|  |
| --- |
| **SMSC RFP**  **APPENDIX 1** |
| **Technical Specifications Document** |

**MOBILE INTERIM COMPANY NO.2 S.A.L.**

**Touch building, Charles Helou Avenue**

**Po.box 175051 Beirut-Lebanon**

1. **Abstract**

This document includes the required technical specifications for the Short Messaging Service Center solution in terms of functional description, features and interfaces with other components, as well as the general guidelines and responsibility matrix for system design, delivery, deployment, integration, migration, management, operation, maintenance and migration from the current SMSC.

1. **Table of Contents**

[1. Background Information 5](#_Toc130551416)

[2. General Requirements 6](#_Toc130551417)

[Further Requirements 8](#_Toc130551418)

[3. Short Messaging Service Center Requirements 10](#_Toc130551419)

[3.1. Solution requirements 10](#_Toc130551420)

[Signaling requirements 11](#_Toc130551421)

[Basic SMSC features 12](#_Toc130551422)

[Antispam features 14](#_Toc130551423)

[SMS Forwarding (subscriber service – quoted separately) 17](#_Toc130551424)

[SMS Autoreply (subscriber service - quoted separately) 18](#_Toc130551425)

[SMS Filtering (subscriber service - quoted separately) 18](#_Toc130551426)

[Interworking with IMS 18](#_Toc130551427)

[Application/Message Router 19](#_Toc130551428)

[MT billing control 21](#_Toc130551429)

[Bulk SMS campaign manager 22](#_Toc130551430)

[Bulk SMS Opt-out solution 24](#_Toc130551431)

[SMS Grouping (subscriber service - quoted separately) 26](#_Toc130551432)

[Optional items 26](#_Toc130551433)

[3.2. Dimensioning, Capacity and Architecture 26](#_Toc130551434)

[4. Billing and Integration Requirements 31](#_Toc130551435)

[4.1. SMSC Solution – Billing System 31](#_Toc130551436)

[4.2. SMSC Solution – Provisioning 32](#_Toc130551437)

[4.3. SMSC Solution – NGBSS/IN/OCS Interface 33](#_Toc130551438)

[5. System Operation and Management 35](#_Toc130551439)

[5.1. Operations Management 35](#_Toc130551440)

[5.2. Performance Management 36](#_Toc130551441)

[5.3. System Failure and Alarm Management 38](#_Toc130551442)

[5.4. Security Management 40](#_Toc130551443)

[6. Interoperability 42](#_Toc130551444)

[7. Professional Services 43](#_Toc130551445)

[7.1. Delivery 43](#_Toc130551446)

[7.2. Installation 43](#_Toc130551447)

[7.3. Implementation 43](#_Toc130551448)

[7.4. Acceptance Testing 43](#_Toc130551449)

[7.5. Quality of Service 44](#_Toc130551450)

[7.6. Project Management 44](#_Toc130551451)

[7.7. Operational Review Meetings 44](#_Toc130551452)

[7.8. Project Progress Reports 44](#_Toc130551453)

[7.9. Training 45](#_Toc130551454)

[7.10. Documentation 45](#_Toc130551455)

[8. Maintenance and Support Services 47](#_Toc130551456)

[9. References & Relevant Experience 49](#_Toc130551457)

[10. Sufficiency of the Tender 50](#_Toc130551458)

# Background Information

MIC2 is in the process of replacing its current SMSC and Antispam platform in order to introduce the latest technologies (ex. 4G, LTE, 5G etc.) in terms of SMS services and SMS anti-spam functionality. SMS remains a convenient communication method for customers and the introduction of additional SMS services encourages them to increase their usage. To maximize the benefit and revenues from this service, it is important to protect both customers and the network from spam and unauthorized messages.

The proposed platform should be able to consolidate all the messaging needs of MIC2. It should also include bulk messaging control tools.

With the introduction of IMS and RCS, it is mandatory for the proposed solution to follow this trend. Great emphasis is placed on the integration with IMS and the support of convergent messaging. The vendors are encouraged to provide their latest comprehensive solution for current and future messaging needs.

# General Requirements

Below is a list of the general requirements that the bidder of the SMSC platform shall ensure:

* The bidder shall propose his state of the art, future proof, SMSC and message filtering solution.
* The bidder shall describe in detail the hardware and software architecture of the proposed SMSC Solution including the built in redundancies.
* The following factors have a  critical business impact and will be considered mandatory in our assessment and will lead to an early disqualification of the bid if not addressed in detail by the bidder
  + The bidder should have an international bank credit rating of a minimum of BBB+ along with a five year roadmap and a minimum of 5 years’ experience in the messaging and VAS platforms (Killing Factor)
  + The bidder shall provide minimum 5 mobile operators references with similar project in different countries and continents whether in MENA, EUROPE or US with a minimum of 3 million subscribers for each deployment (Killing factor)
  + Bidder shall have at least 5 suitably certified & qualified experienced engineers based in the MENA or Gulf region with a min of 5 years’ experience with similar platforms. CVs of such engineers to be submitted with bid. (Killing Factor)
  + The bidder could propose highly qualified regional support for the platform. A minimum of 3 references should be provided for the regional support organization in the information and communications technology field.
  + The bidder should provide a security module enabled on the SMSC platform to enhance protection & prevent vulnerabilities on the Signaling System 7(SS7) & Sigtran links protocol etc. Evidence & reference of deployment in three mobile operators with minimum of 3 subscribers. (Killing Factor)
  + The bidder must have high level of partnership (i.e. Gold, Strategic & Global etc. with the supplier of the platform
  + The bidder must provide escalation chart, hotline in case of trouble incidents.
* The vendor shall include in his offer a detailed Bill of Quantities (BoQ) for all relevant Hardware, Software, and Services that are needed for the delivery of vendor’s proposed solution together with the yearly operation and maintenance support.
* The vendor shall provide maintenance for the SMSC platform and ensure that the solution complies with the telecom industry’s norms including:
  + Maintaining the solution up-to-date
  + Ensuring the solution and network elements availability
  + Ensuring a smooth operation for the solution
* The vendor shall include a free of charge three years warranty period after the full integration and acceptance of the SMSC platform.
* In the commercial offer, the vendor shall provide a separate pricing table for the OpEx and CapEx. For the CapEx as well as for the OpEx, SW and HW pricing needs to be differentiated. In the SW pricing, premium support must be quoted separately, SW licenses, and professional services, each in a separate quotation. In addition, separate pricing should be presented for each feature/service. For the HW elements, the vendor shall provide detailed description about every aspect of the proposed HW including but not limited to CPU, Memory, Hard Disc, Operating system, Cards, Interfaces…
* The solution should offer a flexible licensing model and a low Total Cost of Ownership.
* The vendor shall specify if his solution supports virtualization. In this case, detailed dimensioning requirements should be specified.
* In the commercial offer, the pricing table shall include the quantity, the unit price, the total price, as well as the description of the elements.
* The vendor shall submit proposals, documents, manuals, drawings, circuit diagrams, etc. in English.
* The vendor’s proposed SMSC solution (Hardware/Software) and services shall comply with the RFP requirements. However, since the RFP represents MIC2’s basic requirements, the vendor may include in his proposal value added, cost-effective and OPEX saving solutions. The vendor’s value added solutions shall be included separately in the detailed BoQ and detailed in a separate section in the technical specifications, and executive summary.
* The vendor shall be fully responsible of the interoperability and integration of the SMSC with MIC2 network elements (HSS, MSS, HLR, STP, USSD, IMS, NGBSS, Message Router, Data Core, Billing System, Provisioning System, Content Providers, EMC storage and any other necessary entity to deliver all the services required by MIC2. The vendor will also be fully responsible of the interoperability and integration of SMSC Solution with third party applications or platforms.
* The Vendor shall provide all Hardware requirements (network and power cables, connectors, E1 cards, device for backup…) to install, integrate, connect, and launch the SMSC Solution.
* The vendor’s solution shall provide complete geographical redundancy and continuity of service (Hardware/Software) for the SMSC Solution. The solution should provide 99.999% availability.
* The solution design shall ensure that no single point of failure would affect the operation of the service. The solution shall be easily and smoothly upgradable to new releases with a possibility of rollback without any system interruptions.
* The vendor shall list all features that are available within the SMSC Solution. Accordingly, the Vendor shall specify the offered and non-offered features from the available list. Each feature shall be quoted independently with full functional description and needed integration with MIC2 network entities.
* The vendor shall provide a detailed integration plan with the existing operational network.
* The vendor shall provide detailed information of the company’s ownership, financials, structure, organization and market position specifically for VAS products.
* The vendor shall not be involved in bid rigging directly or indirectly with MIC2 or the concerned public body to ensure fair trading grounds.
* The vendor shall specify the locations of the manufacturing, support, and research and development centers of each product and service offered in the SMSC Solution, supported by references.
* The required delivery, implementation and integration periods are 4 weeks and 12 weeks, respectively.
* The solution shall be capable to interface with standard service providers’ interfaces and protocols.
* Delivery shall be based on DDP (Delivery Duty Paid) incoterms including VAT, transportation and insurance during transportation and all related taxes and charges.
* Applying vendors shall provide upon request, in addition to the required documents, a demo to explain to MIC2 their solution composed of:

1. Technical presentation
2. Live demonstration on a testbed or on a live operating network

### Further Requirements

MIC2 may choose to reject a RFP, without prejudice to any other civil remedies  
available to MIC2 or any criminal liability the proposal may attract, if the bidder:

1. fixes or adjusts the prices shown in its bid by or in accordance with any  
   agreement or arrangement with any other person or by reference to any other  
   RFP; or
2. adjusts or amends or changes the weighting of evaluation matrix or statement of compliance after the RFP is launched; or
3. agrees with any other person to carry bid rigging in this RFP or previous RFP; or
4. attempted directly/indirectly to persuade any servant of a public body or workforce of MIC2 to accept any bid. Obtained directly or indirectly or tried to obtain confidential information from MIC2/or the concerned public body regarding other proposal bids received
5. offers or decides to pay or provide, or does pay or give any sum of money, incentives or gifts directly or indirectly to any person for doing or having done, or for causing or having caused to be done any act of omission in relation to any other bidder whether this RFP or previous RFP within the last 10 years; or
6. in connection with the award of the Contract, commits an offence under the  
   Prevention of Corruption Acts (UNCAC, Council of Europe Criminal Law Convention on Corruption Law, Lebanese legislations No. 154 of 1999, Law No. 44 of 2015, and the Whistleblowers’ Protection Law No. 83 of 2018,  Acts 1889 to 1916 ) or gives any fee or reward the receipt of which is a criminal offence

# Short Messaging Service Center Requirements

This section defines the functional services of the SMSC Solution as well as the required dimensioning specifications. The solution should fulfill all the following requirements.

## Solution requirements

The solution shall handle all SMS traffic in all directions, Mobile Originated (MO) messages, Mobile Terminated (MT) messages and Application Originated (AO) messages.

The solution shall provide advanced anti spoofing and anti-spam functionality for Mobile Originated (MO) messages, Mobile Terminated (MT) messages and Application Originated (AO) messages.

The solution should support home routing of incoming messages.

The solution should support the diameter interface with multiple IN and online charging systems. The current IN is NGBSS from Huawei. All diameter requests should be supported including credit checking, amount deduction, amount reservation, and refund. The solution should comply with the latest diameter standards and support Diameter V8 and above.

The solution should support charging all messages submitted by customers in real time. It should also be able to differentiate between roaming and local traffic in case the operator wants to charge only messages sent while the customer is roaming outside the network. The solution should allow blocking of most short codes while roaming.

The solution shall be able to differentiate between prepaid and postpaid customers based on any of the following methods: HLR or HSS queries, response from OCS, billing database, local database, and number ranges. The Vendor shall list all available methods.

The solution shall support online charging for MT billing services. It should allow charging per MT SMS based on specific rules for each service.

The solution should include a control mechanism to protect the customers from abuse from MT billing. Such controls include preventing MT billing messages from going to customers not subscribed to premium VAS services and controlling the daily/weekly/monthly charges associated with these services.

The solution shall support the SMPP protocol versions 3.3, 3.4 and 5.0. All basic and optional features of the SMPP protocol should be supported including but not limited to UDH support, optional TLV parameters, replace message, silent SMS, flash SMS, source and destination port, sar segmentation, data\_sm etc.

The bidder should propose separately the option to support mobile number portability (MNP) without the need for an upgrade or additional investments. This should be included in the BoQ and clearly demonstrated as optional.

The solution shall provide overload protection to prevent a system crash in case of overload.

The solution shall support lawful interception and provide the needed interface for this functionality.

### Signaling requirements

The proposed solution shall support SIGTRAN/M3UA signaling connectivity with MIC2’s core network elements. SIGTRAN multi homing shall be supported for link redundancy.

Flexible routing shall be available at the signaling layer in order to configure different routing possibilities like primary/secondary or load sharing. Load sharing or message distribution configurations shall be applicable individually to SRI, MO and MT operations.

The solution shall support optimization of the signaling traffic by using all methods that could decrease the signaling load such as:

* Subscriber Location Data Caching
* More Messages to Send
* SRI Results Cache
* MAP Protocol Version Cache

The solution shall support MAP version 3 with support of version negotiation and fallback to version 2 and version 1 as specified in GSM 09.02.

The administrator should have the ability to set the default Map version to use for different country codes or GT prefixes.

The solution shall have a dedicated translation table for the translation of SCCP addresses. The translation is used for routing international traffic to various SMS hubs for delivery by adding certain prefixes to the SCCP GTs.

The solution shall support the AlertSC operation with the possibility to set a configurable deferred trigger value. The deferred trigger allows the handset to be fully initialized before receiving the messages.

The SMSC shall be able to record the Cell\_ID of the message originator and recipient. This could be done by using the MAP extension container that includes the location information.

The solution shall support a single GT addressing where multiple nodes can be seen as one entity by the network.

### Basic SMSC features

The proposed solution shall support multiple character sets and DCS values as defined in GSM 03.38 and 3GPP 23.038:

* 7 bit Alphabet used for plain text messaging
* 8 bit Binary used for sending binary messages such as smart messaging and EMS
* 16 bit UCS2 used for sending non-Latin language based messages such as Arabic messages
* ISO-8859-1 (Latin 1) character encoding should be supported for sending French characters.
* ISO-8859-15 character encoding should be supported

The SMSC shall support all the message classes defined in GSM 03.38 and 3GPP 23.038

* Class 0: Immediate Message Display
* Class 1: Mobile Equipment Specific
* Class 2: SIM Card related
* Class 3: Terminal Equipment specific

The SMSC shall support the store and forward operation mode, the datagram mode and the transaction mode.

The SMSC shall support EMS messaging.

The SMSC shall offer an advanced configurable retry algorithm. The SMSC should have multiple retry profiles and retry schemes that could be set by the administrator. The message retry scheme should be determined by a combination of factors including the message priority, the submission interface, the SMPP account, the network error…

The SMSC shall have a flexible error mapping that enables errors from different networks, from ESMEs, from charging systems to be processed correctly and logged in CDR’s.

The SMSC shall have a flexible address translation table. It should be able to receive messages in multiple number formats and normalize them in the international format. The translation can occur on multiple parameters including originator and destination numbers, TON, NPI, Terminal Type, PID, SC address…

The SMSC should also offer full flexibility in the routing of messages based on different parameters including originator and destination numbers, TON, NPI, Terminal Type, PID, SC address etc.

All address translation and routing operations should be applicable on an exact match or on a prefix match. Wildcard operators to replace a single digit or multiple digits should be supported.

The SMSC shall support multiple number range formats. For example messages could be submitted in the formats 03xxx, 70xxx, 009613xxx, 0096170xxx, etc.

The SMSC shall support all values for the User Data Header. It should be able to support all message types like concatenated messages, picture messages, operator logos, ringing tones, EMS messages, WAP WDP, WAP push, OTA configuration messages…

The SMSC shall support message reassembly and segmentation to the overcome the size limitation of the SMS. When handling long messages, the CDR should clearly indicate the number of segments in each message. It should be possible to bill the message as a single long message or as multiple segments separately. A single delivery report should be returned for long messages.

The SMSC shall support delivery reports. As some handsets do not support sending regular delivery reports, the customer shall be able to request a delivery report from within the message text by using a special character at the beginning of the message.

The SMSC shall support multiple priority levels for messages coming from customers or messages coming from different applications. External applications should be able to flag messages as priority. Also the system administrator can specify if all messages from a particular interface are sent as priority. When sending high priority messages, the HLR/HSS priority flag should be sent to force message delivery when possible. The administrator can choose to apply high priority on all messages handled by the system.

The SMSC should support the message validity period setting and the administrator should be able to set the maximum validity period allowed on the system.

The SMSC shall support message scheduling.

The SMSC shall support black listing and white listing certain numbers or number ranges.

The solution should support the virtual SMSC concept with various service center addresses. Each service center should have an independent configuration profile.

The SMSC shall support inter-ESME routing that allows sending messages from one application to another.

The SMSC shall support duplicate message detection and block duplicate messages if needed.

The SMSC should be able to throttle incoming messages from external content providers according to the threshold set for each one.

The SMSC shall be able to detect whenever a user sends repetitive SMS to short codes which could be used for abusing VAS services. It should be possible to block such messages in real time to prevent fraud.

### Antispam features

All anti-spam features should be applicable selectively to On-Net and Off-Net traffic.

The platform should support Home Routing to filter incoming MT messages from foreign networks. It should be able to send back a fake IMSI to foreign networks to protect the customer identity.

The solution should block all messages coming from international grey routes. It should have enough intelligence and automation to filter spam and application originated traffic while allowing legitimate peer to peer traffic to pass through.

It is important that the detection of spam and flood situations happens in real time and that the proper action is taken automatically to stop the spam situation.

Different profiles and sending rates could be defined for different originator networks. The anti-spam rules could be applied differently to different originator networks. Matching could be done based on prefixes and in case multiple prefixes are matching, the solution should apply the best match algorithm to determine the action to take.

It should be possible to combine the different anti-spam rules differently in each profile defined.

The following actions should be available when defining anti-spam rules:

* Allowing the message
* Marking the message or the sender as suspicious
* Real-time blocking
* Block / Send NACK
* Block / Send ACK
* Generating an alert

Alerts need to be raised immediately in the event of high incoming off-net SMS due to various reasons of spamming or flooding.

The solution shall support TCAP handshake to validate the originating network of the message.

The administrator should be able to define exceptions for some rules.

The solution shall generate detailed statistics on the allowed and blocked traffic. The statistics should be available by blocking reason, by sender, by originating GT, by content list, etc.

Anti-spoofing:

The platform should provide anti-spoofing functionality by making an HLR/HSS interrogation for submitted MO messages. It should be possible to configure per PLMN (set of GT prefixes) the number of prefix digits which should match with the SCCP calling party GT. The administrator should also be able to configure some MSC addresses that are whitelisted and for which no HLR/HSS interrogation is done.

Anti-faking:

The solution should provide advanced anti-faking capability to prevent unauthorized messages from reaching the customers. It should allow the detection and prevention of faking the originator MSISDN, the source SC-Address, the source MSC-Address or any combination of the above.

The solution should also provide delivery procedure integrity check to make sure that MT-FW-SM MAP operations are preceded by a corresponding SRI request. It should be able to prevent cases where a spammer uses different originating SC addresses when obtaining recipient's identities and location information and when sending MT messages.

Anti-flooding:

The solution should be able to automatically detect and prevent flooding situations. Flooding can be determined based on sender, originating network, content, destination numbers....

The solution shall support traffic monitoring based on sliding time slices and take the appropriate action when flood is detected.

The solution shall detect messages submitted to different numbers incrementally or according to a regular pattern.

Content filtering:

The solution should provide advanced content filtering protection. The following are the basic requirements for content filtering and additional features should be described in details in the offer:

* Repeated content with slight modifications in the text should be considered as spam.
* Ability to define blocked keywords in different languages (English, Arabic, French, in Unicode...)
* Keywords defined should be case insensitive.
* Keywords could contain wildcard characters.
* Keyword analysis - must include and not limited to the below in order to monitor suspected messages:
* It should be possible to block messages based on an individual keyword or on a combination of keywords present in the message. Key words can be combined which logical operators like AND, OR & NOT.
* It should be possible to assign a weight for each keyword. A score is calculated for the message based on the keywords present and if the score reaches a certain threshold, the appropriate action could be defined for the message.
* The solution should be able to block binary SMS.
* The solution should be able to block messages even when spammers use different characters to bypass spamming. For example the use of the letter 0 instead of o or 1 instead of i.

SMS Anti-phishing:

* The solution should be able to perform UDH screening and application port filtering to filter messages that contain malicious content that could be used to infect smartphones.
* The solution shall be able to block messages containing malicious content or download links to such content.
* The solution shall be able to block SMS phishing messages that ask subscribers to provide sensitive, personal, and/or financial information

Originator filtering:

* The solution shall be able to block all messages coming from alpha-numeric sender IDs.
* The solution should block all messages coming from foreign networks with an originator that starts with 961 prefix.
* The solution should block all messages coming from foreign networks using a short code originator.

Black and white listing:

* The solution shall provide originating SMSC address blacklist/whitelist.
* The solution shall provide originating MSC address blacklist/whitelist.
* The solution shall provide originating/destination MSISDN blacklist/whitelist.
* The solution shall provide originating/destination IMSI number blacklist/whitelist.
* The solution shall provide monitoring of the outcomes added to the blacklist.
* Blacklisting could be done based on prefix matching. In case multiple prefixes are matching, the solution should apply the best match algorithm to determine the action to take.

In addition, the solution shall provide the following features (and not limited to the below):

* The solution shall provide high frequent monitoring function.
* The solution shall provide high frequent monitoring function.

### SMS Forwarding (subscriber service – quoted separately)

The solution should provide SMS forwarding (SMS divert), hence short message can be forwarded to another user automatically. As an example: If user X forwards all short messages received to user Y, then when user Z sends a short message to user X, the short message are received by user Y, not user X. Note: the solution should permit only forwarding once. (Multi-forwarding will not be allowed/permitted). The solution should identify whether the user requested or it’s a system administrator request.

This feature will be provided as a subscription service through a short code or a web page interface. The interface should be user friendly and easy to use. Operations should be fast and efficient taking into consideration HCI (Human Computer Interaction), UI (User Interface) and UX (User Experience) best practice design. The web interface should integrate seamlessly with MIC2’s website.

### SMS Autoreply (subscriber service - quoted separately)

The solution should provide SMS auto-reply service, whereby the system automatically sends a predefined message back to the sender. The system will allow a maximum short message length of 140 bytes.

This feature will be provided as a subscription service through a short code or a web page interface. The interface should be user friendly and easy to use. Operations should be fast and efficient taking into consideration HCI (Human Computer Interaction), UI (User Interface) and UX (User Experience) best practice design. The web interface should integrate seamlessly with MIC2’s website.

### SMS Filtering (subscriber service - quoted separately)

The solution should provide SMS firewall service, whereby the system blocks certain selected numbers based upon subscriber request.

* The solution shall provide whitelist filtering - only messages from certain specified numbers in the white list will reach
* The solution shall provide blacklist filtering - messages from the specified blacklisted numbers will be blocked up to a maximum of 30. (an as example)
* The solution shall provide time frame whereby no messages are received.

This feature will be provided as a subscription service through a short code or a web page interface. The interface should be user friendly and easy to use. Operations should be fast and efficient taking into consideration HCI (Human Computer Interaction), UI (User Interface) and UX (User Experience) best practice design. The web interface should integrate seamlessly with MIC2’s website.

### Interworking with IMS

The platform should be 3GPP compliant for short message interworking between SIP/IMS endpoints and legacy SMS network with support for both transport and service level

The solution shall support the evolution to convergent messaging and shall support full integration with RCS platform if needed.

The solution should provide all the IP-SM Gateway capabilities to ensure the efficient exchange of SMS messages between SIP-enabled devices, (dual mode) handsets and standard phones by translating SMS messages in the proper format and delivering them in the appropriate domain (SS7 or IMS). The required level of interworking may be determined based on a subscriber profile as well.

The solution shall integrate with Touch IP-SM-GW on the E/Gd interface over MAP.

For messages coming from foreign users, the IP-SM Gateway should include a home routing function that can determine, based on the subscriber profile, if the message must be intercepted for delivery to the SIP-enabled device.

The solution shall support the fallback of delivery to the circuit switched network for delivery of SMS when the IMS registered recipient is not attached to the IMS network

The solution shall support diameter queries of subscriber profile from HSS to apply the preferences of the operator and of IMS-registered mobile subscribers when delivering messages.

The SMSC should support the IMS registration/deregistration process and checking the HSS profile via diameter over the Sh interface.

All requested functionalities including home routing, anti-spoofing, anti-faking, content filtering, anti-flooding should be applicable to both on-net and off net messages whether over the IMS or over the legacy circuit switched networks.

### Application/Message Router

The bulk messaging solution should accept both way SMPP connections form content providers (for sending and receiving messages).

The bulk messaging solution should provide APIs for both way SMS communication. APIs should be easy to use by external parties for sending and receiving messages with the possibility of requesting delivery reports.

The solution should allow load sharing the traffic between multiple SMSCs.

The solution should allow primary/secondary routes. In case the primary connection with the SMSC is not available, the secondary connection is used.

The solution should allow different routing configuration per user account and/or per connection.

The solution should allow the administrator to set a default value for certain message parameters or force these parameters to certain values. For example, it should be possible to set the value of the **service\_type** parameter used in SMPP to a certain value per user account and/or per connection. These parameters include but are not limited to: TON/NPI values, message validity, originator, **service\_type, etc.**

The solution should provide an anti-spam function to filter all submitted messages. Filtering should be based on multiple criteria like originator, destination, content…

The following interfaces should be supported at least with content providers:

* SMPP v3.4
* SOAP/XML
* HTTP
* API
* Other…

The following interface(s) should be supported at least with the SMSC:

* SMPP v3.4

The solution should be able to translate the message to the required protocol according to the interface type.

The solution should allow multiple connections for the same content provider using the same interface as defined by the administrator.

The solution shall allow multiple SMPP connection modes (transmitter, receiver, transceiver).

The solution should be able to throttle incoming messages from external content providers according to the threshold set for each one.

The solution shall allow blacklisting or whitelisting originators for each content provider. The solution shall allow the use of dynamic originators for some connections.

The administrator can restrict the destinations allowed for each content provider (per country and per operator).

The solution should support multiple messaging modes like normal, broadcast and priority.

The solution should allow restricting the IPs used to connect to each user account.

The solution shall allow managing the delivery reports per connection. The administrator can allow or restrict delivery reports for certain connections.

### MT billing control

The solution shall provide an intelligent way to protect customers from abuse when they subscribe to services subject to MT billing. It should be possible to restrict content providers from sending messages to customers who are not subscribed to their services. Also it should be possible to limit the number of messages sent to subscribers from MT billing services to X SMS per service per Y days.

It should be possible to limit the renewal of any service to predefined rules/timeframe: i.e.: if the service is monthly, renewal must be at the end of the month only, no renewal within the same month unless agreed upon.

The solution shall provide the ability to set a maximum number of MT SMS per day/week/month per subscriber per service. If the provider sends more messages than allowed in the service rules, the additional messages can either be blocked or allowed. In the latter case, the application shall not bill the customer as per the MT rates, but instead it should identify the surplus of SMS in another table/report to be billed at the end of the month to the service provider based on the bulk SMS rates.

The solution shall provide multiple interfaces for sending MT billing messages. The minimum required interfaces are SMPP and SOAP/XML APIs.

The system administrator should be able to define accounts for content providers with specific rules for each service.

The system administrator should be able to restrict the sender IDs or short codes used by each content provider for sending his messages.

The solution should allow sending concatenated messages and allow billing them as one or multiple messages.

The solution shall generate all needed reports for MT billing.

### Bulk SMS campaign manager

The solution shall provide a comprehensive end to end solution for SMS bulk broadcasts.

The solution shall provide multiple interfaces for sending bulk SMS campaigns, mainly web interface, PC client, SMPP, HTTP, SMS API, etc.

The interface should be user friendly and easy to use. Operations should be fast and efficient.

The web interface should integrate seamlessly with MIC2’s website. The look and feel of the web interface should be easily modifiable to fit future requirements.

The administrator can define multiple user accounts.

The administrator can define the available features and maximum throughput that can be used by each user account. Features include delivery reports, flash SMS, Wap push SMS, broadcast window…

The administrator can restrict the originators used for sending SMS for each account/subaccount. He can also restrict the destinations allowed for each user account (per country and per operator).

Originators can be requested by account users and sub-users via the provided interface. The request should go to corporate sales for their approval. Once approved, the customer should be able to send messages using this new originator.

Accounts can be defined as postpaid or prepaid. Prepaid accounts use predefined bundles in the system. For example, a prepaid user can purchase a bundle of 10,000 SMS valid for 3 months. Multiple bundles can be defined in the system. A prepaid user should not benefit from the remaining SMS past the expiry date of the bundle. A prepaid user cannot send more than the number of SMS allowed in the package.

The solution shall support SMS bundles of varying denominations and expiry. Bidder shall offer a complete solution to subscribe to and charge these bundles for different user groups.

If a user renews his bundle or subscribes to another one, the new bundle will not be used until the first one is depleted or expires.

If allowed by the administrator, account users can create sub-accounts with less or equal privileges than the account user.

The interface must be adjustable according to the access rights given to the user

The following user accounts shall be supported at the least:

1. System administrators
2. Account user
3. Account sub-user

The bulk messaging solution should support all SMPP v3.4 operations.

The platform should support multiple languages for sending SMS (English, Arabic, French, Unicode…)

The platform should support both ISO Latin 1 and default GSM 7 bit alphabet for English messages.

The solution should allow sending concatenated messages and allow billing them separately. It should indicate on the interface the number of characters and the number of concatenated parts in the message.

The message to be sent can contain multiple parameters. The list of recipients and parameters can be easily uploaded using Excel, comma separated files…

The user can define multiple mailing lists in his address book.

Recipients in the mailing lists should be easily manageable.

The user can upload recipients to the address book or mailing lists in a fast and efficient manner. The uploaded file can contain up to 3 million records. Duplicate and invalid recipients are automatically identified and deleted during the upload process. A notification is sent to the user and deleted records can be retrieved in a separate report.

Mailing lists can be imported in multiple formats like text, excel, csv, access…

The user can easily edit the address book and mailing lists by adding and deleting numbers.

The user can easily search for contacts in the address book.

Mailing lists can handle a large number of contacts (at least 3,000,000)

The solution should filter wrong numbers that do not match certain criteria in the mailing list.

The user can have the option to define his own number for testing the message before it is sent and to receive the message at the beginning and at the end of the campaign.

The throughput for each individual campaign can be controlled separately. The total throughput for each user or connection should not exceed the limit set by the administrator.

A campaign can be set to send X messages per day at a rate of Y msg/sec during a specific interval of time. The campaign will run daily until all the messages are sent.

The campaign can be scheduled at a specific date and time. Recurrent messages can also be scheduled.

The solution should allow scheduling of recurrent SMS

The user or administrator can easily pause or stop a running or scheduled campaign. He can then resume it or cancel it.

The user can request delivery reports if allowed by the administrator and obtain a report regarding the success rate and the list of delivered and undelivered messages at any time during the campaign.

Messages can be saved as templates for use multiple times.

The solution should allow sending messages to predefined distribution lists. These distribution lists are defined by the system administrator while the end users do not have access to the records in the distribution list. End users can only know the total number of records in the list.

### Bulk SMS Opt-out solution

The vendor shall provide a solution to allow individual customers to block incoming A2P messages from a specific sender ID or messages starting with predefined keywords.

The solution provided shall allow the operator to define 2 options described below for opting out of bulk messaging.

**Option 1: Sender ID based solution**

The user must be able to block SMSs from a certain sender ID by sending the command “stop Sender ID” to a pre-defined short code. Any message from the specified Sender ID should be blocked."

**Option 2: Keyword based solution**

With this option it is assumed that any advertising SMS shall include in its content a keyword indicating that the SMS is of an advertising nature and the advertiser’s name. For example the message content could start with ADV\*brand\_name\*

The user must be able to block SMSs from a certain advertiser by sending the command “stop brand\_name” to a specific short code. Any message whose content starts with the specified keyword ADV\*brand\_name\* shall be blocked."

"Each user must be able to manage the sender IDs or keywords for the incoming advertising messages through SMS commands:

• to block messages from certain Sender IDs

• to block messages starting with ADV\*brand\_name\*

• to unblock messages from certain Sender IDs

• to unblock messages starting with ADV\*brand\_name\*

• to Retrieve a list of all blocked advertiser name (i.e. “The following advertisers are currently blocked: name1, name2, name3”)"

The system shall always return a configurable confirmation message (i.e. “All Ad messages from XXX will be blocked/unblocked”)

The solution must include an interface/application to be provided for the user to manage the incoming SMS (block, whitelist, blacklist, per sender, per type etc.)

The solution should be able to differentiate between and identify transactional SMS from advertising Bulk SMS based on preset criteria (for example based on connection or keyword in the message or specific Sender ID…)

The solution must add the opt out instructions to all advertising SMS (i.e.: to block please send block + sender ID or send block + brand\_name to specific Short Code)

The opt-out solution should support all languages including English, Arabic and French.

The opt-out solution shall have a dedicated API which can be called by provisioning to reset the opt-out rules in the case where the GSM line is trashed or deactivated.

The advertiser name and sender ID should be case insensitive.

The subscriber shall also have the choice to unsubscribe from messages of a bulk nature while still receiving one to one messages like banking transactions and notifications.

Messages from providers set as trusted shall not be filtered.

The solution shall generate reports for each connection or content provider which includes the count of messages sent and delivered without taking into account the count of characters of the appended message which contains the instructions for opting out. (for billing purposes)

"The solution shall generate statistical reports (detailed by sender ID and by Service Provider) such as:

- Monthly count of blocked messages due to opt out.

- Monthly count of SMS sent that are not advertising (do not include ADV)

- Statistical reports such as the number of sender ID’s blocked and whitelisted during a specific period"

### SMS Grouping (subscriber service - quoted separately)

SMS grouping (subscriber service) - Possibility to define groups and distribution lists for each subscriber with a limited number of users.

### Optional items

The below list includes some optional items that can be included with the proposed solution. The vendor can list additional optional features that are supported by the system. Optional items should be quoted separately if needed:

* Personalization of MO SMS with signature, alias etc.
* SMS parental controls
* SMS filtering control (subscriber service) – based on keywords
* SMS to Email feature – Possibility to send a short message to an email account
* SMS advertising which allows the insertion of advertisements in messages
* External service application triggering. The SMSC can trigger external application at various points in the message delivery process. Actions could be defined based on the return values of these systems.

## Dimensioning, Capacity and Architecture

The bidder shall provide a test-bed where all rules, features and configurations can be tested before being applied to the live system.

The SMSC Solution license should handle a throughput of at least 1000 SMS/sec.

The hardware provided should allow a throughput of at least 2000 SMS/sec.

The SMSC shall be able to store at least 4 million messages that are pending delivery. The vendor should detail the message storage mechanism and what happens in case the storage is full. The solution must include a monitoring for the SMS within the buffer. The SMSC should provide an alarm if system overloads the control mechanism.

The system should be able to store information, data and CDRs for at least 3 months.

The system shall maintain high KPI levels with a short round trip time upon message submission and delivery.

The system should be connected to MIC2’s EMC storage system. The Vendor should provide the needed interface cards, cables and connectors.

The system shall be able to support virtualization. Detailed requirements and dimensioning information are needed in this case.

There shall be no license on the number of subscribers.

There shall be no license limitation on the number of clients and applications connected to and/or provisioned on the system.

There should be no limit on the number of services created on the system.

The Vendor shall provide all necessary data for the proposed solution (layout, dimensions, servers, power consumption, heat dissipation, floor plan...).

The SMSC Solution shall have enough interfaces to connect to all needed entities in MIC2’s network.

The Vendor shall provide all the hardware requirements (network and power cables, connectors, E1 cards, device for backup, HBA cards, Fiber cables…) to install, integrate, connect, and launch the SMSC Solution. The Vendor shall explicitly state the capacity of each interface card that is used as well as the capacity of each signaling board.

The Vendor shall specify the main performance characteristics and describe the KPI’s to measure the performance of the system.

The solution design shall be done in an optimal way with the efficient use of hardware elements. The solution design shall be flexible in order to introduce upgrades and modifications with a minimum alteration to the system architecture.

The solution shall provide scalability, load balancing and fault tolerance as detailed below:

1. **Redundancy**

The provided system should be **geographically redundant**. The vendor shall describe how geographical redundancy is designed and how the traffic is distributed to the different nodes. Automatic switchover is a must in case of active/standby configuration.

The bidder shall describe in details the hardware and software redundancies in the system.

The system shall handle any failure by having redundant elements in its architecture in order to ensure stability and robustness. Redundancy shall be applied to network links as well as to all system elements. If any of the links or elements shuts down, the load shall automatically transfer to other active links or components to ensure service continuity with minimal loss of information. Such redundancy can be achieved by having redundant servers along with CPUs, RAMs, Ethernet Cards, signaling boards, etc. All databases should work in a cluster mode.

1. **Scalability**

Scalability shall be explicitly and clearly stated, i.e. the exact number of transactions/second, the exact number of simultaneous dialogues that the system can support, the maximum load the system can handle, the SW licenses or HW elements that are the keys for scalability and that might be needed for future expansion.

The system shall be as scalable as possible in order to cope with the increasing traffic demands. Therefore, interface cards, signaling boards or even servers shall be added with ease whenever there is need in order to meet the increase in the number of simultaneous transactions. The system shall be able to add new hardware modules in order to allow an increase of the system’s capacity.

The vendor shall provide a clear description on how to expand the system, what elements (SW licenses and HW) need to be added and their respective quantities. For this, the vendor shall provide a layout detailing the key elements of the end-to-end solution, identifying which components are the keys for such expansion.

1. **Load balancing**

The system shall use a load balancing mechanism in order to distribute the workload evenly over the available links and servers and to assure multilink redundancy.

1. **Fault Tolerance**

The system shall be as resilient as possible in order to identify and respond to hardware and software failures. The system shall raise alarms whenever unexpected errors occur. Components shall have built-in fault tolerance. Failures shall be detected early, isolated, and automatic recovery shall be started immediately. The occurrence of faults in a particular component shall not affect the operation of the system as a whole.

No single point of failure shall exist in the architecture.

The system shall have 99.999% availability, and the highest level of redundancy and reliability

The bidder shall specify the MTBF (mean time between failures per module), the MTTR (mean time to repair per module). Note that no part of the solution should be a single point of failure.

1. **Networking requirements**

The Vendor shall provide all the needed network cabling and network devices confirming and abiding to the following guidelines. The cabling guidelines are the below:

* + CAT6 cabling is required.
  + Patch panels should be used for cabling. Each run of a cable should be terminated to a patch panel termination. Each patch panel termination should be labeled, as well as each port in the building.
  + All needed patch cords should be provided and labeled on both ends
  + Each cabinet should have the needed number of cable organizers, in order to neatly wrap and organize all cables, eliminating the mess of tangled cables.
  + All cabling should be done in a closed cabinet
  + Network devices should also be placed in a closed cabinet
  + Each device should have a redundant power supply from a different source
  + Each server or device shall be clearly labeled
  + Network Devices shall abide by the following:
    - Cisco devices shall be used
    - Latest stable IOS version
    - Manageable by Cisco LMS
    - Support ISE features:
      * MAC Authentication Bypass
      * 802.1x
      * Web Authentication (LWA, CWA)
      * Change Of Authorization (CoA)
      * VLAN
      * DACL
      * Secure Group Access (SGA)
    - Redundant power supplies
    - In addition to the current provided features, all IOS shall support but not limited to:
* ssh service
* SNMP v3
* security features
  + - The Device roadmap shall be provided since the device lifetime will be checked and evaluated.

# Billing and Integration Requirements

In order to assure end-to-end functionality, the system shall be compatible for proper integration with different involved parties and shall provide proper call detailed records.

## SMSC Solution – Billing System

The system shall be integrated with MIC2’s billing system in order to allow charging for bulk messaging. The charging process is performed by generating call detail records (CDRs) upon completion of transaction.

These records shall include all details related to the message like date, timestamp, originator, recipient, originating MSC, destination MSC, Cell\_ID, type, length, size, service type, account, connection, interface, delivery status, content, etc... These CDRs shall be stored locally and transferred to the billing system at the same time.

The generated CDRs should contain the CELL\_ID of the originator and the recipient of the message.

The proposed solution shall be able to generate 2 parallel CDR streams. One CDR stream is used for billing purposes and contains all needed parameters. The second CDR stream contains the message text. Access to the second CDR stream should be highly restricted.

The system shall be able to generate CDRs in CSV format. The included fields shall be configurable by the administrator.

For CDRs that contain message content, the UDH header, if present, shall be generated in a separate field. A specific field shall indicate the data coding scheme used. For Unicode messages, the full Unicode string shall be generated.

CDRs should be generated in one line even if the message text contains a “New Line” character. The field separator shall not appear in the message content.

The system shall be able to integrate with MIC2’s billing system using open protocols and standard interfaces like SFTP over TCP/IP for example.

The system shall be able to generate reports for content provider billing. Reports for postpaid billing shall be generated in real time and shall always be up to date.

Billing file rotation should be configurable. Billing files can be closed after a configurable time or after reaching a pre-determined size or a combination of both.

CDR records should contain at least the following fields:

* ID
* ORIG\_NETWORK\_TYPE
* MSG\_TYPE
* ORIG\_ADDRESS\_TON
* ORIG\_ADDRESS\_NPI
* ORIG\_ADDRESS
* SCCP\_ORIG\_ADDR\_GT\_ADDR
* RECIP\_ADDRESS\_TON
* RECIP\_ADDRESS\_NPI
* RECIP\_ADDRESS
* SCCP\_DEST\_ADDR\_GT\_ADDR
* MSG\_STATUS
* MT\_IMSI
* MSG\_ORIG\_SUBM\_TIME
* PAYLOAD\_INFO\_SIZE
* PAYLOAD\_INFO\_NUM\_CHARS
* CONCAT\_INFO\_MAX\_SEGMENTS
* CONCAT\_INFO\_CURRENT\_SEGMENT
* PAYLOAD\_INFO\_ENCODING
* SM\_SERVICE\_TYPE
* SM\_NUM\_OF\_ATTEMPTS
* SM\_MAPPED\_NETWORK\_ERROR
* ORIG\_APPL\_ID
* MSG\_REJECT\_REASON
* MSG\_ERROR\_CODE
* MSG\_PAYLOAD
* PREPAID/POSTPAID
* CHARGED\_PARTY
* CELL\_ID

## SMSC Solution – Provisioning

The system shall provide, accept and process manual, automatic, single, and bulk provisioning requests. These requests include for instance, activation/deactivation of subscriptions, add/remove/update subscriber profiles...

The Vendor shall describe the provisioning method on the system (Available tools, APIs, interfaces, protocols, data replication, and authorization levels for users…).

The system should have an API to manage customer profiles and customer black/white lists.

The provisioning interface shall at a minimum provide the commands for querying, creating, deleting and updating records.

The system shall send a response for each provisioning request processed. The response shall include an explicit return code indicating the status of the request.

The system shall generate a record in the provisioning log file for each provisioning request which is executed.

The system shall save and archive provisioning records in log files for any necessary O&M purposes. These records for provisioning requests shall be retained for a configurable amount of time.

In case of Master/Slave database configuration, provisioning requests done on one DB shall be automatically propagated to the other DB.

## SMSC Solution – NGBSS/IN/OCS Interface

The system shall communicate with MIC2’s NGBSS/IN/OCS platform to perform various operations like credit checking, amount deduction, amount reservation, refund…

Integration with the NGBSS/IN/OCS is done through the diameter protocol.

The solution should be able to provide subscription based and online charging. It should be also able to support multiple billing factors (originator, destination, SCCP address, connection…). The required AVPs for diameter are included.

To support prepaid SMS roaming, the SMSC shall send the MSC address to the SCP/NGBSS/IN/OCS via real time diameter charging protocol based on which the real time charging system can identify the roaming status and implement different tariff.

The SMSC shall send the destination VLR address of the recipient in the diameter request when charging MT messages.

The SMSC shall record the MO MSC address in the charging CDRs based on which the offline charging system can identify whether the subscriber is roaming.

The SMSC should be able to block the usage of short codes when the customer is roaming. Some short codes could be defined as exceptions and allowed while roaming.

The operator should be able to determine if all messages are charged on the SCP/NGBSS/IN/OCS or if only messages sent while the subscriber is roaming are sent to the real time charging system.

# System Operation and Management

## Operations Management

1. **Application Management**

The solution shall have a graphical user interface (GUI) and command line interface (CLI) that the operator can use for management, configuration, administration, maintenance and monitoring purposes.

The solution shall have a centralized Operation and Maintenance interface used to configure all geographically redundant systems. The operator should be able to apply the changes to individual nodes separately or to all the nodes at once.

Configurations and changes should be dynamically read by the system without the need of process restarts.

The Vendor should provide access to all databases to manage them.

The solution shall have a user friendly management interface to monitor connections, queues, load… It should also allow configuring the system and stopping and starting applications.

1. **Operation and Maintenance**

The Vendor should provide all necessary tools for the operation and maintenance of the system. The proposed equipment should provide a local maintenance terminal in addition to the possibility of performing operation and maintenance activities remotely. The system shall support out of band management.

1. **Logging**

The interface should support certain tools for logging end-to-end user activity and to provide session tracing.

The solution shall provide a configurable mechanism for maintaining log files.

The operation log storage time and size should be configurable by the operator. The system should keep the operations logs for at least 6 months and should provide a log rollover mechanism to avoid the accidental filling up of any storage space.

Logging and debug levels shall be easily adjusted by the administrator without the need for application restart.

It should be possible to easily trace messages sent through the system.

1. **Back Up and Restore**

The system should have a dedicated backup solution for data and platform including software installed, configuration files, databases, CDRs, logs, events, alarms, statistics…

Backup and restore operations should not affect the performance and availability.

The backup and restore procedures shall cause no service interruption and shall minimize impact to customers.

## Performance Management

The vendor shall provide a complete monitoring and business intelligence (BI) solution. The monitoring solution shall include alarms generation, fault detection and handling, configuration and performance management, system administration, and security modules.

1. **Network and System Performance**

Network monitoring and diagnostic tools shall be available for detecting various types of fault scenarios at topology, node and connection levels. Monitoring shall cover traffic levels within the PLMN, verification of the network configuration, resource availability, resource access and Quality of Service (QoS). Operator must be able to view and analyze performance, fault and configuration data in the form of meaningful information that is visualized in graphical and textual reports.

The solution should include tools to monitor KPIs and the message success rate. Exception reports should be generated when needed.

The solution should generate detailed reports on the network performance and the number of returned error from each type. For example, the system shall keep track of the number of network failure errors, absent subscriber errors, memory capacity errors…

1. **Load Details**

This shows information about the system and traffic like CPU usage, memory, module status, links load, traffic management, number of messages/sec handled, etc.

1. **Concurrent Request Management**

The Solution shall provide a load management mechanism to preserve quality and to protect from overload and congestion.

1. **Statistics**

The solution should include a Business Intelligence module to monitor the system and customer behavior.

The system shall generate MO and MT error code statistics report.

Statistics shall be generated in real time customizable charts. They shall also be accessible via command line interface.

The operator should be able to have access to different real time statistics over any time frame- in the form of tables and charts - including active time utilization, data traffic, number of active users and concurrent requests, number of messages sent, reported errors...

The solution shall be able to collect statistics per interface, such as utilization, availability, response time, and error rate.

History of performance measurements should be logged and saved for a configurable period of time.

The system should generate customizable reports in a user friendly format (CSV, fixed length text…).

The statistics should include at least the following:

* + - Successful MO submissions
    - Failed MO submission due to error XX
    - MO submissions by roamers
    - Messages sent by application
    - Total delivery attempts
    - Successful delivery attempts
    - Successful delivery attempts with no retries
    - Successful delivery attempts with retries
    - Failed delivery attempts
    - Failed deliveries caused by XX error
    - Number of retries
    - Round trip time
    - Number of delivery reports delivery attempts
    - SS7 load per link
    - SCCP errors
    - TCAP open dialogues

For the Antispam and filtering module, the statistics should include at least the following:

* + - Messages matching filtering rule X
    - Messages blocked by filtering rule X
    - Messages blocked grouped by blocking reason
    - Messages blocked by originating Sender
    - Messages blocked by originating GT
    - Messages blocked by content list
    - Messages successfully delivered
    - Messages not successfully delivered
    - Total incoming messages
    - Total blocked messages
    - Total successful and failed messages

## System Failure and Alarm Management

It is very important for the system not to be vulnerable to errors, and to be able to detect these errors and locate them once occurred. Under this topic, we mention:

1. Components Failure

The system shall be monitoring the functioning of its individual hardware and software components and keeping logs of any failing events in a structured and informing way in the form of pre-defined and/or user-defined alarms.

* Hardware: Component level
* Software: Module, links, database record level…

The operator shall have the option of restarting individual modules through the user interface without the need of stopping the whole system.

1. Fault Handling

The system shall be able to identify faults occurring at any level in its architecture and shall implement rules and methods (ex. Redundancy) for appropriate fault detection, prevention and correction.

It shall also be ensured that detected failures are isolated to the lowest level in order not to block the whole system or affect any service.

The system shall perform a detailed analysis of received alarms information and be able to identify and diagnose the faults that affected the system in order to facilitate troubleshooting and thereby reducing the impact of the faults on the daily system operation and prevent future threats.

1. Fault Reports and Alarms

The system shall provide organized informative fault reports, alarms and statistics.  
Generated alarms shall provide information to analyze and resolve the fault and enable measurements based on historical information.

Alarm information processing shall support information filtering, alarm confirmation, alarm clearance, alarm notification, alarm synchronization, alarm redefinition.

Alarms based on the statistical counters shall be configurable using the user-defined counter thresholds. Alarms statistics results should be displayed in the form of tables, charts and graphs with printing/emailing options. The classification of statistics shall be sorted according to type, module, importance, etc… and registered in reports (period, times, etc…)

Pre-defined alarms as well as the user-defined alarms shall be configurable or even removable by the system administrators.

Alarms shall be generated for any of the below occurrences:

* Communication failure, process failure, connectivity loss, hardware failure, loss of a system node, Quality of Service (QoS) failure, system or service overload
* Links going down
* System Congestion and out of service
* Any network entity to which the SMSC Solution is connected to becomes unavailable
* Slowed down system performance; for instance, when the time of a request processing or the response generation time goes beyond a given threshold

Operating system alarming shall include at least CPU/disk/network utilization, memory/disk utilization, network link state, RAID and database processes.

Every alarm shall at least be categorized as minor, major or critical according to its severity. It should also include the date/time, alarm status (Active, Acknowledged …) and an informative alarm description.

A detailed alarm description reference shall be available to check the meaning of alarms and the actions that need to be performed.

Alarm filters shall be configurable to suppress particular alarms.

Alarms shall be logged and saved for a configurable period of time. Operator shall be able to browse for current and history of alarms.

The solution shall also send faults/alarms reports to external management systems like the INMS via standard protocols like SNMP or CORBA. It shall also provide alarm statistics and queries according to parameters like time, states, levels, types. In addition, solution shall support screening the repetitive and intermittent alarms.

The SMSC Solution shall generate SNMP and SMTP alarms when needed.

1. Power Failure Recovery

System shall ensure that the system recovers gracefully from power failures, meaning that all hardware and software shall return to service as before the power failure.

## Security Management

The solution shall provide below security measurements to ensure safe access:

1. User Management and Access Control:

The operator should be able to create, delete, modify and query users and user groups and to assign roles and privileges (e.g. administrator, read only...). Providing role-based access and domain-based access should be available through the combination of users/user groups, equipment sets/object sets and operation sets.

The system provides access privileges to different level of users such administrators, operators, customer care, NOC or marketing users that can only access service statistics and reports.

The solution shall provide the capability to authenticate and authorize users (user name/password) based on their privileges.

The solution shall provide the capability to create, collect and store users’ access logs for audit trails. The information collected for the access logs shall include start/stop date and time, operations performed, user/system identification, system usage.

The solution shall support forced logout as well as manual or automatic locking of the terminal

The system should be protected against unauthorized users and unauthorized access.

Each system administrator should have a unique dedicated user able to perform all the needed administrative tasks.

Root access should be restricted on the system. A unique identifier should be provided on the operating system level to each administrator of the system.

1. Logs and Alarms

The solution shall log any activity performed on the system by any user profile.  
An alarm shall be raised in case of any security breach.

1. Encryption

Remote access shall be provided via encrypted communication protocols after MIC2’s approval. All activities performed shall be logged and monitored by MIC2.

Messages stored on the system should be encrypted to prevent un-authorized access to message content. Only system administrators with specific privileges can decrypt the messages to view the content.

The system should ensure data availability, integrity, confidentiality and privacy.

Secure protocols should be used on all system interfaces and communication.

1. System security

Regular security audits and penetration tests should be performed to make sure the system is not vulnerable to external or internal attacks.

The latest releases and patches should be maintained on the operating system, the database and the applications to prevent any security breach.

# Interoperability

The vendor shall be responsible for the interoperability and full integration of the solution in MIC2’s operational network and provide the needed interfaces and connectivity. This includes (but not limited to):

* MSS
* HLR/HSS
* IMS network
* VAS platforms
* Billing system
* Provisioning system (TABS, PPAS, Web)
* USSD gateway
* Online Charging System (OCS)
* Prepaid System (IN)
* Revenue Assurance and Fraud Management platform (RAFM)
* Others

The vendor shall provide integration description documents supporting the above interoperability requirements.

# Professional Services

The required delivery, implementation and integration periods are 4 weeks and 12 weeks, respectively.

The vendor shall provide a detailed integration plan with the existing operational network

The vendor shall be responsible to deliver the following services:

## Delivery

The vendor is responsible for the delivery of equipment based on DDP (Delivery Duty Paid) incoterms including VAT, insurance, transportation, and insurance during transportation and all related taxes and charges.

## Installation

The vendor shall conduct a site survey and provide MIC2 with proposed layout drawings for MIC2’s approval prior to installation. The vendor shall allow MIC2’s team to participate in his activities.

## Implementation

The implementation of the equipment is the responsibility of the vendor. Pre-implementation design documents for the solution to be provided and reviewed jointly with MIC2.

Power consumption including peak and normal operations shall be provided with the design in addition to environmental limitations including humidity, temperature and heat generation.

## Acceptance Testing

The vendor shall provide acceptance tests for the proposed solution including testing of individual elements as well as the end to end system solution, in accordance with the provisions of the Contract of Adherence. These tests have to be reviewed and approved by MIC2. MIC2 can add any test to be performed during the acceptance test phase. Tests shall include all features and functionalities requested in this document as well as 2 testing handsets, an iOS and an Android devices.

## Quality of Service

The vendor shall ensure zero impact on the network performance during and after the integration and implementation of the proposed solution. All activities impacting the quality of service of the existing network shall be subject to MIC2’s approval before proceeding with the work.

## Project Management

The benefits of professional project management to the timely and successful completion of the project are paramount. In recognition of those benefits the vendor shall establish a project organization dedicated to this project. The vendor shall provide details of its project management organization and shall specifically identify a project manager who should be the focal point for all project activities. Also, the vendor should define the project management methodology approach that will be followed during the project execution.

## Operational Review Meetings

Operational review meetings between the Vendor and MIC2 will be held on a weekly basis or as may be otherwise agreed. During the operational meetings the installation activity schedules shall be discussed as well as other operational and support issues.

## Project Progress Reports

Formal written progress reports are required, the format and content of these reports have to be proposed by the Vendor and agreed upon with MIC2 team. The reports shall include the following in conformance with the attached Contract of Adherence:

* Contract status (including any amendments to the Contract).
* Equipment delivery status.
* Installation status, including activities, problems, acceptance, pending issues, dependencies, etc.
* Technical status, covering areas of technical significance only (interfacing, integration, etc).
* Content availability and content management progress report.
* Project risks if any.

## Training

The Vendor shall propose the appropriate training program to develop the following resources:

* System Administration Engineers
* Operation and Maintenance Engineers
* Applications Engineers
* Non-specialist and non-technical including Marketing,

The proposed training courses can be a mixture of in-country and abroad trainings depending on the complexity of the offered courses. System administration training shall be provided in a proper lab environment with hands on experience. A minimum of five (5) trainees per course are required.

The Vendor shall be responsible for all travel related costs including tickets and hotel for trainings given abroad.

The Vendor shall describe the training center organization and give the names and qualifications of the trainers.

## Documentation

The following documents shall be provided by the platform solution providers:

* Technical solution description
* System manuals
* Installation manuals
* Maintenance and Repair manuals
* Features descriptions
* Alarm descriptions
* Training manuals
* Backup and restore documents
* IOT; Interoperability testing with existing operational entities.
* Complete acceptance and commissioning test documents
* Inventory sheets

Other relevant documents pertaining to the vendor’s proposed solution

# Maintenance and Support Services

The support and maintenance activities shall be performed locally on site by the vendor.

Remote monitored access is only provided in exceptional cases upon special approval by MIC2.

The following shall be included in the Maintenance and Support Service (MSS) plan:

1. Fault management
2. Preventative maintenance.
3. Service Levels (SL) to be approved by MIC2. Service Levels shall include without limitation:

* Gold level support during /after warranty for the SMSC Solution (Hardware and Software)
* Restoration time for Severity 1 – Critical problems: 2 hours
* Restoration time for Severity 2 – Major problems: 8 hours
* Restoration time for Severity 3 – Minor problems: 24 hours
* Restoration time for Severity 4 – Non Service impact: 48 hours

etc.

1. Repair and return time for HW issues should be specified
2. The offer shall include, without limitations. the following key 24x7 services during and after the implementation, all in accordance with the provisions of the Contract of Adherence:

* Customer Service Desk
* Grade of Service
* Escalation Procedures
* Resolution Time
* Response Time
* Spare parts management & replenishment
* Technical Assistance Centers
* Service Levels
* Remote Support upon request
* Onsite and infield attendance & Support

The vendor shall be responsible to ensure the continuous availability of spare parts for each HW type to prevent any impact on the service due to a shortage of any HW type.

The vendor shall submit a complete roadmap for offered HW and SW solutions covering EOM, EOS & EOL milestones.

The vendor shall be responsible to deploy efficient processes, reporting procedures and plans for the operation, maintenance and support activities and reporting.

# References & Relevant Experience

The bidder shall provide the Company HQ and R&D center locations.

The bidder shall provide details about the company shareholders and group of sister companies as well as the Investors in the company.

The bidder shall provide valid references with similar deployments and number of subscribers in the form of a certificate with the company stamp. (*This is to be provided from the mobile operator signed and certified by the officials of the company whereby name, role, contact details are clearly provided. The references shall be considered valid provided the mobile operators mentioned are in operation for the period mentioned above. References shall also mention performance of the software and hardware products. In addition to the network elements supplied and installed.*)

The bidder shall indicate the years of experience in the messaging and VAS platforms.

The bidder shall mention in table format, reference (Europe, MENA, US) for the deployment of the SMSC solution.

The bidder shall indicate live deployments for important features requested.

The bidder shall present his roadmap for future features and services.

The bidder shall specify the locations of the manufacturing, support, and research and development centers of each product and service offered in the Solution, supported by references.

The bidder shall provide detailed information of the company’s ownership, financials, structure, organization and market position specifically for VAS products.

# Sufficiency of the Tender

The vendor shall complete all required information before the submission of his offer. The Vendor shall check that the prices quoted in the BoQ (pricing schedule) and the unit prices are adequate to cover all obligations under the contract plus other aspects and items necessary for the proper and sound implementation and operation and maintenance of the offered solution. If the Vendor confronts during the implementation of the works any material difficulty or any abnormal obstacles, which an experienced vendor is not likely to expect rationally, he shall immediately, within a maximum of ten days, notify MIC2 of such difficulty or obstacle in writing. If the Vendor fails to notify MIC2 within the said ten days and claims compensation, his right in such compensation shall lapse.

--------------- End of document --------------.