



**Advanced Services SMS Gateway
HTTP Interface (Simple)
For
Sending & Receiving SMS**

Revision 4.0

October 2004

CONTENTS

1. ACCESS TO HSL SMS GATEWAY SERVICE.....	3
1.1. OPENING AN ACCOUNT.....	3
2. EXAMPLE CODE	3
3. SENDING SMS.....	4
3.1. SECURITY AND AUTHENTICATION	5
3.2. RESPONSE FROM ACTIONS	5
3.3. PARAMETER DEFINITIONS	6
3.4. ACTIONS	9
3.4.1. <i>sendtxt – Sending a simple text message</i>	9
3.4.2. <i>sendnok – Sending Nokia Smart Messaging SMS</i>	10
3.4.3. <i>submitsm – Send raw SMS</i>	11
3.4.4. <i>senducs – Sending multi-byte text messages (UCS2)</i>	12
3.4.5. <i>senddgram – Sending a message</i>	13
3.4.6. <i>querysm – Query the delivery status of a message</i>	14
4. RECEIVING SMS	15
4.1. URL FIELDS.....	15
4.2. RETRIES ON CUSTOMER SERVER UNAVAILABILITY.....	15
4.3. MESSAGE ENCODING	15
4.4. DELIVERY RECEIPTS	15

1. Access to HSL SMS Gateway Service

Hay Systems Ltd (HSL) provides access to its systems using the HTTP interface in this document to enable client applications to send SMS to mobile devices. In order to use the specification in this document it is necessary to have an account with HSL for access to this service.

For further information on HSL's services, other interface protocols, service levels and global coverage please see <http://www.hslsms.com/>.

1.1. Opening an account

To open an account for access to HSL's systems for delivery of messages to mobile devices please complete and return HTTP service application form.

The HTTP service application form can be found in the **Apply** section of the HSL SMS website at <http://www.hslsms.com/>.

2. Example code

Example code can be found on the HSL website at <http://www.hslsms.com/> in the **Sample Code** sub-section of the **Developers** section.

3. Sending SMS

This document includes the actions that can be used to send text messages (Western character sets or Unicode), binary messages and Nokia Smart Messaging content using SMS to mobile phones on mobile networks supported through HSL's systems. These actions create single or multiple SMS messages depending on the parameters.

A regular HTTP POST or GET can be used by a client application to perform an action to send SMS using the SMS gateway HTTP interface. The parameters necessary for each action are shown in the following table (M – mandatory; O – optional):

	sendtxt	sendnok	submitsm	senducs	senddgram	querysm
clientid	M	M	M	M	M	M
password / key	M	M	M	M	M	M
destaddr	M	M	M	M	M	
srcaddr	O	O	O	O	O	
validity	O	O	O	O	O	
scheduled	O	O	O	O	O	
text	M	O				
message			M	M	M	
content		M				
netct		O ¹				
netcn		O ¹				
type		M				
esmcclass			O			
dcs			O		O	
pid			O		O	
regdeliv	O	O	O	O	O	
srcport					O	
destport					O	
msgid						M

¹ Mandatory for operator logo.

The URL that is used has the following format:

http://<server>[:<port>]/<action>/
 or
 https://<server>[:<port>]/<action>/ (secure HTTP)

Following the set-up of your account the actual **server**, **port**, **clientid**, **password** and **secret** for use in the actions for sending SMS will be provided by HSL.

3.1. Security and authentication

The encryption of communication between the application making the request and HSL's systems is achieved through HTTPS.

There are two methods available to the application of authenticating when using HTTP or HTTPS: password or MD5. Either the password or the MD5 method **MUST** be used when submitting a HTTP request.

PASSWORD: A password is included in the parameters (the **password** field) submitted with the HTTP request. The password is assigned when the account is provisioned by HSL. It should be noted that this password is passed "in the clear" (unencrypted) when using HTTP. If HTTPS is used the password will be encrypted.

MD5: An MD5 message digest is included in the parameters (the **key** field) submitted with the HTTP request. The MD5 "message digest" is a 16-byte output calculated from a "secret" known to both the application sending the HTTP request and HSL's server, and other parameters associated with the action. The actual parameters and how the input to the MD5 calculation should be performed are included in the sections below describing the supported actions. Note that the "secret" is **never** passed between the application and HSL "in the clear" – it is used as a seed in the MD5 calculation along with other parameters. The "secret" and parameters are concatenated together to provide the input to the MD5 calculation. The MD5 algorithm is included in various SDKs and programming languages (C/C++, Delphi, Java, JavaScript, PHP, Perl, VB). The MD5 algorithm is defined in <http://www.ietf.org/rfc/rfc1321.txt>.

The IP address of the application making the request can optionally also be verified against the account details known to HSL's server and used to authenticate the user. Requests coming from an application connecting from an IP address other than that set-up in an account will be rejected. IP addresses for applications authorised to make use of a client's account must be provided to HSL so that they can be entered into the account configuration.

3.2. Response from actions

After an action has been sent by the HTTP client application, the action will be performed and a response given back to the HTTP client. The response given will indicate the success or failure of the request and will be returned within the body (or data part) of the HTTP response.

response = [success-response | failure-response]*

success-response = SUCCESS [<SP> message-id]*

failure-response = FAIL [<SP> AUTH | <SP> **error**]

error = value indicating the error code returned from the transaction as defined in section 5.1.3 of the SMPP v3.4 specification (<http://www.smsforum.net/>)

The "FAIL AUTH" response indicates that your **clientid** and **password / key** combination are incorrect.



3.3. Parameter Definitions

Parameter	Description	Type and Example
clientid	Client identifier. Identifier to uniquely identify your account.	String e.g. client-abcd
password	Account password.	String e.g. 1h8g234m5
key	MD5 of action fields and secret. Fields used as input to MD5 are listed in action descriptions in the next section. The <secret> parameter used as the input to the MD5 calculation is never exchanged in the open and is provided to the client by HSL when service is first provisioned.	Hex string e.g. 85943d91966a91e613b5f936c62bd417
destaddr	Mobile telephone number(s) in international format starting with first digit of country code. More than one number can be specified by separating each number by a comma. Destination TON of "international" and NPI of "E.164" automatically selected.	Digits e.g. 4479123456789 or 4479123456789,4479123456789
srcaddr	Originating address or source address of short message. (Support for this parameter is subject to account configuration.) Source TON and NPI will be automatically set.	String (alphanumeric address has max. 11 characters) e.g. BrandName
validity	The expiration time (absolute or relative) of the message. Same as for SMPP validity_period parameter as in section 7.1 of the SMPP v3.4 specification. Alternatively, HTTP absolute date format supported.	String e.g. 0411241134000+
scheduled	The time (absolute or relative) that message delivery is to be attempted. Same as for SMPP schedule_delivery_time parameter as in section 7.1 of the SMPP v3.4 specification. Alternatively, HTTP absolute date format supported.	String e.g. 0411241134000+
text	Short message text in ISO 8859-1.	String e.g. Hello world!
message	Short message.	Hex string



		<p>e.g.</p> <p>003000310032</p> <p>or</p> <p>024A3A6D35A5CDCD2985 8DADCDBDB80400B698E2 EC517624CB14658936C5 96614616614616814616 828DB12658B2CC28C2CC 28C2CC28C2D051B624BA 146E0B2D029024C25428 C2C4497617217628BB12 658A32C49B62CB30A30B 30A30B40A30B4146D893 2C596614616614616814 616828DB125D0A370596 814812812A14616224BB 0000</p>
content	<p>type = rt</p> <p><ringing-tone-programming-language> as in Nokia Smart Messaging Specification for Ringing Tones (hex string); or RTTTL/RTX encoding of ring tone (character string)</p> <p>type = c1</p> <p><ota-bitmap> as in Nokia Smart Messaging Specification for Graphical Logos and Icons (hex string). Supports OTA, BMP and PBM formats.</p> <p>type = pg</p> <p><ota-bitmap> as in Nokia Smart Messaging Specification for Graphical Logos and Icons (hex string). Supports OTA, BMP and PBM formats.</p> <p>type = o1</p> <p><ota-bitmap> as in Nokia Smart Messaging Specification for Graphical Logos and Icons (hex string). Supports OTA, BMP and PBM formats.</p>	<p>Hex string or character string</p> <p>e.g.</p> <p>024A3A6D35A5CDCD2985 8DADCDBDB80400B698E2 EC517624CB14658936C5 96614616614616814616 828DB12658B2CC28C2CC 28C2CC28C2D051B624BA 146E0B2D029024C25428 C2C4497617217628BB12 658A32C49B62CB30A30B 30A30B40A30B4146D893 2C596614616614616814 616828DB125D0A370596 814812812A14616224BB 0000</p> <p>or</p> <p>MyTune:d=4,o=5,b=112: b.6,g.6,16f#6,16g6,1 6f#6,8d.6,8e6,p,16e6 ,16f#6,16g6,8f#.6,8g 6,8a6,b.6,g.6,16f#6, 16g6,16f#6,8d.6,8e6, p,16c6,16b,16a,16b</p>
netcn	Network code for GSM network.	<p>2 x digits</p> <p>e.g. 10</p>
netct	Country code for GSM network.	<p>3 x digits</p> <p>e.g. 244</p>
type	<p>rt – ringtone</p> <p>c1 – group graphic</p> <p>pg – picture message</p>	<p>2 x character</p> <p>e.g. rt</p>



	o1 – operator logo	
esmclass	Message type. Same as for SMPP esm_class parameter.	Integer (decimal) e.g. 0
dcs	Indicates data coding scheme and/or message class. Same as for SMPP data_coding parameter in SMPP v3.4.	Integer (decimal) e.g. 0
pid	Protocol ID value. Same as for SMPP protocol_id parameter as for SMPP v3.4 / GSM.	Integer (decimal) e.g. 0
regdeliv	Request delivery receipt when message reaches completion. 0 – no delivery receipt 1 – delivery receipt requested Delivery receipts will be returned to the same URL as used when receiving inbound SMS. The format of the receipt is as in <i>Appendix B of the SMPP v3.4 specification</i> . Note the “id” field in the delivery receipt will contain the whole message identifier originally returned at the time of message submission. A message that has been delivered will contain the text “stat:DELIVRD” within the received message. See Receiving SMS section for further information.	Integer (decimal) e.g. 1
srcport	Source port for datagram. See GSM 03.40.	Integer (decimal) e.g. 1024
destport	Destination port for datagram. See GSM 03.40.	Integer (decimal) e.g. 1024
msgid	Message identifier from previous submission.	Hex string e.g. 12345678abcdef12

Note: The SMPP (Short Message Peer to Peer) protocol specifications are freely available for download at <http://www.smsforum.net/>.

3.4. Actions

3.4.1. sendtxt – Sending a simple text message

ACTION

sendtxt

PURPOSE

Submit an SMS text message to the gateway using a simple HTTP request. A message that exceeds 160 characters will be split into multiple SMS and a UDH containing segmentation and reassembly information will be added (concatenated SMS).

PARAMETERS

Parameter	Description
destaddr	Mobile telephone number(s).
text	Short message text in ISO 8859-1.
scheduled	The time (absolute or relative) the message delivery is to be attempted.
validity	The expiration time (absolute or relative) of the message.
srcaddr	Originating address or source address of short message. (Subject to account configuration.)
regdeliv	Request delivery receipt when message reaches completion.
key	<secret><text><destaddr>

3.4.2. sendnok – Sending Nokia Smart Messaging SMS

ACTION

sendnok

PURPOSE

Send Nokia Smart Messaging ringtones, operator logos, group graphics (CLI icons) and picture messages.

This action will produce a single or multiple SMS messages containing the content. The necessary segmentation and reassembly information will be included in the SMS messages that are produced for messages that require more than one SMS.

PARAMETERS

Parameter	Description
destaddr	Mobile telephone number(s).
type	rt – ringtone cl – group graphic pg – picture message ol – operator logo
content	type = rt <ringing-tone-programming-language> as in Nokia Smart Messaging Specification for Ringing Tones (hex string); or RTTTL/RTX encoding of ring tone (character string). type = cl, pg or ol <ota-bitmap> as in Nokia Smart Messaging Specification for Graphical Logos and Icons (hex string). Supports OTA, BMP and PBM formats.
netcn	Network code for GSM network (mandatory for operator logos).
netct	Country code for GSM network (mandatory for operator logos).
text	Text message for picture message (where type=pg).
key	<secret><type><content><text><netct><netcn><destaddr> <u>Absent parameters in HTTP request:</u> If no <text> parameter is provided this is assumed to be NULL (i.e. empty). If no <netct> parameter is provided this is assumed to be “000”. If no <netcn> parameter is provided this is assumed to be “00”.

3.4.3. submitsm – Send raw SMS

ACTION

submitsm

PURPOSE

Submits an SMS to the gateway using a method that is functionally equivalent to SMPP submit_sm PDU in SMPP v3.4.

PARAMETERS

Parameter	Description
destaddr	Mobile telephone number(s).
message	Short message.
esmclass	Message type.
dcs	Indicates data coding scheme and/or message class.
pid	Protocol ID value.
scheduled	The time (absolute or relative) the message delivery is to be attempted.
validity	The expiration time (absolute or relative) of the message.
srcaddr	Originating address or source address of short message. (Subject to account configuration.)
regdeliv	Request delivery receipt when message reaches completion.
key	<secret><message><destaddr>

3.4.4. senducs – Sending multi-byte text messages (UCS2)

ACTION

senducs

PURPOSE

Send a text message using UCS2 character encoding using a simple HTTP request. A message that exceeds 70 UCS2 characters will be split into multiple SMS and a UDH containing segmentation and reassembly information will be added (concatenated SMS).

This action allows messages composed of Unicode characters (includes Arabic, Chinese, Greek characters) to be sent using SMS.

PARAMETERS

Parameter	Description
destaddr	Mobile telephone number(s).
message	Short message text in Unicode format using UCS2 data coding.
scheduled	The time (absolute or relative) the message delivery is to be attempted.
validity	The expiration time (absolute or relative) of the message.
srcaddr	Originating address or source address of short message. (Subject to account configuration.)
regdeliv	Request delivery receipt when message reaches completion.
key	<secret><message><destaddr>

3.4.5. senddgram – Sending a message

ACTION

senddgram

PURPOSE

Send a message payload via SMS. A message that exceeds 160 characters or 140 octets will be split into multiple SMS and a UDH containing segmentation and reassembly information will be added (concatenated SMS). This action could be used to send a WAP push message or other similar content.

PARAMETERS

Parameter	Description
destaddr	Mobile telephone number(s).
message	Message content.
scheduled	The time (absolute or relative) the message delivery is to be attempted.
validity	The expiration time (absolute or relative) of the message.
srcaddr	Originating address or source address of short message. (Subject to account configuration.)
regdeliv	Request delivery receipt when message reaches completion.
srcport	Source port.
destport	Destination port.
dcs	Indicates data coding scheme and/or message class.
pid	Protocol ID value.
key	<secret><message><destaddr>

3.4.6. querysm – Query the delivery status of a message

ACTION

querysm

PURPOSE

Queries the status of a message that was previously submitted using one of the other actions contained in this document.

PARAMETERS

Parameter	Description
msgid	Message identifier of previously submitted message.
key	<secret><msgid>

4. Receiving SMS

The HTTP interface allows SMS received by a mobile application number allocated by HSL to a client to be relayed to the client's application. Received SMS can be relayed by HSL calling a URL that has been supplied by the client. This URL can be a PHP, ASP, Java servlet or other page and can be used to process inbound SMS received on a virtual mobile number or SIM.

4.1. URL Fields

When an SMS is received on a number allocated to a customer a HTTP request is made by HSL's systems to relay the mobile number receiving the SMS (recipient), the SMS message text (message) and the mobile number of the sender of the message (mobilenumber).

The following fields are passed to the customer supplied URL using the HTTP GET method:

mobilenumber	Mobile number of sender
message	Message text
recipient	Mobile number receiving message (e.g. virtual mobile number)
charset	Character set of message ISO8859-1 (default) or UCS2

The charset field may be omitted from the request. When this is the case the character set of the message is ISO 8859-1.

In order for HSL's servers to determine that your server has received the SMS from our systems a HTTP "200" response must be given. On receiving this response from a call to your URL our servers will not retry delivery of the message.

4.2. Retries on Customer Server Unavailability

The default behaviour is for HSL's systems to attempt delivery for up to 4 hours if your URL is not reachable or is not responding correctly when we relay a received SMS. After this period of time the received message will not be retried and will be deleted.

4.3. Message encoding

The message field will be URL encoded for transport over HTTP. This means that you can expect all non-printable and special characters to be represented by the character sequence "%nn" where nn is the hexadecimal value of the character. It is necessary to decode the received message prior to further processing of the message.

For example, the message "Hello world" would be encoded as "Hello%20world" where %20 represents the space character. In ISO 8859-1 the space character has value 0x20 (32 decimal).

4.4. Delivery receipts

Receipts indicating the outcome of a sent message, as a result of setting the regdeliv parameter, are formatted according to *Appendix B of the SMPP v3.4 specification*.