US 20160330599A9

(19) **United States**

(12) **Patent Application Publication**

Sigmund et al.

(10) **Pub. No.: US 2016/0330599 A9**

(48) **Pub. Date: Nov. 10, 2016**

CORRECTED PUBLICATION

(54) **SECURE VISUAL VOICEMAIL**

(71) Applicant: **AT&T Mobility II LLC**, Atlanta, GA (US)

(72) Inventors: **William Joseph Sigmund**, Cumming, GA (US); **Michael Robert Zubas**, Marietta, GA (US); **Brian Keith Rainer**, Lawrenceville, GA (US)

(73) Assignee: **AT&T MOBILITY II LLC**, Atlanta, GA (US)

(21) Appl. No.: **14/450,971**

(22) Filed: **Aug. 4, 2014**

Prior Publication Data

(15) Correction of US 2014/0342702 A1 Nov. 20, 2014
See (63) and (60) Related U.S. Application Data.

(65) US 2014/0342702 A1 Nov. 20, 2014

Related U.S. Application Data

(63) Continuation of application No. 12/160,946, filed on Jul. 15, 2008, now Pat. No. 8,798,241, filed as application No. PCT/US2008/065046 on May 29, 2008.

(60) Provisional application No. 60/969,419, filed on Aug. 31, 2007.

Publication Classification

(51) **Int. Cl.**

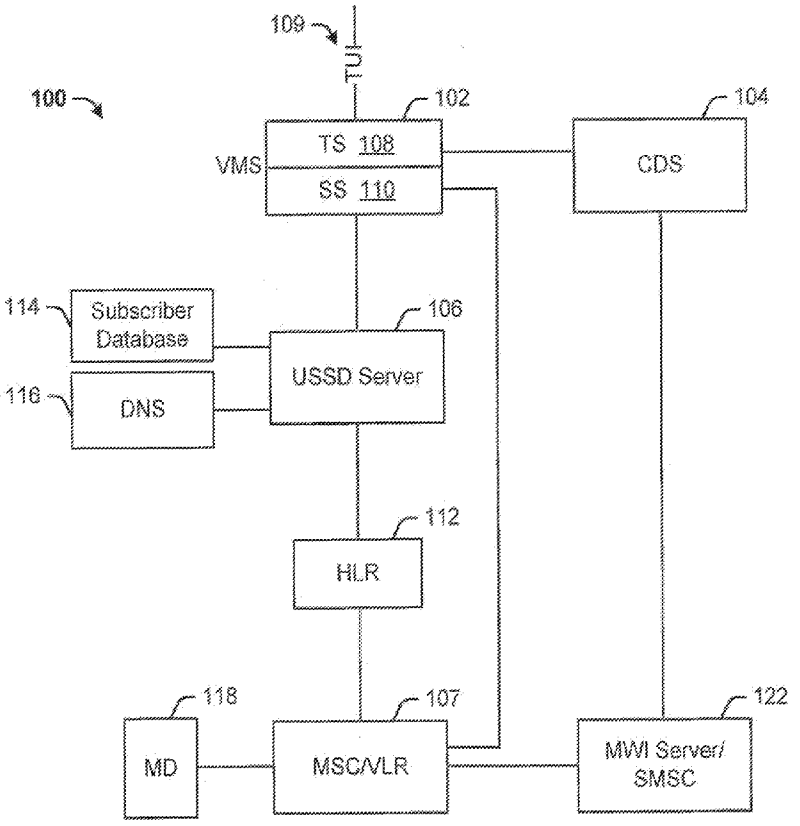
H04W 4/16	(2006.01)
H04W 12/06	(2006.01)
H04M 3/533	(2006.01)

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

CPC ***H04W 4/16*** (2013.01); ***H04M 3/53383*** (2013.01); ***H04M 3/533*** (2013.01); ***H04W 12/06*** (2013.01)

(57) **ABSTRACT**

A method for managing voicemail messages for a visual voicemail system can include establishing a secure data session between a voicemail system and a mobile device. The voicemail system can receive a voicemail message that is directed to a voicemail account associated with a voicemail subscriber. The voicemail system can generate a notification message and can send the notification message to the mobile device that is associated with the voicemail account that received the voicemail message. In response to the notification message, the mobile device can generate and send a first request for voicemail message header information. The voicemail system can send the requested voicemail message header information to the mobile device and, in response, receive a second request for at least one voicemail message. The voicemail message can send at least a portion of the at least one voicemail message to the mobile device.



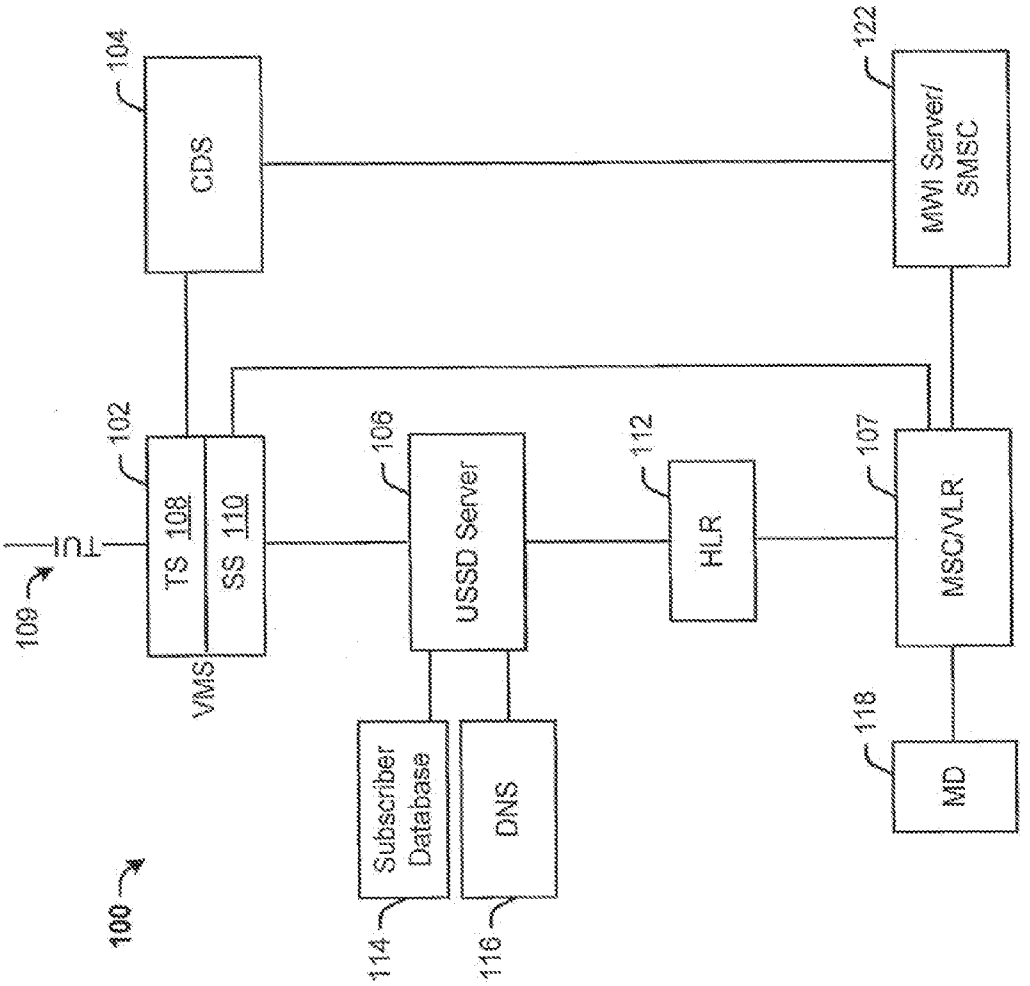

104
CDS
122
MWI Server/ SMSC
102
TS 108
SS 110
VMS
109
106
USSD Server
112
HLR
107
MSC/VLR
118
MD
Subscriber Database
114
DNS
116
100

FIG. 1

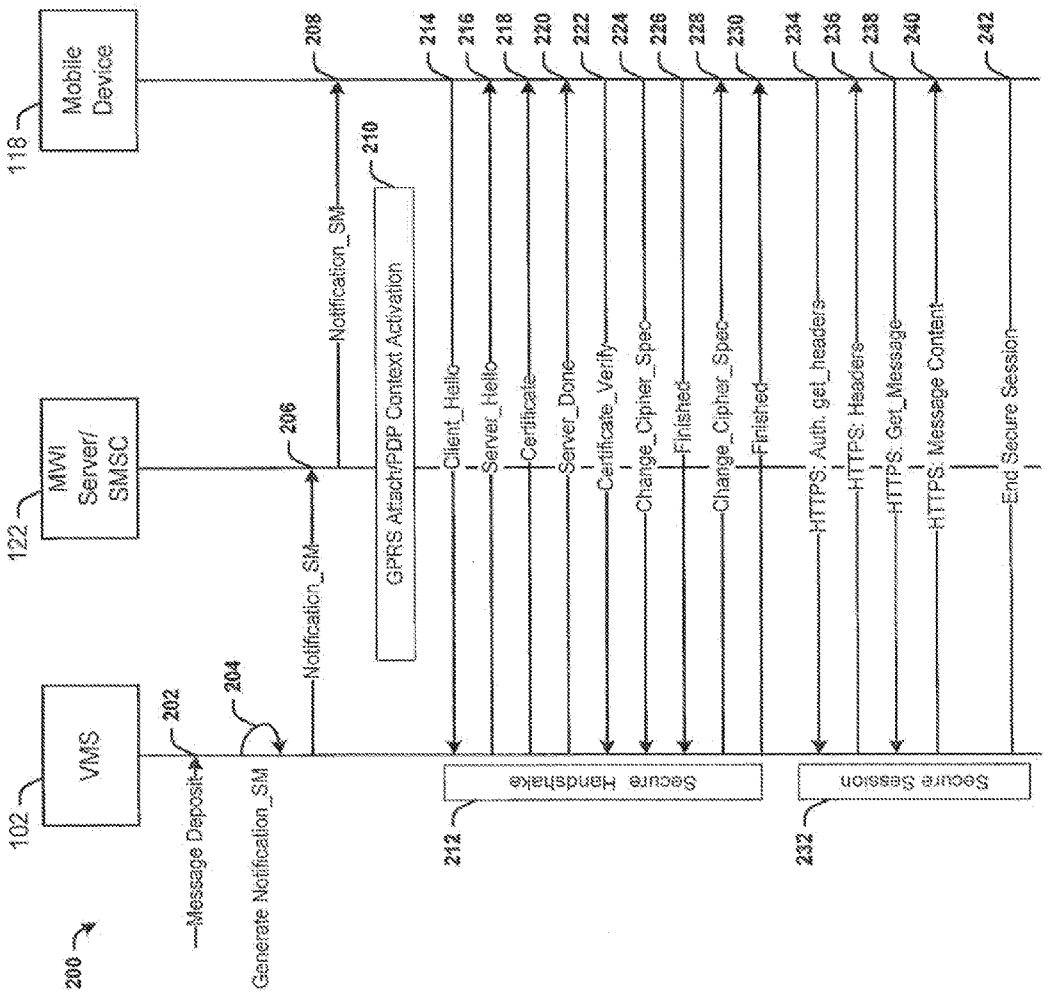

200
102
VMS
122
MWI Server/ SMSC
118
Mobile Device
202
Message Deposit
204
Generate Notification_SM
Notification_SM
206
Notification_SM
208
GPRS Attach/PDP Context Activation
210
Client_Hello
214
Server_Hello
216
Certificate
218
Server_Done
220
Certificate_Verify
222
Change_Cipher_Spec
224
Finished
226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

FIG. 2

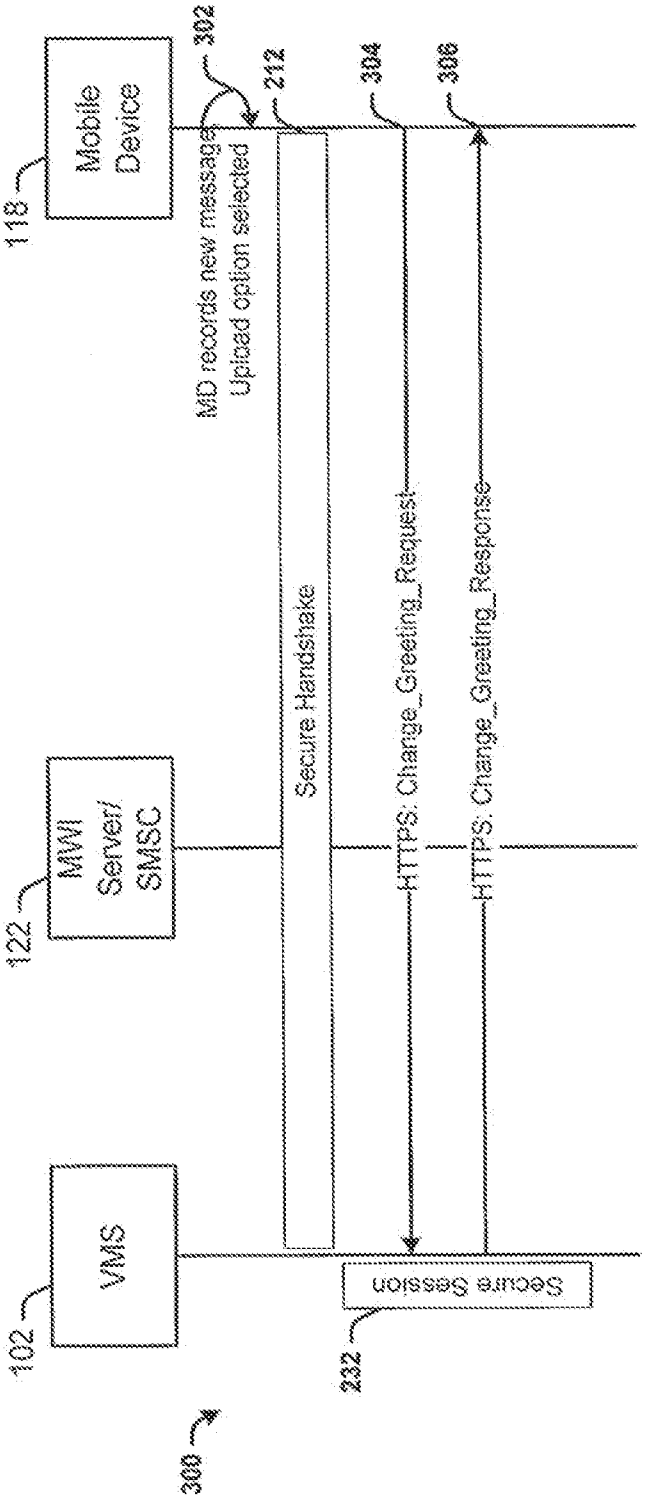

Mobile Device
118
302
212
304
306
MD records new message Upload option selected
Secure Handshake
HTTPS: Change_Greeting_Request
HTTPS: Change_Greeting_Response
MWI Server/ SMSC
122
VMS
102
Secure Session
232
300

FIG. 3

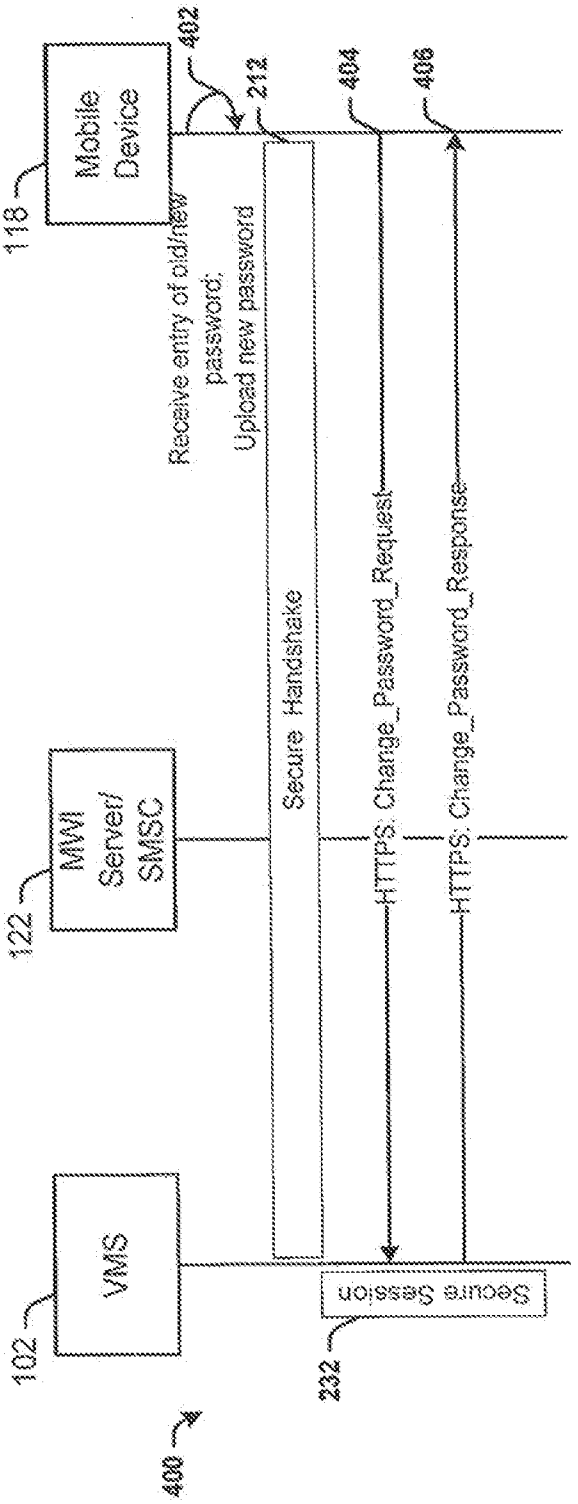

Mobile Device
118
MWI Server/ SMSC
122
VMS
102
400
402
212
404
406
232
Receive entry of old/new password; Upload new password
Secure Handshake
HTTPS: Change_Password_Request
HTTPS: Change_Password_Response
Secure Session

FIG. 4

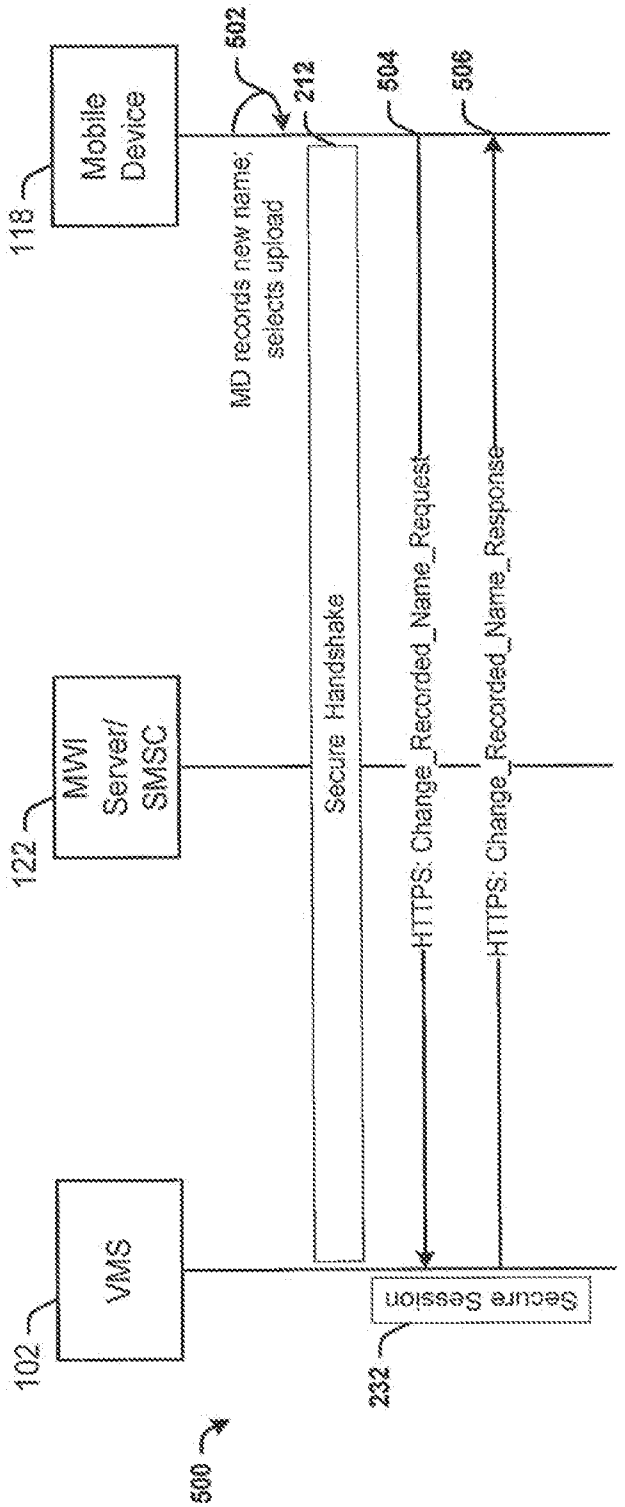

Mobile Device
118
MWI Server/ SMSC
122
VMS
102
500
502
212
504
506
MD records new name; selects upload
Secure Handshake
HTTPS: Change_Recorded_Name_Request
HTTPS: Change_Recorded_Name_Response
Secure Session
232

FIG. 5

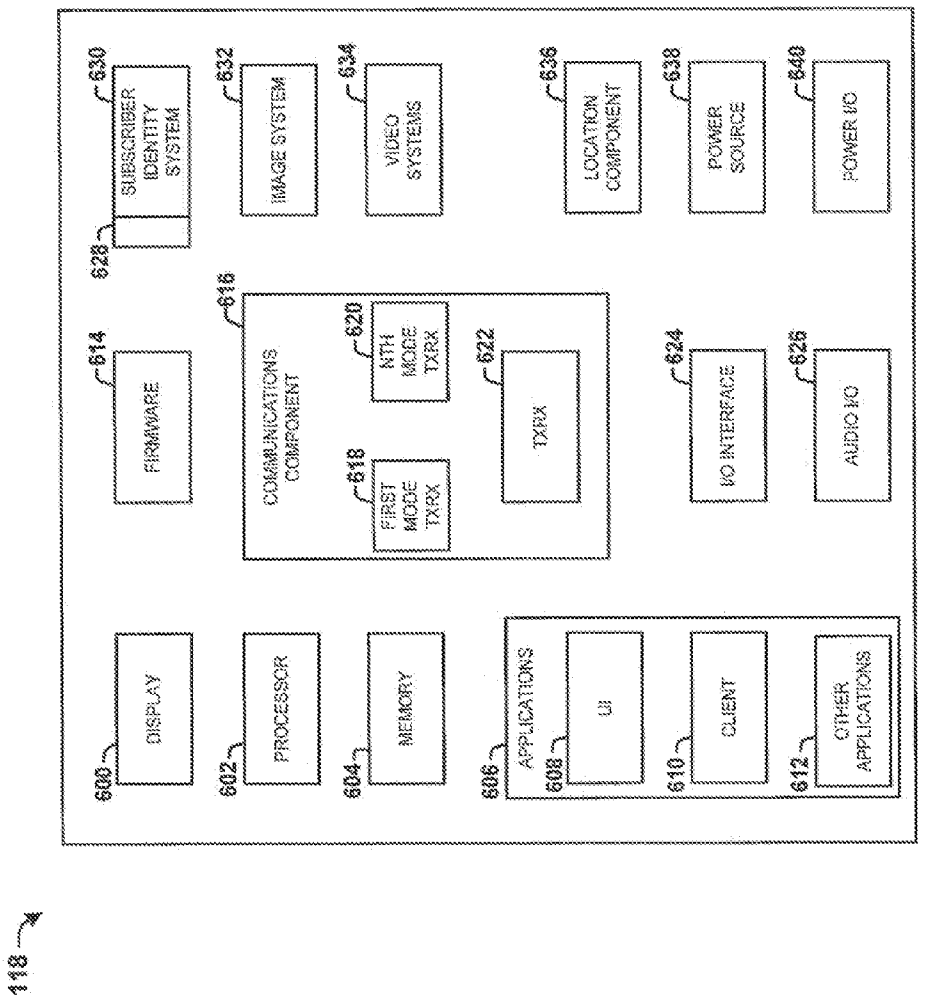

118
600
DISPLAY
602
PROCESSOR
604
MEMORY
606
APPLICATIONS
608
UI
610
CLIENT
612
OTHER APPLICATIONS
614
FIRMWARE
616
COMMUNICATIONS COMPONENT
618
FIRST MODE TXRX
620
NTH MODE TXRX
622
TXRX
624
I/O INTERFACE
626
AUDIO I/O
628
630
SUBSCRIBER IDENTITY SYSTEM
632
IMAGE SYSTEM
634
VIDEO SYSTEMS
636
LOCATION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

FIG. 6

SECURE VISUAL VOICEMAIL

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. patent application Ser. No. 12/160,946, filed Jul. 15, 2008, which is a 371 of International Patent Application No. 2008/065046, filed May 29, 2008, which claims priority to U.S. Provisional Patent Application No. 60/969,419, filed Aug. 31, 2007, the entirety of which are hereby incorporated by reference.

TECHNICAL FIELD

[0002] The present disclosure relates generally to voicemail service and, more particularly, to a secure visual voicemail service.

BACKGROUND

[0003] 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.

[0004] 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.

[0005] 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.

[0006] 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 (VVM) services.

SUMMARY

[0007] 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.

[0008] 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.

[0009] 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.

[0010] 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.

[0011] 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

[0012] FIG. **1** illustrates a portion of an exemplary network in which aspects of the present disclosure can be practiced.

[0013] 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.

[0014] 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.

[0015] 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.

[0016] 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.

[0017] FIG. **6** schematically illustrates an exemplary mobile device and components thereof for use in accordance with an embodiment of the present disclosure.

DETAILED DESCRIPTION

[0018] 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.

[0019] 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.

[0020] 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.

[0021] 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.

[0022] 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 subscrib-

ers. 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.

[0023] 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 deliver SMS messages and message waiting indicator (MWI) messages.

[0024] 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**.

[0025] 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.

[0026] The VMS **102** is accessible via traditional or plain old voicemail (POVM) methods and visual voicemail (VVM) methods described herein. State changes to voicemail messages, whether requested through the TUI **109** via POVM methods or directly on the MD **118** via VVM 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.

[0027] 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 VVM 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.

[0028] Messages used to establish and/or update a VVM 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.

[0029] A first boot process can enable a subscriber to receive confirmation that VVM service is enabled and is immediately accessible via a VVM 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.

[0030] The VVM 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**.

[0031] 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.

[0032] 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.

[0033] 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**.

[0034] 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.

[0035] 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 client_hello 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.

[0036] 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 server_hello 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.

[0037] 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.

[0038] 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.

[0039] 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.

[0040] 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.

[0041] 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.

[0042] 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 get_message 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**.

[0043] 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 VVM 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.

[0044] 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.

[0045] 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.

[0046] 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**.

[0047] Requests to the VMS **102** can be pipelined in accordance with HTTP 1.1 specifications. This can help reduce network latency for multiple requests.

[0048] 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.

[0049] 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.

[0050] 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 VVM 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.

[0051] 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 VVM 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.

[0052] 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.

[0053] 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.

[0054] 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 VVM 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 VVM 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 VVM 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.

[0055] 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.

[0056] At step **402**, the subscriber can enter the old password and new password on the MD **118**. After the passwords have been entered, the VVM 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 VVM application can be configured to receive an error code and provide corrective action to the subscriber to resolve the password issue. For example, the VVM 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.

[0057] 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.

[0058] 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.

[0059] 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 VVM 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 (FLAC), Apple® lossless encoder (ALE), i.e., Apple® lossless audio codec (ALAC), and other open and proprietary audio formats.

[0060] 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.

[0061] After a new name has been recorded, the VVM application can generate a change_recorded_name_request 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**.

[0062] The VVM 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 VVM application can be further configured to retrieve the current voicemail greeting and recorded name using a HTTP request.

[0063] 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.

[0064] 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.

[0065] 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.

[0066] 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).

[0067] 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**.

[0068] The memory **604** can be configured to store one or more applications **606**. The applications **606** can include a user interface (UI) 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**.

[0069] 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.

[0070] 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.

[0071] 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., RJ11, 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.

[0072] 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.

[0073] 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**.

[0074] 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.

[0075] 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.

[0076] 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 **638** can interface with an external power system or charging equipment via a power I/O component **640**.

[0077] 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.

What is claimed is:

1. A method comprising:

completing, by a visual voicemail system, establishment of a secure data session with a mobile device, wherein establishment of the secure data session is initiated by the mobile device;

receiving, by the visual voicemail system, during the secure data session, a request from the mobile device to change visual voicemail account information associated with the mobile device; and

attempting, by the visual voicemail system, to change the visual voicemail account information associated with the mobile device in accordance with the request.

2. The method of claim **1**, wherein the secure data session established between the visual voicemail system and the mobile device comprises a secure sockets layer data session.

3. The method of claim **1**, wherein the secure data session established between the visual voicemail system and the mobile device comprises a transport layer security data session.

4. The method of claim **1** further comprising:

generating, by the visual voicemail system, a response to the request, the response indicating a success or failure of an attempt by the visual voicemail system to change the visual voicemail account information associated with the mobile device in accordance with the request; and

sending the response to the mobile device during the secure data session.

5. The method of claim **1**, wherein the request comprises a change voicemail greeting request, and wherein the visual voicemail account information comprises a voicemail greeting spoken by a user of the mobile device and recorded by the mobile device.

6. The method of claim **1**, wherein the request comprises a change voicemail password request, and wherein the visual voicemail account information comprises a voicemail password entered by a user of the mobile device and recorded by the mobile device.

7. The method of claim **1**, wherein the request comprises a change recorded name request, and wherein the visual voicemail account information comprises a voicemail recorded name spoken by a user of the mobile device and recorded by the mobile device.

8. A visual voicemail system comprising:

a processor; and

a memory comprising computer-executable instructions that, when executed by the processor, cause the processor to perform operations comprising

completing establishment of a secure data session with a mobile device, wherein establishment of the secure data session is initiated by the mobile device,

receiving, during the secure data session, a request from the mobile device to change visual voicemail account information associated with the mobile device, and

attempting to change the visual voicemail account information associated with the mobile device in accordance with the request.

9. The visual voicemail system of claim **8**, wherein the secure data session established between the visual voicemail system and the mobile device comprises a secure sockets layer data session.

10. The visual voicemail system of claim **8**, wherein the secure data session established between the visual voicemail system and the mobile device comprises a transport layer security data session.

11. The visual voicemail system of claim **8**, wherein the operations further comprise:

generating a response to the request, the response indicating a success or failure of an attempt by the visual voicemail system to change the visual voicemail account information associated with the mobile device in accordance with the request; and

sending the response to the mobile device during the secure data session.

12. The visual voicemail system of claim **8**, wherein the request comprises a change voicemail greeting request, and wherein the visual voicemail account information comprises a voicemail greeting spoken by a user of the mobile device and recorded by the mobile device.

13. The visual voicemail system of claim **8**, wherein the request comprises a change voicemail password request, and wherein the visual voicemail account information comprises a voicemail password entered by a user of the mobile device and recorded by the mobile device.

14. The visual voicemail system of claim **8**, wherein the request comprises a change recorded name request, and wherein the visual voicemail account information comprises a voicemail recorded name spoken by a user of the mobile device and recorded by the mobile device.

15. A mobile device comprising:

a processor; and

a memory comprising computer-executable instructions that, when executed by the processor, cause the processor to perform operations comprising

initiating establishment of a secure data session with a visual voicemail system,

generating a request to change visual voicemail account information associated with the mobile device, and

providing, during the secure data session, the request to the visual voicemail system so that the visual voicemail system can attempt to change the visual voicemail.

16. The mobile device of claim **15**, wherein the secure data session comprises a secure sockets layer data session.

17. The mobile device of claim **15**, wherein the secure data session comprises a transport layer security data session.

18. The mobile device of claim **15**, wherein the request comprises a change voicemail greeting request, and wherein the visual voicemail account information comprises a voicemail greeting spoken by a user of the mobile device and recorded by the mobile device.

19. The mobile device of claim **15**, wherein the request comprises a change voicemail password request, and

wherein the visual voicemail account information comprises a voicemail password entered by a user of the mobile device and recorded by the mobile device.

20. The mobile device of claim **15**, wherein the request comprises a change recorded name request, and wherein the visual voicemail account information comprises a voicemail recorded name spoken by a user of the mobile device and recorded by the mobile device.

* * * * *