**INTERNATIONAL A2P SMS AGREEMENT**

Made by and between the undersigned:

**\*\*\*\*\***, a company incorporated at the Register of Commerce in \*\*\*\* under № \*\*\*\*, whose registered office is located \*\*\*\*\*\*\* (hereinafter referred to as the “First Party” or “\*\*\*\*\*\*\*\*\*\*“).

**AND**

**Mobile Interim Company № 2 S.A.L.**, a company incorporated at the Register of Commerce in Beirut - Lebanon under № 1000382, whose principal place of business is at Touch Building (Beirut Central Building – Bloc B), Fouad Chehab Avenue, Beirut, Lebanon (hereinafter referred to as the “Second Party” or “MIC2”)

Both herein after referred individually to as “Party” or collectively as “Parties”.

**PREAMBLE**

Whereas, MIC2 operates the second mobile network for the account and for the benefit of the Republic of Lebanon;

Whereas, MIC2 had launched a request for bidding (RFB) for the provision of International A2P SMS services;

Whereas, the First Party has been selected to be the service provider and subsequently was awarded the agreement for the provision of International A2P SMS services;

IT IS NOW AGREED BETWEEN BOTH PARTIES ON THE FOLLOWING:

**1.** The above Preamble, as well as all Annexes attached hereto constitute an integral part of this Agreement.

**2. SCOPE**

2.1. Subject to the terms and conditions of this Agreement, on an exclusive basis, the Parties shall provide each other the services (Hereinafter referred to as "Services") defined and described in Annex 1 - Services.

2.2. From time to time the Parties may mutually agree in writing to add or remove Services to or from this Agreement by means of an Addendum to be signed and attached to this Agreement.

**3. PRICE, PAYMENT AND TAXES**

3.1. The Services shall be provided at the pricing as determined in Annex 1 - (Services) attached hereto.

Prices are exclusive of all taxes. Each Party shall settle taxes and levies as dictated by the Lebanese laws, rules and regulations.

3.2. MIC2 shall issue one yearly invoice for the yearly minimum committed volume of successfully delivered SMS, Such invoice shall be issued once the SMS Filter Solution has been installed on the MIC2’s Network, the Network is fully secured and prevents any possible international A2P leakage, and all A2P traffic is exclusively routed to the First Party’s SMS Solution & Filter, which is mandatory to start the performance of the Agreement by First Party and needs to be fulfilled within three months from the date of signature of the Agreement.

3.3. In case the First Party exceeds the volume of minimum commitment, MIC2 will issue a new invoice for the excess amount of successfully delivered SMS due ((excess volume \* SMS rate) + VAT (if applicable)) at the end of the 6 months period and invoice shall be due within 30 days from issuance.

In case the First Party fails to comply with the abovementioned yearly minimum commitment and the yearly revenue increase, First Party has acknowledged the right of MIC2 to an indemnity for missed profit, the amount of which shall not exceed 5 Million Euro, without prejudice to other legal remedies available to MIC2.

3.4. The settlement of the annual invoice shall be done in Euro currency exclusively, through two equal prepayments whereby the First Party shall pay in advance the amount due for the first six (6) months upon signature of the agreement, and in advance at the beginning of the second six (6) months.

3.5. All invoices under this Agreement shall be issued and settled exclusively in Euro currency. Settlement shall be made through direct bank wire transfer strictly from a bank account outside of Lebanon to MIC2’s bank account number or from a local Lebanese bank (to be specified by both parties within a letter to be notified to each other upon the signature of the two parties on the A2P Agreement).

The transfer or the conversion of funds from any currency into EURO shall be carried by the First Party free of any charge whatsoever to MIC2, that is without imposing any financial burden such as expenses, transfer fees, or others on MIC2.

3.6. **BILLING DISPUTES AND NON-SETTLEMENT OF DUES**

3.6.1. The First Party’s billable traffic (successfully delivered A2P SMSs) will be based on MIC2’s generated CDRs. If any dispute concerning the accuracy of billing data recorded by either party’s network. The First Party shall notify MIC2 in writing. Said notice shall set forth in writing all details concerning the disputed traffic.

3.6.2. Parties shall co-operate to investigate promptly any dispute concerning the accuracy of any billing data recorded by either Party’s network, or any other amount payable under this Agreement. The disputing Party shall notify the other of any such dispute in writing.

3.6.3. In the event where the Parties are unable to reach agreement within two (2) weeks from the receipt of the abovementioned notice, then the dispute shall be submitted before the competent courts of law in Beirut and settled under the Lebanese laws, rules and regulations.

3.6.4. **Performance Bond:**

First Party shall submit an “on first demand” international irrevocable bank guarantee for the amount of € /1,000,000/ (One Million Euros), in a form and content to be pre-approved by MIC2 prior to signature of the contract, and valid for one year from its date of issuance with a possibility for renewal one or several times as MIC2 may request. The issuing bank must be an international recognized bank whose last two years credit rating was at least “A” (or equivalent) for long term and “A1/A2” (or equivalent) for short term, unless otherwise pre-agreed by MIC2. The payment of the guarantee shall be made directly into the bank account that MIC2 will indicate.

3.6.5. In the event of failure to settle MIC2’s dues as per the payment terms agreed upon, that is within (30) days from relating Invoice issuing date, MIC2 shall be entitled to execute the bank guaranty submitted without prejudice to other legal remedies.

3.7. **UNSOLICITED TRAFFIC**

3.7.1. First Party undertakes that it shall not use any Services for any illegal, immoral or improper purpose, or in any manner which contravenes applicable laws and codes, regulatory requirements of the appropriate jurisdiction or Mobile Operator requirements as they exist and as they change over time, and will do its best effort not to allow any third party to do so.

For the same purpose, First Party shall fully abide by the terms of the Deontology Code signed and attached hereto to form an integral part of this Agreement

3.7.2. Both Parties shall co-operate to prevent, detect and/or eliminate fraudulent use of the Messaging Interworking Services.

3.7.3. If the First Party operates on more than one Lebanese network, the First Party undertakes not allow inter-operator A2P SMS bypass.

3.7.4. The First Party shall be liable for damages in the event of intent and gross negligence on its part, or the part of its statutory representatives or employees, or in the event of a breach of contractual obligations owing to neglect.

3.7.5. The First Party shall be required only to handle the international A2P SMS traffic terminated into MIC2’s network, and no other services related to SMS.

3.7.6. The First Party shall be required to provide periodic statistical reports including but not limited to performance, geographical segmentation etc. and provide online access to MIC2’s technical and commercial teams for such reports.

3.7.7. The A2P platform shall be installed on-site. Remote access is not allowed on the platform. Only in rare cases and upon approval of MIC2, remote access can be provided via encrypted communication protocols where all activities performed shall be logged and monitored by MIC2. First party must abide by the terms of all the A2P solution requirements stipulated in the Annexes attached hereto.

In the event where the First Party fails to abide by the terms stipulated above, MIC2 shall retain the right to take all measures against the First Party, including the application of the provisions of below Clause 5.3.

3.7.8. The First Party shall provide free of charge premium support services for the entire solution including Hardware and Software elements.

3.7.9. The First Party 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.

3.7.10. The First Party shall not have any access to sensitive content like CDRs and message content information.

**4. CONFIDENTIALITY**

4.1. For the purpose of this Agreement, the Parties undertake that they will keep confidential and will not use for their own purposes any information of a confidential nature, either directly or indirectly (“Confidential information”).

4.2. Notwithstanding the above, the Parties agree that information shall not be deemed Confidential Information and the Recipient shall have no obligation to hold in confidence such information, where such information:

(a) Is already known to the Recipient, having been disclosed to the Recipient by a third party without such third party having an obligation of confidentiality to the Disclosing Party; or

(b) Is or becomes publicly known through no wrongful act of the Recipient, its employees, officers, directors, or agents; or

(c) Is independently developed by the Recipient without reference to any Confidential Information disclosed hereunder; or

(d) Is approved for release (and only to the extent so approved) by the Disclosing Party; or

(e) Is disclosed pursuant to the lawful requirement of a court or governmental agency or where required by operation of law.

4.3. MIC2 may disclose Confidential Information to the Lebanese Ministry of Telecommunications.

4.4. The terms of this Clause shall survive expiry or earlier termination of this Agreement.

**5. TERM AND TERMINATION**

5.1. This Agreement shall be effective from the date of its signature by the Parties thereto, and shall remain valid for an initial period of three (3) years (the Initial Term) thereafter.

5.2. The Initial Term shall be automatically extended by the number of days/months taken to fulfill the requirements stipulated in above Clause 3.2, noting that the period of three months stipulated in that clause may not be exceeded.

5.3. MIC2 may terminate this Agreement by a 30 (thirty) days written notice to the other party if the other Party breaches any of its obligations under this Agreement and fails to cure such breach within thirty (30) days of receiving written notice of such breach, requiring its cure;

For the purposes of this sub-clause (5.3), failure of First Party to settle its dues to MIC2 does constitute a breach of this Agreement, without prejudice to MIC2’s right to take any further legal action against First Party to preserve and recover its rights, such as the execution of the bank guarantee provided for in above Clause (3.6.4).

5.4. **Termination for Convenience**

MIC2 may terminate this Agreement by providing First Party with a written notice thirty (30) days before the date of effective termination. In such a case, MIC2 shall refund the First Party of the remaining amount of the prepayment of the yearly minimum commitment following the subtraction of MIC2’s revenues, as per the prices set in Annex 1 attached hereto, up to the date of Termination and shall release the Bank Guaranty;

The revenues in question shall be calculated based on the higher of the pro-rata of the minimum commitment or the actual revenues.

First Party acknowledges and accepts that no termination for convenience from its part is possible during any contractual year under pain of executing the bank guaranty by MIC2 without prejudice to other legal remedies available to MIC2.

**6. ASSIGNMENT**

The First Party shall not assign this Agreement, totally or partially, or any right or obligation hereunder.

However, MIC2 shall have the right to assign, transfer or purport all of its rights and obligations under this Agreement to the Republic of Lebanon or any of its designees, having given the First Party prior written notice of such assignment but without having to obtain their consent prior to such assignment.

**7. FORCE MAJEURE**

7.1. The Parties shall not be liable for any delay or failure of performance caused by a force majeure as defined by the Lebanese laws, rules and regulations, nor shall any delay or failure of performance due to the said force majeure effect be deemed a breach or a default in the performance of this Agreement.

However, the time within which a Party is required to perform any act under this Agreement shall be extended where the delay in the performance of the act is due to any of the events of the said force majeure. In this regard, the Party entitled to the extension of time under any of the provisions of this Agreement shall:

. Notify the other Party promptly of the occurrence of the event resulting in the delay;

. Use its best endeavors to abate the delay, as far as possible; and

. Perform the act delayed immediately after the abatement of the unavoidable delay unless the other Party shall have instructed it not to perform same.

7.2. If the event constituting the force majeure continues for a period of sixty (60) days, then either Party shall be entitled to terminate this Agreement by giving two (2) weeks’ notice in writing to the other Party.

**8. NOTICES**

Any and all notices permitted or required to be given hereunder shall be sent to the address first set forth above and deemed duly given upon actual delivery.

**9. GOVERNING LAW**

9.1. This Agreement, and all matters arising out of or relating to this Agreement, shall be governed by and interpreted in accordance with the laws of Lebanon.

9.2. In the event there is a dispute between the Parties arising out of or otherwise relating to this Agreement, the Parties agree to try in good faith to resolve such dispute. Any and all such disputes that cannot be so resolved by the Parties, within thirty (30) days from the beginning of the good faith trial mentioned herein, shall be submitted to the competent courts in Beirut and settled under the Lebanese laws, rules and regulations.

**10. GENERAL PROVISIONS**

10.1. The failure of either Party to enforce, at any time or for any period of time, the provisions hereof, or the failure of either Party to exercise any option herein, shall not be construed as a waiver of such provision or option and shall in no way affect that Party’s right to enforce such provisions or exercise such option. Any modification or amendment to this Agreement shall be effective only if in writing and signed by both Parties.

10.2. In the event any provision of this Agreement is determined to be invalid or unenforceable, the remainder of this Agreement (and each of the remaining terms and conditions contained herein) shall remain in full force and effect.

10.3. Each Party shall be responsible for its share of taxes and other fiscal duties as may be prescribed by the laws in force.

**11. ATTACHMENTS**

Annex 1 – Services

Annex 2 – Technical Requirements

Annex 3 – The entire RFB documents

All 3 annexes constitute an integral part of this Agreement.

**12. Signature**

This Agreement has been signed in Beirut on …………………………, in (2) two originals, one being retained by each Party hereto.

|  |  |
| --- | --- |
| **FIRST PARTY** | **Mobile Interim Company No. 2 S.A.L.** |
|  | **Chairman General Manager**  **Salem Itani** |
|  | Signature: |
|  | **Chief Financial Officer**  **Nibal Matta Salameh** |
|  | Signature: |

**Annex 1**

**SERVICES**

MIC2 shall provide the First Party with Messaging Interworking Services allowing the latter to terminate international SMS traffic into MIC2’s network.

The First Party shall not use the said Messaging Interworking Services to terminate any traffic which does not adhere to the definition of A2P SMS (which shall mean an SMS where the sender is alphanumeric or a short number), or which is not permitted by applicable laws, or which damages or is likely to cause damage to the network of either Party, or which is spam.

Both Parties shall co-operate to prevent, detect and/or eliminate fraudulent use of the Messaging Interworking Services.

Per SMS-message fees:

MIC2 charges all SMS messages upon successful delivery to its subscribers.

Per SMS-message fees amount as follows:

. EURO /\*/, VAT exclusive, in the first contractual year.

. EURO /\*/, VAT exclusive, in the second contractual year.

. EURO /\*/, VAT exclusive, in the third contractual year.

Said fees may be subject to change from time to time if so requested by the Lebanese Ministry of Telecommunications.

First Party has committed to a Minimum Volume of SMS amounting (\*) million SMS throughout the first contractual year.

For the second contractual year the minimum volume will be (\*) million SMS, and for the third year,

(\*) million SMS.

**Annex 2**

**TECHNICAL REQUIREMENTS**

A2P SOLUTION REQUIREMENTS

The solution ought to offer MIC2 insight to the incoming International A2P SMS traffic into the network. To guarantee that A2P traffic does not enter the network via unauthorized pathways, it is essential to have monitoring, filtering, and control over international A2P SMS traffic.

All international A2P traffic should enter the network through authorized A2P SMS hub gateways to ensure secure and regulated message delivery, compliance with legal operational standards, and to prevent fraud/spam.

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

The Vendor shall not have any access to sensitive content like CDRs and message content information.

The solution should identify and provide protection against the bypass of two Factor Authentication Calls.

The solution shall provide data analytical engine to identify the Flash call numbers being used.

The Flash call solution should provide the option of either blocking the calls directly, or reporting the calls so MIC2 can take the necessary decision.

The Flash call solution should provide additional layer of security measures related to SS7 and signaling monitoring.

Bidder must provide all details related to the architecture of implementation of the Flash Call solution.

Bidder must provide all technical details about the features that will be provided under the Flash call.

The bidder should provide full details of the voice firewall that will be used (including and not limited to deployment details, integration and Call Flow)

The bidder should describe how the voice firewall filtering will be managed and the data that is needed to allow/block

The solution SMS should block bypass SMS traffic.

The solution should detect SIM farming/SIM box fraud traffic.

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.

The A2P solution should detect broad range of fraudulent activities, such as and not limited to faking, flooding, content filtering, malicious content and spoofing using several techniques to detect spam.

The solution is required to protect the network and mitigate fraud by following the GSMA standards AA.50 (SMS Fraud Criteria), IR.71 (SMS SS7 Fraud Prevention), FS.12 (A2P SMS Bypass) and IR.82, while also ensuring compliance with ISO 27k.

The filtering rules shall be dynamically and proactively updated.

The detection of spam and flood situations should happen in real time and the proper action should be automatically taken to stop the spam situation.

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
* 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 alerts should be configured and sent to the appropriate team(s) in order to take action. Depends on the cause of the alert. (VAS/NOC/Fraud Management/Security)

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, by rule matched...

The solution shall include a top-quality SMS firewall that protects against SMS spam, abuse, threats, and has been deployed at Tier 1 operators

The SMS firewall should keep message logs and actions taken to control/prevent/filter

The solution shall provide data analytical engine to identify the destinations and origins of bypass traffic.

The A2P solution should detect wide range of fraudulent activities

The SMS firewall should keep message logs and actions taken to control/prevent/filter

The solution shall provide analysis of A2P traffic by content-type/ origin

The solution shall provide data analytics based on AI analytics and machine learning to analyze the traffic in order to have network visibility and detect bypass destinations

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.

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

The solution should be able to detect unusual patterns and prevent (Denial of Service) DoS attack

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.
* 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.
* 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.
* 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.

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 provide a user-friendly business intelligence (BI) portal for generating reports, data and dashboard. The platform should be able to generate a mixture of standard and bespoke reports/dashboards/data generation upon requirement.

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 interface should support certain tools for logging end-to-end user activity and to provide session tracing. It should be possible to easily trace messages sent through the system.

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.

1. **Dimensioning, Capacity and Architecture**

The bidder shall provide all the needed hardware for the solution.

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.

The provided system should be geographically redundant

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.

All servers and devices should have redundant power supplies.

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.

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

The solution provided should allow a throughput of at least 1000 SMS/sec.

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

The Vendor shall provide all the hardware requirements and accessories (network and power cables, connectors, E1 cards, device for backup, HBA cards, Fiber cables…) to install, integrate, connect, and launch the Solution.

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

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

* CAT6 cabling is required.
* Patch panels should be used for cabling
* All needed patch cords should be provided and labeled on both ends
* Each cabinet should have the needed number of cable organizers
* All Network devices should be available as part of the solution

1. **Billing and Integration Requirements**

The vendor shall be fully responsible of the interoperability and integration of the A2P solution with MIC2 network elements

The platform should generate detailed CDRs. CDRs 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 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.

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

The Vendor is responsible for the integration of the A2P Solution with MIC2’s INMS. The Vendor shall provide feasibility study and all the prerequisites to insure this integration. The interface should include the below functionalities:

* + Alarms generation and handling
  + Fault Management,
  + Performance Management and Statistics
  + Configuration and system administration
  + SNMP support

The bidder shall be fully responsible of the interoperability and integration of the A2P solution with MIC2 Fraud Management platform. The bidder shall provide feasibility study and all the prerequisites to insure this integration. The system should communicate with MIC2’s Fraud Management platform to perform various operations like SMS bypass, Voice bypass, grey routes etc…

1. **Security Management**

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.

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.

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

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.

1. **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:

**8.1 Delivery**

The project including HW delivery, solution implementation, integration, Trainings and testing should be completed in a period not exceeding 3 months.

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.

**8.2 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.

**8.3 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.

The local presence of the vendor is required during all installation and implementation activities.

**8.4 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 to be used for testing & ongoing support (One IOS & one Android) and a laptop for the International A2P operational & platform support

The local presence of the vendor is required for the completion of the acceptance tests.

**8.5 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.

**8.6 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.

**8.7** **Operational Review Meetings**

Operational review meetings between the bidder 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.

**8.8**  **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.

**8.9 Training**

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

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

The bidder should provide different levels of training to ensure the system is used efficiency and effectively.

The advanced certified training should be delivered at bidder expense in an appropriate laboratory setting and include the costs of accommodation and travel. A minimum of four (4) trainees per course are required.

The bidder to specify the training location, duration and courses provided.

The bidder should ensure that MIC2 technical representatives to be present in the workshops to discuss new trends and solutions.

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

**8.8 Documentation**

The platform solution providers shall provide the following documents:

* 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

1. **Maintenance and Support Services**

The vendor should provide free of charge premium support services for the entire solution including Hardware and Software elements.

The bidder must provide escalation chart, hotline in case of trouble incidents.

The bidder should provide an on-site engineer for the initial first year of the operational support.

Remote monitored access to the platform 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:

* Premium level support during /after warranty for the A2P 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.

1. **References & Relevant Experience**

The vendor shall provide valid references with live deployments of similar solutions

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

The vendor shall indicate the years of experience in the A2P monetization solutions

The vendor shall present his roadmap for future features and services

The vendor 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 vendor shall provide detailed information of the company’s ownership, financials, structure, organization and market position.

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 mention in table format, reference (Europe, MENA, US) for the deployment of the International A2P solution.

1. **Questions & Relevant Experience**

The bidder shall attempt to answer the following questions in the Statement of Compliance with any additional relevant information and explanation:

1. Is the bidder part of the A2P ROCCO Report?

* If yes, please elaborate and share the report and your positioning.
* If not, please elaborate and share other reports/standards and your positioning.

1. Is the bidder an A2P aggregator?

* If yes, please proceed with the next question.
* If not, please state the A2P aggregator that you are cooperating with.

1. Is the bidder an SMS firewall owner?

* If yes, please provide the brand name and references of your sms firewall
* If not, please state the brand name and references of the SMS Firewall to be used

1. Has the specified SMS firewall been deployed?

* If yes, please provide the details and number of deployments
* If not, please elaborate.