Statement of Work (SoW) for SMS Gateway

Version 1.7 | 12 November2024

CONFIDENTIAL

Md. Mahfuzul Islam
System Operations

Contents

1.Introduction

This Statement of Work (SoW) details the solution approach for implementing an SMS Gateway solution for Nagad and integration with the Nagad DFS system. The SMS Gateway will enable reliable messaging services tailored for diverse business purposes, such as promotional, transactional, and alert notifications. The solution will include both API and GUI-based interfaces to support MIS management, bulk message distribution, and DFS integration. It will prioritize high availability, scalability, security, and full regulatory compliance with applicable data protection regulations.

2.Objectives

The primary objectives of the SMS Gateway implementation are:

- To provide a **reliable** and **scalable** SMS Gateway solution.
- To support various messaging **types** and **protocols** for SMS delivery.
- To support sending **SMS push** notifications and **push-pull** services for interactive communication.
- To manage **dynamic priority** queues for optimized message delivery.
- To ensure **secure** and **compliant** handling of sensitive data.
- **Seamless integration** with **existing** business systems and third-party services.
- To provide comprehensive **reporting**, **logging**, and **monitoring** capabilities.
- To enable **template-based** SMS broadcast and support **dynamic SMS** for standardized communication.
- To facilitate **SMS campaign** management for any kind of promotional activity.
- To implement **event-based** and **event action-based** SMS notifications.

3.Scope of Work

Provide a PUSH-based SMS delivery service in a 365x24x7 mode, ensuring priority handling of messages. The new SMSGW should replace the existing system while maintaining compatibility with the current DFS-to-SMSGW and SMSGW-to-all-MNO message flows. This includes support for current APIs, processing single/multiple arrays of JSON requests, prioritizing SMS queues, and prefix-based MNO selection if the MNO name is missing

3.1. SMS Delivery Capabilities

The SMS Gateway is designed to support a range of message delivery needs, offering flexibility and precision for both real-time and bulk messaging scenarios. The system ensures secure, scalable, and efficient delivery across multiple channels, with options for customization and scheduling.

1. **API Support for Various Protocols:** Support SMS delivery via HTTPS, HTTP, JSON, and SMPP APIs.
2. **Blacklist/Whitelist/DND Management:** Include options to manage blacklisted, whitelisted, and DND (Do Not Disturb) numbers.
3. **Unicode SMS Option:** Allow Unicode SMS delivery.
4. **Session/Channel Segregation:** Support session/channel segregation based on SMS type.
5. **Push & OTP Message Delivery**: Provides seamless transmission of real-time notifications and secure OTP (One-Time Password) messages via a robust API interface that supports integration with various applications, enabling secure and timely user interactions.
6. **Bulk SMS Distribution**:

    a. **Personalized Bulk Messaging**: Supports the sending of customized SMS messages to multiple recipients simultaneously through file upload (XLS, CSV) or JSON (many-to-many), regardless of mobile network operator (MNO).
    b. **Predefined Bulk Messaging**: Allows for the distribution of predetermined SMS messages to individual recipients through file uploads or JSON requests (one-to-many), offering efficient, large-scale outreach.

7. **Scheduled SMS**: Enables users to schedule SMS delivery for future dates, ensuring campaigns and notifications reach audiences at optimal times, enhancing communication effectiveness.
8. **Retry Mechanism for Failed SMS:** Include a configurable retry mechanism for undelivered SMS.
9. **Configurable Masking/Short Code by SMS Type:** Enable masking/short code configuration based on SMS/user type.
10. **MNP Checking Capabilities:** The SMS Gateway should have the MNP checking capabilities (may be required at a later stage)

3.2. Push-Pull SMS Service

Users can send a text message to the SMS Gateway, which will process the request and respond with the appropriate template message based on the content.

1. **Automated Information Retrieval**: The SMS Gateway will automatically collect and process data from incoming messages, sending personalized, template-based responses to users.

2. **Dynamic Response System**: Depending on the content of the user's request, the SMS Gateway will deliver relevant and predefined template messages, streamlining user interactions.

3.3. SMS Channel Management

NAGAD needs to develop a SMS gateway platform, where Nagad DFS system, SMS bulk push panel, campaign manager application, push-pull service can use & broadcast SMS to end users to all MNO with upgraded features to match the current industry practice.

1. SMSGW can connect multiple delivery channels for single MNO.
    - E.g.: As for Banglalink, it will connect both HTTP/HTTPS API and SMPP, for GP it will connect two different HTTP/HTTPS/JSON API.
2. A configurable GUI interface will manage all the MNO SMS delivery channel based on DFS transactions channel and segregate TPS for different types of priority SMS.
    - E.g.: As an example for Banglalink,
        - USSD user: Transaction SMS will route to HTTP API channel
        - APP user: Transaction SMS will route to SMPP channel.
3. In case any MNO's SMSC channel is down, the SMS Gateway will automatically reroute the SMS through the respective MNO's alternative SMS delivery channel. Similarly, if a transaction is initiated through the mobile app but the associated Bulk SMS channel is inactive, the SMS will be redirected to the defined alternate channel (Third-Parties)Bulk SMS Platform.

The SMS Gateway solution will include a heartbeat mechanism to continuously monitor channel availability. If a primary channel is down, the system will automatically switch to the secondary channel to ensure uninterrupted service. This automatic routing logic is specified in the following table for clarity.

3.4. Store-and-Dispatch Capability for Priority SMS

SMSGW must have the capability that it will store some priority type SMS at the application that comes from DFS and later those SMS will be dispatched when the user triggers

- SMS GW receives Priority type: 50
- SMS GW will store all related information for dispatch (e.g. the priority type, SMS body etc.)
- Later based on user trigger, SMS will dispatch accordingly

3.5. Queue Mechanism for priority base SMS

1. The SMS gateway solution needs to maintain an SMS delivery priority queue.
2. The DFS system will transmit the priority level through the API.
3. Upon receiving the details, the SMS gateway application will validate the MNO and delivery channel combination based on the specified priority.
4. Following this validation, the SMS will be routed through the appropriate gateway, utilizing the required API or SMPP account with the designated TPS allocation.

Priority Selection Table (Example)

Name	Value	Priority
OTP	0	Highest
Transactions	1	High
Bulk Disbursement	2	Medium

Marketing/Campaign	3	Low

3.6. Prefix based MNO selection in API request

The first three digits(prefix) can be added to the system and destination MNO can be configured from BE (backend) system configuration.

3.7. SMS Identification Requirements

To ensure accurate tracking and management, the SMS Gateway will implement unique identification protocols for each message:

1. **Unique SMS Identification**: Assign a distinct identification code to each SMS, enabling precise tracking and traceability for individual messages.
2. **Application-Wise Identification**: Attribute each SMS to its originating application through a unique sub-application ID, ensuring clear visibility of message flow from the DFS to the MNO.

3.8. Web GUI Interface

GUI is to provide seamless experience for admin as well as users to perform relevant operations basis their assigned role. The GUI must have these following features as well as other configurable modules which discussed above.

1. **Web Portal with Role Management**: Vendor to provide a web portal with user role management to control configuration activities and access MIS reports.
   a. Admin, Super Admin, and User roles will have specific functionalities based on their assigned roles.
   b. **Maker-Checker Mechanism for Configurations:** Implement a maker-checker mechanism for portal-based operations and configuration management.
2. **Real-Time Message Status**: Vendor to provide real-time updates on the status of all messages through the web interface/MIS portal.
3. **Failure Notifications for Undelivered SMS**: Vendor provides failure notifications for undelivered SMS, including detailed error descriptions, via the web interface.
4. **SMS Submission Check Status**:
   a. The web GUI should have the SMS **submission to MNO** check capability feature for individual numbers.
   b. The web GUI should have the option of SMS delivery status check from **MNO end to handset** for individual numbers.

3.9. Reporting Module

The vendor will deliver a robust SMS reporting module, offering detailed and summary views of SMS activity. Reports will be customizable based on criteria like Mobile Network Operator (MNO), user, and channel, and can be generated for specific time periods, including monthly and weekly summaries.

1. **MIS Reporting:**
   a. **Detailed and summary reports** on SMS activity, filtered by criteria such as Mobile Network Operator (MNO), user, channel, and time-period.

b. **Example:** reports include MNO-wise, user-wise, channel-wise, as well as monthly and weekly summaries.

3.10. Compliance and Security

1. **Data Protection:** Encrypt sensitive data (e.g., OTPs) in transit and at rest, and apply data masking in logs.
2. **Access Control** (also Mentioned in GUI Module)**:** Implement role-based access control (RBAC), multi-factor authentication (MFA), and IP whitelisting for the management portal.
3. **Logging and Auditing:** Enable comprehensive logging for SMS processing and maintain detailed audit trails for configuration changes and activities.
4. **API Security:** Enforce 0Auth 2.0 or API key authentication, secure all API calls with HTTPS/TLS, IP Whitelisting, and validate payloads to prevent injection attacks.
5. **Data Management:** Require database encryption, data purging, and DND compliance. Ensure system redundancy and load balancing to maintain synchronization.
6. **Application Compatibility:** Ensure the application supports the latest OS versions, patches, and whitelisted third-party tools required by Nagad.
7. **Vulnerability Management:** Vendor must resolve vulnerabilities identified by Nagad's security screenings as needed.
8. **High Availability (HA):** Support high availability in the application architecture, with zero downtime for updates or system upgrades.
9. **Detailed Activity Logs:** Record user and system activity, maintaining standard and detailed audit logs for all events, jobs, and changes.
10. **System Integration:** Ensure seamless integration of the SMS gateway with Nagad's existing systems, such as databases and user authentication systems.
11. **API Documentation:** Provide comprehensive API documentation, including examples and troubleshooting guidance.
12. **Data Retention:** Define retention periods for SMS logs and user data, with purging processes in compliance with Bangladesh Bank regulations.

3.11. Technical Support and Logging

1. **24/7 Technical Support:** Provide continuous technical support, including a dedicated technical SPOC (Single Point of Contact) available around the clock according to signed SLA.
2. **On-Demand SMS Logs:** Maintain detailed logs of all SMS requests, recording individual receipt status with timestamps for sending and delivery, applicable to both API-based and bulk-uploaded requests.
3. **System Monitoring and Performance Tracking:** Implement robust logging and monitoring capabilities to track system performance, message delivery, and all integration points.
4. **Troubleshooting and Audit Logging:** Enable comprehensive logging for effective troubleshooting and to maintain complete audit trails.

3.12. Comprehensive Testing Infrastructure

- **Comprehensive Testing Infrastructure:** Provide a complete test environment to enable end-to-end testing of all integrations.

- Provide a sandbox environment for testing purposes.

3.13. Redundancy & Load Balancing

1. **Dynamic Message Routing:** Enable dynamic message routing based on load balancing, network availability, and cost optimization.
2. **Load Balancing and Redundancy:** Ensure load balancing and redundancy at both the application and database layers.
3. **System Scalability:** System should have the ability to adjust new resources like increasing new servers. There will be no application level limitation and CAP in the SMS Gateway.

3.14. Backup and Recovery

1. Implement a robust backup and recovery plan to ensure data integrity.
2. Provide a comprehensive disaster recovery plan.

3.15 Maintenance & Monitoring

The vendor shall provide monitoring tools and alert notifications for L1 teams to effectively oversee application features and infrastructure components. Key monitoring capabilities include:

1. **Web Server Monitoring**: Track API response status and alert if APIs are not responding with standard HTTP codes.
2. **Application-Level Monitoring**: Monitor for issues like database connection failures, cache reading errors, or other application-level disruptions.
3. **VM Monitoring**: Monitor system resource utilization, including CPU, memory, disk space, swap memory, load average, IOPS, and disk space usage.
4. **MNO Failure Monitoring**: Detect any SMPP/HTTP account failures or message rejections by MNO accounts.
5. **MNO & Delivery Channel Monitoring**: Track requests submitted per MNO and delivery channel, detailing submissions per route.
6. **Submission Success Rate**: Monitor successful message submissions per MNO and delivery channel.
7. **Failure Monitoring**: Track failed submissions per MNO and delivery channel, with insights on top failure reasons.
8. **Queue Monitoring**: Ensure smooth processing of message queues.
9. **Archiving/Purging Mechanism:** Implement archiving and purging mechanisms for database management.

3.16 Control Process & Reporting

1. PIN/OTP/PASSWORD, and Transaction amount should be masked in the SMS while data is in transit or at rest.
2. All SMS sending requests received should be logged with the Source System and Module/API from DFS, along with a Unique Request Identifier. For transactional SMS, the Transaction ID needs to be maintained separately in a database column. For event SMS, the Unique Reference ID needs to be maintained separately in a database column.
3. There should be a fraud management component in the SMS GW Solution. There should be a counter at the SMSGW end to prevent fraudulent activities, either by SMS template, type, individual user, account number, or MSISDN.

4. If any SMS is to be sent using the bulk feature, it should contain a dynamic approval workflow.
5. It's covered with the maker-checker feature.
6. If any OTP SMS delivery is delayed, an auto-purge mechanism should be available to prevent sending the SMS after it has expired. These trends need to be shown on analytical dashboards.
7. All channels and SMS delivery channels should maintain different queues and priorities.
8. Any SMS sent to a non-DFS user needs to be flagged in the system as a non-Nagad user, and these trends need to be shown on analytical dashboards.
9. Production databases need to contain all the said information; however, they also need to generate data feeds for external systems in near real-time, i.e., every 5 minutes or 10MB file, etc.

4.Deliverables

1. Fully implemented and tested SMS Gateway maintain standard security protocols and compliance.
2. **Health Check Report:** Vendor will provide health check analysis report monthly for application and database related components.
3. **DFD/ER Diagram Provision:** Provide Data Flow Diagrams (DFD) and Entity-Relationship (ER) diagrams for the solution.
4. Regular status reports and a final project report on demand.
5. **Training & Documentation:** Conduct hands-on training and provide operational documents to enable NAGAD's maintenance of SMSGW day-to-day operations.

5.Conclusion

The vendor is expected to deliver a robust and comprehensive SMS Gateway solution that meets all the above requirements, ensuring seamless operation and integration with existing systems. The solution should be scalable, secure, and compliant with all relevant regulations and best practices.