SMPP Server User Guide

Version 3.0

Whilst the greatest care has been taken to ensure the accuracy of the information contained herein, NRSGATEWAY does not warrant the accuracy of same. NRSGATEWAY expressly disclaim all and any liability to any person, whether a purchaser of the publication or not, in respect of anything and of the consequences of anything, done or omitted to be done by any such person on reliance, whether whole or partial, upon the whole or any part of the contents of this publication.

Contents

Introduction

SMPP means Short Message Peer to Peer, (SMPP), protocol is an open industry standard messaging protocol designed to simplify integration of data applications with wireless mobile networks such as GSM, TDMA, CDMA and PDC. The protocol is widely deployed in the mobile telecommunications industry. The SMPP protocol specification is freely available from http://www.smpp.org

NRSGATEWAY currently supports version 3.3 and 3.4 of the SMPP protocol.

Requirements

The following requirements must be met to enable the sending of short messages (SMS) via NRSGATEWAY Connectivity:

- You need a customer account
- You need sufficient credit on your NRSGATEWAY Connectivity customer account

Access to the NRSGATEWAY services is subject to our general terms and conditions of business.

Please address technical questions by email to:

sms-support@nrs-group.com

You can reach our technical hotline under the following telephone number:

902 014 480 (from Spain) or +34 964 523 331 (from abroad)

Monday to Friday between 9:00am-07:00pm, CET

Glossary

The parameters used in the NRSGATEWAY SMPPServer:

- **SMS:** Short Message Service
- **PDU:** Protocol Description Unit (way how the SMSs are sent)
- **DR:** Delivery Report notification
- **SMPPServer:** SMPP Server that allows to the clients to send SMSs
- **SMPPClient:** Client that wants to send SMSs through our SMPPServer
- **IP:** IP number where the SMPPServer is hosted*
- **Port:** Connection port that the SMPPServer is listening*
- **System_id:** unique system ID sent to the SMPPClient in a confidential mail
- **Password:** unique system password sent to the SMPPClient in a confidential mail
- **Client_id:** Client identifier provided to the SMPPClient
- **Account_id:** Account identifier when the credits will be charged
- **System_type:** Identifies the type of ESME system requesting to bind as a transmitter with the SMSC. We will use this parameter to specify client_id and account_id.

* NRSGATEWAY will provide you with the IP address and port number

Technical information

The GSM specifications have limited the Short Message from the SMSC to the handset to 140 octets. If 7 bit encoding is used we may deliver 160 characters to the handset, otherwise for 8 bit data the maximum number of characters will be limited to 140.

The character sets supported by NRSGATEWAY Platform are GSM7, UCS2 and ISO-8859-1 (ISO Latin 1)

The SMPPServer allows the SMPPClient to send SMSs. This implies that the SMPPClient must connect to the SMPPServer using some PDU connection parameters.

Connection configuration

- **SMPP Bind Type:** Transceiver or transmitter & receiver
- **Asyncrhonous outstanding operations window**: 10
- **SMPP Version:** 3.3 or 3.4
- **Max allowed sessions per server:** 2

Mandatory parameters

- **Host:** smppv5.nrs-group.com
- **Port:** 5091
- **Port SSL**: 6091
- **System_id:** alphanumerical secret string that will be given to the SMPPClient by phone, email or SMS
- **Password:** alphanumerical secret string that will be given to the SMPPClient by phone, email or SMS

Other recommended parameters

- **bind-mode:** transceiver
- **sync-mode:** async
- **addr-ton:** 1
- **addr-npi:** 1
- **source-ton:** 5
- **source-npi:** 0
- **destination-ton:** 1
- **destination-npi:** 1

Message encoding

- **data-coding:** 0 (for GSM7 encoding)

SMPP TON/NPI Parameters

SMPP parameter	Type of address	TON	NPI
Destination address	Always international	1	1
Source address	International	1	1
	National/shortcode	2	1
	Alphanumeric	5	0

International originators
Source address and destination address in international format shall not contain any leading "+" or "00", but only starting with the countrycode.

Sample International Source Address
Displayed on handset: +34609939891
SMPP Parameter: TON = 1
NPI = 1
SOURCE_ADDRESS = "34609939891"

Alphanumeric originators
Length of an alphanumeric originator is limited to 11 characters; this limit is set by the pertinent GSM Standards.

Error Codes

Bind Response error codes

Error Code	Error Name	Description	Action
0x00000000	OK	Message received and processed	
0x0000000D	ESME_RBINDFAIL	Bind failed (login/bind failed – invalid login credentials or login restricted by IP address)	Verify System_id value and send the proper value
0x0000000E	ESME_RINVPASWD	Invalid password (login/bind failed)	Verify password value and send the proper value
0x0000000F	ESME_RINVSYSID	Authentication failure	Check username, password, client ID and account ID

Submit Response Error codes

Error Code	Error Name	Description
0x00000000	OK	Message received and processed
0x00000401	NO_CREDIT	Account does not have credits
0x000000FE	Delivery Failure	The message can't be routed to SMSC or Gateway. The main reason from that can be internal server issues, losing connection with the SMSC, routing errors or others.
0x00000009	Airbag error	Indicates that the same message has sent more than 3 times within less than 30 minutes. It is considered that the message is the same when the sender, destination and the text are also the same. The objective of this “antifloof” mechanism is avoid possible errors from the client who send the same message several times and avoid loopings
0x0000000A	Invalid Source Address	Invalid Source Address
0x0000000B	Invalid Dest Addr	Invalid Dest Addr
0x00000402	Invalid message	The message has invalid message length.

Delivery Reports

SMPPServer provides for return of an SMSC delivery receipt via the **deliver_sm** or **data_sm** PDU, which indicates the delivery status of the message.

The informational content of an SMSC Delivery Receipt may be inserted into the **short_message** parameter of the **deliver_sm** operation. The format for this Delivery Receipt message is SMSC vendor specific but following is a typical example of Delivery Receipt report:

“id:IIIIIIIIII sub:SSS dlvrd:DDD submit date:YYMMDDhhmm done date:YYMMDDhhmm stat:DDDDDDD err:E Text: . . . .”

The fields of the above delivery receipt example are explained in the following table:

Field	Size(octects)	Type	Description
id	10	C-Octet String (Decimal)	The message ID allocated to the message by the SMSC when originally submitted.
sub	3	C-Octet String (Decimal)	Number of short messages originally submitted. This is only relevant when the original message was submitted to a distribution list.The value is padded with leading zeros if necessary.
dlvrd	3	C-Octet String (Decimal)	Number of short messages delivered. This is only relevant where the original message was submitted to a distribution list.The value is padded with leading zeros if necessary.
submit date	10	C-Octet Fixed Length String	The time and date at which the short message was submitted. In the case of a message which has been replaced, this is the date that the original message was replaced.The format is
done date	10	C-Octet Fixed Length String	The time and date at which the short message reached it’s final state. The format is the same as for the submit date.
stat	7	C-Octet Fixed Length String	The final status of the message.
err	3	C-Octet Fixed Length String	Where appropriate this may hold a Network specific error code or an SMSC error code for the attempted delivery of the message. These errors are Network or SMSC

			specific and are not included here. Probably in next versions this section will be more specified.
text	20	Octet String	The first 20 characters of the short message.

Message States

Message State	Final Message states	DESCRIPTION
DELIVERED	DELIVRD	Message is delivered to destination
EXPIRED	EXPIRED	Message validity period has expired
DELETED	DELETED	Message has been deleted
UNDELIVERABLE	UNDELIV	Message is undeliverable
ACCEPTED	ACCEPTD	Message is in accepted state (i.e. has been manually read on behalf of the subscriber by customer service)
UNKNOWN	UNKNOWN	Message is in invalid state
REJECTED	REJECTD	Message is in a rejected state

Action For Submit Response Error Codes

Billing

When client receives NO_CREDIT error messages,

- Stop sending further messages
- contact call center

Binding Guidelines

Only one session is available for systemID provided to the client.

- When session drops(due to network fluctuation or planned unbind), before rebinding to the server, the client application should wait for 60 sec before issuing the bind request
- The session should not drop frequently. Once bind, session should stay for long time rather than issuing bind request.
- Client should not attempt to spam the server with bind request.
- Before unbind, client should issue unbind request to the system

Enquirelink - Keep Alive Signal

- The Enquirelink signal should be sent for every 30 sec. Otherwise client session will be dropped by the NRSGATEWAY platform
- Client should not attempt to spam the server with Enquirelink request.

Resolving Bind Problems

- First try to ping server IP:

  Ex: ping smppv5.nrs-group.com

  If you are not able to ping Sever IP, contact customer care.
- If ping is Successful do telnet

  Ex: telnet smppv5.nrs-group.com <port> . If you are not able to do telnet, contact customer care
- If you get any error bind response, please check the error code against the error codes mentioned in the section 5.1
- If all confirmations are correct and still you are facing problems in binding, please contact customer care who will redirect you to the technical department.

Frequently Asked Questions

- How Long Should The ESME Application Wait For A submit_sm_response?

  Server provides response in transaction mode. I,e, response from the operator itself. This depends on the operator delay. Otherwise a better option is to send the messages in the async manner.

- What IS "Enquire_Link" And Do I Need To Support It?

  This command is used to provide a confidence-check of the communication path between ESME and the SMSC. All SMPP sessions on the SMSC are configured with an 80 seconds idle timeout. All ESMEs are expected to initiate an enquire_link every 30 seconds to ensure the session is not closed by the SMSC during idle periods