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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 October 2010 (28.10.2010)

PCT

(10) International Publication Number
WO 2010/124299 A2

(51) International Patent Classification:
H04W 4/22 (2009.01) *H04W 24/02* (2009.01)
H04W 4/20 (2009.01)

(21) International Application Number:
PCT/US2010/032460

(22) International Filing Date:
26 April 2010 (26.04.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/172,684 24 April 2009 (24.04.2009) US
61/224,403 9 July 2009 (09.07.2009) US

(71) Applicant *(for all designated States except US)*: **T-MOBILE USA, INC.** [US/US]; 12920 SE 38th Street, Bellevue, WA 98006-1350 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **DUNN, Timothy, N.** [US/US]; 12920 SE 38th Street, Bellevue, WA 98006-1350 (US). **SILIS, Arturo** [CA/US]; 12920 SE 38th Street, Bellevue, WA 98006-1350 (US). **FARRELL, Declan** [GB/US]; 12920 SE 38th Street, Bellevue, WA 98006-1350 (US). **KUMAR, Jyot** [US/US]; 12920 SE 38th Street, Bellevue, WA 98006-1350 (US). **CHAPMAN, Simon** [GB/US]; 12920 SE 38th Street, Bellevue, WA 98006-1350 (US).

(74) Agents: **BISHOP, Stephen** et al.; Perkins Coie LLP, P.O. Box 1247, Seattle, WA 98111-1247 (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, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) **Title**: MONITORING APPLICATION AND METHOD FOR ESTABLISHING EMERGENCY COMMUNICATION SESSIONS WITH DESABLED DEVICES BASED ON TRANSMITTED MESSAGES

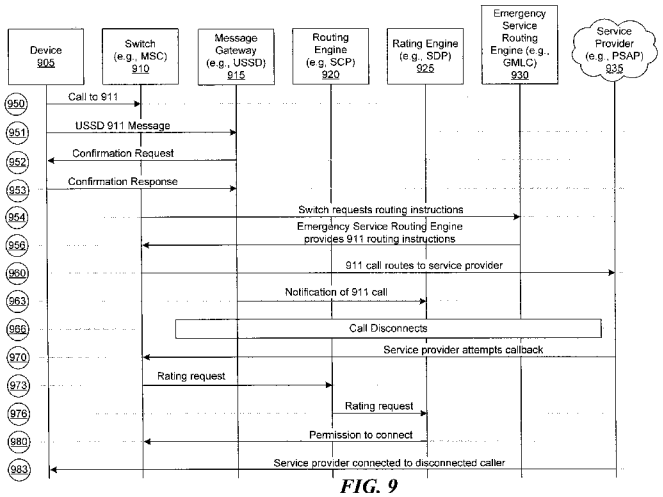

FIG. 9

(57) **Abstract**: A monitoring application and method in a disabled telecommunication device for monitoring communication sessions initiated by the device and detecting an emergency communication session that is initiated by the device. If an emergency communication session is detected, the monitoring application generates and transmits a message to a rating engine over a non-voice channel. The non-voice channel may be an unstructured supplementary service data (USSD) channel, a short message service (SMS) channel, or other like messaging channel. When the message is received via the non-voice channel, various callback techniques may be implemented to allow the disabled device to receive communications after the emergency communication session, even though such communications would normally be prevented as a result of a service lock.

WO 2010/124299 A2

MONITORING APPLICATION AND METHOD FOR ESTABLISHING EMERGENCY COMMUNICATION SESSIONS WITH DISABLED DEVICES BASED ON TRANSMITTED MESSAGES

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 61/224,403, entitled "MONITORING APPLICATION FOR TRANSMITTING MESSAGES REFLECTING ESTABLISHMENT OF EMERGENCY COMMUNICATION SESSIONS ON DISABLED DEVICES," filed July 9, 2009, and U.S. Provisional Application No. 61/172,684, entitled "MONITORING APPLICATION FOR TRANSMITTING MESSAGES REFLECTING ESTABLISHMENT OF EMERGENCY COMMUNICATION SESSIONS ON DISABLED DEVICES," filed April 24, 2009. This application is related to U.S. Patent Application No. 12/265,707, entitled "METHOD AND SYSTEM FOR ALLOWING INCOMING EMERGENCY COMMUNICATIONS ON A DISABLED DEVICE," filed November 5, 2008, which claims priority to U.S. Provisional Application No. 60/985,633, entitled "METHOD AND SYSTEM FOR ALLOWING INCOMING EMERGENCY COMMUNICATIONS ON A DISABLED DEVICE," filed November 5, 2007.

BACKGROUND

[0002] Telephone service providers offer their customers a variety of service plans. A customer may select a plan that is billed at a flat rate every month with additional charges added on the following month for services the customer uses beyond their standard plan (e.g. text messages, used minutes beyond the allocated amount in the plan, downloads, or any number of other extra cost services). In these example payment plans, service may be discontinued for a variety of reasons such as a failure to pay the bill, violating the terms of service (TOS), and/or a report that the phone has been lost or stolen. Additionally, some telephone service providers offer pre-paid phone plans as an alternative to the monthly billed (or other) plan. In a pre-paid plan, a customer may purchase a certain number of minutes, or units of time, before using

those minutes. The network may keep track of minute-, or unit-, usage at a real-time rate, and prompt the customer to purchase more minutes, or units, when the customer has run out or is near running out of usable calling minutes, or units. For example, a unit of time may correspond to a specific amount of minutes depending upon the intended calling location (e.g., more units are required for international telephone calls as compared to the units required for a domestic call for a same amount of minutes). Service may be discontinued when the customer has exhausted all of the pre-paid minutes or units of time, or, for example, service to specific locations may be unavailable due to insufficient or a low number of pre-paid minutes or units.

[0003] Even though a service provider may disable general service to a telecommunications device (e.g., wired phone, cordless phone, mobile telephone, personal digital assistant, smart phone, laptop computer, etc.), the service provider may still allow a user of the disabled device to place an emergency call to pre-approved telephone numbers or URIs (Uniform Resource Identifiers). For example, the service provider may allow an emergency call to be made to emergency services (e.g., 911), to the service provider's customer service number, or to other localized numbers or URIs. An allowed call to emergency services may connect the device to a Public Safety Answering Point (PSAP). The service provider knows which PSAP to route a call to when a user dials for emergency assistance. In a given situation, a caller of 911 or other emergency hotline is routed to a specific emergency call center, commonly referred to as a primary PSAP. The primary PSAP acts to obtain and verify the whereabouts of the caller, determine the nature of the emergency, notify an appropriate response team(s), and/or contact a secondary or other PSAP. In some situations, the primary PSAP may not be responsible for directly dispatching an appropriate response team, and will need to identify and/or contact/conference in a secondary PSAP, e.g., a police dispatcher or a fire team dispatcher.

[0004] In some circumstances, a PSAP may need to call back the disabled device that placed the emergency services call. For example, a call between the parties may have been terminated before all desired information had been exchanged. Currently, however, a PSAP is not able to place a call to a disabled device. The inability of the

PSAP to contact a disabled device is a significant shortcoming that can impact the ability to offer emergency services in a timely fashion to the device user.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Figure 1 is a signaling diagram that depicts allowing callbacks to a disabled device based on an elapsed time.

[0006] Figure 2 is a flowchart illustrating allowing callbacks from a service provider based on a stored list of service provider numbers.

[0007] Figure 3 is a signaling diagram that depicts allowing callbacks to a disabled device based on an associated routing key.

[0008] Figures 4 and 5 are signaling diagrams that depicts allowing callbacks to a disabled device based on an issued passcode.

[0009] Figure 6 is a flowchart illustrating allowing callbacks from a service provider that occur within a threshold time after an emergency call.

[0010] Figure 7 is a flowchart illustrating allowing callbacks from a service provider based on an issued passcode.

[0011] Figure 8 is a flowchart of a monitoring application that generates a message indicating that an emergency communication session is being or has been established by a disabled device.

[0012] Figure 9 is a signaling diagram that depicts receipt of a message indicating that an emergency communication session is being or has been established by a disabled device in order to allow callbacks to the disabled device.

DETAILED DESCRIPTION

[0013] A system and method to allow a disabled device to receive an incoming communication after the termination of an emergency communication session with a service provider is disclosed. A "device" is any telecommunications device (e.g., a wired, wireless, or cordless phone; VoIP device; Unlicensed Mobile Access (UMA) or UMA-enabled device; portable or handheld computer; smartphone; media player; or the like) having a service plan with a telecommunications service provider that allows the

device to communicate with others via voice, video, text, etc. A "disabled" device is a device having the portion of its service plan that allows the device to send or receive communications either temporarily or permanently disabled. For example, a device user may have exhausted a usage allowance (e.g., used all of his/her prepaid minutes) or may have had access suspended by an authorized user (e.g., by a parent or guardian that allocates minutes in a shared family plan), thereby resulting in a "service lock" for the device. Various methods are disclosed herein to allow a disabled device to receive communications after an emergency communication session, even though such communications would normally be prevented as a result of the service lock.

[0014] In some embodiments, the system activates a timer or other time-measurement technique upon detecting that a device user initiated an emergency communication session (e.g., a voice, video, multimedia, Short Message Service (SMS), and/or Instant Messaging (IM) session), such as by dialing 911. The timer may be activated for a defined period of time (e.g., 10 minutes, 5 minutes, etc.). The system allows the device to receive all incoming communications (e.g., any incoming voice, video, multimedia, Short Message Service (SMS), and/or Instant Messaging (IM) session) during the defined period of time. For example, all incoming calls during the defined time period may be rated as free and/or the service lock may be overridden. Alternatively, in some embodiments, the timer may be activated in response to the emergency communication session having been disconnected or dropped.

[0015] In some embodiments, the system may maintain a repository of emergency telephone numbers or URIs (Uniform Resource Identifiers), and all incoming communications from numbers or URIs contained in the repository that occur after a device user has initiated an emergency communication session may be allowed. The repository of telephone numbers or URIs may include all known service providers such as Public Safety Answering Points (PSAPs), telecommunications service providers' customer service numbers, or other desired telephone numbers or URIs. The incoming communication may be allowed by the system by rating the communication as free and/or overriding the service lock.

[0016] In some embodiments, in response to a device user's request to initiate an emergency communication with a service provider (e.g., by dialing 911), the

communication request may be routed to the service provider and a routing key or passcode may additionally be forwarded to the service provider (e.g., to a PSAP, a PSAP operator, a system repository which may be accessible by a PSAP, and/or the specific PSAP to whom the call was routed). Subsequently, the system prompts anyone seeking to contact the disabled device for the routing key or passcode. The system allows communication with the disabled device if the routing key or passcode entered by the caller matches the routing key or passcode initially generated by the system. The routing key or passcode may be kept secret from the service provider operator or made available to the service provider operator. The system may allow the communication by, for example, rating the communication as free and/or overriding the service lock.

[0017] The emergency communication session established with a device may be, for example, a voice, video, multimedia, text, Short Message Service (SMS), and/or IM session. For purposes of clarity, the discussion herein often focuses on establishing a 911 call with a PSAP. The disclosed technology is not limited to use for 911 calls to PSAPs, however, and may be applied to any communication session with one or more service providers.

[0018] In some embodiments, in order to detect that an emergency session has been initiated by a disabled device, the disabled device contains an application that monitors communication sessions initiated by the device to detect an emergency communication session. If an emergency communication session is detected, the monitoring application generates and transmits a message to the system over a non-voice channel. The non-voice channel may be an unstructured supplementary service data (USSD) channel, a short message service (SMS) channel, or other like messaging channel. When the system receives a message via the non-voice channel, the system may implement the techniques described herein to allow the disabled device to receive communications after the emergency communication session, even though such communications would normally be prevented as a result of a service lock.

[0019] Various embodiments of the invention will now be described. The following description provides specific details for a thorough understanding and an enabling description of these embodiments. One skilled in the art will understand, however, that

the invention may be practiced without many of these details. Additionally, some well-known structures or functions may not be shown or described in detail, so as to avoid unnecessarily obscuring the relevant description of the various embodiments. The terminology used in the description presented below is intended to be interpreted in its broadest reasonable manner, even though it is being used in conjunction with a detailed description of certain specific embodiments of the invention.

[0020] As previously described, a device may be placed in a temporary or permanent disabled state for a variety of reasons, such as the exhaustion of a prepaid service plan that covers the device or because a user managing service to the device has elected to restrict access to a service. Even though a device may be in a disabled state, many telecommunications service providers will allow an outgoing emergency communication to be placed from the device, because the service provider is able to identify commonly assigned emergency numbers (such as the sequence 9-1-1) that reflect a user's need to place an emergency communication. Under such circumstances, even if the device is disabled the service provider may allow the communication to proceed. In contrast, it was previously not possible for a PSAP to initiate or otherwise reestablish a communication session with a disabled device, such as may be required if a communication session with the device is terminated. Accordingly, there exists a need to allow PSAPs or other emergency service providers to establish communication with a disabled device.

[0021] Figure 1 is a signaling diagram illustrating a series of messages that are sent between a disabled device 105, a switch (e.g., a Mobile Switching Center or MSC) 110, a routing engine (e.g., an SCP) 115, a rating engine (e.g., an SDP) 120, an emergency service routing engine (e.g., a GMLC) 125 and a service provider 130, in order to establish an emergency communication between the disabled device 105 and the service provider 130, and to reestablish the communication between the same or different service provider and the disabled device 105 if the emergency communication between the disabled device and the service provider is interrupted or otherwise terminated. The service provider 130 may be a Public Safety Answering Point (PSAP), such as a 911 call center, a customer service center, or any other service provider or third party service (e.g., police, fire) that may need to communicate with a device user

during an emergency situation. The device 105 may, for example, be a wired, wireless, or cordless phone, VoIP phone, Unlicensed Mobile Access or UMA enabled device, portable computer, handheld computer, smartphone, media player, or the like. The device 105 has been disabled such that it is not authorized to initiate and/or receive communications with other devices, other than to establish communication with certain service providers.

[0022] A variety of circumstances may cause a device to be placed in a disabled state where it is prevented from initiating or receiving communication (e.g., from placing or receiving calls). The device 105 may, for example, be a real-time rated device that operates on a real-time rated plan (e.g. a pre-paid plan or family allowance plan). In the example of a pre-paid plan, the device user may have purchased a quantity of minutes or units and used up those minutes or units. Until the user purchases more minutes or units, the device may be disabled except for establishing communication with certain service providers. As another example, the real-time rated plan may be a family allowance plan (e.g., such as the Family Allowances^{SM} plan by T-Mobile). In a family allowance plan, an account supervisor (e.g., a parent or guardian) may purchase an allotment of minutes and/or usage units (e.g., downloads, SMSs, etc.) each time period to be shared among various devices participating in the supervisor's family allowance plan. The supervisor allocates a defined amount of usage (e.g., minutes, text messages, multimedia downloads) to a device. Upon reaching the allocated amount of usage, the device is disabled. Alternatively and/or additionally, the supervisor may selectively limit use of the device by causing the device to be automatically disabled at various times of the day and/or particular days of the week and/or defined locations (e.g., near a school). Further details of a family allowance plan may be found in U.S. Application Serial No. 12/246,439, filed October 6, 2008 and entitled "SYSTEM THAT ENABLES A USER TO ADJUST TELECOMMUNICATIONS RESOURCES ALLOCATED TO A GROUP," which is hereby incorporated by this reference in its entirety. While the device is disabled, it may still be operable to initiate communication with pre-approved numbers. Such pre-approved numbers may be numbers selected and/or approved by the account supervisor, and typically, for example, include 9-1-1.

[0023] Various network elements enable communication between the device and the service provider as described herein. The switch 110 is a Mobile Switching Center (MSC) or any other component or platform that is operable to detect an emergency communication request initiated by the device or by the service provider. The routing engine 115 is, for example, an SCP (Service Control Point) or similar component or platform used to control service to the device. The SCP is a standard component of an Intelligent Network (IN) telephone system, which is used to control real-time rated phone services. The rating engine 120 is an SDP (Service Data Point) or any other component or platform that determines whether an emergency communication session may be reestablished between a service provider and the device 105. The SDP may be a node in the service network (e.g., a GSM network) responsible for determining device user information such as, for example, rate plans, rate balance, device identification (e.g., MSISDN), and time an emergency communication session was established and/or disconnected. Further details of the routing engine 115 and the rating engine 120 are described below.

[0024] As shown in Figure 1, to initiate an emergency communication session, at a time 150 a disabled device 105 sends a communication request to the switch 110. Such a request may be, for example, a 911 call. Even though the device is disabled, such a communication is allowed by the system since it is directed to an emergency number. At a time 153, the switch 110 requests a routing instruction, e.g., a Pseudo Automatic Number Identification or pANI (such as an Emergency Services Routing Key (ESRK) or an Emergency Services Query Key (ESQK)) from the emergency service routing engine 125. The emergency service routing engine 125 provides the routing information to the switch 110 to route the communication request. In some embodiments, the emergency service routing engine 125 is a Gateway Mobile Location Center (GMLC) which may interface with one or more other system nodes. At a time 156, the emergency service routing engine 125 forwards the routing instruction(s) to the switch 110. The routing instructions are used to identify the service provider 130 (e.g., a PSAP) where the emergency communication request is to be routed. At a time 160, the switch 110 routes the communication request to the service provider 130 identified via the routing instructions. A communications session is then established between the device 105 and the service provider 130.

[0025] At a time 163, the emergency service routing engine 125 notifies the rating engine that the emergency communication session has been established between the device 105 and the service provider 130. In some embodiments, the emergency service rating engine 125 provides the rating engine 120 with a time the emergency communication session was established and with a device identifier (e.g. telephone number, Mobile Subscriber Integrated Services Digital Network Number (MSISDN), an International Mobile Subscriber Identifier or IMSI, a MAC address, an IP address, etc). The rating engine 120 may then initiate a timer based on the time the emergency communication session was established and associate the timer with the device identifier. The timer and the device identifier may, for example, be stored in the rating engine 120, or in a database and/or directory accessible to the rating engine 120. As will be described below, the timer is utilized by the system to determine whether a defined threshold of time (e.g., 10 minutes, 5 minutes, etc) has elapsed since an emergency communication session was established between a device and the service provider.

[0026] At a time 166, the established communication session is prematurely disconnected or dropped. For example, if the communication is a 911 call, the 911 call may disconnect. The device user may prematurely terminate the communication session, the service provider may prematurely terminate the communication session, or technical difficulties may terminate the communication session. In some embodiments, a notification of the premature termination of the communication session may be sent from the emergency service routing engine 125 to the rating engine 120. In response to receiving the notification of premature termination, the rating engine may restart the timer associated with the device in order to allow the system to measure whether a defined threshold of time (e.g., 10 minutes, 5 minutes, etc) has lapsed since the emergency communication session was terminated.

[0027] Subsequent to the termination of the communication session, the same service provider (e.g., the PSAP) or a different service provider may desire to reestablish the communication session with the device user. In order to do so, at a time 170 the service provider 130 sends a request to reestablish the communication session

to the switch 110. The request may include the device identifier (e.g., MSISDN, MSI, MAC address, IP address, etc.).

[0028] At a time 173, the switch 110 sends a "rating request" or a request to authorize establishment of the communication session to the routing engine 115. At a time 176, the routing engine 115 forwards the request to reestablish a communication session to the rating engine 120. The request may, for example, include the device identifier. The rating engine accesses the database and/or directory storing the timer and associated device identifier. The rating engine 120 identifies the timer associated with the device identifier and determines whether the defined threshold of time has lapsed. As mentioned above, in some embodiments the timer indicates the amount of time since the emergency communication session was initially established, while in other embodiments the timer indicates the amount of time since the emergency communication session was terminated. If the defined threshold period has not lapsed, the rating engine 120 authorizes the request to reestablish the communication session by forwarding a permission message to the switch 110 at a time 180. Otherwise, the communication session is denied by the rating engine.

[0029] In some embodiments, the device 105 may belong to a family allowance plan (e.g., Family Allowances^{SM}). In such an event, the rating engine 120 may deduct minutes and/or usage units from the overall service plan for the duration of the communication sessions, if minutes and/or usage units remain in the plan. Alternatively, if the resources allocated under the plan are exhausted or if the device 105 does not belong to a family allowance plan, the rating engine 120 may track the amount of minutes and/or usage units consumed during the reestablished communication session, and impose a subsequent fee on the device user. In other embodiments, the communication session may be free of charge (similar to outgoing 911 calls, customer service calls, etc.).

[0030] The routing engine 115 may also communicate with peripherals, e.g., to play voice messages, or prompt for information, such as pre-paid minute purchases using account codes.

[0031] At a time 183, the emergency communication session is reestablished between the device 105 and the same or a different service provider 130. In the event

that there is another termination in the communication session, the communication session may be reestablished by repeating the signaling occurring at times 170-183. The rating engine may re-set the timer associated with the device at the time the connection is reestablished, or at the time that the connection is lost. In this manner, communication sessions may be enabled over an extended period having multiple disconnections.

[0032] Figure 2 is a flow chart illustrating an alternate method 200 for establishing a communication session between a disabled device 105 and a service provider 130 (e.g., a PSAP such as a 9-1-1 call center or customer service for a telecommunications service provider). The alternate method depends on a list of "authorized" service providers that are maintained by the system in a database that is accessed by the rating engine 120. At a decision block 270, the service provider 130 requests the establishment of a communication session with the device 105. The request may be in response to a prematurely terminated communication session (e.g., a disconnected communication session or dropped call) or, alternatively, may be a first request for communication with the device 105.

[0033] At a block 273, in response to the communication request, the switch (e.g., a Mobile Switching Center or MSC) 110 requests a rating and/or authorization from the routing engine 115. At a block 276, the routing engine 115 sends the rating request and/or authorization request to the rating engine 120. The rating engine determines whether the requesting service provider is contained in a database or repository of authorized service providers that are identified by one or more identifiers (e.g. telephone numbers, numeric and/or alphanumeric addresses identifiers, uniform resource identifiers (URI), or other identification information). It will be appreciated by those skilled in the art that the identity of the service providers may be stored in any number of available ways.

[0034] At a decision block 278, the rating engine 120 compares the identifier of the requesting service provider 130 with the list of authorized service providers that are located in the repository. Using one or more comparison methods known in the art, the rating engine 120 determines whether the request service provider is found in the repository. At a block 281, if the requesting service provider 130 does not match one of

the identifiers in the repository, the service provider 130 may receive a "subscriber unavailable" message. The attempt to connect with the disabled device may be repeated until the service provider 130 discontinues its communication request (e.g., the PSAP operator hangs up), or the system terminates the service provider's 130 communication request (e.g., the system hangs up on the PSAP operator) after a number of failed communication attempts.

[0035] Alternatively, if the requesting service provider identifier is found in the repository of authorized service providers then at a block 280 the rating engine 120 rates the requested communication session and grants permission to establish the communication session. At a block 283, the communication session between the service provider 130 and the device 105 is established. The method 200 passes control back to decision block 270, and waits for another communication request from the service provider 130.

[0036] As mentioned above, in some embodiments, the device 105 may belong to a family allowance plan (e.g., Family Allowances^{SM}). In such an event, the rating engine 120 may deduct minutes and/or usage units from the overall service plan for the duration of the communication sessions, if minutes and/or usage units remain in the plan. Alternatively, if the service plan resources are exhausted or if the device 105 does not belong to a family allowance plan, the rating engine 120 may track the amount of minutes and/or usage units consumed during the reestablished communication session, and impose a subsequent fee on the device user. In other embodiments, the communication session may be free of charge (similar to outgoing 911 calls, customer service calls, etc.).

[0037] It should be appreciated that the method described in Figure 2 could be used in conjunction with the method described in Figure 1. For example, in one embodiment, a communication session (e.g., call) may be rated as "free" if the identifier of the service provider 130 (e.g., an incoming telephone number) is found in the list of authorized service providers as disclosed in Figure 2, and/or if there is an active timer and the timer indicates that the defined threshold period has not lapsed, as disclosed in Figure 1.

[0038] Figure 3 is a signaling diagram illustrating a series of messages that are sent between the disabled device 105, the switch 110, the routing engine 115, the rating engine 120, an Interactive Voice Response (IVR) system 323, the emergency service routing engine 125 (e.g., a Gateway Mobile Location Center or GMLC) and the service provider 130, in order to establish an emergency communication between the disabled device 105 and the service provider 130, and to reestablish communication between the same or a different service provider and the disabled device 105 if the emergency communication between the disabled device and the service provider is interrupted or otherwise terminated. The method depicted in Figure 3 uses a routing key (e.g., a pANI) to establish and reestablish communication between a service provider and the disabled device.

[0039] At a time 350, the disabled device 105 user attempts to initiate an emergency communication session with the service provider 130, such as by placing a call to 911. At a time 353, the switch 110 requests a routing key unique to the communication session, such as a pANI (e.g., an ESRK or ESQK), from the emergency service routing engine 125. At a time 356, the emergency service routing engine 125 sends to the switch 110 the routing key which contains sufficient information to route the disabled device to the appropriate service provider 130. At a time 360, the switch 110 routes the communication request to the service provider 130. The communication session is thereby established between the disabled device and the service provider. Additional information such as a device identifier (e.g., MSISDN, IMSI, MAC address, IP address) and any location information known about the device 105, may also be provided to the service provider. The pANI is a temporary routing key associated with the specific device it was generated for, and may or may not be known by the device user. At a time 363, the emergency service routing engine 125 provides the rating engine 120 with the routing key, an identifier (i.e., the MSISDN, MSI, MAC address, IP address, or telephone number) associated with device, and/or the time of establishment of the communication session. The routing key, device identifier, and/or time the communication session was established are stored by the rating engine. In some embodiments, additional numbers of comparable routing engines and routing identifiers may also be provided to the rating engine.

[0040] At a time 366, the established communication session between the disabled device and the service provider is prematurely disconnected or dropped due to any number of reasons. For example, the device user may prematurely terminate the communication session, the service provider may prematurely terminate the communication session, or technical difficulties may terminate the communication session. At a time 368, the same or a different service provider attempts to reestablish the communication session with the device 105 user. The service provider 130 therefore sends a request for reestablishing the communication session to the switch 110.

[0041] At a time 370, the switch 110 sends a rating request or a request to authorize reestablishment of the communication session to the routing engine 115. The authorization request may, for example, include the device 105 identifier. At a time 372, the routing engine 115 forwards the rating request to the rating engine 120. Although the rating engine 120 determines that the device 105 is currently disabled, the rating engine allows the communication session to be reestablished since the session relates to a previous emergency communication session.

[0042] At a time 373, the rating engine 120 informs the routing engine 115 that a routing key, e.g., pANI, authentication request should be made. The routing engine 115 is configured to interface with the Interactive Voice Response (IVR) system 323 or other peripheral components. At a time 374, the routing engine 115 forwards the authentication request to the IVR 323 and/or to the other peripheral components.

[0043] The IVR is responsible for accepting and prompting an operator for input that is used to authenticate the service provider and therefore allow the session to be reestablished. Operator input to authenticate the request may come from touch-tone keys and interpreted with tone-recognition software, or may come from spoken words and interpreted with voice-recognition software. At a time 375, the IVR 323 prompts an operator at the service provider 130 to enter the routing key, e.g., the pANI, that was sent to the service provider when the device initiated the emergency communication session with the service provider. The IVR prompt may be a single node in a menu tree, or may be part of a larger menu tree (e.g. "press 1 for English... press 3 if you are a PSAP... please enter the key"). The operator at the service provider 130 may enter

the routing key, recite the routing key, or enter the routing key in any other variety of ways. For example, the operator may be provided with a software user interface that allows the operator to issue an authentication command. In such an interface, the operator may or may not be made aware of the actual alpha- or alpha-numeric construction of the routing key.

[0044] At a time 376, the operator at the service provider 130 enters the routing key (e.g., the pANI). At a time 377, the IVR 323 forwards the entered routing key response to the routing engine 115. The routing engine 115 compares the entered routing key with the routing key associated with the particular device 105. At a time 380, If there is a match between the entered routing key and the stored routing key, the routing engine 115 grants permission to reestablish the communication session via the switch 110. At a time 383, the communication session is therefore reestablished between the disabled device and the service provider. If the entered routing key does not match the stored routing key, the system may provide a failure notice, may provide a certain number of reentry tries, or may perform any number of other actions before the system finally disallows the attempted connection.

[0045] The routing key may be any number and combination of digits (e.g., numeric, alphanumeric, or any combination thereof) to allow a service provider (e.g., PSAP) to connect to a user device (e.g., telephone device such as a wireless landline or mobile phone). The routing key may be automatically, dynamically, or manually generated.

[0046] The embodiments described in Figures 1, 2 and 3 may be used in combination with and without each other. For example, a communication session may be allowed (or "rated as free") if the service provider identifier is found in the repository of known service providers and the service provider operator is able to authenticate the communication using the routing key. In another example, a communication session may be allowed (or "rated as free") if the timer indicates that the defined threshold period has not lapsed, the service provider identifier is contained in the repository of known service providers, and the service provider operator is able to authenticate the communication using the routing key. Different combinations of the disclosed

embodiments could be used to create a permissive callback system to balance the competing concerns of user safety and system abuse.

[0047] Figures 4 and 5 are signaling diagrams illustrating a series of messages that are sent between the disabled device 105, the switch 110, the routing engine 115, the rating engine 120, the emergency service routing engine 125, and the service provider 130, in order to establish an emergency communication between the disabled device 105 and the service provider 130, and to reestablish communication between the same or a different service provider and the disabled device 105 if the emergency communication between the disabled device and the service provider is interrupted or otherwise terminated. The methods depicted in Figures 4 and 5 use passcodes to establish and reestablish communication between the service provider and the disabled device.

[0048] With respect to Figure 4, at a time 450, the disabled device 105 user attempts to initiate an emergency communication session with the service provider 130, such as by placing a call to 911. At a time 453, the switch 110 requests a routing key unique to the communication session, such as a pANI (e.g., an ESRK or ESQK), from the emergency service routing engine 125. At a time 456, the emergency service routing engine 125 provides the switch 110 with the routing instructions. At times 457-458, the switch 110 requests, via the routing engine 115, that the rating engine 120 generate a passcode to associate with the device 105. At a time 459, a temporary passcode is issued to the switch 110 by the rating engine. The passcode may be any unique code, such as a string of alphanumeric characters. At a time 460, the switch routes the communication request to the service provider 130 along with the passcode, thereby establishing an emergency communication session between the device 105 and the service provider 130.

[0049] At a time 466, the emergency communication session is disconnected and, at a time 470, the same or a different service provider attempts to reestablish the communication session with the device 105. At a time 473, the switch 110 sends a "rating request" or a request to authorize reestablishment of the communication session to the routing engine 115 and, at a time 476, the routing engine 115 forwards the request to the rating engine 120. The rating engine 120 receives the rating request,

and, at a time 477, prompts the service provider 130 for the passcode. At a time 478, the service provider enters and transmits the passcode to the rating engine. The passcode may be automatically entered by service provider systems, or manually entered by a system provider operator (e.g., using an IVR system as described with respect to Figure 3). Depending on the systems provided at the service provider, the operator may or may not be made aware of the alpha- or alphanumeric construction of the passcode. At a time 480, the rating engine compares the entered passcode with the previously-stored passcode. If the entered passcode matches the stored passcode, the rating engine 120 grants permission to reestablish the communication session (e.g., to connect the call such as by rating the call as free). At a time 483, the service provider 130 reestablishes the disconnected communication session with the device 105.

[0050] Turning to Figure 5, the messages sent at times 550-570 are substantially similar to the messages sent at times 450-470 in Figure 4. In the method shown in Figure 5, however, upon receiving an attempt to reestablish the communication session from the service provider 130, the switch 110 prompts the service provider 130 for a passcode at a time 571. At a time 572, the service provider enters and transmits the passcode to the switch. The passcode may be automatically entered by service provider systems, or manually entered by a system provider operator (e.g., using an IVR system as described with respect to Figure 3). At a time 572 the switch transmits the received passcode to the rating engine, where the rating engine compares the entered passcode with the previously-stored passcode. If the entered passcode matches the stored passcode, the rating engine 120 grants permission to reestablish the communication session (e.g., to connect the call such as by rating the call as free) at a time 580. At a time 583, the service provider 130 reestablishes the disconnected communication session with the device 105. If the entered passcode does not match the stored passcode, the method may allow for any number of reentry tries before issuance of a failure message and disallowing the reestablishment of the communication session.

[0051] Figure 6 is a partial flowchart of the method depicted in Figure 1 for reestablishing a communication session with the disabled device 105 after an

emergency communication session has been terminated. At block 605, the device user initiates an emergency communication request. At block 610, the network routes the communication request (e.g., call) to the service provider 130 and establishes the emergency communication session. At block 615, the communication session is disconnected for any one of the previously-articulated reasons. In response thereto, a configurable timer or other mechanism for measuring elapsed time is initiated by the system. At block 620, the rating engine 120 receives a request to reestablish the communication session. When a request to reestablish the communication session is received, at a decision block 625 the rating engine checks the state of the timer or the mechanism for monitoring elapsed time. If a threshold period has lapsed (i.e., if the elapsed time is greater than a threshold time), at block 635 the rating engine denies the request for the communication session. If a threshold period has not lapsed (i.e., the elapsed time is less than a threshold time), at block 630 the rating engine allows the request for the communication session, such as by rating it as free of charge. The method passes control back to block 620 and where the rating engine waits for another request to reestablish the communication session. The threshold period may be set by the system operator and may be minutes, tens of minutes, or other time suitable to enable communication sessions to be reestablished. Those skilled in the art will appreciate that whether the threshold period has elapsed may be determined by setting a countdown timer and detecting whether the timer has reached zero, by starting a count-up timer and detecting whether the elapsed time has exceeded the threshold period, by storing a first time when the communication session is either initiated or terminated and comparing the first time with a second time when a request is received for reestablishing a communication session, or by any other means. Moreover, even though the measurement of elapsed time is depicted as starting in block 615, the measurement may begin at any other point associated with the communication session.

[0052] Figure 7 is a partial flowchart of the methods depicted in Figures 4 and 5. At a block 705, a user of a device 105 initiates a request for an emergency communication session. At block 710, the system routes the communication request to the service provider 130 and issues a passcode to the service provider 130. The passcode may be any unique code, such as a string of alphanumeric characters. At block 715, the communication session (e.g., the call) is disconnected for any one of the

previously-articulated reasons. At block 720, the system receives a request to reestablish the communication session. At block 725, in response to the request to reestablish the communication session, the service provider is prompted for the passcode. At block 730, the system receives the passcode and compares the entered passcode with the stored passcode associated with the previous emergency communication session initiated by the device 105. At decision block 735, the system determines whether the stored passcode matches the entered passcode. If the stored passcode matches the entered passcode, the system allows the request to reestablish the communication session (e.g., call) at block 740. The method passes control to block 720 and waits for another request for a communication session. If the stored passcode does not match the entered passcode, the system denies the request to reestablish the communication session at block 745. The system may allow a number of attempted re-connection attempts before issuing a failure message.

[0053] Those skilled in the art will appreciate that the system and methods disclosed herein may be implemented on any computing system or device. Suitable computing systems or devices include server computers, multiprocessor systems, microprocessor-based systems, network devices, minicomputers, mainframe computers, distributed computing environments that include any of the foregoing, and the like. Such computing systems or devices may include one or more processors that execute software to perform the functions described herein. Processors include programmable general-purpose or special-purpose microprocessors, programmable controllers, application specific integrated circuits (ASICs), programmable logic devices (PLDs), or the like, or a combination of such devices. Software may be stored in memory, such as random access memory (RAM), read-only memory (ROM), flash memory, or the like, or a combination of such components. Software may also be stored in one or more storage devices, such as magnetic or optical based disks, flash memory devices, or any other type of non-volatile storage medium for storing data. Software may include one or more program modules which include routines, programs, objects, components, data structures, and so on that perform particular tasks or implement particular abstract data types. The functionality of the program modules may be combined or distributed as desired in various embodiments.

[0054] It should be appreciated that the embodiments disclosed above are only examples of the present invention. The described embodiments may be used in various combinations with and without each other. Additional implementations will be apparent to persons of ordinary skill in the art having the benefit of this disclosure. For example, the presented embodiments refer to rating a call as free to allow an incoming emergency call despite an insufficient amount of pre-paid minutes. However, in some embodiments the issue may not be a lack of minutes, but rather a suspended account, a locked device, or a deactivated account because the device was reported as lost or stolen. In some embodiments, "rating the call as free" is sufficient to enable the communication session to be reestablished. In some embodiments, rather than "rating the call as free" the rating engine or other system component may implement a functional equivalent that allows the device to receive an incoming call despite the device otherwise being unable to receive the communication. For example, if the device (e.g., phone) is locked and the device user does not know or cannot remember the unlock code, a call to the service provider (e.g., 911 call) is typically still allowed. In a callback situation, instead of or in addition to "rating the call as free," the system may remotely and temporarily unlock the device so the user may answer the incoming call.

[0055] In order to enable the previously-described callback techniques, the system receives an indication from network components that an emergency call has been placed by the disabled device. In some circumstances, such as when a device is roaming onto a network of another carrier, such an indication from network components may be delayed or may not be detected when the emergency call is handled by the other network. In these and other circumstances, it may be beneficial to have an alternate mechanism to detect when an emergency communication session is initiated by a disabled device. Figure 8 is a flowchart of a monitoring application 800 that is resident on a device and which generates a message indicating when an emergency communication session is established by the device. At a block 805, the monitoring application detects a request to initiate an emergency communication session. The request may be detected by monitoring key sequences to detect key sequences indicative of an emergency call (e.g., a user dialing "9-1-1") or of an emergency communication (e.g., sending an SMS message to an emergency responder). The request to initiate an emergency communication session may also be detected by a

user unlocking or otherwise enabling a disabled device to make an emergency communication (e.g., when a user affirmatively responds to a question asking the user whether the user intends for an emergency communication to be made).

[0056] At a decision block 810, the monitoring application determines whether the telecommunications network being utilized by the disabled device has the capability to complete the emergency communication session. In some circumstances, the telecommunications network utilized by the disabled device may not be able to establish the requested emergency communication session. For example, when roaming internationally, the "9-1-1" emergency call functionality that is available in the U.S. may not be available using the same keystroke sequence. In order to minimize the possibility that a user might attempt to use the callback functionality for fraudulent purposes (e.g., to use the callback functionality to allow friends or family to contact the user on a disabled device), the monitoring application preferably reports only those emergency communication sessions that are capable of being established by the telecommunications network providing service to the device. If the network is not capable of establishing the emergency communication session, processing returns to block 805 where the monitoring application continues to monitor for additional user requests to establish an emergency communication session. Otherwise, if the network is capable of establishing the emergency communication session, processing continues to a block 820. Those skilled in the art will appreciate that the test performed at decision block 810 may be performed prior to establishing the emergency communication session or may be performed after the emergency communication session has been established.

[0057] At block 820, the monitoring application transmits a message indicating that an emergency communication session is or will be conducted by the disabled device. The message may be transmitted on any non-voice channel available on the device. For example, the non-voice channel may be an unstructured supplementary service data (USSD) channel, a short message service (SMS) channel, or other like messaging channel. Preferably, the non-voice channel used by the device has two characteristics that make it suitable for such a message: (i) the non-voice channel routes the message to its destination without undue delay; and (ii) the non-voice channel provides a high

degree of reliability that the message will be delivered (i.e., a low likelihood that the message will be dropped in transit). The message contains or is associated with a unique identifier to identify the device, such as the International Mobile Subscriber Identity (IMSI) number of the device or the phone number associated with the device. The message also contains an alphanumeric or other code that identifies that the device is initiating or has initiated an emergency communication session. In some circumstances, the code is assigned by the telecommunications network operator and is common across all devices. In such a case, the code is securely stored in all devices so that it is difficult for a party to gain access to the code. In the event of a security breach where a third party learns of the code, a new code may be re-distributed by the telecommunications network operator to all network devices. In other circumstances, the code may be generated by each device, such as by applying a known hash function to a unique identifier associated with the device.

[0058] While the monitoring application may send the message across any non-voice channel to notify the system of the emergency communication session, certain channels may be more reliable than others. For example, sending the message via an SMS channel may not be reliable since the SMS message must be routed through a short message service center (SMSC) and may be delayed as a roaming network operator creates a charge data record for the message. Moreover, most telecommunications networks do not provide a guarantee of delivery for any SMS message. To provide for a more reliable and expeditious message delivery, the monitoring application may therefore use an USSD channel. One advantage of using the USSD channel to transmit a message to the system is that a USSD message sent via the channel is not extensively processed by the roaming telecommunications network. Instead, the USSD message is automatically redirected to reach the device's home telecommunication network where it is delivered to the USSD gateway. As a result, a message sent via the USSD channel will be delivered more quickly and with higher reliability than a message sent via the SMS channel. The monitoring application may transmit the message before, during, or immediately after the emergency communication session is initiated between the disabled device and the contacted service provider.

[0059] Because the message is transmitted by the monitoring application during a situation that is presumed to be an emergency, the monitoring application transmits the message as a background process that does not require user intervention to key-in or otherwise send the message. By making the message transmission occur automatically, the monitoring application ensures that the message will be sent in a timely fashion. To improve management of devices, the automatic generation of messages by the monitoring application is a feature that the telecommunications network operator may turn on or off remotely. Additionally, the automatic generation of messages by the monitoring application may be tied to the presence of a SIM card or other component that identifies the user as being a valid recipient of services from the telecommunications network operator. That is, the monitoring application will not send messages to the system if a valid SIM card is not present in the device.

[0060] While a single message is contemplated as being sent by the monitoring application herein, it will be appreciated that the application may transmit two or more messages as part of the notification associated with the emergency communication session. For example, two or more messages may be required to provide additional information about the emergency communication session, such as a geographic location of the device when the session was established. As another example, a first message may be sent by the monitoring application to signal the beginning of an emergency communication session and a second message may be sent by the monitoring application to signal the end of the emergency communication session.

[0061] Unfortunately, telecommunication network operators need to be aware of attempts to obtain free telecommunication services, such as might be achieved by modifying a mobile device to send a fraudulent message mimicking the message normally sent during an emergency communication session in order to receive incoming calls on a disabled phone. To minimize the risk of such fraud, the monitoring application may further be responsive to a system confirmation process that is designed to determine whether a message was validly sent from a monitoring application on a device. For example, upon receipt of a message indicative of an emergency communication session, the system may send a confirmation request to the device. The confirmation request is received by the monitoring application at a block 820. The

confirmation request contains a unique code or other command that is intended to elicit a certain response from the device if the monitoring application is property installed and operating on the device. For example, a three digit code (e.g., "C?3") may be sent by the system to the device in a confirmation request. The monitoring application receives the confirmation request and at a block 825 uses the received code to derive an appropriate confirmation response. For example, the confirmation request code may be used to look-up a corresponding confirmation response code (e.g., "4#d") from a stored data table, or may be used as a key to a hash function to calculate a confirmation response code. At a block 830, the monitoring application then transmits the confirmation response code to the system using the non-voice channel. If the stored data table, hash function, or other algorithm or mechanism to generate appropriate confirmation response codes is ever compromised, the system may re-distribute new data tables, hash functions, etc. to mobile applications on devices.

[0062] If the confirmation response code that is received by the system matches the expected confirmation response code, the system considers the message indicative of an emergency communication session to be authentic and proceeds to enable the callback mechanism. If, however, the received confirmation response code does not match the expected confirmation response code, the system considers the message indicative of an emergency communication session to be potentially fraudulent and does not enable the callback mechanism. By disabling the callback mechanism, the system minimizes the likelihood of fraudulent activity. Rather than disabling the callback mechanism, if the received confirmation response code does not match the expected confirmation response code, the system may enable the callback mechanism but may put significant limitations on allowed callbacks. For example, the system may limit the device to receiving callbacks from only certain numbers (e.g., PSAPs) or may severely limit the length of time of callbacks (e.g., one minute).

[0063] The message that is transmitted by the disabled device is detected by the system and used to enable a callback mechanism to the device as previously described herein. Figure 9 is a signaling diagram that depicts the receipt and processing by the system of the message transmitted by the monitoring application. As shown in Figure 9, to initiate an emergency communication session, at a time 950 a disabled device 905

sends a communication request to a switch 910. Such a request may be, for example, a 911 call. Even though the device is disabled, such a communication is allowed by the system since it is directed to an emergency number. In addition, at a time 951 a monitoring application in the device 905 automatically transmits a message to a message gateway 915 indicating that an emergency communication session has been initiated by the disabled device. As was described herein, such a message may be sent after the monitoring application verifies that the relevant telecommunication network is capable of establishing the emergency communication session. The message gateway 915 is a network component that is capable of receiving and acting upon the message sent from the monitoring application. If the message is sent via the USSD channel, for example, the message gateway is a USSD gateway. At a time 952, the message gateway sends a confirmation request message to the disabled device 905. As previously described, the confirmation request message contains a unique code or other command that is intended to elicit a certain response from the device 905 if the monitoring application is property installed and operating on the device. At a time 953, the monitoring application on the device 905 transmits a confirmation response code to the message gateway 915 using the non-voice channel. If the confirmation response code that is received by the message gateway 915 matches the expected confirmation response code, the message gateway considers the message received at time 951 to be authentic and proceeds to enable the callback mechanism. If, however, the confirmation response code that is received by the message gateway 915 does not match the expected confirmation response code, the message gateway considers the message received at time 951 to be fraudulent and therefore disables the callback mechanism.

[0064] At a time 954, the switch 910 requests a routing instruction, e.g., a Pseudo Automatic Number Identification or pANI (such as an Emergency Services Routing Key (ESRK) or an Emergency Services Query Key (ESQK)) from the emergency service routing engine 930. The emergency service routing engine 930 provides the routing information to the switch 910 to route the communication request. In some embodiments, the emergency service routing engine 930 is a Gateway Mobile Location Center (GMLC) which may interface with one or more other system nodes. At a time 956, the emergency service routing engine 930 forwards the routing instruction(s) to the

switch 910. The routing instructions are used to identify the service provider 935 (e.g., a PSAP) where the emergency communication request is to be routed. At a time 960, the switch 910 routes the communication request to the service provider 935 identified via the routing instructions. A communications session is then established between the device 905 and the service provider 935. If the device 905 is roaming, some of the depicted network components will be located in the roaming network and some of the depicted network components will be located in the device's home network. For example, the switch 910, emergency service routing engine 930, and the service provider 935 will typically be associated with the roaming network. In contrast, the message gateway 915, routing engine 920, and the rating engine 925 will be associated with the device's home network in the displayed example.

[0065] At a time 963, the message gateway 915 notifies the rating engine 925 that the emergency communication session is being or has been established between the device 905 and the service provider 935. The notification provided by the message gateway 915 may include an approximate time that the emergency communication session was established and an identifier associated with the device (e.g. telephone number, Mobile Subscriber Integrated Services Digital Network Number (MSISDN), an International Mobile Subscriber Identifier (IMSI), a MAC address, an IP address, etc). The rating engine 925 may then initiate a timer based on the time the emergency communication session was established and associate the timer with the device identifier. The timer and the device identifier may, for example, be stored in the rating engine 925, or in a database and/or directory accessible to the rating engine 925. As is described herein, the timer is utilized by the system to determine whether a defined threshold of time (e.g., 10 minutes, 5 minutes, etc.) has elapsed since an emergency communication session was established between a device and the service provider.

[0066] At a time 966, the established communication session is prematurely disconnected or dropped. For example, if the communication is a 911 call, the 911 call may disconnect. The device user may prematurely terminate the communication session, the service provider may prematurely terminate the communication session, or technical difficulties may terminate the communication session.

[0067] Subsequent to the termination of the communication session, the same service provider 935 (e.g., the PSAP) or a different service provider (e.g., an emergency responder) may desire to reestablish the communication session with the device user. In order to do so, at a time 970 the service provider sends a request to reestablish the communication session to the switch 910. The request may include the device identifier (e.g., MSISDN, MSI, MAC address, IP address, etc.). When a callback is attempted from a different network, such as from a PSAP or a different service provider, the callback attempt will be routed through one or more switches until it reaches a switch 910 of the service provider associated with the disabled device. In this circumstance, the switch 910 of the service provider is different than the switch 910 of the roaming network operator that receives the original emergency call at time 950.

[0068] At a time 973, the switch 910 sends a "rating request" or a request to authorize establishment of the communication session to the routing engine 920. At a time 976, the routing engine 920 forwards the request to reestablish a communication session to the rating engine 925. The request may, for example, include the device identifier. The rating engine accesses the database and/or directory storing the timer and associated device identifier. The rating engine 925 identifies the timer associated with the device identifier and determines whether the defined threshold of time has lapsed. As mentioned above, in some embodiments the timer indicates the amount of time since the emergency communication session was initially established, while in other embodiments the timer indicates the amount of time since the emergency communication session was terminated. If the defined threshold period has not lapsed, the rating engine 925 authorizes the request to reestablish the communication session by forwarding a permission message to the switch 910 at a time 980. Otherwise, the communication session is denied by the rating engine.

[0069] At a time 983, the emergency communication session is reestablished between the device 905 and the same or a different service provider 935. In the event that there is another termination in the communication session, the communication session may be reestablished by repeating the signaling occurring at times 970-983. The rating engine may re-set the timer associated with the device at the time the connection is re-established, or at the time that the connection is lost. In this manner,

communication sessions may be enabled over an extended period having multiple disconnections.

[0070] While the monitoring application and transmitted message was described in Figure 9 in the context of a technique using a threshold time to enable callbacks, it will be appreciated that the message could also be used to trigger the callback methods using a routing key or other passcode as described herein. The use of a non-voice messaging channel merely extends the environments in which the disclosed techniques may be used to allow a disabled device to receive communications after an emergency communication session, even though such communications would normally be prevented as a result of a service lock.

[0071] It will also be appreciated that the monitoring application may send messages regardless of the telecommunications network utilized by the device, or may send messages depending of the capabilities of the telecommunications network to detect an emergency communication session. For example, the monitoring application may send messages to establish emergency call back services only when a network-based solution to detect an emergency communication session and establish emergency call back services is not available. Such messages may, for example, be sent when a device is roaming, but may not be sent when the device is on a home network.

[0072] It will also be appreciated that the message that is transmitted by the disabled device may be used to launch other services in addition to or in lieu of the callback mechanism that is described herein. For example, a telecommunications service provider associated with the device's home network may implement one or more notification processes when it receives an indication that a message has been received. If desired by the device user or mandated by the telecommunications service provider, SMS messages, email messages, or automatic calls may be automatically initiated by the telecommunications service provider to warn other people (e.g., friends or family of the device user) that the user has made an emergency call. In addition to launching other services, an indication that a user has made an emergency call on a roaming network provides valuable data to the telecommunications service provider. Prior to the solution disclosed herein, a telecommunications service provider rarely, if

ever, received a complete record of emergency calls made by a subscriber on a roaming network. The technology disclosed herein allows the telecommunications service provider to track such calls, and use statistical information associated with individual subscriber calls or across all subscriber calls to optimize and improve services to subscribers.

[0073] From the foregoing, it will be appreciated that specific embodiments of the invention have been described herein for purposes of illustration, but that various modifications may be made without deviating from the spirit and scope of the invention. For example, while signaling or blocks are presented in a given order, alternative implementations may perform routines having signaling or blocks in a different order, and some signaling or blocks may be deleted, moved, added, subdivided, combined, and/or modified to provide alternative or subcombinations. Each of these signaling or blocks may be implemented in a variety of different ways. Also, while signaling or blocks are at times shown as being performed in series, the signaling or blocks may instead be performed or implemented in parallel, or may be performed at different times. Accordingly, the invention is not limited except as by the appended claims.

CLAIMS

I/We claim:

1. A method in a disabled telecommunications device of notifying a telecommunications network component of an emergency communication session between the disabled telecommunications device and an emergency responder, the notification allowing communication with the disabled telecommunications device to be re-established in the event that the emergency communication session is terminated, the method comprising:

detecting, at a disabled telecommunications device, an attempt to establish an emergency communication session between the disabled telecommunications device and an emergency responder over a telecommunications network, wherein the emergency communication session is initiated by the disabled telecommunications device;

determining whether the telecommunications network is capable of supporting the emergency communication session between the disabled telecommunications device and the emergency responder; and

if the telecommunications network is capable of supporting the emergency communication session between the disabled telecommunications device and the emergency responder, transmitting a message to a network component associated with the disabled telecommunications device via a messaging channel, the message including an identifier associated with the disabled telecommunications device and a code indicating that the emergency communication session is being established, wherein the message enables a callback technique to be implemented in the event that the emergency communication session is terminated between the disabled telecommunications device and the emergency responder.

2. The method of claim 1, wherein the emergency responder is a Public Safety Answering Point (PSAP).

3. The method of claim 1, wherein the attempt to establish an emergency communication session is detected by monitoring key sequences to detect a key sequence indicative of an emergency communication.

4. The method of claim 3, wherein the detected key sequence is "911."

5. The method of claim 3, wherein the detected key sequence is a messaging address of the emergency responder.

6. The method of claim 1, wherein the attempt to establish an emergency communication session is detected by receiving an affirmative indication from a user to establish an emergency communication session.

7. The method of claim 1, wherein the messaging channel is an unstructured supplementary service data (USSD) channel.

8. The method of claim 1, wherein the messaging channel is a short message service (SMS) channel.

9. The method of claim 1, wherein the identifier is a telephone number, a Mobile Subscriber Integrated Services Digital Network Number (MSISDN), an International Mobile Subscriber Identifier (IMSI), a MAC address, or an IP address.

10. The method of claim 1, wherein the code is shared by multiple telecommunications devices.

11. The method of claim 1, wherein the code is generated by the disabled telecommunications device.

12. The method of claim 1, further comprising:

receiving a confirmation request from the network component seeking to confirm the validity of the message sent to the network component; and

transmitting a confirmation response to the network component indicating that the transmitted message was validly sent.

13. The method of claim 12, wherein the confirmation response is a confirmation code.

14. The method of claim 13, wherein the confirmation code is generated by a look-up table or a hash function.

15. The method of claim 1, wherein the network component is a ratings engine.

16. A computer-readable medium containing instructions that, when executed by a processor of a telecommunications device having disabled communication service, cause the telecommunications device to implement a method to notify a telecommunications network component of an emergency communication session between the telecommunications device and an emergency responder, the notification allowing communication with the telecommunications device to be re-enabled in the event that the emergency communication session is terminated, the method comprising:

detecting, at a disabled telecommunications device, an attempt to establish an emergency communication session between the disabled telecommunications device and a Public Safety Answering Point (PSAP) over a telecommunications network, wherein the emergency communication session is initiated by the disabled telecommunications device;

determining whether the telecommunications network is capable of supporting the emergency communication session between the disabled telecommunications device and the PSAP; and

if the telecommunications network is capable of supporting the emergency communication session between the disabled telecommunications device and the PSAP, transmitting a message to a network component associated with the disabled telecommunications device via a messaging channel, the message including an identifier associated with the disabled telecommunications device and a code indicating that the emergency communication session is being established, wherein the message enables a callback technique to be implemented in the event that the emergency communication session is terminated between the disabled telecommunications device and the PSAP.

17. The computer-readable medium of claim 16, wherein the attempt to establish an emergency communication session is detected by monitoring key sequences to detect a key sequence indicative of an emergency communication.

18. The computer-readable medium of claim 17, wherein the detected key sequence is "911."

19. The computer-readable medium of claim 17, wherein the detected key sequence is a messaging address of the PSAP.

20. The computer-readable medium of claim 16, wherein the attempt to establish an emergency communication session is detected by receiving an affirmative indication from a user to establish an emergency communication session.

21. The computer-readable medium of claim 16, wherein the messaging channel is an unstructured supplementary service data (USSD) channel.

22. The computer-readable medium of claim 16, wherein the messaging channel is a short message service (SMS) channel.

23. The computer-readable medium of claim 16, wherein the identifier is a telephone number, a Mobile Subscriber Integrated Services Digital Network Number (MSISDN), an International Mobile Subscriber Identifier (IMSI), a MAC address, or an IP address.

24. The computer-readable medium of claim 16, further including instructions that, when executed by the processor of the telecommunications device, cause the telecommunications device to:

receive a confirmation request from the network component seeking to confirm the validity of the message sent to the network component; and

transmit a confirmation response to the network component indicating that the transmitted message was validly sent.

25. The computer-readable medium of claim 16, wherein the network component is a ratings engine.

26. A method in a telecommunications network of allowing an emergency responder to establish an emergency communication session with a telecommunications device following the termination of a prior emergency communication session with the telecommunications device, the telecommunications device having disabled service that would normally prevent a communication session from being established with the telecommunications device, the method comprising:

receiving a message from a telecommunications device via a messaging channel, the message including an identifier associated with the telecommunications device and a code indicating that an emergency communication session is being initiated by the telecommunications device with a first emergency responder;

storing an indication that the emergency communication session has been established between the telecommunications device and the first emergency responder;

receiving a request from a second emergency responder to establish an emergency communication session with the telecommunications device, the request to establish an emergency communication session occurring after the termination of the emergency communication session between the first emergency responder and the telecommunications device, the telecommunications device having disabled service that would normally prevent communication sessions from being established by the second emergency responder with the telecommunications device; and

authorizing the second emergency responder to establish the emergency communication session with the telecommunications device based on the stored indication of the prior emergency communication session between the telecommunications device and the first emergency responder.

27. The method of claim 26, wherein the first emergency responder is the same as the second emergency responder.

28. The method of claim 26, wherein the first emergency responder is a Public Safety Answering Point (PSAP).

29. The method of claim 26, wherein the messaging channel is an unstructured supplementary service data (USSD) channel.

30. The method of claim 26, wherein the messaging channel is a short message service (SMS) channel.

31. The method of claim 26, wherein the identifier is a telephone number, a Mobile Subscriber Integrated Services Digital Network Number (MSISDN), an International Mobile Subscriber Identifier (IMSI), a MAC address, or an IP address.

32. The method of claim 26, wherein the code is shared by multiple telecommunications devices.

33. The method of claim 26, further comprising:

transmitting a confirmation request to the telecommunications device seeking to confirm the validity of the received message; and

receiving a confirmation response from the telecommunications device indicating that the received message was validly sent,

wherein the second emergency responder is authorized to establish the emergency communication session with the telecommunications device only if the confirmation response is received.

34. The method of claim 33, wherein the confirmation response is a confirmation code.

35. The method of claim 26, wherein the stored indication is a threshold time and wherein the second emergency responder is authorized to establish the emergency communication session if the request from the second emergency responder is received within the threshold time.

36. A computer-readable medium containing instructions that, when executed by a processor of a telecommunications network component, cause the telecommunications network component to implement a method to allow an emergency responder to establish an emergency communication session with a telecommunications device following the termination of a prior emergency communication session with the telecommunications device, the telecommunications device having disabled service that would normally prevent a communication session from being established with the telecommunications device, the method comprising:

receiving a message from a telecommunications device via a messaging channel, the message including an identifier associated with the telecommunications device and a code indicating that an emergency

communication session is being initiated by the telecommunications device with a Public Safety Answering Point (PSAP);

storing an indication that the emergency communication session has been established between the telecommunications device and the PSAP;

receiving a request from an emergency responder to establish an emergency communication session with the telecommunications device, the request to establish an emergency communication session occurring after the termination of the emergency communication session between the PSAP and the telecommunications device, the telecommunications device having disabled service that would normally prevent communication sessions from being established by the emergency responder with the telecommunications device; and

authorizing the emergency responder to establish the emergency communication session with the telecommunications device based on the stored indication of the prior emergency communication session between the telecommunications device and the PSAP.

37. The computer-readable medium of claim 36, wherein the emergency responder is the PSAP.

38. The computer-readable medium of claim 36, wherein the messaging channel is an unstructured supplementary service data (USSD) channel.

39. The computer-readable medium of claim 36, wherein the messaging channel is a short message service (SMS) channel.

40. The computer-readable medium of claim 36, wherein the identifier is a telephone number, a Mobile Subscriber Integrated Services Digital Network Number (MSISDN), an International Mobile Subscriber Identifier (IMSI), a MAD address, or an IP address.

41. The computer-readable medium of claim 36, wherein the code is shared by multiple telecommunications devices.

42. The computer-readable medium of claim 36, further including instructions that, when executed by the processor of the telecommunications network component, cause the telecommunications network component to:

transmit a confirmation request to the telecommunications device seeking to confirm the validity of the received message; and

receive a confirmation response from the telecommunications device indicating that the received message was validly sent,

wherein the emergency responder is authorized to establish the emergency communication session with the telecommunications device only if the confirmation response is received.

43. The computer-readable medium of claim 42, wherein the confirmation response is a confirmation code.

44. The computer-readable medium of claim 36, wherein the stored indication is a threshold time and wherein the emergency responder is authorized to establish the emergency communication session if the request from the emergency responder is received within the threshold time.

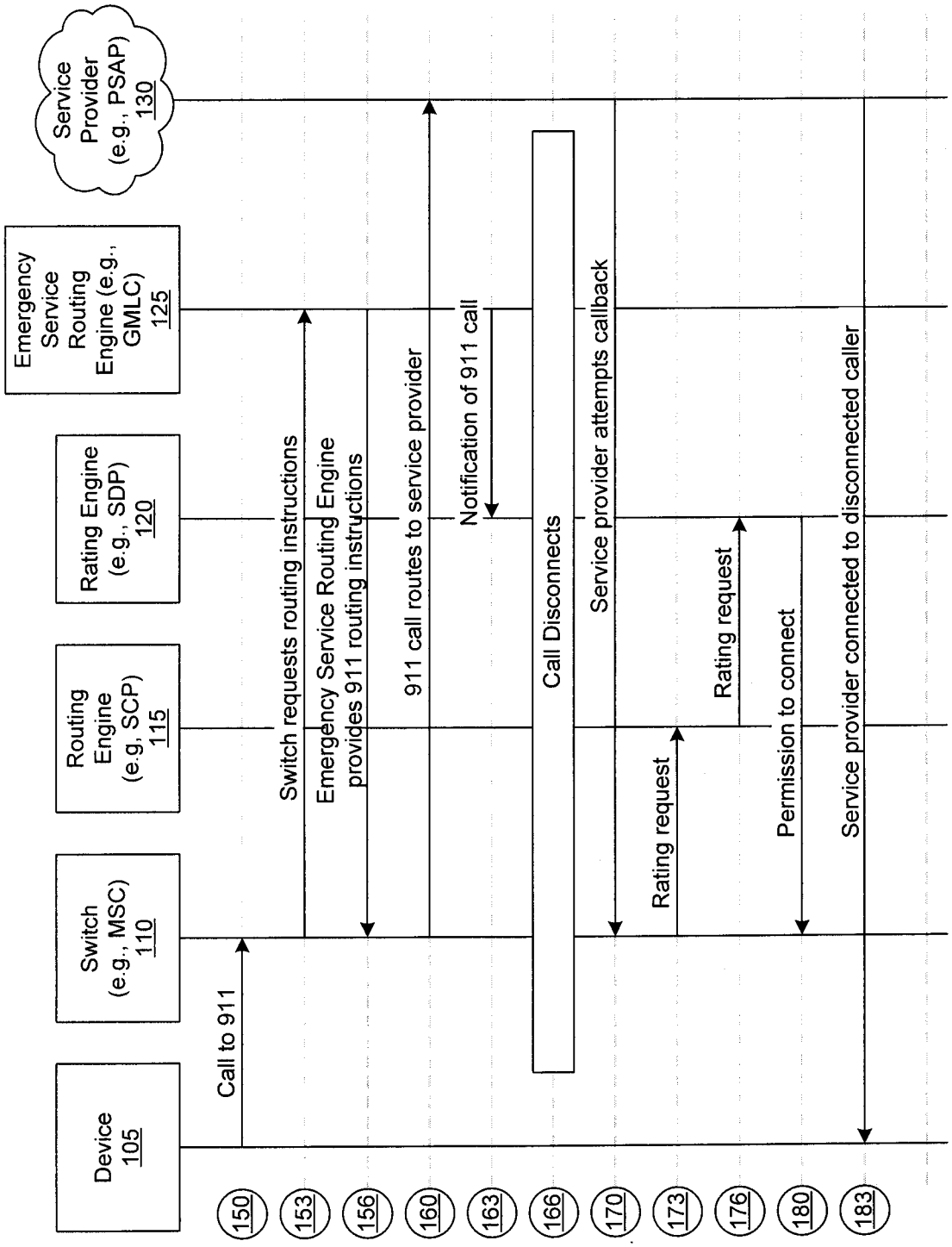
Device 105
Switch (e.g., MSC) 110
Routing Engine (e.g, SCP) 115
Rating Engine (e.g., SDP) 120
Emergency Service Routing Engine (e.g., GMLC) 125
Service Provider (e.g., PSAP) 130
Call to 911
Switch requests routing instructions
Emergency Service Routing Engine provides 911 routing instructions
911 call routes to service provider
Notification of 911 call
Call Disconnects
Service provider attempts callback
Rating request
Rating request
Permission to connect
Service provider connected to disconnected caller
150
153
156
160
163
166
170
173
176
180
183

FIG. 1

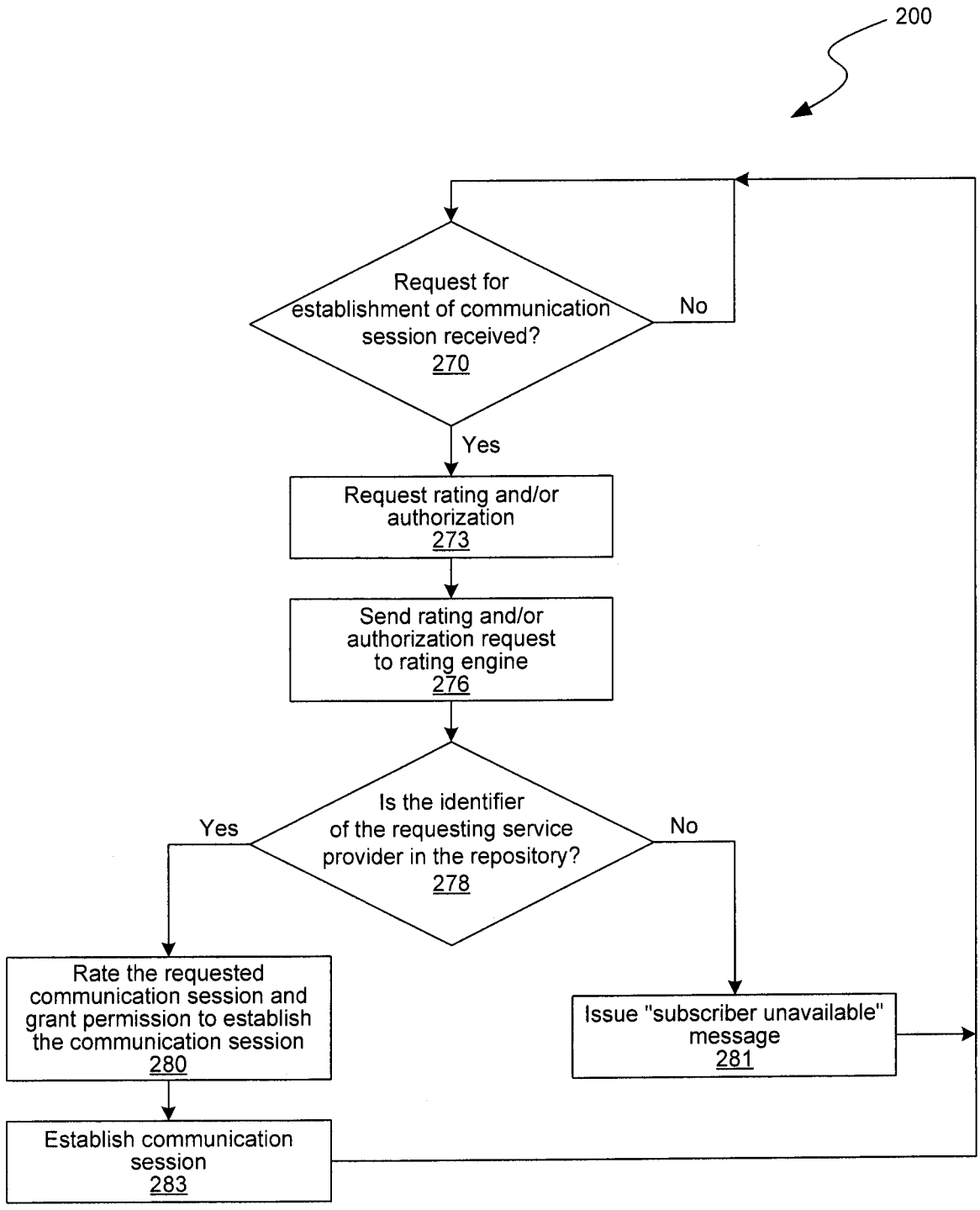
200
Request for establishment of communication session received? 270
No
Yes
Request rating and/or authorization 273
Send rating and/or authorization request to rating engine 276
Is the identifier of the requesting service provider in the repository? 278
Yes
No
Rate the requested communication session and grant permission to establish the communication session 280
Issue "subscriber unavailable" message 281
Establish communication session 283

FIG. 2

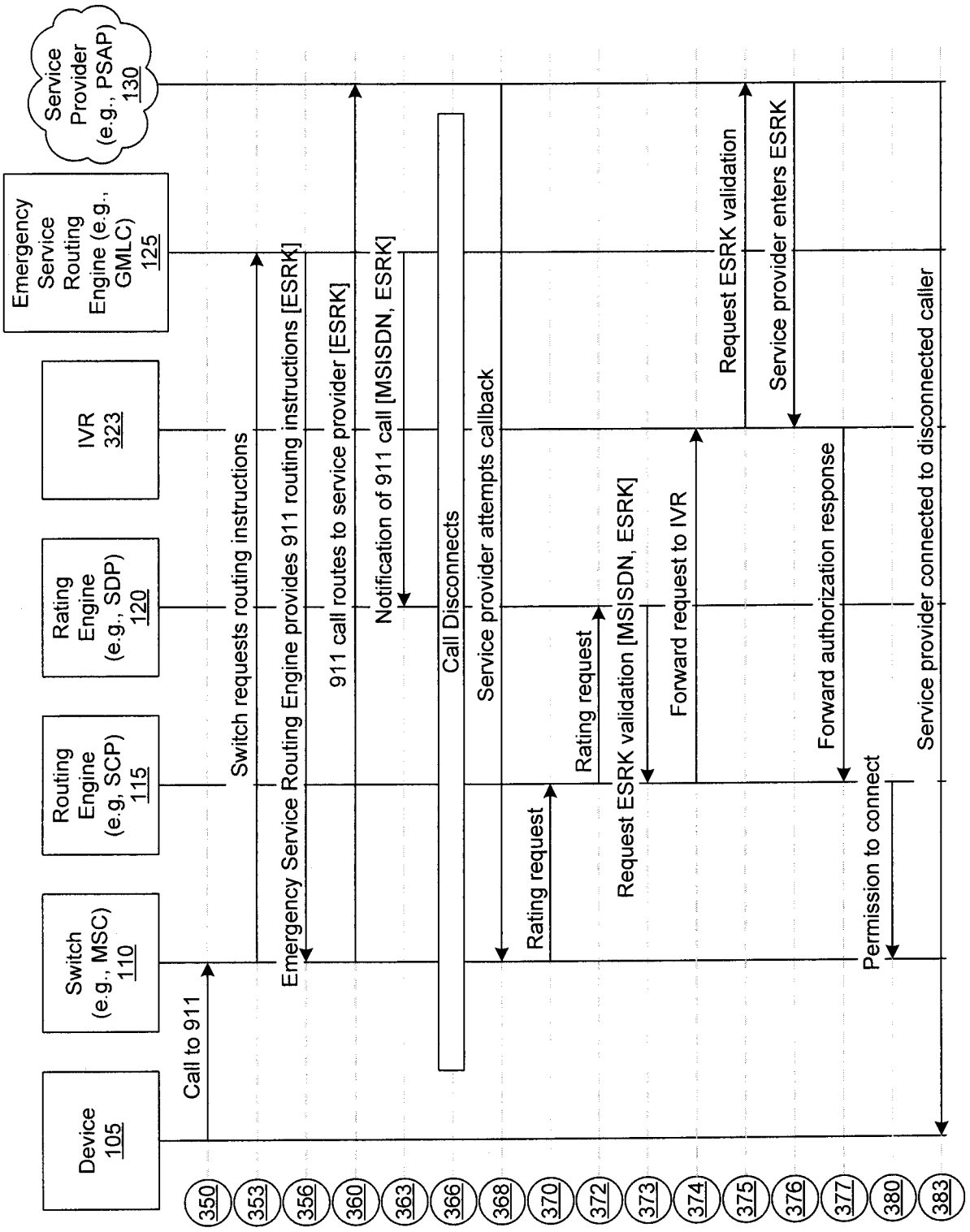
Device 105
Switch (e.g., MSC) 110
Routing Engine (e.g, SCP) 115
Rating Engine (e.g., SDP) 120
IVR 323
Emergency Service Routing Engine (e.g., GMLC) 125
Service Provider (e.g., PSAP) 130
Call to 911
Switch requests routing instructions
Emergency Service Routing Engine provides 911 routing instructions [ESRK]
911 call routes to service provider [ESRK]
Notification of 911 call [MSISDN, ESRK]
Call Disconnects
Service provider attempts callback
Rating request
Rating request
Request ESRK validation [MSISDN, ESRK]
Forward request to IVR
Request ESRK validation
Service provider enters ESRK
Forward authorization response
Permission to connect
Service provider connected to disconnected caller
350
353
356
360
363
366
368
370
372
373
374
375
376
377
380
383

FIG. 3

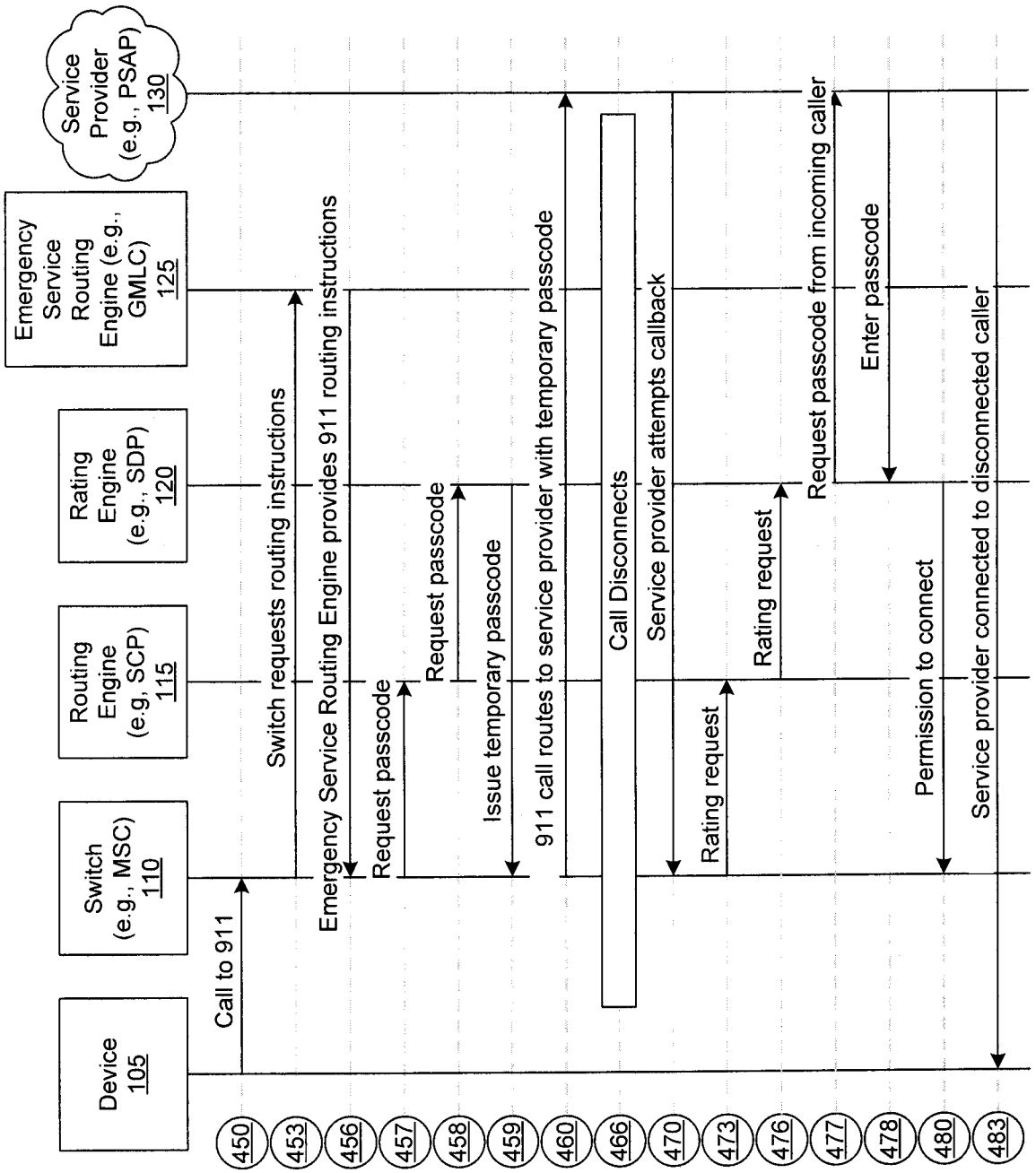
Device 105
Switch (e.g., MSC) 110
Routing Engine (e.g, SCP) 115
Rating Engine (e.g., SDP) 120
Emergency Service Routing Engine (e.g., GMLC) 125
Service Provider (e.g., PSAP) 130
Call to 911
Switch requests routing instructions
Emergency Service Routing Engine provides 911 routing instructions
Request passcode
Request passcode
Issue temporary passcode
911 call routes to service provider with temporary passcode
Call Disconnects
Service provider attempts callback
Rating request
Rating request
Request passcode from incoming caller
Enter passcode
Permission to connect
Service provider connected to disconnected caller
450
453
456
457
458
459
460
466
470
473
476
477
478
480
483

FIG. 4

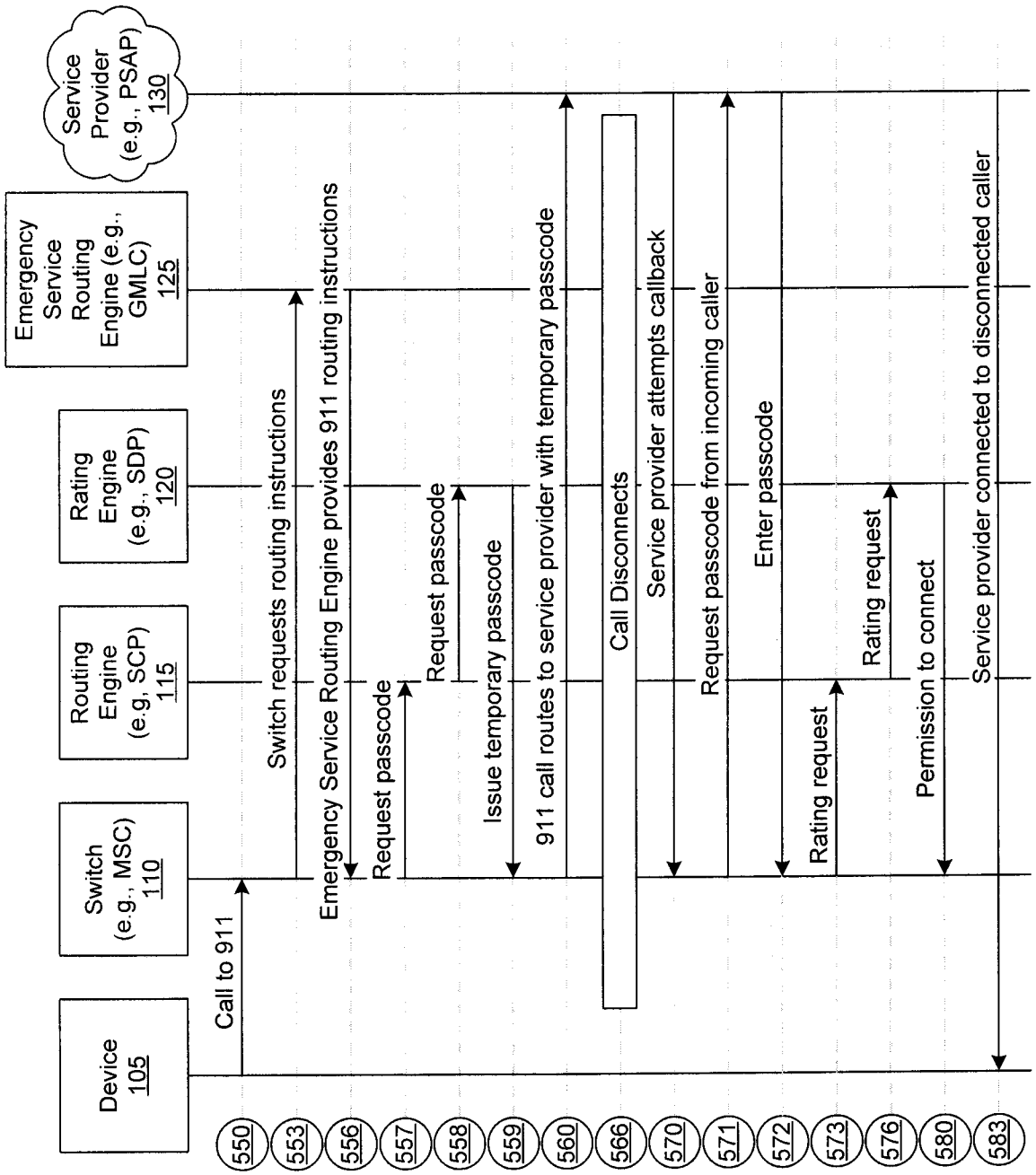
Device 105
Switch (e.g., MSC) 110
Routing Engine (e.g, SCP) 115
Rating Engine (e.g., SDP) 120
Emergency Service Routing Engine (e.g., GMLC) 125
Service Provider (e.g., PSAP) 130
Call to 911
Switch requests routing instructions
Emergency Service Routing Engine provides 911 routing instructions
Request passcode
Request passcode
Issue temporary passcode
911 call routes to service provider with temporary passcode
Call Disconnects
Service provider attempts callback
Request passcode from incoming caller
Enter passcode
Rating request
Rating request
Permission to connect
Service provider connected to disconnected caller
550
553
556
557
558
559
560
566
570
571
572
573
576
580
583

FIG. 5

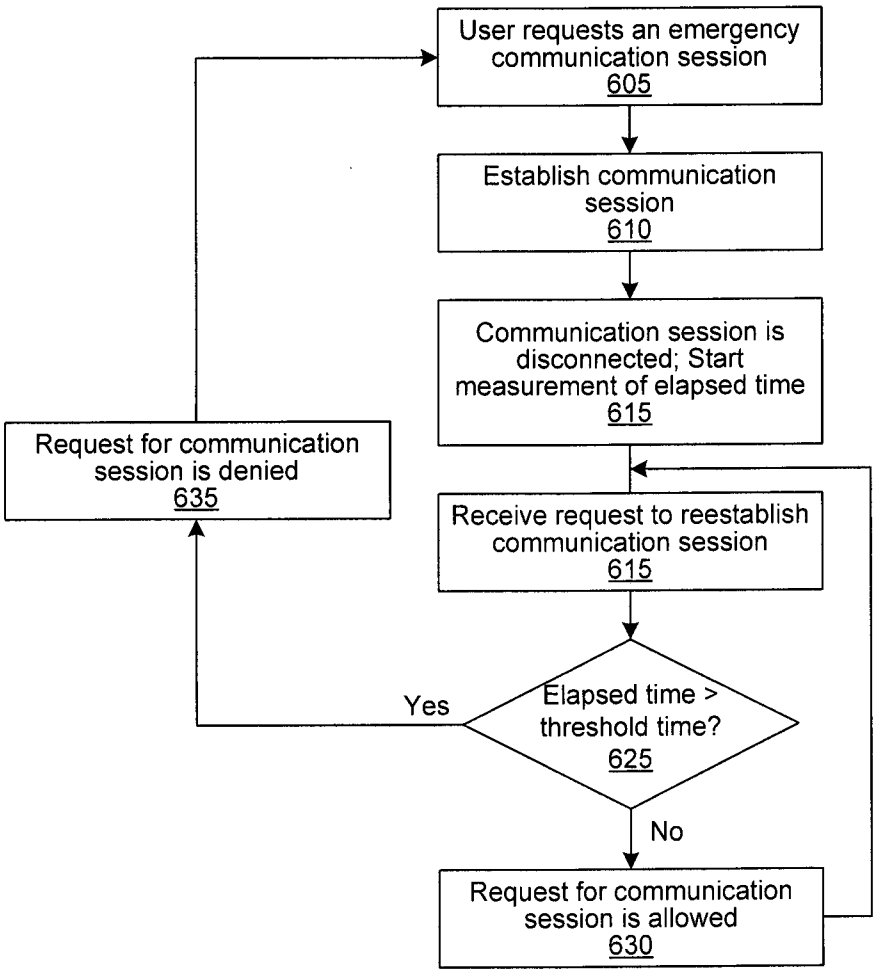
User requests an emergency communication session
605
Establish communication session
610
Communication session is disconnected; Start measurement of elapsed time
615
Receive request to reestablish communication session
615
Elapsed time > threshold time?
625
Yes
No
Request for communication session is denied
635
Request for communication session is allowed
630

FIG. 6

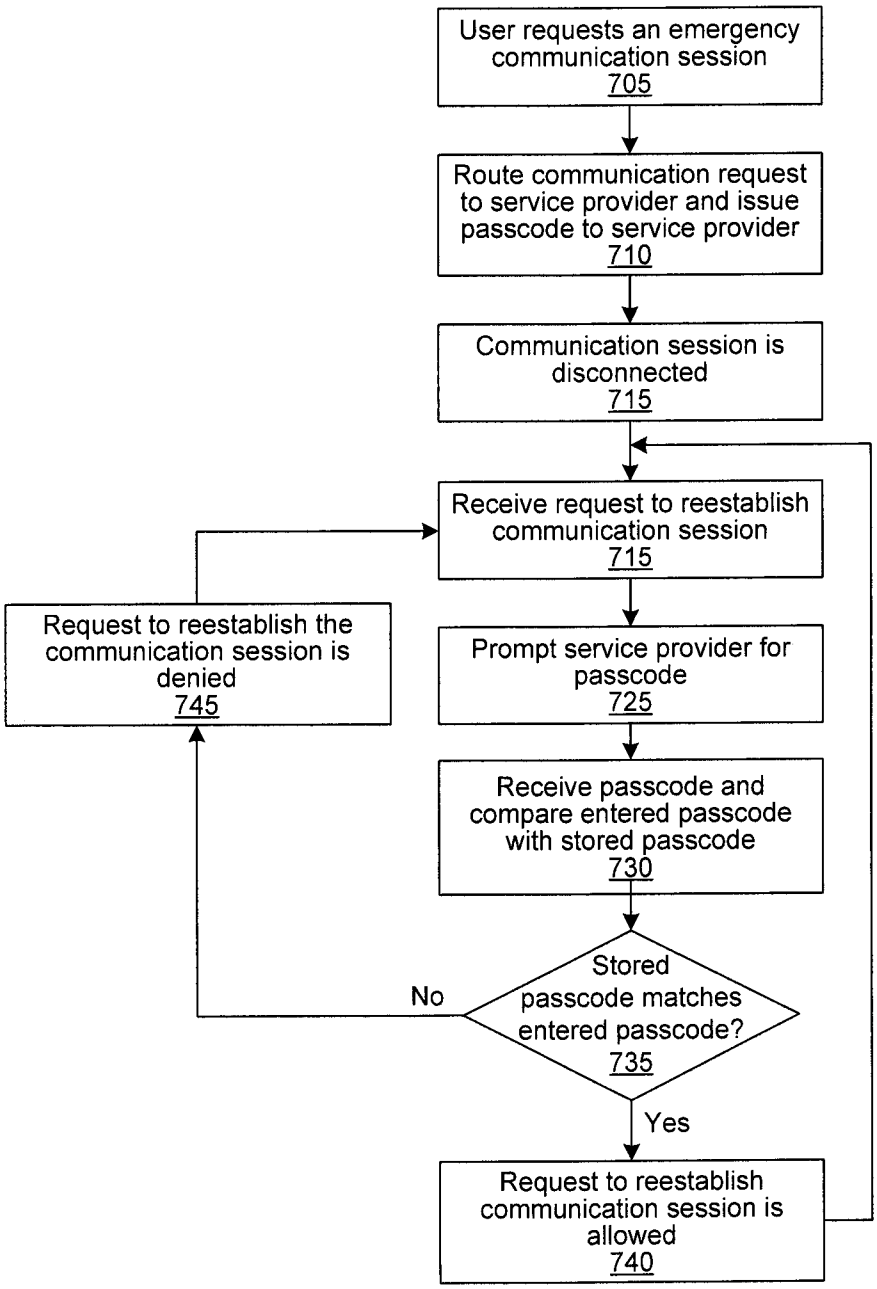
User requests an emergency communication session
705
Route communication request to service provider and issue passcode to service provider
710
Communication session is disconnected
715
Receive request to reestablish communication session
715
Prompt service provider for passcode
725
Receive passcode and compare entered passcode with stored passcode
730
Stored passcode matches entered passcode?
735
No
Yes
Request to reestablish the communication session is denied
745
Request to reestablish communication session is allowed
740

FIG. 7

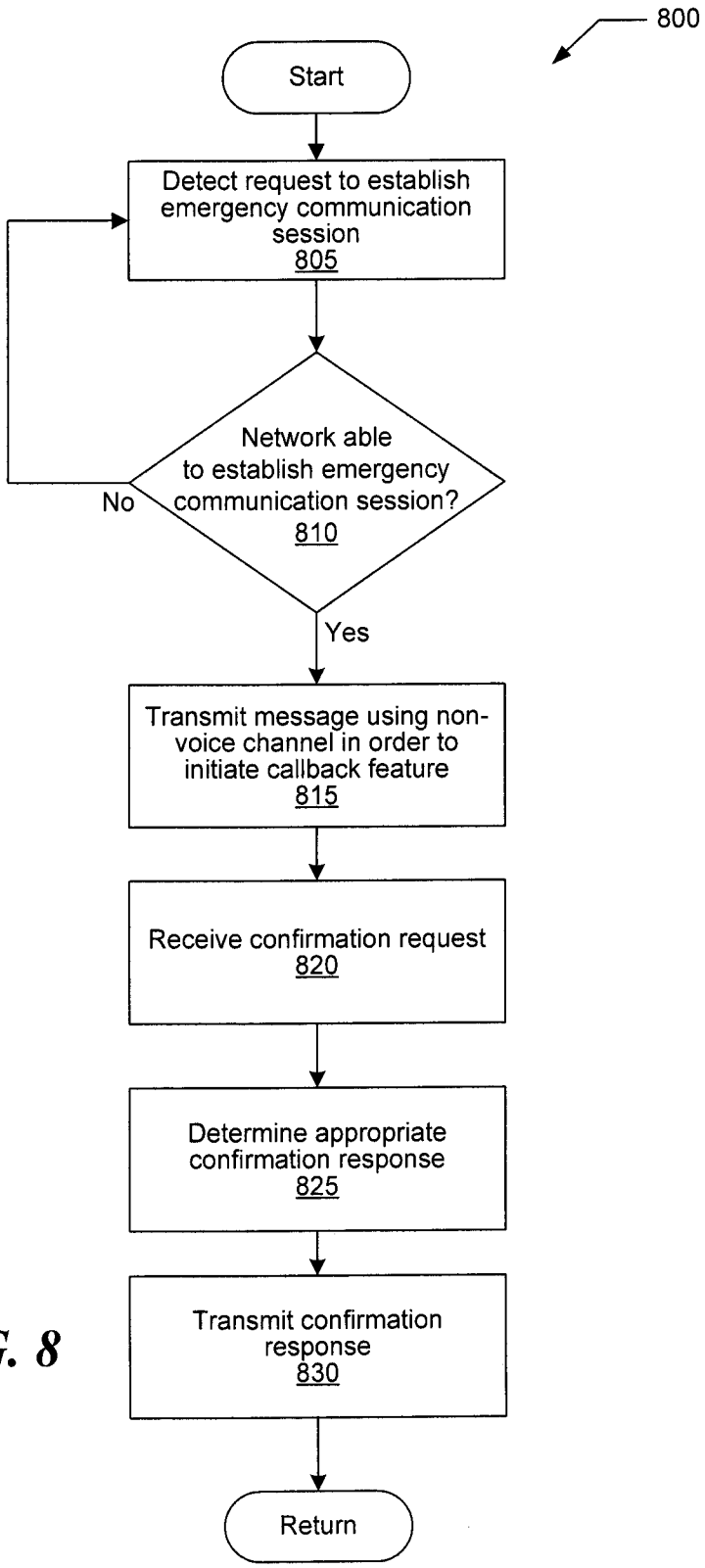
800
Start
Detect request to establish emergency communication session
805
Network able to establish emergency communication session?
810
No
Yes
Transmit message using non-voice channel in order to initiate callback feature
815
Receive confirmation request
820
Determine appropriate confirmation response
825
Transmit confirmation response
830
Return

FIG. 8

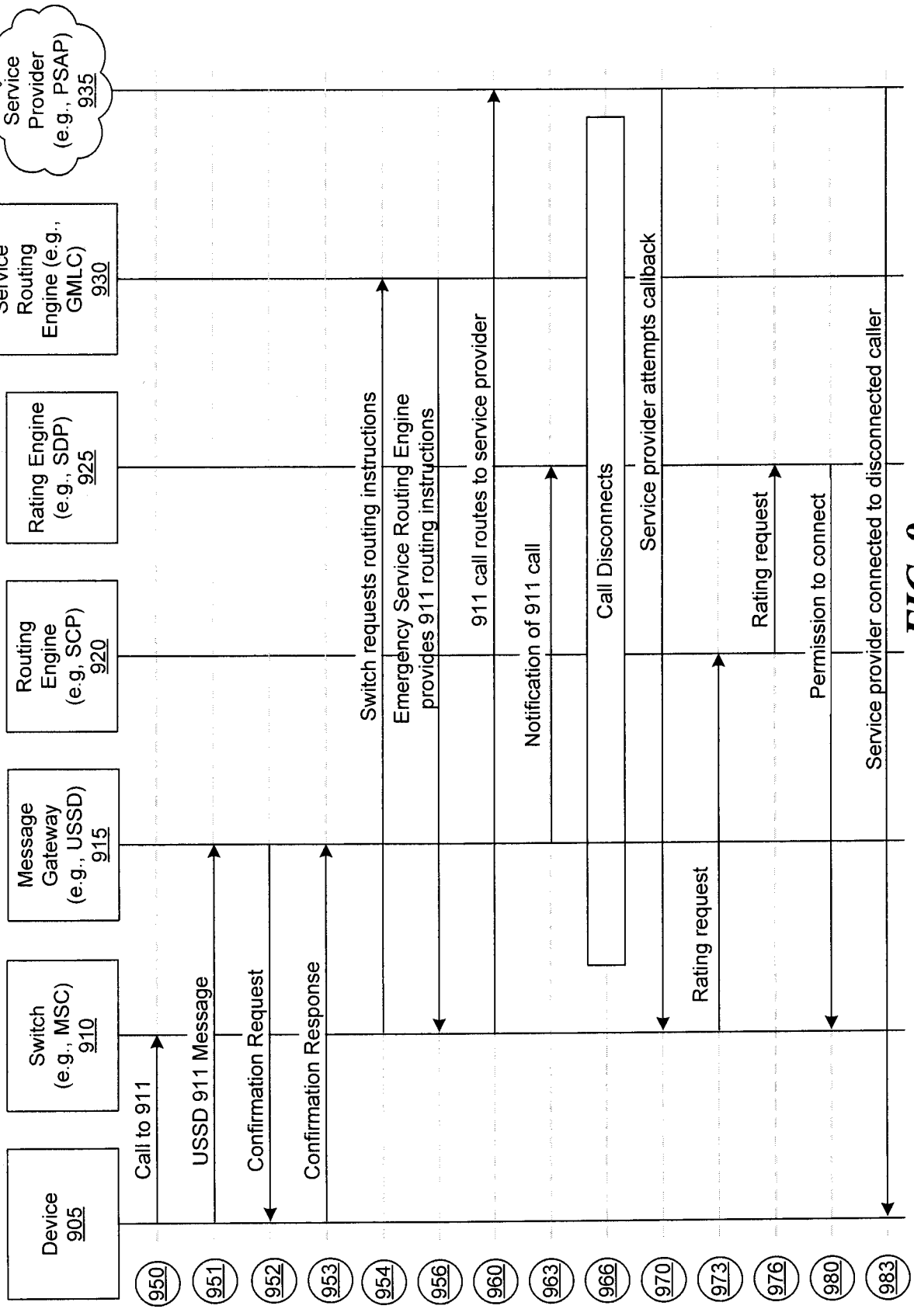
Device 905
Switch (e.g., MSC) 910
Message Gateway (e.g., USSD) 915
Routing Engine (e.g, SCP) 920
Rating Engine (e.g., SDP) 925
Emergency Service Routing Engine (e.g., GMLC) 930
Service Provider (e.g., PSAP) 935
950 Call to 911
951 USSD 911 Message
952 Confirmation Request
953 Confirmation Response
954 Switch requests routing instructions
956 Emergency Service Routing Engine provides 911 routing instructions
960 911 call routes to service provider
963 Notification of 911 call
966 Call Disconnects
970 Service provider attempts callback
973 Rating request
976 Rating request
980 Permission to connect
983 Service provider connected to disconnected caller

FIG. 9