



SMPP PLATFORM

USER GUIDE

Version 1.0

Whilst the greatest care has been taken to ensure the accuracy of the information contained, 360NRS does not warranty the accuracy of this user guide. 360NRS 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

1. Introduction	Page 3
1.1 Requirements	Page 3
2. Glossary	Page 4
3. Technical information	Page 5
3.1 SMPP TON/NPI Parameters	Page 7
4. Error Codes	Page 8
4.1 Bind Response error codes	Page 8
4.2 Submit Response Error codes	Page 8
5 Delivery Reports	Page 9
6 Message States	Page 10
7 Action for Submit Response Error codes	Page 10
7.1 Billing	Page 10
8 Binding Guidelines	Page 11
9 Enquirelink - keep alive signal	Page 11
10 Resolving bind problems	Page 11
11 Frequently Asked Questions	Page 12

1 INTRODUCTION

SMPP means Short Message Peer to Peer, (SMPP), this 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>

360NRS currently supports version 3.3 and 3.4 of the SMPP protocol.

1.1 REQUIREMENTS

The following requirements must be met to enable the sending of short messages (SMS) via 360NRS Connectivity:

- You need a customer account
- You need enough credit on your 360NRS Connectivity customer account

Access to the 360NRS services is subject to our general terms and conditions of business.

Please send any technical questions by email to:

tech@360nrs.com

You can reach our technical hotline or 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

2 GLOSSARY

The parameters used in the 360NRS SMPPServer:

Parameter	Description
SMS	Short Message Service
PDU	Protocol Description Unit (the way how the SMSs are sent)
DR	Delivery Report notification
SMPPServer	SMPP Server that allows the clients to send SMSs
SMPPClient	Clients that wants to send SMSs through our SMPPServer
IP	IP number where the SMPPServer is hosted *
Port	Connection port that the SMPPServer is connectected *
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 are charged
System_type	Identifies the type of ESME system requesting to bind as a transmitter with the SMSC. This parameter is used to specify client_id and account_id.

* 360NRS will provide you with the IP address and port number

3 TECHNICAL INFORMATION

The GSM specifications have limited the Short Message from the SMSC of 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 characters supported by 360NRS 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

Asynchronous outstanding operations window: 10

SMPP Version: 3.3 or 3.4

Max allowed sessions per server: 2

Mandatory parameters

Hosts: You can connect to any of the following servers. The ESMSC can only get delivery report by the server that has accepted the message.

If you want to use both servers at same time you need to connect a transceiver or receiver to each server to ensure the receipt of all delivery reports.

89.17.205.211 (primary server)

89.17.205.234 (backup server)

Port: 5091

System_id: alphanumeric secret code that will be given to the SMPPClient by phone, email or SMS

Password: alphanumeric secret code 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)

data-coding: 3 (for ISO-8859-1)

data-coding: 8 (for UTF-16)

When data-coding is set to ISO-8859-1 text is transliterated to avoid errors when text is internally transcoded to GSM7. The table of equivalence is:

"á"=>"a", "í"=>"i", "ó"=>"o", "ú"=>"u", "ç"=>"Ç", "Á"=>"A", "Í"=>"I", "Ó"=>"O", "Ú"=>"U", "À"=>"A", "È"=>"E", "Ì"=>"I", "Ò"=>"O", "Ù"=>"U", "Õ"=>"O", "â"=>"a", "ê"=>"e", "î"=>"i", "ô"=>"o", "û"=>"u", "Â"=>"A", "Ê"=>"E", "Î"=>"I", "Ô"=>"O", "Û"=>"U", "ã"=>"a", "Ã"=>"A"

3.1 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”, only the countrycode is needed.

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.

4 ERROR CODES

4.1 Bind Response error codes

Error Code	Error Name	Description	Action
0x00000000	OK	Message received and processed	1
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

4.2 Submit Response Error codes

Error Code	Error Name	Description
0x00000000	OK	Message received and processed
0x00000401	NO_CREDIT	Account does not have enough 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 "anti-flood" 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.

5 DELIVERY REPORTS

SMPPServer provides a 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 specific vendor but below there is a typical example of Delivery Receipt report:

“id:IIIIIIII sub:SSS dlvr: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.
dlvr	3	C-Octet String (Decimal)	Number of short messages delivered. This is only relevant when 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 when the short message was submitted. In the case of a replaced message, this is the date that the original message was replaced.
done date	10	C-Octet Fixed Length String	The time and date when 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	This may be a Network specific error code or an SMSC error code for the attempted delivery of the message. These errors are Network or SMSC related and are not included in here. <u>Probably in next versions this section will be more specified.</u>
text	20	Octet String	The first 20 characters of the short message.

6 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 status (i.e. has been manually read on behalf of the subscriber by customer service)
UNKNOWN	UNKNOWN	Message is in invalid status
REJECTED	REJECTD	Message is in a rejected status

7 ACTION FOR SUBMIT RESPONSE ERROR CODES

7.1 Billing

When client receives **NO_CREDIT** error messages,

1. Stop sending further messages
2. Contact call center

8 BINDING GUIDELINES

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

1. 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.
2. The session should not drop frequently. Once binded, session should stay for long time rather than issuing bind request.
3. Client should not attempt to spam the server with bind request.
4. Before the unbinding, client should issue unbind request to the system.

9 ENQUIRELINK - KEEP ALIVE SIGNAL

1. The Enquirelink signal should be sent every 30 sec. Otherwise client session will be dropped by the 360NRS platform.
2. Client should not attempt to spam the server with Enquirelink request.

10 RESOLVING BIND PROBLEMS

1. First try to ping server IP:
Ex: ping 89.17.205.211
If you are not able to ping Sever IP, contact customer care.
2. If ping is Successful do telnet
Ex: telnet 89.17.205.211<port> . If you are not able to do telnet, contact customer care.
3. If you get any error bind response, please check the error code with the error codes mentioned in the section 5.1
4. If all confirmations are correct and you are still facing binding problems, please contact customer care who will redirect you to the technical department.

11 FREQUENTLY ASKED QUESTIONS

1. 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 better option is to send the messages in the async manner.

2. 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 60 seconds to ensure the session is not closed by the SMSC during idle periods