



(51) International Patent Classification:

H04L 12/06 (2006.01) *H04W 8/24* (2009.01)
H04L 29/06 (2006.01) *H04W 8/30* (2009.01)
H04W 4/12 (2009.01) *H04M 3/533* (2006.01)
H04W 8/20 (2009.01)

(21) International Application Number:

PCT/GB2010/001532

(22) International Filing Date:

12 August 2010 (12.08.2010)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

09252314.1 30 September 2009 (30.09.2009) EP
09252507.0 29 October 2009 (29.10.2009) EP

(71) Applicant (for all designated States except US):
BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81, Newgate Street, London EC1A 7AJ (GB).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SMITH, Fraser** [GB/GB]; BT Group Legal, Intellectual Property Department, PP:C5A, BT Centre, 81 Newgate Street, London EC1A 7AJ (GB). **PUNWANI, Mohit** [GB/GB]; BT Group Legal, Intellectual Property Department, PP:C5A, BT Centre, 81 Newgate Street, London EC1A 7AJ (GB).

(74) Agent: **LIDBETTER, Timothy Guy Edwin**; BT Group Legal, Intellectual Property Department, PP:C5A, BT Centre, 81 Newgate Street, London EC1A 7AJ (GB).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

- with international search report (Art. 21(3))
- with amended claims (Art. 19(1))

(54) Title: METHOD FOR RE-CONFIGURING A COMMUNICATIONS DEVICE

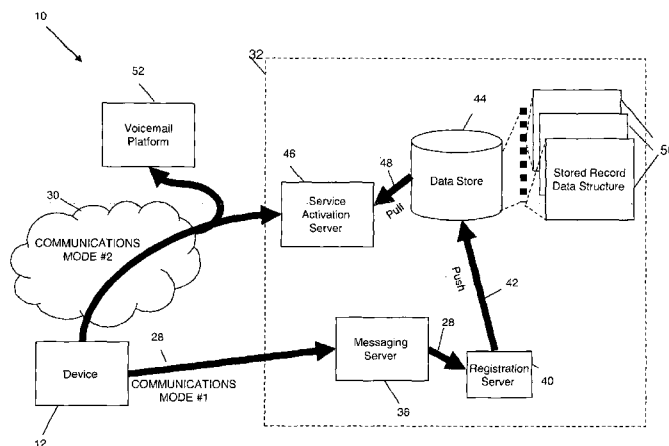


FIGURE 2

(57) Abstract: A communications device (12) maintains profile data including a device identity and a calling line identity (CLI) associated with a PSTN connection (28) both on the device itself and also on an authentication platform (32), in order that the device can access a service (52) which requires knowledge of the CLI by way of a packet-switched connection (30). In the event that the CLI data in the communications device is corrupted or lost, the communications device transmits a request for re-authentication to a reactivation server (46) together with the device identity. On receipt of the request, the reactivation server retrieves the stored profile (50) from the authentication platform (32), and returns it to the communications device (12) to allow the profile to be restored. This process can be done without the user needing to send a new request for service over the PSTN link (28).

WO 2011/039495 A1

METHOD FOR RE-CONFIGURING A COMMUNICATIONS DEVICE

The present invention relates to a method of operating a communications device, in particular to a method for the reactivation of a communications device which uses a connection-less packet-oriented communications protocol session for a service which requires the provision of credentials such as a password and/or identification of a physical communications line to which the communications device is attached.

The Internet Protocol is a connection-less packet-based communications protocol over which a number of telephony services can be provided, for example, VoIP (Voice over Internet Protocol), and also voicemail services. Access to voicemail service information using a conventional telephone communications device is well known in the art.

It is known for voicemail messages to be stored either in memory on the communications device itself, or in a remote storage facility, for subsequent retrieval. Functionality also exists for retrieving voicemail data from such a remote storage facility, using either the same communications device or another such communications device, or for retrieving voicemail data remotely from one communications device using a second communications device.

However, a user of a PSTN (public switched telephone network) connection cannot detect that a voicemail message is being left during a call with another user, even if a service such as "caller waiting" is provided. The "caller waiting" service merely alerts the user that there is another caller attempting to make a connection. Moreover, a user cannot retrieve a voicemail message stored in association with the calling line identity of a PSTN phone line whilst the PSTN phone line is being used conventionally, as the line is already occupied.

In some voicemail services, in order to access voicemail message information, a user needs to provide authentication information such as a user identity and password. This is time-consuming and problematic for the user. A communications device cannot automatically retrieve information if a user must provide such credentials every time that new information is to be retrieved.

It is possible for a communications device to access service information associated with a service identifier, in which authentication information is generated remotely from the communications device to uniquely configure access by the communications device to service information associated with said service identifier. The authentication information and the service identifier are presented to a service platform

when the required service is to be initiated. This allows an identifier specific to the communications device to be used for retrieval. In particular, it allows data associated with a fixed line, such as a voicemail, to be retrieved over a connectionless packet switched system by the communications device, because its own identity has previously been
5 associated with the line identity.

Figures 1 and 2 illustrate a communications system embodying such a system. Figure 1 shows a communications system 10 in which a communications device 12 is arranged to access and retrieve service information from a remote service platform 32 by providing appropriate credential information to authenticate a data retrieval request. An
10 example of a service platform 32 comprises a server offering a voicemail service. The service information to be retrieved is uniquely associated with a service identifier, for example, a calling line identifier. A calling line identifier is generated by any call originating from a specific termination of a public switched telephone network 28.

However, the service platform 32 as shown in Figure 1 is also configured to
15 enable service information to be retrieved using a service request sent using a second mode of communication 30 from which the service platform cannot directly retrieve the service identifier. For example, if a request for voicemail is sent to a server using a broadband IP session, the calling line identifier of the communications line 28 would not be apparent from the communications mode used to send the request.

20 The communications system 10 depicted in Figure 1 comprises a plurality of communications devices 12 located on premises associated with respective communications service subscribers, although only one such communications device 12 is shown in Figure 1. The communications device 12 shown in Figure 1 comprises suitable data processing components 54, a data store 56, a display 14 and a user
25 interface 16 which enables a user to control operation of the communications device and/or provide data input.

The communications device 12 is provided with two modes of communications capability. Telephone-type functionality, for example, may be provided on the communications device 12 through appropriate transmission and receiving components
30 for connecting to the public switched telephone network (PSTN), means to go on/off-hook, microphone and speaker components. The communications device 12 may also, or instead, be provided with a communications-enabled interface 18 for communicating with at least one peripheral communications device 20, for example, a telephone communications device, using a suitable communications link 22, for example via a

wireless local area connection (WLAN) such as Digital Enhanced Cordless Telecommunications (DECT) such as is shown in Figure 1.

The communications device 12 is arranged to communicate over a conventional public switched telephone network (PSTN) line 28 between the subscriber premises and the local exchange of the PSTN (not shown in Figure 1) using at least two different modes of communications via a suitable interface 27 which provides connectivity with a separate base-station 24 via a suitable wireless or wired communication link 26. As will be apparent to those of ordinary skill in the art, some or all of the communications functionality of base-station 24 may be integrated into the communications device 12.

10 The PSTN mode provides the identity of the communications line between the local exchange of the public switched telephone network (PSTN) and the subscriber premises on which the communications device 12 is located, and to which the communications device 12 is connected to via base station 24. This mode may also be used by other communications devices on the subscriber premises and the calling line identity or CLI will be directly derivable for the communications traffic sent using this mode of communication by any of the communications devices using the line in this mode of communication.

A second mode of communication 30 uses the same physical communications line as the first mode 28, but supports traffic sent using a connection-less data-packet mode of communication 30. This second mode of communication 30 provides a data communications service, for example an "always on" type of service such as that known as a "broadband" service. Broadband services offer a relatively high-bandwidth connection at least in the direction from the local exchange to the subscriber premises. Such services may use data communications protocols such as the Asymmetrical Digital Subscriber Line (ADSL) for example. The second mode of communications may be accessible directly by the communications device 12 and/or base station 14, or may instead be by way of a suitable data network access point 34, for example, a router or hub. Such an access point 34 may support wireless connectivity with the base station 24 and/or communications device 12 and/or with the server 32, using an appropriate high-bandwidth wireless communications protocol, for example, WiMax and/or WiFi.

30 In the communications system shown in Figure 1, the communications device 12 uses the second mode of communication 30 to establish a data session between the communications device 12 and a service supporting platform or server 32. The same server 32 also provides a connection over the PSTN using the first mode of communication 28. However, the PSTN calling line identity information is not

35

automatically determinable from the communications protocols which are used on the second means of communication 30. The second mode of communication 30 therefore does not associate the traffic with the physical line's CLI between the customer premises and the local exchange of the PSTN. This means that the CLI is not directly derivable for
5 communications traffic sent using the second mode of communication 30.

In the embodiment shown in Figure 1, the first mode of communication 28 and the second mode of communication 30 both utilise the same physical communications line linking the subscriber premises to the local exchange of the public switched telephone network (PSTN). However, it may instead utilise a wireless connection for at least part of
10 the path taken between the communications device and the server 32. In either case, the identity of the telephone line associated with the subscriber premises is only capable of being detected from activity on the line associated with the first mode of communication 28. The second mode of communication uses a data session, for example an IP session as is shown schematically in Figure 1. The data session is established and supported
15 using data traffic which is packetised using a protocol such as the Internet Protocol which disassociates the data from a fixed path to its destination. As a result the data traffic sent using the second mode of communication 30 does not automatically contain any information providing a CLI for the physical line to the subscriber premises. Consequently, the CLI cannot be automatically determined from a data session using the
20 second mode of communication 30, for example an Internet Protocol session, even when running over the same physical line as the first mode of communication 28.

As previously mentioned above, in Figure 1, the communications device 12 communicates using both the first and second modes of communication via one or more suitable interfaces 27 with base station 24. However, in alternative embodiments of the
25 invention, the communications device 12 incorporates some or all of the communications functionality of the base-station 24 directly. Where all communications functions are incorporated into the communications device 12, a separate base-station 24 is not required. Similarly, as would be well known to one of ordinary skill in the art, either or
30 both of the base-station 24 and/or communications device 12 may also incorporate the communications functionality of a data network access point 34.

The service platform 32 provides service information, for example stored voicemails, to a communications device 12 requesting the service information if it is able to present credentials including an appropriate service identifier. Thus, if the service platform 32 is set up to recognise a calling line identifier as a service identifier, it can
35 retrieve service information comprising voicemail information left for the PSTN number

associated with that calling line identifier and thus provide the requested voicemail service. The service information (for example, voice messages and/or equivalently any other subscription specific service data, such as video messages, facsimile messages, electronic mail messages, text-messaging messages, etc) is stored in association with the service identifier so that the service information stored for one subscriber can be distinguished from service information stored for other subscribers to the service.

The service platform 32 can only deliver the required data if the required service identifier can be associated with the request for service information generated by the communications device 12 generating the request. As shown in Figure 1, the communications device 12 is configured to use the second data communications mode 30 to establish a connection-less packet-based session with the remote service providing platform 32, and this mode of communications does not enable the service platform to determine the service identifier from the service request which is needed to access the service data provided by service platform 32. The service identifier is needed as this provides authentication information which is required to associated the voicemail service with a particular subscriber to the PSTN telephone service for whom the original voicemail is intended (the PSTN number to which the initial call was made), identified through the CLI of the communications link between the local exchange to the customer premises associated with that particular subscriber.

In order to retrieve the correct voicemail or other user-specific data using the service platform 32, the communications device 12 must be configured appropriately so that it can generate requests which include credentials which enable the service identifier to be presented to the service platform 32 when the communications device 12 seeks to retrieve service information. The communications device 12 may be configured to include the service identifier with any requests it generates for service information, or it may be configured to provide its communications device identifier in any such requests, so as to enable an intermediate server to retrieve a service identifier and/or any other authentication information required and to forward these to the service platform.

Each communications device 12 is configured and activated using configuration information unique to that device so that service information can be retrieved without requiring manual input (e.g. by a user) of authentication data such as a username and/or password to identify the specific service subscription. In this way, the configured communications device 12 is able to automatically retrieve the service information from a remote service platform 32 using the communications system.

Figure 2 of the accompanying drawings shows a communications device configuration process in which, as part of the configuration process, a configuration computer program is run on the communications device 12. The same numbering system as was used in Figure 1 is retained for like elements of the system depicted in Figure 2.

5 In Figure 2 the communications device runs a configuration computer program which automatically triggers the generation of a first communications message which uniquely identifies the communications device by incorporating a unique communications device identifier, for example, its serial number, which is addressed to a registration server 40.

10 As part of this configuration process, the line identity and communications device identity are stored by an authorisation server in the network to allow new services to be activated as required. There is therefore a requirement for an initial association to be established between the PSTN line and the communications device's identity, by a registration process by which the CLI of the telephone line, generated in a call made to
15 the server, is used to make this association.

The first communications message is sent out over the communications line via the local exchange using the first mode of communications 28 to the addressed registration server 40 by way of a message server 36. For example, in one embodiment of the invention, the first communications message comprises a short message service
20 (SMS) text message and the message server 36 comprises a PSTN SMS server.

The message server 36 processes the received first message and processes it to extract the forwarding address for the registration service and the CLI of the line used by the first communications mode 38. The message server 36 determines from the registration server address that even if that CLI has not registered for the message
25 service, the message to the registration server should be forwarded. This is advantageous as it means that a user of the service for which the communications device 12 is to be configured need not have previously registered with the message server 36 for the messaging service over the PSTN.

As shown in Figure 2, the first communications message is then forwarded to a
30 registration server 40 which processes the message to determine the presence of the communications device identifier and associates this identifier with the service identifier, here the CLI of the communications line used by the first mode of communications via which the first communications message was sent.

The registration server 40 then pushes the service identifier (the CLI) and the
35 communications device identifier information to a data store 44 to locate and/or update

credential data stored on data store 44 to associate the service identified by the CLI with the communications device identifier and the CLI. For example, a data record 50 may be stored which has a data structure which associates the CLI with the communications device identity of communications device 12. In some embodiments of the invention, the data record 50 has a data structure which associates the CLI with one or more entries for communications device and/or service characteristics, for example, if one or more services are to be provided for a CLI and if so, whether the service has been activated on a particular communications device identified in the data structure. This enables service identifiers to be associated with the communications device identifier for a plurality of different service subscriptions and also enables unique configuration information, for example, additional authentication information such as a network generated password or authentication code can be associated with a particular service identifier and/or communications device identifier.

The data is stored in such a way that a look-up operation can be performed using the communications device identifier to retrieve the associated credential information, for example, the associated CLI and/or any authentication information such as a passwords etc.

As shown in Figure 2, the registration server 40 pushes the service identifier (the CLI) and any other information extracted from the SMS such as the communications device identifier via a communications link 42 to a remote data store 44 however it is not essential for data store 44 and registration server 40 to be remotely located. As would be obvious to one of ordinary skill in the art the data store 44 and registration server 40 may be supported by the same physical platform. The data store 44 is any suitable indexed data storage facility, for example, a database, which is configured to associate a service identifier such as a CLI for a subscriber with a particular communications device identifier etc. It may also provide a means to store other information in association with a CLI, such as authentication information, as well as information for billing and/or service provision related purposes.

After the data store 44 has been updated, the record for a service identifier such as a CLI is associated with a communications device identity for the communications device 12. The updating of the record may also generate additional authentication information for the service identified by the service identifier in some embodiments of the invention.

The data records 50 of the data store 44 thus have a data structure enabling a data record 50 to be located when the activation server 46 performs a look-up operation

or similar index retrieval operation based on at least a communications device identifier and/or additional information. If the communications device identifier is determined to be associated with a service-identifier, the activation server 46 amends the data record 50 to indicate that the service is now active for the communications device and CLI.

5 The data record 50 for a particular communications device identifier may also store additional information in association with the communications device and/or service identifiers, for example, authentication information may be stored and/or other information with which the communications device 12 may be uniquely configured. This configuration data is retrieved by the authentication server 46, or it may be generated in another
10 embodiment of the invention by the server 46 once it has received confirmation that the service is now active.

The configuration process continues with the communications device 12 being sent a registration acknowledgement, in response to a prompt transmitted over one or other of the available means of communication 28, 30. This acknowledgement includes
15 service profile data including the service identifier (CLI), and other data necessary to access the service. The communications device 12 stores the profile data in a memory 56.

Once unique configuration data has been sent to communications device 12 using the data session supported by the second mode of communication 30, it is used by the continuing configuration process to uniquely configure communications device 12.

20 Thus the communications device 12, after the configuration data has been downloaded from the service activation server 46, is able to complete the configuration process. The configuration information downloaded enables the communications device to generate requests for one or more service that the communications device was found to be associated with in the data store 12.

25 In order to access a service platform 52 over the second communications network 30, the communications device retrieves the service profile from its memory 56 and generates a communication message includes data which at least identifies the communications device 12 by means of the communications device identifier.

A problem may arise if the authentication data stored in a communications device
30 becomes corrupted, such that it can no longer automatically provide its profile information (specifically the CLI) when required to access a service using the connectionless packet system.

The present invention provides a process by which a communications device can re-generate its profile automatically, without following the initial registration system. This

process is particularly suited to the service described in the previous application, but may be used in other contexts as well.

According to the invention, there is provided a method for re-configuring a communications device in which profile data is maintained for access to a
5 communications service platform, wherein

profile data relating to the communications device is stored on an authentication platform, and the profile data is also stored in the communications device

and in which:

if the communications device detects that the profile data is no longer stored in the
10 communications device, the communications device generates a request for re-authentication, and transmits the request to a reactivation server together with the communications device identity,

on receipt of the request, the reactivation server retrieves the stored profile data associated with the communications device identity from the authentication platform and
15 returns it to the communications device

the communications device stores the retrieved profile data.

In practice, the reactivation process is an additional function of the activation server which initially generated the profile data.

A second aspect of the invention provides a communications device in which
20 profile data is maintained for access to a communications service platform, having provision for storing profile data relating to the communications device

and configured such that, in the event of such profile data being determined to be absent from the communications device, it generates a request for re-authentication, and transmits the request to a reactivation server together with the communications device
25 identity,

and on receipt of the requested re-authentication profile data, to store the retrieved profile data.

Complementary to the second aspect, a third aspect of the invention provides a communications service platform, comprising an authentication platform for storing profile
30 data relating to one or more associated communications devices, together with identity data for the associated communications devices,

and configured to receive a request from a communications device for re-authentication together with an identity for the communications device,

and comprising a reactivation server for retrieving the stored profile data associated with the communications device identity in response to such a request and returning it to the communications device.

In the preferred arrangement, the profile data is initially generated by a first mode
5 of communications in which a calling line identity apparent to the authentication platform is associated with a device identity, and the calling line identity is stored by the authentication platform and the device as part of the profile data for use in subsequent interactions between the communications device and the authentication platform over a second mode of communications in which the calling line identity is not apparent to the
10 authentication platform except as part of the profile data delivered to the authentication platform. If the profile data is lost by the user device, it can then be retrieved using the second mode although the second mode does not have visibility of the CLI when interacting with the device.

An embodiment of the invention will now be described by way of example, with
15 reference to the accompanying drawings, in which:

Figure 1 shows schematically a communications system for providing a service to a communications device, as already described;

Figure 2 shows schematically a service activation system for the initial activation
20 of a communications device to allow access to a service, by generating providing user profile data for use by the communications device, as already described;

Figure 3 shows schematically a process for re-activating the communications device in the event of loss of the profile data provided to the communications device in the initial activation process, according to the present invention.

Figures 1 and 2 relate to various methods of configuring a communications
25 device for use in a method of accessing service information as already discussed.

It is possible for the data in the memory 56 of the communications device to become corrupted or deleted by accident, or if settings have to be restored to a state previous to that at which the settings were stored. It would be possible to reinstate the profile data by repeating the initial configuration process, but this may be difficult to
30 achieve, and inconvenient if the profile includes access to a large number of services.

The present invention allows the profiles to be re-instated on the communications device 12 automatically. This is achieved by using the profile data previously stored in the network, specifically in the data store 44, as will now be described with reference to Figure 3.

Figure 3 depicts the information flows transmitted over the data network 30 (Figure 2) between the network elements depicted in Figure 2, namely the user's communications device 12, the service platform 52, the activation server 46, and the data 50 stored in the directory 44 associated with the activation server.

5 The process begins when the user communications device 12 initiates an attempt 61 to access the service platform 52. In normal use, the user communications device provides its profile information as part of the request, in particular the calling line identity associated with the communications device's address on the PSTN 28, which has previously been identified as described above, and any authentication data. This
10 information is used by the service platform 52 to identify the user to which the request relates. This allows the service platform to provide user-specific data, for example voicemail messages sent by callers to the PSTN line.

However, it is possible for the profile data stored by the user communications device 12 to have been corrupted or lost, such that it no longer corresponds to the data
15 required by the service platform. It is also possible for the data held by the service platform 52 to have been modified, perhaps because the user's subscription to the service has ceased, or because the owner has requested service no longer be made available to that particular communications device because it is no longer in the subscriber's possession, having been replaced, sold, lost or stolen. In either case, there will be a
20 mismatch between the profile data provided by the communications device 12 making the request 61 and the profile data held by the service provider 52, and the service platform 52 will return an authentication failure message 62.

The communications device 12 is programmed to respond to such a failure message by attempting to restore its profile data. This may be done by the
25 communications device automatically, or in response to an input provided by a user in response to a message displayed on the communications device when it receives a service failure message 62.

In order to attempt to re-establish the service, the communications device 12 initiates a session with the activation server 46. This is done through a handshake
30 process 63-66 in which the communications device 12 and the activation server 46 exchange public key certificates, and each performs a respective validation processes 64, 65 on the other's certificate to ensure authenticity. If these validations are successful, they each transmit an acknowledgement 66 to the other.

A secure communications session 67 has now been established between the
35 communications device 12 and the activation server 46. The communications device 12

now transmits a request 70 to check its subscription, using the encryption provided by the activation server's public key. The request includes the device's equipment code. The activation server decrypts the request using its private key (step 71) and retrieves the user profile 50 from the directory 44 (step 72). The activation server 46 checks whether the
5 required service is marked "active" on the user profile 50 (step 73).

The activation server 46 now returns a message 74 to the communications device 12. This message is encrypted using the public key provided by the device 12. If the required service is not marked "active" the message is such as to cause the display 14 on the device to display a message to that effect. If the required service is marked "active"
10 the activation server extracts the information required to reconfigure the device from the profile data and transmits it to the device 12 in the message 74. This information includes the CLI data needed to match the device identity to the user details required by the service platform 52.

The communications device 12, on receiving the encrypted message, uses its
15 private key to decrypt the message (step 68) and uses the data in the message to restore its user profile.

For security, the profile 50 is updated with a new password, which is communicated to the activation server 46 (step 72) and thus to the device 12 (step 68).

The device may now re-attempt connection to the service platform 52 (step 61
20 repeated). As before, the user communications device provides its profile information as part of the request, in particular the calling line identity associated with the communications device's address on the PSTN 28, which has previously been identified as described above, and any authentication data. This information is used by the service platform 52 to identify the user to which the request relates, allowing the service platform
25 to provide user-specific data, for example voicemail messages sent by callers to the PSTN line.

This process allows re-configuration to take place in the background without any active participation by the user.

If the device is not currently registered with the activation server, the information
30 required will not be present in the user profile 50. In such a case the user may be prompted to initiate the activation process which has been described previously with reference to Figure 2.

CLAIMS

1. Method for re-configuring a communications device in which profile data is maintained for access to a communications service platform, wherein
- 5 profile data relating to the communications device is stored on an authentication platform, and
- the profile is also stored in the communications device
- and in which:
- if the communications device detects that the profile data is no longer stored in the
- 10 communications device, the communications device generates a request for re-authentication, and transmits the request to a reactivation server together with the communications device identity,
- on receipt of the request, the reactivation server retrieves the stored profile data associated with the communications device identity from the authentication platform and
- 15 returns it to the communications device
- the communications device stores the retrieved profile data.
- 20 2. Method according to claim 1, in which the communication device detects the absence of the required profile data by receipt from a service platform, in response to an attempt to access a service from the service platform, of a notification of failure to access the service.
- 25
3. Method according to claim 1 or claim 2, wherein the profile data is initially generated by interaction of the communications device with the authentication platform, such that the authentication platform generates a profile associated with the
- 30 communications device identity, for storage by the authentication platform, such that the data can subsequently retrieved by the communications device.

4. Method according to claim 3, wherein the profile data is initially generated by a first mode of communications in which a calling line identity apparent to the authentication platform is associated with a device identity, and the calling line identity is stored by the authentication platform and the device as part of the profile data for use in subsequent
5 interactions between the communications device and the authentication platform over a second mode of communications in which the calling line identity is not apparent to the authentication platform except as part of the profile data delivered to the authentication platform.

10

5. Method according to claim 3 or 4, wherein the reactivation process is a function of the authentication platform.

15 6. A communications device in which profile data is maintained for access to a communications service platform, having provision for storing profile data relating to the communications device

and configured such that, in the event of such profile data being determined to be absent from the communications device, it generates a request for re-authentication, and
20 transmits the request to a reactivation server together with the communications device identity,

and on receipt of the requested re-authentication profile data, to store the retrieved profile data.

25

7. Communications device according to claim 6, configured to attempt to access a service from a service platform and, in response of a notification of failure to access the service, identifying that the required profile data is absent.

30

8. Communications device according to claim 6 or claim 7, configured to generate profile data by interaction with the authentication platform, such that the data can subsequently retrieved by the communications device.

9 Communications device according to claim 8, configured to store a calling line identity as part of the profile data for use in subsequent interactions between the communications device and the authentication platform over a second mode of communications in which the calling line identity is not apparent to the authentication
5 platform except as part of the profile data delivered to the authentication platform.

10. A communications service platform, comprising an authentication platform for
10 storing profile data relating to one or more associated communications devices, together with identity data for the associated communications devices,
 and configured to receive a request from a communications device for re-authentication together with an identity for the communications device,
 and comprising a reactivation server for retrieving the stored profile data
15 associated with the communications device identity in response to such a request and returning it to the communications device.

20 11. A communications service platform according to claim 10, comprising means for interaction with the communications device so as to generate a profile associated with the communications device identity, for storage such that the data can subsequently retrieved by the communications device.

25

12. Communications service platform according to claim 11, configured to generate the profile data by a first mode of communications in which a calling line identity apparent to the authentication platform is associated with a device identity, and the calling line
30 identity is stored by the authentication platform as part of the profile data for use in subsequent interactions between the communications device and the authentication platform over a second mode of communications in which the calling line identity is not apparent to the authentication platform except as part of the profile data delivered to the authentication platform.

35

AMENDED CLAIMS**received by the International Bureau on 16 February 2011 (16.02.2011)**

1. Method for re-configuring a communications device in which profile data is maintained for access to a communications service platform, wherein
- 5 profile data relating to the communications device is stored on an authentication platform, and
- the profile is also stored in the communications device
- and in which:
- if the communications device detects that the profile data is no longer stored in the
- 10 communications device, the communications device generates a request for re-authentication, and transmits the request to a reactivation server together with the communications device identity,
- on receipt of the request, the reactivation server retrieves the stored profile data associated with the communications device identity from the authentication platform and
- 15 returns it to the communications device
- the communications device stores the retrieved profile data.
- 20 2. Method according to claim 1, in which the communication device detects the absence of the required profile data by receipt from a service platform, in response to an attempt to access a service from the service platform, of a notification of failure to access the service.
- 25
3. Method according to claim 1 or claim 2, wherein the profile data is initially generated by interaction of the communications device with the authentication platform, such that the authentication platform generates a profile associated with the
- 30 communications device identity, for storage by the authentication platform, such that the data can subsequently retrieved by the communications device.

4. Method according to claim 3, wherein the profile data is initially generated by a first mode of communications in which a calling line identity apparent to the authentication platform is associated with a device identity, and the calling line identity is stored by the authentication platform and the device as part of the profile data for use in subsequent interactions between the communications device and the authentication platform over a second mode of communications in which the calling line identity is not apparent to the authentication platform except as part of the profile data delivered to the authentication platform.

10

5. Method according to claim 3 or 4, wherein the reactivation process is a function of the authentication platform.

15 6. A communications device in which profile data is maintained for access to a communications service platform, having provision for storing profile data relating to the communications device

and configured such that, in the event of such profile data being determined to be no longer stored in the communications device, it generates a request for re-authentication, and transmits the request to a reactivation server together with the communications device identity,

20

and on receipt of the requested re-authentication profile data, to store the retrieved profile data.

25

7. Communications device according to claim 6, configured to attempt to access a service from a service platform and, in response of a notification of failure to access the service, identifying that the required profile data is absent.

30

8. Communications device according to claim 6 or claim 7, configured to generate profile data by interaction with the authentication platform, such that the data can subsequently retrieved by the communications device.

9 Communications device according to claim 8, configured to store a calling line
identity as part of the profile data for use in subsequent interactions between the
communications device and the authentication platform over a second mode of
communications in which the calling line identity is not apparent to the authentication
5 platform except as part of the profile data delivered to the authentication platform.

10. A communications service platform, comprising an authentication platform for
storing identity data for one or more associated communications devices, together with
10 profile data relating to, and also stored on, one or more associated communications
devices,

 the platform being configured to receive a request from a communications device
for re-authentication together with an identity for the communications device,

 and comprising a reactivation server for retrieving the stored profile data
15 associated with the communications device identity in response to such a request and
returning it to the communications device.

11. A communications service platform according to claim 10, comprising means for
20 interaction with the communications device so as to generate a profile associated with the
communications device identity, for storage such that the data can subsequently retrieved
by the communications device.

25 12. Communications service platform according to claim 11, configured to generate
the profile data by a first mode of communications in which a calling line identity apparent
to the authentication platform is associated with a device identity, and the calling line
identity is stored by the authentication platform as part of the profile data for use in
subsequent interactions between the communications device and the authentication
30 platform over a second mode of communications in which the calling line identity is not
apparent to the authentication platform except as part of the profile data delivered to the
authentication platform.

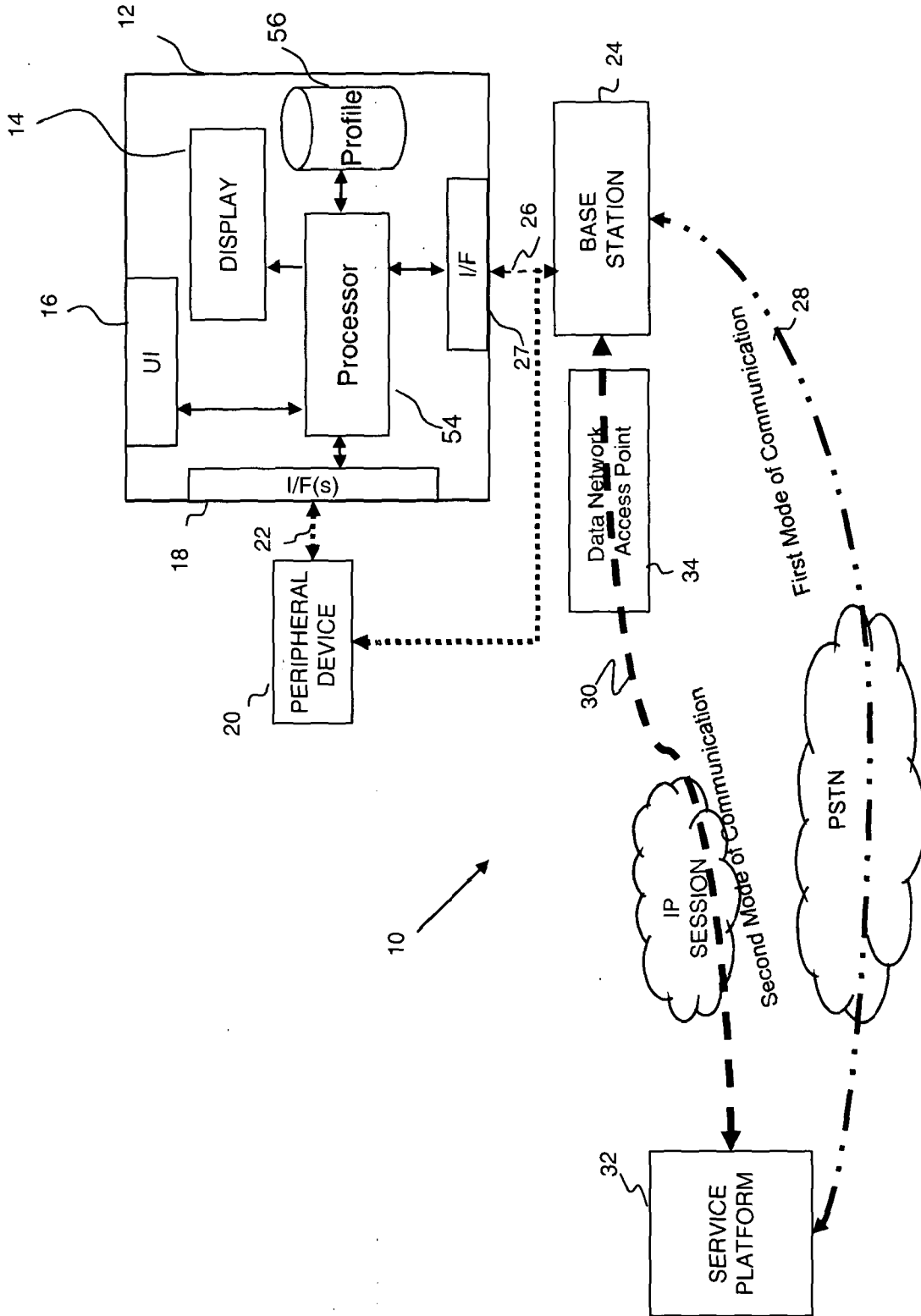


FIGURE 1

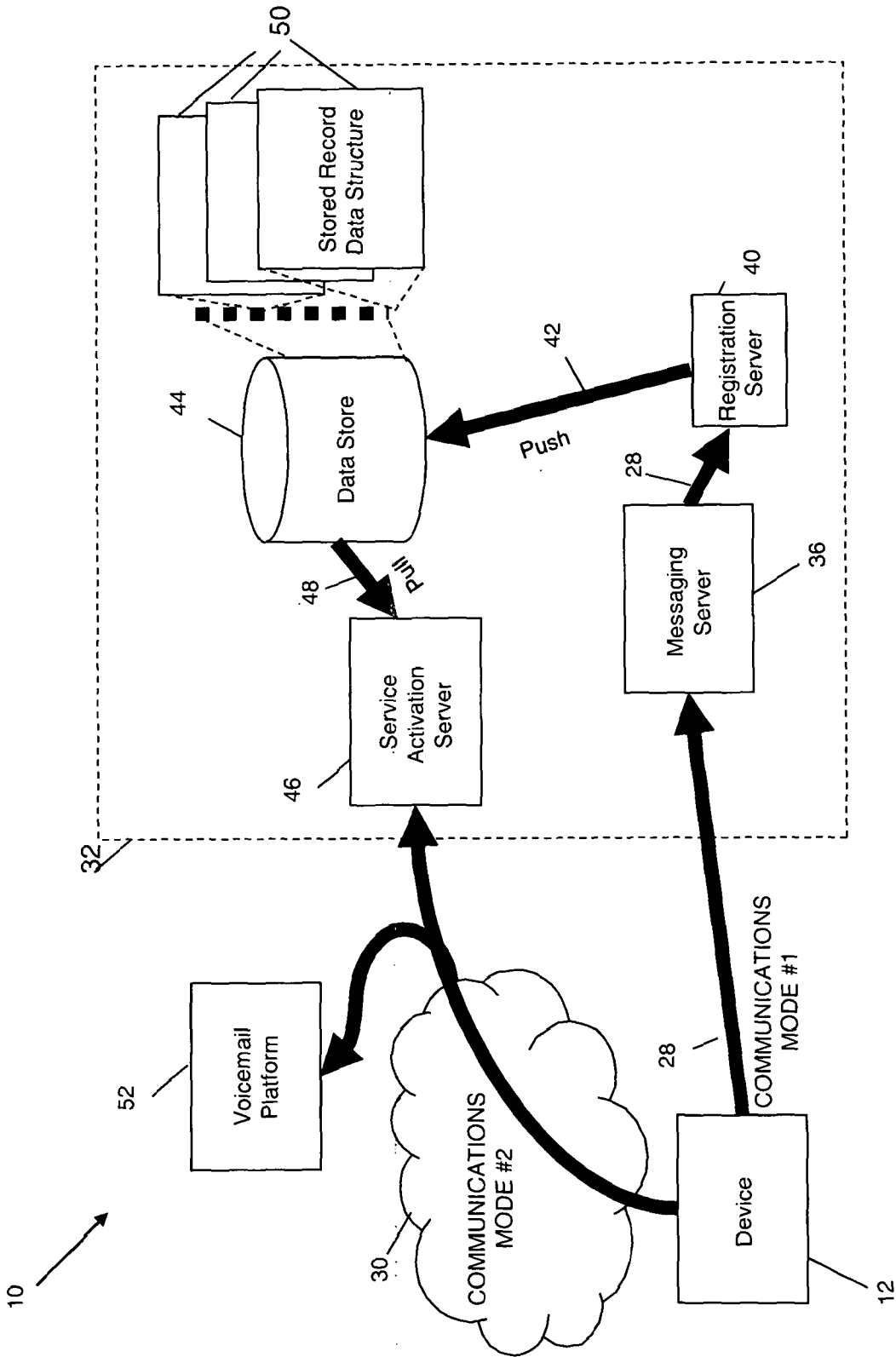
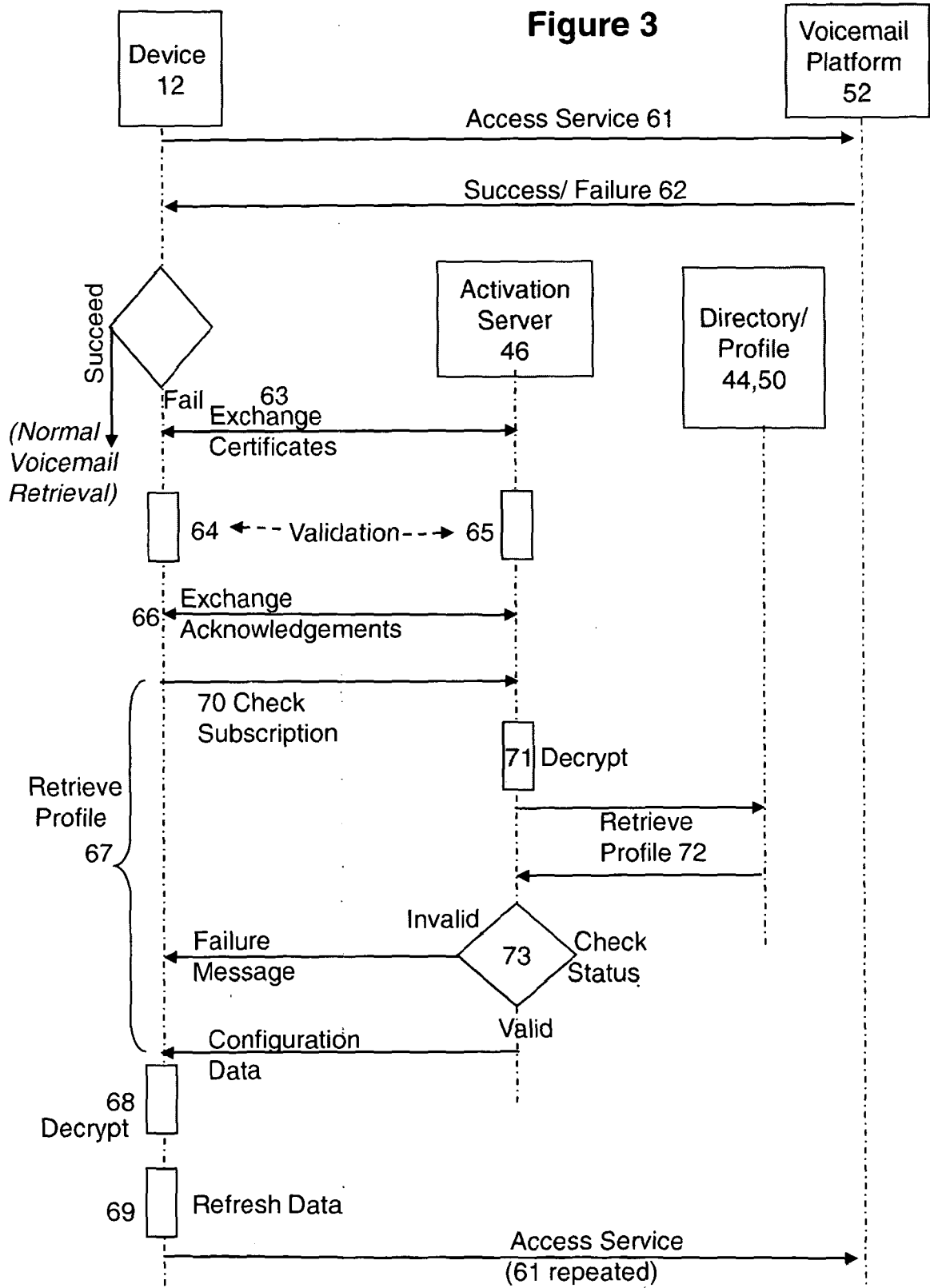


FIGURE 2

Figure 3



INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2010/001532

<p>A. CLASSIFICATION OF SUBJECT MATTER</p> <p>INV. H04W12/06 H04L29/06 H04W4/12 H04W8/20 H04W8/24 H04W8/30 H04M3/533</p> <p>ADD.</p> <p>According to International Patent Classification (IPC) or to both national classification and IPC</p>								
<p>B. FIELDS SEARCHED</p> <p>Minimum documentation searched (classification system followed by classification symbols) H04W H04L H04M</p> <p>Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched</p> <p>Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal, COMPENDEX, INSPEC, PAJ, IBM-TDB, WPI Data</p>								
<p>C. DOCUMENTS CONSIDERED TO BE RELEVANT</p> <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>A</td> <td> <p>US 2005/228874 A1 (EDGETT JEFF S [US] ET AL EDGETT JEFF STEVEN [US] ET AL) 13 October 2005 (2005-10-13) * abstract paragraph [0008] paragraph [0058] paragraph [0062] - paragraph [0065] figure 6</p> <p style="text-align: center;">----- -/--</p> </td> <td>1-12</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	A	<p>US 2005/228874 A1 (EDGETT JEFF S [US] ET AL EDGETT JEFF STEVEN [US] ET AL) 13 October 2005 (2005-10-13) * abstract paragraph [0008] paragraph [0058] paragraph [0062] - paragraph [0065] figure 6</p> <p style="text-align: center;">----- -/--</p>	1-12
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.						
A	<p>US 2005/228874 A1 (EDGETT JEFF S [US] ET AL EDGETT JEFF STEVEN [US] ET AL) 13 October 2005 (2005-10-13) * abstract paragraph [0008] paragraph [0058] paragraph [0062] - paragraph [0065] figure 6</p> <p style="text-align: center;">----- -/--</p>	1-12						
<p><input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.</p>								
<p>* Special categories of cited documents :</p> <table border="0"> <tr> <td style="vertical-align: top;"> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> </td> <td style="vertical-align: top;"> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.</p> <p>"&" document member of the same patent family</p> </td> </tr> </table>			<p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.</p> <p>"&" document member of the same patent family</p>				
<p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.</p> <p>"&" document member of the same patent family</p>							
<p>Date of the actual completion of the international search</p> <p style="text-align: center;">20 January 2011</p>		<p>Date of mailing of the international search report</p> <p style="text-align: center;">10/02/2011</p>						
<p>Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016</p>		<p>Authorized officer</p> <p style="text-align: center;">Horn, Marc-Philipp</p>						

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2010/001532

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/156176 A1 (HAO JACK JIANXIU [US] ET AL) 18 June 2009 (2009-06-18)	6-12
A	* abstract paragraph [0017] paragraph [0027] paragraph [0045] paragraph [0060] - paragraph [0065] paragraph [0068] paragraph [0082] - paragraph [0085] paragraph [0095] - paragraph [0099] figures 1, 7, 10, 13 -----	1-5
X	US 2009/154663 A1 (THAPER ATUL [US] ET AL) 18 June 2009 (2009-06-18)	6-12
A	* abstract paragraph [0042] - paragraph [0056] figures 4a-4c -----	1-5
A	US 2008/181141 A1 (KRANTZ ANTON [US] ET AL) 31 July 2008 (2008-07-31) * abstract paragraph [0034] - paragraph [0041] figure 3A -----	1-12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/GB2010/001532

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International Application No. PCT/ GB2010/ 001532

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-5

Restoring lost or corrupted profile data in a communications device

2. claims: 6-12

Configuring a communications device

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No PCT/GB2010/001532

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005228874	A1	13-10-2005	EP 1743252 A2 17-01-2007 US 2009150525 A1 11-06-2009 WO 2005104425 A2 03-11-2005

US 2009156176	A1	18-06-2009	CN 101933317 A 29-12-2010 CN 101933318 A 29-12-2010 CN 101933319 A 29-12-2010 EP 2232836 A1 29-09-2010 EP 2232837 A1 29-09-2010 EP 2232839 A1 29-09-2010 US 2009154667 A1 18-06-2009 US 2009154668 A1 18-06-2009 US 2009157732 A1 18-06-2009 US 2009154663 A1 18-06-2009 WO 2009076050 A1 18-06-2009 WO 2009076051 A1 18-06-2009 WO 2009076052 A1 18-06-2009

US 2009154663	A1	18-06-2009	CN 101933317 A 29-12-2010 CN 101933318 A 29-12-2010 CN 101933319 A 29-12-2010 EP 2232836 A1 29-09-2010 EP 2232837 A1 29-09-2010 EP 2232839 A1 29-09-2010 US 2009154667 A1 18-06-2009 US 2009154668 A1 18-06-2009 US 2009157732 A1 18-06-2009 US 2009156176 A1 18-06-2009 WO 2009076050 A1 18-06-2009 WO 2009076051 A1 18-06-2009 WO 2009076052 A1 18-06-2009

US 2008181141	A1	31-07-2008	NONE
