(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
5 March 2009 (05.03.2009)

PCT

(10) **International Publication Number**
WO 2009/029313 Al

(51) **International Patent Classification:**
***H04M 3/533* (2006.01)**

(21) **International Application Number:**
PCT/US2008/065046

(22) **International Filing Date:** 29 May **2008 (29.05.2008)**

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
60/969,419 31 August 2007 (3 1.08.2007) US

(71) **Applicant** *(for all designated States except US):* **AT & T MOBILITY π LLC** [US/US]; 5565 Glenridge Connector, Atlanta, GA 30342 (US).

(72) **Inventors; and**
(75) **Inventors/Applicants** *(for US only):* **SIGMUND, William, Joseph** [US/US]; 5110 Apple Grove Drive, Cumming, GA 30040 (US). **ZUBAS, Michael, Robert** [US/US]; 535 Chapman Lane, Marietta, GA 30066 (US). **RAINER, Brian, Keith** [US/US]; 695 River Oak Loop, Lawrenceville, GA 30044 (US).

(74) **Agents: KNOWLTON, Paul,** E. et al.; Parks Knowlton LLC, 1117 Perimeter Center West, Suite E402, Atlanta, GA 30338 (US).

(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, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(54) **Title:** SECURE VISUAL VOICEMAIL

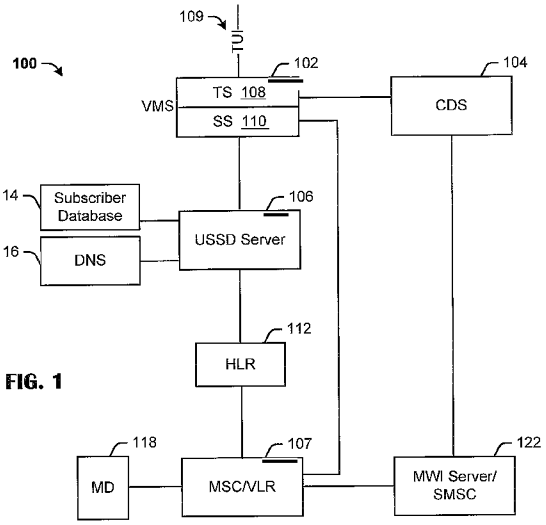

FIG. 1

(57) **Abstract:** A method (200) for managing voicemail messages for a visual voicemail system (102) can include establishing a secure data session (212) between a voicemail system (102) and a mobile device (118). The voicemail system (102) can receive a voicemail message (202) that is directed to a voicemail account associated with a voicemail subscriber. The voicemail system (102) can generate a notification message and can send the notification message (208) to the mobile device (118) that is associated with the voicemail account that received the voicemail message. In response to the notification message, the mobile device (102) can generate and send a first request for voicemail message header information (234). The voicemail system (118) can send the requested voicemail message header information (236) to the mobile device (102) and, in response, receive a second request for at least one voicemail message (238). The voicemail message can send at least a portion of the at least one voicemail message (240) to the mobile device (118).

PATENT APPLICATION

SECURE VISUAL VOICEMAIL

RELATED APPLICATION

This application claims priority to U.S. Provisional Patent Application Number 60/969,419, filed August 31, 2007, the entirety of which is hereby incorporated by reference.

TECHNICAL FIELD

The present disclosure relates generally to voicemail service and, more particularly, to a secure visual voicemail service.

BACKGROUND

Voicemail systems allow a caller to leave a voice message if the desired recipient is unavailable. Traditional voicemail systems (referred to herein as plain old voicemail or POVM) allow a subscriber to place a call to a voicemail system to access messages stored in his or her voicemail box. This is often done through a telephone user interface (TUI) that facilitates interaction between the subscriber and the voicemail system. The TUI provides functions for the subscriber to listen to messages, skip messages, delete messages, and save messages. The TUI can also provide functions for the subscriber to set a voicemail greeting, record a voicemail greeting, record a name, and set/change a password.

With some voicemail systems, a subscriber with multiple voicemail messages is required to listen to, skip, delete, or save each message while reviewing the voicemail box. This is time consuming and can be frustrating for the subscriber in situations where an important message has been deposited, requiring the subscriber to listen to, skip, delete or save each message in search of the important message.

To help reduce the need to search through multiple messages, various improved voicemail systems have been developed that allow messages to be stored based on a priority scheme to increase the efficiency of listening to voicemail messages. Often, these systems use a telephone number of the caller to identify a priority for a message and position the voicemail messages in order based on the assigned priorities. When the recipient accesses the voicemail system to acquire voicemail messages, the recipient is presented with each voicemail message in order of the priority or importance to the recipient. Accordingly, the recipient is must listen to and/or skip through multiple voicemail messages to find an important message. However, an important message can be easily relegated to a position of low importance if the subscriber previously has not set the priority for the caller. In this system, the priority for an incoming voicemail message is determined directly by the telephone number associated with the caller.

The aforementioned systems fail to allow a subscriber to select the exact voicemail message the subscriber would like to hear. Furthermore, the aforementioned systems require the use of a TUI to access the voicemail system to listen to voicemail messages and manage a voicemail account. These systems merely notify a subscriber of a pending voicemail message with a message waiting indicator (MWI) and require that the subscriber access the voicemail system to retrieve the pending message(s). Thus, it is desirable to create new enhanced voicemail systems and novel methods for providing secure visual voicemail (WM) services.

SUMMARY

A method for managing incoming voicemail messages for a visual voicemail system can include establishing a secure data session between a voicemail system and a mobile device, receiving a new voicemail message at the voicemail system, wherein the new voicemail message is directed to a voicemail account associated with a voicemail subscriber, generating a notification message in response to the new voicemail message, sending the notification message to the mobile device associated with the voicemail account that received the new voicemail message, receiving a first request for voicemail message header information in response to the notification message, sending the requested voicemail message header information to the mobile device in response to the first request, receiving a second request for at least one voicemail message, and sending the at least one voicemail message to the mobile device in response to the second request. Establishing the secure data session between the voicemail system and the mobile device can include establishing a secure sockets layer (SSL) data session or a transport layer security (TLS) data session, for example.

A method for setting or changing a voicemail greeting for visual voicemail service can include establishing a secure data session between a voicemail system and a mobile device, receiving a request from the mobile device to change a voicemail greeting, wherein the request can include a new voicemail greeting recorded on the mobile device, and saving the new voicemail greeting at the voicemail system. The method can further include generating a response indicating the success or failure of the request, and sending the response to the mobile device. Establishing the secure data session between the voicemail system and the mobile device can include establishing a secure sockets layer (SSL) data session or a transport layer security (TLS) data session, for example.

A method for changing a password for accessing visual voicemail service can include establishing a secure data session between a voicemail system and a mobile device, receiving a request from the mobile device to change a voicemail password, wherein the request can include an old password and a new password entered on the mobile device, and saving the new password, thereby replacing the old password. The method can further include generating a response indicating the success or failure of the request, and sending the response to the mobile device. Establishing the secure data session between the voicemail system and the mobile device can include establishing a secure sockets layer (SSL) data session or a transport layer security (TLS) data session, for example.

A method for setting or changing a recorded name for a visual voicemail service can include establishing a secure data session between a voicemail system and a mobile device, receiving a request from the mobile device to change a recorded name, wherein the request can include a new recorded name recorded on the mobile device, and saving the new recorded name, thereby replacing an old recorded name. The method can further include generating a response indicating the success or failure of the request, and sending the response to the mobile device. Establishing the secure data session between the voicemail system and the mobile device can include establishing a secure sockets layer (SSL) data session or a transport layer security (TLS) data session, for example.

A method for managing voicemails from a mobile device can include establishing a secure data session between a mobile device and a voicemail system, receiving a notification message identifying that at least one new voicemail message has been deposited into a voicemail account associated with the mobile device, generating a first request for voicemail header information from the voicemail system, sending the first request to the voicemail system, receiving, in response to the first request, the requested voicemail message header information, generating a second request for at least one voicemail message identified in the requested voicemail message header information, sending the second request to the voicemail system, and receiving, in response to the second request, the requested at least one voicemail message. The method can further include saving the at least one voicemail message at least temporarily in a memory of the mobile device. Establishing the secure data session between the voicemail system and the mobile device can include establishing a secure sockets layer (SSL) data session or a transport layer security (TLS) data session, for example. Establishing the secure data session between the voicemail system and the mobile device can include establishing a secure sockets layer (SSL) data session or a transport layer security (TLS) data session, for example.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a portion of an exemplary network in which aspects of the present disclosure can be practiced.

FIG. 2 is a message flow diagram illustrating a process for voicemail message deposit and subsequent secure retrieval of message content for local storage on a mobile device, according to an exemplary embodiment present disclosure.

FIG. 3 is a message flow diagram illustrating a secure process for setting or changing a voicemail greeting, according to an exemplary embodiment of the present disclosure.

FIG. 4 is a message flow diagram illustrating a secure process for setting or changing a voicemail password, according to an exemplary embodiment of the present disclosure.

FIG. 5 is a message flow diagram illustrating a secure process for setting or changing a recorded name, according to an exemplary embodiment of the present disclosure.

FIG. 6 schematically illustrates an exemplary mobile device and components thereof for use in accordance with an embodiment of the present disclosure.

DETAILED DESCRIPTION

As required, detailed embodiments of the present disclosure are disclosed herein. It must be understood that the disclosed embodiments are merely exemplary examples of the disclosure that may be embodied in various and alternative forms, and combinations thereof. As used herein, the word "exemplary" is used expansively to refer to embodiments that serve as an illustration, specimen, model or pattern. The figures are not necessarily to scale and some features may be exaggerated or minimized to show details of particular components. In other instances, well-known components, systems, materials or methods have not been described in detail in order to avoid obscuring the present disclosure. Therefore, specific structural and functional details disclosed herein are not to be interpreted as limiting, but merely as a basis for the claims and as a representative basis for teaching one skilled in the art to variously employ the present disclosure.

Referring now to the drawings wherein like numerals represent like elements throughout the several views, **FIG.** 1 schematically illustrates a portion of an exemplary wireless communications network **100** in which some embodiments of the present disclosure can be implemented. By way of example, the wireless communications network **100** can be configured as a 2G GSM (Global System for Mobile communications) network and can provide data communications via GPRS (General Packet Radio Service), and EDGE (Enhanced Data rates for GSM Evolution). By way of further example, the wireless communications network 100 can be configured as a 3G UMTS (Universal Mobile Telecommunications System) network and provide data communications via the HSPA (High-Speed Packet Access) protocol family, such as, HSDPA (High-Speed Downlink Packet Access), EUL (Enhanced Uplink) or otherwise termed HSUPA (High-Speed Uplink Packet Access), and HSPA+ (Evolved HSPA). The wireless communications network 100 is also compatible with future mobile communications standards including, but not limited to, pre-4G and 4G, for example. The wireless communications network 100 can be configured to provide messaging services via Short Message Service (SMS), Multimedia Message Service (MMS), instant messaging and unstructured supplementary service data (USSD), for example. The wireless communications network 100 can also be configured to provide advanced voicemail messaging features, such as visual voicemail.

The illustrated wireless communications network 100 includes a voicemail system (VMS) 102 that is illustrated as being in communication with a content delivery server (CDS) 104, a USSD server 106, and a mobile switching center (MSC) and visiting location register (VLR) 107, although this is not necessarily the case. The VMS 102 can include a telephony server (TS) 108 for handling incoming voicemail inquiries via a telephone user interface (TUI) 109 and a storage server (SS) 110 for storing and managing voicemail messages for a plurality of voicemail accounts.

The USSD server 106 can be configured to receive, decode, and process new USSD messages, perform database queries to retrieve the VMS hostname serving a subscriber, perform database queries to resolve the VMS hostname to the corresponding IP address, obtain the subscriber's voicemail class of service (COS), and send the subscriber's voicemail COS to the subscriber's mobile device. The USSD server 106 is illustrated as being in communication with a home location register (HLR) 112, a subscriber database 114, and a domain name server (DNS) 116 to facilitate these functions.

The subscriber database 114 can be configured to store and manage subscriber data, such as, for example, account information, billing information, services information, and equipment information for a plurality of subscribers. The DNS server 116 can be configured to maintain a database for resolving host names and IP addresses for various network nodes, such as the VMS 102, for example. The USSD server 106 can retrieve the VMS hostname serving a subscriber from the subscriber database 114 and query the DNS 116 by specifying the VMS hostname to resolve the corresponding IP address.

The HLR 112 can be configured to provide routing information for mobile-terminated calls and short message service (SMS) messages. The HLR 112 is illustrated as being in communication with the MSC/VLR 107. The MSC/VLR 107 is in communication with a MD 118 and a short message service center (SMSC) 122. The MD 118 can be, but is not limited to, a user equipment, a mobile terminal, a cellular telephone, a personal digital assistant (PDA), a handheld computer, or combinations thereof, and the like. The SMSC 122 can be configured to delivery SMS messages and message waiting indicator (MWI) messages.

The VMS 102 can be configured to store a plurality of voicemail accounts. Each voicemail account can include a voicemail box in which voicemail messages can be deposited for a subscriber. The number of voicemail messages capable of being stored per account can be determined by the voicemail service provider or any third party provider, such as the system manufacturer, for example. The maximum voicemail message length can also be set, if desired. The number of voicemail messages and the maximum voicemail message length can be configured on the VMS 102.

Prior to a subscriber being provisioned for visual voicemail service, the voicemail box is in a *not provisioned* state. After being provisioned for visual voicemail service, the subscriber's voicemail box state is changed to *provisioned - not initialized* to reflect that the subscriber is provisioned for service but has not yet initialized service via a boot message process that is described below. After completion of the boot message process, the VMS 102 state can be changed to *provisioned - initialized* to reflect that the subscriber is provisioned for voicemail service and has completed the first boot access process.

The VMS 102 is accessible via traditional or plain old voicemail (POVM) methods and visual voicemail (WM) methods described herein. State changes to voicemail messages, whether requested through the TUI 109 via POVM methods or directly on the MD 118 via W M methods, are automatically updated in both the voicemail box and on the subscriber's MD 118. This ensures automatic and full synchronization between the subscriber's MD 118 and the VMS 102 so that the latest voicemail information is stored on the subscriber's MD 118. The subscriber's VMS-hosted voicemail box recognizes and maintains message states for each message, such as, but not limited to, an *unheard- new* state, a *skipped* state, and a *saved- read* state. Deleted messages can be deleted from the VMS 102, via the TUI 109 or directly on the MD 118. The message is deleted on both the VMS 102 and the MD 118. Alternatively, a message can remain accessible on the MD 118 and/or on the VMS 102 for a specified period of time to allow the message to be recovered in the case of accidental or premature deletion. The VMS 102 can discard all messages after the MD 118 has successfully received and stored the available message content.

The MD 118 voicemail box also can recognize and maintain message states. The MD 118 voicemail box can have message states for each message including, but not limited to, an *unheard- new* state, a *saved - read* state, and a *deleted* state. The MD 118 does not require a *skipped* state because W M provides an interface that allows a subscriber to access any message regardless of the order in which the message was received and is not subject to restraint of a priority scheme. As mentioned above, the MD 118 voicemail box *deleted* state can be configured such that the message is available for recovery or merely as an indication that the message has been deleted. Either of these options can be set to be available for a time specified by either the subscriber via a device input or by the voicemail service provider.

Messages used to establish and/or update a W M account can be sent using a variety of protocols, such as, but not limited to, short message peer-to-peer (SMPP), domain name server (DNS) protocol, lightweight directory access protocol (LDAP), unstructured supplementary service data (USSD) protocol, Internet message access protocol version 4 (IMAP4), and hypertext transfer protocol (HTTP), HTTP over secure socket layer (HTTPS), for example. Moreover, protocols to provide or enhance the security of data transmission to and from the various nodes described above can be provided via cryptographic protocols, such as, but not limited to, transport layer security (TLS), secure sockets layer (SSL), improvements, versions, variations, or evolutions thereof, and the like. The description provided below assumes an understanding of these protocols and as such further explanation is not provided. The use of alternative protocols or additional protocols to acquire similar results is deemed to be within the scope of the present disclosure and the attached claims.

A first boot process can enable a subscriber to receive confirmation that W M service is enabled and is immediately accessible via a W M application on the MD 118. A visual prompt can be presented to the subscriber as a cue or reminder to setup a voicemail box prior to receipt of incoming voice messages. Conventional voicemail, in contrast, can block receipt of new messages until the mailbox is set up, or can notify the subscriber of the first new voice messages thereby prompting the subscriber to place a call to retrieve them, but can bar access to those messages until the subscriber sets up the mailbox. The visual prompt of the present disclosure advantageously can eliminate the need to access the voicemail system 102 via the TUI 109 to setup the voicemail box and can help to ensure that the subscriber sets up a voicemail box. The notification message also can be used to reset a voicemail password after a voicemail account is enabled.

The W M service uses several parameters to enable automatic synchronization between the MD 118 and the VMS 102. For example, prior to first boot, the MD 118 does not have the CDS ID, port number, mailbox ID, initial or reset password, and a token value, if applicable. Accordingly, an initial or first boot SMPP message can include a basic set of parameters for future synchronization sessions including a default password. If a subscriber forgets the password or otherwise needs to have the voicemail password reset, the subscriber can initiate a password reset by selecting a password reset option on the MD 118. In this example, a new boot message can be sent to the MD 118 including a new default password in response to a password reset request from the MD 118.

Referring now to FIG. 2, a flow diagram illustrating a process 200 for voicemail message deposit and subsequent secure retrieval of message content for local storage on a mobile device 118 is illustrated, according to an exemplary embodiment of the present disclosure. It should be understood that the steps of the process 200 are not necessarily presented in any particular order and that performance of some or all the steps in an alternative order(s) is possible and is contemplated. The steps have been presented in the demonstrated order for ease of description and illustration. Steps can be added, omitted and/or performed simultaneously without departing from the scope of the appended claims. It should also be understood that the illustrated process 200 can be ended at any time. Some or all steps of this process, and/or substantially equivalent steps, can be performed by execution of computer-readable instructions included on a computer readable medium.

The process 200 is illustrated as including the VMS 102, the SMSC 122, and the MD 118. In the illustrated process 200, various messages and/or commands are exchanged among these network elements using various protocols, such as, for example, SMPP and HTTPS, although other protocols are contemplated as described above. The process 200 can be modified to include other network elements, such as the CDS 104. In one embodiment, CDS 104 acts in an intermediary capacity, facilitating communication between the MD 118 and the VMS 102. The CDS 104 can communicate with the VMS 102 via the IMAP protocol, for example.

The process 200 begins, at step 202, when a message is deposited into a voicemail box established at the VMS 102. At step 204, the VMS 102 can generate a notification short message (notification_sm) and send the notification_sm to the SMSC 122, at step 206. The SMSC 122 can temporarily store and forward the notification_sm message to the MD 118, at step 208.

The MD 118 can attach to a data network, for example, by a GPRS attach process and can perform a PDP context activation to connect to the data network via an access point name (APN) provided to the MD 118 by the service provider. The APN can be included in the notification_sm message, in a first boot message, or other communication between the MD 118 and the VMS 102 or other network elements, such as the CDS 104, a serving GPRS support node (SGSN), or a gateway GPRS support node (GGSN), for example. Accordingly, a GPRS attach and PDP context activation process 210 is illustrated. The MD 118 can perform these functions as is known in the art at any time prior to activating a secure handshake process 212. The handshake process 212 can be a handshake process of a cryptographic protocol, such as, but not limited to, SSL or TLS.

The illustrated secure handshake process 212 establishes the MD 118 as the client and the VMS 102 as the server, although this is not necessarily the case. As such, references to client refer to the MD 118 and references to server refer to the VMS 102 in the illustrated embodiment and description thereof. The secure handshake process 212 begins when the MD 118 generates and sends a clientjiello command to the VMS 102, at step 214. The client_hello command can include the version(s) of SSL or TLS that is supported by the MD 118, the cipher(s) supported by the MD 118 sorted in order of preference, the data compression algorithm(s) that is supported by the MD 118, and a session ID. The client_hello command can also include random data that is generated by the MD 118 for use in a key generation process.

At step 216, the VMS 102 receives the client_hello command and, in response, generates and sends a server_hello command to the MD 118. The serverj]ello command can include the SSL or TLS version that will be used for the secure session, the cipher that will be used for the secure session, the session ID, and, if applicable, the compression algorithm that will be used for the secure session. The server_hello command can also include random data that is generated by the VMS 102 for use in a key generation process.

At step 218, the VMS 102 can generate and send a certificate command to the MD 118. The certificate command can include a public key and an authentication signature. In addition, the certificate command can include a chain of certificates beginning with the certificate of the certificate authority that assigned the server's certificate.

At step 220, the VMS 102 can generate and send a server_done command to the MD 118 to indicate that the VMS 102 has completed this phase of the secure handshake process 212. If the MD 102 will be authenticated to the VMS 102, additional commands can flow between the MD 118 and the VMS 102. For example, the MD 118 can provide a certificate to authenticate to the VMS 102. This certificate can be sent, for example, in the first boot message, or other communication.

At step 222, the MD 118 can verify the server's certificate and can generate and send a certificate_verify command to the VMS 102 to inform the VMS 102 that the MD 118 has verified the certificate. Likewise, the VMS 102 can verify a client certificate, should one be used, and can generate and send a similar certificate_verify command to the MD 118 to inform the MD 118 that the VMS 102 has verified the certificate.

At step 224, the MD 118 can generate and send a change_cipher_spec command to convey to the VMS 102 that the contents of subsequent SSL transmissions sent by the MD 118 will be encrypted. At step 226, the MD 118 can generate and send a finished command to the VMS 102. The finished command can include a list of all secure handshake commands exchanged between the MD 118 and the VMS 102 to validate that none of the unencrypted commands sent to establish a secure session were changed.

At step 228, the VMS 102 can generate and send a change_cipher_spec command to convey to the MD 118 that the contents of subsequent SSL transmissions sent by the VMS 102 will be encrypted. At step 230, the VMS 102 can then generate and send a finished command. The finished command can include a list of all secure handshake commands exchanged between the VMS 102 and MD 118 to validate that none of the unencrypted commands sent to establish a secure session were changed. A secure session 232 is now established. HTTPS is described as the protocol used to send the various commands between the VMS 102 and the MD 118 in the secure session 232, although other secure protocols are contemplated, as described above.

The secure session 232 can begin when the MD 118 generates and sends a get_headers command to the VMS 102, at step 234. The get_headers command can include parameters, such as, but not limited to, the date, time, and calling line identity (CLI). The get_headers message can additionally include authentication information. At step 236, the VMS 102 retrieves the voicemail message headers for the voicemail account associated with the MD 118 and sends the headers to the MD 118. The MD 118 uses the headers to determine the status of each voicemail message stored on the MD 118 and to identify any new voicemail messages in the subscriber's voicemail account. After the MD 118 determines which message(s) needs to be retrieved, if any, the MD 118 can generate and send a getjnessage command with the header information for at least one requested message, at step 238. At step 240, the VMS 102 receives the get_message command and sends the requested message content to the MD 118. The secure session 232 can end at step 242.

The MD 118 can receive the message content and store the content under the appropriate header in a memory and permit a subscriber to access the content via a W M application graphical user interface (GUI). The message content can be formatted using any audio codec, such as, but not limited to, waveform audio (WAV), audio interchange file format (AIFF), RAW, encoded in GSM CODEC, advanced audio coding (AAC), MPEG-1 audio layer 3 (MP3), MPEG-4 Part 14 (MP4), Windows® media audio (WMA), RealAudio (RA), free lossless audio codec (FLAC), Apple® lossless encoder (ALE), *i.e.,* Apple® lossless audio codec (ALAC), and other open and proprietary audio formats.

An if-modified-since command can be used to occasionally poll the VMS 102 for an inbox voicemail message list and update any voicemail message if the voicemail was modified since the last update, for example, if a message was deleted or added. This can help reduce the amount of data traversing the network thereby reducing network congestion. In some instances, however, the header information is relatively small and as such no noticeable improvement may be available for sending only the modified voicemail message header.

More than one connection can be established to the VMS 102 or in some cases to multiple or redundant VMSs. This can allow for simultaneous requests in order to serve a subscriber's request to view or listen to a message faster. Load balancing techniques can also be implemented.

Message downloads that are interrupted, via cancellation or connection failure, can be resumed starting at the last received byte, for example. This assumes the message is stored in full, at least temporarily, on the VMS 102. In some instances, however, the VMS 102 can delete the message after the message content is sent to the MD 118. A subsequent request for one or more previously sent messages can be facilitated by re-retrieving the message, re-transcoding the message, and sending the message to the MD 118.

Requests to the VMS 102 can be pipelined in accordance with HTTP 1.1 specifications. This can help reduce network latency for multiple requests.

Referring now to FIG. 3, a flow diagram illustrating a secure process 300 for setting or changing a voicemail greeting is illustrated, according to an exemplary embodiment of the present disclosure. It should be understood that the steps of the process 300 are not necessarily presented in any particular order and that performance of some or all the steps in an alternative order(s) is possible and is contemplated. The steps have been presented in the demonstrated order for ease of description and illustration. Steps can be added, omitted and/or performed simultaneously without departing from the scope of the appended claims. It should also be understood that the illustrated process 300 can be ended at any time. Some or all steps of this process, and/or substantially equivalent steps, can be performed by execution of computer-readable instructions included on a computer readable medium.

The process 300 is illustrated as including the VMS 102, the SMSC 122, and the MD 118. In the illustrated process 300, various messages and/or commands are exchanged among these network elements using various protocols, such as, for example, HTTPS, although other protocols are contemplated as described above. The process 300 can be modified to include other network elements, such as the CDS **104.** In one embodiment, the CDS **104** acts in an intermediary capacity, facilitating communication between the MD **118** and the VMS **102.** The CDS **104** can communicate with the VMS **102** via the IMAP protocol, for example.

The illustrated process **300** begins at step **302,** wherein the MD **118** records a new voicemail greeting, such as, for example, a voicemail greeting dictated by a subscriber. The subscriber can select an upload function on the W M application to upload the new greeting. The greeting can be formatted using any audio codec, such as, but not limited to, waveform audio (WAV), audio interchange file format (AIFF), RAW, encoded in GSM CODEC, advanced audio coding (AAC), MPEG-1 audio layer 3 (MP3), MPEG-4 Part 14 (MP4), Windows® media audio (WMA), RealAudio (RA), free lossless audio codec (FLAC), Apple® lossless encoder (ALE), *i.e.,* Apple® lossless audio codec (ALAC), and other open and proprietary audio formats.

The MD **118** can establish a secure session using, for example, SSL or TLS, via a secure handshake process **212,** as described in FIG. 2. At step **304,** the MD **118** can generate and send a change_greeting_request to the VMS **102** via HTTPS, for example. The change_greeting_request can include the recorded greeting in one or more formats. The change_greeting_request can be sent to the VMS **102.** The VMS **102** can save the recording as the active or primary voicemail greeting for the subscriber. If a custom voicemail greeting is not set, a default voicemail greeting *(e.g.,* a network default greeting) can be replaced with the new voicemail greeting. At step **306,** the success or failure of the save can be reported back to the MD **118** via a change_greeting_response. If the change_greeting_request fails, the W M application can notify the subscriber to retry, offer customer support, and/or refer the subscriber to a telephone number or website address for further information and troubleshooting.

Referring now to **FIG.** 4, a message flow diagram illustrating a secure process **400** for setting or changing a voicemail password is illustrated, according to an exemplary embodiment of the present disclosure. It should be understood that the steps of the process **400** are not necessarily presented in any particular order and that performance of some or all the steps in an alternative order(s) is possible and is contemplated. The steps have been presented in the demonstrated order for ease of description and illustration. Steps can be added, omitted and/or performed simultaneously without departing from the scope of the appended claims. It should also be understood that the illustrated process 400 can be ended at any time. Some or all steps of this process, and/or substantially equivalent steps, can be performed by execution of computer-readable instructions included on a computer readable medium.

The process 400 is illustrated as including the VMS 102, the SMSC 122, and the MD 118. In the illustrated process 400, various messages and/or commands are exchanged among these network elements using various protocols, such as, for example, HTTPS, although other protocols are contemplated as described above. The process 400 can be modified to include other network elements, such as the CDS 104. In one embodiment, the CDS 104 acts in an intermediary capacity, facilitating communication between the MD 118 and the VMS 102. The CDS 104 can communicate with the VMS 102 via the IMAP protocol, for example.

If a password has not been set, the default password provided in a notification_sm can be required to be initialized prior to the subscriber accessing the voicemail box, setting the greeting, or setting a recorded name. If the password has not been initialized, the VMS 102 can send the current password in a notification_sm message. The current password can be used to access the voicemail box to configure the new password. The password can be any combination of numbers and/or characters and can be any length. The password can be set with a minimum and maximum length. The W M application can be configured to verify that the password complies with this requirement prior to attempting to change the password on the VMS 102. The password can be set with a minimum or maximum amount of numbers and/or characters. The W M application can be configured to verify that the password complies with this requirement prior to attempting to change the password on the VMS 102. Other requirements can be established. If the subscriber enters a password that fails to comply with any requirement, the W M application can notify the user to retry with a password that satisfies the requirement(s), offer customer support, and/or refer the customer to a telephone number or website address for further information and troubleshooting.

The illustrated process **400** begins when the subscriber is prompted to enter both the old password and the new password. The MD **118** can establish a secure session using, for example, SSL or TLS, via a secure handshake process **212,** as described above in FIG. 2, so that any password sent between the MD **118** and the VMS **102** is encrypted.

At step **402,** the subscriber can enter the old password and new password on the MD **118.** After the passwords have been entered, the W M application can generate a change_password_request. The change_password_request can be sent to the VMS **102** for storage, at step **404.** The VMS **102** can perform a password validation and save the new password. At step **406,** the VMS **102** can generate and send a change_password_response to report the success or failure of the change_password_request. Error codes can be set for the VMS **102** to return to the MD **118** in case the password is found invalid for any reason or if the password has expired. The W M application can be configured to receive an error code and provide corrective action to the subscriber to resolve the password issue. For example, the W M application can notify the user to retry, offer customer support, and/or refer the customer to a telephone number or website address for further information and troubleshooting.

Referring now to **FIG.** 5, a message flow diagram illustrating a secure process for setting or changing a recorded name is illustrated, according to an exemplary embodiment of the present disclosure. It should be understood that the steps of the process **500** are not necessarily presented in any particular order and that performance of some or all the steps in an alternative order(s) is possible and is contemplated. The steps have been presented in the demonstrated order for ease of description and illustration. Steps can be added, omitted and/or performed simultaneously without departing from the scope of the appended claims. It should also be understood that the illustrated process **500** can be ended at any time. Some or all steps of this process, and/or substantially equivalent steps, can be performed by execution of computer-readable instructions included on a computer readable medium.

The process 500 is illustrated as including the VMS 102, the SMSC 122, and the MD 118. In the illustrated process 500, various messages and/or commands are exchanged among these network elements using various protocols, such as, for example, HTTPS, although other protocols are contemplated as described above. The process 500 can be modified to include other network elements, such as the CDS 104. In one embodiment, CDS 104 acts in an intermediary capacity, facilitating communication between the MD 118 and the VMS 102. The CDS 104 can communicate with the VMS 102 via the IMAP protocol, for example.

The process 500 can begin when a subscriber records a new name on the MD 118, at step 502. The subscriber can then select an upload function on the W M application to upload the new name. The recorded name can be formatted using any audio codec, such as, but not limited to, waveform audio (WAV), audio interchange file format (AIFF), RAW, encoded in GSM CODEC, advanced audio coding (AAC), MPEG-1 audio layer 3 (MP3), MPEG-4 Part 14 (MP4), Windows® media audio (WMA), RealAudio (RA), free lossless audio codec (FLAG), Apple® lossless encoder (ALE), *i.e.,* Apple® lossless audio codec (ALAC), and other open and proprietary audio formats.

The MD 118 can establish a secure session using, for example, SSL or TSL, via a secure handshake process 212, as described above in FIG. 2, so that any password sent between the MD 118 and the VMS 102 is encrypted.

After a new name has been recorded, the W M application can generate a change_recorded_name_jequest containing the recorded name in the selected format, at step 504. The VMS 102 can receive the change_recorded_name_request and save the new recorded name. The VMS 102 can generate a change_recorded_name_response to report the success or failure of the save and send the change_recorded_name_response to the MD 118, at step 506.

The W M application can be configured to switch between the standard greeting without name, the standard greeting with name, and a custom greeting. The standard greeting can be, for example, a greeting provided by the VM service provider as a default with or without the recorded name. The W M application can be further configured to retrieve the current voicemail greeting and recorded name using a HTTP request.

FIG. 6 is a schematic block diagram illustrating an exemplary mobile device 118 for use in accordance with an exemplary embodiment of the present disclosure. Although no connections are shown between the components illustrated and described in FIG. 6, the components can interact with each other to carry out device functions.

As illustrated, the mobile device 118 can be a multimode handset. FIG. 6 and the following discussion are intended to provide a brief, general description of a suitable environment in which the various aspects of an embodiment of the present disclosure can be implemented. While the description includes a general context of computer-executable instructions, the present disclosure can also be implemented in combination with other program modules and/or as a combination of hardware and software.

Generally, applications can include routines, program modules, programs, components, data structures, and the like. Applications can be implemented on various system configurations, including single-processor or multiprocessor systems, minicomputers, mainframe computers, personal computers, hand-held computing devices, microprocessor-based, programmable consumer electronics, combinations thereof, and the like.

The illustrated device 118 includes a display 600 for displaying multimedia, such as, for example, text, images, video, telephony functions, such as, visual voicemail data, caller line ID data, setup functions, menus, music metadata, messages, wallpaper, graphics, and the like. The display 600 finds particular application in the present disclosure for displaying visual voicemail data in visual voicemail headers. The visual voicemail headers can include the date, time, CLI data, message length, and message status *(i.e.,* new-unread, read, saved, or deleted).

The device 118 can include a processor 602 for controlling, and/or processing data. A memory 604 can interface with the processor 602 for the storage of data and/or applications 606. The memory 604 can include a variety of computer readable media, including volatile media, non-volatile media, removable media, and non-removable media. Computer-readable media can include device storage media and communication media. Storage media can include volatile and/or non-volatile, removable and/or non¬removable media, such as, for example, RAM, ROM, EEPROM, flash memory or other memory technology, CD ROM, DVD, or other optical disk storage, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to store the desired information and that can be accessed by the device 118.

The memory 604 can be configured to store one or more applications 606. The applications 606 can include a user interface (Ul) application 608. The UI application 608 can interface with a client 610 (e.g., an operating system) to facilitate user interaction with device functionality and data, for example, managing voicemails in a visual voicemail application, answering/initiating calls, entering/deleting data, configuring settings, address book manipulation, multimode interaction, and the like. The applications 606 can include other applications 612 such as, for example, visual voicemail software, add-ons, plug-ins, voice recognition software, call voice processing, voice recording, messaging, e-mail processing, video processing, image processing, music play, combinations thereof, and the like, as well as subsystems and/or components. The applications 606 can be stored in the memory 604 and/or in a firmware 614, and can be executed by the processor 602. The firmware 614 can also store code for execution during initialization of the device 118.

A communications component 616 can interface with the processor 602 to facilitate wired/wireless communications with external systems including, for example, cellular networks, VoIP networks, LAN, WAN, MAN, PAN, that can be implemented using WiFi, WiMax, combinations and/or improvements thereof, and the like. The communications component 616 can also include a multimode communications subsystem for providing cellular communications via different cellular technologies. For example, a first cellular transceiver 618 can operate in one mode, for example, GSM, and an Nth transceiver 620 can operate in a different mode, for example WiFi. While only two transceivers 618, 620 are illustrated, it should be appreciated that a plurality of transceivers can be included. The communications component **616** can also include a transceiver **622** for unlicensed RF communications using technology such as, for example, WiFi, WiMAX, NFC, other RF and the like. The transceiver **622** can also be configured for line-of-sight technologies, such as, for example, infrared and IRDA. Although a single transceiver **622** is illustrated multiple transceivers for unlicensed RF and line-of-sight technologies are contemplated.

The communications component **616** can also facilitate communications reception from terrestrial radio networks, digital satellite radio networks, Internet-based radio services networks, combinations thereof, and the like. The communications component **616** can process data from a network, such as, for example, the Internet, a corporate intranet, a home broadband network, and the like, via an ISP, DSL provider, or other broadband service provider.

An input/output (I/O) interface **624** can be provided for input/output of data and/or signals. The I/O interface **624** can be a hardwire connection, such as, for example, a USB, PS2, IEEE 1394, serial, parallel, IEEE 802.3 (e.g., Ethernet - RJ45, RJ48), traditional telephone jack (e.g., RJ1 1, RJ14, RJ25) and the like, and can accept other I/O devices, such as, for example, a keyboard, keypad, mouse, interface tether, stylus pen, printer, plotter, jump/thumb drive, touch screen, touch pad, trackball, joy stick, controller, monitor, display, LCD, combinations thereof, and the like.

Audio capabilities can be provided by an audio I/O component **626** that can include a speaker (not shown) for the output of audio signals and a microphone (not shown) to collect audio signals.

The device **118** can include a slot interface **628** for accommodating a subscriber identity system **630,** such as, for example, a SIM or universal SIM (USIM). The subscriber identity system **630** instead can be manufactured into the device **118,** thereby obviating the need for a slot interface **628.**

The device **118** can include an image capture and processing system 632. Photos and/or videos can be obtained via an associated image capture subsystem of the image system **632,** for example, a camera. The device **118** can also include a video systems component 634 for processing, recording, and/or transmitting video content.

A location component 636 can be included to send and/or receive signals, such as, for example, GPS data, assisted GPS data, triangulation data, combinations thereof, and the like. The device 118 can use the received data to identify its location or can transmit data used by other devices to determine the device 118 location.

The device 118 can include a power source 638 such as batteries and/or other power subsystem (AC or DC). The power source 638 can be single-use, continuous, or rechargeable. In the case of the latter, the power source 640 can interface with an external power system or charging equipment via a power I/O component 640.

The law does not require and it is economically prohibitive to illustrate and teach every possible embodiment of the present claims. Hence, the above-described embodiments are merely exemplary illustrations of implementations set forth for a clear understanding of the principles of the disclosure. Variations, modifications, and combinations may be made to the above-described embodiments without departing from the scope of the claims. All such variations, modifications, and combinations are included herein by the scope of this disclosure and the following claims.

CLAIMS

What is claimed is:

1. A method (200) for managing voicemail messages for a visual voicemail system, comprising:

receiving a voicemail message (202) at a voicemail system (102), the voicemail message being directed to a voicemail account associated with a voicemail subscriber;

generating a notification message (204), at the voicemail system (102);

sending the notification message (208) to a mobile device (118) associated with the voicemail account that received the voicemail message;

establishing a secure data session (212) between the voicemail system (102) and the mobile device (118);

receiving, at the voicemail system (102), a first request for voicemail message header information in response to the notification message (234);

sending the requested voicemail message header information (236) to the mobile device (118) in response to the first request;

receiving, at the voicemail system (102), a second request for at least one voicemail message (238); and

sending at least a portion of the at least one voicemail message (240) to the mobile device (118) in response to the second request.

2. The method (200) of claim 1, wherein establishing the secure data session (212) between the voicemail system (102) and the mobile device (118) comprises establishing a secure sockets layer (SSL) data session.

3. The method (200) of claim 1, wherein establishing the secure data session (212) between the voicemail system (102) and the mobile device (118) comprises establishing a transport layer security (TLS) data session.

4. A method (300) for setting or changing a voicemail greeting for visual voicemail service, comprising:

establishing a secure data session (212) between a voicemail system (102) and a mobile device (118);

receiving, at the voicemail system (102), a request from the mobile device (118) to change a voicemail greeting (304), the request comprising a new voicemail greeting recorded on the mobile device (118); and

saving the new voicemail greeting (304) at the voicemail system (102).

5. The method (300) of claim 4 further comprising:

generating, at the voicemail system (118), a response indicating the success or failure of the request (306); and

sending the response (306) to the mobile device (118).

6. The method (300) of claim 4, wherein establishing the secure data session (212) between the voicemail system (102) and the mobile device (118) comprises establishing a secure sockets layer (SSL) data session.

7. The method (300) of claim 4, wherein establishing the secure data session (212) between the voicemail system (102) and the mobile device (118) comprises establishing a transport layer security (TLS) data session.

8. A method (400) for changing a password for accessing visual voicemail service, comprising:

establishing a secure data session (212) between a voicemail system (102) and a mobile device (118);

receiving, at the voicemail system (102), a request from the mobile device (118) to change a voicemail password (404), the request comprising an old password and a new password entered on the mobile device (118); and

saving (404), at the voicemail system (102), the new password, thereby replacing the old password.

9. The method (400) of claim 8 further comprising:

generating, at the voicemail system, a response indicating the success or failure of the request (406); and

sending the response (406) to the mobile device (118).

10. The method (400) of claim 8, wherein establishing the secure data session (212) between the voicemail system (102) and the mobile device (118) comprises establishing a secure sockets layer (SSL) data session.

11. The method (400) of claim 8, wherein establishing the secure data session (212) between the voicemail system (102) and the mobile device (118) comprises establishing a transport layer security (TLS) data session.

12. A method (500) for setting or changing a recorded name for a visual voicemail service, comprising:

establishing a secure data session (212) between a voicemail system (102) and a mobile device (118);

receiving, at the voicemail system (102), a request (504) from the mobile device (118) to change a recorded name, the request comprising a new recorded name recorded on the mobile device (118); and

saving, at the voicemail system (102), the new recorded name (504), thereby replacing an old recorded name.

13. The method (500) of claim 12 further comprising:

generating, at the voicemail system (102), a response (506) indicating the success or failure of the request; and

sending the response (506) to the mobile device (118).

14. The method (500) of claim 12, wherein establishing the secure data session (212) between the voicemail system (102) and the mobile device (118) comprises establishing a secure sockets layer (SSL) data session.

15. The method (500) of claim 12, wherein establishing the secure data session (212) between the voicemail system (102) and the mobile device (118) comprises establishing a transport layer security (TLS) data session.

16. A method (200) for managing voicemails from a mobile device (118), the method comprising:

receiving, at a mobile device (118), a notification message (208) identifying that at least one voicemail message has been deposited into a voicemail account associated with the mobile device (118);

establishing a secure data session (212) between the mobile device (118) and a voicemail system (102);

generating, at the mobile device (118), a first request for voicemail header information (234) from the voicemail system (102);

sending the first request (234) to the voicemail system (102);

receiving, in response to the first request, the requested voicemail message header information (236);

generating, at the mobile device (118), a second request (238) for at least one voicemail message identified in the requested voicemail message header information;

sending the second request (238) to the voicemail system (102); and

receiving, in response to the second request, at least a portion of the requested at least one voicemail message (240).

17. The method (200) of claim 16, wherein establishing the secure data session (212) between the voicemail system (102) and the mobile device (118) comprises establishing a secure sockets layer (SSL) data session.

18. The method (200) of claim 16, wherein establishing the secure data session (212) between the voicemail system (102) and the mobile device (118) comprises establishing a transport layer security (TLS) data session.

19. The method (200) of claim 16 further comprising:

saving the at least a portion of the at least one voicemail message at least temporarily in a memory (604) of the mobile device (118).

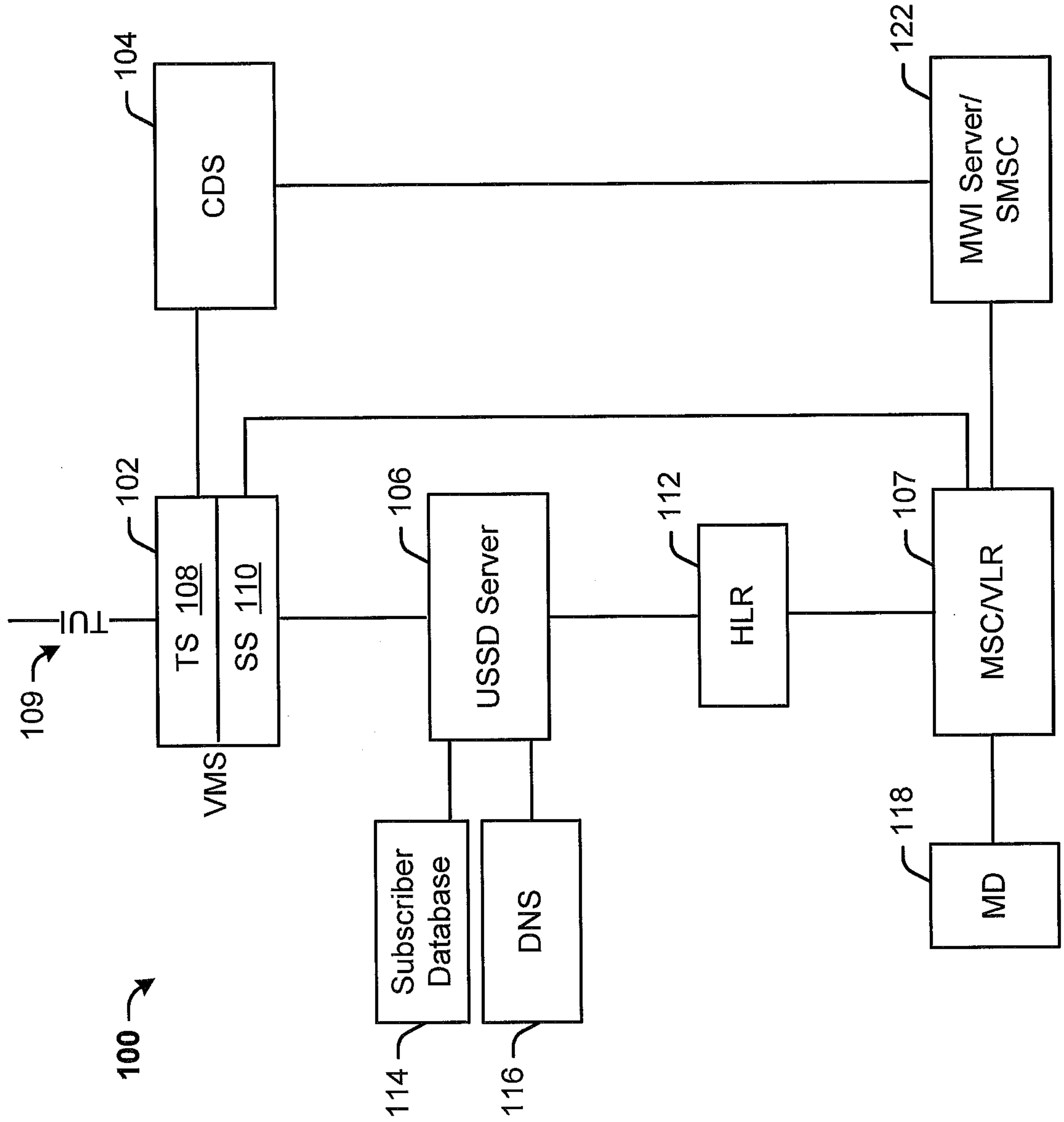
100
109
TUI
TS 108
SS 110
VMS
102
CDS
104
USSD Server
106
Subscriber Database
114
DNS
116
HLR
112
MSC/VLR
107
MD
118
MWI Server/ SMSC
122

FIG. 1

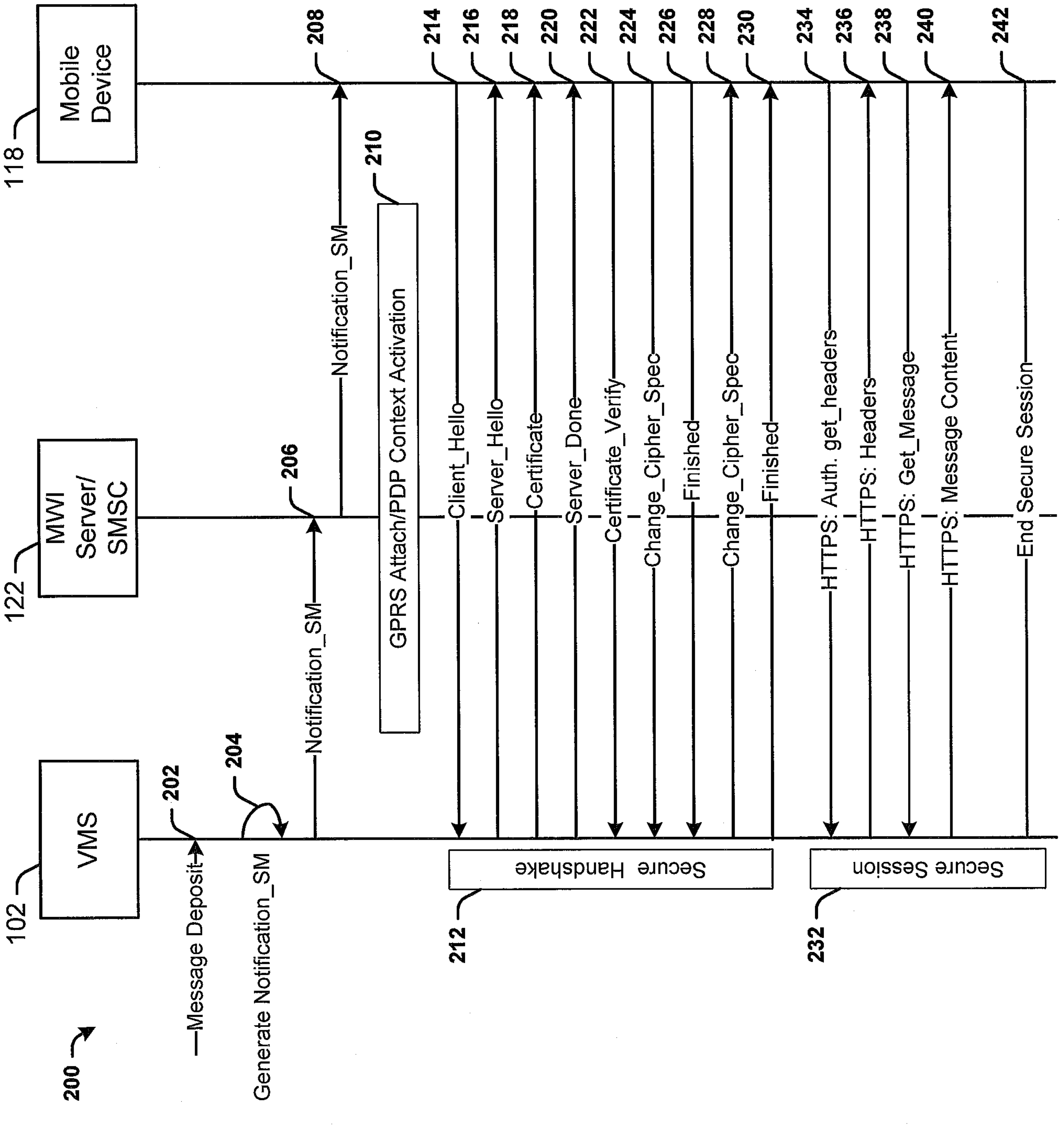
200
102
VMS
122
MWI Server/ SMSC
118
Mobile Device
Message Deposit
202
Generate Notification_SM
204
Notification_SM
206
Notification_SM
208
GPRS Attach/PDP Context Activation
210
Secure Handshake
212
Client_Hello
214
Server_Hello
216
Certificate
218
Server_Done
220
Certificate_Verify
222
Change_Cipher_Spec
224
Finished
226
Change_Cipher_Spec
228
Finished
230
Secure Session
232
HTTPS: Auth. get_headers
234
HTTPS: Headers
236
HTTPS: Get_Message
238
HTTPS: Message Content
240
End Secure Session
242

FIG. 2

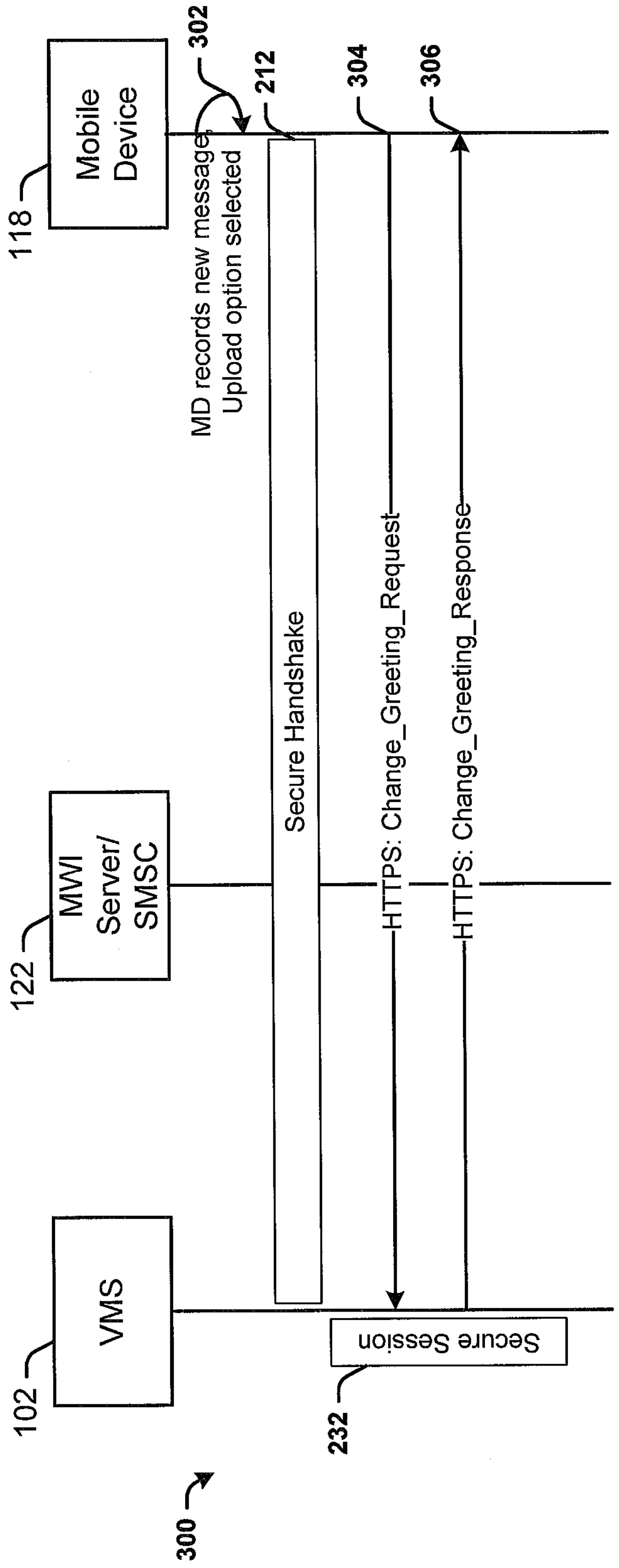
300
102
VMS
122
MWI Server/ SMSC
118
Mobile Device
302
MD records new message, Upload option selected
212
Secure Handshake
304
HTTPS: Change_Greeting_Request
306
HTTPS: Change_Greeting_Response
Secure Session
232

FIG. 3

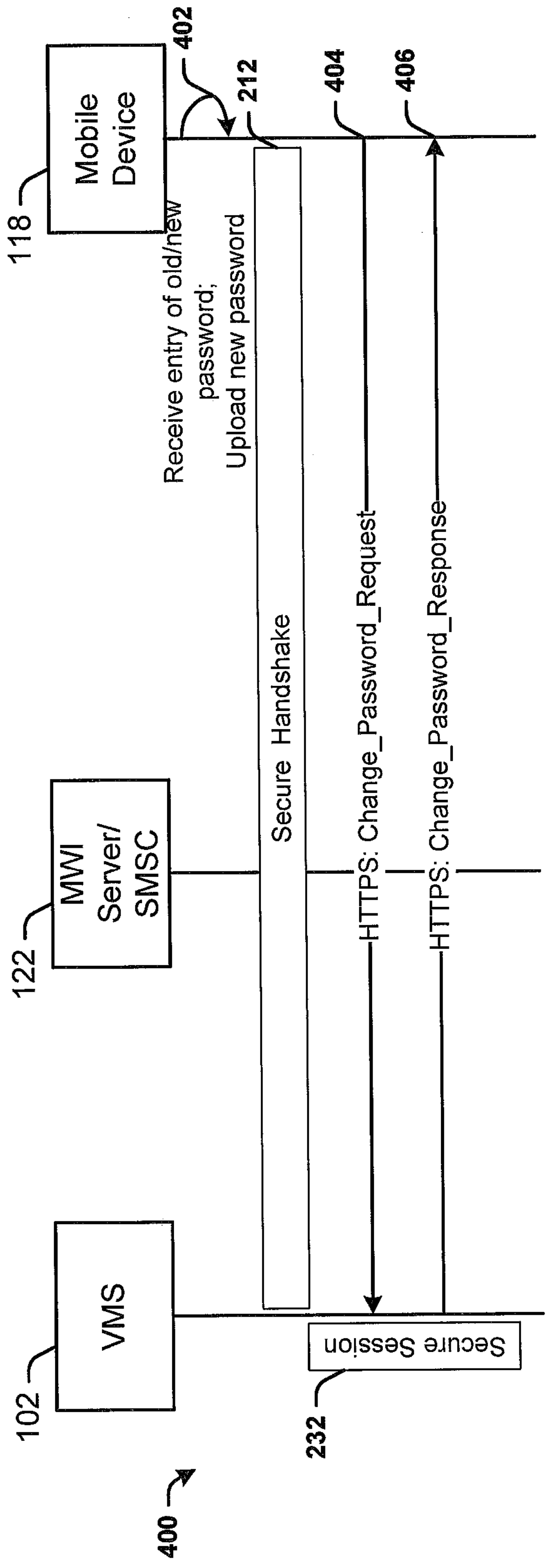
118
Mobile Device
122
MWI Server/ SMSC
102
VMS
402
Receive entry of old/new password;
Upload new password
212
Secure Handshake
404
HTTPS: Change_Password_Request
406
HTTPS: Change_Password_Response
232
Secure Session
400

FIG. 4

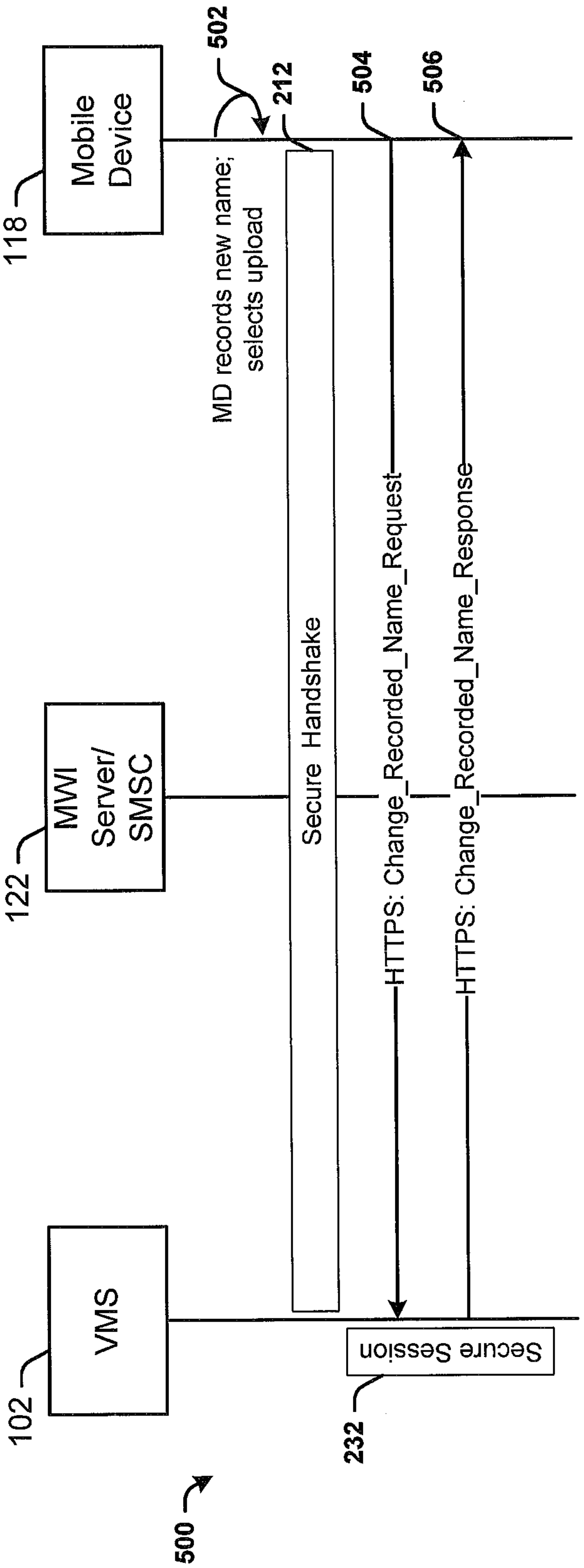
500
102
VMS
122
MWI Server/ SMSC
118
Mobile Device
502
MD records new name; selects upload
212
Secure Handshake
504
HTTPS: Change_Recorded_Name_Request
506
HTTPS: Change_Recorded_Name_Response
232
Secure Session

FIG. 5

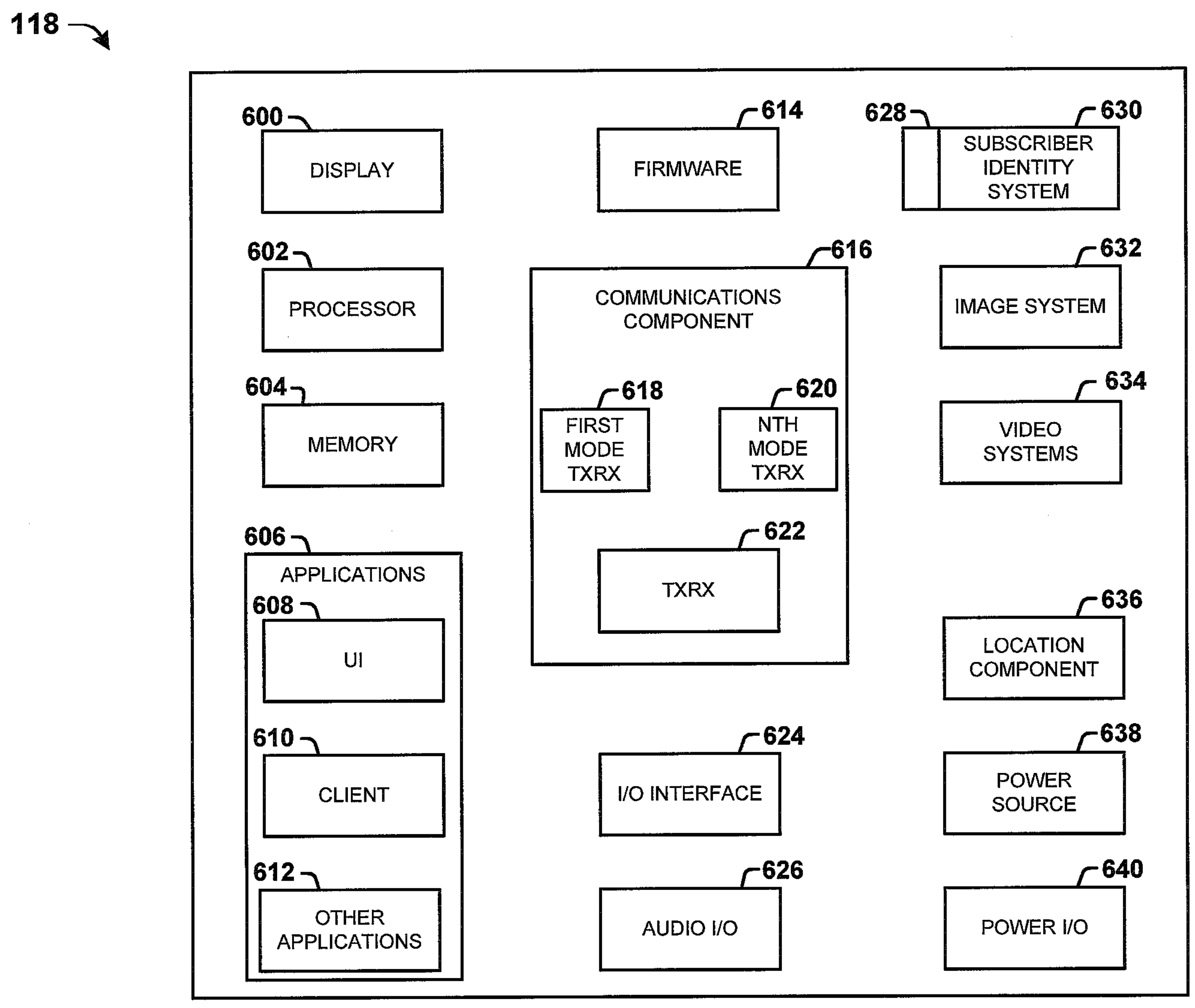
118
600
DISPLAY
602
PROCESSOR
604
MEMORY
606
APPLICATIONS
608
UI
610
CLIENT
612
OTHER APPLICATIONS
614
FIRMWARE
616
COMMUNICATIONS COMPONENT
618
FIRST MODE TXRX
620
NTH MODE TXRX
622
TXRX
624
I/O INTERFACE
626
AUDIO I/O
628
630
SUBSCRIBER IDENTITY SYSTEM
632
IMAGE SYSTEM
634
VIDEO SYSTEMS
636
LOCATION COMPONENT
638
POWER SOURCE
640
POWER I/O

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2008/065046

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04M3/533

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical,- search terms used)

EPO-Internal , WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2007/081929 A (ORATIVE CORP [US]; CHATTERJEE SAURAV [US]; DREWRY JOHN [US]; FULLARTON) 19 July 2007 (2007-07-19) abstract page 4, lines 1-27 page 7, lines 7-15 page 10, lines 3-18 -----	1-3

D Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

^{1}A" document defining the general state of the art which is not considered to be of particular relevance

^{1}E" earlier document but published on or after the international filing date

^{1}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)

^{1}O" document referring to an oral disclosure, use, exhibition or other means

^{1}P" document published prior to the international filing date but later than the priority date claimed

"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

^{1}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

^{1}Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document ls combined with one or more other such docu¬ments, such combination being obvious to a person skilled in the art.

"&^{1} document member of the same patent family

Date of the actual completion of the international search 25 August 2008	Date of mailing of the international search report 12/11/2008
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	Authorized officer Wi 11ems , Branko

INTERNATIONAL SEARCH REPORT	International application No. PCT/US2008/065046

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 allsearchable 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 reportcovers 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.:

1-3, 16-19

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 applicanf 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.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

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

1. claims: 1-3,16-19

   A method for managing voicemail messages for a visual voicemail system

   ---

2. claims: 4-7

   A method for setting or changing a voicemail greeting for visual voicemail service

   ---

3. claims: 8-11

   A method for changing a password for accessing visual voicemail service

   ---

4. claims: 12-15

   A method for setting or changing a recorded name for a visual voicemail service

   ---

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2008/065046

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2007081929 A	19-07-2007	EP 1987659 A2	05-11-2008