

A COMMUNICATION SYSTEM

BACKGROUND

[0001] WiMAX or LTE communications networks are used to provide “last
5 mile” wireless broadband internet access. Being wireless however, the
microwave air traffic between the device and the access point has security
vulnerabilities, for example wireless eavesdropping may be possible. The
Transport Layer Security (TLS) protocol is thus commonly used for access
authentication. The TLS protocol however ties the device to a subscriber.

[0002] WiMAX or LTE communications networks may also provide
10 multimedia services using servers in the backend of the network. Such
multimedia services typically require one or more security logins. This results in
inconvenience for the user as the user will need to provide at least two different
logins to access multimedia services – a login for access to the WiMAX or LTE
15 communications network, as well as a login for multimedia services. Typical
multimedia backends may also use XML Configuration Access Protocol (XCAP)
as the protocol for synchronizing user configuration and information between
server components of the backend.

[0003] Beyond the usage of WiMAX or LTE, communications networks may
20 also be implemented using multiple other access modes such as Wi-Fi or fixed
line services. Each of these different access modes typically may have their own
authentication and access control frameworks.

[0004] In order for communications to take place between devices in a
network, each device traditionally is uniquely associated with a phone number.

25 Should a user be carrying multiple devices, each of these devices will have its

own unique phone number. Communications links can thus be established by calling at an originating device the phone number of a destination device. The trend ahead however points towards a proliferation of devices where each user may have many devices associated with him. This result in a multitude of phone numbers associated with each user, thus making communications inconvenient.

SUMMARY

[0005] In an embodiment, a wireless communications system is disclosed. The wireless communications system comprises a network configured to wirelessly connect a plurality of devices via plurality of modes of network access, and wherein the plurality of modes of network access includes a WiMAX or LTE access mode, and wherein the WiMAX or LTE access mode is configured for device independent authentication.

[0006] Optionally, the device independent authentication may comprise TTLS. The system may further comprise a database comprising user datasets, each user dataset configured to associate a user identity with a device independent public identity, and wherein the TTLS authentication is performed using the public identity of one of the user datasets. The system may further comprise an IP multimedia subsystem configured to connect each device via the backhaul network to a core network, and wherein each user dataset is further configured to associate the user identity with a private identity, the private identity used for authenticating the connection of each device to the core network. Each user dataset may be further configured to associate the user identity with one or more devices. The private identity may be uniquely associated with one of the one or more devices of the user identity. The private identity may be

automatically generated by an algorithm. Optionally, the algorithm may combine the public identity of the user dataset with an identifier selected from the group consisting of the type of one of the one or more devices of the user dataset, a model of one of the one or more devices of the user dataset, and a number uniquely identifying one of the one or more devices from amongst the other of the one or more devices. Optionally, a request for a communication link to a user identity may be sent to all of the devices associated with that user identity. All of the devices associated with each user identity may be assigned a priority value. A request for a communication link to a user identity may be sent to one of the devices associated with that user identity according to the priority value of the device. Each user identity may be associated with a profile page. Each profile page may comprise a plurality of public fields viewable depending on a friend status with the associated user identity. Optionally, the IP multimedia subsystem may comprise a server configured to serve the profile pages. Each profile page may be served using a schema.

[0007] In an embodiment, a wireless communication device is disclosed. The wireless communication device comprises a communications circuit configured to wirelessly connect via plurality of a modes of network access, a secure login interface configured to authenticate a user with a user identity of a communications system, wherein the device is configured to allow concurrent association of a plurality of user identities, wherein request for a communications link to any of the user identities currently logged into the device are received by the device.

[0008] Optionally, the device may further comprise an interface for a network-based address book, stored on a remote server and accessible via the device. The device may further comprise an interface for a network-based address book, stored on a remote server and accessible via the device. The device may also
5 further comprise an interface for a network-based address book, stored on a remote server and accessible via the device. The device may further comprise an interface for a locally stored address book, wherein a copy of the locally stored address book is stored on a remote server and refreshed/synchronised with the locally stored address book. The remotely stored address book may be
10 stored using XCAP, and wherein SyncML is used to refresh/synchronise the remotely stored address book.

[0009] In an embodiment, a method of registering a wireless communication device is disclosed. The method of registering a wireless communication device comprises connecting a communication device via a wireless access network,
15 registering the device on a multimedia sub-system using a common public identifier and a common password associated with the common public identifier, and requesting a communication link with the device according to the common public identifier and a common password.

[0010] These and other features will be more clearly understood from the
20 following detailed description taken in conjunction with the accompanying drawings and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] For a more complete understanding of the present disclosure, reference is now made to the following brief description, taken in connection with

the accompanying drawings and detailed description, wherein like reference numerals represent like parts.

[0012] FIG. 1 is a schematic drawing of a communication system according to an embodiment of the disclosure.

5 [0013] FIG. 2 is a schematic drawing of the core network of the communication system of FIG. 1.

[0014] FIG. 3 is a flow chart showing a method of registering a device with the communication system of FIG. 1.

10 [0015] FIG. 4 is a flow chart showing a method for establishing a communication link between devices of the communication system of FIG. 1.

[0016] FIG. 5 is a schematic drawing illustrating a user dataset for the communication system of FIG. 1.

DETAILED DESCRIPTION

15 [0017] It should be understood at the outset that although illustrative implementations of one or more embodiments are illustrated below, the disclosed systems and methods may be implemented using any number of techniques, whether currently known or not yet in existence. The disclosure should in no way be limited to the illustrative implementations, drawings, and techniques illustrated below, but may be modified within the scope of the
20 appended claims along with their full scope of equivalents.

[0018] As the number of devices that are capable of providing communications services increases; users may carry multiple mobile phones. Also other devices such as digital cameras or MP3 players or home appliances

such as refrigerators or televisions may also require communications connectivity. Thus each user may have wireless connectivity via many devices.

[0019] The present disclosure thus contemplates providing convenient access to the multiple devices associated with each user. This may be done in a secure and device agnostic manner, and the devices may be access agnostic. Each user may be associated with a single user profile that provides connectivity to all the devices associated with the user across different modes of network access. Taking Voice-over-IP (VoIP) as an example, such a user profile may be associated with multiple phone numbers. Calling any of the phone numbers associated with a user results in all the devices associated with the user ringing. The user may then accept the call on any of the ringing devices without additional logins. This may thus result in a secure and easy way of establishing a communication link between users.

[0020] In certain embodiments, the association of each user with a single profile may take the form of a single login – a user provides a single login on a device in order to have network access, as well as access to the multimedia services provided by the network. Such a single login may be implemented at an enhanced level of authentication security with for example, the Tunnelled Transport Layer Security (TTLS) protocol.

[0021] The conceptual association of each user with his or her user identifiers, devices and subscriber information may further enhance the concept of unified communications. Each user may be associated with one or many user identities taking the form of for example, phone numbers. Each user identity may be associated with one or many devices. Each device also may be associated

with multiple user identities. In other words, certain devices may be configured to be associated with multiple user identities, in which case these devices may be reachable by placing a connection to any of the multiple user identities associated with the user profile.

5 [0022] Turning now to FIG. 1, a schematic drawing of a communication system 100 according to an embodiment of the present invention is shown. The communication system 100 comprises a plurality of network appliances 120a – 120g and a plurality of access points 130a – 130c that communicate with each other using Internet Protocol (IP). The network appliances 120a – 120g may be
10 any of a variety of devices known to a skilled person, for example mobile devices such as mobile phones or laptop computers, or alternatively, static devices such as computer servers, desktop computers or gateways to client local area networks (LANs). It however is envisaged in a preferred embodiment that the network appliances 120a – 120g may be proprietary mobile devices having a
15 form factor similar to that of a mobile phone. Also, the access points 130a – 130c may be any of a variety of wired or wireless access points known to the skilled person. The access points 130a – 130c may for example be, as illustrated in FIG. 1, wireless access points such as WiMAX or LTE base stations 130a, 130b or Wi-Fi base stations 130c. Alternatively, other modes of wireless access such
20 as High-Speed Downlink Packet Access (HSDPA), General Packet Radio Service (GPRS) or satellite connection may be used. Optionally, the access points 130a – 130c may also be wired connections such as for example Digital Subscriber Lines (DSL), telephone lines or power-line internet.

[0023] In the case where WiMAX or LTE is used as a mode of access, it is envisaged that appliances which do not have built-in WiMAX or LTE access capability may gain WiMAX or LTE access using a Customer Premises Equipment (CPE) 160 or a WiMAX or LTE router 162. The WiMAX or LTE router 162 is capable of sharing a single WiMAX or LTE connection with multiple appliances. In the example illustrated in FIG. 1, the network appliance 120f uses the CPE 160 to gain WiMAX or LTE access and the network appliances 120c-120e share a WiMAX or LTE connection using the router 162.

[0024] The access points 130a – 130c are interconnected by way of a backhaul network 110. The backhaul network 110 uses the IP protocol for connections. The backhaul network 110 typically has a high connection bandwidth and may comprise wired and/or wireless connections. The backhaul network 110 also connects the access points 130a – 130c to a core network 150. The core network 150 is comprised of a network of interconnected servers responsible for providing services such as user registration and authentication, call routing or multi-media services. Collectively, the WiMAX or LTE access points 130a, 130b and the associated backhaul network 110 may be referred to as the WiMAX or LTE radio access network (RAN).

[0025] The network appliances 120a – 120g are typically associated with subscribed users 140a – 140c. In FIG. 1, the network appliance 120b is associated with a subscribed User A 140a, the network appliances 120c – 120e are associated with another subscribed User B 140b, while the network appliances 120e – 120g are associated with a subscribed User C 140c. Some appliances thus may be associated with more than one user, for example the

network appliance 120e is associated with both subscribed User B 140b and User C 140c.

[0026] FIG. 2 shows a schematic drawing of the core network 150 of the communication system 100 of FIG. 1. The core network 150 is comprised of a plurality of servers each responsible for providing a service. The skilled person will understand that the network topology illustrated in FIG. 1 is only an example and other network topologies may be used. For example, the core network 150 may be connected to the backhaul network 110 across multiple redundant connections. Alternatively, the core network 150 may also be connected to the backhaul network 110 across a single gateway.

[0027] The core network 150 comprises an Authentication, Authorization and Accounting (AAA) server 210. This server is responsible for authenticating the network appliances 120a – 120g and then allowing appliances which have passed authentication access to the communication system 100. The AAA server 210 is primarily used to control access via the WiMAX or LTE access points 130a, 130b. However, a common AAA server 210 may be used to control access for all the different access modes in a unified manner. In the latter case, the AAA server 210 controlling access via the WiMAX or LTE access points 130a, 130b may be the same server controlling access via Wi-Fi access points 130c and/or other wired and wireless access points.

[0028] The core network 150 also comprises a Content Services Gateway (CSG) server 276 and a Billing and Revenue Management (BRM) server 278. The CSG server 276 and the BRM server 278 work together to perform subscriber usage metering and billings. The CSG server 276 serves as a

gateway which performs the actual usage metering according to the operator's usage and pricing strategy. The usage measured for each subscriber is sent to the BRM server 278. The BRM server 278 then calculates the usage costs incurred by each subscriber and bills the subscriber. The CSG server 276 may be from a vendor like Cisco Systems Inc. while the BRM server 278 may be from a vendor like Oracle Inc. In this case, the CSG server 276 communicates using the GPRS tunnelling protocol (GTP) while the BRM server 278 communicates using the Diameter protocol. Since different protocols are used for the servers, a bridge is implemented between both servers to perform two-way interpretation of the communications between the servers. An example of such a bridge may be the Openet Platform software.

[0029] The core network 150 also comprises a Dynamic Host Configuration Protocol (DHCP) server 258. The DHCP server 258 is responsible for allocating IP addresses to the network appliances 120a – 120g. This is done primarily during device registration when an appliance negotiates for access to the communication system 100 via WiMAX or LTE. It is however envisaged that the DHCP server 258 may not be used exclusively for WiMAX or LTE access, in which case a single DHCP server 258 may be used to allocate IP addresses across multiple modes of access.

[0030] The core network 150 further also comprises a Service Control Engine (SCE) 272 and a Home Agent (HA) 274. The SCE 272 is responsible for monitoring end-to-end traffic QoS measures between the core network 150 and the network appliances 120a – 120g, as well as propagating QoS policies and settings to the routers and/or switches. The HA 274 serves as a static point of

contact on the core network 150 for the network appliances 120a – 120g so that if a network appliance were to switch to a different access network, traffic can still be conveyed between the core network 150 and the network appliance without interruption.

5 [0031] Further, the core network 150 also comprises an IP Multimedia Subsystem (IMS) 250 which is connected to the backhaul network 110. The IMS 250 comprises a plurality of servers which together provide multimedia functionality such as, but not limited to, Voice-over-IP (VoIP), Instant Messaging (IM) and information synchronization.

10 [0032] The IMS 250 comprises one or more Call Session Control Function (CSCF) gateways 260. The CSCF gateways 260 serve as an initial point of contact for the network appliances 120a – 120g to access the IMS 250. There may be multiple CSCF gateways 260 in the IMS 250 in which case the gateways may be configured such that different modes of access utilize different gateways.

15 Alternatively, the IMS 250 may use a single CSCF gateway 260 such that all modes of access will utilize the common CSCF gateway 260.

20 [0033] The IMS 250 also comprises a Home Subscriber Server (HSS) 252 that is responsible for authenticating users and authorizing access to the services provided by the IMS 250. The HSS 252 may have a user information database separate from that of the AAA server 210. In this case, different user identities may be used to login to the WiMAX or LTE and IMS networks.

[0034] Optionally, the databases associated with the AAA server 210 and HSS server 252 may be synchronized with each other. This synchronization may be partial or may be complete. With partial synchronization each database may

respectively contain only data fields relevant to its associated server, whilst still having common data fields. As an example, the database co-located with the AAA server 210 may contain data fields specific for network access control, as well as general user information and the HSS 252 may contain data fields relating to IMS 250 user rights in addition to the general user information. In such a case, only the general user information is synchronized between both databases. By synchronizing the databases of the AAA server 210 with the HSS server 252, a common login may be used for WiMAX or LTE access and IMS access, thus providing the advantage of a single login. A single login may require a user to enter his login ID and password only once per session. Alternatively, this single login identity may be stored on the appliance and be used for automated logins.

[0035] The IMS 250 further comprises a Session Border Controller (SBC) 254 that is responsible for setting up, maintaining and terminating communication links between network appliances 120a – 120d. Examples of such communication links may be VoIP links or video conferencing links.

[0036] The IMS 250 also comprises an IMS server 262. The IMS server 262 is responsible for session control and in conjunction with the SBC 254 is responsible for communications link establishment. The IMS server 262 also serves as a link to the feature servers 256 and/or application servers 264.

[0037] The IMS 250 also comprises one or more feature servers 256 or application servers (AS) 264. The feature servers 256 provide features for the establishment and functioning communication links, for example call forwarding or voice mail routing features for a VoIP link. The application servers 264 then

provide multimedia services such as Instant Messaging, a network based address book, user profile services or user information synchronization for refreshable phones.

[0038] The IMS 250 is interconnected with other existing communication networks by the use of gateways. For example, the IMS 250 allow incoming links from a Public Switched Telephone Network (PSTN) to be established with one of the network appliances 120a – 120g by having a Multimedia Gateway (MGW) server 266 between the PSTN and the IMS 250. Further, the IMS 250 is connected to the Internet 270 by an Session Border Controller (SBC) 254. The Internet 270 exists outside of the communication system 100 and the Session Border Controller (SBC) 254 thus serves as a gateway between the IMS 250 and the Internet 270 for the purpose of providing voice services.

User dataset

[0039] FIG. 5 is a schematic drawing illustrating a user dataset 500 for the communication system of FIG. 1. The dataset 500 contains the relationships between a user, and the user's identities, appliances and subscriber information. User B 140b is used as an example in FIG. 5. The various attributes illustrated in FIG. 5, such as e.g. the number of network appliances 510, the user identities 520 or the subscriber information 530 that is stored, may be varied.

[0040] In the user dataset 500 of FIG. 5, the User B 140b is associated with multiple network appliances 510 comprising network appliances 120c – 120e. User B 140b is also associated with multiple user identities 520 comprising for example a phone number 522 and/or a user name 524. User B 140b is also associated with subscriber information 530. The subscriber information 530 may

for example comprise status information 532 and/or access control rights 534. The access control rights 534 in turn may comprise a public ID 536, a private ID 540 and a password 538 that is associated with the public ID 536 and/or the private ID 540. The public ID 536, private ID 540 and password 538 may be used
5 in the method 300 of registering an appliance with the communication system 100 that will be described later.

[0041] An appliance may also be associated with multiple user identities. Taking network appliance 120e as an example, the network appliance 120e is associated with the user profiles of User B 140b and User C 140c. The network
10 appliance 120e may thus be reachable using any of the user identities associated with the user profiles of User B 140b or User C 140c.

[0042] The subscriber information 530 of User B 140b may be stored in a single database, or alternatively be stored across a number of different databases. In the latter case, the distribution of data across databases may be
15 done according to data type, for example the status information 532 may be stored in an Instant Messaging server which is separate from the access control rights 534. The access control rights 534 in turn may also be stored across multiple servers, e.g. the public ID 536 and password 538 may be stored in the AAA server 210 while the private ID 540 and password 538 may be stored in the
20 HSS 252. Optionally, the data may also be divided into sub-sets of users for distribution across databases, for example where a server is implemented using multiple servers which are distributed geographically. Where multiple databases are used to store the user profiles, there may be a replication of data across the

multiple databases. The replicated data may thus be synchronized between databases.

[0043] The concept of a user dataset 500 may permit the unified functioning of the components of the communication system 100. In such a scenario, there is a conceptual linkage between the subscribed user 140b and the associated network appliances 510, user identities 520, subscriber information 530, user and device status information 532, and/or user and device access control rights 534. All or some of the components of the communication system 100 may commonly use the relationships contained in the user dataset 500 for functions such as communications routing, status updates, access control, etc.

Device Registration

[0044] FIG. 3 is a flow chart showing a method 300 of registering a device with the communication system 100 of FIG. 1. The method 300 connects the network appliance 120c to the communication system 100 via the WiMAX or LTE access point 130a and negotiates for access to the services provided by the IMS 250. Authentication for the access point 130a and the IMS 250 may be performed automatically without user intervention by using stored login identities. This method 300 may also be implemented without the use of a SIM card.

[0045] In 310, the process of registering the network appliance 120c is initiated by the network appliance 120c. The initiation may occur automatically for example when the network appliance 120c is powered up, or alternatively may be done manually when the User B 140b chooses to register to the communication system 100.

[0046] In 320, the network appliance 120c authenticates itself with the AAA server 210. This is done using phase II of the Tunnelled Transport Layer Security (TTLS) standard as the Extensible Authentication Protocol (EAP). The EAP-TTLS authentication can be done using for example, the method described in
5 "Request for Comments 5281, Network Working Group, <http://tools.ietf.org/html/rfc5281>", the contents of which are incorporated herein by reference.

[0047] With EAP-TTLS authentication, a public ID and a password are encrypted and transmitted from the network appliance 120c to the AAA server
10 210 via the WiMAX or LTE access point 130a. The public ID is a login identity that is uniquely associated with User B 140b and the password is associated with the public ID. There thus may be greater security against wireless eavesdroppers as EAP-TTLS is used. Also, it is noted that the usage of EAP-TTLS may provide the advantage of device independence as no hardware or
15 device dependent identities are used.

[0048] In 330, the public ID and password are received by the AAA server 210 from the network appliance 120c. The AAA server 210 looks up its user information database to authenticate the public ID and password. If the authentication is a success, the AAA server 210 may then grant the network
20 appliance 120c access to the WiMAX or LTE RAN.

[0049] In 340, the network appliance 120c has been granted access to the WiMAX or LTE RAN and the DHCP server 258 then allocates an IP address to the network appliance 120c. Also, the AAA server 210 then starts the process of usage accounting.

[0050] In 350, IMS gateway discovery occurs where the network appliance 120c is provided with the IP address of the CSCF gateway 260. The CSCF gateway 260 serves as an initial point of contact for the network appliance 120c to access the IMS 250. The network appliance 120c negotiates for access to the
5 IMS 250 via the CSCF gateway 260.

[0051] In 360, the network appliance 120c negotiates for access to the services provided by the IMS 250. It transmits via the CSCF gateway 260 to the HSS 252 a private ID and the password associated with the private ID.

[0052] In 370, the HSS server 252 receives the private ID and password from
10 the network appliance 120c. The HSS server 252 looks up its user information database to authenticate the private ID and password. If the authentication is a success, the HSS server 252 may then grant the network appliance 120c access to the services provided by the servers in the IMS 250 and send to the network appliance 120c a message informing that access is granted. Should
15 authentication however be unsuccessful, the HSS 252 may inform the network appliance 120c that access is denied, in which case the network appliance 120c may choose to repeat step 360 where the network appliance 120c negotiates for access.

[0053] It is envisaged that each appliance of the communication system 100
20 be associated with a unique private ID. The private ID may be used for authenticating access to the IMS 250 and may thus uniquely identify an appliance on the IMS 250. The usage of a private ID separate from the public ID may have the advantage of decoupling the appliance's identity from the user identity. Multiple appliances may share a public ID across both the WiMAX or

LTE and IMS networks, with each appliance having a unique private ID. This may enable the concurrent and unique yet related registration of the different appliances using the same user identity.

[0054] The private ID may be generated automatically using an algorithm.

5 This may be done by the IMS 250 and be allocated to the network appliances 120a – 120g. An example of such an algorithm would be to form the private ID by appending a device suffix after the user's public ID. The device suffix in turn may be a number uniquely identifying the network appliance 120c from amongst the appliances owned by the user, or alternatively may be a text string containing
10 the model, make, type and/or name of the network appliance 120c. For example, in a specific embodiment, the device suffix is a four-letter string indicating the appliance category. The usage of such an algorithm may have the advantage of being automatic and repeatable. Further, as the private ID is derived from the public ID, the user convenience of a single login may be realized while
15 maintaining separate login IDs for WiMAX or LTE access and IMS access.

[0055] While the method 300 of registering the network appliance 120c is illustrated using separate login identities for WiMAX or LTE access and IMS access, i.e. respectively using the public ID and private ID, it is envisaged that a single login identity may be used for both WiMAX or LTE and IMS access. An
20 example of such a single login identity may be the public ID. In such a case, the AAA 210 and the HSS 252 may use a single user login in order to authenticate and authorize access and the network appliance 120c may transmit the same login identity in steps 320 and 360. The AAA 210 and HSS 252 may then perform access authentication using the same login identity in steps 330 and

370. The login data for the AAA 210 may be synchronized with the HSS 252 of the IMS. Using a similar user login for both WiMAX or LTE and IMS access may enable the concept of a single login, and may bring about the advantage of user convenience while still decoupling of the WiMAX or LTE mode of access from the IMS system.

[0056] Certain appliances may be configured to be associated with more than one user. As an example the network appliance 120e is shown in FIG. 1 to be associated with both User B 140b and User C 140c. In such a situation, the network appliance 120e may perform device registration twice i.e. once for User B 140b and another time for User C 140c. Two user profiles for Users B and C can then be concurrently active on the network appliance 120e. Optionally, the association of network appliance 120e with Users B 140b and C 140c may be made in the user information databases of the AAA server 210 and the HSS server 252. In such a case, the network appliance 120d may have only a single session active, the single session being associated with both Users 140b and C 140c. Device registration thus may be performed only once.

[0057] Certain users may also be associated with multiple appliances. As an example, User B 140b is shown in FIG. 1 to be associated with three network appliances 120c - 120e. In such a case, each of the network appliances 120c - 120e independently performs device registration with the AAA server 210 and HSS server 252. The network appliances 120c - 120e however may all be associated with User B 140b in the user information databases and thus may use a common public ID and password for authentication with the AAA server 210 and HSS server 252.

[0058] Although the network appliances 120c – 120e belonging to User B 140b may use the same login information, it however is notable that the network appliances 120c – 120e may be authenticated and registered with the system 100 concurrently. Thus for example, User B 140b may have a laptop, a mobile phone, as well as a mobile router and all three appliances may access the system 100 at the same time. Since the multiple appliances of a user may access the system 100 concurrently, it is envisaged that a first appliance of the user may establish a communication link with a second appliance of the same user. As an example, for User B 140b, the appliance 120c may be a mobile phone and may establish a VoIP call to the appliance 120d which may be a home phone.

[0059] The method 300 of registering the network appliance 120c may be further extended for use in registering the network appliance 120c for access via other modes of access, for example for access via the Wi-Fi access point 130c. Should a mode of access other than WiMAX or LTE be used, the step of IMS gateway discovery 350 may not occur. In such a case, a network appliance 120c may access the CSCF gateway 260 using a fixed IP address. The CSCF gateway 260 for access modes other than WiMAX or LTE may be configured to be different from that for access using WiMAX or LTE.

[0060] It is also envisaged that the method 300 may be further used for registering a single network appliance 120c for access via multiple concurrent access modes, for example by registering a single network appliance 120c for concurrent connections via both the WiMAX or LTE access point 130a and the Wi-Fi access point 130c.

Link Establishment

[0061] FIG. 4 is a flow chart showing a method 400 for establishing a communication link between appliances of the communication system 100 of FIG. 1. As an example, the method 400 shall be disclosed using a communication link established from an originating network appliance 120b of an originating User A 140a to the network appliances 120c – 120e of a destination User B 140b of the communication system 100. Before the link establishment is initiated, the network appliance 120b and network appliances 120c - 120e are registered with the AAA server 210 and HSS server 252.

[0062] The establishment of a link between two users allows for the direct communications between the users. Services such as VoIP, video conferencing, Short Messaging Service (SMS) or Instant Messaging can then take place between the users over the link. The IMS 250 is envisaged to be access agnostic and thus the mode of access (e.g. WiMAX or LTE, WiFi, etc) may have no bearing on call control or how the link is established.

[0063] In 410, the link establishment is initiated by the originating User A 140a on the network appliance 120b, the link directed to the destination User B 140b. This may take place for example when User A 140a dials on the originating network appliance 120b a phone number uniquely associated with User B 140b.

[0064] Alternatively in place of dialing a phone number, User A 140a may initiate the connection by entering or selecting from an electronic address book a user ID that is uniquely associated with User B 140b.

When the link establishment is initiated, the originating network appliance 120b sends a link establishment message to the SBC 254. This message contains a destination user identifier that identifies User B 140b as the link destination. The destination user identifier may for example be User B's phone number or User B's user ID. The link establishment message may be sent a signalling protocol that is known in the art, for example using the Session Initiation Protocol (SIP) that is defined in "*Request for Comments 3261, Network Working Group, <http://tools.ietf.org/html/rfc3261>*", the contents of which are incorporated herein by reference.

[0065] The destination User B 140b may have multiple destination user identifiers associated with it, for example where User B 140b has multiple phone numbers. In such a case, since the multiple destination user identifiers are all associated with the User B 140b and accordingly all also associated with the network appliances 120c – 120e, User A 140a can establish a link with the network appliances 120c – e of User B 140b using any of the destination user identifiers for User B 140b.

[0066] In line with the access agnostic nature of the IMS 250, the originating appliance may for example be a telephone on a PSTN network. In this case, a voice call may be established between the PSTN originating telephone and the network appliances 120c-120e belonging to the destination User B 140b by dialling a traditional telephone number at the originating telephone. The call from the originating telephone is routed through the PSTN network and arrives at the MGW server 266 of the IMS 250. This call is then routed to the IMS server 262 for resolution in the same way as is done in the subsequent steps 420 to 450.

[0067] In 420, the SBC 254 forwards the link establishment message to the IMS server 262. The IMS server 262 resolves the destination user identifier. The IMS server 262 contains a record of the statuses of the network appliances 120c – 120e associated with User B 140b. Using the status records, the IMS server
5 262 determines if any of the network appliances 120c – 120e are registered with the communication system 100. If one or many of the network appliances 120c – 120e are registered, the IMS server 262 then provides the SBC 254 with the IP addresses of those appliances of the destination User B 140b that are registered. If none of the network appliances 120c – 120e are registered, the
10 HSS 252 then notifies the SBC 254 of that fact.

[0068] In 430, the IMS server 262 optionally interacts with the feature server 256 for supplementary services. The feature server 256 may be implemented as a single server providing multiple supplementary services, or may also be implemented as a collection of servers each providing a supplementary service.
15 Examples of such supplementary services are call forwarding or voice mail routing.

[0069] The call forwarding service permits the link that is directed to User B 140b to be forwarded to another user, e.g. User C 140c. In this case, the feature server 256 informs the IMS server 262 that the link is to be forwarded from User
20 B 140b to User C 140c and the IMS server 262 instead resolves the destination user identifier to be User C 140c.

[0070] The voice mail routing service permits the link that is directed to User B 140b to terminate as a voice mail recording service. In this case, the IMS

server 262 terminates the link establishment and the User A 140a is offered the opportunity to leave a voice mail recording for User B 140b.

[0071] In 440, the SBC 254 sends a link establishment message to each of the network appliances 120c - 120e associated with the destination User B 140b.

5 The SBC 254 may not send a message to the appliances which are not registered. This can happen, for example when the appliance is turned off or in airplane mode. If none of the network appliances 120c - 120e are registered with the system 100, the SBC 254 may notify the originating network appliance 120b of that fact. The messages sent from the SBC 254 to each of the network
10 appliances 120c - 120e may be done using a signaling protocol such as SIP.

[0072] Upon receiving the message from the SBC 254, the network appliances 120c - 120e may then each indicate an incoming link establishment by ringing. In other words, should there be multiple registered appliances associated with User B 140b, all of these registered appliances may ring.

15 Optionally, the network appliances 120c - 120e may be configured to automatically accept incoming links. Should there be more than one of network appliances 120c - 120e registered with the communication system 100, a hierarchy may be used to determine which of the registered appliances should automatically accept the incoming link. Such a hierarchy may for example be
20 implemented at the IMS server 262 or alternatively be implemented at the SBC server 254. An example of a hierarchy would be the Q-value system. The Q-value system prioritizes the network appliances 120c - 120e of User B 140b by assigning each appliance with a Q-value. The Q-values denote an appliance's priority - the lower the Q-value, the higher is the appliance's priority. In such a

case, the link establishment message is directed first to the appliance with the lowest Q-value, failing which the message is then directed to the appliance with the next highest Q-value. Should there be two appliances with similar Q-values, the appliances may have an equal priority. Thus when the link is directed to a priority level where there are multiple appliances with that Q-value, all the appliances with that Q-value receives the link establishment message at the same time.

[0073] In 450, the destination User B 140b accepts the incoming link establishment on one of the network appliances 120c - 120e. As an example, User B 140b may accept the incoming link on network appliance 120c. When this happens, a bearer path is established between the originating network appliance 120b of User A 140a and the network appliance 120c of User B 140b. The originating network appliance 120b may then communicate directly with the destination appliance to the exclusion of other appliances associated with Users A or B. Thus if the incoming link establishment was accepted on network appliance 120c, the other appliances associated with User B e.g. network appliance 120d or 120e may not be able to listen in on the communication between the network appliances 120b and 120c. Further, should the incoming link establishment also comprise a message that is to be delivered e.g. an SMS or an IM message, that message may be received and displayed on all of the network appliances 120c – 120e.

[0074] In cases where an appliance is configured to be associated with more than one user, the appliance rings when any of the users are selected to be the link destination. As an example the network appliance 120e shown in FIG. 1 is

associated with both Users B 140b and C 140c. The network appliance 120e may thus be configured to notify or accept a connection when a communication link arriving at network appliance 120e is directed to either of User B 140b or User C 140c.

5 [0075] In the case where the originating appliance is a device on the PSTN network, the link is established between the originating appliance and the appliance upon which User B 140b accepts the incoming link. This link is established via the MGW server 266 which converts between PSTN telephone traffic and VoIP traffic.

10 [0076] In cases where the signalling protocol used is based upon internet protocol (IP) e.g. SIP, and the originating network appliance 120b and/or one of the destination network appliances 120c – 120e are resident on the Internet 270, SIP packets may be prevented from reaching the IMS 250. This is because a firewall running on the IP network 268 may filter out IP packets originating from
15 the Internet 270.

 [0077] In such a situation, Network Address Translation (NAT) traversal may be performed at the routers which are connecting the network appliances 120b – 120e to the Internet 270 (i.e. the users' routers). This allows SIP packets to arrive at the IMS 250 while the firewall is active. Similarly, NAT traversal may also be
20 performed in the reverse direction at the SBC 254. This allows SIP packets originating from the IMS 250 to bypass any firewalls which may be active at the users' routers.

 [0078] It is envisaged that while the present disclosure refers to the servers such as the SBC 254, the feature server 256 or the IMS server 262 as single

servers, the SBC 254, the feature server 256 or the IMS server 262 may optionally each be implemented as a plurality of servers. Having a plurality of servers for each function may allow the servers to be geographically distributed and may permit a larger area to be served.

5 Quality of Service (QoS)

[0079] The QoS of WiMAX or LTE access in the system 100 is maintained at the IMS 250 by prioritizing traffic and reserving bandwidth. Traffic packets are prioritized based on the time urgency of the application. The urgency is determined using a Differentiated Services Code Point (DSCP) field present in the header of each packet. As an example, traffic from applications such as VoIP or live video may utilize a DSCP field code which accords a higher priority than web page traffic. The network routers and/or switches between the originating and destination network appliances will route each packet on the basis of the DSCP field; VoIP or live video traffic packets are deemed to be more time sensitive and are thus routed ahead of the web page traffic packets. Since the web page traffic is deemed to be less time sensitive, it is thus routed on a "best-effort" basis.

[0080] Bandwidth reservation is used in conjunction with traffic prioritization in order to guarantee QoS for certain classes of traffic. It works by ensuring that for each time interval, a minimum number of packets belonging to a higher priority class are transmitted before packets of a lower priority class are transmitted. In other words, the higher priority class has a minimum bandwidth threshold. Such a bandwidth reservation scheme may be adaptive in that the threshold for a class of traffic may rise or fall depending on the overall bandwidth utilization.

Bandwidth reservation is implemented by the SCE 272. The SCE 272 is responsible for monitoring end-to-end traffic QoS measures, as well as propagating QoS policies and settings to the routers and/or switches. Where Wi-Fi is used as the mode of access, QoS may be achieved by establishing a VPN tunnel between the HA 274 and the network appliances 120c - 120e. In the case of a connection between a first of the network appliances 120c - 120e and a second, VPN tunnels are maintained between the HA 274 and each of the first and second network appliances. Similar to that described above for WiMAX or LTE, traffic packets travelling through the tunnel are prioritized based on the time urgency of the application and bandwidth reservation is performed.

Network appliances 120a – 120g

[0081] Example embodiments of the network appliances 120a – 120g are described next. By allowing a wide variety of appliances to work with the system 100, users may choose an appliance of the most convenient form factor for the task at hand. For example, a user who wants to send an SMS may choose to do so using a WiMAX or LTE enabled laptop, thus taking advantage of the laptop's full size keyboard.

WiMAX- or LTE- enabled mobile phone

[0082] The network appliances 120a – 120g may include a WiMAX- or LTE-enabled mobile phone. Such a mobile phone may have built-in WiMAX or LTE access, or WiMAX or LTE access may be available by pairing the mobile phone with WiMAX or LTE access devices such as those that will be described later.

[0083] Such a mobile phone registers with the communication system 100 using the method 300 without having Subscriber Identity Module (SIM) cards in

the mobile phone. Subscriber information comprising the public ID and password used for authentication in 320 is stored within the mobile phone, for example in an onboard memory. In order to register the mobile phone with the system 100, a user enters the public ID and password associated with his account into the mobile phone. Account portability may then be achieved by allowing the public ID and passwords to be stored and used across different mobile phones and network appliances 120a – 120g.

[0084] Since the mobile phone is no longer reliant on a physical SIM card for subscriber information, account portability may be achieved more conveniently; a single user account may be used across multiple mobile phones without the need for additional SIM cards.

[0085] Additionally, a WiMAX- or LTE- enabled mobile phone may also take the form of an embedded device. In this case, services e.g. VoIP, IM or SMS may be accessible on the mobile phone in an “as is” manner without the need for a user to actively run and maintain a client program. As an example, incoming and outgoing VoIP functionality may be constantly available on the mobile phone without the user having to actively keep a VoIP client program running in the foreground. In this case, the user may thus experience seamless access to services with the complexities of the underlying technology being hidden from the user.

[0086] Further, the WiMAX- or or LTE- enabled mobile phone may be a “refreshable” appliance. A “Refreshable” appliance is a device which decouples the user identity from the device, thus allowing any user to take over a “refreshable” appliance simply by logging in to the “refreshable” appliance. Once

a user is logged into the “refreshable” appliance, the user may then use the appliance as if it is his personal device.

[0087] The “refreshable” mobile phone may be proprietary in nature and may be configured to protect sensitive user specific data. This may be done by making the “refreshable” mobile phone fully refreshable, i.e. all sensitive user specific data is synchronized back to the network and deleted from the mobile phone once a user logs out of the phone. This may also be done by hiding sensitive user specific data within the mobile phone using for example, encryption technology or operating system access rights. Further, sensitive user data may also be hidden on “refreshable” mobile phones by using the concept of “guest” and “owner” accounts. “Guest” accounts may have a lower access privilege than “owner” accounts and consequently may not be able to view or access data belonging to the “owner” account. In such a configuration, the “refreshable” mobile phone may still require user logins, but the phone would recognize a specific user to be the “owner” account whilst other users would be “guest” accounts.

Personal Computer

[0088] The network appliances 120a – 120g may also include a personal computer. Such a computer may have built-in WiMAX or LTE functionality. Alternatively, WiMAX or LTE access may be achieved by pairing the computer with WiMAX or LTE access devices such as those that will be described later. In addition to WiMAX or LTE, the computer may also have access to Wi-Fi or wired internet.

[0089] The computer gains access to the services e.g. VoIP, SMS or IM offered by the IMS 250 by running a client program. Such a client program may be web-based and may be hosted on an application server 264. The IMS 250 is connected to the Internet 270 by way of the IP network 268 and in the case where the computer is used outside of the system 100, the computer is still capable of accessing the IMS 250 by way of the Internet 270. In this case, IMS access negotiation (i.e. the step 360 of the method 300) takes place between the computer and the CSCF gateway 260.

[0090] It is thus envisaged that the IMS 250 and its services may be accessible from anywhere in the Internet at large and thus by using a PC, VoIP roaming outside of the system 100 may be possible across the entire Internet. This may result in cost savings for the user as the user no longer needs to subscribe to a mobile operator's roaming service in order to remain contactable overseas.

WiMAX or LTE access devices

[0091] In the case where a network appliance 120a – 120g does not have in-built WiMAX or LTE access capability, the network appliance 120a – 120g may gain WiMAX or LTE access using a WiMAX or LTE access device taking the form of e.g. a WiMAX or LTE CPE 160 or a WiMAX router 162. This is shown in FIG. 1 where the network appliance 120f is paired with a CPE 160 in order to gain WiMAX or LTE access, and the network appliances 120c-120e share a WiMAX or LTE connection via a WiMAX or LTE router 162.

[0092] Where a CPE 160 is used as the access device, the host appliance i.e. the network appliance 120f is paired with the access device using a wired or

wireless pairing standard that is known in the art, e.g. Universal Serial Bus (USB), wired Ethernet connection, Wi-Fi or Bluetooth. By using a widely available pairing standard, the access device may be used with a wide variety of host appliances. For example, using Wi-Fi, a user pairs the WiMAX or LTE access device with his laptop in order to gain Internet access on the laptop and the same WiMAX or LTE access device may then also be paired with a tablet device in order to gain VoIP functionality on the tablet device.

[0093] The WiMAX or LTE CPE 160 is capable of storing a subscriber's authentication and login information in its onboard memory and thus the network appliances 120f does not need to run a client program in order to gain access to the WiMAX or LTE RAN. The CPE 160 may be configured to perform automatic authentication such that it automatically detects the presence of WiMAX or LTE service and logs into the RAN once the CPE 160 is turned on. The user may thus experience seamless WiMAX or LTE connectivity with the complexities of negotiating for access hidden from the user.

[0094] The WiMAX or LTE CPE 160 may also function as a VoIP Analogue Terminal Adapter (ATA). In this case, the WiMAX or LTE CPE 160 is capable of converting between VoIP traffic and analogue telephone signals. The WiMAX or LTE CPE 160 enables telephone connectivity across the WiMAX or LTE RAN by sending and receiving VoIP telephone traffic between the WiMAX or LTE CPE 160 and the IMS 250. VoIP traffic is then converted to or from analogue PSTN telephone signals in the CPE 160. The CPE 160 possesses a telephone jack (e.g. a jack of the RJ11 standard) by way of which the PSTN phone is plugged. The PSTN phone may then be used to receive or initiate telephone calls.

[0095] A WiMAX or LTE router 162 may also be used to share a single WiMAX or LTE connection amongst multiple network appliances 120c-120e. In this case, the WiMAX or LTE router 162 independently registers and authenticates itself with the WiMAX or LTE RAN. Like in the case of the WiMAX or LTE CPE 160, the subscriber's authentication and login information may be stored in an onboard memory. Each of the network appliances 120c-120e separately establishes a connection with the router 162 and the WiMAX or LTE connection is then shared via the router 162 with each of the network appliances 120c-120e. The connection between the router 162 and each of the network appliances 120c-120e may be wired (e.g. using USB or IEEE 802.3 wired Ethernet) or wireless (e.g. using Wi-Fi or Bluetooth). Further, it is envisaged that the WiMAX or LTE router 162 may also contain all/any of the functionality of the WiMAX or LTE CPE 160 that is described earlier.

Network based services

[0096] The communication system 100 of FIG. 1 may also be configured to provide network based services by providing servers offering services in the IMS 250 of the core network 150.

[0097] As an example, the core network 150 shown in FIG. 2 may be configured to provide a network-based address book (NAB) service that runs on an application server (AS) 264. The NAB service allows the synchronization of address book data for a user across multiple appliances. When a change is made to the address book of an appliance belonging to a user, this change is propagated across all the other appliances belonging to that user. Thus taking FIG. 1 as an example, when a change is made to the address book on network

appliance 120b of User B 140b, this change is propagated to the network appliances 120a – 120c. Such a change to the address book may for example be an amendment to an address book entry, the deletion of an entry, or the addition of a new entry.

5 [0098] The NAB service may use SyncML to synchronize data between appliances and the AS 264. SyncML is a standard defined by the Open Mobile Alliance (OMA) and is an open standard. The usage of SyncML thus may confer the advantage of interoperability between service providers, network access providers and/or equipment vendors, and thus may contribute towards the
10 advantage of being access and device agnostic.

[0099] Another service that may be offered is that of having a profile page for each user of the IMS 250. The profile pages may permit social networking between users. These profile pages may be served from an AS 264, for example as a HTML webpage the presentation and layout of which are controlled using a
15 schema. The AS 264 serving the profile pages may either be the same or a different server from that for the NAB service.

[00100] A profile page may contain selected information about a user. This information may be divided into shareable public fields and private fields. An example of a shareable public field may be a user's online status while a private
20 field may be a user's subscription account number. The concept of "friends" and "non-friends" may be used to control who can view the public fields of a user - the "friends" of a user may view the public fields of the user while "non-friends" may not do so. A user may then have the ability to make another user a "friend" via the user interface of the profile pages.

[00101] The profile page may further also publish status information indicating a user's status, for example whether the user is registered with the communication system 100 or whether the user is signed in to one of the services offered by the IMS 250. The AS 264 may obtain the user status information directly from the application server which provides Instant Messaging services, or alternatively may also obtain such information from the HSS 252 and/or the AAA server 210.

[00102] It is envisaged that the profile page of a user may also function as a social network page. The profile page may for example contain an electronic notice board or "wall" which allows a user to publish information about himself. Such information may be multimedia, e.g. photographs or videos and may comprise information about the user's status and location. The "wall" may also allow other users to post comments about the user's published information. Access to this "wall" may be controlled by the "friend" status of the other users.

[00103] The provision of a profile page for each user may also allow for ease in populating one's address book. In such a scenario, a person may populate his address book by visiting the user profiles of other users, and add the contact information of these other users to his address book by for example, clicking a button. These address book entries may then exist as references to the profile pages – should any user's contact information change, the revised contact information may be automatically updated in the address book entry. To further add to the ease of populating an address book, it is envisaged that the contact list information of a third-party service may be integrated into the address book. In this case, contact information is imported into the address book from a third-

party service e.g. Yahoo. This may be done, for example, using a client program running on a PC.

[00104] In addition to the profile page, each user of the communication system 100 may have a configuration page associated with his account. This configuration page may take the form of a web page, or may be a user interface provided by a client program running on the appliance. The configuration page allows the user to set his user settings, e.g, information privacy settings, or call handling and routing settings. The information privacy settings for example control the amount of private information the user places on his profile page, as well as control whether his contact details are to be listed in a directory service.

[00105] The call handling or routing settings may comprise instructions on how an incoming call is to be handled. Such routing instructions may take the form of the Q-values hierarchy which was described earlier; the user may set how he wishes his calls to be routed by amending the Q-values associated with his appliances. Further, call handling instructions may be set where for example, incoming calls from a specific originating phone number are rejected, or where incoming calls are automatically answered after a predetermined number of rings. The call handling or routing settings when set or changed on the configuration page are then propagated to the respective feature server 256 or application server 264 of the IMS 250 which is responsible for providing the associated service.

[00106] While several embodiments have been provided in the present disclosure, it should be understood that the disclosed systems and methods may be embodied in many other specific forms without departing from the spirit or

scope of the present disclosure. The present examples are to be considered as illustrative and not restrictive, and the intention is not to be limited to the details given herein. For example, the various elements or components may be combined or integrated in another system or certain features may be omitted or not implemented.

[00107] Also, techniques, systems, subsystems, and methods described and illustrated in the various embodiments as discrete or separate may be combined or integrated with other systems, modules, techniques, or methods without departing from the scope of the present disclosure. Other items shown or discussed as directly coupled or communicating with each other may be indirectly coupled or communicating through some interface, device, or intermediate component, whether electrically, mechanically, or otherwise. Other examples of changes, substitutions, and alterations are ascertainable by one skilled in the art and could be made without departing from the spirit and scope disclosed herein.

[00108] For example, as will be understood by the skilled person, a “server” as referred to in this specification may be a single server computer, or may comprise multiple server computers. In the latter case, the multiple server computers may function as a server cluster, or may also function as a distributed server. It is further understood that multiple “servers” each providing different services may be arranged to be running on a single server computer.

[00109] WiMAX and LTE are examples of 4G, and the invention is also intended to cover other variants of 4G, for example HSPA+. 4G networks are recognised under the ITU-R organization and specified in the IMT-Advanced

standard. For example typically 4G networks may be characterised by techniques such as OFDMA, MIMO, dynamic channel allocation and/or channel-dependent scheduling.

CLAIMS

1. A wireless communications system comprising:

5 a network configured to wirelessly connect a plurality of devices via plurality of modes of network access; and

wherein the plurality of modes of network access includes a WiMAX or LTE access mode, and wherein the WiMAX or LTE access mode is configured for device independent authentication,

wherein the network is primarily a mobile cellular network,

10 wherein the WiMAX or LTE network is the home network, and

wherein voice calls over the WiMAX or LTE network are packet switched and/or VOIP, with a prioritised QOS.

2. The system of claim 1 wherein both data and voice services are
15 transported on the same all-IP network, each with its own assigned QOS.

3. The system of claim 1 or 2 wherein the prioritised QOS comprises an adaptive bandwidth reservation scheme in conjunction with traffic prioritization.

20 4. The system of claim 3 wherein a single subscriber can have multiple devices registered to a single user ID and mobile number, thereby enabling concurrent access and concurrent telephony services delivery.

5. The system of any preceding claim wherein the device independent authentication comprises TTLS subscriber authentication without a hardware or device dependent identification.

5 6. The system of claim 5 further comprising
a database comprising user datasets, each user dataset configured to
associate a user identity with a device independent public identity; and
wherein the TTLS authentication is performed using the public identity
of one of the user datasets.

10

7. The system of claim 6 further comprising
an IP multimedia subsystem configured to connect each device via the
backhaul network to a core network; and

15

wherein each user dataset is further configured to associate the user
identity with a private identity, the private identity used for authenticating the
connection of each device to the core network.

20

8. The system of claim 7 wherein each user dataset is further configured
to associate the user identity with one or more devices.

9. The system of claim 8 wherein the private identity is uniquely
associated with one of the one or more devices of the user identity.

10. The system of claim 6 wherein the private identity is automatically generated by an algorithm.

11. The system of claim 6 wherein the algorithm combines the public
5 identity of the user dataset with an identifier selected from the group consisting of:

the type of one of the one or more devices of the user dataset;

a model of one of the one or more devices of the user dataset; and

a number uniquely identifying one of the one or more devices from
10 amongst the other of the one or more devices.

12. The system of claim 6 wherein a request for a communication link to a user identity is sent to all of the devices associated with that user identity.

13. The system of claim 6 wherein all of the devices associated with each
15 user identity are assigned a priority value.

14. The system of claim 13 wherein a request for a communication link to a user identity is sent to one of the devices associated with that user identity
20 according to the priority value of the device.

15. The system of claim 7 wherein each user identity is associated with a profile page.

16. The system of claim 15 wherein each profile page comprises a plurality of public fields viewable depending on a friend status with the associated user identity.

5 17. The system of claim 16, wherein the IP multimedia subsystem comprises a server configured to serve the profile pages.

18. The system of claim 17 wherein each profile page is served using a schema.

10

19. A wireless communication device comprising
a communications circuit configured to wirelessly connect via plurality of a modes of network access,

15

a secure login interface configured to authenticate a user with a user identity of a communications system, wherein the device is configured to allow concurrent association of a plurality of user identities,

wherein request for a communications link to any of the user identities currently logged into the device are received by the device.

20

20. The device of claim 19 further comprising an interface for a network-based address book, stored on a remote server and accessible via the device.

21. The device of claim 19 further comprising an interface for a locally stored address book, wherein a copy of the locally stored address book is stored

on a remote server and refreshed/synchronised with the locally stored address book.

22. The device of claim 21 wherein the remotely stored address book is
5 stored using XCAP, and wherein SyncML is used to refresh/synchronise the
remotely stored address book.