



US009271148B2

(12) **United States Patent**  
**Bone**

(10) **Patent No.:** **US 9,271,148 B2**  
(45) **Date of Patent:** **Feb. 23, 2016**

(54) **AUTHENTICATION IN A WIRELESS TELECOMMUNICATIONS NETWORK**

(75) Inventor: **Nicholas Bone**, Thatcham (GB)

(73) Assignee: **Vodafone IP Licensing Limited**, Newbury Berkshire (GB)

(\* ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(58) **Field of Classification Search**

CPC ..... H04W 12/06; H04L 63/0853  
USPC ..... 726/5  
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,466,804 B1 10/2002 Pecen et al.  
2009/0233583 A1\* 9/2009 Weiner et al. .... 455/414.1  
2011/0032914 A1\* 2/2011 Venkateswaran et al. .... 370/338

FOREIGN PATENT DOCUMENTS

EP 1 487 228 A2 12/2004  
EP 1487228 A2 \* 12/2004

OTHER PUBLICATIONS

International-Search-Report-for-PCT-GB2011-051718 dated Dec. 21, 2011.

(Continued)

Primary Examiner — Jeffrey D Popham

(74) *Attorney, Agent, or Firm* — Workman Nydegger

(57) **ABSTRACT**

To facilitate authentication over a wireless access network, it is proposed to provide a hub device having an authentication storage means (i.e. a (U)SIM) to which one or more machine devices are connected. Each machine device connects to a wireless access network and in order to authenticate with that network requests authentication information from the hub device. The core network of the wireless access network, authenticates each machine device and provides the machine devices with parallel access to the access network in accordance with authentication information obtained from the hub device. The authentication information is unique to the respective machine device but also associated with information stored on the authentication storage means of the hub device.

**10 Claims, 5 Drawing Sheets**

(21) Appl. No.: **13/823,572**

(22) PCT Filed: **Sep. 14, 2011**

(86) PCT No.: **PCT/GB2011/051718**

§ 371 (c)(1),  
(2), (4) Date: **Jul. 2, 2013**

(87) PCT Pub. No.: **WO2012/035335**

PCT Pub. Date: **Mar. 22, 2012**

(65) **Prior Publication Data**

US 2014/0150073 A1 May 29, 2014

(30) **Foreign Application Priority Data**

Sep. 14, 2010 (GB) ..... 1015322.9

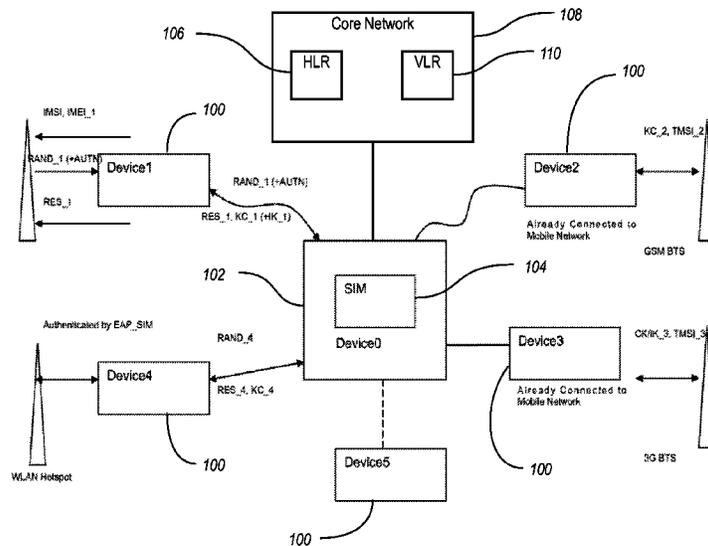
(51) **Int. Cl.**

**H04W 12/06** (2009.01)

**H04L 29/06** (2006.01)

(52) **U.S. Cl.**

CPC ..... **H04W 12/06** (2013.01); **H04L 63/0853**  
(2013.01)



(56)

**References Cited**

OTHER PUBLICATIONS

"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on the Security Aspects of Remote Provisioning and Change of Subscription for M2M Equipment;(Release 9)", 3GPP Draft; 53-091154-V3-

TR33812-140 Clean, 3rd Generation Partnership Project (3GPP), Mobile Competence Centre; 650,Route Des Lucioles; F-06921 Sophia-Antipolis Cedex ; France, no. Shanghai; 20090605, Jun. 5, 2009, XP050347761, [retrieved on Jun. 5, 2009] paragraph [0005] Paragraph [06.2].

\* cited by examiner

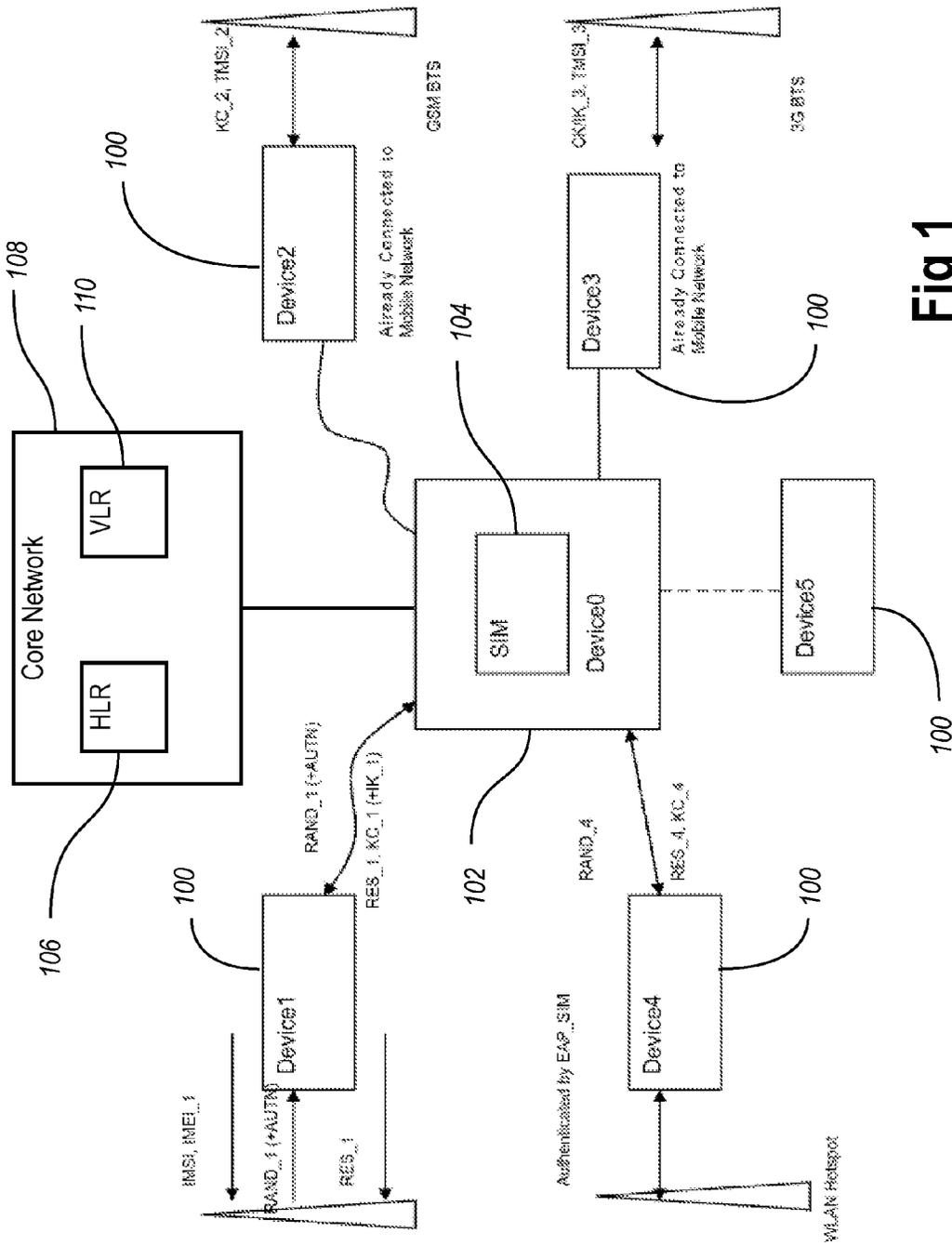


Fig 1

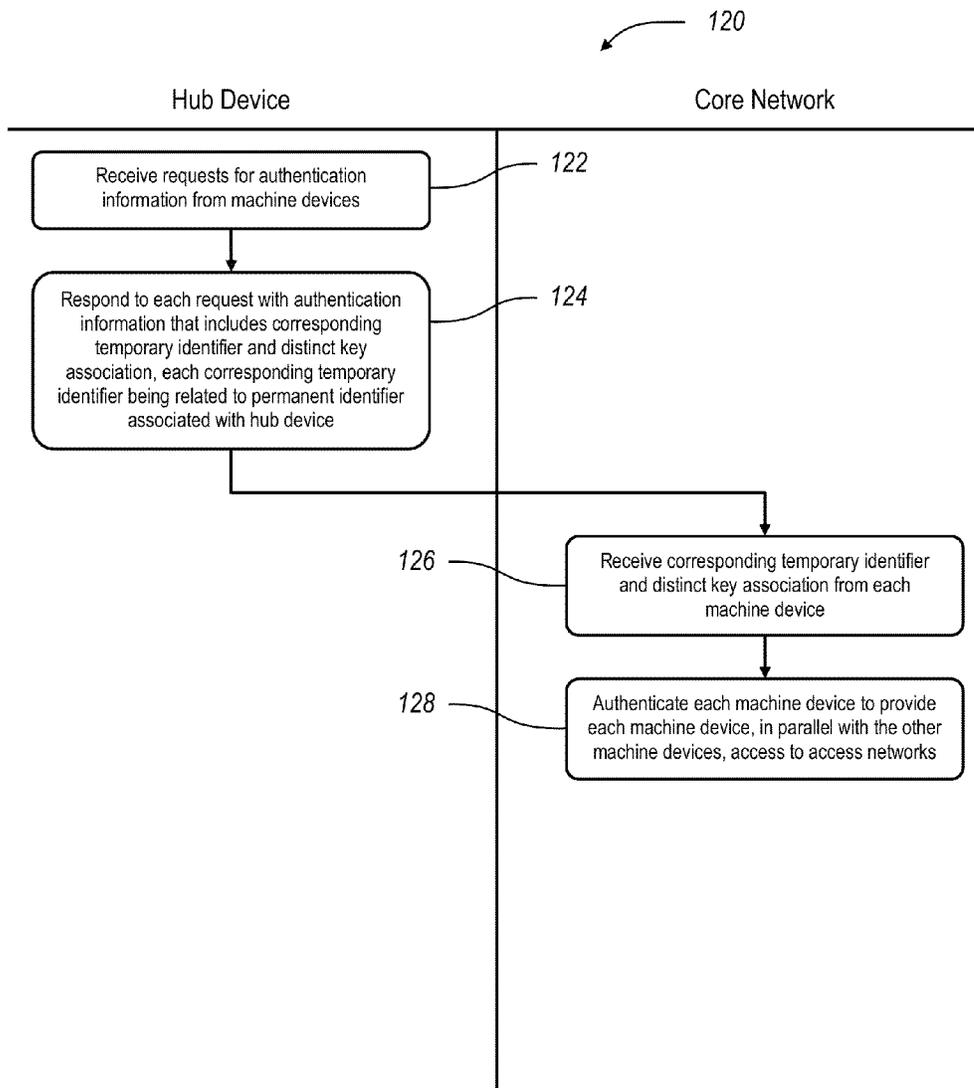


Fig. 2

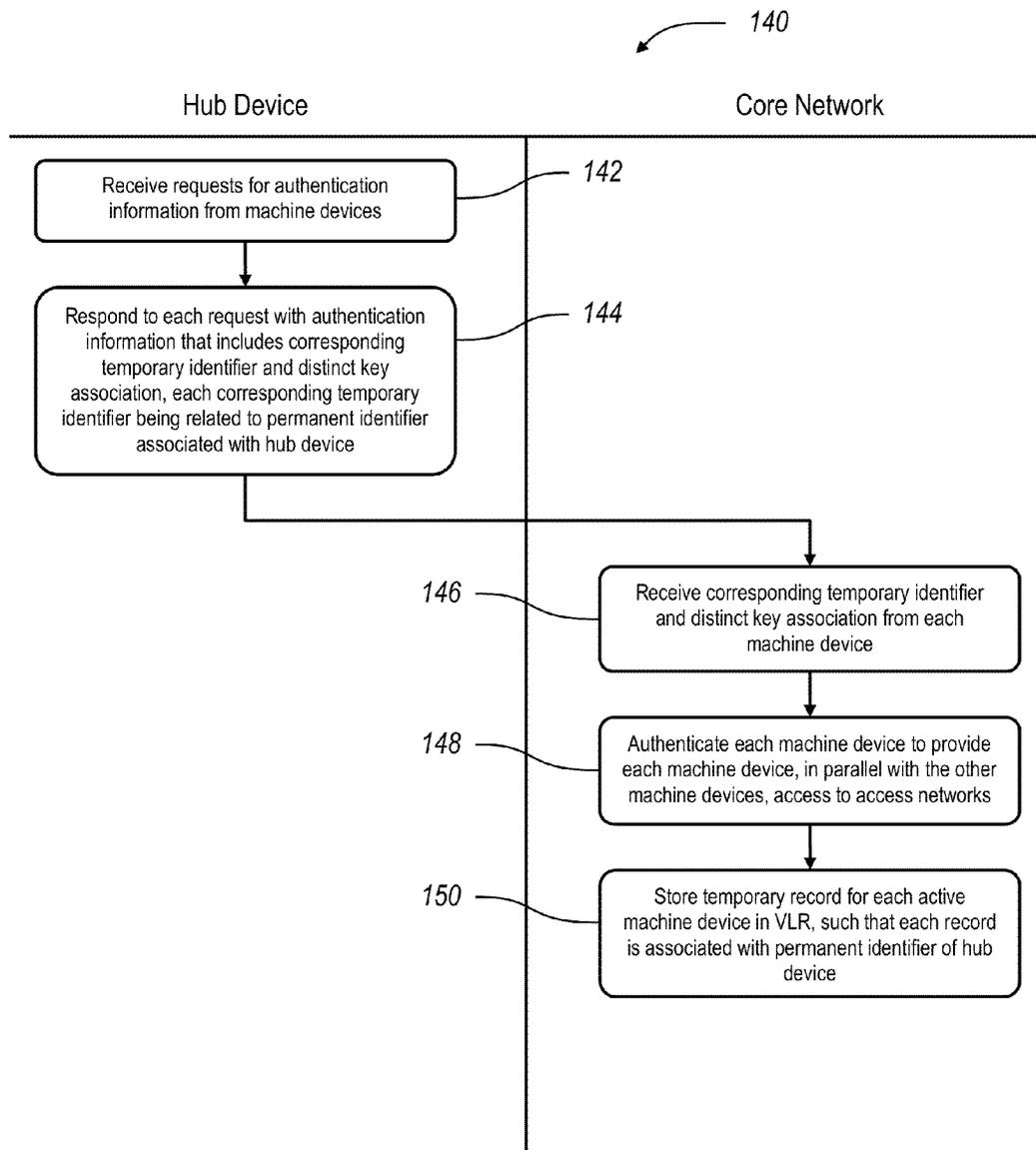


Fig. 3

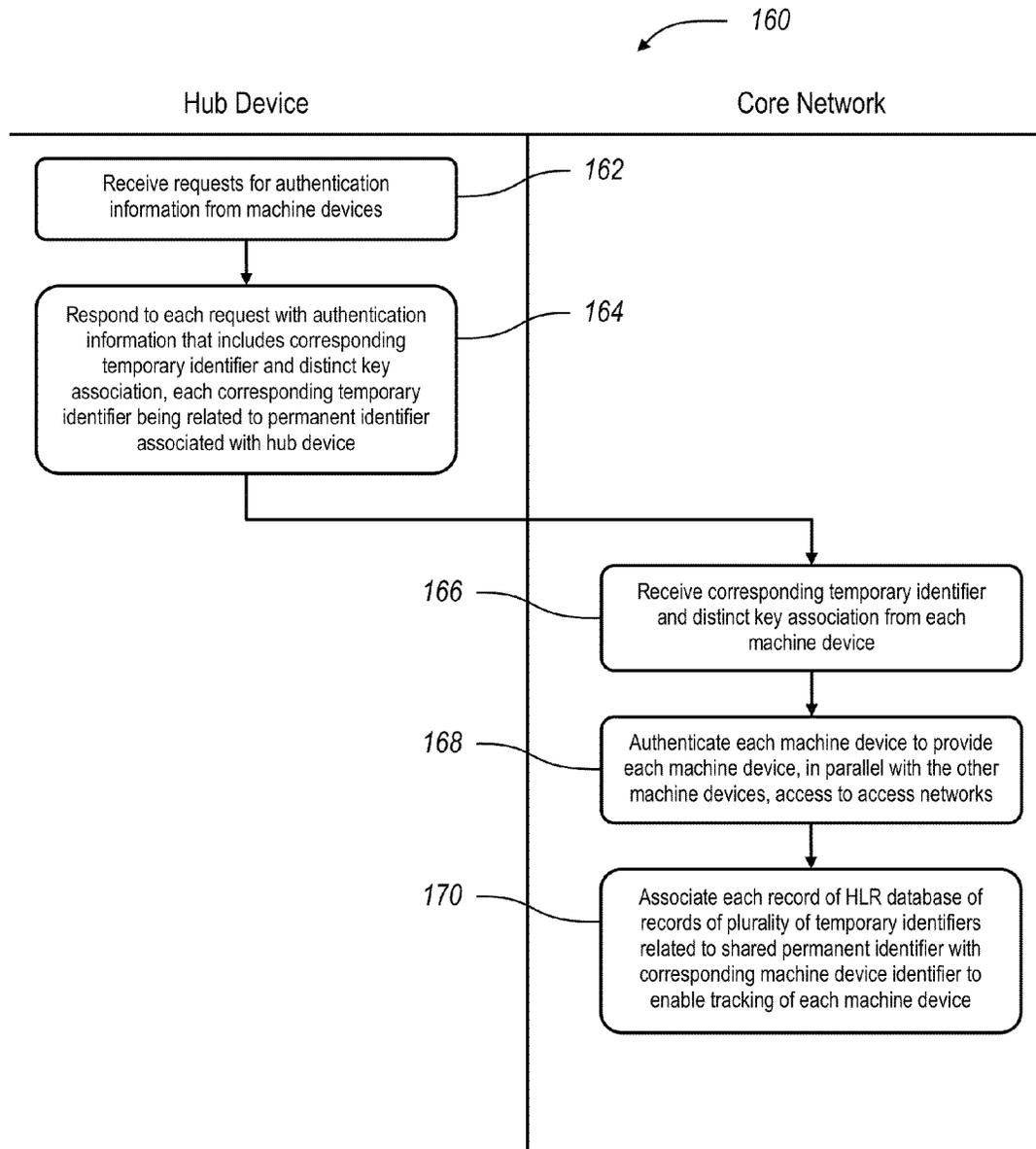


Fig. 4

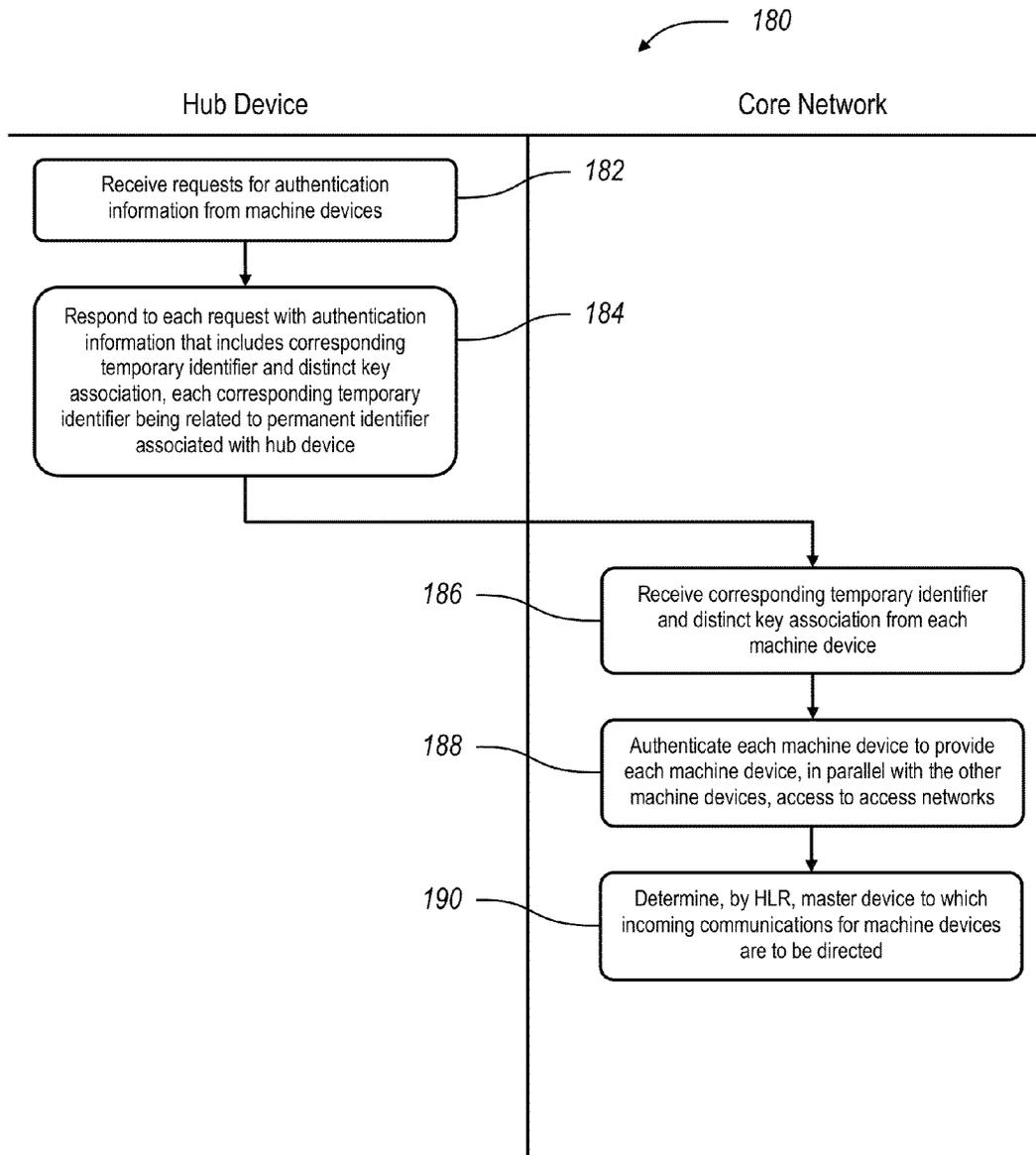


Fig. 5

1

**AUTHENTICATION IN A WIRELESS  
TELECOMMUNICATIONS NETWORK****CROSS REFERENCE TO RELATED  
APPLICATIONS**

This application is a U.S. Nationalization of International Application Number PCT/GB2011/051718, filed on Sep. 14, 2011, which claims priority to United Kingdom Patent Application No. 1015322.9, filed on Sep. 14, 2010, the entireties of which are incorporated herein by reference.

**FIELD OF THE INVENTION**

The invention relates to a method for authenticating large numbers of devices to a wireless telecommunications network.

**BACKGROUND TO THE INVENTION**

As a consequence of the decreasing costs of wireless telecommunications apparatus, tighter safety and climate regulation and vigorous market competition, an ever increasing number of devices (“machines”) are being provided with wireless telecommunications apparatus to facilitate additional information services. A particular driving factor in this trend has been the provision of wireless services to so-called machine to machine (M2M) solutions.

The term “M2M” has been used to describe applications in such diverse fields as: tracking and tracing; payment; remote maintenance; automotive and electronic toll; metering; and consumer devices. The augmentation of M2M to allow wireless communications between devices (often referred to as mobile M2M) makes new services possible in some cases (within the automotive industry, for instance) and in others extends existing M2M services (within the field of smart metering).

With mobile M2M, machines numbering in the order of millions and located anywhere within mobile network coverage, can be simultaneously monitored to provide real-time information that an individual or enterprise can analyze and act upon.

It is predicted that large numbers of “machines” will require access to wide-area mobile networks (such as the GSM, GPRS and/or 3G cellular networks). Each of these machines may only require authentication very occasionally but may have all the basic equipment to allow connection to at least one access network when that is required. However, just requiring that each device be allowed to authenticate itself to the network from time to time, may undermine the benefits of certain mobile M2M services (particularly those services that are predicated on a low cost machine/service).

Consider the implications of providing all such devices with a separate, provisioned SIM card. For each SIM card, the network operator must create a corresponding subscription and “provision” the SIM with a valid MSISDN corresponding to that subscription (i.e. a telephone number), both for the reservation of the MSISDN (regulators such as the ITU assign ranges of MSISDN numbers to operating companies) and overheads in registering the selected number for use with a given access network.

Where that SIM appears no longer (or never to have been) used for a predetermined period, the network operators typically note this fact and initiate a “quarantine” process for returning the telephone number to the set of available numbers. Of course, this quarantining process has an associated

2

cost: so too does reassigning that MSISDN number as ultimately will happen when it is confirmed unused after the quarantine period expires.

As the reader will readily appreciate, the provisioning of SIMs that are infrequently or never used represents a distinct inconvenience to the network operator. While this inconvenience is significant when considering the conventional provision of mobile telephones and data card/modems with SIMs, SIM-enablement of “machines” present additional problems simply by virtue of the number of these devices and their typical (low and sporadic) frequency of use. M2M applications are expected to increase significantly the number of unused or infrequently used SIMs and to cause a consequently greater level of disruption to the network operator who wishes to enable such devices. All the additional costs in terms of provisioning, quarantining (or keeping minimally active) etc of such machines can be relatively expensive and when compared with the potential market for the mobile M2M service may be found incompatible with low cost services.

Alternatively devices could have a “soft SIM” (a SIM module in software or firmware) instead, but this has major security issues, and there is still significant cost to the network operator (requiring heavy usage of the core network components in particular the home location register (HLR) and the authentication centre (AuC)) and arranging provisioning/creating subscriptions.

In a further alternative, it would be possible for devices to have some other form of authentication technology. However such a solution would require major network re-design, and could potentially prevent connection onto existing 3G and GSM networks.

It is therefore an object of the invention to obviate or at least mitigate the aforementioned problems.

In accordance with one aspect of the present invention, there is provided a system for facilitating authentication over a wireless access network, the system comprising:

a hub device having an authentication storage means, which is operable to provide authentication information during an authentication process;

at least one machine device being operable to connect to the wireless access network and having a communication interface with the hub device, through which a request for authentication information is made; and

a core network, which is operable to authenticate each machine device and provide said machine devices with parallel access to one or more access networks in accordance with authentication information obtained from the hub device.

It is preferred that a plurality of machine devices are provided with parallel access and the authentication information obtained from the hub device for each machine device includes a corresponding temporary identifier (such as the TMSI for UTRAN or GUTI for LTE) and a distinct key association (e.g. in LTE, K\_ASME), each corresponding temporary identifier being related to a permanent identifier (e.g. an IMSI) associated with the hub device.

**BRIEF DESCRIPTION OF THE DRAWINGS**

For a better understanding of the present invention, reference will now be made, by way of example only, to the accompanying drawings in which:

FIG. 1 illustrates the operation of the present invention.

FIG. 2 illustrates a method of the present invention according to one embodiment.

FIG. 3 illustrates a method of the present invention according to one embodiment.

FIG. 4 illustrates a method of the present invention according to one embodiment.

FIG. 5 illustrates a method of the present invention according to one embodiment.

#### DETAILED DESCRIPTION

Rather than provide each machine with its own SIM and tolerate the level of signalling that that would entail, the invention facilitates authentication of multiple devices using the same (U)SIM.

Typically, as shown in FIG. 1, the devices 100 are joined to a SIM-containing device 102 (referred to hereafter as the “hub” device) via a variety of short-range connections (USB, WLAN, ZigBee®, NFC etc.) and/or long-range connections and secure channels.

When each device 100 needs to authenticate to a wide-area mobile network (or heterogeneous access network) it forwards a challenge to the (U)SIM 104 and receives back a RES and key material (Kc or CK||IK).

Multiple devices can thus be connected substantially simultaneously, each with a distinct TMSI (or in LTE, GUTI) and key association (in LTE, K\_ASME) but all related to the underlying IMSI, and billed against the same subscription.

To facilitate this behaviour in a cellular telecommunications access network (such as a GSM network, 3G network or LTE network), some changes to the HLR 106 and other parts of the core network 108 are required. In a first instance, the HLR must track multiple devices at once, and single out a “master” device (for example, the hub device) to receive incoming calls, SMS etc. In an alternative, the HLR may only track the “master” device, on the assumption that the other devices never need to be routed to (i.e. they have data-only connections and there is no incoming traffic accepted).

A number of mechanisms are available to indicate to the HLR which device is the “master”, examples include: a special flag in the IMSI (dedicated bit) which indicates when connecting or doing location-updates with the master; or use of the IMEI which is presented at connection or location update (with a separate record indicating which device is the master).

Further core network changes are necessitated by the invention:

The visitor location register (VLR) 110, associated with a mobile switching centre (MSC) currently maintains only one record per IMSI, with associated TMSI and Kc (or CK||IK for UMTS). To support the above, the VLR must maintain multiple records i.e. same IMSI may have multiple TMSIs at once, and the VLR must associate each TMSI with corresponding IMEI.

The HLR may maintain multiple records per IMSI, and associate each record with IMEI so it can track each device’s location. This requires IMEI to be reported to HLR along with IMSI during Location Updates. This can be done using techniques such as the “Automatic Device Detection” facility standardised in 3GPP Release 6

Alternatively, the HLR only tracks the location of one device (e.g. “master” device for incoming calls, SMS etc.). Location Updates with the “master” device conveniently report a base IMSI (say IMSI\_0) and other devices report an offset IMSI, say IMSI\_0+1. The HLR then need only track updates reporting IMSI\_0.

FIG. 2 illustrates one embodiment 120 of a method for facilitating authentication of machine devices over one or more wireless access networks via a hub device having an

authentication storage means. At step 122, the hub device receives requests for authentication information from a plurality of machine devices. At step 124, the hub device responds to each request with authentication information that includes a corresponding temporary identifier and a distinct key association, each corresponding temporary identifier being related to a permanent identifier associated with the hub device. At step 126, the core network associated with the one or more wireless access networks receives the corresponding temporary identifier and distinct key association from each machine device. At step 128, the core network authenticates each machine device to provide each machine device, in parallel with the other machine devices, access to access the one or more access networks.

FIG. 3 illustrates another embodiment 140 of a method for facilitating authentication of machine devices over one or more wireless access networks via a hub device having an authentication storage means. Steps 142-148 are identical to steps 122-128 of method 120. However, method 140 includes an additional step 150. At step 150, the core network stores in the VLR a temporary record for each active machine device such that each record is associated with the permanent identifier of the hub device.

FIG. 4 illustrates another embodiment 160 of a method for facilitating authentication of machine devices over one or more wireless access networks via a hub device having an authentication storage means. Steps 162-168 are identical to steps 122-128 of method 120. However, method 160 includes an additional step 170. At step 170, the core network associates each record of an HLR database of records of a plurality of temporary identifiers related to the shared permanent identifier with a corresponding machine device identifier to enable tracking of each machine device.

FIG. 5 illustrates another embodiment 180 of a method for facilitating authentication of machine devices over one or more wireless access networks via a hub device having an authentication storage means. Steps 182-188 are identical to steps 122-128 of method 120. However, method 180 includes an additional step 190. At step 190, the core network determines, by the HLR, a master device to which incoming communications for the machine devices are to be directed.

A number of implementations may be considered:

In a first embodiment, consider a vast array of sensors in a building or on a campus. With the present invention, a single SIM-holding device, to which sensors are locally connected, may be used to perform authentication on behalf of each sensor. Sensors have a low bandwidth radio (just to confirm that they are “OK” or “alert” every so often). The SIM-holding device is preferably portable (e.g. a security guard carrying a mobile phone); devices only temporarily in range.

In another embodiment, sensors are installed on parcels, delivery crates etc. travelling away from a depot, then back again, or between depots. They connect to the SIM-holding device when in depot.

In a third embodiment, consider a home energy system with multiple devices reporting usage, adapting usage, sending alarms etc. In this case the SIM-holding device is the home owner’s mobile phone; and the owner is only around in the evening.

The invention claimed is:

1. A system for facilitating authentication of machine devices over a wireless access network, the system comprising:

a hub device having an authentication storage means operable to provide authentication information during an authentication process;

5

a plurality of machine devices each operable to connect to a wireless access network and each having a communication interface with the hub device, through which requests for authentication information are made to the hub device; and

a core network operable to authenticate each machine device;

wherein, during the authentication process, the hub device is operable to respond to each request with authentication information that includes a corresponding temporary identifier and a distinct key association, each corresponding temporary identifier being related to a permanent identifier associated with the hub device,

wherein the authentication information provided to the machine devices enables said machine devices to be concurrently authenticated with the core network so as to allow the machine devices to concurrently access the wireless access network,

wherein the core network includes a home location register operable to maintain a database of records of the temporary identifiers corresponding to the authenticated machine devices so as to associate each temporary identifier with the permanent identifier of the hub device and to associate each record with the corresponding machine device identifier to enable tracking of the location of each machine device, the home location register also being operable to identify a master device as representative of the plurality of machine devices associated with the hub device by incorporating a flag in the permanent identifier or the temporary identifiers, or by using a base as the permanent identifier and offsets from the base as the temporary identifiers, and

wherein the core network includes a visitor location register for storing temporary records corresponding to the machine devices that are authenticated with the core network, wherein the visited location register is configured to store a record for each authenticated machine device, such that each temporary record is related to the permanent identifier of the hub device.

2. The system as claimed in claim 1, wherein the requests for authentication information are challenges to the authentication storage means and wherein the authentication information obtained from the hub device includes key material.

3. The system as claimed in claim 1, wherein the a home location register is operable to redirect to the master device all incoming communications directed to any of the machine devices, the master device being the hub or one of the machine devices.

4. The system as recited in claim 1, wherein the permanent identifier associated with the hub device is an International Mobile Subscriber Identity (IMSI).

5. The system as recited in claim 1, wherein the authentication storage means comprises a Subscriber Identity Module (SIM).

6

6. The system as recited in claim 1, wherein the base is an International Mobile Subscriber Identity (IMSI) and the temporary identifiers are offset from the IMSI.

7. A method for facilitating concurrent authentication of machine devices via a hub device having an authentication storage means, the method comprising:

at the hub device,

receiving requests for authentication information from each of a plurality of machine devices; and

responding to each request with authentication information that includes a corresponding temporary identifier and a distinct key association, each corresponding temporary identifier being related to a permanent identifier associated with the hub device;

in each of the machine devices,

receiving the corresponding temporary identifier and distinct key association from the hub device; and

sending the corresponding temporary identifier and distinct key association to a core network associated with a wireless access network; and

in the core network,

receiving the corresponding temporary identifier and distinct key association from each machine device, authenticating each machine device to provide said machine devices with concurrent access to the wireless access network;

maintaining a home location register that includes records of the temporary identifiers corresponding to the authenticated machine devices so as to associate each temporary identifier with the permanent identifier of the hub device and to associate each record with the corresponding machine device identifier to enable tracking of the location of each machine device, the home location register being operable to identify a master device as representative of the plurality of machine devices associated with the hub device by incorporating a flag in the permanent identifier or the temporary identifiers, or by using a base as the permanent identifier and offsets from the base as the temporary identifiers; and

storing a temporary record for each authenticated machine device in a visitor location register, such that each temporary record is related to the permanent identifier of the hub device.

8. The method as recited in claim 7, further comprising redirecting to the master device all incoming communications directed to any of the machine devices, the master device being the hub or one of the machine devices.

9. The method as recited in claim 7, wherein the permanent identifier associated with the hub device is an International Mobile Subscriber Identity (IMSI).

10. The method as recited in claim 7, wherein the base is an International Mobile Subscriber Identity (IMSI) and the temporary identifiers are offset from the IMSI.

\* \* \* \* \*