

User Notifications

Ericsson Service-Aware Policy Controller

FACILITY DESCRIPTION

Copyright

© Ericsson España, S.A. 2016. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.

Abstract

This document provides a description of User Notifications function in the SAPC.



Contents

1	Introduction	1
1.1	Document Purpose and Scope	1
1.2	Concepts	1
1.3	Revision Information	1
2	Function	2
2.1	Overview	2
2.2	Notification Mechanism	3
2.3	Notification Policies	4
2.4	Events and Conditions Triggering Notifications	4
2.5	Notification Message Text	8
2.6	Notification Messages to Multiple Destinations	8
2.7	Notification Message Control	9
2.8	Notification Sending Procedure	12
2.9	Load Balancing Mechanism	15
3	Traffic Cases	17
3.1	SMS	18
3.2	SOAP	20
4	Capabilities	22
5	Restrictions	22
6	Security	22
	Glossary	23
	Reference List	25





1 Introduction

1.1 Document Purpose and Scope

The purpose of this document is to provide a description of User Notifications function in the SAPC.

1.2 Concepts

Destination	It is either an end user or an external system that receives notification messages.
External System	Machine or system in the network that can receive notification messages.
Load balancing	Load balancing is a computer networking method for distributing workloads across multiple computing resources, such as computers, a computer cluster, network links, central processing units, or disk drives.
Notification	It is the decision of informing, to one or several destinations, about an event occurred related to a subscriber. The destination is notified with a notification message.
Notification Address	IP address or URL belonging to a Notification Server which is identified as contact point where notification delivery requests are sent.
Notification Message	Message sent by the SAPC to an external destination with information related to an event occurred to a subscriber.
Notification Receiver	Identity of one or several external systems.
Notification Server	Target system where notification delivery requests are sent. This Notification Server may comprise a set of Notifications Addresses.

1.3 Revision Information

Rev. A	This is the first release of this document.
---------------	---

2 Function

2.1 Overview

The user notification function enables the SAPC to notify a destination (either an end user or an external system) of certain events related to a subscriber. For example, if the user has exceeded the allowed consumption during a period, the conditions of the service delivery may be affected in the way that this user may have the access to certain services blocked or the available bandwidth restricted. As it may not be easy for the user to track the consumption, a network notification is desirable to let the user know when the remaining volume/time is about to expire or when it is already finished.

Notifications can be sent to end users by SMS and to external systems by SMS and SOAP.

The next figure shows a scenario where SMS notifications and SOAP notifications are sent on response to some events happening at traffic plane. When the 80% of the allowed limit is reached, an SMS is delivered to the end user. When the 100% of the allowed limit is reached, an SMS is delivered to the end-user and a SOAP Notification is sent to the external system.

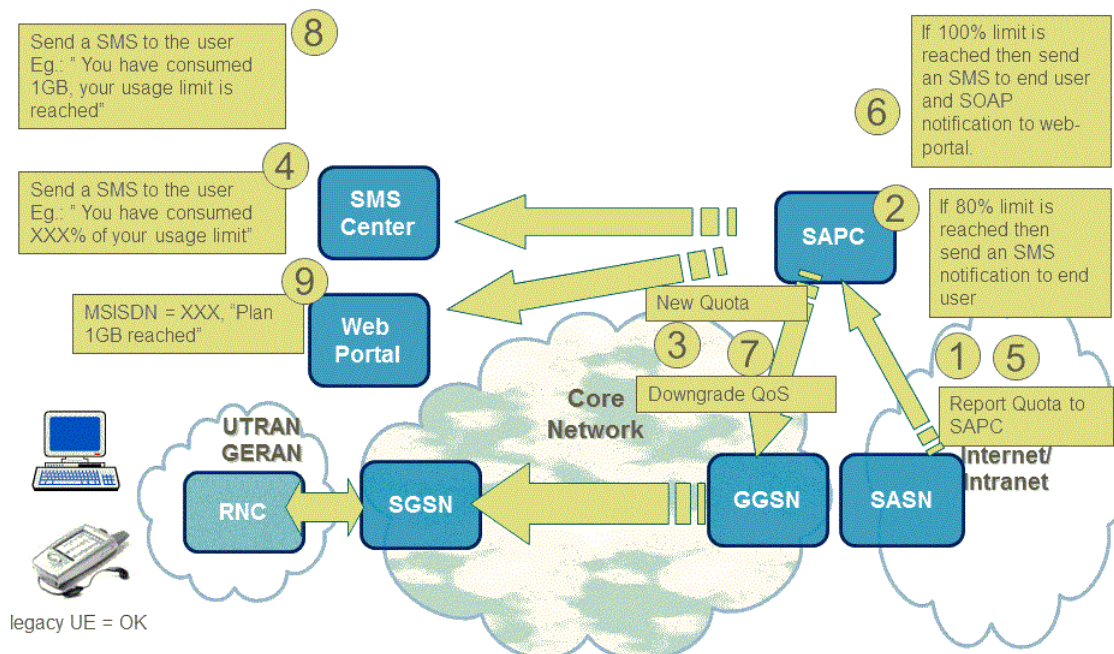


Figure 1 User Notifications Example

The events that may trigger notifications are configured in the SAPC as policy conditions. Notification messages are sent according to the notification mechanisms and addresses configured when a policy condition is fulfilled.



This function gives end users the chance to take some actions, such as subscribe to new services or changing to a different subscriber group. The end user cannot contact directly any SAPC node but it does through the Customer Care Service. Notifications are also useful for operators that want to use the notification messages to be processed by intermediate systems that could take some actions, for example, reformatting or counting.

2.2 Notification Mechanism

The SAPC can use SMPP and SOAP protocol to send notification messages, see Figure 2:

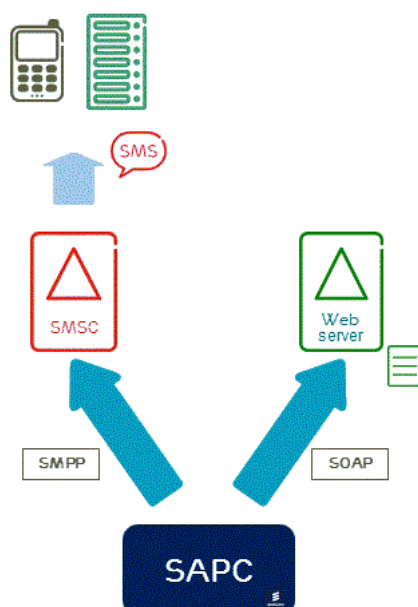


Figure 2 User Notifications Network View

- **Short Message Service (SMS).** SMS messages are sent using Short Message Peer-to-Peer (SMPP) protocol towards one Short Message Service Center (SMSC) node. SMPP protocol uses TCP/IP as transport protocol and it is specified by the SMPP Developers Forum, see Reference [7].

The SAPC supports the configuration of one or several SMSC addresses, to which the SAPC sends notifications following an even distribution mechanism, see Section 2.9 on page 15.

- **Simple Object Access Protocol (SOAP).** SOAP uses Hypertext Transfer Protocol (HTTP) as transport protocol. SOAP protocol is specified by the World Wide Web Consortium (W3C), see Reference [4]. For more details about HTTP, see Reference [5].



2.3 Notification Policies

The SAPC allows configuring the conditions that must be fulfilled to trigger a notification by policies. The usage of policies provides a flexible way of using operator defined conditions to perform tasks, as notifications in this case. For such purpose, the SAPC defines a specific policy context and action to be used in configuring notification policies. See more information about how policies are evaluated in the SAPC in [Subscription and Policy Management](#), Reference [1].

The notification policies can be defined per subscriber, per subscriber-group or at a global scope. The SAPC searches all notification policies applicable to the subscriber (the notification policies applicable to a subscriber are those associated to the subscriber, to the active groups which the subscriber belongs to and to the global policies). All the rules included in all applicable policies for the subscriber are evaluated to get the set of notifications to be sent. For such purpose, the SAPC provides a rule combination algorithm which returns the result of all the rules that evaluates to true. Finally, for each selected rule whose condition evaluates positively, a notification is triggered.

Conditions based on date and time can be also included as part of the notification policies and they are evaluated by the SAPC policy engine as other logical condition. When the policy is evaluated, if the time and date condition is fulfilled, the notification is triggered. For example, it is possible to include a time condition in a notification policy to avoid triggering the notification if another condition that triggers the notification happens at night. Unlike other policy types, the SAPC does not trigger any particular action when the time condition changes during the IP session lifetime, if no external stimulus is received.

However, it must be taken into account that some notifications could be sent by the SAPC as a consequence of a reauthorization process triggered by the validity expiration of some other policy, see Section 2.4 on page 4 for a detailed description of the events producing notification policies evaluation.

2.4 Events and Conditions Triggering Notifications

Notifications in the SAPC are intended as a way to notify one or several destinations about a change in the service conditions applying to an end user, not for a general-purpose notification mechanism. Therefore, only some events under certain circumstances can make the SAPC trigger a notification, that is, only some events trigger a notification policy evaluation in the SAPC.

Basically the SAPC evaluates such policies when some event is received in the SAPC indicating some change in the access session for a user or when some other event is received that makes the SAPC initiate a reauthorization for an active IP session. According to this, the SAPC can only trigger notifications related to subscribers with an active IP session. For example, the SAPC is not able to send a notification related to a subscriber which has changed the profile if there is not any active session for that subscriber.



The SAPC makes notification policies evaluation when one of the following events happens:

- After a Gx-CCR message is received and processed and the corresponding Gx-CCA is sent.
- After a SAPC initiated reauthorization. Whether a Gx-RAR message is sent or not, the notification policies are always evaluated and the notification is triggered if applies.
- After a Fair Usage reauthorization.

Time and date conditions in notifications policies do not trigger sending any notification.

When one of the previous events is triggered, the SAPC performs the selection and evaluation of the applicable notification policies. Notification messages are then sent for those policies that meet the conditions and the notification has not been already sent.

As summary, the notification policies are always evaluated when the SAPC answers a Gx-CCA message or when the SAPC initiates a reauthorization.

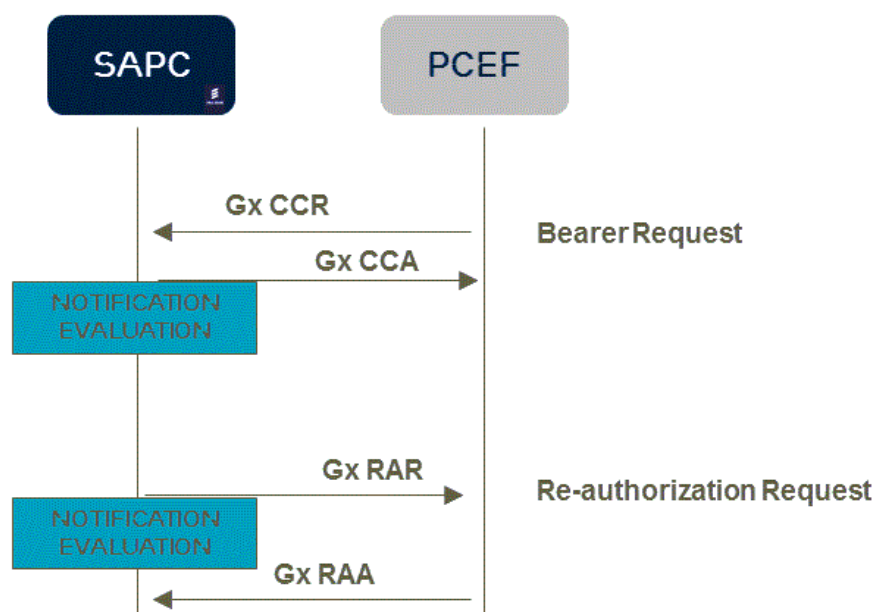


Figure 3 Triggers for Notification Policies Evaluation

It is important to highlight that notification policies evaluation is always done after the corresponding message has been sent to the PCEF to avoid affecting the performance.

Notification policies are evaluated by the SAPC in the same way as it is done for the rest of policies, so every condition that can be used in the rest of policies can also be used in the notification ones. In fact, taking into account that the SAPC



makes PCC decisions based on such dynamic conditions, operator can decide to configure the same conditions in the notification policies to alert the user whether the SAPC requests the PCEF to enforce such decisions.

Even though the SAPC notifications are intended to notify a destination about a change in the subscriber service conditions, not all the notifications sent by the SAPC have to be linked to some policy enforcement requested by the node. Notifications can be also related to some events received in the IP Session which can have no action in the SAPC, for example, a change in the roaming conditions or the surpassing of intermediate limits.

For the sake of clarity, some typical examples of SAPC notifications are described below.

- Whenever any of the usage limits (either volume or time) are surpassed per reporting period or per session and reporting group.

The SAPC allows also the configuration of intermediate limits. The usage of this intermediate limits is very useful, for example to handle the roaming data bill shock prevention use case.

Operators in the European Union are obliged by law to agree a specified bill threshold, after which the customer is automatically cut-off from their data connection while roaming following a warning. The warning comes when 80% of the limit is reached. See in the next figure a diagram with an example of this case:

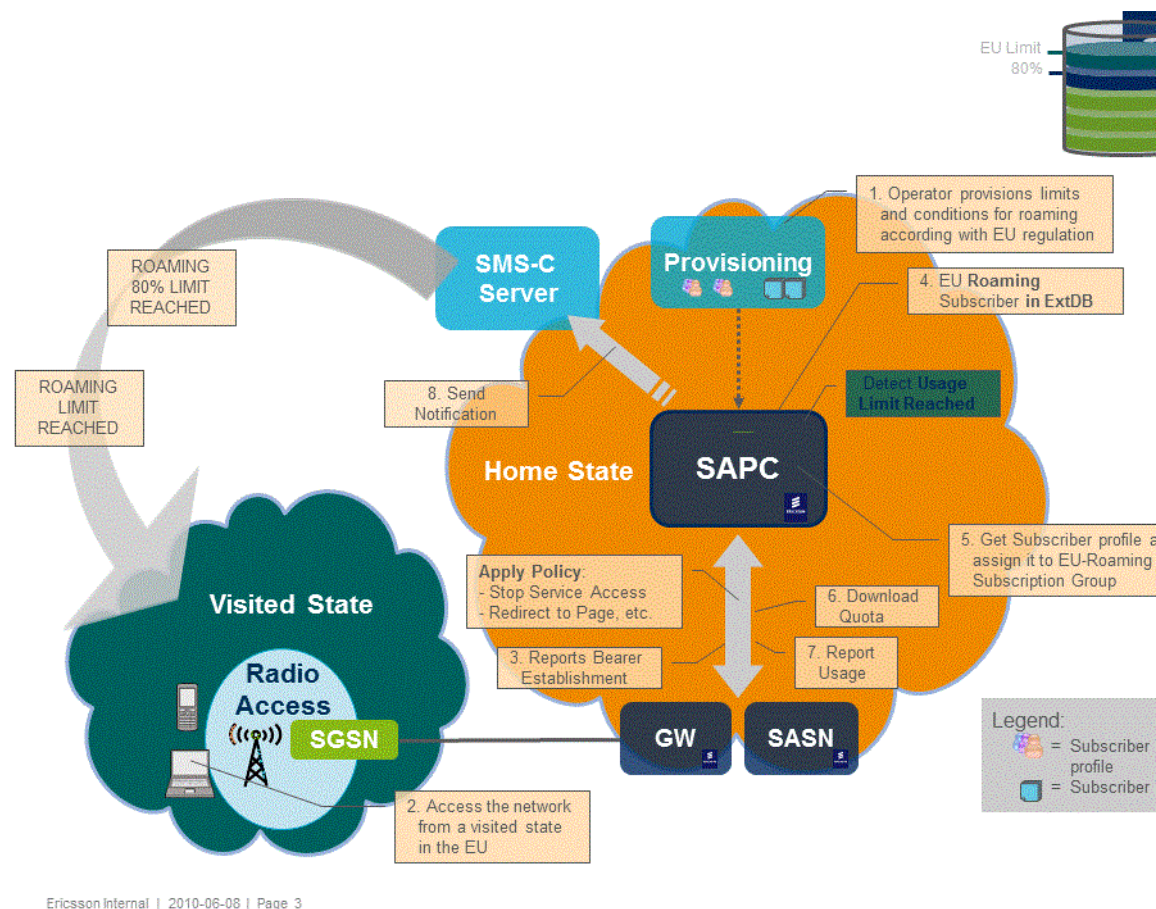


Figure 4 Bill Shock Prevention Traffic Case

- Whenever a usage limit/intermediate limit is surpassed in case of Shared Subscriber Plans.

The SAPC allows, among others, to notify the owner/head (the one paying for the Shared Subscriber Plan) when any of the subscribers sharing the plan reaches the limit, to notify both the owner/head and the subscriber reaching the limit, or only to the subscriber reaching the limit.

- Whenever an IP Session is not authorized

For example, if an IP Session should not be authorized when the user is roaming out of the home area, a policy for bearer access control must be configured including a rule with this condition. If a notification message should be sent to alert the user when this restriction is applied, a different policy for notifications must be configured in the SAPC, including a rule with the same condition than the one for bearer access control. In this way, every time the policy conditions for the first policy (bearer access control) are fulfilled, it is also fulfilled the conditions for the second one (notifications) and the notification is sent when the access bearer is restricted (only in case the same notification was not already sent for the same conditions as explained in Section 2.7 on page 9).



- Whenever a service access is restricted
- Whenever a bandwidth restriction is applied
- Whenever the Quality of Service (QoS) is upgraded or downgraded
- Whenever the user is doing roaming

Even when the SAPC does not perform any enforcement related with this condition, it could be interesting for the user to be notified when the roaming condition is satisfied

- Whenever a subscriber group becomes active or inactive for the subscriber.

2.5 Notification Message Text

The SAPC also allows the configuration of the text to send in each notification. Using the output attribute of the rules, the operator can send a customized description of the event produced in each case. Configured text for each notification can also include dynamic information by using any of the policy engine supported functions and tags. For example, the text to send in a notification could include the MSISDN.

Multi-language character sets are allowed in the text of the notifications. SMS and SOAP mechanisms support ASCII and UTF-8 character encoding. For SMS Notifications, owing to SMPP protocol limitations, if ASCII is used, up to 160 characters can be included in the SMS. But, if UTF-8 is used, the amount of characters fitting in an SMS is reduced to 70. If more than 160 or 70 characters respectively are used, then the SMS is truncated into several messages. The number of available characters per segment is 153 and 67 characters respectively.

2.6 Notification Messages to Multiple Destinations

The SAPC allows operator to send notification messages to multiple destinations when an event related to a subscriber occurs. The SAPC supports the following combinations regarding notification destinations and messages:

- Sending a notification message to one end user or to an external system.
- Sending the same notification message to several end users or external systems: this includes sending the same notification message to one/several end users and to one/several external systems.
- Sending different notification messages to different destinations (statement valid only for external systems).



2.6.1 Notification Messages Sent to End Users

The SAPC allows configuring several MSISDN per each subscriber as destination. When a notification is triggered, the SAPC sends notification messages towards all the destinations configured for such subscriber.

Moreover, it is also possible to configure at subscriber group level that notifications for all subscribers belonging to this subscriber group are to be sent to the MSISDN received in the protocol message for this subscriber, simplifying greatly the configuration of destination addresses for subscribers. If there is at least one destination addressed configured at subscriber level, notifications are not sent to the MSISDN received in the traffic message; notification configuration at subscriber level takes precedence over the notification configuration at group level.

All applicable notifications for a subscriber are always sent to all configured destination addresses.

2.6.2 Notification Messages Sent to External Systems

The SAPC allows operators to send notification messages to one or several external systems. An external system is configured as part of a Notification Receiver. A Notification Receiver groups the destination addresses of the external systems together with the mechanisms to use for sending the notification messages (SMPP or SOAP protocol).

2.7 Notification Message Control

For each subscriber that the notification policies are evaluated over, the SAPC maintains a control of the notification messages sent to avoid that the same notification message is sent several times for that subscriber under the same conditions. When the conditions that have launched certain notification cease, the SAPC triggers the notification again if the conditions are fulfilled any time afterwards.

The SAPC identifies the notification messages sent as follows:

- If the notification is sent to an end user, the notification message is identified by the text within the notification message itself. For this reason, it is important to configure always a different text for every subscriber notification; in other case, some notifications may not be sent. In case the same policy for a notification returns a different message in each different evaluation owing to the inclusion of some dynamic text, the SAPC handles them as different notifications.
- If notification is sent to external systems, the notification message is identified using the identifier of the Notification Receiver.

The next figure describes the steps included in the execution of the SAPC notification control:

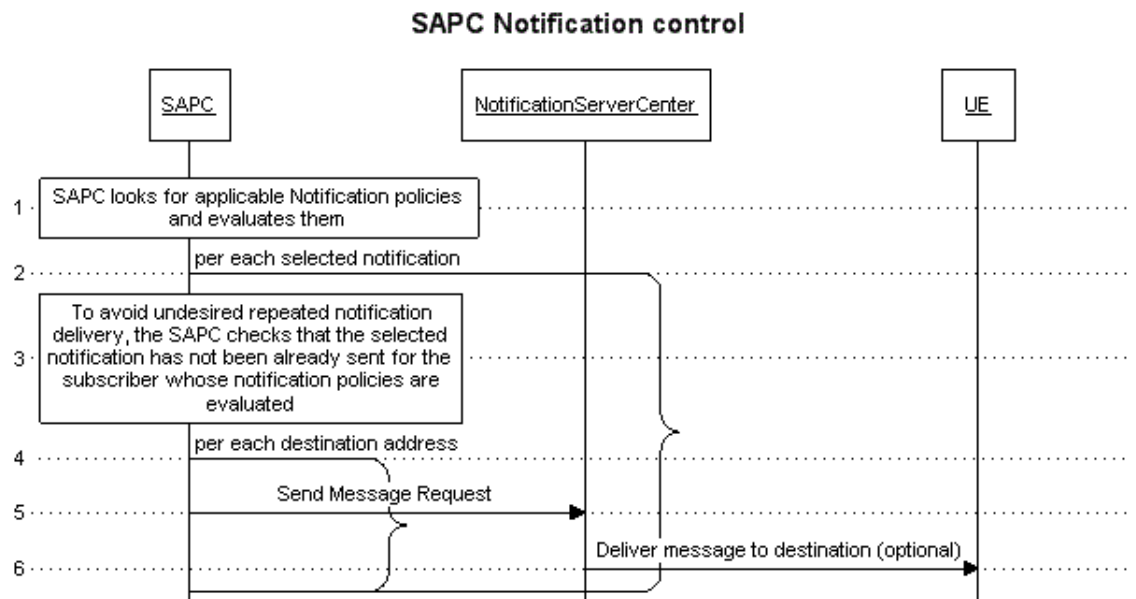


Figure 5 SAPC Notification Control

If several notification mechanisms are configured for a destination, the SAPC iterates through the notification mechanisms, sending a notification message to every address configured at notification mechanism.

- 1.-The SAPC looks for the applicable notification policies for the affected subscriber and evaluates them. The output of the policy may provide a notification to send, the message to use in the notification and the destination address. A single policy can imply sending several notifications messages.
- 2-6: For each selected notification
 - 3.- To avoid undesired repeated notification delivery, the SAPC checks that the selected notification has not already been sent for the subscriber whose notification policies are evaluated.
 - Note:** This means that, in case the configured notification destination addresses are the same for different subscribers, the same notification could be received several times for the same destination address.
 - 4-6: For each destination address:
 - 5.- The SAPC sends the appropriate notification message to the Notification Server Center, including the message content as configured by the operator (obtained as output attribute of the rule).
 - 6.- The Notification Server Center may deliver the message to the selected destination.

For example, if there is a notification to send to an end user because the usage limit has been surpassed, the event is notified just once to the subscriber receiving



the usage reporting when the limit is surpassed for the reporting period, see next figure.

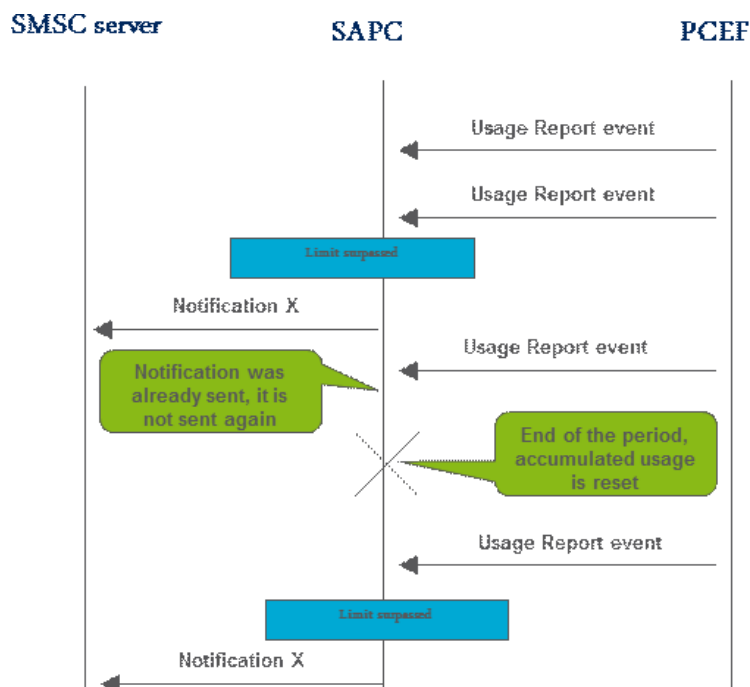


Figure 6 Avoiding Sending the Same Notification Twice

The next time a usage reporting event is received for this subscriber in the same reporting period and the condition for the notification is fulfilled, the SAPC realizes this notification message was already sent for this subscriber, and the event is not be notified again until the accumulated usage is reset at the end of the reporting period and the limit is reached again at next billing period.

Other example could be a notification owing to a roaming condition. If a notification is configured to be sent to an end user and to an external system when a subscriber is out of the home area, notification is only sent once to each destination when the user roams out of this area. Each time the SAPC evaluates again this policy when the user is roaming, the condition is fulfilled but the notification is not sent. When the subscriber is back to the home area and roams again then a new notification is sent.

In the case of notifications about active or inactive subscriber groups, if a notification is configured to be sent to an end user and to an external system when a group becomes active/inactive for the subscriber, the notification is sent only once to each destination when the group becomes active/inactive for the subscriber.

If the same policy for a notification returns a different message in each different evaluation owing to the inclusion of some dynamic text, the SAPC handles them as different notifications. For example, this is the case when a notification should be sent every time a subscriber establishes a new IP session in a roaming scenario; including only static text the SAPC only sends a notification message for the first



session. However, including the IP address as part of the text (assuming each different session is using a different IP address) the SAPC handles the same notification as different ones because the resulting text in each case is different. In that case, a notification message is sent every time a new session is established for the subscriber out of the home area.

If the destination address is updated for a destination (list of SMS), the list of sent notifications for such destination is deleted, so the same notification could be sent to the new destination address. This behavior is useful if a notification has been sent to an incorrect address and the destination address is corrected.

2.8 Notification Sending Procedure

2.8.1 Notification Queue Management

Before sending notifications to the notification address, the SAPC schedules the notifications in a queue following a First-In First-Out (FIFO) strategy: There is one single notification queue for the SMS notifications and there is one queue for every external system configured. The SAPC allows up to a maximum number of notifications in every queue, default value 2000 (configured by Ericsson personnel).

The notifications stored in the queue are concurrently sent to the notification address through several connections. The maximum number of concurrent notifications delivered depends the number of connections established with the notification server.

One important issue worth mentioning is the way notifications generated by the Notification Policies evaluation are handled. The SAPC logic may generate so many notifications that surpass the notification delivery capacity of the SAPC. In such case, the SAPC prioritizes the notifications to deliver: Newer notifications take precedence over older notifications.

For this reason, when there are so many notifications to be delivered as consequence of having configured so many notifications in the logic or because the Notification Server cannot cope with the amount of notification traffic, it may happen that some notifications are dropped.

A notification may be dropped when one of the following conditions occurs:

- Notification not delivered owing to internal buffer overflow. If the queue is full and a new notification needs to be scheduled, the SAPC removes the oldest notification in the queue, issuing a logging event and stepping up the measure of failed notifications by one.
- Notification not delivered because the SAPC may be overloaded
- Notification not delivered owing to network / server problems (issuing a logging event)



2.8.2 Notification Server Connection Management

Whenever the SAPC sends a notification, the SAPC uses an SMPP / HTTP connection towards the notification address. An SMPP / HTTP connection is established when the first SMS/SOAP notification message is to be sent. Such connection may be reused when delivering further SMS/SOAP notification messages (the same connection may be reused by different subscribers).

The number of established connections which is a dynamic value is directly dependent on the SAPC load at the moment and the network delay between the SMS-Center / SOAP Notification Server and the SAPC.

If all the established connections are in use (this means that the SAPC is using every established connection for sending one notification request) and the number of connections established has not reached the maximum allowed number of connections, default value 50 (configured by Ericsson personnel), the SAPC tries to establish a new connection to the notification address.

If all the established connections are in use (this means that the SAPC is using every established connection for sending one notification request) and the number of connections established has reached the maximum allowed number of connections, the SAPC will not be able to create a new connection to the notification address, and the SAPC inserts this notification again in the FIFO queue (at last position) if there is room for this notification.

Also, the SAPC periodically checks the connection status, default value 60 seconds (configured by Ericsson personnel), releasing connections not used during a certain period, default value 5 minutes (configured by Ericsson personnel), or occasionally used and hanged up (connections established between the SAPC and the notification server with broken status but not correctly released) during at least 30 seconds.

2.8.3 Connection Error Handling

When sending a notification or when attempting to establish a connection to the notification address, the SAPC waits for the acknowledgment during a time-out period, default value 5 seconds.

The SAPC attempts to establish the connection up to a maximum number of times, default value 3 (configured by Ericsson Personnel).

After the connection is established, the notification is tried to send up to the maximum number of retries, default value 3.

If the connection is not established after the connection reattempts, or the connection is established but the notification delivery fails (an error is received at protocol level), the SAPC inserts this notification in the FIFO queue at the last position if there is room for one more notification.

The errors which cause the SAPC to insert the notification in the notification queue are the following:



— SMPP Protocol:

- SYSTEM ERROR
- MESSAGE QUEUE FULL
- SUBMITTING MESSAGE HAS FAILED
- THROTTLING ERROR
- ESME RECEIVER TEMPORARY ERROR
- ESME RECEIVER REJECT MESSAGE ERROR
- MESSAGE QUERY REQUEST FAILED
- TRANSACTION DELIVERY FAILURE
- UNKNOWN ERROR

— HTTP Protocol

- Any error different from 400, 401, 403, 404, 405, 406, 407, 410, 413, 414, 415, 416, 417, 418, 422, 423, 424, 5xx

— SOAP Protocol

- No SOAP error code causes the notification to be inserted: The notification is discarded.

If all connection establishment attempts or all notification delivery attempts fail, the notification is not delivered and the logging event is issued. A connection is considered broken when no response is received after the maximum number of delivery attempts is reached.

If no connection can be established with the notification address, an alarm is raised. After the alarm is raised, to avoid flooding the notification address with connection establishment attempts raised at every notification delivery attempt, the SAPC attempts to establish the connection at regular time intervals, default value 4 seconds (configured by Ericsson personnel), when new notifications need to be sent. The alarm is cleared once the SAPC successfully sends a notification to the corresponding notification address.

A Server Address is considered unavailable in the following cases:

- During new connection establishment towards a Notification Address: After the maximum number of configured consecutive failed connection attempts when there is not any established connection towards this Notification Address, SAPC marks the Server Address as unavailable. New notifications are not delivered towards this Server Address but towards other available Server Addresses belonging to the same Notification Server. If there is not an available Server Address, the notifications are inserted in the notifications queue.



- When using a broken connection: This scenario comprises the situation where a notification server goes down and ongoing connections exist. In this case, the following situations may happen:
 - When trying to use an ongoing connection, the delivery of the notification fails. This ongoing connection is dropped out, since it is useless (issuing a logging event).
 - When trying to use an ongoing connection, the delivery of the notification fails and it is the last connection towards a Notification Address. Then, the Notification Address is considered unavailable. An alarm informing about this situation is raised.

2.9 Load Balancing Mechanism

The SAPC implements a load balancing mechanism for delivering notification towards a configured Notifications Server. The load balancing mechanism used by the SAPC distributes the delivery of notifications among the set of configured Notification Addresses, belonging to a Notification Server, using the so-called round robin algorithm.

Load balancing mechanism implemented by the SAPC comprises:

- The SAPC delivers the notifications evenly among the available configured Notification Addresses until loss of connectivity of one Notification Address.
- When the SAPC detects one of the configured Notification Addresses is not available (see Section 2.8 on page 12), the SAPC stops sending further notifications towards that Notification Address. An alarm informing about this situation is raised (one alarm for each unavailable Notification Address). The notifications are sent to the rest of available Notification Addresses.
- When the connection towards a Notification Address is restored, the SAPC starts again sending notifications towards this Notification Address. Notifications are evenly distributed between the previous Notification Addresses and the new available Notification Address. The availability of the Notification Address is checked at regular time intervals, default value 4 seconds (configured by Ericsson personnel).

The following picture depicts how the round robin algorithm is implemented by the SAPC:

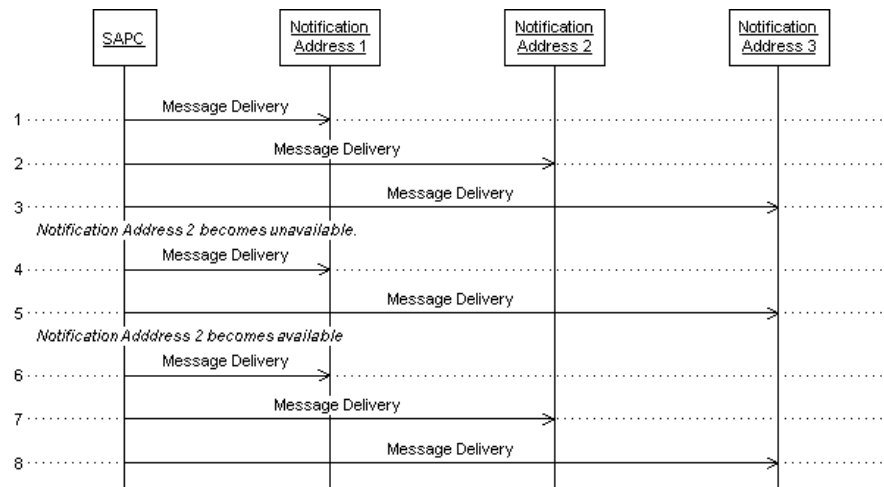


Figure 7 Load balancing mechanism

As precondition, it is assumed that the operator has configured three Notification addresses belonging to the same Notification Address where Notifications are delivered.

- Steps 1–3: Initially, all addresses are available. As consequence, the SAPC delivers the notifications evenly among the notifications addresses, following a round robin algorithm:

- Step 1: One notification is delivered to Notification Address 1.
- Step 2: Another notification different than the notification in step 1 is delivered to Notification Address 2, which is the next available Notification Address.
- Step 3: Next notification to be sent by the SAPC is delivered to the Notification Address 3, which is the next available Notification Address.

After having sent one notification towards each notification Address, the next round implies sending the next set of notifications to each available Notification Address following the same order and repeating the sequence depicted in steps 1–3.

- Steps 4–5: The Notification Address 2 becomes unavailable, and for this reason, notifications are sent only to Notification Address 1 and Notification Address 3.
- Steps 6–8: Once the Notification Address 2 becomes available, the notifications are sent to Notification Address 1, Notification Address 2, and Notification Address 3 following the round robin algorithm.



3 Traffic Cases

This chapter explains the interfaces involved in sending user notifications and the common traffic case for notifications.

The notification traffic case can be triggered for two different reasons as described in Section 2.4 on page 4, the reception of a bearer event from the PCEF and other events producing SAPC reauthorizations.

Next figure describes how the SAPC executes notification control in both scenarios:

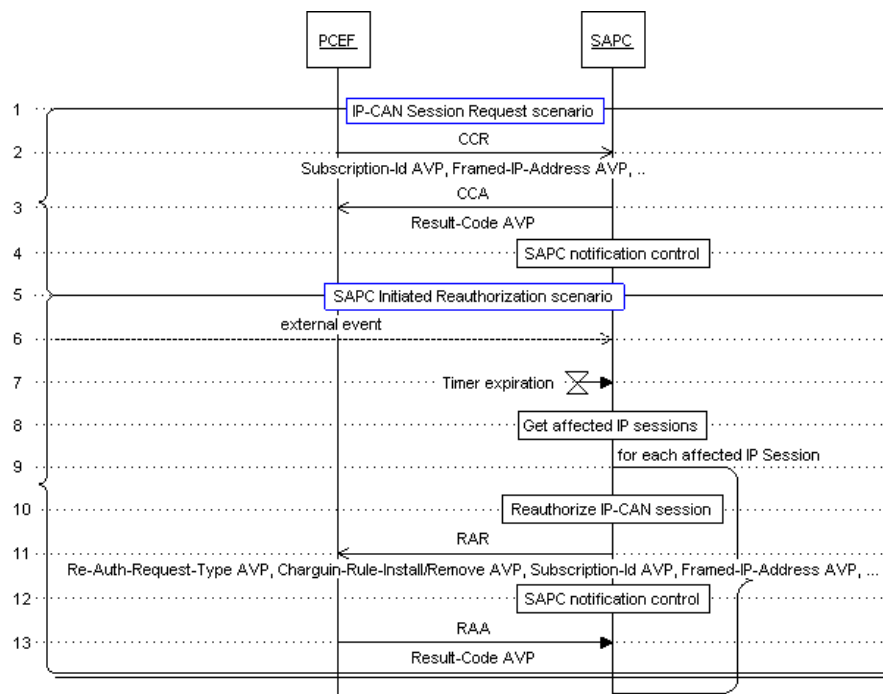


Figure 8 Traffic Case for Notifications

As it is shown in the previous figure (steps 6 and 7), the SAPC reauthorization can be triggered by the reception of an external message (for example, a NetConf message updating the user profile or a Gx-CCR for usage reporting when some limit is surpassed) or an internal event as a timer expiration.

It is important to take into account that events triggering reauthorization could affect more than one IP session, therefore notification policy evaluation is performed once per each affected IP session.

The notification control is executed after the Gx-CCA message is sent back to the PCEF. In a SAPC initiated reauthorization scenario, the notification control is performed after the corresponding Gx-RAR message is sent or when the reauthorization process finishes.



The communication towards the corresponding notification server center is described in next sections.

3.1 SMS

If the SMS Notification mechanism is configured, then the SAPC sends the notification message to the configured SMSC center using SMPP protocol version 3.4.

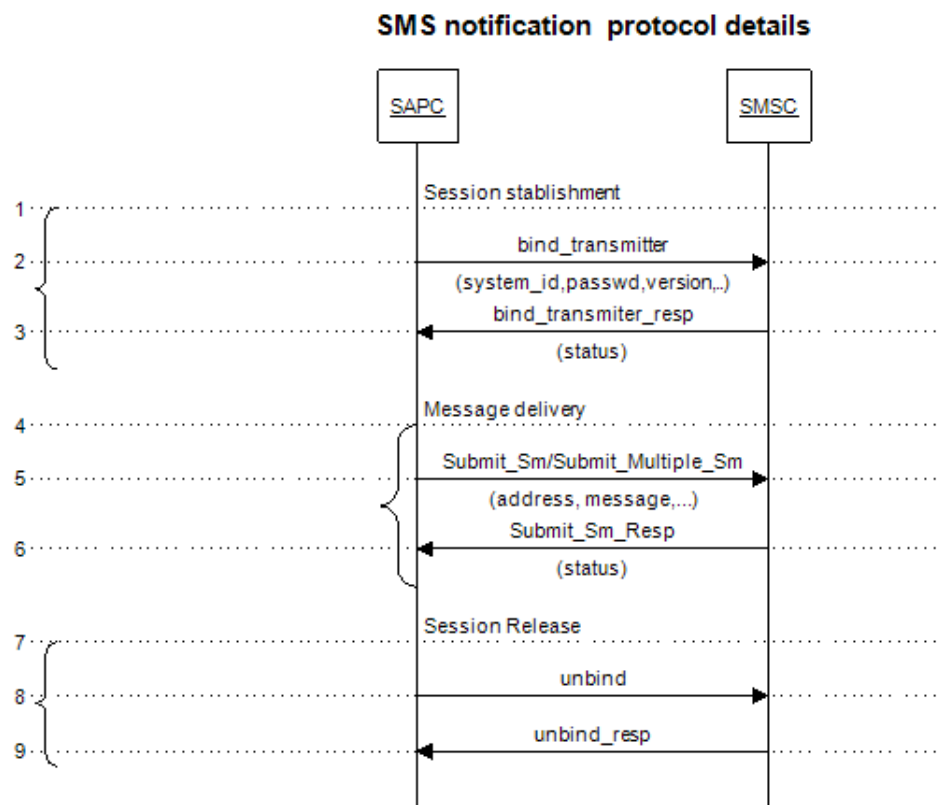


Figure 9 SMS Protocol Binding

- 1-3: Session establishment procedure is performed in case there is not a session established yet:
 - 2.- `Bind_transmitter` Protocol Data Unit (PDU) is sent to the SMSC including the following parameters
 - **System_id**: SAPC identifier towards the SMSC included in the SMSC configuration.
 - **Password**: the password included in the SMSC configuration.
 - **System_Type**: NULL.



- **interface_version**: value 0x34 indicating SMPP version 3.4.
- **addr_ton**: 0x0 value indicating Unknown.
- **addr_npi**: 0x0 value indicating Unknown.
- **address_range**: NULL.
- 3.- Bind_transmitter_Resp PDU is received with the status of the operation.
- 4-6: Message delivery procedure contains the interactions needed to perform the message delivery to the SMSC.
- 5.- Submit_sm (or Submit_multi_sm when there are multiple destination addresses for the message) PDU is sent including the following parameters:
 - **service_type**: NULL.
 - **source_addr**: NULL.
 - **number_of_dests**: It is only included if Submit_multiple_sm is used and includes the number of different destinations for the message.
 - **destination_addr**: Destination address (or addresses if Submit_multiple_sm is used) for the short message. The value can be taken from the configured MSISDN value included in the applicable notification data (for subscriber, subscriber group or notification receiver) or from the one included in the traffic message.
 - **esm_class** = It indicates Message Mode (always Default SMSC Mode) and Message Type (always Default Message type).
- Note:** UDHI flag is set to zero.
- **protocol_id**: GSM.
- **priority_flag**: non-priority.
- **schedule_delivery_time**: NULL (immediate message delivery).
- **validity_period**: NULL.(SMSC default validity period)
- **registered_delivery**: 0x00. The SAPC does not request any SMSC delivery receipt, so no notification is received in the SAPC after SMSC deliver the message to the end user.
- **replace_if_present_flag**: 0x00 (Don't replace, default value).
- **data_coding**: 0x00 (SMSC Default Alphabet).
- **sm_default_msg_id**: NULL (not canned message).



- **short_message**: UTF-8 encoding is supported. The length of the notification for different languages varies. If the maximum number of characters is reached, several short messages are sent.
 - **sm_length**: Length of short message user data.
 - Optional parameters: **sar_msg_ref_num**: originator generated reference number allowing the parallel transmission of several segmented messages, **sar_total_segments**: the total number of fragments within the concatenated short message, and **sar_segment_seqnum**: the sequence number of a particular message within the concatenated short message, are used to deliver concatenated messages.
- 6.- Submit_sm_resp (or Submit_multi_sm_resp when there were multiple destination addresses) PDU is received including the status of the request.
- 7-9: Session release block is not performed after the delivery of a message but after an inactivity period of 5 minutes.
- 8.- Unbind PDU is sent
 - 9.- Unbind_resp PDU is received

The enquire link commands are used to check the connectivity between the SAPC and SMSC. **Enquire_link** message can only be issued from SMSC and is answered back by the SAPC with resp: "Ok".

3.2 SOAP

SOAP mechanism is configured at Notification Receiver level, as a subscriber is not able to receive a SOAP notification message. SOAP mechanism is intended to send notifications to an external system (web server). As an example, these notifications can be used by the operator for statistical purposes. The SOAP notification is sent to the Web Service End Points configured through the Notification Receiver.

The text in a SOAP notification message must follow the SOAP syntax. The next figure shows an example:



```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-Instance">
  <soap:Body>
    <SAPCNotification>
      <Header>
        <from> SAPC </from>
        <to> Webserver1 </to>
      </Header>
      <Message>
        <MSISDN> 447773609630 </MSISDN>
        <queryString> Quota limit reached, IMSI=123456789 </queryString>
      </Message>
    </SAPCNotification>
  </soap:Body>
</soap:Envelope>
```

Figure 10 Example of SOAP Notification Message

More details about the structure of the SOAP notification message can be found in Configuration Guide for End User Notifications

SOAP uses HTTP as transport protocol. The protocol versions used are SOAP 1.1 and HTTP 1.1. Persistent connections are the default behavior of any HTTP connection in HTTP 1.1, so once a connection is established, several SOAP notification messages may be sent using that connection. For more information, refer to Reference [5].

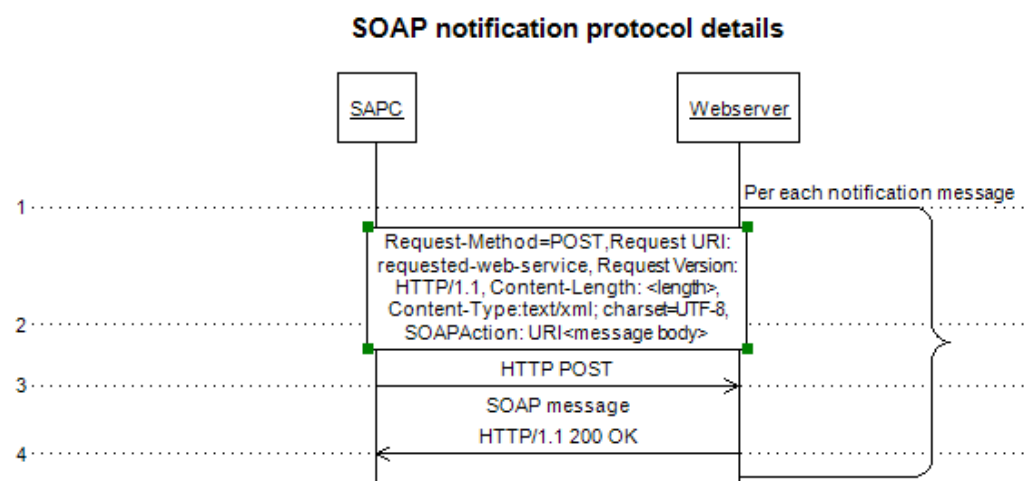


Figure 11 SOAP over HTTP Protocol Case

See more details about the structure of the SOAP notification message in Reference [4].



4 Capabilities

Several notification connections per payload processor may be established towards the Notification Server. The number of notification connections established towards the Notification Server depends on the amount of Notifications to deliver.

5 Restrictions

The following restrictions are applicable to User Notifications

- Time and date conditions in notifications policies do not trigger sending any notification.
- User notifications are only sent for subscribers with an active Gx session.

6 Security

It is supported user and password authentication when sending messages to the SMPP notification servers.

Information contained in notifications may be confidential. For this reason, it is highly recommended to implement IPsec between both parties of the communication channel (the SAPC and the Notification Server).



Glossary

IMSI

International Mobile Subscriber Identity

IPsec

Internet Protocol Security

MSISDN

Mobile Subscriber ISDN Number

PDU

Protocol Data Unit

QoS

Quality of Service

SMPP

Short Message Peer-to-Peer

SMS

Short Message Service

SMSC

Short Message Service Center

UTF

Unicode Transformation Format





Reference List

Ericsson Documents

- [1] Subscription and Policy Management
- [2] Configuration Guide for End User Notifications

Standards

- [3] 3GPP TS 23.040, V12.2.0 . Technical realization of the Short Message Service (SMS)
- [4] Simple Object Access Protocol (SOAP) 1.1, W3C Note 08 May 2000
- [5] Hypertext Transfer Protocol -- HTTP/1.1, RFC 2616
- [6] The TLS Protocol, version 1.0, RFC 2246

Online References

- [7] SMPP Developers Forum, http://docs.nimta.com/SMPP_v3_4_Issue1_2.pdf