GLOBAL MESSAGE SERVICES

Technical Plan
Protocol SMPP API

1. IP Connection

Connection of the Customer with SMS-G Performer is organized as follows:

Through the Internet using VPN	☐
Through the Internet without the use of VPN	☑

Technical IP data

VPN Gateway Device Information	GMSU VPN Device	"We need to specify the name of the customer» VPN Device
Name/FQDN	GMSU-VPN-GATE	
IP Address: Port	185.46.88.212	
VPN Device Description	Cisco ASA 5525-x	
VPN Device Version	Cisco ASA Software 9.6	

Tunnel Properties		GMSU VPN Device	"We need to specify the name of the customer» VPN Device
Phase 1	Authentication Method	PRE-Shared	
	Encryption Scheme	IKE	
	Diffie-Hellman Group	Group2	
	Encryption Algorithm	3DES	
	Hashing Algorithm	SHA-1	
	Main or Aggressive Mode	Main	

	Lifetime (for renegotiation)	86400 sec	
Phase 2	Encapsulation (ESP or AH)	ESP	
	Encryption Algorithm	3DES	
	Authentication Algorithm	SHA-1	
	Perfect Forward Secrecy	Group2	
	Lifetime (for renegotiation)	3600 sec	
	Lifesize in KB (for renegotiation)	4608000	
	Key Exchange for Subnets?	Not used	

Access rules

Firewall/VPN Policy Rules	Source (IP Address & FQDN) or Network	Destination (IP Address & FQDN) or Network	Service (TCP, UDP, or ICMP and port #)	Action (Allow/Deny)	Duration
Rule 1	To be specified	185.46.88.6	ICMP TCP - 20510	*Allow*	*Permanent*
Rule 2	185.46.88.1	To be specified	IP	*Allow*	*Permanent*

Note: You must use public IP addresses for all devices. Not allowed to use private addresses according to RFC-1918. The following IP address ranges are defined in RFC-1918 as private IP addresses.

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

2. SMSC – SMPP: General information

GMS can act both as an SMPP server and as a client, and supports all connection types (Receiver, Transmitter and Transceiver). Please fill in the desired settings in the table below. If more connections are required, add columns to the table.

Connection Number		№1	
GMSU Role		Server	
Client Role		Client	
Message Mode		Store and Forward	
Mode of Connections	Number of Connections	Transmitter	0
		Receiver	0
		Transceiver	1
IP Address and port of server		185.46.88.6:20510	
IP Address of client		To be specified	
SMPP System ID		To be specified	
SMPP Password		To be specified	
SMPP System type		N/A	
SMPP Version		3.4	
Enquire_link		60 sec	
Transaction timeout		30 sec	
Throttling value for one Transmitter/ Receiver/ Transceiver connection		5 msg/sec	
Source Address TON		5	
Source Address NPI		0	
Destination Address TON		1	

Destination Address NPI	1
Validity period	☑ Absolute (client defined) ☐ Relative (client defined) ☐ Default by SMSC
Delivery Report	☐ Requested by Client ☑ Forced by GMSU (always requested)

3. SMPP Settings

3.1 Client-server interconnection

SMPP server provides for reception of SMPP connections from SMPP clients which may work in transmitter, receiver or transceiver modes.

The Customer may set up several SMPP connections distinguished by System ID or several sessions within the same ESME in accordance with the Technical Plan.

If the SMPP server is unavailable or not responding, the SMPP client should repeat connection attempts once a minute at most.

3.2 SMPP protocol commands

The GMS's SMS-G supports the following command types for SMPP v3.4:

Check if the Customer wishes to use the command	Command types
☑	BIND_TRANSMITTER
☑	BIND_TRANSMITTER_RESP
☑	BIND_TRANSCEIVER
☑	BIND_TRANSCEIVER_RESP
☑	BIND_RECEIVER
☑	BIND_RECEIVER_RESP
☑	UNBIND

☑	UNBIND_RESP
☑	SUBMIT_SM
☑	SUBMIT_SM_RESP
☑	DELIVER_SM
☑	DELIVER_SM_RESP
☑	ENQUIRE_LINK
☑	ENQUIRE_LINK_RESP

Other commands or Messages will not be processed if an error code ESME_RINVCMDID is returned.

3.3 Long Messages

Long Message attribute should be sent by the User-Data-Header setting.

At SMPP v.3.4. protocol level, long Message sending settings should be expressed as follows (in accordance with the protocol specification):

- *esm_class* setting = 0 1 x x x x x x (Bits: 7 6 5 4 3 2 1 0)
  UDHI Indicator (only relevant for MT short messages)

short_message setting should contain a UDH heading

4.1 User phone numbers translation

User phone numbers translation required	☐
User phone numbers translation not required	☑

If User phone numbers translation is required, please indicate translation rules:

Original Source Address	Translated Source Address	Original Destination Address	Translated Destination Address
-	-	-	-

4.2 Message encoding

Encoding scheme	Text length of a short SMS Message in the Message segment	Text length of a long SMS Message in the Message segment	Supported
GSM 7-bit default alphabet (GSM 03.38)*	160 characters	153 characters	☐
UCS2 (ISO/IEC-10646) 16-bit	70 characters	67 characters	☐

*The length of Message segments is given based on usage of characters of GSM 7-bit default alphabet table. In this case, it should be noted that if the characters of GSM 7-bit default alphabet extended table are used, the length of Message segments will decrease, since each character of the extended table is transmitted as two octets, and is counted as two characters.

The extended table of GSM 7-bit default alphabet characters			
Hex	Dec	Character name	Character
0x1B0A	27 10	FORM FEED (PAGE BREAK)	
0x1B14	27 20	CIRCUMFLEX ACCENT	^
0x1B28	27 40	LEFT CURLY BRACKET	{
0x1B29	27 41	RIGHT CURLY BRACKET	}
0x1B2F	27 47	REVERSE SOLIDUS (BACKSLASH)	\
0x1B3C	27 60	LEFT SQUARE BRACKET	[
0x1B3D	27 61	TILDE	~
0x1B3E	27 62	RIGHT SQUARE BRACKET	]
0x1B40	27 64	VERTICAL BAR	|
0x1B65	27 101	EURO SIGN	€
0x1B1B	27 27	RESERVED	

4.3 Message's Time To Live

At the protocol level SMPP v.3.4, the lifetime of the message must be passed by the parameter_valid_period (according to the protocol specification).

If the Customer specifies the lifetime of the message in explicit form, in accordance with the specification of SMPP v.3.4, then the validity_period parameter specified by the Customer will be applied. But keep in mind that the value of this parameter can not exceed the default values for the SMSC Operators or Executer, which are listed below.

If the Customer does not indicate the lifetime of the message, then the time of life is determined by the default value on SMSC Operators or Performer:

Operator	The default parameter of validity -period for SMSC Operator
lifecell	24h
Kyivstar	72h
VF Ukraine	72h
3Mob	72h
PeopleNet	72h
Intertelecom	24h

Validity-Period value by default on SMSC Executer is 72 hours.

4.4 Delivery reports

If the sender is willing to receive Message delivery reports, the *registered_delivery* setting at SMPP v.3.4. protocol level should have the value x x x x x x 0 1 (Bits: 7 6 5 4 3 2 1 0). The delivery report in this case will be sent via *deliver_sm* command in accordance with the protocol specification.

5 Curfew time

Sending messages is allowed in the period *	☐ from 9:00 until 20:00 (weekdays) and from 11:00 until 18:00 (weekends and holidays)
Curfew is absent **	¨ 00:00 to 24:00

** when carrying out the transfer of confirmation of banking transactions (withdrawal of funds, replenishment of accounts, etc.), registration on the Internet site, Messages from taxi services and other 24-hour service messages, previously agreed with the Contractor.

* All other text messages.

6 Identification and blocking of Duplicate Messages

Duplicate Messages are Messages having identical content, sender and recipient addresses.
Duplicate Message are blocked automatically on the following condition:
more than two Messages in seventy seconds.
The customer may change the policy of blocking the Messages with the consent of the Contractor