network 102 using an initial eUICC profile 107 d different than the eUICC profile 107 d depicted in FIG. 2a. Or, module 101 could receive a profile 107 c using a wireless LAN network or a wired connection via a physical interface 101 a such as a USB interface 101 v. In another exemplary embodiment, module 101 can receive the profile 107 c from a manufacturer, distributor, end user, or technician taking steps to load the profile 107 c into a nonvolatile memory within module 101 or eUICC 107. Upon receipt of a profile 107 c by module 101, the module 101 can record or store the profile 107 c with an eUICC 107.

A module 101 can use an eUICC 107 to decrypt the first portion or ciphertext 208 a in a profile 107 c using a step 206. Before a step 206, a module 101 can receive an eUICC profile key 107 b, where the eUICC profile key 107 b can comprise a symmetric ciphering key. The use of a step 206 by module 101 and/or eUICC 107 is also depicted and described in connection with FIG. 2b and FIG. 3 below. Note that both eUICC subscription manager 109 and module 101 can record profile 107 c with ciphertext 208 a for a period of time, and the step 206 can be taken (i) after receiving eUICC profile key 107 b and (ii) before module 101 authenticates with a wireless network 102 using the eUICC profile 107 c. A step 206 can convert the ciphertext 208 a into plaintext, such that an eUICC 107 can read the values in order to authenticate with a wireless network 102 using the first key K 203. By encrypting the first network module identity 202 and the first key K 203, these network access credentials can remain secure, such that a profile 107 c can be transferred in normal physical media (such as disks, drives, or files transferred electronically) or in communications channels outside the control of a mobile network operator 104 and/or eUICC subscription manager 109.

As depicted in FIG. 2a, after a step 206 to convert profile 107 c into profile 107 d, where the ciphertext 208 a is decrypted using the eUICC profile key 107 b, the ciphertext 208 b with the second key K 204 a can remain encrypted and thus the second key K can continue to remain secure within a profile 107 d. In addition, although ciphertext 208 b is depicted in a profile 107 c as external to, or separate from, ciphertext 208 a, ciphertext 208 b could optionally be included within ciphertext 208 a. In this case, where ciphertext 208 b is within ciphertext 208 a for a profile 107 c, the result of a step 206 to generate a profile 107 d can remain the same, where the ciphertext 208 a can be decrypted by step 206 and ciphertext 208 b remains encrypted in the resulting profile 107 d from a step 206.

A module 101 can use an eUICC 107 to decrypt the second portion or ciphertext 208 b in a profile 107 d using a step 207. Before a step 207, a module 101 can take the previous steps 205 and 206 in order to record a profile 107 d with an eUICC 107. Before a step 207, module 101 can receive a symmetric key 127, where the symmetric key 127 can comprise a symmetric ciphering key. In exemplary embodiments, module 101 can receive the symmetric key 127 from a mobile network operator 104 after a user associated with module 101 performs a separate authentication step 308 b as depicted and described in connection with FIG. 3 and FIG. 4 below. By a mobile network operator 104 only sending symmetric key 127 after the second authentication step 308 b, the second key K 204 can remain secured, while a user is allowed to access the wireless network 102 (perhaps temporarily or with other constraints such as limiting access to the Internet but allowing emergency calls) using the first key K 203.

In this manner and by using a second, separate authentication step 308 b before sending symmetric key 127, the decryption of network access credentials such as the second key K 204 can remain in the control of a mobile network operator 104, thereby increasing the security of exemplary systems illustrated herein, such as systems 100, 300, and 500. By ciphering the second key K 204 with symmetric key 127, security over conventional technology for an eUICC can be increased for both a user and a mobile network operator. With conventional technology for an eUICC, where only the first key K 203 is used for authentication and ciphering of data between module 101 and wireless network 102, the decryption of the first key K 203 can be outside the control of a mobile network operator 104. With conventional technology contemplated for an eUICC, an end user outside the control or a contractual relationship with mobile network operator 104, including possibly fraudulent users or imposters of valid users, could (i) take steps to obtain a plaintext first key K 203 and associated plaintext first network module identity 202 and (ii) use the credentials to fraudulently access the wireless network 102. In contrast and as contemplated herein, the symmetric key 127 to decrypt the second key K 204 a can preferably be only made available to users who authenticate with mobile network operator using a step 308 b as described below (or an equivalent step or related commercial arrangements between a user and a mobile network operator 104).

In exemplary embodiments, use of two sets of network access credentials comprising at least the first key K 203 and the second key K 204 allows a user with an eUICC profile 107 c to connect to the wireless network 102 using the first key K 203, such that the module 101 can have connectivity to the mobile network operator 104 via the wireless network 102 (and also IP network 111) in order to conduct separate authentication steps 308 b. The security steps for a mobile network operator 104 to control the decryption of the first key K 203 can be lowered (thus making the distribution of profile 107 c simpler, less costly, and less complex), while a mobile network operator 104 can retain full control over the decryption of the second key K 204 a into a usable second key K 204 associated with the second network module identity 209.

The use of a step 207 by module 101 with an eUICC is also depicted and described in connection with FIG. 2c and FIG. 3 below. A module 101 can record profile 107 d with ciphertext 208 b for a period of time, and the step 207 can be taken (i) after recording profile 107 d, and (ii) before module 101 authenticates with a wireless network 102 using the second key K 204. A step 207 can convert the ciphertext 208 b into plaintext, such that an eUICC 107 can read the values in order to authenticate with a wireless network 102 using the second key K 204.

A step 207 can convert the encrypted second key K 204 a into a plaintext key K 204. As illustrated in FIG. 2a, a step 207 can also convert the encrypted network module identity 209 a into a plaintext network module identity 209 as well. As discussed above in this FIG. 2a, the network module 209 can be optionally omitted from a step 207, such that the plaintext network module identity 209 could be recorded in a profile 107 d, and the plaintext network module identity 209 could be included in the first portion, or ciphertext 208 a, in a profile 107 c. In another embodiment, the second network module identity 209 can be received by module 101 from wireless network 102 after the module authenticates using the first key K 203. Although not illustrated in FIG. 2a, an eUICC 107 can continue to record the plaintext network module identity 209 and plaintext second key K 204 in an eUICC profile after the second key K 204 is decrypted using the symmetric key 127. The module 101 can record the second key K 204 in a protected memory address within ROM 101 c or nonvolatile memory 101 w.

For embodiments where the first key K 203 is recorded within a ciphertext 208 c in a profile 107 d after a step 206, the first key K 203 can be converted from ciphertext 208 c into a plaintext first key K 203 using a key deciphering step 217 as depicted and described in connection with FIG. 2e below. The key deciphering step 217 could use an asymmetric ciphering algorithm 219 with input of (i) ciphertext 208 c and (ii) the eUICC private key 215 in order to output the plaintext first key K 203. As described above, the use of a ciphertext 208 c can be optionally omitted, and the first key K 203 could be recorded as plaintext in a profile 107 d. In this case, a step 217 for data in profile 107 d can be omitted, and thus step 217 with ciphertext 209 c is depicted in FIG. 2a with a dashed line.

Although the first key K 203 and the second key K 204 a are depicted in FIG. 2a as recorded within an eUICC profile 107 c or eUICC profile 107 d, the first key K 203 and the second key K 204 a can be (i) recorded in a nonvolatile memory of module 101, such as, but not limited to, a flash memory 101 w, and (ii) without the use of an eUICC 107. In other words, embodiments contemplated herein can be used without an eUICC 107, such that (i) a module 101 can use a first key K 203 to authenticate with a wireless network 102, (ii) after authentication with the first key K 203, the module can receive a symmetric key 127 to decrypt the second key K 204 a into second key K 204, and (iii) the module can authenticate with the wireless network 102 using the second key K 204. In other words, an eUICC 107 can be omitted and a module 101 can perform the same steps for (i) receiving encrypted network access credentials and (ii) decrypting the encrypted network access credentials without requiring the use of an eUICC 107.

In embodiments where a module 101 does not include an eUICC 107, the module can record the first key K 203 and the encrypted second key K 204 a in a file or memory address without requiring the use of a profile 107 c and 107 d. For example, the first key K 203 could be recorded in a regular, physical UICC, and the second key K 204 a could also be recorded in a regular, physical UICC as well. The regular, physical UICC could (i) receive the symmetric key 127 and decrypt the second key K 204 a, and (ii) subsequently record the decrypted second key K 204. The module 101 and UICC could use the decrypted second key K 204 to authenticate with the wireless network 102 where the first key K 203 was previously used. Other possibilities exist as well for a module 101 to (i) use a first key K 203 and an encrypted second key K 204 a without departing from the scope of the present invention.

FIG. 2b

FIG. 2b is a graphical illustration for ciphering and deciphering a profile using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments. An eUICC profile 107 d can be (i) ciphered using a profile ciphering algorithm 210 and (ii) deciphered with a profile deciphering algorithm 206. Both the profile ciphering algorithm 210 and the profile deciphering algorithm 206 can include a symmetric ciphering algorithm 211 and the use of an eUICC profile key 107 b. An eUICC subscription manager 109, or another node outside a module 101 as illustrated in FIG. 1a, can use a profile ciphering algorithm 210 to encrypt an eUICC profile 107 c. The processing and computational steps for performing a profile ciphering algorithm 210 could be conducted on a server associated with the eUICC subscription manager 109. The server associated with the eUICC subscription manager 109 can be similar to a server 105 illustrated in FIG. 1a, with the difference being the server associated with the eUICC subscription manager 109 can be co-located, associated with, or under the operational control of an eUICC subscription manager 109. Data for an eUICC profile 107 d used in a profile ciphering algorithm 210 can comprise the exemplary data illustrated for a profile 107 d in FIG. 2a above, and an eUICC subscription manager 109 could receive the data for the profile 107 d from a mobile network operator 104. The mobile network operator 104 could process, generate, or derive the exemplary values in a profile 107 d that can include the network parameters 201, the first network module identity 202, the first key K 203, and the ciphertext 208 b. As contemplated herein, the MNO 104 could also function as a eUICC subscription manager 109, and thus in embodiments the profile 107 d could be generated by a MNO 104 as well.

Symmetric ciphering algorithm 211 in a profile ciphering algorithm 210 can utilize a key such as an eUICC profile key 107 b to encrypt or cipher data. Examples of symmetric ciphers for a symmetric ciphering algorithm 210 include (i) an Advanced Encryption Standard (AES) cipher, as specified in Federal Information Processing Standards (FIPS) Publication 197, and (ii) Triple Data Encryption Standard (Triple DES), as described in NIST Special Publication 800-67 Revision 1, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher (Revised January 2012)". Other symmetric ciphers and/or combinations of symmetric ciphers can be utilized as well for a symmetric ciphering algorithm 210 without departing from the scope of the present invention. In general, a symmetric ciphering algorithm 211 in a profile ciphering algorithm 210 (and other steps for symmetric ciphering contemplated herein) can accept input of plaintext and a key, and using the two sets of input data, the symmetric ciphering algorithm 211 can perform multiple rounds of mixing, substituting, rotating, and/or perform XOR functions with the input in order to produce a ciphertext output. Although not illustrated in FIG. 2b and FIG. 2c, a set of cryptographic parameters can also be input into symmetric ciphering algorithms 211 in order to specify parameters or configurations of the symmetric ciphering algorithm 211, such as, but not limited to, the selection of 128, 192, or 256 bits with AES.

A cipher key used with a symmetric ciphering algorithm 211, such as, but not limited to, the exemplary eUICC profile key 107 b can comprise a random or pseudo-random number, with an appropriate length or number of bits for the symmetric ciphering algorithm 211. The exemplary eUICC profile key 107 b for use in a profile ciphering algorithm 210 could be shared between an eUICC subscription manager 109 and an eUICC 107 in a module 101 in several different ways. The eUICC profile key 107 b could be recorded in or with the eUICC 107 upon manufacturing of module 101. The eUICC profile key 107 b could be securely received by a module 101 using a wireless network 102 from the eUICC subscription manager 109 before the module 101 performs a step that includes a profile deciphering algorithm 206. An encrypted eUICC profile key 107 b could be received by module 101 and then decrypted by module 101 using an asymmetric ciphering algorithm 219 as depicted and described in connection with FIG. 2e below. The eUICC profile key 107 b could also be derived by a module 101 and an eUICC subscription manager 109 (or another server performing the steps in a profile ciphering algorithm 210) using a key exchange such as, but not limited to, a Diffie-Hellman key exchange or an Elliptic Curve Diffie-Hellman key exchange.

Other possibilities exist as well for a module **101** and an eUICC subscription manager **109** (or another server performing the steps in a profile ciphering algorithm **210**) to securely share a eUICC profile key **107 b** without departing from the scope of the present invention. In addition, although a single eUICC profile key **107 b** is illustrated in FIG. 2b, an eUICC subscription manager **109** and an eUICC **107** could use multiple eUICC profile keys **107 b**, including embodiments where a first encrypted eUICC profile **107 c** is associated with a first eUICC profile key **107 b** and a second encrypted eUICC profile **107 c** is associated with a second eUICC profile key **107 b**. Further, each encrypted eUICC profile **107 c** could be uniquely associated with a different eUICC profile key **107 b**. Each of the different eUICC profile keys **107 b** could be securely transferred between the eUICC **107** and the eUICC subscription manager **109** using either (i) asymmetric ciphering **219** as illustrated in FIG. 2e below, or (ii) a key exchange, as depicted and described in connection with step **303** of FIG. 3 below.

With a profile ciphering algorithm **210**, the symmetric ciphering algorithm **211** can accept input of (i) the eUICC profile key **107 b**, and (ii) an eUICC profile **107 d** plus an optional security token **212**, in order to output an encrypted eUICC profile **107 c**. The encrypted eUICC profile **107 c** can be reasonably secured, such that deciphering the profile **107 c** without the eUICC profile key **107 b** would be infeasible. After ciphering with a symmetric ciphering algorithm **211**, deciphering the ciphertext without the cipher key would require extensive dedicated computational resources such as hundreds of servers or more for many years or longer. The optional security token **212** can include a string or number in order to enhance the security of the ciphertext output by a symmetric ciphering algorithm **211**. The optional security token **211** could comprise a random number or other value, such that the input and output of a symmetric ciphering algorithm **211** is properly padded, where the length of input and output are appropriate for the symmetric ciphering algorithm.

Although the input of eUICC profile **107 d** is depicted in FIG. 2b with a label of "plaintext", the eUICC profile **107 d** in a profile ciphering algorithm **210**, the "plaintext" eUICC profile **107 d** can include encrypted data such as ciphertext **208 b**, where ciphertext **208 b** can include encrypted data ciphered with a different key than eUICC profile key **107 b**. In other words, a profile **107 c** can include multiple layers of ciphering, where different layers use different cipher keys, and the exemplary profile ciphering algorithm **210** with the eUICC profile key **107 b** can be used to encrypt the ciphertext **208 a** illustrated in FIG. 2a above. As noted above with FIG. 2a, ciphertext **208 b** can be either (i) included inside ciphertext **208 a**, or (ii) remain external to ciphertext **208 a**.

After a server associated with an eUICC subscription manager **109** generates the output of an encrypted profile **107 c** from a profile ciphering algorithm **210**, the encrypted profile **107 c** can be transferred to module **101** through either unsecured channels, or channels that are not under the full control of an eUICC subscription manager **109** or a mobile network operator **104** associated with the profile **107 c**. The module **101** can receive the profile **107 c** through an IP network **111**, including using the public Internet, or a manufacturer, distributor, technician, or end user could load the profile **107 c** into the module (such as, but not limited to, using a USB interface **101 v**). This initial loading of profile **107 c** by a manufacturer, distributor, technician, or end user may be required for the first use or startup of a module **101**, but then module **101** may preferably receive additional or subsequent profiles **107 c** at later times using IP network **111** and other automated, electronic means using a network including a wireless network **102**.

A module **101** or an eUICC **107** within module **101** can process the encrypted profile **107 c** using a profile deciphering algorithm **206** as depicted in FIG. 2b and also depicted and described in FIG. 2a. Note that the module **101** or eUICC **107** could record the encrypted profile **107 c** for a period of time, and take the steps to decrypt the profile **107 c** in a profile deciphering algorithm **206** after receiving the eUICC profile key **107 b** associated with the profile **107 c**. Or the eUICC profile key **107 b** could be recorded in a module **101** or with an eUICC **107** before profile **107 c** is received, and the steps for a profile deciphering algorithm **206** could be performed after the receipt of an instruction from an eUICC subscription manager **109** or at a specified time or under specified conditions (such as a module **101** needing or preferring to connect to a wireless network **102** for the first time). An exemplary use and sequence for a profile deciphering algorithm **206** is depicted and described in connection with FIG. 3 below. Other possibilities exist as well for the time that a module **101** or an eUICC **107** can process a profile deciphering algorithm **206** without departing from the scope of the present invention. As contemplated herein, the use of the term "step **206**" can refer to the use of a profile deciphering algorithm **206**, and a "step **207**" can refer to the use of a key K deciphering algorithm **207**, etc.

A profile deciphering algorithm **206** can include a symmetric ciphering algorithm **211**. The symmetric ciphering algorithm **211** can be equivalent to or the same as the symmetric ciphering algorithm **211** in a profile ciphering algorithm **210** operated by a server and as described above. The symmetric ciphering algorithm **211** can accept input of the eUICC profile key **107 b** as a cipher key. The module **101** or eUICC **107** could securely receive the eUICC profile key **107 b** using the steps described above in connection with a profile ciphering algorithm **210**. An exemplary transfer or key exchange for module **101** to receive eUICC profile key **107 b** is also described in FIG. 2e and FIG. 3 below. The symmetric ciphering algorithm **211** in a profile deciphering algorithm **206** can also accept input of the encrypted eUICC profile **107 c**, which could comprise ciphertext **208 a**.

The symmetric ciphering algorithm **211** in a profile deciphering algorithm **206** can decrypt the ciphertext **208 a** in order to output the profile **107 d**, where the ciphertext **208 a** is converted to plaintext. Ciphertext **208 b** in a profile **107 c** can remain encrypted using the symmetric key **127** after a profile deciphering algorithm **206**. In other words, the profile deciphering algorithm **206** can convert a portion of the profile **107 c** into plaintext, where the portion comprises ciphertext **208 a**. As depicted in FIG. 2a above, exemplary plaintext in a profile **107 d** resulting from a profile deciphering algorithm **206** can include a first network module identity **202** and the first key K **203**. The resulting plaintext from a profile deciphering algorithm **206** can also optionally include a security token **212**. Security token **212** could comprise the string or value also optionally input into the symmetric ciphering algorithm **211** in a profile ciphering algorithm **210**. The security token **212** can include a padding value to make the length of the security token **212** and profile **107 d** a desired value for the symmetric ciphering algorithm **211** or other requirements such as making the encrypted profile **107 c** a desired length.

FIG. 2c

FIG. 2c is a graphical illustration for ciphering and deciphering a key K using a symmetric ciphering algorithm with input of a key, in accordance with exemplary embodiments. A second key K **204 a** can be (i) ciphered using a key K ciphering algorithm **213** and (ii) deciphered with a key K deciphering algorithm **207**. Both the key K ciphering algorithm **213** and the key K deciphering algorithm **207** can include a symmetric ciphering algorithm **211** and the use of a symmetric key **127**. A mobile network operator **104** can use a key K ciphering algorithm **213** to encrypt the second key K **204 a**. The processing and computational steps for performing a key K ciphering algorithm **213** could be conducted on a server associated with the mobile network operator **104** such as a server **105** illustrated in FIG. 1a. Other possibilities exist as well for the location or association of a computer to process a key K ciphering algorithm **213** without departing from the scope of the present invention.

A key K ciphering algorithm 213 can include a symmetric ciphering algorithm 211. The symmetric ciphering algorithm 211 can be similar to the symmetric ciphering algorithm 211 as depicted and described in connection with FIG. 2b above. A symmetric ciphering algorithm 211 can include a collection of different symmetric ciphers, such that a first symmetric cipher comprising the AES cipher could be used in a FIG. 2b, while a different symmetric cipher could be used in a FIG. 2c. Or, the same algorithm within symmetric ciphering algorithm 211 can be used in a symmetric ciphering algorithm 211 in FIG. 2b and FIG. 2c. The symmetric ciphering algorithm 211 in a key K ciphering algorithm 213 can accept input of a symmetric key 127 and plaintext in the form of a second key K 204. The second key K 204 could represent a random number, such as, but not limited to, an exemplary 128 random number currently used as a shared secret key K in standard LTE networks and a different length for second key K 204 could be used as well. The second key K 204 could be derived or processed by the function of an authentication center with a home subscriber server (HSS). Although not illustrated in FIG. 2c, but as illustrated in FIG. 2a, the plaintext as input into a symmetric ciphering algorithm 211 can also include a second network module identity 209. The input into a symmetric ciphering algorithm 211 for a key K ciphering algorithm 213 can also include a number, value, or string for a security token 212. The use of a security token 212 is depicted and described in connection with FIG. 2b above. Thus, a mobile network operator 104 could also use a key K ciphering algorithm 213 to encrypt other data in addition to a second key K 204.

The symmetric key 127 input into a symmetric ciphering algorithm 211 in a key K ciphering algorithm 213 can comprise a random number processed or generated by a server 105, where the server 105 is associated with a mobile network operator 104. The server processing or deriving a symmetric key 127 can comprise or be associated with an HSS for an LTE or LTE advanced network. As illustrated in FIG. 2c, the symmetric key 127 can comprise a cipher key for the symmetric ciphering algorithm 211. A cipher key used with a symmetric ciphering algorithm 211, such as, but not limited to, the exemplary symmetric key 127 can comprise a random or pseudo-random number, with an appropriate length or number of bits for the symmetric ciphering algorithm 211 in a key K ciphering algorithm 213. Using the input of the symmetric key 127 and the plaintext second key K 204, the symmetric ciphering algorithm 211 could output an encrypted second key K 204 a. As illustrated in FIG. 2c and FIG. 2a above, the encrypted second key K 204 a could be included in ciphertext 208 b. The symmetric ciphering algorithm 211 in a key K ciphering algorithm 213 may also optionally include a security token 212, as illustrated.

After processing the ciphertext 208 b, the mobile network operator 104 can either (i) include the ciphertext 208 b in a profile 107 d and send the profile 107 d to an eUICC subscription manager 109, or (ii) send the ciphertext 208 b directly to an eUICC subscription manager 109 for the eUICC subscription manager 109 to include the ciphertext 208 b in a profile 107 d. Ciphertext 208 b could be recorded in or with an eUICC profile 107 d, where an eUICC subscription manager 109, or another server associated with an eUICC subscription manager 109 can subsequently encrypt the eUICC profile 107 d using a profile ciphering algorithm 210 depicted and described in connection with FIG. 2b above. Other possibilities exist as well for the timing of a sequence of steps for transferring and recording a ciphertext 208 b output from a key K ciphering algorithm 213 without departing from the scope of the present invention. After profile 107 d with ciphertext 208 b has been created, the profile 107 d can be ciphered with a profile ciphering algorithm 210 to create an encrypted profile 107 c, as illustrated in FIG. 2b above.

The exemplary symmetric key 127 for use in a key K ciphering algorithm 213 could be shared between a module 101 with an eUICC 107 and the mobile network operator 104 in several different ways. The symmetric key 127 could be sent from the mobile network operator 104 (possibly using a server 105) to a module 101 after (i) the module properly authenticates with the mobile network operator 104 and/or a wireless network 102 associated with the MNO 104 using the first key K 203, and (ii) a user 113 associated with the module 101 authenticates with the MNO 104. Note that if MNO 104 sends the symmetric key 127 to module 101 after module 101 uses the first key K 203 to authenticate, then the ciphering or encryption of the channel used to send the symmetric key K 127 can be within the control of MNO 104 (whereas the communications channel and ciphering keys used to send encrypted profile 107 c may be outside the control of MNO 104). The symmetric key K 127 could also be derived by a module 101 and an MNO 104 using a key exchange, where the symmetric key K 127 could be derived using a RAND 118 value received by the module 101 after authenticating with the first key K 203, where the module 101 and/or eUICC 107 derives the symmetric key K 127 using the RAND 118 value and the first key K 203. Other possibilities exist as well for a module 101 and a mobile network operator 104 to securely share a symmetric key 127 without departing from the scope of the present invention.

A module 101 or an eUICC 107 within module 101 can process the ciphertext 208 b using a key K deciphering algorithm 207 as depicted in FIG. 2c. Note that the module 101 or eUICC 107 could record the ciphertext 208 b for a period of time, and take the steps to decrypt the ciphertext 208 b with a key K deciphering algorithm 207 after receiving or deriving the symmetric key 127. Or the symmetric key 127 could be recorded in a module 101 or with an eUICC 107 before ciphertext 208 b is decrypted, and the steps for a key K deciphering algorithm 207 could be performed after the receipt of an instruction from the MNO 104 to decrypt the second key K 204 a. An exemplary use and sequence for a key K deciphering algorithm 207 is depicted and described in connection with FIG. 3 below. Other possibilities exist as well for the time that a module 101 or an eUICC 107 can process a key K deciphering algorithm 207 without departing from the scope of the present invention.

A key K deciphering algorithm 207 can include a symmetric ciphering algorithm 211. The symmetric ciphering algorithm 211 can be equivalent to or the same as the symmetric ciphering algorithm 211 in a key K ciphering algorithm 213 performed by an MNO 104 and as described in this FIG. 2c above. The symmetric ciphering algorithm 211 can accept input of the symmetric key 127 as a cipher key. The module 101 or eUICC 107 could securely receive or derive the symmetric key 127 using the steps described above in connection with a key K ciphering algorithm 213. The symmetric ciphering algorithm 211 in a key K deciphering algorithm 207 can also accept input of the encrypted key K 204 a, which could comprise ciphertext 208 b. Additional data, such as, but not limited to a second module identity 209 a could optionally be included within ciphertext 208 b.

The symmetric ciphering algorithm 211 in a key K deciphering algorithm 207 can decrypt the ciphertext 208 b in order to output the plaintext second key K 204, such that the ciphertext 208 b is converted to plaintext. The resulting plaintext from a key K deciphering algorithm 207 can also optionally include a security token 212. Security token 212 could comprise the string or value also optionally input into the symmetric ciphering algorithm 211 in a key K ciphering algorithm 213. The security token 212 can include a padding value to make the length of the security token 212 and second key K 204 a a desired value for the symmetric ciphering algorithm 211 or other requirements such as making the ciphertext 208 b a desired length.

FIG. 2d

FIG. 2d is a graphical illustration of a public key and a private key for an eUICC, in accordance with exemplary embodiments. An eUICC 107 within a module 101 can include an eUICC private key 215, which can be associated with an eUICC public key 214. The eUICC private key 215 and eUICC public key 214 can comprise a public key infrastructure (PKI) key pair for eUICC 107. The eUICC subscription manager 109 can record the eUICC public key 214

along with an eUICC identity **107 a**, such that the eUICC subscription manager **109** can properly associate one of a plurality of eUICC public keys **214** with the proper eUICC **107**. Although not illustrated in FIG. 2d, an eUICC subscription manager **109** could record the eUICC public key **214** and an associated eUICC identity **107 a** in a database. The use of an eUICC ID **107 a** is also depicted and described in connection with FIG. 3 below.

The eUICC private key **215** and eUICC public key **214** could be processed using RSA algorithms or elliptic curve cryptography (ECC) algorithms, and other possibilities exist as well for the format of PKI keys without departing from the scope of the present invention. An ECC key length of 283 bits provides security similar to an RSA key length of approximately 2048 bits, and in an exemplary embodiment the eUICC key pair can utilize an ECC algorithm, although an RSA algorithm or other algorithms for PKI keys could also be utilized by an eUICC **107**. The eUICC private key **215** can be processed or derived using a random number. eUICC public key **214** can comprise a key recorded in an X.509 certificate that also includes a module identity **110** and/or eUICC identity **107 a**, although the use of an X.509 certificate with an eUICC public key **214** is not required. The eUICC public key **214** in the form of an X.509 certificate can optionally be signed by a certificate authority. The keys can support standards such as, but not limited to, the International Organization for Standardization (ISO) ISO/IEC 9594 series of standards (herein incorporated by reference) and the Internet Engineering Task Force (IETF) RFC 5280 titled "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" (herein incorporated by reference), including future updates to these standards.

Several possibilities exist for the source of an eUICC private key **215** and eUICC public key **214**. The eUICC private key **215** and eUICC public key **214** be generated using standard software tools such as, but not limited to, Openssl, libmccrypt, and/or and Crypto++, and other tools to generate public and private keys exist as well. Public and private keys as contemplated herein could be recorded in a file such as, but not limited to, a *.pem file (Privacy-enhanced Electronic Mail), a file formatted according to Basic Encoding Rules (BER), Canonical Encoding Rules (CER), or Distinguished Encoding Rules (DER), or as text or binary file. Other formats for public and private keys may be utilized as well, including proprietary formats. A module **101** could derive the PKI key pair using a set of cryptographic algorithms and a key pair generation algorithm. The module **101** could derive the PKI key pair using a random number generator **128** and a set of cryptographic algorithms **141**, where the random number generator **128** uses input from a sensor **101 f** and/or a clock **160** in order to obtain a random number with a high degree of information entropy.

A manufacturer of module **101** or an eUICC subscription manager **109** could also derive the eUICC private key **215** and eUICC public key **214** in a server, and load the eUICC private key **215** into a nonvolatile memory of module **101** before distribution of the module **101**. The manufacturer of module **101** could send or make available the eUICC public key **214** to an eUICC subscription manager **109**. The module **101** could send record the eUICC public key **214** and send the eUICC public key **214** along with the eUICC identity **107 a** (possibly with or in the form of a module identity **110**) to an eUICC subscription manager **109** before the module **101** receives the encrypted eUICC profile **170 c**.

Although FIG. 2d illustrates an eUICC private key **215** and eUICC public key **214**, a module **101** could use a PKI key pair associated with module **101** instead of being associated with an eUICC **107** in order to use an asymmetric ciphering algorithm as depicted in FIG. 2e below. In other words, a module **101** and an eUICC subscription manager **109** could use a module private key **112 a** and a module public key **112 b** in order to obtain the same functionality of an eUICC private key **215** and an eUICC public key **214**. A module private key **112 a** and a module public key **112 b** for a module **101** could have the same properties and characteristics for an eUICC private key **215** and an eUICC public key **214** as described herein. Other possibilities exist as well for the source or use of a PKI key pair for an eUICC private key **215** and eUICC public key **214** without departing from the scope of the present invention.

In exemplary embodiments, both the eUICC subscription manager **109** and the eUICC **107** can include a set of digital signature algorithms **221**, in order to sign and verify messages between (i) an eUICC **107** and eUICC subscription manager **109**, and (ii) eUICC subscription manager **109** and MNO **104**. Digital signature algorithms **221** can also verify signatures such as, but not limited to, comparing that (i) a first secure hash value received from a sending node matches (ii) a second secure hash value calculated using a recorded public key associated with the sending node. Digital signature algorithms **221** can utilize algorithms in National Institute of Standards (NIST) "FIPS 186-4: Digital Signature Standard", or IETF RFC 6979 titled "Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)". The use of ECDSA algorithm within a set of digital signature algorithms **221** may be preferred if keys such as, but not limited to, eUICC private key **215** and eUICC public key **214** are based on elliptic curve cryptography. Digital signature algorithms **221** could also include an RSA digital signature algorithm (DSA) for use with RSA-based public and private keys. Other PKI standards or proprietary techniques for securely generating digital signatures and verifying digital signatures may be utilized as well in digital signature algorithms **221**. As depicted and described in connection with FIG. 3 below, a digital signature algorithm **221** can be used in a step **205** in order to authenticate an eUICC **107** operating in a module **101** with an eUICC subscription manager **109**.

As illustrated in FIG. 2d, the eUICC subscription manager **109** may also be associated with an eUICC subscription manager public key **220** and an eUICC subscription manager private key **222**, and the two keys can comprise a PKI key pair for the eUICC subscription manager **109**. The eUICC subscription manager public key **220** and an eUICC subscription manager private key **222** can be formatted and processed by algorithms equivalent or similar to the algorithms and format for the eUICC public key **214** and the eUICC private key **215** described in this FIG. 2d above. The eUICC subscription manager public key **220** can optionally be signed by a certificate authority. An eUICC **107** can use the digital signature algorithms **221** and the eUICC subscription manager public key **220** to verify a digital signature from the eUICC subscription manager **109**. Although not illustrated in FIG. 2d, the eUICC **107** or module **101** could also record a public key associated with the mobile network operator **104**, and use the public key associated with the mobile network operator **104** to verify a digital signature from the mobile network operator **104** using the digital signature algorithms **221**.

FIG. 2e

FIG. 2e is a graphical illustration for ciphering and deciphering a key for an eUICC using an asymmetric ciphering algorithm using a PKI key pair, in accordance with exemplary embodiments. An eUICC subscription manager **109** could process or calculate a key ciphering algorithm **216** and a module **101** or eUICC **107** could process or calculate a key deciphering algorithm **217**. The eUICC key ciphering algorithm **216** can use an asymmetric ciphering algorithm **219** with an input of (i) an eUICC public key **214** as a cipher key and (ii) the eUICC profile key **107 b** as plaintext in order to output ciphertext of an encrypted eUICC key **218**. The plaintext eUICC profile key **107 b** can comprise a random number of appropriate length for processing a profile ciphering algorithm **210** and profile deciphering algorithm **206** as depicted and described in connection with FIG. 2b above. As illustrated in FIG. 2e, the input into a key ciphering algorithm **216** could also include an optional security token **212**, where a security token **212** is depicted and described in connection with FIG. 2b above.

An asymmetric ciphering algorithm 219 within a key ciphering algorithm 216 and a key deciphering algorithm 217 comprise an algorithm for utilizing public key infrastructure (PKI) techniques to both (i) encrypt plaintext with a public key and (ii) decrypt plaintext with a private key. Example algorithms within asymmetric ciphering algorithm 219 include an RSA algorithm and an elliptic curve cryptography (ECC) algorithm, and other asymmetric ciphering algorithms could be utilized as well. The use and application of RSA algorithms and cryptography are described within IETF RFC 3447 titled "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", herein incorporated by reference, among other published standards for the use of RSA algorithms. The use of an RSA algorithm in an asymmetric ciphering algorithm 219 for encryption and decryption, can also be processed according to the description of the RSA algorithm according to the Wikipedia entry for "RSA (algorithm)" as of Sep. 9, 2013, which is incorporated by reference herein. The use and application of an ECC algorithm for asymmetric ciphering algorithm 219 can conform with algorithms within IETF RFC 6090 titled "Fundamental Elliptic Curve Cryptography Algorithms" (herein incorporated by reference), among other published standards using ECC. Asymmetric ciphering algorithm 219 can also utilize elliptic curve cryptography algorithms for the Wikipedia entry for "Elliptic curve cryptography" as of Sep. 9, 2013, which is incorporated by reference herein.

ECC algorithms (with corresponding ECC-based PKI keys) may be utilized for asymmetric ciphering algorithm 219 according to exemplary preferred embodiments in order to maintain high security with smaller key lengths, compared to RSA, thereby helping to comparably reduce the message lengths, radio frequency spectrum utilization, and processing power required by module 101. RSA algorithms (with corresponding RSA-base PKI keys) for asymmetric ciphering algorithm 219 may be utilized in other embodiments in order to maintain compatibility with deployed or legacy software and systems that support RSA based keys and algorithms.

After an eUICC subscription manager 109 uses a eUICC key ciphering algorithm 216 to convert a plaintext eUICC profile key 107 b into a ciphertext as an encrypted eUICC key 218, the eUICC subscription manager can send the ciphertext to the module 101. The eUICC subscription manager could send the ciphertext as an encrypted eUICC key 218 to module 101 using an IP network 111, and the IP network 111 could comprise the public Internet. In this manner, the module 101 can securely receive the encrypted eUICC key 218 in order to perform, process, or calculate a key deciphering algorithm 217. Third parties with access to the encrypted eUICC key 218 would not feasibly be able to read the plaintext eUICC profile key 107 b, even with access to the eUICC public key 214. The module 101 could receive the encrypted eUICC key 218 along with an eUICC profile identity 107 e in order to determine a profile 107 c associated with the encrypted eUICC key 218, where a subsequent step (after deciphering the encrypted eUICC key 218) could comprise a profile deciphering algorithm 206. The module 101 could receive the encrypted eUICC key 218 either before or after receiving the profile 107 c.

After receiving the encrypted eUICC key 218, the module 101 or eUICC 107 could decrypt the encrypted eUICC key 218 using a key deciphering algorithm 217. A key deciphering algorithm 217 can include an asymmetric ciphering algorithm 219. The asymmetric ciphering algorithm 219 can be equivalent to or the same as the asymmetric ciphering algorithm 219 in a key ciphering algorithm 216 operated or processed by an eUICC subscription manager 109 as described in this FIG. 2e above. The asymmetric ciphering algorithm 219 in a key deciphering algorithm 217 can accept input of the eUICC private key 215 as a cipher key. The asymmetric ciphering algorithm 219 in a key deciphering algorithm 217 can also accept input of the encrypted eUICC key 218 as a ciphertext. The key deciphering algorithm 217 can use an asymmetric ciphering algorithm 219 with an input of (i) an eUICC private key 215 as a cipher key and (ii) the encrypted eUICC key 218 as ciphertext in order to output plaintext of an eUICC profile key 107 b. As illustrated in FIG. 2e, the plaintext could also optionally include a security token 212. After processing a plaintext eUICC profile key 107 b from a key deciphering algorithm 217, module 101 or eUICC 107 could use the plaintext eUICC profile key 107 b in order to perform a profile deciphering algorithm 206 as illustrated in FIG. 2b.

Although exemplary embodiments can include the use of a key ciphering algorithm 216 and a key deciphering algorithm 217 in order to securely transfer the eUICC profile key 107 b from an eUICC subscription manager 109 to a module 101, a key ciphering algorithm 216 and a key deciphering algorithm 217 can be omitted in other exemplary embodiments. For example, if the eUICC subscription manager and module 101 or eUICC 107 support the use of a secure key exchange such as Diffie-Hellman or ECDH, then the eUICC profile key 107 b could be mutually derived by the two nodes and the encrypted eUICC key 218 would not need to be transferred through an IP network 111 between the two nodes.

In another embodiment, as depicted in FIG. 2e, the key ciphering algorithm 216 and key deciphering algorithm 217 may also be used with ciphertext 208 c with an encrypted first key K 203 and a plaintext of the first key K 203, if a profile 107 d includes ciphertext 208 c with encrypted first key K 203. In this case, a mobile network operator 104 could perform the key ciphering algorithm 216 with input of (i) the plaintext first key K 203 and (ii) the eUICC public key 214 in order to output ciphertext 208 c. The ciphertext 208 c can include the encrypted first key K 203, although the ciphertext 208 c could also include other data such as the network parameters 201. The MNO 104 could send the ciphertext 208 c (with the encrypted first key K) to the eUICC subscription manager 109 in a step 302 b in FIG. 3 for inclusion in the profile 107 d and profile 107 c. As depicted in FIG. 2e, a module 101 or eUICC 107 could perform the key deciphering algorithm 217 on the ciphertext 208 c with the first encrypted key K 203 in order to obtain the plaintext first key K 203. In this manner, the first key K 203 is not shared as plaintext with any entities besides the MNO 104 and a module 101 with the eUICC 107. In other words, a MNO 104 can use a key ciphering algorithm 216 to prevent the sharing of a plaintext first key K 203 with an eUICC subscription manager 109.

In addition, although FIG. 2e illustrates an eUICC subscription manager as performing the eUICC key ciphering algorithm 216 and the module 101 or eUICC 107 as performing the eUICC key deciphering algorithm 217, an alternative embodiment contemplates that the eUICC subscription manager 109 performs the eUICC key deciphering algorithm 217 and the module 101 or eUICC 107 performs the eUICC key ciphering algorithm 216. In this alternative embodiment, the module 101 can (i) derive the eUICC profile key 107 b, and (ii) send the ciphertext comprising the encrypted eUICC key 218 to the eUICC subscription manager 109. In this alternative embodiment, the module 101 can (i) use the eUICC subscription manager public key 220 to cipher the derived eUICC profile key 107 b, (ii) send the encrypted eUICC profile key 107 b to the eUICC subscription manager 109, and (iii) the eUICC subscription manager 109 can decrypt the encrypted eUICC profile key 107 b using the eUICC subscription manager private key 222. In this alternative embodiment, the eUICC subscription manager 109 could (i) use the eUICC key deciphering algorithm 217 to decrypt the encrypted eUICC key 218 received from the module 101, and then (ii) subsequently encrypt the profile 107 d into a profile 107 c using a profile ciphering algorithm 210 as depicted and described in connection with FIG. 2b above.

FIG. 3

FIG. 3 is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments. System 300 can include an eUICC subscription manager 109, an IP network 111, a mobile network operator 104, a module 101. A module 101 can include a network application 101 x and an eUICC 107. The network application 101 x can perform the operations

for communicating with the wireless network **102** (i) at the data-link layer using standards for PLMN networks such as, but not limited to exemplary radio resource control standards within ETSI TS 136 331 v.10.7 entitled "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification", which is herein incorporated by reference, and (ii) at the network layer using Internet Protocol. Other standards for communication at the data-link layer between a network application **101 x** and a mobile network operator **104** can be utilized as well without departing from the scope of the present invention. The (i) mobile device **101**, using the network application **101 x**, and (ii) the mobile network operator **104** can send and receive data using the wireless network **102** depicted and described in connection with FIG. 1a. Although a single module **101** is illustrated in system **300** in FIG. 3, a system **300** could include a plurality of modules **101**.

The network application **101 x** and the eUICC **107** can send and receive data locally within the module **101** using an operating system **101 h** and/or a system bus **101 d**. The network application **101 x** and the eUICC **107** can send and receive data locally within the module **101** using an eUICC driver **128** as depicted and described in connection with FIG. 1b and FIG. 1e. The module **101**, using a network application **101 x**, can send and receive data with the eUICC subscription manager **109** using the IP network **111**. As illustrated in FIG. 3, the module **101** can send and receive data with the eUICC subscription manager **109** in a step **205** using an initial network.

The initial network could comprise a different wireless network **102** than a wireless network **102** (i) for the mobile network operator **104**, and (ii) used for a first authentication **304** and a second authentication **310**. In other words, module **101** can send and receive data for an eUICC profile **107 c** through a initial network that is different than the wireless network **102** associated with the mobile network operator **104**. The network application **101 x** could support different standards for wireless networking technologies, such that the different wireless network **102** used to access the eUICC subscription manager **109** could comprise exemplary networks such as WiFi or LTE Advanced, and the network application **101 x** could use LTE to communicate with the mobile network operator **104**. Other possibilities exist as well for the network application **101 x** to support communication with a variety of different networks without departing from the scope of the present invention.

The left side of network application **101 x** in FIG. 3 for communication with the mobile network operator **104** can comprise communication through a radio **101 z** with the wireless network **102**, and the right side of network application **101 x** can comprise internal communication within module **101** as described in the paragraph above and also FIG. 1e above. The internal communication between network application **101 x** and eUICC **107** using an operating system **101 h** could comprise either (i) sharing memory **101 e**, where module **101** writes data such as, but not limited to, an exemplary RAND **118** value and eUICC **107** reads the values from the shared memory **101 e**, or (ii) using loopback UDP ports within operating system **101 h**, such that network application **101 x** sends a UDP datagram with the RAND **118** value using a first UDP loopback port, and the eUICC **107** receives the UDP datagram with the RAND **118** value using a second UDP loopback port. For an operating system **101 h** within module **101** using IPv4 addresses, the addresses used for the UDP loopback ports could comprise addresses in the range of the 127.0.0.0/8 address block. For an operating system **101 h** within module **101** using IPv6 addresses, the addresses used for the UDP loopback ports could comprise an ::1 address. In another embodiment illustrated in FIG. 1f above, the eUICC **107** can communicate with the MNO **104** directly for embodiments where the eUICC **107** includes an IP address **106 c**.

At a step **301**, a module **101** can record an eUICC identity **107 a**, an address **109 a** of an eUICC subscription manager **109**, and an eUICC private key **215** associated with the eUICC **107**. A manufacturer, distributor, technician, end user, or installer of module **101** could record the data for a step **301** in module **101**, or the data could be downloaded or accessed separately via an IP network **111**, including the public Internet. Other data could be included in a step **301** as well, such as, but not limited to, the software or firmware comprising the eUICC **107**, an eUICC profile key **107 b**, an eUICC public key **214**, an eUICC subscription manager public key **220**, an eUICC driver **128**, an initial profile **107 d** or **107 c**, and policy rules for allowing access to the profiles, and other additional data could be included in a step **301** as well. Additional optional data for recording with an eUICC **107** in a step **301** are depicted on the second line of step **301** in FIG. 3.

In an exemplary embodiment, a manufacturer of module **101** records the exemplary data for an eUICC **107** in a step **301**, such that a module **101** can begin operations and connecting to an initial wireless network **102** upon power-up in order to establish initial communications, including allowing the communication with the eUICC subscription manager **109** through the initial wireless network **102**. As noted above in this FIG. 3, an initial wireless network **102** used for the eUICC **107** to access the eUICC subscription manager **109** can be different than the wireless network **102** used to access the mobile network operator **104**. The address **109 a** of an eUICC subscription manager **109** could comprise either an IP address or a domain name, and in an exemplary embodiment the address **109 a** comprises a domain name and the module **101** can query for the IP address associated with the domain name for address **109 a** via either a domain name system (DNS) query or a secured DNS query (DNSSEC). A module **101** can connect with an initial wireless network **102** (different than the depicted wireless network **102** in FIG. 3) after a step **301** in order to communicate with an eUICC subscription manager **109**.

At a step **302 a**, an eUICC subscription manager **109** could record data for the eUICC **107**. The data could include (i) an eUICC identity **107 a**, (ii) a profile **107 c**, (iii) an eUICC public key **214**, (iv) an eUICC subscription manager public key **220** and private key **222**, (v) an eUICC profile key **107 b** with an associated eUICC profile identity **107 e**, (vi) a module identity **110** (for embodiments where the module identity **110** for the eUICC **107** is known before the eUICC **107** sends and receives data with the eUICC subscription manager **109**), (viii) and parameters for a symmetric ciphering algorithm **211** and an asymmetric ciphering algorithm **219** used by the eUICC **107**. The parameters for a symmetric ciphering algorithm **211** and an asymmetric ciphering algorithm **219** used by the eUICC **107** could specify the ciphers used, such as (i) selecting an exemplary 128 or 192 bit keys for use with an AES cipher for a symmetric ciphering algorithm **211** used with a eUICC **107** and eUICC identity **107 a**, and (ii) selecting an exemplary elliptic curve or RSA algorithm for use with an asymmetric ciphering algorithm **219**. The eUICC subscription manager **109** could also record related data for the operation of eUICC **107** with eUICC subscription manager **109** in a step **302 a**.

At a step **302 a**, the eUICC subscription manager **109** could receive the profile **107 d** from the mobile network operator **104**, and an exemplary profile **107 d** is depicted and described in connection with FIG. 2a. Or, eUICC subscription manager **109** could receive a subset of data for the exemplary profile **107 d** from the MNO **104** in a step **302 a** without receiving the entire profile **107 d**. As one example, the MNO **104** may not know the eUICC profile identity **107 e** for the eUICC profile **107 d**, and thus the MNO **104** may not send the complete profile **107 d** but the MNO **104** could send data for the profile **107 d** to the eUICC subscription manager **109** in a step **302 a**. In an exemplary embodiment, the eUICC subscription manager **109** could receive a subset of data for the profile **107 d** using the IP network **111** over a secured link or connection to the MNO **104**. The profile **107 d** in a step **302 a** could include both ciphertext **208 b** and plaintext of a set of network parameters **201**, a first network module identity **202**, and a first key **203**. As depicted and described in

connection with FIG. 2a, the ciphertext 208b could comprise an encrypted secondkey K 204a. The ciphertext 208b could also include the second network module identity 209a. In an exemplary embodiment, the plaintext firstkey K 203 could be optionally omitted from being received from an MNO 104 in a step 302a, and the eUICC subscription manager 109 can receive the firstkey K 203 in the form of a ciphertext 208c below in a step 302b. The eUICC subscription manager 109 could use a server or a plurality of servers similar to server 105 in order to take the processing and communication steps described herein for an eUICC subscription manager 109 in this step 302a and also additional steps for an eUICC subscription manager 109 described throughout FIG. 3.

After a module 101 powers up and established connectivity with the network 111, an eUICC 107 operating in a module 101 could then perform a step 205 in order to receive an eUICC profile 107c using the network 111. The use and operation of a step 205 is also depicted and described in connection with FIG. 2a above. In a step 205, an eUICC 107 could send an eUICC identity 107a to the eUICC subscription manager 109. The module 101 could use a network application 101x to send the eUICC identity 107a, such as the network application 101x writing data with the eUICC identity 107a to a physical interface 101a, and the physical interface 101a could include a radio 101z. Or, using the exemplary embodiment illustrated in FIG. 1a above, the eUICC 107 could be associated with an IP address 106c, and the eUICC 107 could send the eUICC identity 107a to the eUICC subscription manager 109 without using a separate network application 101x associated with the wireless network 102. During a step 205 for a module 101 or eUICC 107, an eUICC subscription manager 109 could receive the eUICC identity 107a and perform a step 302b. In an exemplary embodiment, both a module identity 110 and an eUICC identity 107a could be sent by an eUICC 107 or a module 101 in a step 205. Or, the eUICC identity 107a could comprise a module identity 110, and the module identity 110 could be sent in a step 205. Other possibilities exist as well for identifying a module 101 or an eUICC 107 with an eUICC subscription manager 109 without departing from the scope of the present invention.

In an exemplary embodiment, a message with the eUICC identity 107a in a step 205 could include a digital signature, where the digital signature is processed using (i) the eUICC private key 215 recorded in a step 301 and (ii) a digital signature algorithm 221. The message with the eUICC identity 107a and a digital signature in a step 205 could preferably include a random number or string, including a nonce or a "number used once" such as, but not limited to, an exemplary security token 212 in order to prevent replay attacks.

An eUICC subscription manager 109 can take several actions in a step 302b after receiving an identity for the eUICC 107 or module 101. A first action in a step 302b could comprise authenticating an eUICC 107 or a module 101 based on the eUICC identity 107a received in the message. In a step 302b, eUICC subscription manager 109 can authenticate the message with the eUICC identity 107a according to message digest, or using the eUICC profile key 107b which could be recorded in the eUICC 107 in a step 301 above. In addition, the eUICC subscription manager could authenticate using digital signature algorithm 221, where the message with the eUICC identity 107a could include a digital signature, as described in the paragraph above.

Both the eUICC 107 and the eUICC subscription manager 109 could use the eUICC profile key 107b as a cipher key with asymmetric ciphering algorithm 211 to encrypt/decrypt data sent with the eUICC identity 107a, where the successful encryption and decryption of data with the eUICC identity 107a using the eUICC profile key 107b on both ends could be confirmation that the eUICC 107 or module 101 is authenticated, since both parties would only be able to mutually successfully encrypt and decrypt by sharing the same eUICC profile key 107b. In another embodiment, the eUICC profile key 107b could be used as a private key with a digital signature algorithm 211 (instead of the eUICC private key 215), in order for the eUICC 107 with the eUICC 107a to be authenticated. For embodiments where the module 101 with the eUICC 107 sends a digital signature with the eUICC identity 107a, the eUICC subscription manager 109 could use the eUICC identity 107a to select the eUICC public key 214 or eUICC profile key 107b from a database. In this manner, the eUICC subscription manager 109 could communicate with a plurality of eUICCs 107 and select the appropriate keys using the eUICC identity 107a.

A second action in a step 302b could comprise the eUICC subscription manager 109 authenticating with an eUICC 107 or a module 101. The eUICC subscription manager 109 could also authenticate with an eUICC 107 at a step 302b within a step 205, such that the eUICC 107 can confirm an identity of the eUICC subscription manager 109, using any of the same or equivalent steps described in the paragraph above for an eUICC 107 to authenticate with an eUICC subscription manager 109. The eUICC subscription manager 109 could send the eUICC 107 a digital signature processed using a digital signature algorithm 221 and the eUICC subscription manager private key 222. The eUICC 107 could verify the digital signature using a eUICC subscription manager public key 220 (which could be recorded with an eUICC 107 in a step 301). The eUICC 107 could also receive data encrypted with a eUICC profile key 107b, and successful decryption of the data by the eUICC 107 using a symmetric ciphering algorithm 211 could confirm the eUICC subscription manager 109 also holds the eUICC profile key 107b. Note that a system 300 could include multiple eUICC keys 107b, such that a first eUICC profile key 107b is used with a step 301 and a step 205 in FIG. 3, and a second eUICC profile key 107b could be used with a subsequent step 206 below. Other possibilities exist as well for an eUICC 107 and an eUICC subscription manager 109 to perform a 2-way authentication in a step 205 and a step 302b in FIG. 3 without departing from the scope of the present invention.

In another exemplary embodiment, where data received from an MNO 104 does not include a plaintext firstkey K 203 for inclusion in a profile 107d, for a third action in a step 302b, the eUICC subscription manager 109 could send the eUICC identity 107a (or the module identity 110) and the eUICC public key 214 to the MNO 104. In this embodiment, the MNO 104 could also use the key ciphering algorithm 216 depicted and described in connection with FIG. 2e above in order to encrypt the firstkey K 203 with the eUICC public key 214. The output of an MNO 104 using a key ciphering algorithm 216 could comprise a ciphertext 208c of an encrypted firstkey K 203. Thus, at a step 302b for the embodiment described in this paragraph, the eUICC subscription manager 109 could receive the firstkey K 203 for a profile 107d as ciphertext 208c (instead of a plaintext firstkey K 203 for profile 107d in FIG. 2a). In this manner, the firstkey K 203 in a profile 107d could be recorded as ciphertext 208c, which is also depicted and described as an optional format for the firstkey K 203 in FIG. 2a and FIG. 2e.

In an exemplary embodiment, the MNO 104 can send the ciphertext 208c only after a user 113 conducts a separate authentication step 308b below. In other words, a step 308b could also be used concurrently with a step 302b, where the step 302b includes the receipt of an encrypted firstkey K 203 in a ciphertext 208c. In this manner, the MNO 104 can retain control over the release of an encrypted firstkey K 203, such that the firstkey K 203 in a ciphertext 208c is only received by an eUICC subscription manager 109 in a step 302b or a eUICC 107 in a step 205 after a user 113 (associated with the module 101 with the eUICC 107) authenticates with the MNO 104. In this embodiment, a separate authentication step 308b below can be optionally omitted, and the use of an encrypted secondkey K 204a in ciphertext 208b can also be omitted. In this embodiment, a user 113 of the module 101 can access the wireless network 102 of the mobile network operator 104 using the firstkey K 203 which has been (i) encrypted by the mobile network

operator 104 using a key ciphering algorithm 216 in a step 302 b, and (ii) only available to module 101 or eUICC 107 (or eUICC subscription manager 109) after a user 113 conducts an authentication step 308 b with MNO 104.

After the eUICC subscription manager 109 receives and/or processes all the data for a profile 107 d, including subsets of data from a MNO 104 described for this step 302 b above, a fourth action in a step 302 b could comprise the eUICC subscription manager 109 ciphering a profile 107 d using a profile ciphering algorithm 210, in order to convert profile 107 d with plaintext into a profile 107 c with ciphertext. Some elements in a profile 107 c could remain plaintext as well, such as the exemplary profile identity 107 e. The eUICC subscription manager 109 could use an eUICC profile key 107 b, where the eUICC profile key 107 b in a profile ciphering algorithm 210 can be different than an eUICC profile key 107 b used to authenticate eUICC 107 with eUICC identity 107 a. Or, the same eUICC profile key 107 b could be used to both cipher profile 107 d and authenticate eUICC 107. Note that this fourth action in a step 302 b could also take place at an earlier time than a step 302 b, such that eUICC subscription manager 109 could assemble and cipher the profile 107 d into a profile 107 c at an earlier time, such as before receiving the eUICC identity 107 a, or concurrent with a step 301 a. Other possibilities exist as well for the timing and sequence for an eUICC subscription manager to assemble and process a profile 107 c without departing from the scope of the present invention.

After a step 302 b, the eUICC subscription manager 109 can send the authenticated eUICC 107 a profile 107 c in a step 205, as depicted in FIG. 3. Either the eUICC subscription manager 109 or the eUICC 107 can select the profile 107 c to be received by the eUICC 107. In one embodiment, a module 101 can search for radio beacons from base stations 103 for wireless networks 102 surrounding the module 101, and upon finding a new possible wireless network 102 to connect with, the module 101 or eUICC 107 could query or request the eUICC subscription manager 109 for a profile 107 c associated with a mobile network operator 104 for a radio beacon observed by the module 101. Commercial business arrangements among the user of module 101, the eUICC subscription manager 109, and the mobile network operator 104 can determine the availability of a profile 107 c for a module 101 with an eUICC 107.

In another embodiment, the eUICC subscription manager 109 could periodically send the module 101 and/or eUICC 107 new profiles 107 c as they become available to a user 113 of a module 101 or available to the eUICC subscription manager 109. In a preferred embodiment, the eUICC subscription manager 109 can send the profile 107 c to the module 101 using a network application 101 x, where the network application 101 x forwards the data to the eUICC 107. As described above in this FIG. 3, the network application 101 x could communicate with the eUICC 107 using the operating system 101 h as illustrated in FIG. 1e, and other possibilities exist as well. Note that the eUICC subscription manager 109 sends the profile 107 c, where the network access credentials (including the first key K203) are encrypted with an eUICC profile key 107 b, and in this manner intermediate nodes on the network 111 would not feasibly be able to read the data within the profile 107 c.

In an exemplary embodiment, the eUICC subscription manager 109 can send the module 101 a pointer, uniform resource locator (URL), domain name, or related address for a location of the eUICC profile 107 c in a step 205 as opposed to the actual, full profile 107 c. In this embodiment, the module 101 could receive the pointer, uniform resource locator, domain name, or related address for the location of the eUICC profile 107 c and subsequently download the eUICC profile 107 c from an IP address associated with the pointer, uniform resource locator, domain name, or related address for a location of the eUICC profile 107 c.

As depicted in FIG. 3, after receiving the profile 107 c from the eUICC subscription manager 109 in a step 205, the eUICC 107 can receive data for decrypting the profile 107 c in a step 303. Note that if eUICC profile key 107 b (in the form of a symmetric key as illustrated in FIG. 2a) has already been shared between the eUICC 107 and the eUICC subscription manager 109 before a step 206 below, then a step 303 could separately be omitted. For example, if an eUICC profile key 107 b has been recorded with an eUICC 107 in a module 101 by a manufacturer of module 101, then that eUICC profile key 107 b could be used in a step 206 below, and a separate step 303 could be omitted. In other exemplary embodiments, the eUICC 107 can receive data for processing or deriving the eUICC profile key 107 b for a step 206 below using the step 303 illustrated in FIG. 3. A step 303 can include the receipt by eUICC 107 of either (i) an encrypted eUICC key 218, or (ii) data for a key exchange. The encrypted eUICC key 218 received by an eUICC 107 in a step 303 could comprise an eUICC profile key 107 b that is ciphered using a key ciphering algorithm 216 illustrated in FIG. 2a. For embodiments where data for a key exchange is received in a step 303, the algorithms used with a key exchange could comprise a Diffie Hellman key exchange, or an Elliptic Curve Diffie Hellman key exchange (ECDH).

An eUICC 107 within a module 101 could use an ECDH key exchange in a step 303 when ECC algorithms are utilized for eUICC public key 214, eUICC private key 215, and eUICC subscription manager private key 222 and eUICC subscription manager public key 220. A summary of ECDH is included in the Wikipedia article titled "Elliptic Curve Diffie-Hellman" (http://en.wikipedia.org/wiki/Elliptic_curve_Diffie-Hellman) from Sep. 24, 2013, which is herein incorporated by reference. An ECDH key exchange in a step 303 could comprise the message received by an eUICC 107 including a common base point G. The base point G could also be sent from an eUICC 107 to eUICC subscription manager 109. The base point G for an ECDH key exchange in a step 303 could also be recorded with the eUICC in a step 301 above, and in this case the message at a step 303 received by an eUICC 107 could comprise a signal to initiate or use a key exchange for deriving the eUICC profile key 107 b. Note that the eUICC subscription manager 109 and the eUICC 107 could take additional steps to process the eUICC profile key 107 b after an ECDH key exchange at a step 303, such as taking the output of an ECDH key exchange and inputting that output into a secure hash algorithm in order to obtain the eUICC profile key 107 b. Other algorithms besides an ECDH or Diffie Hellman key exchange can be utilized as well at a step 303, including a key exchange according to the American National Standards Institute (ANSI) standard X-9.63.

After completing a step 303, an eUICC 107 operating in a module 101 could read and utilize the eUICC profile key 107 b. In embodiments where the eUICC profile key 107 b in a step 303 above comprises an encrypted eUICC key 218, a step 217 from FIG. 2a can be utilized by the eUICC 107 in order to decrypt the eUICC key 218 into a plaintext of eUICC profile key 107 b. The plaintext eUICC profile key 107 b can be used by the eUICC 107 in a step 206 to decrypt (x) the profile 107 c received in a step 205 above into (y) a profile 107 d. The use of an eUICC profile key 107 b for a step 206 is also depicted and described in connection with FIG. 2a above and also FIG. 2b. Plaintext within a profile 107 d can be read after a step 206, although in exemplary embodiments and as illustrated in FIG. 2a, the profile 107 d can continue to record ciphertext 208 b and ciphertext 208 c.

In an exemplary embodiment, after a step 206 in FIG. 3 to convert received profile 107 c to profile 107 d, if (A) a ciphertext 208 c that includes the first key K203 is present in profile 107 d (as depicted in FIG. 2a above), then (B) eUICC 107 could also use a key deciphering algorithm 217 on ciphertext 208 c in order to extract the plaintext first key K203. Note that ciphertext 208 a could be ciphered by an eUICC subscription manager 109 using a profile ciphering

algorithm 210) and ciphertext 208 b and/or ciphertext 208 c could be encrypted by a mobile network operator 104 (using a key ciphering algorithm 214). In other words, a module 101 with an eUICC 107 can use (i) a profile deciphering algorithm 206 with an eUICC profile key 107 b to decrypt ciphertext 208 a, (ii) a key deciphering algorithm 217 with an eUICC private key 215 to decrypt ciphertext 208 c, and/or (iii) a key deciphering algorithm 207 with a symmetric key 127 to decrypt ciphertext 208 b.

After reading plaintext in profile 107 d, module 101 could then utilize the profile 107 d to conduct a first authentication 304 with the mobile network operator 104. As depicted in FIG. 3 the first authentication 304 can comprise (i) module 101 sending an attach message 305 with network module identity 202, (ii) the eUICC 107 and module 101 receiving a RAND 118, (iii) the eUICC 107 using a step 306 in order to calculate a RES 119, and (iv) the module 101 sending the RES 119. Although not illustrated in FIG. 3, a first authentication 304 could include other data such as receiving the equivalent of an "OK" message upon successful authentication, the receipt of additional network parameters 202 after successful authentication, etc. The module 101 can use a profile 107 d from a step 206 above in order to conduct the first authentication 304. The profile 107 d in an eUICC 107 could be selected and activated in order to connect with a wireless network 102 associated with mobile network operator 104. As contemplated herein and throughout the present invention, an activated profile 107 d can comprise a selected and enabled network access application state as illustrated in Figure D.1 of ETSI TS 103 383 v.2013-02 for the activated profile 107 d, and other possibilities exist as well. As illustrated in FIG. 3 after step 206, the module 101 can use a network application 101 x in order to attach to the wireless network 102 and communicate with the mobile network operator 104.

Within a first authentication 304, the module 101 can send a first attach message 305, and the first attach message 305 can include the first network module identity 202. With a 4G LTE network, the first attach message 305 could comprise a radio resource connection request message, or a similar message could be utilized with other wireless networking standards as well, such as LTE Advanced or WiMAX. An exemplary radio resource connection request is described in section 5.3.3 within ETSI TS 136 331 v.10.7 entitled "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification", which is herein incorporated by reference. Although not illustrated in FIG. 3, the module 101 and wireless network 102/mobile operator 104 could take additional related steps before sending the exemplary first attach message 305, such as, but not limited to, module 101 synchronizing a clock 160 with wireless network 102, module 101 sending a message on a random access control channel (RACH) in order to have a timeslot and frequencies for sending the first attach message 305, etc.

As depicted in FIG. 3, after receiving and processing the first attach message 305, the mobile network operator can send a first random number (RAND) 118. Although not illustrated in FIG. 3, a network authentication token "AUTN" and a sequence number could be sent with the first RAND 118. An exemplary format for the use of a RAND 118 with a response RES 119 is described in ETSI standard TR 131 900 v.10.0.0 and related documents. In first authentication 304 the module 101 and the eUICC 107 can receive the first RAND 118. The eUICC 107 can conduct a step 306 with an input of the first RAND 118 and the first key K 203 in order to calculate a first RES 119. The use of a RAND 118 with a RES 119 in a step 306 could comprise a general use of a message digest authentication, and another exemplary message digest authentication is also described in IETF RFC 2617, titled "HTTP Authentication: Basic and Digest Access Authentication". After receiving the exemplary first RAND 118 message, in order to conduct a first authentication 304, module 101 using an eUICC 107 could take steps to demonstrate to MNO 104 that module 101 has access to the same first key K 203 as recorded by the MNO 104 in a step 302 a or step 302 b above. MNO 104 could record the expected RES 119 value with a set of authentication vectors 117 for the first network module identity 202, as depicted in FIG. 1d and FIG. 1e.

Module 101 can properly respond to a challenge/nonce (such as a first RAND 118) in a message digest authentication by sending a secure hash value calculated using (i) the challenge/nonce and (ii) the first key K 203. The secure hash value can comprise the first RES 119. In exemplary embodiments, eUICC 107 and wireless network 102 could use algorithms specified in ETSI TS 135 205-209, as well as subsequent and related standards, in order for module 101 using eUICC 107 to (i) calculate a secure hash value, and (ii) process related steps for a first authentication 304. After processing a first RES 119 in a step 306 using the first key K 203, the eUICC 107 could send the first RES 119 to the network application 101 x in module 101. Module 101 could then send the first RES 119 to the mobile network operator 104 using the wireless network 102, as depicted in FIG. 3 and thereby complete a first authentication step 304 for the module 101.

In another embodiment for a first authentication step 304, (i) module 101 could send (i) the first network module identity 202 a digital signature processed using a digital signature algorithm 221 and the eUICC private key 215, and (ii) MNO 104 could verify the digital signature using a digital signature algorithm 221 and the eUICC public key 214. Other possibilities exist as well for steps within a first authentication 304 using an eUICC private key 215 with the first network module identity 202 or the eUICC identity 107 a in a first authentication step 304 without departing from the scope of the present invention. In an exemplary embodiment, as depicted in FIG. 1a above, the eUICC 107 could include an IP address 106 c with an interface identifier 106 e associated with the eUICC 107, and in this case the module 101 could send the first RES 119 value from the eUICC 107 to the MNO 104 through the wireless network 102.

In a step 308 a the mobile network operator 104 can receive the first RES 119. A server 105 such as a mobility management entity (MME) for the mobile operator network 104 associated with the wireless network 102 could compare the received first RES 119 with an internally recorded RES 119 from the authentication vector 117. As noted above, the authentication vector 117 could be received by the server 105 from the HSS of the mobile network operator 104 before a step 308 a. If the received first RES 119 matches the internally stored first RES 119 value, the wireless network 102 and mobile network operator 104 can consider or process that the module 101 is authenticated for a step 308 a. The wireless network 102, the MNO 104, and the module 101 can take subsequent steps (not shown) for the module 101 to access the IP network 111, in order to conduct authentication of the module 101 or a user associated with the module 101 with a second factor in a step 308 b below.

In a step 308 b, the mobile network operator 104 can conduct a separate authentication of either a user 113 associated with a module 101 or the module 101 using a second factor. In other words, the mobile network operator 104 can use a step 308 b to authenticate the user 113 of module 101 or the module 101 using steps and a process that is different than the first authentication 304. Note that this use of a separate authentication step 308 b can be different than conventional technology used in authenticating module 101 in a step 304, since other values and tokens besides the first key K 203 can be used in the authentication step 308 b. The additional authentication step 308 b can be useful for a mobile network operator 104 to authenticate a module 101 with an eUICC 107 and profile 107 d, since the profile 107 d with the first key K 203 may be transferred to module 101 in a communications channel outside the control of mobile network operator 104. As one example, the profile 107 d with the first network key K 203 could be transferred to an eUICC 107 from the eUICC subscription manager 109 using an IP network 111, as depicted in FIG. 3 in a step 205. The mobile network operator 104 may not

have control over the IP network 111 used in a step 205. The mobile network operator 104 may not have control over the security keys and algorithms used to encrypt the profile 107 d into a profile 107 c, and thus the security of the first key K 203 upon which the MNO 104 depends for authentication and ciphering of data with module 101 may be outside the control of MNO 104. As one example, the MNO 104 may not be able to separately authenticate the identity of a user of module 101 with the eUICC 107, before the profile 107 d was received by module 101 and eUICC 107 in a step 205.

Consequently, without a separate authentication step 308 b the user 113 of module 101 with the eUICC 107 may be unknown to MNO 104, and a separate identity of the user 113 or module 101 (other than network module identity 202) may preferably be authenticated in a step 308 b. Thus, a MNO 104 may use a separate authentication step 308 b in order to authenticate a user 113 of module 101 with the eUICC 107 and the first key K 203 in exemplary embodiments. The user 113 can have a contractual or business relationship with MNO 104 in order to pay for voice and/or data services from the MNO 104, and thus the MNO 104 can preferably identify and authenticate a user 113 in a step 308 b.

A step 308 b can comprise the authentication and/or secure identification of (i) a user 113 of module 101 or (ii) module 101 using a second factor. Although a step 308 b is depicted in FIG. 3 as being performed after a first authentication 304, a step 308 b could be performed before a step 304 (including with a step 302 b as described in step 302 b above). The use of a second factor in an authentication step 308 b can comprise a two-factor authentication, where the first factor can be the successful completion of authentication using a step 304 and step 308 a described above. The steps for authenticating a user 113 or module 101 in a step 308 b could comprise many different forms without departing from the scope of the present invention. In one embodiment, where the user 113 of module 101 comprises a subscriber to telecommunication and data services from MNO 104, the user 113 could present identification to a representative of the MNO 104 in a step 308 b. The identification could be in the form of a physical identity such as, but not limited to, a driver's license or a passport (along with a value that can be associated with the eUICC profile 107 d such as the module identity 110 or the eUICC identity 107 a). The representative of the MNO 104 could record the identification in a web browser with connectivity to a database shared by a server 105.

In another embodiment of an authentication of a user 113 of module 101 (with the eUICC profile 107 d recorded with an eUICC 107 in module 101 from a step 205) could enter information into a web page provided by MNO 104, where the user 113 first (i) authenticates on the web page and then (i) enters identification information for the module 101 or eUICC 107. The user 113 could first authenticate with the MNO 104 via a web page by entering a valid identity and a password (where the identity and password for the web page in a step 308 b could be previously established between the user 113 and the MNO 104 before a step 308 b). In another embodiment for a step 308 b, a user 113 could call a telephone number operated by or associated with the MNO 104 and provide identification information via voice or entering information such as dual-tone multi-frequency (DTMF) digits via interactive voice response (IVR). The identification information could include either a credit card number or a personal identification number (PIN) for the user 113 (where the PIN may be previously shared or established between the user 113 and the mobile network operator 104). The user 113 could also send a text message to MNO 104 from module 101 (i) using the module 101 authenticated link with MNO 104 established in a first authentication 304, where (ii) the text message include identification information for a user 113.

In accordance with preferred exemplary embodiments for the verification of an identity of a user 113 in a step 308 b (including an authentication of a user 113 in a step 308 b), the user 113 can send data to a MNO 104 from module 101 using a data connection via a wireless network 102 associated with (and established after) the first authentication 304. In this manner, data and voice connectivity between the MNO 104 and module 101 could be established with a first authentication step 304, and the user 113 and MNO 104 can conduct an authentication step 308 b (or equivalently a verification of an identity of the user 113) to confirm the identity of the user 113 via the established data and voice connectivity using the wireless network 102. In other words, the user 113 could verify or authenticate an identity of the user 113 of module 101 through the wireless network 102 in a step 308 b, where (a) module 101 had conducted a first authentication step 304 and 308 a with MNO 104 using the first key K 203 recorded in a profile 107 d, in order to (b) support or conduct a separate verification or authentication of a user 113. In an exemplary embodiment, the user 113 could enter identifying information for a step 308 b in a web page accessed through a user interface 101 j on module 101, where data connectivity for the web page is provided to module 101 through the wireless network 102 after a first authentication step 304.

The authentication or verification of a user 113 identity in a step 308 b can comprise authenticating module 101 with a second factor, where the first factor can comprise the first key K 203 and the second factor can comprise information provided by a user 113 in a step 308 b. Other possibilities exist as well for those of ordinary skill in the art for (a) a user 113 of module 101 with the first key K 203 to (b) authenticate or verify an identity of the user 113 in a step 308 b without departing from the scope of the present invention. In these exemplary embodiments for a user 113 to authenticate or verify an identity for the user 113 for module 101 with the MNO 104, the MNO 104 could record information or data received from the user 113 in a database, such that a server 105 for MNO 104 sends the symmetric key 127 in a step 309 below after an identity of the user 113 is verified or authenticated in a step 308 b. In exemplary embodiments illustrated in FIG. 3, the module 101 can access the wireless network 102 with the first key K 203 in order to (i) establish communication with the IP network 111, (ii) support authentication of a user 113 in a step 308 b through the IP network 111, and then (iii) subsequently receive a symmetric key 127 in order to decrypt a ciphertext 208 b with a second key K 204 a.

In other exemplary embodiments, module 101 could comprise a module supporting "machine-to-machine" applications and communications, and the module could be different than a traditional mobile phone or smartphone for (i) placing voice telephone calls or (ii) supporting a user interface 101 j in the form of a touch screen and web browser. The module 101 could include a sensor 101 f for collecting data and an actuator 101 y for controlling or changing a state associated with a monitored unit for the module 101. In these embodiments, and as depicted and described in connection with FIG. 4, module 101 can be associated with an M2M service provider 115, and the M2M service provider 115 could be associated with a plurality of modules 101, as opposed to an individual with a telephone number for voice services to module 101.

Each of the different modules 101 in the plurality of modules 101 could include different values for module identities 110, eUICC identities 107 a, profile identities 107 e, and the first network module identities 202. In these embodiments for a step 308 b where the module 101 supports M2M applications for an M2M service provider 115, in a step 308 b in FIG. 3, the MNO 104 could verify that (a) module 101 with eUICC 107 and the profile 107 d from a step 304 is (b) properly associated with an M2M service provider 115. In exemplary embodiments, the MNO 104 could conduct a step 308 b by securely or properly determining that an identity from module 101 is associated with an M2M service provider 115, and an exemplary identity for module 101 include any of a module identity 110, an eUICC identity 107 a, a profile identity 107 e, and/or the first network module identity 202.

In exemplary embodiments where module 101 supports M2M application and the module 101 is associated with an M2M service provider 115, MNO 104 could take several possible actions in a step 308 b for authenticating or verifying that an identity from module 101 in FIG. 3 is associated with an M2M service provider 115. The proper association of an identity of module 101 with M2M service provider 115 may be necessary or useful for contractual and business relationships between MNO 104 and M2M service provider 115, such as, but not limited to, allowing MNO 104 to bill or invoice M2M service provider 115 for data services that MNO 104 provides to module 101. In a first exemplary embodiment for a step 308 b in FIG. 3 where module 101 supports M2M applications with an M2M service provider 115, MNO 104 could securely send to M2M service provider 115 an identity of module 101, such as, but not limited to module identity 110, eUICC identity 107 a, profile identity 107 e, and/or the first network module identity 202 through an IP network 111. The MNO 104 could also send the identity of module 101 in a query or request message. Although not illustrated in FIG. 3, the MNO 104 could also send the M2M service provider 115 a digital signature received from module 101 before a step 308 b, where the digital signature was (i) processed by module 101 using a digital signature algorithm 221 and an eUICC private key 215, and (ii) sent from the module 101 to the MNO 104.

In a step 308 b, the M2M service provider 115 could (i) receive the identity of module 101 (such as, but not limited to module identity 110, eUICC identity 107 a, profile identity 107 e, and/or the first network module identity 202), (ii) verify or determine the identity of module 101 properly belongs to M2M service provider 115, and (iii) send a response confirming the module 101 with the identity is validly associated with the M2M service provider 115. The response from the M2M service provider 115 (or data within a message from M2M service provider 115 to MNO 114) for a step 308 b can comprise a second factor for MNO 104 in authenticating module 101 with eUICC 107 and profile 107 d. In this manner, MNO 104 can confirm module 101 with the first network identity 202 is authenticated or verified as belonging to or being associated with M2M service provider 115 in a step 308 b.

In another exemplary embodiment for a step 308 b, the M2M service provider 115 could also send MNO 104 a list of pre-authorized identities for one or a plurality of modules 101 before a step 308 b (and in this case the list can comprise the second factor to authenticate module 101). MNO 104 could query the list of identities received upon receiving an identity of module 101, such as, but not limited to, the first network module identity 202 received in the first attach message 305. Other possibilities exist as well for MNO 104 to authenticate or verify that an identity of module 101 is associated with an M2M service provider 115 in a step 308 b without departing from the scope of the present invention.

After successfully verifying or confirming in a step 308 b that module 101 in FIG. 3 is associated with a known user 113 or M2M service provider 115, MNO 104 can send a symmetric key 127 in a step 309. A network application 101 x in the module 101 can receive the symmetric key 127 and the module 101 can forward the symmetric key 127 to the eUICC 107. As depicted and described in connection with FIG. 2 and FIG. 2c, the symmetric key 127 can be used by module 101 to decrypt the ciphertext 208 b, where the ciphertext 208 b can include a second key K 204 a. The symmetric key 127 can also previously be used by MNO 104 to encrypt the ciphertext 208 b. The ciphertext 208 b could be delivered to eUICC subscription manager 109 for including the ciphertext 208 b in the profile 107 d, as described above in step 302 a. The ciphertext 208 b could be sent to module 101 from the eUICC subscription manager 109 across the IP network 111 as profile 107 c in a step 205 as described above in this FIG. 3.

In exemplary embodiments, the MNO 104 can send the symmetric key 127 in a step 309 through the wireless network 102, where the connection between module 101 and MNO 104 could be initiated by the first attach message 305 and authenticated by a first authentication 304. Since the MNO 104 controls the nodes and ciphering steps for the transmission of symmetric key 127, the symmetric key 127 can be securely sent by MNO 104 and received by module 101 with ciphering and keys used at the data-link layer under the control of MNO 104 (whereas MNO 104 may not control the keys and ciphering of sending the first key K 203). Also note no entities, including the module 101, a user 113, an M2M service provider 115, an eUICC subscription manager 109, or unauthorized third parties could feasibly read the ciphertext 208 b with the second key K 204 a until they receive the symmetric key 127.

In an exemplary embodiment of a step 309 in FIG. 3, the symmetric key 127 can first be encrypted with a key ciphering algorithm 216. An encrypted symmetric key 127 ciphered with the key ciphering algorithm 216 could be received by module 101 in a step 309. As described in connection with a key ciphering algorithm 216 in FIG. 2e, the MNO 104 could select and read the eUICC public key 214 (using a received associated identity such as the first network module identity 202), and use an asymmetric ciphering algorithm 219 to encrypt the symmetric key 127. The module 101 could receive the encrypted symmetric key 127 and decrypt the symmetric key 127 in a step 309 by using a key deciphering algorithm 217 with the eUICC private key 215 and the asymmetric ciphering algorithm 219. For a step 309 in FIG. 3, the use of encryption for asymmetric key 127 with an asymmetric ciphering algorithm 219 is optional, and the symmetric key 127 could be sent in a form where encryption is applied at the data-link layer according to standards for the wireless network 102. Other possibilities exist as well for module 101 to securely receive asymmetric key 127 in a step 309 without departing from the scope of the present invention. As described above in connection with a step 302 b, in exemplary embodiments, the module 101 receives the symmetric key 127 after the MNO 104 authenticates or verifies that a user 113 or M2M service provider 115 is associated with module 101, and until the receipt of the symmetric key 127 the ciphertext 208 b cannot be feasibly decrypted.

After a step 309, a module 101 with an eUICC 107 can use the symmetric key 127 to decrypt ciphertext 208 b, where ciphertext 208 b can include the second key K 204 a. A module 101 or eUICC 107 can use a key K deciphering algorithm 207 with input from the received symmetric key 127 and the ciphertext 208 b from profile 107 d to output a plaintext second key K 204. Although not illustrated in a step 207 in FIG. 3, but as illustrated in a step 207 in FIG. 2a, a module 101 can use an eUICC 107 to also decrypt a second network module identity 209 a for the second key K 204 using the symmetric key 127. The second network module identity 209 a can be recorded in the ciphertext 208 b. The second network module identity 209 a can be different than the first network module identity 202, such as a different number or value for an IMSI. The second network module identity 209 a can be the same length as the first network module identity 202. The use and operation of a key K deciphering algorithm 207 is also depicted and described in connection with FIG. 2a and FIG. 2e above.

The module 101 or eUICC 107 can record the plaintext second key K 204 in a nonvolatile memory such as, but not limited to, flash memory 101 w such that the plaintext second key K 204 remains available to module 101 after power or a battery 101 k is removed from module 101. The plaintext second key K 204 could also be recorded in a protected memory within module 101, such that the operating system 101 h or CPU 101 b may prevent read or write access to the protected memory by other processes than the eUICC 107. In other words, with a protected memory, other applications such as, but not limited to, applications that are downloaded from an "app store" or equivalent and installed by end users on the module 101 may be prevented by the operating system 101 h from having access to the plaintext second key K 204 recorded in the protected memory.

In another embodiment, a module 101 may optionally not store the plaintext second key K 204 in nonvolatile memory, such that the second key K 204 continues to be recorded for a long-term basis only as ciphertext 208 b in a nonvolatile memory such as flash 101 w. The module 101 could perform a key

K deciphering algorithm 207 each time a plaintext secondkey K 204 is needed for authentication purposes, including related key derivation of a CK and IK plus other derived keys. In this manner (by storing the secondkey K 204 in ciphertext 208 b in module 101) a plaintext secondkey K 204 may not be (i) stored in module 101 for a relatively long time such as several hours or longer, and also (ii) recorded outside a nonvolatile memory.

In another embodiment, (A) the plaintext secondkey K 204 is recorded only in a volatile memory within CPU 101 b such as a register or cache memory, where access to the register or cache memory is limited to the eUICC 107, and (B) after a successful authentication using the secondkey K 204, such as, but not limited to, a second authentication 311 below, the plaintext secondkey K 204 is flushed from the register or cache memory within CPU 101 b. In this manner, after (A) a first time that module 101 conducts a step 207 to obtain a plaintext secondkey K 204 and the module 101 completes a full power cycling, then (B) the plaintext secondkey K 204 may not be recorded in any of a volatile memory, a non-volatile memory, or a protected memory within module 101 (but module 101 could record an encrypted secondkey K 204 a in a ciphertext 208 b).

For the embodiments where the secondkey K 204 is not recorded as plaintext in a nonvolatile memory within module 101, the module 101 can perform a step 207 with a ciphertext 208 b recorded in a nonvolatile memory a second time to process or obtain the plaintext secondkey K 204. In other words, the secondkey K 204 can be recorded on a long-term basis as ciphertext 208 b for eUICC 107 within module 101, in an exemplary embodiment, thereby increasing the security of the secondkey K 204. In this case, either (i) the symmetric key 127 could be recorded in a nonvolatile memory 101 w in order to allow decrypting of the ciphertext 208 b, or (ii) the module 101 could receive the symmetric key 127 a second time by conducting a step 309 a second time. The module 101 can reconnect with the wireless network 102 and the MNO 104 using the first network identity 202 and the first key K 203 a second time, after the module 101 has already received the symmetric key 127 a first time. The MNO 104 may optionally authenticate the user 113 or M2M service provider 115 a second time such as a second step 308 b (before sending the symmetric key 127 a second time) in order to confirm a second use of the first key K 203 is authorized.

After a module 101 with an eUICC 107 processes a key K deciphering algorithm 207 to obtain a plaintext secondkey K 204, the module 101 can connect with the wireless network 102 and mobile network operator 104 using the second network module identity 209 and the second network key 204. The module 101 using a network application 101 x could send a second attach message 305 with the second network module identity 209. In another embodiment, the module 101 could send the second attach message 305 with the first network module identity 202, and in this case the MNO 104 could record from the previous steps 302 b and 308 b that a key K associated with the first network module identity 202 should change to the secondkey K 204.

But, given existing deployed infrastructure and systems for a mobile network operator 104, the use of two different keys K with the same network module identity may be more difficult to support, and for this case and with preferred embodiments, the module 101 attaches with the MNO 104 the second time with the second network module identity 209 that has been deciphered from (i) ciphertext 208 b in a step 207 above, or (ii) ciphertext 208 a in a step 206 above. The second attach message 305 can be equivalent to the first attach message 305, but with a change of module 101 sending the second network module identity 209. With a 4G LTE network, the second attach message 305 could comprise a radio resource connection request message, or a similar message could be utilized with other wireless networking standards as well, such as LTE Advanced or WiMAX. An attach message such as 305 FIG. 3 could also comprise module 101 using a globally unique temporary identity (GTUI) that can be associated with the second network module identity 209. Other possibilities exist as well for the format or structure of an attach message 305 without departing from the scope of the present invention.

After sending the second attach message 305, the module 101 with an eUICC 107 can conduct a second authentication 310 with the mobile network operator 104. The module 101 and eUICC 107 could take the equivalent steps as the first authentication 304 depicted and described in this FIG. 3, but with a difference of using the second network module identity 209 and the secondkey K 204. In a second authentication 310, the mobile network operator 104 could send the module 101 a second RAND value 118 through the wireless network 102. A server 105 associated with MNO 104, such as, but not limited to, a HSS could have previously processed an authentication vector 117 comprising at least (i) the second RAND value 118, (ii) a network authentication token AUTN and sequence number (not shown), and (iii) a response value RES 119 for the second network module identity 209 and the secondkey K 204. The server 105 or HSS associated with the MNO 104 could send the authentication vector 117 to a server or MME that module 101 communicates with through the wireless network 102. The module 101 could receive the second RAND 118 using the network application 101 x, and forward the second RAND 118 to the eUICC 107. The communication steps between a network application 101 x and an eUICC 107 in FIG. 3 could also use the steps depicted and described in connection with FIG. 1 e.

At a step 311, the eUICC 107 could calculate the second RES 119 using (i) the second RAND 118 received and (ii) the secondkey K 204. After receiving the exemplary second RAND 118 message, in order to conduct a second authentication 310, module 101 using an eUICC 107 could take steps to demonstrate to MNO 104 that module 101 has access to the same secondkey K 204 as recorded by the MNO 104 in an authentication vector 117. The MNO could record the secondkey K 204 in an authentication vector 117 a step 302 a or step 302 b above. Module 101 can properly respond to a challenge/nonce (such as a second RAND 118) in a message digest authentication by sending a secure hash value calculated using (i) the challenge/nonce and (ii) the secondkey K 204. The secure hash value can comprise the second RES 119. In exemplary embodiments, the eUICC 107 and wireless network 102 could use algorithms specified in ETSI TS 135 205-209, as well as subsequent and related standards, in order for module 101 using eUICC 107 to (i) calculate a secure hash value, and (ii) process related steps for a second authentication 310. After processing a second RES 119 in a step 311 using the secondkey K 204, the eUICC 107 could send the second RES 119 to the network application 101 x in module 101. Module 101 could then send the second RES 119 to the mobile network operator 104 using the wireless network 102, as depicted in FIG. 3 and thereby complete a second authentication step 310 for the module 101. In an exemplary embodiment, as depicted in FIG. 1 f above, the eUICC 107 could include an IP address 106 c with an interface identifier 106 e associated with the eUICC 107, and in this case the module 101 could send the second RES 119 value from the eUICC 107 to the MNO 104 through the wireless network 102.

At a step 312, the mobile network operator can receive the second RES 119 from the module 101 using the wireless network 102. A server 105 for the mobile operator network 104 associated with the wireless network 102 could compare the received second RES 119 with an internally recorded RES 119. The server 105 could receive an authentication vector 117 comprising at least the second RAND 118, second RES 119, and AUTN token for the second network module identity 209 before sending the second RAND 118 in a step 310 above. If the received second RES 119 matches the internally stored second RES 119 value, the wireless network 102 and mobile network operator 104 can consider or process that the module 101 is authenticated for a step 312. The wireless network 102, the MNO 104, and the module 101 can take subsequent steps (not shown) for the module 101 to access the IP network 111, including allowing module 101 to place and receive telephone calls and/or access the public Internet.

In an exemplary embodiment that utilizes the steps illustrated in FIG. 3, the first key K 203 can comprise a null value or the number zero, which is contemplated in standards and supported by commercial wireless networks 102 in order to support emergency services for a module 101 without a valid UICC or eUICC. The MNO 104 and wireless network 102 can provide limited access to the IP network 111, such that a user 113 of module 101 with a null or zero value for the first key K 203 could perform steps to authenticate or verify the user 113 identity in a step 308 b. The limited access to the IP network 111 may not include access to the public Internet, but could include access to a server such as a web server for the user 113 to enter identification information. The data-link layer may not be encrypted due to the use of a null value for the first key K 203, but the application or transport layer could secure communication from a web browser on the module 101 to the web server, such as using transport layer security (TLS). Other possibilities exist as well for ciphering or securing data at the application or transport layer in step 308 b to authenticate a user 113 without encryption at the data-link layer (such as without encryption by the wireless network 102 due to a null value for first key K 203). In this embodiment where the first key K 203 comprises a null or zero value, after authentication of user 113 or M2M service provider 115 in a step 308 b, the second key K 204 used with a second authentication 310 can comprise a regular key K such as a non-null value or a random number.

FIG. 4

FIG. 4 is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments. The processes and operations, described below with respect to all of the logic flow diagrams may include the manipulation of signals by a processor and the maintenance of these signals within data structures resident in one or more memory storage devices. For the purposes of this discussion, a process can be generally conceived to be a sequence of computer-executed steps leading to a desired result.

These steps usually require physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, compared, or otherwise manipulated. It is convention for those skilled in the art to refer to representations of these signals as bits, bytes, words, information, elements, symbols, characters, numbers, points, data, entries, objects, images, files, or the like. It should be kept in mind, however, that these and similar terms are associated with appropriate physical quantities for computer operations, and that these terms are merely conventional labels applied to physical quantities that exist within and during operation of the computer.

It should also be understood that manipulations within the computer are often referred to in terms such as listing, creating, adding, calculating, comparing, moving, receiving, determining, configuring, identifying, populating, loading, performing, executing, storing etc. that are often associated with manual operations performed by a human operator. The operations described herein can be machine operations performed in conjunction with various input provided by a human operator or user that interacts with the computer.

In addition, it should be understood that the programs, processes, methods, etc. described herein are not related or limited to any particular computer or apparatus. Rather, various types of general purpose machines may be used with the following process in accordance with the teachings described herein.

The present invention may comprise a computer program or hardware or a combination thereof which embodies the functions described herein and illustrated in the appended flow charts. However, it should be apparent that there could be many different ways of implementing the invention in computer programming or hardware design, and the invention should not be construed as limited to any one set of computer program instructions.

Further, a skilled programmer would be able to write such a computer program or identify the appropriate hardware circuits to implement the disclosed invention without difficulty based on the flow charts and associated description in the application text, for example. Therefore, disclosure of a particular set of program code instructions or detailed hardware devices is not considered necessary for an adequate understanding of how to make and use the invention. The inventive functionality of the claimed computer implemented processes will be explained in more detail in the following description in conjunction with the remaining Figures illustrating other process flows.

Further, certain steps in the processes or process flow described in all of the logic flow diagrams below must naturally precede others for the present invention to function as described. However, the present invention is not limited to the order of the steps described if such order or sequence does not alter the functionality of the present invention. That is, it is recognized that some steps may be performed before, after, or in parallel other steps without departing from the scope and spirit of the present invention.

The processes, operations, and steps performed by the hardware and software described in this document usually include the manipulation of signals by a CPU or remote server and the maintenance of these signals within data structures resident in one or more of the local or remote memory storage devices. Such data structures impose a physical organization upon the collection of data stored within a memory storage device and represent specific electrical or magnetic elements. These symbolic representations are the means used by those skilled in the art of computer programming and computer construction to most effectively convey teachings and discoveries to others skilled in the art.

At step 401, a module 101 can connect with a first wireless network 102. The first wireless network 102 could comprise a public land mobile network, a local area network such as WiFi, or the use of white-space spectrum. The module 101 could connect with the first wireless network 102 in order to obtain access to IP network 111 which could comprise the public Internet, although the IP network 111 could comprise a private network in some embodiments. Although not depicted in FIG. 4, a step 401 could also comprise the module 101 connecting to a wired network through a USB interface 101 v. Upon conclusion of a step 401 the module 101 can use an IP address such as IP address 106 b in FIG. 1f in order to communicate with an eUICC subscription manager 109. As illustrated in FIG. 1f, in an exemplary embodiment the eUICC 107 could also have an IP address 106 c after a step 401, although the use of an IP address for eUICC 107 is not required and the module 101 can be associated with one IP address for all external communications.

The module 101 can then use a step 205 in order to receive an eUICC profile 107 c. The eUICC profile 107 c could be received from the eUICC subscription manager 109 using the wireless network 102 and/or IP network 111 from a step 401 above. The module 101 could record the received eUICC profile 107 c with the eUICC 107, including sending the eUICC profile 107 c to the eUICC 107 or sharing memory 101 e or 101 w between the eUICC 107 and a network application 101 x. The module 101 could use a network application 101 x in order to receive the eUICC profile 107 from the eUICC subscription manager in a step 205, as depicted and described in connection with FIG. 3. The module 101 with an eUICC 107 could then decrypt the profile 107 c in a step 206 using an eUICC profile key 107 b. The eUICC profile key 107 b could be recorded with an eUICC 107 before a step 206. The module 101 and/or eUICC 107 could receive the eUICC profile key 107 b using a step 303 as depicted and described in connection with FIG. 3. The eUICC profile key 107 b could be received using a key exchange, such as a Diffie-Hellman key exchange or an ECDH key exchange. Or, the eUICC profile key 107 b could be recorded with

the eUICC 107 by a module manufacturer. Other possibilities exist as well for a module 101 to record an eUICC profile key 107 *b* before a step 206 without departing from the scope of the present invention. A module 101 and/or an eUICC 107 could use a profile deciphering algorithm 206 in a step 206, as depicted and described in connection with FIG. 2 and FIG. 2b. Upon conclusion of a step 206, a profile 107 *d* could be recorded in an eUICC 107.

In a step 402, a module 101 can then select and activate the profile 107 *d* from a step 206 in order to connect with a second wireless network 102. A module 101 could take several possible steps in order to select and activate the profile 107 *d*. A module 101 could use radio 101 *z* to search for radio beacons from base stations 103 for wireless networks 102 surrounding the module 101, and upon finding the second wireless network 102 to connect with, the module 101 could select the profile 107 *d*. The profile 107 *d* could include values in the set of network parameters 201 that match or conform with values transmitted by the wireless network 102, such as using the same mobile country code (MCC) and mobile network code (MNC) as recorded in the profile 107 *d*. A module 101 could receive an instruction from an eUICC subscription manager 109 in order to activate the profile 107 *d*, where the instruction could be received through the first wireless network 102 in a step 401 above.

In another embodiment, a module 101 or eUICC 107 could query the eUICC subscription manager 109 through the first wireless network 102 before activating the profile 107 *d* in a step 402. Commercial business arrangements among the user 113 of module 101, the eUICC subscription manager 109, and the mobile network operator 104 can determine the timing for activating a profile 107 *d* for a module 101 with an eUICC 107 in a step 402, such as a user 113 entering a new contract for service with a MNO 104 for the profile 107 *d*. As contemplated herein and throughout the present invention, an activated profile 107 *d* can comprise a selected and enabled network access application state as illustrated in Figure D.1 of SI TS 103 383 v.2013-02 for the activated profile 107 *d*. Other possibilities exist as well for a module 101 to activate a profile 107 *d* in a step 402 without departing from the scope of the present invention.

In a step 304 in FIG. 4, a module 101 using eUICC 107 can conduct a first authentication 304 with the second wireless network 102, using the first key *K* 203 recorded in the activated profile 107 *d*. The module 101 could also send the first network module identity 202 from a profile 107 *d* to the mobile network operator 104 in a step 304 in FIG. 4. The second wireless network 102 in a step 304 in FIG. 4 can be associated with a mobile network operator 104. The use of a first authentication 304 is also depicted and described in connection with FIG. 3 above. As noted in a first authentication 304, the first key *K* 203 could comprise a key with a null value in an exemplary embodiment, although a random number could be used for a first key *K* 203 as well. As depicted in FIG. 4, the steps 401 through 304 could comprise substeps within a step 403. The combined substeps comprising a step 403 can be used by a module 101 in exemplary embodiments including an embodiment illustrated in FIG. 6 below.

Although not depicted in FIG. 4, the mobile network operator 104 can conduct a separate step 308 *b* to authenticate module 101 or a user 113 of module 101 using a second factor after a step 304. As described in a step 308 *b* above, the second factor could comprise verifying or authenticating an identity of a user 113 associated with module 101. Note that the authentication of a user 113 can be conducted through the module 101 accessing a server 105 or a web page through the P-network 111 via the second wireless network 102 after the first authentication 304 using the first key *K* 203 (including embodiments where the first key *K* 203 comprises a null value).

In a step 309, the module 101 can receive a key from the second wireless network. The key in a step 309, as depicted in FIG. 3 above, can comprise a symmetric key 127 in order to decrypt a ciphertext 208 *b* within profile 107 *d*. As also contemplated and described in connection with a step 309 in FIG. 3, the key could comprise a module 101 receiving a ciphertext that includes an asymmetric key 127 that has been ciphered with a key ciphering algorithm 216 using an asymmetric ciphering algorithm 219 and the eUICC public key 214, as illustrated in FIG. 2e. For a key ciphering algorithm 216 used with a step 309, (i) the symmetric key 127 can comprise the plaintext (as opposed to the eUICC profile key 107 *b* depicted in FIG. 2e), and (ii) the MNO 104 could operate the key ciphering algorithm 216 instead of the eUICC subscription manager 109 depicted. In this embodiment of a step 309, a module 101 and/or an eUICC 107 could receive the key in the form of a ciphertext of symmetric key 127 in a step 309 and decrypt the ciphertext of symmetric key 127 with the eUICC private key 215 in order to read a plaintext symmetric key 127.

In a step 207 in FIG. 4, the module 101 and/or eUICC 107 can decrypt the ciphertext 208 *b* with the second key *K* 204 *a* using the symmetric key 127. The module 101 can use a key *K* deciphering algorithm 207 as depicted and described in connection with FIG. 2c above in order to read and record a plaintext second key *K* 204 from the ciphertext 208 *b* in the profile 107 *d*, where the profile 107 *d* was previously decrypted and recorded using a step 206 above. As depicted in FIG. 2a, the ciphertext 208 *b* can also include a second network module identity 209 *a*, so the eUICC 107 can also read the plaintext second network module identity 209 *a* in a step 207, if a second network module identity 209 *a* is included in a ciphertext 208 *b*. In an exemplary embodiment, the second plaintext key *K* 204 is recorded in a protected, nonvolatile memory such as, but not limited to, flash memory 101 *w*. In this embodiment, the protected nonvolatile memory could comprise a memory address designated by the module 101, CPU 101 *b*, operating system 101 *h*, a module program 101 *i*, or the eUICC 107 as a memory address that can only be written and read by the eUICC 107. Other possibilities exist as well to those of ordinary skill in the art for a plaintext second key *K* 204 to be recorded in a protected, nonvolatile memory in a step 207 without departing from the scope of the present invention.

In another embodiment, as described in a step 207 in FIG. 3, the module 101 could record the encrypted second key *K* 204 *a* in a nonvolatile memory, along with a symmetric key 127 (or an encrypted symmetric key 127 ciphered by a key ciphering algorithm 216). The module 101 or eUICC 107 could decrypt the encrypted symmetric key 127 in order to decrypt the ciphertext 208 *b* that contains the second key *K* 204 *a* each time the module 101 or eUICC 107 needs to read a plaintext second key *K* 204 for an conducting an authentication step 310, plus the subsequent derivation of additional keys such as CK and IK, K_{asme}, K_{upenc}, etc. using the plaintext second key *K* 204 and a RAND 118 value.

After reading a plaintext second key *K* 204 from a ciphertext 208 *b* in a step 207 using the symmetric key 127, the module 101 and/or eUICC 107 can conduct a second authentication 310 step using the plaintext second key *K* 204, in order to authenticate with the second wireless network 102. The second wireless network 102 can comprise the same wireless network 102 the module 101 communicates with in a step 304 above. The use of a plaintext second key *K* 204 in a second authentication 310 step is depicted and described in connection with FIG. 3. Although not illustrated in FIG. 4, the module 101 could send a detach message or equivalent to temporarily disconnect from the second wireless network 102 after a step 309 and before a step 310 illustrated in FIG. 4. A step 310 can comprise the module 101 sending a radio resource connection request to the second wireless network 102 with a network module identity associated with the second key *K* 204. A step 310 can be completed by a module 101 and/or an eUICC 107 sending a RES 119 value calculated using (i) a RAND 118 received and (ii) the second key *K* 204.

Although not illustrated in FIG. 4, after a step 310 by a module 101 and/or an eUICC 107, the MNO 104 could verify the RES 119 and then the module 101 and the wireless network 102 associated with the MNO 104 could take subsequent steps for a module 101 to have access to the IP network 111 including the public Internet. The module 101 and/or eUICC 107 could derive session keys (such as, but not limited to a key CK) for encrypting data through the wireless network using a RAND 118 received in a step 310 and the second key K 204, and the module 101 and/or eUICC 107 could also derive an integrity key for a session (such as, but not limited to, an integrity key IK). Using an authenticated module 101 from a step 310, the MNO 104 can meter services rendered to a module 101 after a step 310 in order to bill or invoice a user 113 or M2M service provider 115.

FIG. 5a

FIG. 5a is a graphical illustration of a public key, private key, and a key derivation algorithm, in accordance with exemplary embodiments. An eUICC 107 within a module 101 can include an eUICC private key 215, which can be associated with an eUICC public key 214. The eUICC private key 215 and eUICC public key 214 can comprise a public key infrastructure (PKI) key pair for eUICC 107. The MNO 104 can record the eUICC public key 214 along with an eUICC identity 107a, such that the MNO 104 can properly associate one of a plurality of eUICC public keys 214 with the proper eUICC 107. Although not illustrated in FIG. 5a, a MNO 104 could record the eUICC public key 214 and an associated eUICC identity 107a in a database. The MNO 104 could receive the eUICC public key 214 and the eUICC identity 107a from an eUICC subscription manager 109 through an IP network 111 in a step 302a or step 302b of FIG. 3. The use of, source, and additional details regarding an eUICC public key 214 and eUICC private key 215 are also depicted and described in connection with FIG. 2d above.

The mobile network operator 104 could also be associated with an MNO private key 501 and an MNO public key 502, which could comprise a PKI key pair for the mobile network operator. The mobile network operator 104 could process or derive the PKI key pair using steps and algorithms equivalent to the steps and algorithms for an eUICC 107 to obtain the eUICC public key 214 and eUICC private key 215. The PKI keys depicted in FIG. 5a could be processed using RSA algorithms or elliptic curve cryptography (ECC) algorithms, and other possibilities exist as well for the format of PKI keys without departing from the scope of the present invention. The public keys in FIG. 5a can comprise keys recorded in an X.509 certificate, although the use of an X.509 certificate with public keys 214 and 502 are not required. The public key 214 and 502 in the form of an X.509 certificate can optionally be signed by a certificate authority. As illustrated in FIG. 5a, the mobile network operator public key 502 can be recorded in the eUICC profile 107d. The MNO 104 could send the MNO public key 502 to the eUICC subscription manager 109 in a step 302a or 302b depicted and described in FIG. 3 and the eUICC subscription manager 109 could include the MNO public key 502 in the profile 107d. An eUICC profile 107d could also include the additional data for an eUICC profile 107d as depicted and described in FIG. 2a, in addition to the MNO public key 502.

As illustrated in FIG. 5a, the MNO 104 and eUICC 107 can both record a key derivation algorithm 503. Exemplary key derivation algorithm 503 could support a Diffie-Hellman key exchange, an Elliptic Curve Diffie-Hellman (ECDH) key exchange (ECDH), or similar algorithms for each node to mutually derive a key using public and private keys. For embodiments where (A) eUICC public key 214, eUICC private key 215, MNO public key 502, and MNO private key 501 utilize (i) elliptic curve cryptography (ECC) and (ii) a common, shared elliptic curve, then (B) key derivation algorithm 503 in FIG. 5a can comprise an algorithm for conducting an ECDH key exchange. The use of an ECDH key exchange was also described and contemplated between eUICC subscription manager 109 and an eUICC 107 in step 303 in FIG. 3 above. For embodiments where a key derivation algorithm 503 supports a Diffie-Hellman key exchange, the key derivation algorithm 503 could record a multiplicative group of integers modulo p, where p is prime, and g is a primitive root mod p. In exemplary embodiments, p can be sufficiently large, such as, but not limited to, and exemplary prime number of at least 250 digits, and g can be a small number, such as, but not limited to, the number 5. In exemplary embodiments, additional values pertaining to the operation of key derivation algorithm 503 can be transferred between two nodes using a token 506 described in a FIG. 5b and FIG. 5c below.

FIG. 5b

FIG. 5b is a graphical illustration of deriving a second key K using public keys, private keys, and a key derivation algorithm, in accordance with exemplary embodiments. A mobile network operator 104 could process a MNO key exchange algorithm 504 in order to output or determine a second key K 204. A module 101 with an eUICC 107 could process an eUICC key exchange algorithm 505 in order to output or determine the same second key K 204. The MNO key exchange algorithm 504 and the eUICC key exchange algorithm 505 could include a key derivation algorithm 503, and a key derivation algorithm 503 is also depicted and described in connection with FIG. 5a above. The MNO 104 and module 101 could share or communicate a key exchange token 506 in order to operate the key exchange algorithm 505. In this manner, a module 101 with an eUICC 107 and a mobile network operator 104 could mutually derive or share the second key K 204 without MNO 104 transmitting or sending the second key K 204, even in an encrypted form such as a second key K 204a in a ciphertext 208b, to either (i) eUICC subscription manager 109 in a step 302a or step 302b, or (ii) to a module 101 in a profile 107c.

For a MNO key exchange algorithm 504, a mobile network operator 104 using a server 105 could input the mobile network operator private key 501, the eUICC public key 214, and a key exchange token 506 into a key derivation algorithm 503 in order to output the second key K 204. Note that the key derivation algorithm 503 in both a MNO key exchange algorithm 504 and an eUICC key exchange algorithm 505 can include additional or separate processing steps than those contemplated in a Diffie-Hellman key exchange and an ECDH key exchange. Additional steps than those contemplated in a Diffie-Hellman key exchange or ECDH key exchange for a key derivation algorithm 503 include transforming key output by these key exchange protocols into a key length and format compatible and suitable for a key K for use with wireless networks. In key derivation algorithm 503, the output of a Diffie-Hellman key exchange and an ECDH key exchange could be input into a secure hash algorithm, such as SHA-256, which could then be truncated to select a 128 bit second key K 204 using a key derivation algorithm 503. For a MNO key exchange algorithm 504, the security key exchange token 506 can depend upon the algorithm used in a key derivation algorithm 503.

For embodiments where key derivation algorithm 503 comprises a Diffie-Hellman key exchange, the key exchange token 506 can comprise integer values of p and g. Or, with a Diffie-Hellman key exchange the security key exchange token 506 sent from a MNO 104 could comprise a value equal to $g(\text{circumflex over ()})^a \text{ mod } p$ where (x) the values p and g have been previously shared between MNO 104 and eUICC 107, and (y) the value "a" can comprise the MNO private key 501. A security key exchange token 506 received by MNO 104 for input into a key derivation algorithm for eUICC 107 could comprise a value of $g(\text{circumflex over ()})^b \text{ mod } p$, where b comprises the eUICC private key 215. For embodiments where key derivation algorithm 503 comprises an ECDH key exchange, the key exchange token 506 can be a common base point G. The base point G could also be (i) recorded in an eUICC profile 107d, or (ii) sent from a mobile network operator 104 to module 101, or (iii) sent from the module 101 to the mobile network operator 104. Other algorithms besides an ECDH or Diffie-Hellman key exchange can be utilized as well at step 503, including a key exchange according to the American National Standards

Institute (ANSI) standard X-9.63, and a key exchange token 506 could include a number or value associated with these other algorithms for key derivation algorithm 503.

For an eUICC key exchange algorithm 505, a module 101 with an eUICC 107 could input the eUICC private key 215 and the mobile network operator public key 502 into a key derivation algorithm 503. Note that the input into the key derivation algorithm 503 could also optionally include a key exchange token 506. The key derivation algorithm 503 in an eUICC key exchange algorithm 505 could accept the input and output the second key K 204. The key derivation algorithm 503 in an eUICC key exchange algorithm 505 could be equivalent to the key derivation algorithm 503 in a MNO key exchange algorithm 504 described above. The key exchange token 506 in an eUICC key exchange algorithm 505 could comprise a value similar to the key exchange token 506 used in a MNO key exchange 504 described above. In a Diffie-Hellman key exchange for a key derivation algorithm 503 in an eUICC key exchange algorithm 505, the key exchange token 506 can comprise a value of either (i) integers p and g as described in a MNO key exchange 504, or (ii) number $g(\text{circumflex over } ())a \bmod p$. In an ECDH key exchange for a key derivation algorithm 503 in an eUICC key exchange algorithm 505, the key exchange token 506 can comprise a base point G . A key derivation algorithm 503 can output a second key K 204. Other possibilities exist as well for the use of PKI keys and tokens in key exchange algorithms for those of ordinary skill in the art without departing from the scope of the present invention.

FIG. 5c

FIG. 5c is a simplified message flow diagram illustrating an exemplary system with exemplary data sent and received by a module with an eUICC, in accordance with exemplary embodiments. System 500 can include an eUICC subscription manager 109, an IP network 111, a mobile network operator 104, a mobile device 101. A module 101 can include a network application 101x and an eUICC 107. The operation of a system 500 can be similar to a system 300 in FIG. 3, except for the steps noted in this FIG. 5c where different steps can be taken than those within a FIG. 3. As depicted for a system 500 in FIG. 5c, like numerals for steps and messages for a system 500 in FIG. 5c can comprise like steps and messages within a FIG. 3. Different numerals discussed below can comprise different steps or messages for a system 500. Many of the same steps common for a system 500 in FIG. 5c and a system 300 in FIG. 3 will be summarized in this FIG. 5c, while differences between the two systems (including the use of different numerals for different steps or messages) are described in more detail herein. As described in a step 302a and 302b in FIG. 3, a mobile network operator 104 can send the eUICC subscription manager 109 information for a profile 107d in a step 302a or 302b, where the information can include the network parameters 201, the first network module identity 202, and the first key K 203. The listed exemplary data for a profile 107d from the previous sentence are also discussed for a profile 107d in FIG. 2a.

For a step 507 in a system 500, the MNO 104 can omit sending an encrypted second key K 204a in a ciphertext 208b within the data for the profile 107d. In other words, the profile 107d can omit the second key K 204 in either a plaintext or ciphertext form after a step 507 in a system 500. The second key K 204 for a module 101 with eUICC 107 can be derived by a mobile network operator 104 in a MNO key exchange algorithm 504 and an eUICC key exchange algorithm 505 below in FIG. 5c. Thus, in an embodiment illustrated in FIG. 5c, the second key K 204 for a second authentication 310 does not need to be transferred to the eUICC subscription manager 109 from MNO 104 for the eUICC subscription manager 109 to include in a profile 107d. Similarly, in a system 500, the second key K 204 does not need to be transferred to the eUICC 107 in a profile 107c. In embodiments where (x) the MNO sends network access credentials such as the first and second network module identities 202 and 209a and a first key K 203 are sent in a step 302b, then (y) a step 507 to omit the sending of the second key K 204 could take place with a step 302b instead of the step 302a as depicted. The MNO 104 can send the first and second network module identities 202 and 209a and a first key K 203 in a step 302a or a step 302b to the eUICC subscription manager 109. The MNO 104 can send to the eUICC subscription manager 109 the first and second network module identities 203 and 209a and a first key K 203 in a profile 107d in a step 302a or 302b, and the eUICC subscription manager 109 could receive the first and second network module identities 202 and 209a and a first key K 203 in a step 302a or a step 302b. Other possibilities for combinations of data sent from a MNO 104 to an eUICC subscription manager 109 in a step 302a, 302b, and 507 without departing from the scope of the present invention.

As depicted in FIG. 5c, an eUICC 107 in module 101 could perform steps 301, then step 205 to receive a profile 107c, then receive an eUICC profile key 107b, and then convert the profile 107c into a profile 107d using the eUICC profile key 107b in a step 206. The eUICC profile key 107b could also be (i) ciphered with a key ciphering algorithm 216, sent from the eUICC subscription manager 109 as an encrypted eUICC profile key 218, (ii) and then deciphered by a module 101 and/or eUICC 107 with a step 217, as described in connection with FIG. 2a above. The module 101 and/or an eUICC 107 could (i) receive an encrypted eUICC profile key 107b in the form of a key 218 and (ii) use a key deciphering algorithm 217 to decrypt the encrypted eUICC profile key 107b in order (iii) to read a plaintext eUICC profile key 107b and then (iv) use the plaintext eUICC profile key 107b to decrypt the ciphertext 208a.

As depicted in FIG. 5c, after a module 101 sends an eUICC identity 107a and receives an eUICC profile 107c in a step 205, the module 101 can conduct a step 206 in order to decrypt a ciphertext 208a that can include a first key K 203 using an eUICC profile key 107b. For the embodiments contemplated in FIG. 5c, where the second key K 204 can be derived or determined using a key exchange in steps 504 and 505 below, the second network module identity 209a can be included in the ciphertext 208a (as opposed to being included in the ciphertext 208b as depicted in FIG. 2a). One reason can be that a ciphertext 208b can be omitted from an eUICC profile 107d in embodiments where the second key K 204 can be mutually derived by the eUICC 107 and the MNO 104, so there may be no need to include a separate ciphertext 208b within the eUICC profile 107d.

After reading a first network module identity 202 and the first key K 203, the module 101 can conduct a first authentication 304. Note that the first key K 203 can comprise key with a null value, as contemplated in wireless network 102 standards which support the use of emergency services where a module 101 may not include a valid first key K 203. In this case where the first key K 203 comprises a null value, the use of a ciphertext 208a can also be optionally omitted, such that the receipt of an eUICC profile key 107b and the use of a ciphertext 208a could also be optionally omitted and a profile 107c could include plaintext for the first key K 203 and network module identity 202. As depicted and described in connection with FIG. 3a module 101 and MNO 104 could conduct a first authentication step 304 in order to authenticate the module 101 using the first key K 203. The first key K could comprise a non-null value in exemplary embodiments. A step 306 to calculate a first RES 119 value using the first key K 203 from a profile 107d could be included in a first authentication step 304.

The mobile network operator 104 could compare the first received RES 119 with a recorded RES 119 in order to authenticate the module 101 with the eUICC 107 in a step 308a. A mobile network operator 104 can authenticate the module 101 using a step 308a in order to provide access to the IP network 111, and the access to the IP network 111 can be limited (such as, but not limited to excluding access to the public Internet after a step 308a).

The module 101 could use access to the limited or restricted P network 111 in order for a user 113 of module 101 to conduct an authentication with the mobile network operator 104 using a second factor, as described in step 308 b in FIG. 3.

After authenticating the module 101 with the first network module identity 202 and the first key K 203 in a step 308 a, the mobile network operator 104 could authenticate a user 113 or verify a M2M service provider 115 is associated with the module 101 in a step 308 b. The authentication of a user 113 or M2M service provider 115 in a step 308 b could comprise authenticating module 101 and/or eUICC 107 with a second factor, where the second factor comprises or includes a secure association of a user 113 or M2M service provider 115 with the module 101. As described in FIG. 3 above, a step 308 b could result in the secure association of an identity for the user 113 or the M2M service provider 115 with an identity of the module 101. After conducting a step 308 b as depicted and described in connection with FIG. 3 above, the MNO 104 can record the second network module identity 209 in the eUICC profile 107 d is associated with a particular user 113 or a particular M2M service provider 115.

In a step 308 b, the MNO 104 can also determine (i) the first network module identity 202 used in step 304 is associated with other identities such as module identity 110, profile identity 107 e, eUICC identity 107 a, and the second network module identity 209. By (i) authenticating a user 113 or (ii) verifying an identity for module 101 is associated with a M2M service provider 115 in a step 308 b, MNO 104 can determine the second network module identity 209 (used in a subsequent authentication step 310) belongs to or is associated with a particular user 113 or M2M service provider 115. In other words, without a separate authentication step 308 b in FIG. 5 and FIG. 3, MNO 104 may not be able to securely determine that the second network module identity 209 from a profile 107 d belongs to a particular user 113 or M2M service provider 115. For embodiments where the module 101 is associated with a M2M service provider 115, then a step 308 b in FIG. 5c could comprise the MNO 104 verifying that an identity received in a first authentication 304 such as, but not limited to, the first network module identity 202 is associated with an M2M service provider 115, such as checking the identity in a list of identities for modules 101 belonging to M2M service provider 115.

After successfully authenticating or verifying an identity of a user 113 or an M2M service provider 115 is associated with module 101 in a step 308 b, MNO 104 could process an MNO key exchange algorithm 504 in order to record a second key K 204 for use in a subsequent second authentication 310 for module 101. The second authentication 310 can use different network access credentials (i) associated with the module 101 and (ii) obtained by module 101 using an eUICC key exchange algorithm 505. Although not illustrated in FIG. 5c, a MNO 104 could obtain the data for processing a MNO key exchange algorithm 504 in several different ways. A MNO 104 could receive the eUICC public key 214 for an MNO key exchange algorithm 504 from either (i) the module 101 or eUICC 107 directly after the first authentication 304 or (i) the eUICC subscription manager 109 in a step 302 b above, where the eUICC subscription manager 109 could record the eUICC public key 214. Other possibilities exist as well for a MNO 104 to receive an eUICC public key 214 associated with an identity for module 101 such as the eUICC identity 107 a. The recording of an eUICC public key 214 with an MNO 104 is also depicted and described in connection with FIG. 5a above.

For a MNO key exchange algorithm 504 in FIG. 5c, the MNO 104 could also input a key exchange token 506 and a MNO private key 501, in addition to the eUICC public key 214, as illustrated in FIG. 5b above. After performing a MNO key exchange algorithm 504 in FIG. 5c, the MNO 104 can record the second key K 204 for the second module identity 209 (which is associated with the first module identity 202 in the profile 107 d). As contemplated for a key exchange token 506 in FIG. 5a and FIG. 5c, the key exchange token 506 could be any of the cases (A) initially processed, derived, or determined by the MNO 104, (B) shared between the MNO 104 and module 101 with the eUICC 107, such as, but not limited to, recording the key exchange token 506 in the profile 107 d, or (C) initially processed, derived, or determined by module 101. FIG. 5c illustrates an embodiment for case (A) with key exchange token 506, where the MNO 104 derives or determines the key exchange token 506 value and subsequently sends the key exchange token 506 value to the module 101 with the eUICC 107. The MNO 104 can send the key exchange token 506 in a message 508, and a network application 101 x for the module 101 can receive the key exchange token 506 in the message 508 and forward the key exchange token 506 to the eUICC 107. For case (A) the MNO 104 can omit sending the key exchange token 506 until after the user 113 or M2M service provider 115 for module 101 has been successfully authenticated or verified in a step 308 b.

In a related embodiment to the embodiment depicted in FIG. 5, for case (B) with key exchange token 506, a separate message 508, to communicate or transfer the key exchange token 506 between the MNO 104 and module 101 after a step 504, can optionally be omitted, since both sides (MNO 104 and module 101) could record the key exchange token 506 before a step 505 by a module 101 with an eUICC 107 below. For case (B), the MNO 104 could send a signal in a message 508 to the module 101 that the authentication step 308 b of a user 113 or an M2M service provider 115 has been successfully completed, and thus module 101 could proceed with an eUICC key exchange algorithm 505 using the recorded key exchange token 506.

For case (C) with key exchange token 506, the eUICC 107 could derive or determine the key exchange token 506 and subsequently send the key exchange token 506 to the MNO in a message 508. In this case (C), the MNO 104 could receive the key exchange token 506 (i) before processing the MNO key exchange algorithm 504, and (ii) using the connection with module 101 from the first authentication 304. For case (C), the MNO 104 can require the successful completion of an authentication step 308 b for a user 113 or M2M service provider 115 before accepting the key exchange token 506 from the module 101.

In another exemplary embodiment step 504 and step 505 can use different values for the key exchange token 506, and both MNO 104 and module 101 can send the tokens 506 in a message 508 to the other node. In exemplary embodiments, a message 508 comprising the key exchange token 506 can be transferred through the P network 111, where access to the P network 111 can be enabled by the first authentication 304 with the first key K 203. Other possibilities exist as well for the transfer of a key exchange token 506 between a MNO 104 and a module 101 with an eUICC 107 for conducting a key exchange without departing from the scope of the present invention.

As depicted in FIG. 5c, a module 101 with an eUICC 107 can conduct an eUICC key exchange algorithm 505 in order to determine or read a second key K 204. As depicted and described for an eUICC key exchange algorithm 505 in FIG. 5b above, the module 101 can input an MNO public key 502, an eUICC private key 215, and the key exchange token 506 into a key derivation algorithm 503 in order to output the second key K 204. Note that the number, value, or sequence of bits for the second key K 204 determined by a MNO 104 in a step 504 can be equal to the number, value, or sequence of bits for the second key K 204 determined by a module 101 with an eUICC 107 in a step 505. The mutual derivation of the second key K 204 by a MNO 104 in a step 504 and a module 101 in a step 505 can be different and superior to conventional technology for either (i) a physical UICC or (ii) an eUICC, since the second key K 204 does not need to be transferred in either physical or electronic form, where the electronic form could include encrypting the second key K 204 into a ciphertext. Supporting the derivation of a second key K 204 as depicted and described herein can be superior to the electronic or physical

distribution of a key K, since a different secondkey K 204 can be utilized by repeating steps 504 and 505 a second time, such as with a different key exchange token 506. In this manner, the secondkey K 204 associated with the second network module identity 209 could be rotated or changed periodically, thereby increasing the security of a system 500 compared to the use of a static, non-changing secondkey K 204 for the lifetime of a module 101 with a profile 107 d.

After a step 505 in FIG. 5c, the subsequent steps and messages for communication between the module 101 and the MNO 104 can be the same or equivalent to those in FIG. 3 after a step 207. In other words, the secondkey K 204 as used by a module 101 and/or eUICC 107 for embodiments in a FIG. 5c can be equivalent or similar to the processing and recording steps depicted and described in FIG. 3 on module 101 with an eUICC 107 reading the second key K 204 in a step 207 in FIG. 3. In a system 500, the module 101 or eUICC 107 could record the secondkey K 204 in a protected, nonvolatile memory as described in step 207 of FIG. 3. Other possibilities exist as well without departing from the scope of the present invention for the location or techniques of storing the secondkey K 204 resulting from step 505.

As depicted and described in connection with FIG. 6 below, the module 101 could record the secondkey K 204 in a volatile memory (and not storing the second key K 204 in nonvolatile memory), including potentially only within a register or cache memory of a CPU 101 b. In this manner, the security of the derived secondkey K 204 can be enhanced, since upon or after power off of a module 101, a third party could not probe or read nonvolatile memory looking for the secondkey K 204. Since a volatile memory could be flushed upon loss of power or other circumstances, MNO 104 and module 101 could repeat the steps 504 and 505, respectively, including the transfer of a key exchange token 506, a subsequent time when a module 101 needs to process or derive a new, subsequent secondkey K 504. In other words, a module 101 can conduct a step 505 with a different key exchange token 506 at a later time after the first instance of step 505 in order to derive a different, subsequent secondkey K 204.

After deriving the secondkey K 204 in a step 505 in FIG. 5c, the module 101 with the eUICC 107 can authenticate with the MNO 104 using the wireless network 102, the second network module identity 209, the secondkey K 204. The module 101 could conduct a second authentication 310 with the mobile network operator using the secondkey K 204, as depicted in FIG. 5c, which is also equivalent to the second authentication 310 depicted in FIG. 3 above. Note that the module 101 could detach or disconnect from the wireless network 102 (i) after a sending/receiving a message 508 with key exchange token 506 and (ii) before sending the exemplary second attach message 303 with the second network module identity 209.

The eUICC 107 within module 101 could use (i) the secondkey K 204 from a step 505, and (ii) a second RAND 118 value from the MNO 104 to calculate a second RES 119 value in a step 311. The eUICC 107 can send the second RES 119 to the network application 101 x, and the module 101 can send the second RES 119 to the mobile network operator 104 through the wireless network 102. The MNO 104 could complete the second authentication in a step 312 by verifying the second RES 119 is correct using (i) the secondkey K 204 derived by the MNO 104 in a step 504 above, and (ii) the second RAND 118 value sent to the module 101. Upon successful authentication using the secondkey K 204, as depicted and described in connection with FIG. 3 the module 101 and MNO 104 could take subsequent steps after a step 312 for the module 101 to have access to the P network 111 and also the public Internet.

In another embodiment contemplated in FIG. 5c, the mobile network operator 104 can send the secondkey K 204 to the module 101 using the wireless network 102 in a message 508. In other words, the exemplary token 506 in FIG. 5c could comprise the secondkey K 204, as opposed to an exemplary key exchange token 506. In this embodiment, the use of a key derivation algorithm 503 in a step 504 could use input of a random number from a random number generator 128 into the key derivation algorithm 503 (instead of PKI keys), and the output could be the secondkey K 204. Or, the key derivation algorithm 503 in a step 504 could simply assign a random number to the secondkey K 204. After a step 308 b and step 504, the mobile network operator 104 could send the secondkey K 204 in a message 508. The secondkey K 204 in a message 508 could be encrypted using a key ciphering algorithm 216. The message 508 with the secondkey K 204 as the token 506 could be received by the module 101 and decrypted using a key deciphering algorithm 217. In another embodiment, the token 506 received by a module 101 could comprise (i) the secondkey K 204 as plaintext at the application layer, but (ii) ciphered at the data-link layer using the first RAND value from a step 304 and the first key K 203. Other possibilities exist as well for a token 506 to comprise a secondkey K 204 without departing from the scope of the present invention.

The order of many of the steps and messages depicted within a system 500 could be changed without departing from the scope of the present invention. For example, a step 504 could also be conducted concurrently with a step 302 b (instead of with a step 308 b), such that a mobile network operator 104 could calculate a secondkey K 204 using a MNO key exchange algorithm 504 at the same time when MNO 104 sends the first network module identity 202 and first key K 203 to the eUICC subscription manager 109. After receiving (i) an eUICC identity 107 a from an eUICC subscription manager 109 and (ii) an eUICC public key 214 in a step 302 b, the mobile network operator 104 can process a MNO key exchange algorithm 504 in order to calculate or process a secondkey K 204.

In an exemplary embodiment, a mobile network operator 104 could receive a list of eUICC public keys 214 and eUICC identities 107 a from an M2M service provider 115 before eUICC subscription manager 109 receives the eUICC identity 107 a in a step 205. The MNO 104 could use the data received from a M2M service provider 115 (including a list of eUICC identities 107 a and eUICC public keys 214) in order to derive the secondkey K 204 using a MNO key derivation algorithm 504 and the key exchange token 506. The MNO 104 could send the key exchange token 506 to an eUICC subscription manager 109 before the eUICC subscription manager 109 participates in a step 205 as illustrated in FIG. 5c, and the eUICC subscription manager 109 could include the key exchange token 506 with the eUICC profile 107 c, such that module 101 could receive the key exchange token 506 in the eUICC profile 107 c.

In this embodiment (which can also comprise a case (B) for the transfer of key exchange token 506 for a message 508 as described above), a module 101 using an eUICC 107 with profile 107 d and key exchange token 506 could potentially derive the secondkey K 204 before a step 308 b, but in preferred embodiments the mobile network operator 104 does not allow the use of the secondkey K 204 until after an authentication step 308 b of a user 113 or M2M service provider 115. In another embodiment, the values for the first network module identity 202 and the second network module identity 209 could be the same or equal, such that the module 101 uses the same network module identity for both first authentication 304 and a second authentication 310. In this case, the MNO 104 can support a change in key K used with the first network module identity 202 from the first key K 203 to the second key K 204. The first key K 203 can be included in a profile 107 d, but the secondkey K 204 can be derived by an MNO 104 using a step 504 and a module 101 using a step 505. Other possibilities exist as well for an MNO 104 and a module 101 to mutually derive a secondkey K 204 for use with an eUICC 107 without departing from the scope of the present invention.

FIG. 6

FIG. 6 is a flow chart illustrating exemplary steps for a module to use an eUICC and authenticate with a wireless network, in accordance with exemplary embodiments. An exemplary system 500 depicted and described in connection with FIG. 5c can also support the repeated derivation of a second key K 204 for a MNO 104 and module 101 with an eUICC 107. The use and support for different second keys K 204 over time can increase security, since the second key K 204 can be securely and periodically rotated, thereby enhancing the security and efficiency of system 500, compared to either (i) physically changing a UICC each time a new key K is desired, or (ii) querying, downloading, and selecting a new profile 107 c or profile 107 d each time the use of a different key K is desired (including steps to communicate and record a second key K 204 in the profile 107 d). In other words, the use of multiple second keys K 204 over time can be accomplished for the same profile 107 d.

A step 403 in FIG. 6 can comprise a module 101 with an eUICC 107 conducting the substeps for a step 403 as depicted and described in connection with FIG. 4. In a step 403, a module 101 could connect with a first wireless network 102, receive an eUICC profile 107 c, decrypt the profile 107 c using an eUICC profile key 107 b, activate the profile 107 d, and authenticate with a second wireless network 102 using a first key K 203 from the profile 107 d. As noted above, other possibilities exist as well for module 101 to record an eUICC profile 107 d, such as the loading of a profile 107 d by a manufacturer, without departing from the scope of the present invention.

After successful authentication of the module 101 at the conclusion of a substep 304 in a step 403, a user 113 associated with the module 101 could conduct an authentication step 308 b with the mobile network operator 104. A step 308 b can be useful for a mobile network operator 104 to authenticate or securely associate (i) a module 101 with (ii) a legal entity contractually responsible for the services used by a module 101. The use of a step 308 b is also described in FIG. 3. Note that module 101 could be associated with an M2M service provider 115 instead of a mobile phone subscriber such as an individual, and in this case the M2M service provider 115 could take steps before a step 308 b in order to inform or confirm with MNO 104 that module 101 with an identity such as module identity 110 or the first network module identity 202 belongs to or is associated with the M2M service provider 115.

In other words, a MNO 104 may not have control over the distribution or recipient of a profile 107 c from an eUICC subscription manager 109 in a step 403, and a user authentication in a step 308 b allows a MNO 104 to confirm, verify, or establish a contractual relationship with a user 113. Business contracts and procedures for a MNO 104 to provide service to a module 101 with an eUICC 107 with profile 107 d could require that a user 113 successfully completes an authentication step 308 b (with example steps described in FIG. 3a above), before the MNO 104 provides service such as voice calls or access to the public Internet. The second factor in a step 308 b can be data communicated between the MNO 104 and the user 113 to confirm an identity of the user 113. Examples of data for the second factor in a step 308 b are described in connection with a step 308 b in FIG. 3. The first factor contemplated in a system 300 or system 500 can be the successful receipt of a RES 119 value in a first authentication 304. Upon conclusion of a step 308 b the MNO 104 could securely determine and record that a module 101 with the first network module identity 202 and/or the second network module identity 209 from the profile 107 d is associated with an authenticated user 113.

The module 101 could then perform a step 508 in order to access a key exchange token 506. As described for a key exchange token 506 in FIG. 5c, the module 101 could receive the token 506 in a step 508 (case A), or the module 101 could send the token 506 in a step 508 (case B). Step 508 can comprise sending or receiving the message 508 from FIG. 5c. The key exchange token 506 could comprise a key exchange token 506 as depicted and described in connection with FIG. 5. Or, as described for a message 508 in FIG. 5c, the key exchange token 506 could comprise the second key K 204, such as the second key K 204 encrypted by MNO 104 with a key ciphering algorithm 216 and decrypted by the module 101 with the eUICC 107 using a key deciphering algorithm 217. The key exchange token 506 at a step 508 could comprise parameters for a key derivation algorithm 503, such as a base point G if elliptic curve cryptography PKI keys are used with MNO public key 502, MNO private key 501, eUICC public key 214, and eUICC private key 215.

In another exemplary embodiment, a key exchange token 506 with a Diffie Hellman key exchange for a key derivation algorithm 503 could comprise a multiplicative group of integers modulo p, where p is prime and g is primitive root mod p. Other possibilities for a key exchange token 506 in a message 508 exist as well without departing from the scope of the present invention, including the use of multiple values and numbers for a key exchange token 506. The key exchange token 506 transfer between MNO 104 and module 101 in a step 508 can use the second wireless network after the module 101 authenticates with the first key K 203, and thus the data-link layer for transfer of the key exchange token 506 could be ciphered using the first key K 203 (where a cipher key for the data-link layer is derived from the first key K 203 and a RAND 118 from a first authentication 304).

A module 101 with an eUICC 107 could then perform a step 505, which could comprise an eUICC key exchange algorithm 505 as depicted in FIG. 5c using (i) the token 506 from a message 508 above, and (ii) the eUICC private key 215 and MNO public key 502. The output from an eUICC key exchange algorithm 505 can comprise the second key K 204. In an exemplary embodiment, the second key K 204 output from the eUICC key exchange algorithm 505 is recorded within a memory of module 101 on a temporary basis. After obtaining and reading the second key K 204 from a step 505, the module 101 can conduct a second authentication 310 with the MNO 104 using the second key K 204. The second key K 204 can be associated with a second network module identity 209, which could be recorded in the profile 107 c and profile 107 d for the eUICC 107 from a step 403 above. Exemplary details and steps for a second authentication 310 using the second key K 204 are depicted and described in connection with FIG. 3 and FIG. 5c above.

After the conclusion of a second authentication 310, the module 101 could have access to the public Internet through the P network 111 of the wireless network 102. After a step 310 and before a subsequent step 601 below, the module 101 could continue using the second key K 204 with the second network identity 209 in many additional repeated steps 310, such that module 101 could use the second key K 204 for an exemplary period of time such as several days or several months, and other possibilities exist as well for the continued use of a second key K 204 after a step 310 and before a step 601 in FIG. 6. For example, a module 101 could repeat a step 311 in a second authentication 310 multiple times with the same wireless network 102 using the same number of value for the second key K 204 during a period of time before a step 601.

At a step 601 in FIG. 6, a module 101 or a MNO 104 could determine if the use of a new second key K 204 is required or preferred. There could be several reasons that a different second key K 204 may be periodically preferred. Exemplary reasons include (i) the second key K 204 may only be temporarily stored within a volatile memory in CPU 101 b, such that a power cycle of module 101 or CPU 101 b could flush the volatile memory, and in this case module 101 and MNO 104 may need to derive a new second key K 204, (ii) ownership of module 101 may change, and business or legal contracts could stipulate that a previous second key K 204 with the prior owner of module 101 may no longer be valid and thus a new second key K 204 may be required, (iii) a MNO 104 and a module 101 or M2M service provider 102 may prefer to periodically rotate the second key K 204 in order to increase security of a

system 500. For example, a module 101 may have a planned lifetime of more than a decade, and given the speed of change for mobile networking technology, a module 101 may prefer to support the change in a secondkey K 204 for accessing a wireless network 102 without downloading and installing a new, different profile 107 d. Other possibilities exist as well for exemplary reasons why a module 101 and/or a MNO 104 could determine that the use of a new, secondkey K 204 is preferred or required in a step 601 without departing from the scope of the present invention. If a module 101 or MNO 104 determine a value of "no" for a step 601, then the module 101 could continue periodically performing repeated second authentication 310 steps using the same secondkey K 204, as illustrated in FIG. 6.

As depicted in FIG. 6, upon determination of a value of "yes" for a step 601, a module 101 could return to a step 508 and receive another key exchange token 506. As depicted in FIG. 6 the module 101 could use a first authentication 304, which could comprise an authentication with the firstkey K 203. A return to the first authentication 304 with the firstkey K 203 could be omitted in some embodiments, and thus the box for 304 depicted in FIG. 6 is a dashed line.

In this embodiment where module 101 or MNO 104 determine or evaluates that a new secondkey K 204 is preferred at a step 601, the module 101 could return to a step 508 by attaching with the wireless network 102 again using the first network module identity 202 and the firstkey K 203. For example, if the secondkey K 204 is not available (such as being flushed from being stored only in a volatile memory, a potential error condition such as a reset of module 101, or the secondkey K 204 is no longer preferred to be used), then the module 101 with the eUICC 107 could use data recorded in the profile 107 d to reconnect with the wireless network 102. For example, the firstkey K 203 and the first network identity 202 may be recorded in generally accessible nonvolatile memory, such as, but not limited to, flash memory 101 w within module 101 and subsequently the firstkey K 203 and the first network identity 202 could be used in a step 304 before a return to a step 508. Or, the module 101 and MNO 104 could continue to use the previous secondkey K 204 (if available) for a communications link to transfer the key exchange token 506, and thus the use of a step 304 with the firstkey K 203 is optional.

Upon return to a step 508 module 101 and MNO 104 could transfer a key exchange token 506 as described in a step 508 in FIG. 6 above. Upon return to a step 508, the module 101 and MNO 104 could transfer a key exchange token 506 that has a different value or number from a key exchange token 506 transferred earlier (in order to support the derivation of a different secondkey K 204 than from a previous iteration). Using the new, different value for the key exchange token 506, the module 101 with the eUICC 107 could derive a new, different secondkey K 203. In this manner and by using the steps illustrated in FIG. 6 a secondkey K 204 could operate as a key K for "temporary use", and a different secondkey K 204 for use in a subsequent authentication 310 could be obtained by a repeated use of a step 505 with a new, different key exchange token 506 for module 101 connecting with the same wireless network 102.

The module 101 and MNO 104 could continue to use the same network module identity (such as a second network module identity 209) upon a return to steps 508 through 310, or the MNO 104 could also send the module 101 a new, different network module identity in a message 508 upon a return to steps 508 through 310. A MNO 104 and a module 101 can repeat the use of the steps 508 through 601 depicted and described in this FIG. 6 in order to derive a series over time of secondkeys K 204 for the module 101 with the eUICC 107. Each member of the series (comprising a different secondkey K 204) could be associated with the second network module identity 209, and the second network module identity 209 could remain constant or can also change to different numbers or values for use in a step 310. Supporting a change in the secondkey K 204 can both increase the flexibility and security of a system 500 and related systems for a user and a mobile network operator 104.

CONCLUSION

Various exemplary embodiments have been described above. Those skilled in the art will understand, however, that changes and modifications may be made to those examples without departing from the scope of the claims.

Patent Citations (250)

Publication number	Priority date	Publication date	Assignee	Title
US5216715A	1989-06-16	1993-06-01	Siemens Aktiengesellschaft	Key distribution in public communication networks taking account of security gradations
US5319710A	1986-08-22	1994-06-07	Tandem Computers Incorporated	Method and means for combining and managing personal verification and message authentication encryptions for network transmission
US5642420A	1994-03-03	1997-06-24	Fujitsu Limited	Cryptoinformation repeater, subscriber terminal connected thereto, and cryptocommunication method
US5664017A	1995-04-13	1997-09-02	Fortress U & T Ltd.	Internationally regulated system for one to one cryptographic communications with national sovereignty without key escrow
US5852665A	1995-04-13	1998-12-22	Fortress U & T Ltd.	Internationally regulated system for one to one cryptographic communications with national sovereignty without key escrow
DE19803936A1	1998-01-30	1999-08-05	Patent Treuhand Ges Fuer Elektrische Gluehlampen MbH	Expansion-compensated optoelectronic semiconductor component, in particular UV-emitting light-emitting diode and method for its production
US5995625A	1997-03-24	1999-11-30	Certco, LLC	Electronic cryptographic packing
US6038322A	1998-10-20	2000-03-14	Cisco Technology, Inc.	Group key distribution

US6256733B1	1998-10-08	2001-07-03	Entrust Technologies Limited	Access and storage of secure group communication cryptographic keys
US20010029581A1	2000-04-06	2001-10-11	Knauff Christopher L.	System and method for controlling and enforcing access rights to encrypted media
US20020018569A1	1998-12-04	2002-02-14	Prakash Panjwani	Enhanced subscriber authentication protocol
US20030003895A1	2001-05-11	2003-01-02	Telefonaktiebolaget Lm Ericsson (Publ).	Authentication of termination messages in telecommunications system
US20030211842A1	2002-02-19	2003-11-13	James Kempf	Securing binding update using address based keys
US6721886B1	1998-05-20	2004-04-13	Nokia Corporation	Preventing unauthorized use of service
US20040162472A1	1999-09-28	2004-08-19	Nellcor Puritan Bennett Incorporated	Sensor with signature of data relating to sensor
US20040179684A1	2003-03-14	2004-09-16	Identicrypt, Inc.	Identity-based-encryption messaging system
US6804357B1	2000-04-28	2004-10-12	Nokia Corporation	Method and system for providing secure subscriber content data
US20040221163A1	2003-05-02	2004-11-04	Jorgensen Jimi T.	Pervasive, user-centric network security enabled by dynamic datagram switch and an on-demand authentication and encryption scheme through mobile intelligent data carriers
US6842628B1	2001-08-31	2005-01-11	Palmone, Inc.	Method and system for event notification for wireless PDA devices
US20050008159A1	2003-07-07	2005-01-13	Francesco Grilli	Secure registration for a multicast-broadcast-multimedia system (MBMS)
US20050021875A1	2003-04-11	2005-01-27	Jean-Luc Bouthemey	User identification module for access to multiple communication networks
US20050050323A1	2003-09-02	2005-03-03	Authenture, Inc.	Communication session encryption and authentication system
US20050058294A1	2003-03-22	2005-03-17	Liquan Chen	Method, system and device for enabling delegation of authority and access control methods based on delegated authority
US20050120202A1	2001-11-29	2005-06-02	Jorge Cuellar	Use of a public key key pair in the terminal for authentication and authorization of the telecommunication user with the network operator and business partners
US20050138353A1	2003-12-22	2005-06-23	Terence Spies	Identity-based-encryption message management system
US20050177723A1 *	2004-02-10	2005-08-11	Industrial Technology Research Institute	SIM-based authentication method capable of supporting inter-AP fast handover
US20050193199A1	2004-02-13	2005-09-01	Nokia Corporation	Accessing protected data on network storage from multiple devices
US20050246282A1	2002-08-15	2005-11-03	Mats Naslund	Monitoring of digital content provided from a content provider over a network
US20050278787A1	2002-08-15	2005-12-15	Mats Naslund	Robust and flexible digital rights management involving a tamper-resistant identity module
US20060021063A1	2004-07-22	2006-01-26	Yoshihiro Hori	Method for transmission/reception of contents usage right information in encrypted form, and device thereof
US20060059344A1	2004-09-10	2006-03-16	Nokia Corporation	Service authentication
US20060056355A1	2004-09-16	2006-03-16	Love Robert T	System and method for downlink signaling for high speed uplink packet access
US20060095771A1	2004-11-02	2006-05-04	Guido Appenzeller	Security device for cryptographic communications
US20060129848A1	2004-04-08	2006-06-15	Texas Instruments Incorporated	Methods, apparatus, and systems for securing SIM (subscriber identity module) personalization and other data on a first processor and secure communication of the SIM data to a second processor

US20060206710A1	2005-03-11	2006-09-14	Christian Gehrmann	Network assisted terminal to SIM/UICC key establishment
US20060281442A1	2005-06-03	2006-12-14	Samsung Electronics Co., Ltd.	Method for inclusive authentication and management of service provider, terminal and user identity module, and system and terminal device using the method
US20070033403A1	2005-07-21	2007-02-08	Microsoft Corporation	Extended authenticated key exchange
US20070101400A1	2005-10-31	2007-05-03	Overcow Corporation	Method of providing secure access to computer resources
US20070158439A1	2005-12-01	2007-07-12	Conner Investments, Llc	High speed smart card with flash memory
US20070206799A1	2005-09-01	2007-09-06	Qualcomm Incorporated	Efficient key hierarchy for delivery of multimedia content
US20080016230A1	2006-07-06	2008-01-17	Nokia Corporation	User equipment credential system
US20080022089A1	2006-06-26	2008-01-24	Leedom Charles M	Security system for handheld wireless devices using-time variable encryption keys
US20080031204A1	2006-05-10	2008-02-07	Kapil Sood	Quality of service resource negotiation
US20080044032A1	2005-11-14	2008-02-21	Bce Inc.	Method and system for providing personalized service mobility
US20080107083A1	2003-10-21	2008-05-08	Qualcomm Incorporated	Method and apparatus for network initiated data services
US20080114978A1	2005-02-14	2008-05-15	Vesa Petteri Lehtovirta	Key Delivery Method and Apparatus in a Communications System
US20080130879A1	2006-10-23	2008-06-05	Valimo Wireless Oy	Method and system for a secure PKI (Public Key Infrastructure) key registration process on mobile environment
US20080165698A1	2007-01-08	2008-07-10	Lars Dalsgaard	Method, Apparatus and System for Providing Reports on Channel Quality of a Communication System
EP1981224A1	2007-04-13	2008-10-15	Samsung Electronics Co., Ltd.	Transitioning radio resource control state of user equipment to idle state
US20080307218A1	2007-06-05	2008-12-11	Oleg Logvinov	System and method for using an out-of-band device to program security keys
US20090011320A1	2005-02-07	2009-01-08	Gs Yuasa Corporation	Catalyst-supporting powder and method for producing same
US20090028341A1	2006-03-20	2009-01-29	Canon Kabushiki Kaisha	Communication system, communication device and processing method therefor
US20090041110A1	2007-03-27	2009-02-12	Qualcomm Incorporated	Rate matching with multiple code block sizes
US20090060197A1	2007-08-31	2009-03-05	Exegy Incorporated	Method and Apparatus for Hardware-Accelerated Encryption/Decryption
US20090077643A1	2007-09-19	2009-03-19	Interdigital Patent Holdings, Inc.	Virtual subscriber identity module
US20090113203A1	2007-10-26	2009-04-30	Hitachi Ltd.	Network System
US20090116642A1	2006-07-04	2009-05-07	Huawei Technologies Co., Ltd.	Method and device for generating local interface key
US20090125996A1	2007-09-19	2009-05-14	Interdigital Patent Holdings, Inc.	Virtual subscriber identity module
US20090132806A1	2004-06-10	2009-05-21	Marc Blommaert	Method for agreeing between at least one first and one second communication subscriber to security key for securing communication link
US20090183541A1	2006-04-28	2009-07-23	Babak Sadighi	Access Control System and Method for Operating Said System
US20090191857A1	2008-01-30	2009-07-30	Nokia Siemens Networks Oy	Universal subscriber identity module provisioning for machine-to-machine communications
US20090209232A1	2007-10-05	2009-08-20	Interdigital Technology Corporation	Techniques for secure channelization between uicc and a terminal
US20090217348A1	2008-02-22	2009-08-27	Patrik Mikael Salmela	Methods and Apparatus for Wireless Device Registration

US20090268909A1	2006-06-12	2009-10-29	Nec Europe Ltd.	Method for operating a wireless sensor network
US20090274306A1	2005-04-21	2009-11-05	Wincor Nixdorf International GmbH	Method for Key Administration for Cryptography Modules
US20090282246A1	2006-09-11	2009-11-12	Guenther Christian	Method and system for continuously transmitting encrypted data of a broadcast service to a mobile terminal
US20090313472A1	2008-04-07	2009-12-17	Interdigital Patent Holdings, Inc.	Secure session key generation
US20100023771A1	2006-11-15	2010-01-28	Marinus Struik	Implicit certificate verification
US20100031042A1	2007-10-26	2010-02-04	Telcordia Technologies, Inc.	Method and System for Secure Session Establishment Using Identity-Based Encryption (VDTLS)
US20100062808A1	2008-08-25	2010-03-11	Interdigital Patent Holdings, Inc.	Universal integrated circuit card having a virtual subscriber identity module functionality
US20100093347A1	2007-04-18	2010-04-15	Gene Beck Hahn	Method for performing initial ranging in wireless communication system
US20100098253A1	2007-02-28	2010-04-22	France Telecom	Broadcast Identity-Based Encryption
US20100166167A1	2005-04-04	2010-07-01	Nokia Siemens Networks GmbH & Co. Kg	Method and Apparatus for Managing Subscriber Profile Information
US20100199334A1	2006-04-24	2010-08-05	Cypak Ab	Device and method for identification and authentication
US20100195833A1	2006-07-14	2010-08-05	Vodafone Group Plc	Telecommunications device security
US20100211779A1	2009-02-17	2010-08-19	Sundaram Ganapathy S	Identity Based Authenticated Key Agreement Protocol
US20100223461A1	2009-02-27	2010-09-02	Marc Drader	Secure data transfer on a handheld communications device
US20100275028A1	2008-02-20	2010-10-28	Mitsubishi Electric Corporation	Verification apparatus
US20110016321A1	2009-07-14	2011-01-20	Sundaram Ganapathy S	Automated Security Provisioning Protocol for Wide Area Network Communication Devices in Open Device Environment
US20110035604A1	2008-10-21	2011-02-10	Habraken G Wouter	Dual-Interface Key Management
US20110035584A1	2009-03-05	2011-02-10	Interdigital Patent Holdings, Inc.	Secure remote subscription management
US20110055553A1	2009-08-26	2011-03-03	Lee Sung-Young	Method for controlling user access in sensor networks
US7921292B1	2003-04-04	2011-04-05	Voltage Security, Inc.	Secure messaging systems
US7957532B2	2006-06-23	2011-06-07	Microsoft Corporation	Data protection for a mobile device
US20110158411A1	2009-12-29	2011-06-30	General Instrument Corporation	Registering client devices with a registration server
US20110167272A1	2010-01-06	2011-07-07	Kolesnikov Vladimir Y	Secure Multi-UIM aka key exchange
US20110213959A1	2008-11-10	2011-09-01	Nokia Siemens Networks Oy	Methods, apparatuses, system and related computer program product for privacy-enhanced identity management
US20110237281A1	2008-10-28	2011-09-29	Koninklijke Kpn N.V.	Telecommunications Network and Method of Transferring User Data in Signalling Messages from a Communication Unit to a Data Processing Centre
US20110270747A1	2010-04-28	2011-11-03	Xu Richard H	System and Method for Adding Funds to a Prepaid Account for a Mobile Device Associated with Multiple Communication Profiles
US20110268022A1	2010-04-28	2011-11-03	Xu Richard H	System and Method for Routing Signals Using Network-Specific Identifiers for a Common Server Module
US20110269461A1	2010-04-28	2011-11-03	Xu Richard H	System and Method for Dynamically Providing Communication Profiles for Mobile Devices
US20110269472A1	2010-04-28	2011-11-03	Xu Richard H	System and Method for Routing a Call to a Mobile Device Associated with Multiple Communication Profiles

US20110269422A1	2010-04-28	2011-11-03	Xu Richard H	System and Method for Routing a Message to a Mobile Device Associated with Multiple Communication Profiles
WO2011138238A1	2010-05-03	2011-11-10	Alcatel Lucent	Managing the operation of a machine type communication device in a mobile communication system
US20110291803A1	2010-05-27	2011-12-01	Zeljko Bajic	Rfid security and mobility architecture
US20110314287A1	2010-06-16	2011-12-22	Qualcomm Incorporated	Method and apparatus for binding subscriber authentication and device authentication in communication systems
US20120011362A1	2010-07-08	2012-01-12	Certicom Corp.	System and Method for Performing Device Authentication Using Key Agreement
US20120011360A1	2010-06-14	2012-01-12	Engels Daniel W	Key management systems and methods for shared secret ciphers
US20120023336A1	2009-12-10	2012-01-26	Vijayarangan Natarajan	System and method for designing secure client-server communication protocols based on certificateless public key infrastructure
US20120030461A1	2001-02-06	2012-02-02	Certicom Corp.	Mobile certificate distribution in a pki
US20120033613A1	2010-08-04	2012-02-09	National Taiwan University	Enhanced rach design for machine-type communications
US8127142B2	2005-09-09	2012-02-28	University Of South Florida	Method of authenticating a user on a network
US20120072732A1	2009-06-12	2012-03-22	Canard Sebastien	cryptographic method for anonymous authentication and separate identification of a user
US20120084568A1	2010-10-01	2012-04-05	Futurewei Technologies, Inc.	Lightweight Secure Neighbor Discovery Protocol for Low-Power and Lossy Networks
US20120087493A1	2010-10-12	2012-04-12	Research In Motion Limited	Method for securing credentials in a remote repository
US20120089568A1	2010-09-03	2012-04-12	Stephen Manley	Adaptive Data Transmission
US20120108205A1	2010-10-28	2012-05-03	Schell Stephen V	Methods and apparatus for storage and execution of access control clients
US20120117635A1	2010-11-04	2012-05-10	Schell Stephan V	Simulacrum of physical security device and methods
US20120159153A1	2010-12-13	2012-06-21	Korea Basic Science Institute	Efficient Identity-Based Ring Signature Scheme With Anonymity And System Thereof
US20120170451A1	2011-01-05	2012-07-05	Harish Viswanathan	System and method for communicating data between an application server and an m2m device
US20120190354A1	2010-12-06	2012-07-26	Gemal To Sa	UICCs EMBEDDED IN TERMINALS OR REMOVABLE THERE FROM
US20120214444A1	2011-02-15	2012-08-23	Research In Motion Limited	System and Method for Identity Management for Mobile Devices
US20120260095A1	2011-04-05	2012-10-11	Jerrold Von Hauck	Apparatus and methods for controlling distribution of electronic access clients
US20120260090A1	2011-04-05	2012-10-11	Jerrold Von Hauck	Apparatus and methods for storing electronic access clients
US20120260086A1	2011-04-05	2012-10-11	Haggerty David T	Apparatus and methods for distributing and storing electronic access clients
US20120263298A1	2009-12-31	2012-10-18	Samsung Electronics Co. Ltd.	Method and system for supporting security in a mobile communication system
US20120272064A1	2011-04-22	2012-10-25	Sundaram Ganapathy S	Discovery of security associations
US20120278490A1	2011-04-27	2012-11-01	At&T Mobility Ii Llc	Distributed machine-to-machine connectivity
US20120300932A1	2011-05-26	2012-11-29	First Data Corporation	Systems and Methods for Encrypting Mobile Device Communications
CA2775853A1	2011-06-01	2012-12-01	Research In Motion Limited	Using multiple user accounts on a mobile device
US20120331287A1	2011-06-21	2012-12-27	Research In Motion Limited	Provisioning a Shared Secret to a Portable Electronic Device and to a Service Entity

US20120331292A1	2011-04-26	2012-12-27	Haggerty David T	Electronic access client distribution apparatus and methods
US20120331298A1	2010-03-11	2012-12-27	Huawei Technologies Co., Ltd.	Security authentication method, apparatus, and system
US20130007442A1	2011-06-30	2013-01-03	Qualcomm Incorporated	Facilitating group access control to data objects in peer-to-peer overlay networks
US8352739B2	2003-06-27	2013-01-08	Kt Corporation	Two-factor authenticated key exchange method and authentication method using the same, and recording medium storing program including the same
US20130012168A1	2010-03-15	2013-01-10	Samsung Electronics Co. Ltd.	Method and system for secured remote provisioning of a universal integrated circuit card of a user equipment
US20130028184A1	2010-01-06	2013-01-31	Electronics And Telecommunications Research Institute	Machine type communication system
WO2013027085A1	2011-08-22	2013-02-28	Nokia Corporation	Multi-sim enabling application and use of euicc in legacy terminals
KR20130026352A	2011-09-05	2013-03-13	주식회사 케이티	Method and apparatus for managing key information of embedded uicc, mno system, provisioning method and mno-changing method using the same
KR20130026958A	2011-09-05	2013-03-14	주식회사 케이티	Method for verification of embedded uicc using euicc certificate, method for provisioning and mno switching, euicc, mno system and recording medium for the same
US20130091556A1	2010-06-21	2013-04-11	Nokia Siemens Networks Oy	Method for establishing a secure and authorized connection between a smart card and a device in a network
US8434139B1	2009-09-10	2013-04-30	Symantec Corporation	Utilizing communications obfuscation proxy to protect system services
US20130114810A1	2010-07-23	2013-05-09	Nippon Telegraph And Telephone Corporation	Cryptographic system, cryptographic communication method, encryption apparatus, key generation apparatus, decryption apparatus, content server, program, and storage medium
US20130117824A1	2010-06-22	2013-05-09	Telefonaktiebolaget L M Ericsson (Publ)	Privacy preserving authorisation in pervasive environments
WO2013066077A1	2011-11-04	2013-05-10	주식회사 케이티	Method for managing multiple profiles in an embedded uicc, and embedded uicc and terminal therefor
US20130122864A1	2011-05-06	2013-05-16	David T. Haggerty	Methods and apparatus for providing management capabilities for access control clients
US8452017B2	2007-12-21	2013-05-28	Research In Motion Limited	Methods and systems for secure channel initialization transaction security based on a low entropy shared secret
US20130145151A1	2011-12-02	2013-06-06	Research In Motion Limited	Derived Certificate based on Changing Identity
US20130149996A1	2011-12-09	2013-06-13	Verizon Patent And Licensing Inc.	Public key cryptography for applications requiring generic bootstrap architecture
US20130157673A1	2011-09-16	2013-06-20	Alcatel-Lucent Usa Inc.	Network operator-neutral provisioning of mobile devices
US20130165073A1	2011-12-23	2013-06-27	Nokia Corporation	Method and apparatus for emulating a plurality of subscriptions
US20130166915A1	2011-12-22	2013-06-27	Research In Motion Limited	Secure text-to-speech synthesis in portable electronic devices
US20130165075A1	2011-05-23	2013-06-27	Gigsky, Inc.	Devices and systems that obtain and manage subscriptions for accessing wireless networks on an ad hoc basis and methods of use
US20130173926A1	2011-08-03	2013-07-04	Olea Systems, Inc.	Method, Apparatus and Applications for Biometric Identification, Authentication, Man-to-Machine Communications and Sensor Data Processing
US20130173747A1	2011-11-21	2013-07-04	Young Jin Kim	System, method and apparatus providing address invisibility to content provider/subscriber
US20130179962A1	2001-02-14	2013-07-11	Endeavors Technologies, Inc.	Intelligent Network Streaming and Execution System for Conventionally Coded Applications

US20130182586A1	2012-01-18	2013-07-18	Qualcomm Incorporated	Obtaining communication session initiation information in a wireless communications system
US20130183932A1	2012-01-18	2013-07-18	Renesas Mobile Corporation	Method and apparatus for network access
US20130212637A1	2010-03-02	2013-08-15	Interdigital Patent Holdings, Inc.	Migration of credentials and/or domains between trusted hardware subscription modules
US8522013B2	2009-08-31	2013-08-27	Telcordia Technologies, Inc.	System and methods to perform public key infrastructure (PKI) operations in vehicle networks using one-way communications infrastructure
US20130227646A1	2012-02-14	2013-08-29	Apple Inc.	Methods and apparatus for large scale distribution of electronic access clients
US8526606B2	2010-12-20	2013-09-03	GM Global Technology Operations LLC	On-demand secure key generation in a vehicle-to-vehicle communication network
US20130231087A1	2012-03-05	2013-09-05	Rogers Communications Inc.	Radio management method and system using embedded universal integrated circuit card
US8555067B2	2010-10-28	2013-10-08	Apple Inc.	Methods and apparatus for delivering electronic identification components over a wireless network
US20130283047A1	2010-08-05	2013-10-24	Gemalto Sa	System and method for securely using multiple subscriber profiles with a security component and a mobile telecommunications device
US20130294602A1	2012-05-02	2013-11-07	Horatio Nelson Huxham	Small Form-Factor Cryptographic Expansion Device
US20130305345A1	2012-05-10	2013-11-14	Centurylink Intellectual Property Llc	System and method for secure machine-to-machine communications
US8590028B2	2007-07-09	2013-11-19	Infosys Limited	Content licensing and conditional access using a mobile device
US20130322621A1	2012-05-31	2013-12-05	Snu R&Db Foundation	Private key generation apparatus and method, and storage media storing programs for executing the methods
US20130331063A1	2012-06-11	2013-12-12	Research In Motion Limited	Enabling multiple authentication applications
US20130340040A1	2012-05-23	2013-12-19	Chul Hyun Park	Method and apparatus of constructing secure infra-structure for using embedded universal integrated circuit card
US20130344864A1	2012-05-25	2013-12-26	Kt Corporation	METHOD FOR PROVIDING SUBSCRIBER PROFILE OF eUICC
US2014003604A1	2012-06-27	2014-01-02	Certicom Corp.	Authentication of a mobile device by a network and key generation
US20140040628A1	2012-08-03	2014-02-06	Vasco Data Security, Inc.	User-convenient authentication method and apparatus using a mobile authentication application
US20140049653A1	2012-08-20	2014-02-20	Jon N. Leonard	Authentication and Validation of Smartphone Imagery
US20140053241A1	2011-04-27	2014-02-20	Telefonaktiebolaget L M Ericsson (Publ)	Authenticating a Device in a Network
US20140073375A1	2012-09-12	2014-03-13	Li Li	Methods and apparatus for managing data within a secure element
US20140082358A1	2012-09-17	2014-03-20	General Instrument Corporation	Efficient key generator for distribution of sensitive material from multiple application service providers to a secure element such as a universal integrated circuit card (uicc)
US20140087790A1	2010-12-22	2014-03-27	Vodafone Ip Licensing Limited	Sim locking
US20140101444A1	2012-10-09	2014-04-10	Samsung Sds Co., Ltd.	Apparatus and method for transmitting data, and recording medium storing program for executing method of the same in computer
US20140115335A1	2012-10-19	2014-04-24	Caterpillar Inc.	Secure machine-to-machine communication protocol
US20140122878A1	2012-10-30	2014-05-01	Kt Corporation	Security management in m2m area network

US20140120874A1	2012-10-25	2014-05-01	Samsung Electronics Co., Ltd	Method and device for managing security key for communication authentication of subscriber station used in cooperative communication of multiple base station in radio communication system
US20140143826A1	2012-11-21	2014-05-22	Apple Inc.	Policy-based techniques for managing access control
US20140140509A1	2012-11-16	2014-05-22	At&T Mobility II, LLC	Methods for provisioning universal integrated circuit cards
US20140143534A1	2012-11-19	2014-05-22	At&T Mobility II, LLC	Systems for provisioning universal integrated circuit cards
US20140140507A1	2011-07-08	2014-05-22	Kt Corporation	Method for changing mno in embedded sim on basis of dynamic key generation and embedded sim and recording medium therefor
US20140165155A1	2012-12-06	2014-06-12	Qualcomm Incorporated	Management of network devices utilizing an authorization token
US20140161113A1	2012-12-06	2014-06-12	At&T Intellectual Property I, L.P.	Location-Based Wi-Fi Radio Activation And Deactivation For Mobile Devices
US20140192976A1	2012-10-31	2014-07-10	Snu R&Db Foundation	Method and system for id-based encryption and decryption
US8782774B1	2013-03-07	2014-07-15	Cloudflare, Inc.	Secure session capability using public-key cryptography without access to the private key
US20140219448A1	2011-08-24	2014-08-07	Deutsche Telekom Ag	Authenticating a telecommunication terminal in a telecommunication network
US20140219447A1	2011-09-05	2014-08-07	Kt Corporation	Method for managing profile of embedded uicc, and embedded uicc, embedded uicc-equipped terminal, provision method, and method for changing mno using same
US20140237101A1	2011-09-28	2014-08-21	Kt Corporation	Profile management method, embedded uicc, and device provided with the embedded uicc
US20140244994A1	2011-11-11	2014-08-28	Zte Corporation	Method, apparatus and system for binding MTC device and UICC
US20140281483A1	2013-03-12	2014-09-18	Silver Spring Networks	System and method for enabling a scalable public-key infrastructure on a smart grid network
US20140273913A1	2013-03-12	2014-09-18	Oberthur Technologies	Emergency call system and method
US8843179B2	2012-05-11	2014-09-23	Li Li	Provisioning an embedded subscriber identity module
US20140287725A1 *	2011-11-04	2014-09-25	Kt Corporation	Method for forming a trust relationship, and embedded uicc therefor
US20140308991A1	2011-11-04	2014-10-16	Kt Corporation	Method for managing multiple profiles in an embedded uicc, and embedded uicc and terminal therefor
US20140337937A1	2013-05-10	2014-11-13	Research In Motion Limited	Methods and devices for detecting unauthorized access to credentials of a credential store
US20140351403A1	2012-01-19	2014-11-27	Huawei Tech Co Ltd	Method for switching of a device, m2m platform and network system
US20140357229A1	2013-05-30	2014-12-04	Samsung Electronics Co., Ltd.	Method and apparatus for setting profile
US20150012743A1	2012-02-14	2015-01-08	Nokia Corporation	Device to device security using naf key
US20150017910A1	2013-07-12	2015-01-15	Apple Inc.	Apparatus and methods for near-field communication based device configuration and management
US8965366B1	2010-02-18	2015-02-24	Amazon Technologies, Inc.	World SIM
US20150071139A1	2013-09-10	2015-03-12	John A. Nix	Power Management and Security for Wireless Modules in "Machine-to-Machine" Communications
US20150089214A1 *	2013-09-23	2015-03-26	Deutsche Telekom Ag	Enhanced authentication and/or enhanced identification of a secure element of a communication device
US20150095514A1	2012-03-31	2015-04-02	Orange	Content Centric M2M System

US20150092590A1	2013-09-27	2015-04-02	Cellco Partnership D/B/A Verizon Wireless	Category 1 m2m device data transmission via a long term evolution network
US9002018B2	2006-05-09	2015-04-07	Sync Up Technologies Corporation	Encryption key exchange system and method
GB2518976A	2013-09-13	2015-04-08	Vodafone Ip Licensing Ltd	Secure communication with a mobile device
US20150113275A1	2013-10-18	2015-04-23	Alcatel-Lucent Usa Inc.	Tamper-resistant and scalable mutual authentication for machine-to-machine devices
US9020479B1	2010-02-18	2015-04-28	Amazon Technologies, Inc.	Single version of a user device modem for use with different wireless carriers
US20150121495A1	2012-10-15	2015-04-30	Huawei Device Co., Ltd.	Method and Device for Switching Subscription Manager-Secure Routing Device
US20150215126A1	2009-01-05	2015-07-30	Imation Corp.	Data authentication using plural electronic keys
US9100175B2	2013-11-19	2015-08-04	M2M And Iot Technologies, Llc	Embedded universal integrated circuit card supporting two-factor authentication
US20150222604A1	2011-12-21	2015-08-06	Ssh Communications Security Oyj	Automated Access, Key, Certificate, and Credential Management
US20150222619A1	2012-08-30	2015-08-06	Los Alamos National Security, Llc	Multi-factor authentication using quantum communication
US20150281964A1	2012-11-19	2015-10-01	Kt Corporation	Method for configuring profile of subscriber authenticating module embedded and installed in terminal device, and apparatus using same
US20150350881A1	2012-12-21	2015-12-03	Giesecke & Devrient Gmbh	Methods and Devices for OTA Subscription Management
US20160014112A1	2013-03-14	2016-01-14	Hewlett-Packard Development Company, L.P.	Wireless communication of a user identifier and encrypted time-sensitive data
US9253643B2	2009-03-05	2016-02-02	Interdigital Patent Holdings, Inc.	Method and apparatus for H(e)NB integrity verification and validation
US9270653B2	2011-05-11	2016-02-23	At&T Mobility Ii Llc	Carrier network security interface for fielded devices
US20160057725A1	2013-04-15	2016-02-25	Samsung Electronics Co., Ltd.	Security method and system for supporting re-subscription or additional subscription restriction policy in mobile communications
US20160088096A1	2013-05-07	2016-03-24	Gemalto Sa	Method for accessing a service, corresponding device and system
US9332129B2	2012-06-21	2016-05-03	Apple Inc.	Methods and apparatus for automated communications forwarding
US20160127132A1	2013-05-30	2016-05-05	Samsung Electronics Co., Ltd.	Method and apparatus for installing profile
US20160149903A1	2013-04-15	2016-05-26	Samsung Electronics Co., Ltd.	Method for supporting subscriber's service provider change restriction policy in mobile communications and apparatus therefor
US20160212617A1	2013-08-26	2016-07-21	Ntt Docomo, Inc.	Subscriber profile transfer method, subscriber profile transfer system, and user equipment
US20160294829A1	2015-04-02	2016-10-06	The Boeing Company	Secure provisioning of devices for manufacturing and maintenance
US9572016B2	2012-07-06	2017-02-14	Blackberry Limited	Methods and apparatus for use in transferring an assignment of a secure chip between subscription managers
US9628981B2	2011-07-08	2017-04-18	Kt Corporation	Method for changing MNO in embedded SIM on basis of special privilege, and embedded SIM and recording medium therefore
US9674690B2	2012-05-23	2017-06-06	Kt Corporation	Method for control and enforcement of policy rule and EUICC
US20170206532A1	2007-12-03	2017-07-20	Yu Yung Choi	System and method for streamlined registration and management of products over a communication network related thereto

US9794775B2	2013-08-09	2017-10-17	Giesecke+Devrient Mobile Security	Methods and devices for performing a mobile network switch
US10169587B1	2018-04-27	2019-01-01	John A. Nix	Hosted device provisioning protocol with servers and a networked initiator
WO2019178312A1	2018-03-16	2019-09-19	lot And M2M Technologies, Llc	Configuration systems and methods for secure operation of networked transducers
US20190313246A1	2018-04-06	2019-10-10	lot And M2M Technologies, Llc	Device default wifi credentials for simplified and secure configuration of networked transducers
CA3110468A1	2018-05-17	2019-11-21	lot And M2M Technologies, Llc	A hosted device provisioning protocol with servers and a networked responder
WO2019246206A1	2018-06-20	2019-12-26	lot And M2M Technologies, Llc	An ecde key exchange for server authentication and a key server
WO2020006162A1	2018-06-28	2020-01-02	lot And M2M Technologies, Llc	Ecdhe key exchange for mutual authentication using a key server
WO2020061023A1	2018-09-18	2020-03-26	lot And M2M Technologies, Llc	Storage memory unit with a shared nonvolatile memory interface for a radio
US20200162247A1	2018-11-15	2020-05-21	lot And M2M Technologies, Llc	Secure firmware transfer from a server to a primary platform
US20200162269A1	2018-11-20	2020-05-21	lot And M2M Technologies, Llc	Mutually authenticated ecde key exchange for a device and a network using multiple pki key pairs
WO2020123959A1	2018-12-14	2020-06-18	lot And M2M Technologies, Llc	Secure ids certificate verification for a primary platform
US10764066B2*	2016-05-18	2020-09-01	Apple Inc.	EUICC secure timing and certificate revocation
US20200280436A1	2019-03-01	2020-09-03	John A. Nix	Public key exchange with authenticated ecde and security against quantum computers
WO2020223319A1	2019-05-01	2020-11-05	Nix John A	Distributed eap-tls authentication for wireless networks with concealed subscriber identities
WO2021007235A1	2019-07-08	2021-01-14	Nix John A	Eap-tls authentication with concealed user identities and wireless networks
US20210126801A1	2019-10-25	2021-04-29	John A. Nix	Secure configuration of a secondary platform bundle within a primary platform
WO2021087221A1	2019-10-30	2021-05-06	Nix John A	Secure and flexible boot firmware update for devices with a primary platform
Family To Family Citations				
DE3108085C2	1981-03-04	1984-05-03	Karl 7298 Loßburg Hehl	Angular strain relief device for introducing electrical supply lines into a device
JP2009025765A	2007-07-24	2009-02-05	Seiko Epson Corp	Liquid material discharge method, color filter manufacturing method, organic EL element manufacturing method
US8798613B2 *	2007-09-17	2014-08-05	Wavemarket, Inc.	Systems and method for triggering location based voice and/or data communications to or from mobile ratio terminals
US9148785B2 *	2012-05-16	2015-09-29	At&T Intellectual Property I, Lp	Apparatus and methods for provisioning devices to utilize services of mobile network operators
KR102173534B1 *	2012-05-24	2020-11-03	삼성전자 주식회사	Methods for providing information of mobile network operator and apparatus for performing the same
JP6116167B2	2012-09-14	2017-04-19	キャノン株式会社	Image processing apparatus, image processing method, and program
US9285979B2	2012-09-17	2016-03-15	Adobe Systems Incorporated	Computer-implemented methods and systems for multi-touch duplication and swapping interactions
GB201506045D0 *	2015-04-09	2015-05-27	Vodafone Ip Licensing Ltd	SIM security

* Cited by examiner; † Cited by third party

Non-Patent Citations (120)

Title
3GPP, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3, 3GPP TS 24.301 v12.2.0, Sep. 2013 pp. 1-6, 63-100.
3GPP, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture, 3GPP TS 33.401 V12.9.0 (Sep. 2013) pp. 1-75.
A. Wander et al. Energy Analysis of Public-Key Cryptography on Small Wireless Devices, Sun Microsystems Laboratories, pp. 1-16, Dated Apr. 2005.
ANSI X9.63 Overview, Key Agreement and Key Transport Using Elliptic Curve Cryptography, Simon Blake-Wilson, Certicom (2000).
Appenzeller et al., Identity-Based Encryption Architecture and Supporting Data Structures RFC 5408, 2009, pp. 1-30.
AU 2019246774, filed Oct. 8, 2019, pending.
Baugher et al., Group Key Management Architecture, RFC Draft, 2001, pp. 1-20.
Ben Saïed, Yosra; Olivereau, Alexis; Laurent, Maryline; "A Distributed Approach for Secure M2M Communications", 5th International Conference on New Technologies, Mobility and Security (NTMS), May 7-10, 2012, pp. 1-7.
Bender et al., Evolution of SIM provisioning towards a flexible MCIM provisioning in M2M vertical industries, 16th International Conference on Intelligence in Next Generation Networks, IEEE, 2012, pp. 57-64.
Boyen et al., Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles), 2006.
Boyen et al., Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems, RFC 5091, 2007, pp. 1-63.
BSMG, Reprogrammable SIMs: Technology, Evolution and Implications, Sep. 25, 2012, pp. 1-95.
C. Downey, Migrating Legacy M2M Systems to the Cloud, http://www.ecnmag.com/articles/2013/02/migratinglegacy-m2m-systems-cloud , Feb. 2013, pp. 1-2.
CA 2,965,119, filed Oct. 27, 2014, Published on May 7, 2015.
CA 2,969,829, filed Dec. 4, 2014, Published on Jun. 11, 2015.
Cakulev et al., "An EAP Authentication Method Based on Identity-Based Authenticated Key Exchange," Aug. 2012, pp. 1-32.
Chang-Seop Park, On Certificate-Based Security Protocols for Wireless Mobile Communication Systems, Dankook University, IEEE Network Sep./Oct. 1997, pp. 50-55.
Chris Foresman, Embedded SIM could cause carrier conflict for Apple, Nov. 19, 2010, pp. 1-2.
Chris Foresman, Embedded SIM could cause carrier conflict for Apple, Nov. 19, 2010, pp. 1-2.
CSMG, SMG, Reprogrammable SIMs: Technology, Evolution and Implications, Sep. 25, 2012, pp. 1-95.
D. Cooper, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Engineering Task Force RFC 5282, pp. 1-133, dated May 2008.
D. McGrew et al, Fundamental Elliptic Curve Cryptography Algorithms, Internet Engineering Task Force RFC 6090, Feb. 2011, pp. 1-34.
Embedded UICC Remote Provisioning Discussion, Source: Rogers Wireless, 3GPP/SA3-LI#46, Quebec City, Canada, Jul. 17-19, 2012, pp. 1-39.
Embedded UICC Remote Provisioning Discussion, Source: Rogers Wireless, Contact: Ed O'Leary (ed_oleary@rcirogers.com), George Babut (gbabut@rcirogers.com), 3GPP/SA3-LI#46, Quebec City, Canada, Jul. 17-19, 2012, pp. 1-39.
ETSI, Machine-to-Machine communications (M2M), mla, dla, and mid interfaces, TS 102.921 v1.1.1, Feb. 2012, pp. 1-538.
ETSI, Smart Cards; Embedded UICC; Requirements Specification, TS 103383 v1.1.0, Jun. 2013, pp. 1-20.
ETSI, Smart Cards; UICC-Terminal Interfaces; Physical and Logical Characteristics, TS 102 221 v1.1.0.0, Jun. 2012, pp. 1-181.
ETSI, UMTS/LTE; SIM/USIM Internal and External Interworking Aspects, TR 131 900 v1.0.0.0, May 2011, pp. 1-41.
EU 14868381.6, filed Dec. 4, 2014, Published on Jan. 1, 2017.
Eun-Jun Yoon, et al., Secure Deniable Authentication Protocol Based on ElGamal Cryptography, 2008 International Conference on Information Security and Assurance, pp. 36-39.
F. Qian et al., TOP: Tail Organization Protocol for Cellular Resource Allocation, 18th IEEE International Conference on Network Protocols (ICNP), 2010, pp. 285-298.

GB 1608573, filed Oct. 27, 2014, published on Aug. 3, 2016.
GB 2100530, filed Oct. 27, 2014, Published on May 12, 2021.
GlobalPlatform Inc., GlobalPlatform Card Specification, Version 2.2.1, Jan. 2011, pp. 1-303.
GlobalPlatform Inc., GlobalPlatform Card Security Upgrade for Card Content Management, Card Specification v 2.2—Amendment E, Version 1.0, Nov. 2011, pp. 1-35.
GlobalPlatform Inc., GlobalPlatform Card Specification, Version 2.2.1, Jan. 2011, pp. 1-303.
Gollmann, "Authentication—Myths and Misconceptions," Progress in Computer Science and Applied Logic, vol. 20, 2001, pp. 203-225.
GSM Association, Embedded SIM Task Force Requirements and Use Cases, Version 1.0, Feb. 21, 2011, pp. 1-38.
GSM Association, Embedded SIM Task Force Requirements and Use Cases, Version 1.0, 21 Feb. 2011, pp. 1-38.
GSMA Launches Embedded SIM Initiative to Support the Connected Future, Nov. 18, 2010, pp. 1-4.
Harney et al., Group Key Management Protocol (GKMP) Architecture, 1994, pp. 1-19.
Hegland et al., "A Framework for Authentication in NBD Tactical Ad Hoc Networks," IEEE Communications Magazine, Oct. 2011, pp. 64-71.
HK 17101082.8, filed Oct. 27, 2014, Published on Oct. 20, 2017.
HK 17106540.3, filed Dec. 4, 2014, Published on Jan. 19, 2018.
International Search Report and Written Opinion for PCT/US2014/062435 dated Feb. 6, 2015.
International Search Report for PCT/US2014/068544 dated Feb. 13, 2015.
J. Huang et al., A Close Examination of Performance and Power Characteristics of 4G LTE Networks, Mobisys' 12, Jun. 25-29, 2012, pp. 1-14.
J. Jonsson et al., Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, Internet Engineering Task Force RFC 3447, Feb. 2003, pp. 1-72.
Jun Shao, et al., an Improved Deniable Authentication Protocol, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200030, People's Republic of China, pp. 13, First published: Aug. 30, 2006.
Kiltz et al., CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption, 2008.
Kirk H.M. Wong et al., A Dynamic User Authentication Scheme for Wireless Sensor Networks, Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), pp. 1-8.
Kirk H.M. Wong et al., A Dynamic User Authentication Scheme for Wireless Sensor Networks, Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), pp. 1-8.
Krylov, What is Kerberos Authentication?, 2003, pp. 1-4.
L. Larzon, The Lightweight User Datagram Protocol (UDP-Lite), Internet Engineering Task Force RFC 3828, Jul. 2004, pp. 1-12.
M. Prasad, et al., Secure Authentication Key Agreement Protocol for Long Term Evolution Advanced, Research Scholar, Associate Professor, Department of Computer Science & Engineering, Pondicherry Engineering College, Puducherry, India, Elsevier, 2012, pp. 158-162.
Martin, Introduction to Identity-Based Encryption, ISBN-13 978-1-59693-238-8, 2008.
Merrian-Webster, Network, 2014.
N. Chu et al. EXALTED: Expanding LTE for Devices, European Commission for Information Society and Media, Oct. 31, 2012, pp. 1-141.
Nicholson et al., "Mobile Device Security Using Transient Authentication," IEEE Transactions on Mobile Computing, vol. 5, No. 11, Nov. 2006, pp. 1489-1502.
Park et al., A New Practical Identity-Based Encryption System, 2003, pp. 1-27.
Park et al., Secure Profile Provisioning Architecture for Embedded UICC, 2013 International Conference on Availability, Reliability and Security, IEEE, 2013, pp. 297-303.
Pierre E. Abi-Char, et al., A Fast and Secure Elliptic Curve Based Authenticated Key Agreement Protocol for Low Power Mobile Communications, The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2007), pp. 1-6.
Pietre-Cambacedes et al., Cryptographic key management for SCADA systems—issues and perspectives, 2008 International Conference on Information Security and Assurance, IEEE, pp. 156-161.
Schwaiger et al., "Smart Card Security for Fieldbus Systems," 2003, pp. 398-406.

Search Report and Written Opinion for PCT/US2014/068544 (13/1714-WO).
Search Report issued in UK Application No. GB2108534.5 dated Jul. 7, 2021.
Shih, Jie-Ren et al., "Securing M2M with Post-Quantum Public-Key Cryptography", IEEE Journal on Emerging and Selected Topics in Circuits and Systems, Mar. 7, 2013, pp. 106-116.
Sollmann, "Authentication—Myths and Misconceptions," Progress in Computer Science and Applied Logic, vol. 20, 2001, pp. 203-225.
T. Pornin, Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA), Internet Engineering Task Force RFC 6979, Aug. 2013, pp. 1-79.
Tin et al., "Provably Secure Mobile Key Exchange: Applying the Canetti-Krawczyk Approach," Information Security Research Centre, Queensland University of Technology, Australia, 2003, pp. 166-179.
TLS 1.3 Wish List Presentation, IETF 87 (Eric Rescorla), dated Aug. 1, 2013.
U.S. Appl. No. 14/023,181, filed Sep. 10, 2013, U.S. Pat. No. 9,350,550.
U.S. Appl. No. 14/039,401, filed Sep. 27, 2013, U.S. Pat. No. 9,288,059.
U.S. Appl. No. 14/055,606, filed Oct. 16, 2013, U.S. Pat. No. 9,276,740.
U.S. Appl. No. 14/064,618, filed Oct. 28, 2013, U.S. Pat. No. 9,118,464.
U.S. Appl. No. 14/084,141, filed Nov. 19, 2013, U.S. Pat. No. 9,319,223.
U.S. Appl. No. 14/099,329, filed Dec. 6, 2013, U.S. Pat. No. 9,100,175.
U.S. Appl. No. 14/136,711, filed Dec. 20, 2013, U.S. Pat. No. 9,300,473.
U.S. Appl. No. 14/139,419, filed Dec. 23, 2013, U.S. Pat. No. 9,351,162.
U.S. Appl. No. 14/751,119, filed Jun. 25, 2015, U.S. Pat. No. 9,961,060.
U.S. Appl. No. 14/789,255, filed Jul. 1, 2015, U.S. Pat. No. 9,596,078.
U.S. Appl. No. 15/010,905, filed Jan. 29, 2016, U.S. Pat. No. 9,641,327.
U.S. Appl. No. 15/043,293, filed Feb. 12, 2016, U.S. Pat. No. 9,998,280.
U.S. Appl. No. 15/130,146, filed Apr. 15, 2016, U.S. Pat. No. 9,742,562.
U.S. Appl. No. 15/162,292, filed May 23, 2016, U.S. Pat. No. 10,362,012.
U.S. Appl. No. 15/162,302, filed May 23, 2016, U.S. Pat. No. 9,698,981.
U.S. Appl. No. 15/457,700, filed Mar. 13, 2017, U.S. Pat. No. 9,998,281.
U.S. Appl. No. 15/583,968, filed May 1, 2017, U.S. Pat. No. 10,057,059.
U.S. Appl. No. 15/642,088, filed Jul. 5, 2017, U.S. Pat. No. 10,003,461.
U.S. Appl. No. 15/680,758, filed Aug. 18, 2017, U.S. Pat. No. 10,187,206.
U.S. Appl. No. 15/928,848, filed Mar. 22, 2018, U.S. Pat. No. 10,084,768.
U.S. Appl. No. 15/972,914, filed May 7, 2018, U.S. Pat. No. 10,652,017.
U.S. Appl. No. 15/973,012, filed May 7, 2018, U.S. Pat. No. 10,250,386.
U.S. Appl. No. 15/983,957, filed May 18, 2018, U.S. Pat. No. 10,177,911.
U.S. Appl. No. 16/036,506, filed Jul. 16, 2018, U.S. Pat. No. 10,530,575.
U.S. Appl. No. 16/110,804, filed Aug. 23, 2018, U.S. Pat. No. 10,382,422.
U.S. Appl. No. 16/200,118, filed Nov. 26, 2018, U.S. Pat. No. 10,498,530.
U.S. Appl. No. 16/201,401, filed Nov. 27, 2018, U.S. Pat. No. 10,700,856.
U.S. Appl. No. 16/271,428, filed Feb. 8, 2019, U.S. Pat. No. 10,523,432.

U.S. Appl. No. 16/271,455, filed Feb. 8, 2019, U.S. Pat. No. 10,594,679.
U.S. Appl. No. 16/453,682, filed Jun. 26, 2019, Notice of Allowance dated Jun. 29, 2021.
U.S. Appl. No. 16/453,682, filed Jun. 26, 2019, Present application.
U.S. Appl. No. 16/593,561, filed Oct. 4, 2019, Docketed for examination.
U.S. Appl. No. 16/593,561, filed Oct. 4, 2019, Non-Final Rejection dated Jul. 6, 2021.
U.S. Appl. No. 16/721,153, filed Dec. 19, 2019, Final Office Action dated Apr. 15, 2021.
U.S. Appl. No. 16/843,107, filed Apr. 8, 2020, Docketed for examination.
U.S. Appl. No. 16/843,107, filed Apr. 8, 2020, Non-Final Rejection dated Jul. 2, 2021.
U.S. Appl. No. 16/879,325, filed May 20, 2020, Application to issue U.S. Pat. No. 11,082,218 on Aug. 3, 2021.
U.S. Appl. No. 16/879,325, filed May 20, 2020, Notice of Allowance dated Mar. 31, 2021.
U.S. Appl. No. 17/249,242, filed Feb. 24, 2021, Application Dispatched from Preexam.
U.S. Appl. No. 17/304,922, filed Jun. 28, 2021, Application Undergoing Preexam Processing.
V. Martinez et al, A Survey of the Elliptic Curve Integrated Encryption Scheme, Journal of Computer Science and Engineering, vol. 2, Aug. 2010, pp. 7-13.
Voltage Security, The Identity-Based Encryption Advantage, 2015.
Wikipedia, Digital Signature, http://en.wikipedia.org/wiki/Digital_Signature , Sep. 9, 2013, pp. 1-10.
Wikipedia, Elliptic Curve Cryptography, http://en.wikipedia.org/wiki/Elliptic_curve_cryptography , Sep. 9, 2013, pp. 1-8.
Wikipedia, Elliptic Curve Diffie-Hellman, http://en.wikipedia.org/wiki/Elliptic_curve_Diffie-Hellman , Sep. 24, 2013, pp. 1-2.
Wikipedia, RSA (algorithm), http://en.wikipedia.org/wiki/RSA_(algorithm) , Sep. 9, 2013, pp. 1-12.
Yang et al., Identity-Based Key Agreement and Encryption for Wireless Sensor Networks, IJCSNS International Journal of Computer Science and Network Security, vol. 6, No. 5B, May 2006, pp. 182-189.
Youngblood, An Introduction to Identity-based Cryptography, 2005.
Zhu et al., Public Key Cryptography for Initial Authentication in Kerberos (PPKINIT), RFC 4556, 2006, pp. 1-42.

* Cited by examiner, † Cited by third party

Cited By (164)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US9712996B2	2011-09-28	2017-07-18	Kt Corporation	Profile management method, embedded UICC, and device provided with the embedded UICC
US9231931B2 *	2012-05-23	2016-01-05	Kt Corporation	Method and apparatus of constructing secure infrastructure for using embedded universal integrated circuit card
KR102138315B1 *	2013-05-30	2020-07-27	삼성전자주식회사	Method and Apparatus for Provisioning Profile
US9100175B2	2013-11-19	2015-08-04	M2M And Iot Technologies, Llc	Embedded universal integrated circuit card supporting two-factor authentication
US9350550B2	2013-09-10	2016-05-24	M2M And Iot Technologies, Llc	Power management and security for wireless modules in "machine-to-machine" communications
GB2586549B	2013-09-13	2021-05-26	Vodafone Ip Licensing Ltd	Communicating with a machine to machine device
US10498530B2	2013-09-27	2019-12-03	Network-1 Technologies, Inc.	Secure PKI communications for "machine-to-machine" modules, including key derivation by modules and authenticating public keys

US10700856B2	2013-11-19	2020-06-30	Network-1 Technologies, Inc.	Key derivation for a module using an embedded universal integrated circuit card
EP3073770A4 *	2013-12-05	2016-10-26	Huawei Device Co Ltd	Security control method for euicc, and euicc
US20150160925A1 *	2013-12-06	2015-06-11	Sonic Ip, Inc.	Methods, Systems, and Media for Generating Random Numbers
EP2887702B1*	2013-12-17	2016-11-02	Giesecke & Devrient GmbH	Method and device for providing a secure element with a subscription profile
US9538311B2 *	2014-02-04	2017-01-03	Texas Instruments Incorporated	Auto-provisioning for internet-of-things devices
US9867125B2 *	2014-04-07	2018-01-09	Google LLC	Systems for enabling modular mobile electronic devices
KR102200209B1 *	2014-04-22	2021-01-08	삼성전자 주식회사	Method and apparatus for provisioning profiles
US9537858B2 *	2014-05-15	2017-01-03	Apple Inc.	Methods and apparatus to support globalplatform™ usage on an embedded UICC (eUICC)
US10277559B2*	2014-05-21	2019-04-30	Excalibur Ip, LLC	Methods and systems for data traffic control and encryption
EP3149994B1*	2014-06-02	2019-10-02	Telefonaktiebolaget LM Ericsson (publ)	Merging proxy
US9509664B2 *	2014-06-16	2016-11-29	Verizon Deutschland GmbH	Data exchange in the internet of things
KR102331692B1	2014-06-30	2021-11-30	삼성전자 주식회사	Method and apparatus for selecting profile of terminal in a mobile network
KR102191017B1 *	2014-07-19	2020-12-15	삼성전자주식회사	Method and server device for provisioning an embedded SIM
US10111100B2*	2014-08-25	2018-10-23	Microsoft Technology Licensing, LLC	Multidevice authentication
US11051140B2*	2014-09-19	2021-06-29	Texas Instruments Incorporated	Compression of internet protocol version 6 addresses in wireless sensor networks
KR102331695B1	2014-10-27	2021-11-26	삼성전자 주식회사	Method for changing a profile in accordance with an identification module and an electronic device implementing the same
EP4096260B1*	2014-11-17	2025-01-01	Samsung Electronics Co., Ltd.	Apparatus and method for profile installation in communication system
US10051111B2*	2014-11-20	2018-08-14	At&T Intellectual Property I, L.P.	Separating sensitive data from mobile devices for theft prevention
FR3030817B1 *	2014-12-22	2017-01-13	Oberthur Technologies	USER AUTHENTICATION METHOD, SECURE MODULE, ELECTRONIC APPARATUS AND SYSTEM THEREOF
US9525694B2	2015-01-15	2016-12-20	Bank Of America Corporation	Authenticating customers and managing authenticated sessions
US9491170B2 *	2015-01-15	2016-11-08	Bank Of America Corporation	Authenticating customers and managing authenticated sessions
US9853977B1	2015-01-26	2017-12-26	Winklevoss Ip, LLC	System, method, and program product for processing secure transactions within a cloud computing system
US10142834B2*	2015-01-29	2018-11-27	Motorola Mobility LLC	Method and apparatus for operating a user client wireless communication device on a wireless wide area network
DE102015001900A1*	2015-02-09	2016-08-11	Giesecke & Devrient GmbH	Method for operating a security element
EP3057350A1 *	2015-02-13	2016-08-17	Gemalto Sa	Method for remote subscription management of an eUICC, corresponding terminal
US10785645B2*	2015-02-23	2020-09-22	Apple Inc.	Techniques for dynamically supporting different authentication algorithms
US10084820B2*	2015-02-27	2018-09-25	Konica Minolta Laboratory U.S.A., Inc.	Method and system for IPSec security for IPP-USB data

US10158480B1	2015-03-16	2018-12-18	Winklevoss Ip, Llc	Autonomous devices
US10915891B1	2015-03-16	2021-02-09	Winklevoss Ip, Llc	Autonomous devices
KR102284954B1 *	2015-04-08	2021-08-03	삼성전자 주식회사	Method and apparatus for downloading a profile in a wireless communication system
GB201506045D0 *	2015-04-09	2015-05-27	Vodafone Ip Licensing Ltd	SIM security
EP3562184B1 *	2015-04-13	2020-08-12	Samsung Electronics Co., Ltd.	Technique for managing profile in communication system
EP3284093B1	2015-04-14	2021-08-04	Cambou, Bertrand, F.	Memory circuits using a blocking state
US11080414B2	2015-05-22	2021-08-03	Huawei Device Co., Ltd.	Cryptographic unit for public key infrastructure (PKI) operations
FR3038421B1 *	2015-06-30	2017-08-18	Oberthur Technologies	METHOD FOR MANAGING PROFILES IN A SECURE ELEMENT
US10356091B2 *	2015-07-14	2019-07-16	Ujet, Inc.	Communication enhancement methods
WO2017020003A1 *	2015-07-30	2017-02-02	Reliance Jio Infocomm Usa, Inc.	Method and system for routing ip based messaging, voice and video calling based on the network parameters the device is connected to and the location
US9955353B2	2015-08-14	2018-04-24	Microsoft Technology Licensing, Llc	Delegated profile and policy management
CN106470430A *	2015-08-14	2017-03-01	中兴通讯股份有限公司	The processing method of operator's configuration, equipment and system
US9767318B1 *	2015-08-28	2017-09-19	Frank Dropps	Secure controller systems and associated methods thereof
CN108028758B *	2015-08-31	2021-06-25	三星电子株式会社	Method and apparatus for downloading a profile in a communication system
JP5951094B1 *	2015-09-07	2016-07-13	ヤフー株式会社	Generation device, terminal device, generation method, generation program, and authentication processing system
US20170078255A1 *	2015-09-11	2017-03-16	iAspire, LLC	Systems and methods for implementing modular digital encryption key management solutions
KR102362395B1 *	2015-09-22	2022-02-14	삼성전자 주식회사	Method and apparatus for download of profile in a wireless communication system
US10396981B2 *	2015-09-30	2019-08-27	Apple Inc.	Pre-personalization of electronic subscriber identity modules
WO2017078459A1 *	2015-11-05	2017-05-11	Samsung Electronics Co., Ltd.	Method, ue and network node for protecting user privacy in networks
US10601831B2 *	2015-11-17	2020-03-24	Avaya Inc.	Accessing local information based on a browser session
US11063939B2 *	2015-12-01	2021-07-13	Huawei Technologies Co., Ltd.	Method and apparatus for secure interaction between terminals
FI128171B	2015-12-07	2019-11-29	Teliasonera Ab	Network authentication
DE102015016302A1 *	2015-12-15	2017-06-22	Giesecke & Devrient Gmbh	Agreement of exchange keys based on two static asymmetric key pairs
WO2017117357A1 *	2015-12-30	2017-07-06	Xiaolin Zhang	System and method for data security
GB2547039A *	2016-02-05	2017-08-09	Vodafone Ip Licensing Ltd	Secured service provisioning
WO2017177383A1 *	2016-04-12	2017-10-19	华为技术有限公司	Remote management method and device
CN107342964B *	2016-04-28	2019-05-07	华为技术有限公司	A message parsing method and device
CN105763325A *	2016-05-10	2016-07-13	中国联合网络通信集团有限公司	Encryption authentication method and device

KR101838511B1*	2016-05-17	2018-03-14	현대자동차주식회사	Method of providing security for controller using encryption and apparatus for implementing the same
CN106060069B*	2016-06-30	2019-09-13	飞天诚信科技股份有限公司	A kind of delivering key, dynamic password generate and the method and apparatus of certification
US10701206B2	2016-07-01	2020-06-30	Genesys Telecommunications Laboratories, Inc.	System and method for contact center communications
US10382475B2*	2016-07-01	2019-08-13	Genesys Telecommunications Laboratories, Inc.	System and method for preventing attacks in communications
KR102405409B1	2016-07-05	2022-06-08	삼성전자 주식회사	method and apparatus for specified attach procedure and mobility and paging support in data communication network
EP3482549A1 *	2016-07-11	2019-05-15	Telit Communications S.P.A.	Method and system for dual-network authentication of a communication device communicating with a server
WO2018018636A1*	2016-07-29	2018-02-01	北京小米移动软件有限公司	Information writing method and device
US11678291B2*	2016-08-21	2023-06-13	Qualcomm Incorporated	Methods and systems for support of location for the Internet of Things
US10394674B2*	2016-08-24	2019-08-27	Apple Inc.	Local recovery of electronic subscriber identity module (eSIM) installation flow
US10348502B2	2016-09-02	2019-07-09	Blackberry Limited	Encrypting and decrypting data on an electronic device
US10341102B2*	2016-09-02	2019-07-02	Blackberry Limited	Decrypting encrypted data on an electronic device
US10506439B2*	2016-09-16	2019-12-10	Apple Inc.	Secure control of profile policy rules
US11405863B2	2016-10-05	2022-08-02	Qualcomm Incorporated	Systems and methods to enable combined periodic and triggered location of a mobile device
WO2018067865A1*	2016-10-06	2018-04-12	Cryptography Research, Inc.	Generating an authentication result by using a secure base key
FR3060161A1 *	2016-12-08	2018-06-15	Orange	TECHNIQUE FOR MANAGING A RIGHT OF ACCESS TO A SERVICE FOR A COMMUNICATOR DEVICE
US10237063B2*	2016-12-13	2019-03-19	Nxp B.V.	Distributed cryptographic key insertion and key delivery
US9888385B1 *	2016-12-19	2018-02-06	Kwangwoon University Industry-Academic Collaboration Foundation	Method for subscriber authentication in cellular IoT device, IoT device for subscriber authentication, and base station apparatus for subscriber authentication
WO2018127278A1*	2017-01-04	2018-07-12	Gerhard Schwartz	Asymmetrical system and network architecture
US11832347B2	2017-01-13	2023-11-28	Huawei Technologies Co., Ltd.	Subscription profile downloading method, device, and server
FR3062768A1 *	2017-02-09	2018-08-10	Orange	TECHNIQUE FOR OBTAINING A PROFILE OF ACCESS TO A NETWORK
FR3062767A1 *	2017-02-09	2018-08-10	Orange	TECHNICAL ADMINISTRATION OF SUBSCRIPTION TO AN OPERATOR
KR102293683B1	2017-02-13	2021-08-26	삼성전자 주식회사	Apparatus and Methods for Access Control on eSIM
US10311224B1*	2017-03-23	2019-06-04	Amazon Technologies, Inc.	Digitally sealing equipment for authentication of components
US11533160B2*	2017-04-05	2022-12-20	Apple Inc.	Embedded universal integrated circuit card (eUICC) profile content management
US10579542B2*	2017-05-10	2020-03-03	Revbits, LLC	Browser session storage as storage for private key in public-key encryption schema
DE102017212994B3*	2017-05-31	2018-11-29	Apple Inc.	INSTALLATION AND TESTING OF AN ELECTRONIC PARTICIPANT IDENTITY MODULE (eSIM)
CN107248984B*	2017-06-06	2020-06-05	北京京东尚科信息技术有限公司	Data exchange system, method and device

US11061660B2	2017-06-07	2021-07-13	Huawei Technologies Co., Ltd.	Method for authenticating and updating EUICC firmware version and related apparatus
US10574662B2	2017-06-20	2020-02-25	Bank Of America Corporation	System for authentication of a user based on multi-factor passively acquired data
US10360733B2	2017-06-20	2019-07-23	Bank Of America Corporation	System controlled augmented resource facility
US11233634B1	2017-06-23	2022-01-25	Wells Fargo Bank, N.A.	Systems and methods for network authentication with a shared secret
FR3069680B1 *	2017-07-25	2019-09-20	Airbus Operations	DEVICE MANAGING INTERFACES IN AN AIRCRAFT
US11937080B2 *	2017-07-28	2024-03-19	Huawei Technologies Co., Ltd.	Method for updating network access application authentication information, terminal, and server
US10104078B1 *	2017-08-07	2018-10-16	Motorola Solutions, Inc.	Method and apparatus for associating sim card with a group of mobile communications devices
US20190052610A1 *	2017-08-11	2019-02-14	Honeywell International Inc.	Apparatus and method for encapsulation of profile certificate private keys or other data
CN109587674B *	2017-09-28	2022-04-29	展讯通信（上海）有限公司	Cloud SIM user identity recognition method and device and operator network side equipment
JP6818220B2 *	2017-10-19	2021-01-20	三菱電機株式会社	Key sharing device, key sharing method and key sharing program
US10306578B2 *	2017-10-24	2019-05-28	Verizon Patent And Licensing Inc.	Easy connectivity provisioning for cellular network
FR3074002B1 *	2017-11-21	2019-11-08	Sigfox	METHOD FOR ASSISTING THE REMOTE CONFIGURATION OF A EUICC CARD AND SYSTEM IMPLEMENTING SAID METHOD
US10708763B2 *	2017-11-30	2020-07-07	T-Mobile Usa, Inc.	On-boarding entity for remote embedded universal integrated circuit card management
US10349266B1 *	2018-01-23	2019-07-09	Nishi Kant	Method and system for programmatically changing the (U)SIM parameters to aid provisioning and distribution of internet of things devices globally
WO2019179925A1	2018-03-22	2019-09-26	British Telecommunications Public Limited Company	Wireless communication network authentication
GB2572326B *	2018-03-22	2020-09-30	British Telecomm	Wireless communication network authentication
WO2019213645A1 *	2018-05-04	2019-11-07	Tata Communications (America) Inc.	System and method for interoperability in remote provisioning architectures for embedded universal integrated circuit cards
EP3585083A1 *	2018-06-19	2019-12-25	Uros Technology S.à r.l.	Use of esim profile based on a list of geographical locations
EP3614706A1 *	2018-08-23	2020-02-26	Thales Dis France SA	Method for personalizing an improved uicc cooperating with a terminal
EP3621333A1 *	2018-09-05	2020-03-11	Thales Dis France SA	Method for updating a secret data in a credential container
US20220038431A1 *	2018-09-21	2022-02-03	Mark Macy	A Secure Multi-Layered Infrastructure Monitoring and Remote Connectivity System and Method
US11183773B2	2018-10-16	2021-11-23	Hook'd WiFi Inc.	Configurable communication system using stacked antennas
US11239570B2	2018-10-16	2022-02-01	Hook'd WiFi Inc.	Wireless communications system with scalable architecture
US20200119458A1 *	2018-10-16	2020-04-16	Hook'd WiFi Inc.	Wireless Access Point Using Stacked Antennas
US11232446B2	2018-10-26	2022-01-25	Hewlett Packard Enterprise Development Lp	Carrier grade telecom blockchain
US11310225B2	2018-10-26	2022-04-19	Hewlett Packard Enterprise Development Lp	Access to telecom blockchain-based services with digital passport

IT201800009905A1 *	2018-10-30	2020-04-30	St Microelectronics Srl	Procedure for the generation of customized profile package data in integrated circuit cards, corresponding system and IT product
US10911945B1*	2018-11-19	2021-02-02	Sprint Spectrum L.P.	Automated eUICC service profile configuration in view of operational issue with respect to eUICC service profile
US11483706B2*	2018-12-21	2022-10-25	Sprint Communications Company L.P.	Wireless media conferencing
US11625459B2	2019-02-08	2023-04-11	Raytheon Technologies Corporation	Embedded processing system with multi-stage authentication
US10757676B1*	2019-03-08	2020-08-25	Tile, Inc.	Commissioning electronic devices for use in a tracking system
EP3939213A4 *	2019-03-13	2022-10-05	Hitachi Vantara LLC	SYSTEMS AND METHODS FOR CONFIGURING AND TESTING AN EXTERNAL DEVICE VIA A MOBILE DEVICE
JP7231010B2 *	2019-03-20	2023-03-01	日本電気株式会社	CONTROL DEVICE, WIRELESS COMMUNICATION SYSTEM, CONTROL METHOD AND PROGRAM
US11956626B2*	2019-04-17	2024-04-09	Nokia Technologies Oy	Cryptographic key generation for mobile communications device
DE102019003674A1 *	2019-05-24	2020-11-26	Giesecke+Devrient Mobile Security GmbH	PROCEDURE FOR SETTING UP A SUBSCRIPTION PROFILE, PROCEDURE FOR PROVIDING A SUBSCRIPTION PROFILE, SUBSCRIBER IDENTITY MODULE
US11496299B2*	2019-06-18	2022-11-08	Thales Dis Cpl Usa, Inc.	Method and chip for authenticating to a device and corresponding authentication device and system
EP3757934A1 *	2019-06-27	2020-12-30	AGCO International GmbH	Integrated agricultural production system and method
US11039296B2*	2019-07-08	2021-06-15	Motorola Mobility Llc	Method and apparatus for disabling a carrier eSIM profile
WO2021040784A1*	2019-08-30	2021-03-04	Visa International Service Association	Gateway agnostic tokenization
US12047493B2*	2019-10-30	2024-07-23	EMC IP Holding Company LLC	Threshold-based override of data privacy using distributed ledgers and key shares
CN111083129A *	2019-12-09	2020-04-28	广州信天翁信息科技有限公司	Data secure transmission method, heterogeneous data transmission layer and system
WO2021115686A1*	2019-12-11	2021-06-17	Telefonaktiebolaget Lm Ericsson (Publ)	Enhancement of authentication
CN113038459A *	2019-12-25	2021-06-25	中兴通讯股份有限公司	Private information transmission method and device, computer equipment and computer readable medium
CN111162907B*	2019-12-28	2023-05-23	飞天诚信科技股份有限公司	Generation method of negotiation key and smart card device
KR102897283B1 *	2020-02-10	2025-12-09	삼성전자주식회사	Electronic device and method for processing profile policy rules of a embedded subscriber identity module in the electronic device
US11349664B2	2020-04-30	2022-05-31	Capital One Services, Llc	Local device authentication system
US11172350B1*	2020-06-15	2021-11-09	Apple Inc.	Subscription activation for mobile wireless devices
EP4172961A4 *	2020-06-29	2024-07-17	Allink Co., Ltd.	METHOD FOR UNLOCKING A VEHICLE DOOR USING A MOBILE TERMINAL
CN111797431B*	2020-07-07	2023-04-28	电子科技大学	A Method and System for Encrypted Data Anomaly Detection Based on Symmetric Key System
EP4179751A4 *	2020-08-07	2023-12-27	Samsung Electronics Co., Ltd.	METHOD AND DEVICE FOR INSTALLING AND MANAGING MULTIPLE ESIM PROFILES
ES2957476T3*	2020-08-11	2024-01-19	Marc Zacher	Procedure and system for the authentication of a computer device
CN112218294B*	2020-09-08	2021-08-27	深圳市燃气集团股份有限公司	5G-based access method and system for Internet of things equipment and storage medium

US12108305B2	2020-09-29	2024-10-01	Qualcomm Incorporated	System and methods for power efficient positioning of a mobile device
CN114760031A *	2020-12-26	2022-07-15	西安西电捷通无线网络通信股份有限公司	Identity authentication method and device
US11075901B1 *	2021-01-22	2021-07-27	King Abdulaziz University	Systems and methods for authenticating a user accessing a user account
US11831731B2	2021-02-23	2023-11-28	Prove Identity, Inc.	Proving possession of a communications device via a directed connection
CN113115307B *	2021-04-12	2021-10-26	北京邮电大学	Two-factor identity authentication method oriented to smart home scene
FR3122799B1 *	2021-05-06	2024-09-06	Continental Automotive	Method, device and system for transmitting confidential data between vehicles.
US12127305B2	2021-05-10	2024-10-22	Apple Inc.	Off-line profile provisioning for wireless devices
WO2022245817A1 *	2021-05-17	2022-11-24	Matrics2, Inc.	Using globally-unique numbers for all secure unique transactions, authentications, verifications, and messaging identities
US11792165B2 *	2021-06-04	2023-10-17	Bank Of America Corporation	Supporting data processing transactions using machine to machine (M2M) data transfer
US11784981B2 *	2021-06-04	2023-10-10	Bank Of America Corporation	Data processing transactions using machine to machine (M2M) data transfer
US12081988B2 *	2021-06-23	2024-09-03	Cisco Technology, Inc.	Authentication service with address rotation support
CN113573346B *	2021-07-12	2023-10-20	中国联合网络通信集团有限公司	Data processing method and device
US12432806B2 *	2021-08-03	2025-09-30	Nokia Technologies Oy	Inactive user equipment verification for data transmission in communication network
US12462871B2 *	2021-08-11	2025-11-04	Intel Corporation	Voltage detector for supply ramp down sequence
US11968523B2	2021-08-19	2024-04-23	Prove Identity, Inc.	Secure channel formation using embedded subscriber information module (ESIM)
US12316626B2	2021-09-14	2025-05-27	Prove Identity, Inc.	Device authentication via high-entropy token
DE102022001094A1 *	2022-03-30	2023-10-05	Giesecke+Devrient ePayments GmbH	Method for managing an application for the electronic identification of a user
GB2618143B *	2022-04-29	2025-08-06	Entotem Ltd	Locating a mobile radio-enabled tag
US20240080186A1 *	2022-09-07	2024-03-07	Google LLC	Random Trigger for Automatic Key Rotation
US12034496B1 *	2022-12-20	2024-07-09	Te Connectivity Solutions GmbH	Active module for high-speed cable assembly
US12457191B2 *	2023-03-06	2025-10-28	T-Mobile Usa, Inc.	User plane function configured to prioritize using a preferred internet protocol to establish a connection between user device and host server
EP4429293A1 *	2023-03-07	2024-09-11	Giesecke+Devrient Mobile Security Germany GmbH	Profile provisioning from euicc production machine to euicc
EP4601342A1 *	2024-02-12	2025-08-13	Giesecke+Devrient Mobile Security Germany GmbH	Providing an euicc with profile data of at least one profile

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
US12207094B2	2025-01-21	Embedded universal integrated circuit card supporting two-factor authentication
US11736283B2	2023-08-22	Key derivation for a module using an embedded universal integrated circuit card

US10187206B2	2019-01-22	Key derivation for a module using an embedded universal integrated circuit card
HK40064054A	2022-06-30	Mobile device with an embedded universal integrated circuit card
HK40064054B	2023-04-28	Mobile device with an embedded universal integrated circuit card
HK1233114B	2022-02-04	An embedded universal integrated circuit card supporting two-factor authentication

Priority And Related Applications

Parent Applications (2)

Application	Priority date	Filing date	Relation	Title
US16/110,804	2013-12-06	2018-08-23	Continuation	Embedded universal integrated circuit card supporting two-factor authentication
US16/110,804	2013-12-06	2018-08-23	Continuation-In-Part	Embedded universal integrated circuit card supporting two-factor authentication

Child Applications (1)

Application	Priority date	Filing date	Relation	Title
US17/547,990	2013-12-06	2021-12-10	Continuation	Embedded universal integrated circuit card supporting two-factor authentication

Priority Applications (6)

Application	Priority date	Filing date	Title
US16/453,682	2013-12-06	2019-06-26	Embedded universal integrated circuit card supporting two-factor authentication
US17/547,990	2013-12-06	2021-12-10	Embedded universal integrated circuit card supporting two-factor authentication
US18/416,534	2013-12-06	2024-01-18	Embedded universal integrated circuit card supporting two-factor authentication
US18/433,683	2013-12-06	2024-02-06	Embedded universal integrated circuit card supporting two-factor authentication
US18/435,042	2013-12-06	2024-02-07	Embedded universal integrated circuit card supporting two-factor authentication
US18/587,462	2013-12-06	2024-02-26	Embedded universal integrated circuit card supporting two-factor authentication

Applications Claiming Priority (5)

Application	Filing date	Title
US14/099,329	2013-12-06	Embedded universal integrated circuit card supporting two-factor authentication
US14/751,119	2015-06-25	Embedded universal integrated circuit card supporting two-factor authentication
US15/928,848	2018-03-22	Embedded universal integrated circuit card supporting two-factor authentication
US16/110,804	2018-08-23	Embedded universal integrated circuit card supporting two-factor authentication
US16/453,682	2019-06-26	Embedded universal integrated circuit card supporting two-factor authentication

Legal Events

Date	Code	Title	Description
2019-06-26	FEPP	Fee payment procedure	Free format text ENTITY STATUS SET TO UNDISCOUNTED (ORIGINAL EVENT CODE: BIG.); ENTITY STATUS OF PATENT OWNER: SMALL ENTITY
2019-07-08	FEPP	Fee payment procedure	Free format text ENTITY STATUS SET TO SMALL (ORIGINAL EVENT CODE: SMAL); ENTITY STATUS OF

PATENT OWNER: SMALL ENTITY

2019-07-12	STPP	Information on status: patent application and granting procedure in general	Free format text DOCKETED NEW CASE - READY FOR EXAMINATION
2019-07-24	AS	Assignment	Owner name M2M AND IOT TECHNOLOGIES, LLC, ILLINOIS Free format text ASSIGNMENT OF ASSIGNORS INTEREST;ASSIGNOR:NIX, JOHN;REEL/FRAME:049843/0981 Effective date 20171229
2019-08-13	AS	Assignment	Owner name NIX, JOHN A., ILLINOIS Free format text ASSIGNMENT OF ASSIGNORS INTEREST;ASSIGNOR:VOBAL TECHNOLOGIES, LLC;REEL/FRAME:050037/0798 Effective date 20180102
2019-08-14	AS	Assignment	Owner name NETWORK-1 TECHNOLOGIES, INC., NEW YORK Free format text ASSIGNMENT OF ASSIGNORS INTEREST;ASSIGNOR:M2M AND IOT TECHNOLOGIES, LLC;REEL/FRAME:050052/0487 Effective date 20171229
2021-01-15	STPP	Information on status: patent application and granting procedure in general	Free format text NON FINAL ACTION MAILED
2021-03-21	STPP	Information on status: patent application and granting procedure in general	Free format text RESPONSE TO NON-FINAL OFFICE ACTION ENTERED AND FORWARDED TO EXAMINER
2021-06-29	STPP	Information on status: patent application and granting procedure in general	Free format text NOTICE OF ALLOWANCE MAILED – APPLICATION RECEIVED IN OFFICE OF PUBLICATIONS
2021-08-09	STPP	Information on status: patent application and granting procedure in general	Free format text DOCKETED NEW CASE - READY FOR EXAMINATION
2021-08-19	STPP	Information on status: patent application and granting procedure in general	Free format text NOTICE OF ALLOWANCE MAILED – APPLICATION RECEIVED IN OFFICE OF PUBLICATIONS
2021-08-26	STPP	Information on status: patent application and granting procedure in general	Free format text DOCKETED NEW CASE - READY FOR EXAMINATION
2021-09-14	STPP	Information on status: patent application and granting procedure in general	Free format text NOTICE OF ALLOWANCE MAILED – APPLICATION RECEIVED IN OFFICE OF PUBLICATIONS
2021-12-10	STPP	Information on status: patent application and granting procedure in general	Free format text PUBLICATIONS – ISSUE FEE PAYMENT RECEIVED
2021-12-13	STPP	Information on status: patent application and granting procedure in general	Free format text PUBLICATIONS – ISSUE FEE PAYMENT VERIFIED
2022-01-05	STCF	Information on status: patent grant	Free format text PATENTED CASE
2025-09-10	AS	Assignment	Owner name NETWORK-1 TECHNOLOGIES, INC., CONNECTICUT Free format text CHANGE OF ADDRESS;ASSIGNOR:NETWORK-1 TECHNOLOGIES, INC.;REEL/FRAME:072827/0540 Effective date 20250606

2025-09-15	FEPP	Fee payment procedure	Free format text MAINTENANCE FEE REMINDER MAILED (ORIGINAL EVENT CODE: REM.); ENTITY STATUS OF PATENT OWNER: SMALL ENTITY
2025-11-11	FEPP	Fee payment procedure	Free format text SURCHARGE FOR LATE PAYMENT, SMALL ENTITY (ORIGINAL EVENT CODE: M2554); ENTITY STATUS OF PATENT OWNER: SMALL ENTITY
2025-11-11	MAFP	Maintenance fee payment	Free format text PAYMENT OF MAINTENANCE FEE, 4TH YR, SMALL ENTITY (ORIGINAL EVENT CODE: M2551); ENTITY STATUS OF PATENT OWNER: SMALL ENTITY Year of fee payment 4

Data provided by IFI CLAIMS Patent Services