sinch

User Guide - API Specification Push (v3.6)

Document Control

Document Name	User Guide - API Specification – Push
Document Reference Number	Sinch India-Guide-ISMS-Push API Specification
Classification	Confidential
Initial Release Date	10/08/2005
Owner	Rahul Singh

Revision History

Version	Description	Reviewed By	Review Date	Approved By	Approve Date
1	First release	Pranay Saxena	10/8/2005	Pranay Saxena	10/8/2005
1.1	SI push incorporated	Pranay Saxena	15/05/2006	Pranay Saxena	15/05/2006
1.2	# Introduction of parameter “Subappid” in section “Push using XML” #Introduction of more error & codes # Description of parameters in section “push using XML” added	Pranay Saxena	10/7/2006	Pranay Saxena	10/7/2006
1.3	DRM Content Support	Pranay Saxena	25/02/2007	Pranay Saxena	25/02/2007
1.4	DND Check	Pranay Saxena	5/10/2007	Pranay Saxena	5/10/2007
1.5	One-2-One Messaging Functionality	Pranay Saxena	6/6/2008	Pranay Saxena	6/6/2008
1.6	Error Codes Implemented	Rashmi Mishra	30/06/2008	Rashmi Mishra	30/06/2008
2	Introduction of Language parameter, error codes, post method	Rashmi Mishra	7/10/2015	Rashmi Mishra	7/10/2015
2.1	Added short URL API parameters with samples and error codes	Rashmi Mishra	1/5/2017	Rashmi Mishra	1/5/2017
2.2	Added samples of http(s) request URLs	Rashmi Mishra	28/08/2019	Rashmi Mishra	28/08/2019
2.3	Added App URL	Rashmi Mishra	21/09/2019	Rashmi Mishra	21/09/2019
3	# Introduction of additional Error code & description. # Introduction of synchronous and asynchronous Error code & description in JSON. # Added support for JSON data type. # Added support for AES 256encryption in JSON data type.	Rashmi Mishra	9/1/2020	Rashmi Mishra	9/1/2020
3.1	Push JSON API now supports bulk request up to 10,000	Rashmi	27/03/2020	Rashmi	27/03/2020

	records in a single request.	Mishra		Mishra	
3.2	Implemented DLT template Scrubbing -Included DLT Parameters	Rashmi Mishra	10/3/2021	Rashmi Mishra	10/3/2021
3.4	Added support for # Scheduling # Pull DLR – async	Rashmi Mishra	23/6/2021	Rashmi Mishra	23/06/2021
3.5	# Added support for cancellation API # Updated the scheduling signature. # Added support for sync. Fetch DLR API # Change the doc format	Rashmi Mishra	27/08/2021	Rashmi Mishra	27/08/2021
3.6	# Updated SMS Gateway error codes # Added support for DLT DLR parameters	Rahul Singh	14/08/2021	Rahul Singh	14/08/2021

Distribution

- Email Communication
- Printed Copy
- File Server

Documentation status

This is a controlled document. This document may be printed; however, any printed copies of the document should be controlled. The electronic version maintained in the file server.

Abbreviations, Acronyms & Definitions

IS	Information Security
ISMS	Information Security Management System
IT	Information Technology
OTP	One-Time-Password
SMS	Short Message Service
SMPP	Short Message Peer to Peer
MNO	Mobile Network Operator
DLR	Delivery Receipt
ISDN	International Services Digital Network
PRI	Primary Rate Interface
MSISDN	Mobile Subscriber International Services Digital Network
SMSC	Short Message Service Centre
HLR	Home Location Register

MSC	Mobile Switching Centre
VLR	Visitor Location Register
Trans	The message due to some transaction with the merchant
Promo	Marketing Messages
Unicode	Multilingual Message Text
DLT	Distributed Ledger Technology
PE	Principal Entity

Table of Contents

1. Introduction

This document outlines the specification of Managed Mobility to PUSH messaging system.

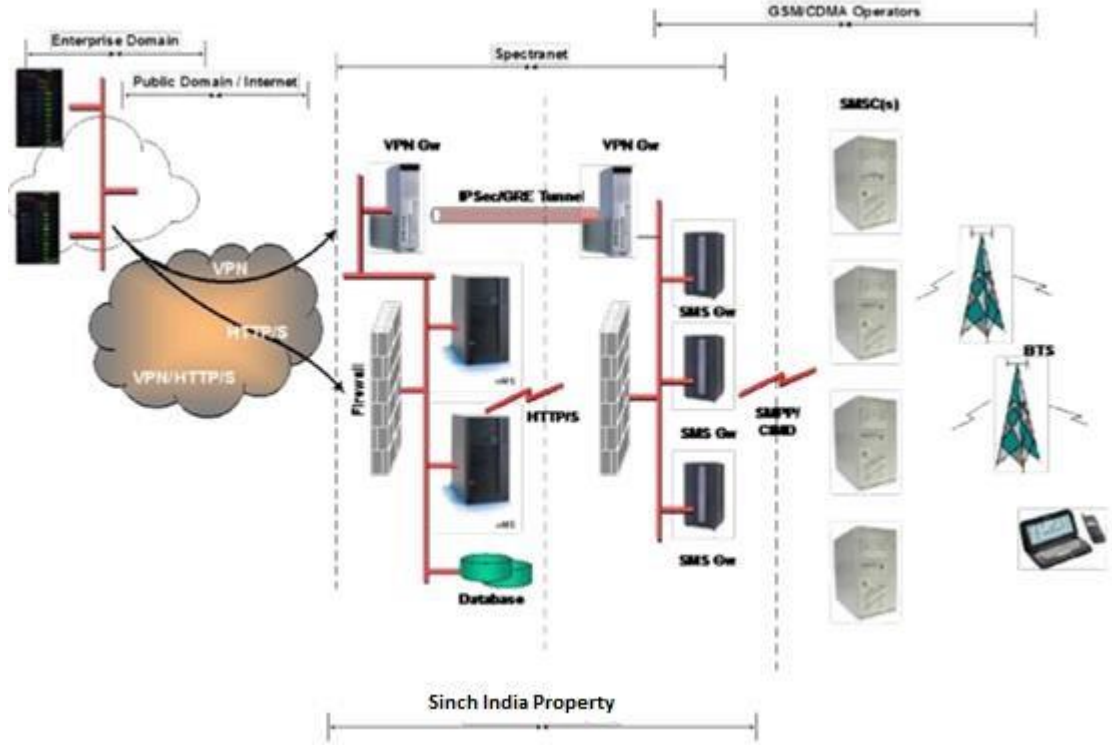
The target audience of this document is internal customers, stakeholders, Sinch India existing andpotential Enterprise Customers.

2. Functional Model

The following diagram depicts the interaction domains of the Enterprise, Sinch India SMS Gateway,and the Operator's delivery infrastructure. The domain of responsibilities, namely, Enterprise, Service Provider and Cellular Operator, has been distinctly segregated in the visualization.

3. Protocol Support

This section details the various protocol supports across domains of the functional model.



3.1. Gateway Connectivity with SMSC(S)

Sinch India’s Push SMS Gateway connects to the SMSC using standard and universallyaccepted protocol - SMPP 3.3 / 3.4.

3.2. Enterprise Connectivity to Sinch India’s Push Platform

Enterprise customers connect to the push platform, over the public domain, via – https protocol.

4. Service Infrastructure Redundancy

It is Sinch India continuous endeavor to attain the highest levels of customer satisfaction. From a service delivery point of view, it has built-in fault tolerance, to mitigate service disruptions, on the connectivity, messaging platform, SMS gateways and SMSC accounts front.

4.1. Enterprise Connectivity

The first point of failure for the Service is connectivity to Sinch India’s SMS Push Platform.For this redundancy to be realized, it is imperative that the customer extends its choice of connectivity (HTTPS) over the public domain and configures, if required, the backup connection at its end in a standby ready state.

Note: This might require that the customer have a redundant / failover WAN connectivity viasome internet provider's international gateway.

4.2. Sinch India Push Platform

Availability of the Sinch India platform is critical towards the success of the Messaging Service. To overcome any unforeseen and untimely shortcoming on this front, Sinch Indiahas hosted redundant (standby) server(s) at Class-I Data Centre.

4.3. SMS Gateways

Multiple SMS gateways are configured in redundant and standby modes within theOperators domain, to alleviate service disruption due to binding problems with the SMSC(s).

Cautiously, Sinch India has also positioned some SMS gateway(s) within the ISP's premise to avoid the remote possibility of service disruption due to interconnect problemsbetween the ISP and the Operator.

4.4. SMSC(S)

Referring to Figure above service delivery of the highest order is ensured by multiple SMPP connectivity(s), procured by Sinch India, from all the Cellular Operators in the domestic arena

ensuring load sharing during peak hours and in situations of traffic congestion at theprimary operators end.

5. Push Messaging Specification

Sinch India connectivity platform provides two methods for pushing SMS. For an enterprise to send A2P SMS using Sinch India SMS gateway following is recommended to enterprise.

- The enterprise must register with DLT as a Principal Entity
- The PE must register the SMS template with the DLT under Principal Entity.
- The PE must register the sender's name with the DLT under Principal Entity.
- The PE must map the template and the sender's name with the DLT.
  Any sender name (CLI) and SMS template if not registered with DLT, the request will be rejected by Mobile Number Operator.

5.1. Push using URL

Enterprise can push message through URL using the GET method.

5.1.1. Push URL [GET method]

Choosing GET as the "method" will append all the data to the URL; hence it is restricted to only 1024 characters.

Sinch India provides following URLs that take few parameters as a query string for pushing the message.

https://push3.aclgateway.com/servlet/com.aclwireless.pushconnectivity.listeners.TextListener?appid=xxxx&userId=xxxx&pass=xxxx&contenttype=1&from=xxxx&to=91XXXXXXX&text=this is a demo message with url
https://abcd.com/accountdetails?account=123456.&alert=1&selfid=true&intflag=false&language=hi&s=1&f=1&dpi=xxxxxx&dtm=xxxxxx&tc=xxxxxx

5.1.2. Parameter Description

Following are the list of supported parameters with description:

S.No.	Parameter Name	Parameter Description	Criteria*
1	userId	User Id provided by SINCH INDIA to an enterprise for authentication	M
2	pass	Password provided by SINCH INDIA for authentication of User Id	M
3	appid	Application Id associated with an enterprise, provided by SINCH INDIA	O

4	subappid	If Enterprise has subdivisions, then provided by SINCH INDIA for a particular division	O
5	msgid	The unique id for every request sent to the SMS gateway. The value will be generated by the gateway, when the selfid is false. Max length allowed is 100 and data type is string.	O
6	to	The Mobile number(s) where SMS to be sent. For more than one Mobile number comma used asa separator. e.g.,9810790950,9810549171	M
7	from	Sender id to be sent with the SMS.	M
8	contenttype	“1” for text SMS. Details as mentioned below	M
9	selfid	It should be set “true”, SINCH INDIA platform maps a message id along with the request	M
10	text	Message Text	M
11	auth	These are dummy fields, with max allowed length as 50. If not provided app id is passed.	O
12	subauth	These are dummy fields, with max allowed length as 50. If not provided subapp id is passed.	O
13	brd	The is a campaign name with the max allowed limit as 50. If not provided, the systems allocates the name.	O
14	dpi	DLT principal entity ID	O
15	dtm	DLT template ID	O
16	tc	Template category Transactional – the value to-be sent is 1 Promotional – the value to-be sent is 2 Service Implicit – the value to-be sent is 3Service Explicit – the value to- be sent is 4	O
17	intflag	the identifier for domestic and international traffic	O
18	alert	To be set either 0 or 1, by default its value will be 0 means request will pass through DND Check.	O
19	language	The language parameter is used to convert English message with whitelisted template to be delivered in a regional language. The regional language template needs to be pre-configuredwith us. The specific language to be used is mentioned in the language table. Note: for English message, the language parameter is not required.	O
20	s	Flag to invoke URL shortening. Please contact the service operations team for enabling URLshortening for your account. - 0 to disable shortening for the request - 1 to enable shortening for the request - Invalid values return negative response code	O
21	d	The parameter to define a custom short domain to be used. Should match one of the pre-configured values. Please contact the service operations team for configuration.	O
22	p	The parameter to invoke and define the alias or description to be added in the short URL created,it helps make the short URL relevant to the purpose of the message request or the landing page and improves conversion rate. - 1-30 characters - a-z,A-Z,0-9,-,_,.,(,)	O
23	f	Flag to request click forwarding in real-time to pre-configured web-service URL. Please contactthe service operations team for configuration. The parameters supported are defined in a later section. - 0 to disable forwarding for the request	O

		- 1 to enable forwarding for the request Invalid values return negative response code	
24	dr	Flag to request placeholder replacement with App URLs in real-time. App URLs support OS-specific dynamic redirection to allow iOS, Android and Other OS device users to be redirected to different destinations. Please contact the service operations team for enabling dynamic redirection for your account. - 0 to disable dynamic redirection for the request - 1 to enable dynamic redirection for the request Invalid values return negative response code. If request specific flag cannot be provided, then default App URL insertion can be set up by contacting Service Operations to shorten placeholder in all messages without providing flag in every request.	O
25	iu	The parameter to define iOS destination URL to redirect users clicking an App URL in message text from iOS running phones. Should be valid http URL with protocol prefix http:// or https://. If request specific destination cannot be provided, then default values can be configured to redirect users without providing iOS destination in every request.	O
26	au	The parameter to define iOS destination URL to redirect users clicking an App URL in message text from iOS running phones. Should be valid http URL with protocol prefix http:// or https://. If request specific destination cannot be provided, then default values can be configured to redirect users without providing iOS destination in every request.	O
27	fb	The parameter to define Fallback or default destination URL to redirect users clicking an App URL in message text from any other OS device. Should be valid http URL with protocol prefix http:// or https://. If request specific destination cannot be provided, then default values can be configured to redirect users without providing Fallback destination in every request.	M (if dr is set and default destinations are not configured)
* **M**=Mandatory, **O**=Optional			
Placeholder: The placeholder in the message text is replaced with a dynamic App URL if a valid App URL insertion request is received. By-default, the SINCH INDIA system expects the placeholder to be http://acl.cc, but it can be customized for your account if needed. The custom placeholder should be prefixed with http:// or https://.			

Language Codes:

S.No	Language	Code
1.	Bengali	bg
2.	Gujarati	gu
3.	Hindi	hi
4.	Marathi	mr
5.	Tamil	ta
6.	Telugu	te
7.	Assames	as
8.	Kannada	kn
9.	Malayalam	ml
10.	Nepali	ne
11.	Oriya	or
12.	Punjabi	pa
13.	Sanskrit	sa
14.	Urdu	ur

5.2. Push using XML

Enterprise can PUSH message using XML chunk via URL over http. Max allowed datapoints in a

packet is 500.

5.2.1. Push URL

SINCH INDIA supports 2 types of XML packets as:

For One-To-Many SMS

SINCH INDIA will provide a URL to the enterprise as mentioned below:
https://push3.aclgateway.com/servlet/com.aclwireless.pushconnectivity.listeners.PushXMLListener?

Enterprise must invoke this URL and pass an XML formatted data chunk as per below specification.
The format of XML chunk will be like this:

```
<?xml version="1.0"?>
<push>
<appid>XXXXXX</appid>
<subappid>XXXXXX</subappid>
<userid>XXXXXX</userid>
<pass>XXXXXX</pass><msgid>MSGID</msgid>
<content-type>1</content-type>
<from>FROM</from>
<dpi>xxx</dpi>
<to>
<address>MobileNum1</address><address>MobileNum2</address><address>Mob
ileNum..n</address>
</to>
<dtm>xxxx</dtm>
<tc>xxxx</tc>
<msg>MESSAGETEXT with url https://abcd.com/accountdetails?account=123456.</msg>
<alert>0/1</alert>
<intflag>false</intflag>
<shorten>1</shorten>
<forward>1</forward>
</push>
```

For One-To-One SMS

Sinch India will provide a URL to the enterprise as mentioned below:

https://push3.aclgateway.com/servlet/com.aclwireless.pushconnectivity.listeners.XmlLangaugeAPIListener?

The format of XML chunk for sending one-to-one messages is as given below:

```
<?xml version='1.0'?>
<push>
<appid>XXXXXX</appid>
<subappid>XXXXXX</subappid>
<userid>XXXXXX</userid>
<pass>XXXXXX</pass>
<msgid>MSGID</msgid>
<content-type>1</content-type>
<from>FROM</from>
<dpi>xxxx</dpi>
<multisms>
<detail id='1' msisdn='91XXXXXXXXXX' msg='this is a test sms1 with url
https://abcd.com/accountdetails?account=123456.' language='en' dtm='xxx' tc='xxx'
shorten='1'/>
<detail id='2' msisdn='91XXXXXXXXXX' msg='this is a test sms2 with url
https://abcd.com/accountdetails?account=123456.' language='en' dtm='xxx' tc='xxx'
shorten='1' forward='1'/>
<detail id='3'  msisdn='91XXXXXXXXXX' msg='this is a test sms3' language='en' dtm='xxx'
tc='xxx'/>
</multisms>
<alert>0/1</alert>
<intflag>false</intflag>
</push>
```

Note:

ALERT = <alert>0</alert> for DND Check

<alert>1</alert> for Alert messages

MSGID = this should be unique id for every request, generated by enterprise.

FROM = this will go as a sender that can be either alphabet or numeric and up to 6 characters.

MESSAGETEXT = Actual SMS message text to be sent.

5.2.2. Description of Parameters

S.No.	Parameter Name	Parameter Description	Criteria*
1	userid	User Id provided by Sinch India to an enterprise for authentication	M
2	pass	Password provided by Sinch India for authentication of User Id	M
3	appid	Application Id associated with an enterprise, provided by Sinch India	M
4	subappid	If Enterprise has subdivisions, then provided by Sinch India for a particular division	O
5	msgid	it should be unique id for every request, generated by enterprise.	M
6	id	This is a unique id provided if the request has multiple mobile numbers. If not provided, then it is added by the platform as an incremental value.	O
7	msisdn	The Mobile number(s) where SMS to be sent. For more than one Mobile number comma used as a separator. E.g.9810790950,9810549171	M
8	from	Sender id to be sent with the SMS.	M
9	content-type	“1” for text SMS. Details as mentioned below	M
10	selfid	It should be set “true”, Sinch India platform maps a message id along with the request	M
11	text	Message Text	M
12	auth	These are dummy fields, with max allowed length as 50. If not provided app id is passed.	O
13	subauth	These are dummy fields, with max allowed length as 50. If not provided subapp id is passed.	O
14	brd	The is a campaign name with the max allowed limit as 50. If not provided, the systems allocate the name.	O
15	dpi	DLT principal entity ID	O
16	dtm	DLT template ID	O
17	tc	Template category Transactional – the value to-be sent is 1 Promotional – the value to-be sent is 2 Service Implicit – the value to-be sent is 3 Service Explicit – the value to-be sent is 4	O
18	intflag	the identifier for domestic and international traffic	O
19	alert	To be set either 0 or 1, by default its value will be 0 means request will pass through DND Check.	O
20	language	The language parameter is used to convert English message with whitelisted template to be delivered in a regional language. The regional language template needs to be pre-configured with us. The specific language to be used is mentioned in the language table. Note: for English message, the language parameter is not required.	O
21	shorten	Flag to invoke URL shortening. Please contact the service operations team for enabling URL shortening for your account. - 0 to disable shortening for the request - 1 to enable shortening for the request Invalid values return negative response code	O

22	domain	The parameter to define a custom short domain to be used. Should match one of the pre-configured values. Please contact the service operations team for configuration.	O
23	p	The parameter to invoke and define the alias or description to be added in the short URL created, it helps make the short URL relevant to the purpose of the message request or the landing page and improves conversion rate. - 1-30 characters - a-z,A-Z,0-9,-,_,.,(,)	O
24	forward	Flag to request click forwarding in real-time to pre-configured web-service URL. Please contact the service operations team for configuration. The parameters supported are defined in a later section. - 0 to disable forwarding for the request - 1 to enable forwarding for the request Invalid values return negative response code	O
25	dr	Flag to request placeholder replacement with App URLs in real-time. App URLs support OS-specific dynamic redirection to allow iOS, Android and Other OS device users to be redirected to different destinations. Please contact the service operations team for enabling dynamic redirection for your account. - 0 to disable dynamic redirection for the request - 1 to enable dynamic redirection for the request Invalid values return negative response code. If request specific flag cannot be provided, then default App URL insertion can be set up by contacting Service Operations to shorten placeholder in all messages without providing flag in every request.	O
26	iu	The parameter to define iOS destination URL to redirect users clicking an App URL in message text from iOS running phones. Should be valid http URL with protocol prefix http:// or https://. If request specific destination cannot be provided, then default values can be configured to redirect users without providing iOS destination in every request.	O
27	au	The parameter to define iOS destination URL to redirect users clicking an App URL in message text from iOS running phones. Should be valid http URL with protocol prefix http:// or https://. If request specific destination cannot be provided, then default values can be configured to redirect users without providing iOS destination in every request.	O
28	fb	The parameter to define Fallback or default destination URL to redirect users clicking an App URL in message text from any other OS device. Should be valid http URL with protocol prefix http:// or https://. If request specific destination cannot be provided, then default values can be configured to redirect users without providing Fallback destination in every request.	M (if dr is set and default destinations are not configured)
* M=Mandatory, O=Optional			
Placeholder: The placeholder in the message text is replaced with a dynamic App URL if a valid App URL insertion request is received. By default, the SINCH INDIA system expects the placeholder to be http://acl.cc, but it can be customized for your account if needed. The custom placeholder should be prefixed with http:// or https://.			

5.2.3. XML Response format

Response XML after successful submission of request:

```
<push>
<status>1</status>
<response-id>demoacl2-1629114743615-9238-0225</response-id>
<msgid>MSG1ID</msgid>
<acceptance-time>16-08-2021 05:22:23</acceptance-time>
<desc>ACL Gateway Accepted Successfully</desc>
```

</push>

Note:

MSGID = It will be same that is submitted by the enterprise. In case of any error SINCH INDIA will return the error code

Note:

Status is always zero for error case

<push>

<status>0</status>

<error>

<code>-15</code>

<description>Mailformed XML Data Received</description>

</error>

</push>

S.No.	Parameter Name	Parameter Description
1.	error	Shows code and description of the error
2.	code	This shows error code
3.	description	A short detail of the error

5.2.4. XML Encoding

Since XML does not support some characters, these characters to be replaced withproperly encoded characters as mentioned in the list below.

Character	Replacement
"	&quot;
&	&amp;
<	&lt;
>	&gt;
©	&copy;
´	&acute;
«	&laquo;
»	&raquo;
¡	&iexcl;
¿	&iquest;
À	&Agrave;
À	&agrave;
Á	&Aacute;
Á	&aacute;
Â	&Acirc;

Â	&acirc;
Ã	&Atilde;
Ã	&atilde;
Ä	&Auml;
Ä	&auml;
Å	&Aring;
Å	&aring;
Æ	&AElig;
Æ	&aelig;
Ç	&Ccedil;
Ç	&ccedil;
Ð	&ETH;
Ð	&eth;
È	&Egrave;
È	&egrave;
É	&Eacute;
É	&eacute;
Ê	&Ecirc;
Ê	&ecirc;
Ë	&Euml;
Ë	&euml;
Ì	&Igrave;
Ì	&igrave;
Í	&Iacute;
Í	&iacute;
Î	&Icirc;
Î	&icirc;
Ï	&Iuml;
Ï	&iuml;
Ñ	&Ntilde;
Ñ	&ntilde;
Ò	&Ograve;
Ò	&ograve;
Ó	&Oacute;
Ó	&oacute;
Ô	&Ocirc;
Ô	&ocirc;
Õ	&Otilde;
Õ	&otilde;
Ö	&Ouml;
Ö	&ouml;

Ø	Ø
Ø	ø
Ù	Ù
Ù	ù
Ú	Ú
Ú	ú
Û	Û
Û	û
Ü	Ü
Ü	ü
Ý	Ý
Ý	ý
Ÿ	ÿ
Þ	Þ
Þ	þ
ß	ß
§	§
¶	¶
µ	µ
¦	¦
±	±
¨	¨
¸	¸
ª	ª
º	º
¬	¬
¯	¯
°	°
¹	¹
²	²
³	³
¼	¼
½	½
¾	¾
×	×
÷	÷
¢	¢
£	£
¤	¤
¥	¥

5.2.5. Content Type Parameter Value

Supported Content Types are:

Content Description	Content Type value
Plain 7-Bit Text	1
For Unicode	3
Flash Unicode	42
Flash Message	13

5.2.6. Response Id

For every successful submission to Sinch India's platform, the platform generates aunique transaction id and returns as a response in the same URL call.

Response id format: AppId-1105346352818-592770-010
Max length is 50

5.3. Push Using JSON

Enterprise can PUSH message using JSON packets via URL over http.

5.3.1. Single JSON

5.3.1.1. Request

- **URL:** https://push3.aclgateway.com/v1/enterprises/messages.json
- **Sample Request**
  - Header:
    Content-type: application/JSON
  - Body:

```
{
"appid":"xxxx",
"userId":"xxxx",
"pass":"xxxx",
"contenttype":"1",
"from":"aclmob",
"to":"91XXXXXXXXX",
"alert":"1",
"selfid":"true",
"intflag":"false",
"dpi":"xxxx",
```

"dtm": "xxxx",

"tc":"xxxx",

"text":"This is a test message."

}

5.3.1.2. Response

For every request, SINCH INDIA will return the response either as success or failure

- **Sample Response**
  - SUCCESS

    {"respid":"demoacl2-1629115369238-3389- 0216","accepted":"true","msgid":""}

  - FAILED

    {"accepted":"false","msgid":"","error":"-1"}

5.3.2. Multi JSON with encryption

The web-service allows an enterprise to send a request in bulk in a single requestas an encrypted string.

The allowed request per JSON packet is 5,000.

5.3.2.1. Request

- **URL – https://push3.aclgateway.com/v2/enterprises/messages.json**
- **Sample SMS JSON Request**

{

"appid":"demoacl6",

"contenttype":"1",

"auth":"demoacl", "subauth":"demoacl", "brd":"broadcastname", "intflag":"false", "msgid":"msgid_12231", "selfid":"true",

"dpi":"xxxx",

"alert":"1",

"messages":[

{"id":"1","msg":"hi account no 11 due date is dd-mm-yy","to":"9810199991","from":"ACLMOB","language":"en","dtm":"xxx","tc":"xx",

{"id":"2","msg":"This is a test message from XYZ","to":"9810199992","from":"ACLMOB","language":"en","dtm":"xxxx","tc":"xxx"}]

}

The above needs to be encrypted using AES 256 encryption (CBC mode with PKCS5Padding), before sending it to SINCH INDIA. Thesample Java code for AES 256 bit encryption is attached for reference.

- **Sample JAVA Code**

Encrypter5.java

- **Sample encrypted request**
  - Header

    Content-type: application/Json
  - POST Body
    {"appid":"xxxxxx",

    "encryptedData":"6xDxPQMGUUhbqm4wpelBl/J4WjapmFvzRu
    qv9uekw67ejZcRaJFCLW+8FY+nTP2zJ83Qw6WqRPS2nf5Ay/
    drM16m4yHQBkGVbvLGO5wl+w/0+34+XfbWccmckrvf1sfMj8+
    0GssaSo4k2Fa+GX0rV87oHt88f0s7If/ACBsncEEYqJzUjFMJt8
    YDIQHWLwmSt/xGE77dNOuSCG2lanRr3gVw5YrGnv2g0w1g0
    8VchGsfMUe3JZ7Ve6P9tm2RjKnCqwxucXyZyE1yZwyoX6PF2
    PVH+MnKKUcvJwqCydz4JE8egi++dFzWX2Rs1UFz6W6/jnvq2
    cUCwNN8Eu9/9fqiuE3SKVcCUdnNzHDZ6/gR0OvCRvqcY8KQ
    44nmBJ32St+ZsU8coRAviwtozE+Mir/sZj4AzHo9pADvv7dnT8iq
    PG+il/NHVcPKh2Lp0lbcFqmxMOooiqQi2xXZHj763D5uaJVs4o
    T5TTLj+I63O0w2u0RHJq0AZtJWCQwZHdEayBqj/hvm8263o1s
    b6U/ZSP8Pqq08Fh6E8bL4nnM8Ou8AU0cEFLXMos081NADG
    B94jV8/YP19tMI2gysoiRFCULYqQ7v5dfVwTZTNZXUOUnxuT
    Hb4AAIjzSIbBUSaFsfgvivaKyA02G/ZOLEgx3kZKDACrw==}

5.3.2.2. Response

For every request, SINCH INDIA will return the response either as success or failure

- **Sample Response**
  - SUCCESS

    {"respid":"demoacl2-1629115369238-3389- 0216","accepted":”true”,"msgid":""}
  - FAILED

    {"accepted":”false”,"msgid":"","error":"-1"}

5.3.3. Multi JSON without encryption

The web-service allows an enterprise to send a request in bulk in a single request.

The allowed request per JSON packet is 5,000

5.3.3.1. Request

- **URL –** https://push3.aclgateway.com/v4/enterprises/messages.json
- **Sample Request**
  - Header

    content-type=application/json
  - Post Body

    {"appid":"demotst", "subappid":"demotst", "userId":"demotst",

    "pass":"demotst",

    "contenttype":"1",

    "auth":"demotst", "subauth":"demotst", "dpi":"xxxx", "brd":"broadcastname", "intflag":"false", "msgid":"msgid_12231", "selfid":"true",

    "alert":"1",

    "messages":[{"id":"1","msg":" Hi a test message from acl mobile limited the premium vas company.","to":"9810199991","from":"ACLMOB","language":"en

    ","dtm":"xxxx","tc":"xxxx"},

    {"id":"2","msg":" Hi a test message from acl mobile limited the premium vas company.","to":"9810199992","from":"ACLMOB","language":"en

    ","dtm":"xxxx","tc":"xxxx"}]

    }

5.3.3.2. Response

For every request, SINCH INDIA will return the response either as success or failure

- **Sample Response**
  - SUCCESS

    {"respid":"demoacl2-1629115369238-3389- 0216","accepted":"true","msgid":""}
  - FAILED

    {"accepted":"false","msgid":"","error":"-1"}

5.3.4. Description of Parameters

S.No.	Parameter Name	Parameter Description	Criteria*
1	userId	User Id provided by Sinch India to an enterprise for authentication	M
2	pass	Password provided by Sinch India for authentication of User Id	M
3	appid	Application Id associated with an enterprise, provided by Sinch India	O
4	subappid	If Enterprise has subdivisions, then provided by Sinch India for a particular division	O

5	to	The Mobile number(s) where SMS to be sent. For more than one Mobile number comma used as a separator. E.g.9810790950,9810549171	M
6	from	Sender id to be sent with the SMS.	M
8	contenttype	“1” for text SMS. Details as mentioned below	M
9	selfid	It should be set “true”, Sinch India platform maps a message id along with the request	M
10	text	Message Text	M
11	auth	These are dummy fields, with max allowed length as 50. If not provided app id is passed.	O
12	subauth	These are dummy fields, with max allowed length as 50. If not provided subapp id is passed.	O
13	brd	The is a campaign name with the max allowed limit as 50. If not provided, the system allocates the name.	O
14	dpi	DLT principal entity ID	O
15	dtm	DLT template ID	O
16	tc	Template category Transactional – the value to-be sent is 1 Promotional – the value to-be sent is 2 Service Implicit – the value to-be sent is 3 Service Explicit – the value to-be sent is 4	O
17	intflag	the identifier for domestic and international traffic	O
18	alert	To be set either 0 or 1, by default its value will be 0 means request will pass through DND Check.	O
19	language	The language parameter is used to convert English message with whitelisted template to be delivered in a regional language. The regional language template needs to be pre-configured with us. The specific language to be used is mentioned in the language table. Note: for English message, the language parameter is not required.	O
20	s	Flag to invoke URL shortening. Please contact the service operations team for enabling URL shortening for your account. - 0 to disable shortening for the request - 1 to enable shortening for the request Invalid values return negative response code	O
21	d	The parameter to define a custom short domain to be used. Should match one of the pre-configured values. Please contact the service operations team for configuration.	O
22	p	The parameter to invoke and define the alias or description to be added in the short URL created, it helps make the short URL relevant to the purpose of the message request or the landing page and improves conversion rate. - 1-30 characters - a-z,A-Z,0-9,-,_,.,(,)	O
23	f	Flag to request click forwarding in real-time to pre-configured web-service URL. Please contact the service operations team for configuration. The parameters supported are defined in a later section. - 0 to disable forwarding for the request - 1 to enable forwarding for the request Invalid values return negative response code	O

24	dr	Flag to request placeholder replacement with App URLs in real-time. App URLs support OS-specific dynamic redirection to allow iOS, Android and Other OS device users to be redirected to different destinations. Please contact the service operations team for enabling dynamic redirection for your account. - 0 to disable dynamic redirection for the request - 1 to enable dynamic redirection for the request Invalid values return negative response code. If request specific flag cannot be provided, then default App URL insertion can be set up by contacting Service Operations to shorten placeholder in all messages without providing flag in every request.	O
25	iu	The parameter to define iOS destination URL to redirect users clicking an App URL in message text from iOS running phones. Should be valid http URL with protocol prefix http:// or https://. If request specific destination cannot be provided, then default values can be configured to redirect users without providing iOS destination in every request.	O
26	au	The parameter to define iOS destination URL to redirect users clicking an App URL in message text from iOS running phones. Should be valid http URL with protocol prefix http:// or https://. If request specific destination cannot be provided, then default values can be configured to redirect users without providing iOS destination in every request.	O
27	fb	The parameter to define Fallback or default destination URL to redirect users clicking an App URL in message text from any other OS device. Should be valid http URL with protocol prefix http:// or https://. If request specific destination cannot be provided, then default values can be configured to redirect users without providing Fallback destination in every request.	M (if dr is set and default destinations are not configured)
* M=Mandatory, O=Optional			
Placeholder: The placeholder in the message text is replaced with a dynamic App URL if a valid App URL insertion request is received. By default the SINCH INDIA system expects the placeholder to be http://acl.cc, but it can be customized for your account if needed. The custom placeholder should be prefixed with http:// or https://.			

6. Scheduling API

The API allows enterprise to define the schedule of the campaign. The enterprise can schedule the request with API details as mentioned below.

Scheduling API allows client to request the scheduling within 24 hours from the current time.Expiry time should always be greater or equal to 60 seconds from the scheduled time.

6.1. Single request

The single request can be sent to the Push over GET and POST Method

6.1.1. Get Method

This would allow user to send the request payload as query string in the url, the sample request and response signature is as mentioned below. The request and response are synchronous

https://shc.aclgateway.com/servlet/com.aclwireless.pushconnectivity.listeners.TextListener?userId=sch&pass=sch&contenttype=1&from=schon&to=918588836715&text=request1&alert=1&selfid=true&intflag=false&brd=case1&bsize=10&schedule=2020 02111659&expire=202002111959

6.1.2. Post Method - JSON

This would allow user to send the request payload in JSON, the sample request and response signature is as mentioned below. The request and response are synchronous

6.1.2.1. Request

- **URL** - https://shc.aclgateway.com/v1/enterprises/messages.json
- **Sample Request**
  - Header

    Content-type: application/JSON
  - Body

    {
    "appid":"sch",
    "userId":"sch",
    "pass":"sch",
    "contenttype":"1",
    "from":"aclaut", "to":"918588836715",
    "alert":"1",
    "selfid":"true",
    "intflag":"false",
    "text":"schon", "schedule":"202105181722", "expire":"202105181732"
    }

6.1.2.2. Response

For every request, SINCH INDIA will return the response either as success or failure

- **Sample Response**
  - SUCCESS

    {"respid":"demoacl2-1629115369238-3389-0216","accepted":true,"msgid":""}
  - FAILED

    {"accepted":false,"msgid":"","error":"-1"}

6.2. Bulk Request

The user can send the send multiple requests in the single payload. The allowed payloadlimit is 5,000 mobile number their respective message text. The user can send the data inbulk over POST Method with support over JSON only.

6.2.1. Post Method Multi-JSON

This would allow remote client to send the request payload in JSON, the samplerequest and response signature is as mentioned below.
The request and response are synchronous i.e., either a response id as an acknowledgement would return as an acceptance or a negative acknowledgementwould be returned in case of rejection.
The client can define the bulk camping schedule for the broadcast i.e., singleschedule will be applied for the all the request in the payload.

6.2.1.1. Request

- **URL** - https://shc.aclgateway.com/v12/enterprises/messages.json
- **Sample Request**
  - Header

    Content-type: application/JSON
  - Body

```
{
"auth": "XXXXX",
"pass": "xxxxxx_1234", "msgid": "1580644639903",
"userId": "xxxxxxx",
"intflag": "false", "subauth": "xxxxxxxxx", "contenttype": "1",
"alert": "1",
"brd": "broadcastname", "appid": "xxxxxxxx",
"selfid": "true", "messages": [
{
"msg": "hi this is demo template.", "from": "ACLMOB",
"id": "0",
"to": "919899261111"
},
{
"msg": "hi this is demo template.", "from": "ACLMOB",
"id": "1",
"to": "919899265555"
}
],
```

"subappid": "xxxxxxxx", "schedule": "202008241342",

"expire": "202008241402"

}

6.2.1.2. Response

For every request, SINCH INDIA will return the response either as success or failure

- **Sample Response**
  - SUCCESS

    {"respid":"demoacl2-1629115369238-3389-0216","accepted":”true”,"msgid":""}
  - FAILED

    {"accepted":”false”,"msgid":"","error":"-1"}

6.2.2. Post Method Multi-JSON – Individual Schedule

This would allow remote client to send the request payload in JSON, the samplerequest and response signature is as mentioned below.

The request and response are synchronous i.e. either a response id as an acknowledgement would return as an acceptance or a negative acknowledgementwould be returned in case of rejection.

The client can define the bulk camping schedule for the individual record in the payload i.e. schedule for every mobile number will shared in the request payload.

6.2.2.1. Request

- **URL** - https://shc.aclgateway.com/v4/enterprises/messages.json
- **Sample Request**
  - Header

    Content-type: application/JSON
  - Body

    {

    "auth": "XXXXX",

    "pass": "xxxxxx_1234", "msgid": "1580644639903",

    "userId": "xxxxxxx",

    "intflag": "false", "subauth": "xxxxxxxxx", "contenttype": "1",

    "alert": "1",

"brd": "broadcastname", "appid": "xxxxxxxx", "subappid": "xxxxxxxx", "selfid": "true", "messages": [
{
"msg": "hi this is demo template.", "from": "ACLMOB",
"id": "0",
"to": "919899261111",
"language": "xx",
"s":"1",
"schedule": "202008241342",
"expire": "202008241402"
},
{
"msg": "hi this is demo template.", "from": "ACLMOB",
"id": "1",
"to": "919899265555",
"language": "xx",
"s":"1",
"schedule": "202008241342",
"expire": "202008241402"
}
]
}

6.2.2.2. Response

For every request, SINCH INDIA will return the response either as success or failure

- **Sample Response**
  - SUCCESS

    {"respid":"demoacl2-1629115369238-3389-0216","accepted":"true","msgid":""}
  - Failure

    {"accepted":"false","msgid":"","error":"-1"}

6.3. Supported Time stamp

The below mentioned time format is supported with scheduling API for schedule and expiry.This is configurable specific to appid.

- yyyyMMddHHmm
- yyyyMMddHHmmss

- yyyyMMddHHmmssSSS
- yyMMddHHmm
- yyMMddHHmmss
- yyMMddHHmmssSSS
- milliseconds
- epoch

6.4. Parameters & Description

The request parameter and their description are as mentioned below

S.No.	Parameter Name	Parameter Description	Criteria*
1	userId	User Id provided by Sinch India to an enterprise for authentication	M
2	pass	Password provided by Sinch India for authentication of User Id	M
3	appid	Application Id associated with an enterprise, provided by Sinch India	O
4	subappid	If Enterprise has subdivisions, then provided by Sinch India for a particular division	O
5	to	The Mobile number(s) where SMS to be sent. For more than one Mobile number comma used as a separator. E.g.9810790950,9810549171	M
6	from	Sender id to be sent with the SMS.	M
8	contenttype	“1” for text SMS. Details as mentioned below	M
9	selfid	It should be set “true”, Sinch India platform maps a message id along with the request	M
10	text	Message Text	M
11	auth	These are dummy fields, with max allowed length as 50. If not provided app id is passed.	O
12	subauth	These are dummy fields, with max allowed length as 50. If not provided subapp id is passed.	O
13	brd	The is a campaign name with the max allowed limit as 50. If not provided, the systems allocate the campaign name.	O
14	intflag	the identifier for domestic and international traffic	O
15	alert	To be set either 0 or 1, by default its value will be 0 means request will pass through DND Check.	O
16	schedule	the schedule time for the request, the time format is mentioned above	O
17	expire	the expiry time for the request, the time format is mentioned above	O
18	language	The language parameter is used to convert English message with whitelisted template to be delivered in a regional language. The regional language template needs to be pre-configured with us. The specific language to be used is mentioned in the language table. Note: for English message, the language parameter is not required.	O
19	s	Flag to invoke URL shortening. Please contact the service operations team for enabling URL shortening for your account. - 0 to disable shortening for the request - 1 to enable shortening for the request Invalid values return negative response code	O

20	d	The parameter to define a custom short domain to be used. Should match one of the pre-configured values. Please contact the service operations team for configuration.	O
21	p	The parameter to invoke and define the alias or description to be added in the short URL created, it helps make the short URL relevant to the purpose of the message request or the landing page and improves conversion rate. - 1-30 characters - a-z,A-Z,0-9,-,_,.,(,)	O
22	f	Flag to request click forwarding in real-time to pre-configured web-service URL. Please contact the service operations team for configuration. The parameters supported are defined in a later section. - 0 to disable forwarding for the request - 1 to enable forwarding for the request Invalid values return negative response code	O
23	dr	Flag to request placeholder replacement with App URLs in real-time. App URLs support OS-specific dynamic redirection to allow iOS, Android and Other OS device users to be redirected to different destinations. Please contact the service operations team for enabling dynamic redirection for your account. - 0 to disable dynamic redirection for the request - 1 to enable dynamic redirection for the request Invalid values return negative response code. If request specific flag cannot be provided, then default App URL insertion can be set up by contacting Service Operations to shorten placeholder in all messages without providing flag in every request.	O
24	iu	The parameter to define iOS destination URL to redirect users clicking an App URL in message text from iOS running phones. Should be valid http URL with protocol prefix http:// or https://. If request specific destination cannot be provided, then default values can be configured to redirect users without providing iOS destination in every request.	O
25	au	The parameter to define iOS destination URL to redirect users clicking an App URL in message text from iOS running phones. Should be valid http URL with protocol prefix http:// or https://. If request specific destination cannot be provided, then default values can be configured to redirect users without providing iOS destination in every request.	O
26	fb	The parameter to define Fallback or default destination URL to redirect users clicking an App URL in message text from any other OS device. Should be valid http URL with protocol prefix http:// or https://. If request specific destination cannot be provided, then default values can be configured to redirect users without providing Fallback destination in every request.	M (if dr is set and default destinations are not configured)
* M=Mandatory, O=Optional			
Placeholder: The placeholder in the message text is replaced with a dynamic App URL if a valid App URL insertion request is received. By default, the SINCH INDIA system expects the placeholder to be http://acl.cc, but it can be customized for your account if needed. The custom placeholder should be prefixed with http:// or https://.			

7. Cancelation API

The remote client can cancel the scheduled request using the below mentioned API. The request can be canceled 30 minutes from the scheduled time. Following cases are supported to cancel the scheduled request basis, the “broadcast name”, “msg id”, “response id” and “Mobile number” with the possible combination as mentioned below. It only supports GET Method.

Sl. No.	Parameters	Description
1	brdname	Cancel the scheduled campaign basis the broadcast name
2	brdname + mobile	Cancel the scheduled campaign basis the broadcast name and mobile number
3	brdname + msgId	Cancel the scheduled campaign basis the broadcast name and message id.
4	brdname + msgid + mobile	Cancel the scheduled campaign basis the broadcast name, message id & Mobile number.
5	brdname + responseId	Cancel the scheduled campaign basis the broadcast name and response id.
6	brdname + responseId + mobile	Cancel the scheduled campaign basis the broadcast name, response id & mobile number.
7	brdname + msgId + responseId	Cancel the scheduled campaign basis the broadcast name, message id & Response id.
8	brdname + msgId + responseId + mobile	Cancel the scheduled campaign basis the broadcast name, message id, response id & Mobile number
9	msgid	Cancel the scheduled campaign basis the message id.
10	msgid + mobile	Cancel the scheduled campaign basis the message id and Mobile number.
11	responseId	Cancel the scheduled campaign basis the response id.
12	responseId + mobile	Cancel the scheduled campaign basis the response id & Mobile number
13	msgId + responseId	Cancel the scheduled campaign basis the message id & response id
14	msgId + responseId + mobile	Cancel the scheduled campaign basis the message id, response id & Mobile number.

Supported Time Format – this is the time format, which is configured for an app id as per the requirement to send the schedule and expiry time.

- yyyyMMddHHmm
- yyyyMMddHHmmss
- yyyyMMddHHmmssSSS
- yyMMddHHmm
- yyMMddHHmmss
- yyMMddHHmmssSSS
- milliseconds
- epoch

Sample Cancelation URL

https://shc.aclgateway.com/ScheduleCancel?userId=schtest&pwd=xxxxxx&msgId=1221

Please Note user id and Password are mandate. This will be provided by SINCH INDIA which willbe used while invoking the cancellation request.

8. DLR API

This allows an enterprise to get the status of the SMS transaction with the SINCH INDIA's SMS gateway.

8.1. Push DLR (supports both GET & POST method)

Here the customer provides the API for GET method, the format of which is listed below:
http://xxxxxxxxxx/UrlListner/requestListener?msg_id=%messageId&mobile_no=%reciever&rqst_ack_id=%responseid&vendor_recv_dttime=%receivedRequestTime&sms_delv_status=%status&sms_delv_dttime=%dlrReceivedTime&Num_Retries=1&vendor_name=SINCHINDIA&channel_name=SMS&remarks=%stat&msg_sent_dttime=%submitTime&submitTime=%submitTime&requestReceivedTime=%receivedRequestTime&dlrtime=%dlrReceivedTime&handsetTime=%time&msg=%msgText
The DLR will be pushed to the client web-service in 500 request per packet in POST Method. The endpoint url should be provided by the client.

Sample query string body construct for POST Method

msg_id=%messageId&mobile_no=%reciever&rqst_ack_id=%responseid&vendor_recv_dttime=%receivedRequestTime&sms_delv_status=%status&sms_delv_dttime=%dlrReceivedTime&Num_Retries=1&vendor_name=SINCHINDIA&channel_name=SMS&remarks=%stat&msg_sent_dttime=%submitTime&submitTime=%submitTime&requestReceivedTime=%receivedRequestTime&dlrtime=%dlrReceivedTime&handsetTime=%time&msg=%msgText

Sample JSON Construct for POST Method.

{"dlrtime":"2021-03-1817:22:16.059","rqst_ack_id":"5555173092-1616068333246-8837-0216","submitTime":"2021-03-18 17:22:13","mobile_no":"919999911139","vendor_recv_dttime":"2021-03-18 17:22:13","handsetTime":"2021-03-1817:22:14.000","msg_id":"msgid-5555173092-1616068333245-9213-0216","sms_delv_status":"delivered"}

The details of the parameter are:

Parameter description	The real-time der URL value
Mobile Number	%reciever
Response id	%responseid
Status Description	%status
Submitted to operator time	%submitTime

Sender Id	%senderid
Failed description	%stat
Failed code	%err
Message id received	%messageId
Time of Request received at SINCH INDIA	%receivedRequestTime
Last Update Time	%lastUpdateTime
Delivery received time	%dlrReceivedTime
Time of delivery on Handset	%time
DLT template Id	%dltTempId%
DLT Principal Entity Id	%dltPEId%
DLT template category	%templateCategory%

8.2. Pull DLR

The enterprise can query the DLR from SINCH INDIA in Synchronous and Asynchronous mode with the details are as mentioned below.
Supported Methods are GET and POST with JSON body.
Allowed request per packet is 500.

8.2.1. Sync Mode

The request and response are synchronous. Enterprise needs to request DLR in below format.

8.2.1.1. Sample request

- **URL** - https://dlrfetch.aclgateway.com/dlrhandler/dlrfetchlistener
- **Protocol** - https
- **Method** - POST
- **Data Form** - JSON
- **Sample Header**
  - “Content-type” : application/json
  - “randomKey” : “random number”
- **Sample Body**

{
"hashKey":"dba85732ab9bb1ba7dc031cedea14e41c083433a125a6ab7ccd2831f13ce6cdbb517b2e43da1c446a86470d63c29d73f3d0b9efbc7072ec78bc7acff3e312",
"entid":"abc", "responseId":
[

{
"id":"abc-1586349376147-580-12"
},
{
"id":"abc-1586349376147-580-12"
}
],
"messageId":
[
{
"id":"a648fdf93db1ad4fb59d6b5757e64953"
},
{
"id":"a648fdf93db1ad4fb59d6b5757e64953"
}
],
"date":"2020-04-08"
}

8.2.1.2. Sample response


```
[
{
        "failedCode":"1001",
        "failedDesc":"NA",
        "appId":"abc",
        "mobile":"918006727764",
        "messageId":"a648fdf93db1ad4fb59d6b5757e64953",
        "intflag":"0",
        "responseId":"abc-1586349376147-580-12",
},
{
        "failedCode":"1012",
        "failedDesc":"NA",
        "appId":"abc",
        "mobile":"918006727765",
        "messageId":"a648fdf93db1ad4fb59d6b5757e64953",
        "intflag":"0",
        "responseId":"abc-1586141372547-580-12",
}
]
```


Hash Key generation

- Hash Key is used for Authentication.
- Algorithm used to generate Hash Key – **SHA512**
- Client will generate the unique hash key for every request using SHA 512.
- Input required to generate the hash key is (user id+ password+ random key)
- Random Key is pseudo random alphanumeric value, and its length should be less than or equal to16 characters, to-be provided by the client in the request.
- Push will regenerate the hash key and if the hash key matched then only the data would be provided; else return the authentication error code for the requested dlr.

Note - User id & password will be provided by SINCH INDIA and is known to client and Sinch India only.

8.2.2. Async Mode

The request and response are asynchronous. Upon request on the below web-service, the DLR will pushed to the client DLR URL as configured with SINCH INDIA.

8.2.2.1. Sample request

- **URL** - https://dlrfetch.aclgateway.com/dlrhandler/dlrfetchlistener
- **Protocol** - https
- **Method** - POST
- **Data Form** - JSON
- **Sample Header**
  - “Content-type” : application/json
  - “randomKey” : “random number”
- **Sample Body**

{

"hashKey" : "dba85732ab9bb1ba7dc031cedea14e41c083433a125a6ab7ccd2831f13ce6cdbb517b2e43da1c446a86470d63c29d73f3d0b9efbc7072ec78bc7ac9e7ff3e312",

"entid" : "abc", "responseId" : [

{

"id" : "abc-1586349376147-580-12"

},

{

"id" : "abc-1586349376147-580-12"

}],

"messageId" : [

{

"id" : "a648fdf93db1ad4fb59d6b5757e64953"

},

{

"id" : "a648fdf93db1ad4fb59d6b5757e64953"

}],

"date" : "2020-04-08"}

Hash Key generation

- Hash Key is used for Authentication.
- Algorithm used to generate Hash Key – **SHA512**
- Client will generate the unique hash key for every request using SHA 512.
- Input required to generate the hash key is (user id+ password+ random key)
- Random Key is pseudo random alphanumeric value, and its length should be less than or equal to16 characters, to-be provided by the client in the request.
- Push will regenerate the hash key and if the hash key matched then only the data would be provided; else return the authentication error code for the requested dlr.
- Date is a mandatory parameter to be passed while requesting for DLR.

Note - User id & password will be provided by SINCH INDIA and is known to client and SINCH INDIA only.

8.3. DLR on SFTP

The DLR can be made available to the enterprise over the SFTP location in form of a flatfile. The frequency of the report will be daily once a day. Following are the supported configuration types for DLR over SFTP:

Configuration Type	Parameters sent as part of DLR
T1	Message id, ResponseId, Mobile Number, delivery time, sender, dlr Status, failed code, failed description, intflag

Source IP should be whitelisted with SINCH INDIA in case if the SINCH INDIA's SFTP is used for DLR dump sharing. The SFTP credentials will be shared by SINCH INDIA team. Alternatively, enterprise can share the credentials of their SFTP location, which can be configured with SINCH INDIA system.

9. SMS Gateway Rejection Error codes and Description

9.1. SMS Gateway Error codes

The SMS gateway rejection error code and their descriptions are as mentioned below.

Error Description	Rejection Code
User Id/ Password Incorrect or Appid Missing	-1
User Id Missing	-2
Password Missing	-3
Content type Missing	-4
Sender Missing	-5
MSISDN Missing	-6
Message Text Missing	-7

Message Id Missing	-8
WAP Push URL Missing	-9
Authentication Failed	-10
Service Blocked for User	-11
Repeated Message Id Received	-12
Invalid Content Type Received	-13
International Messages Not Allowed	-14
Incomplete or Invalid XML Packet Received	-15
Invalid alert Flag value	-16
Direct Pushing Not Allowed	-17
CLI not registered	-18
Operator Specific MSISDN Blocked	-19
ACL_ERROR_INVALID_SHORTEN_FLAG	-41
ACL_ERROR_SHORTENING_NOT_ALLOWED	-42
ACL_ERROR_INVALID_DOMAIN	-43
ACL_ERROR_INVALID_ALIAS	-44
ACL_ERROR_INVALID_FORWARD	-45
ACL_ERROR_FORWARD_NOT_ALLOWED	-46
ACL_ERROR_INVALID_DYNAMIC	-47
ACL_ERROR_DYNAMIC_REDIRECTION_NOT_ALLOWED	-48
ACL_ERROR_FALLBACK_DESTINATION_NOT_DEFINED	-49
ACL_ERROR_INVALID_DESTINATION	-50
ACL_ERROR_MISSING_DESTINATION	-51
ACL_ERROR_INVALID_JSONEXCEPTION	-75
ACL_ERROR_INVALID_ENCRYPTED_DATA	-76
ACL_ERROR_ACCESSTOKEN_NOT_FOUND	-77
ACL_ERROR_ACCESSTOKEN_EXPIRED	-78
JSON batch size exceeded	-79

9.2. Scheduling Error Codes

The scheduling error code and their description is as mentioned below.

Error Description	Error Code
ACL_ERROR_SCHEDULING_NOT_SUPPORTED	-81
ACL_ERROR_INVALID_SCHEDULE_FORMAT	-82
ACL_ERROR_INVALID_SCHEDULE_PARAMETER	-83
ACL_ERROR_SCHEDULE_TIME_LESS_THAN_CURRENT_TIME	-84
ACL_ERROR_SCHEDULE_TIME_NOT_ALLOWED	-80
ACL_ERROR_EXPIRY_NOT_SUPPORTED	-85
ACL_ERROR_INVALID_EXPIRY_FORMAT	-86
ACL_ERROR_INVALID_EXPIRY_PARAMETER	-87
ACL_ERROR_INSUFFICIENT_TIME_FOR_PROCESSING	-88
ACL_ERROR_EITHER_TO_OR_MSISDN_ALLOWED	-89

ACL_ERROR_UNKNOWN	-90
ACL_ERROR_INVALID_SCHEDULING_REQUEST	-91
ACL_ERROR_MANDATORY_PARAMETERS_MISSING	-92
ACL_ERROR_MANDATORY_PARAMETERS_SMS_EXPIRED	-93
ACL_ERROR_MISSING_USERID	-2
ACL_ERROR_MISSING_PASSWORD	-3
ACL_ERROR_AUTHENTICATION_FAILED	-10

10. SMS Failure Codes from Mobile Network Operator

Following are the failure codes:

ACL_100=Mob. Abst._nt ext_out ser

ACL_101=Call or SMS Bared

ACL_102=MT SMS Not Supported

ACL_103=Network Weakness

ACL_104=Multiple SMS in Queue

ACL_105=Mob. in Initializing State

ACL_106=Mobile Inbox is Full

ACL_107=SMSC is Congested

ACL_108=Number Not Found

ACL_109=Other Trans is Running

ACL_110=Mobile Switch Off

ACL_111=Junk in SMS

ACL_112=Mob. is not Acknowledging

ACL_113=Max Retry Exceeded

ACL_114=Timeout Frm Dest. HLR

ACL_115=HLR-MSC not resp._Int roam

ACL_116=Dest opr nt res. time being

ACL_117=Net or Protocol err

ACL_118=Blacklist Subscriber

ACL_119=MSISDN in DND

ACL_120=Sender id rejected

ACL_121=Service blocked

ACL_122=Routing Id Not Found

ACL_123=MNP-Mobile Number Protability

ACL_124=Invalid-Empty-Long Message_ID

ACL_125=Parental Lock_Cannot verify age

ACL_255=Reason Not Available

ACL_126=Parameter Missing_invalid param

ACL_127=Component Error

ACL_129=Insufficient Credits
ACL_130=Internal Error
ACL_131=Mobile No. is Incorrect.
ACL_132=Service Restricted by OPT
ACL_133=No record EID
ACL_134=EID not found on DLT
ACL_135=Entity is inactive
ACL_136=Entity is blacklisted
ACL_137=Reserved for Entity
ACL_138=No entry of TMID
ACL_139=Telemarketer is inactive
ACL_140=Telemarketer is blacklisted
ACL_141=Reserved for TeleMarketer
ACL_142=header not found_case sensitive
ACL_143=Header is inactive
ACL_144=Header is blacklisted
ACL_145=Reserved for Header
ACL_146=TemplateID not found
ACL_147=Template is inactive
ACL_148=Template is blacklisted
ACL_149=Template not matched
ACL_150=Header not registered_template
ACL_151=exceeded max length
ACL_152=template not identified
ACL_153=Reserved for Template
ACL_154=Blocked in preferences
ACL_155=SE_CATEGORY_BLOCK
ACL_156=General error Consent
ACL_157=Reserved for Consent
ACL_158=General error code exceptions
ACL_159=Reserved for scrubbing
ACL_160=Validity Expired
ACL_162=Invalid Promo Time
ACL_163=Spam content Keyword filtered Text
ACL_164=BLOCKED FOR MNRL
ACL_165=BLOCKED MSISDN RECEIVED FOR ENTERPRISE
ACL_166=EId and Header Id mismatch
ACL_233=Template Not Found at ACL

11. Short URL Click Forwarding

11.1. Forwarding over web-service in real-time

Clicks registered on the short URLs generated by SINCH INDIA can be forwarded to the client system in real-time if the forward flag is set in the request and the web-service URL is configured. The clicks forwarded have duplicate clicks removed if multiple clicks are done bythe user either due to mistake or on purpose to spam the system. This is done to protect thereceiving system from unwanted clicks. The duplicate removal is done for a specific time during which only one click is forwarded. Fresh clicks can be forwarded once the time elapses. By default, the time value is set to 24 hours but can be reduced by requesting the service operations team.

11.2. Forwarding over web-service in real-time

The clicks will be forward to the client web-service over https/http GET Method. All clicks even duplicate ones are forwarded in the file. Please get in touch with service operations toget the columns configured.

11.3. Short URL Click Forwarding Parameters

Parameter description	The real-time der URL value
Messageid	%MESSAGEID
Response	%RESPONSEID
Enterprise Id	%ENTERPRISE
Campaign Name	%CAMPAIGNID
Mobile Number	%MSISDN
Short Url sent in message post shortening	%SHORTURL
Destination Url Sent In The Original Message	%DESTINALTIONURL
Ip Of The Subscriber Who Clicked	%IP
Device Of The Subscriber Who Clicked	%DEVICE
Os Of The Subscriber Who Clicked	%OS
The browser Of The Subscriber Who Clicked	%BROWSER
Time when Clicked	%CLICKTIME

Here the customer provides the API, a sample of which is listed below:
http://xxxxxxxxxx/UrlListner/requestListener?MESSAGEID=%MESSAGEID&RESPONSEID=%RESPONSEID&ENTERPRISE=%ENTERPRISE&CAMPAIGNID=%CAMPAIGNID&MSISDN=%MSISDN&SHORTURL=%SHORTURL&DESTINALTIONURL=%DESTINALTIONURL
&IP=%IP&DEVICE=%DEVICE&OS=%OS&BROWSER=%BROWSER&CLICKTIME=%CLICKTIME