Terms of Reference
For
Development of e-Government Architecture and Frameworks

1. Introduction

The United Nations e-Government Survey 2016 emphasizes three things - a Whole-of-Government approach, Policy integration and use of Big Data Analytics – as the important means of achieving the Sustainable Development Goals (SDGs). The purpose of adopting the Whole-of-Government Approach is to provide integrated and joined up services that cut across not only the economic, social and environmental dimensions but also between various sectors, sub-sectors and activities. Policy integration entails recognition of the inter-linkages between different areas of policy and adopting a holistic approach. Big data Analytics is a tool for gaining deep insights into a range of complex issues and using the same for policy formulation and decision-support. All these three globally significant trends invariably require breaking of sectoral barriers and silos and re-architecting the Government as a single enterprise.

Government of Bangladesh has comprehensive "Digital Bangladesh" agenda which have become popular concept among citizen of Bangladesh. It has also identified the important role of ICT for its Seventh Five Year plan for improving governance and empowering citizens. Numerous initiatives and projects have been undertaken to support the ambitious ICT targets and also already implemented a significant e-government component under the leadership of a2i.

Traditional system development approach for e-governance solution will create chaotic situation when different vendor usage different choices of technology, platform, framework and it becomes difficult to maintain interoperability among the system. Along with these there are various capacity and resource issues like poor management of systems, challenges in integration, interoperability, data and information sharing between internal and external systems.

Considering these issues it is necessary to take more strategic, holistic and integrated Whole of Government (WoG) approach for G2C, G2B and G2G services. Hence it is necessary to develop e-government architecture and framework which will comprise principles, reference models, standards and guidelines.

2. Business Case & Business Realization

- Government has already been developed few enterprise level e-government solutions and have some others upcoming solutions and platform to be developed. At the same time government has tried to develop enterprise architecture for establishing whole of government approach as well as has tried to develop some sector wise frameworks.
- For the development of enterprise level e-government architecture, frameworks and solutions, it is very much need to develop principles, standards and guidelines.
- There is a need to involve third party specialized firm for development, documentation, maintenance for such kind of standards and guideline for specific architecture, framework and solution.
- Procurement of such service is a time consuming job and it really hampers the continuity of the existing solutions/platform and make delay the development of new solutions and platform.
- If there is a pool of pre-qualified vendors exists then it will reduce the time tremendously to engage third party specialized firm for a particular solution/ service.

3. Scope of works

- Collaborate, conceptualize, plan and design to establish and maintain national e-service architecture and framework which will enables the government to efficiently apply ICT to achieve its near-term and long term digital Bangladesh goals.
- Implementing the vision and strategies of the government to establish conceptual architecture that will ensure the smooth transition of technology changes of existing e-services.
- Develop enterprise principles, standards, frameworks and best practices by working along with a2i architecture team in acceptable vetting and enacting process.
- Develop various reference models (ie. Business reference model, performance reference model, Integration reference model, Security reference model, Architecture governance reference model, Technology reference model, Data reference model, Application reference model etc.) for both nation and individual sector (ie. land, business, agriculture, industry, judiciary, education, health etc.) as per need by working along with a2i technology team in acceptable vetting and enacting process.

- Must perform feasibility analysis, up to and including the most complex and advanced on current and potential future e-service projects from internal and external service providers.
- Coordinate and provide guidance to architecture professional from across the government and industry sectors to achieve highly complex e-service system architecture objectives.
- Work effectively with e-service provider at various ministries/agencies as well as with the industries. Clarify processes to technical/non-technical users and industry/academy stakeholders as required.
- Work with data owners to fix data issues.
- Provide continuous improvement of relevant new thinking and technology solutions

3.1 E-Service Bus

E-Service Bus is actually a custom-built middleware that acts as a conduit between the Information Consumer Applications and the Information Provider Applications, across the Whole-of-Government. E-Service Bus has 3 basic components – the Information Exchange, which is a standards-based gateway, the Access Control List, which validates the rights of the consumer and the provider in relation to exchanging the data in each proposed exchange and the Information Directory, which is a standards-based registry of all datasets that are registered by their owners for positioning in the exchange pool along with the metadata of each dataset.

- The E-Service Bus must support HTTP, HTTPS, Web Socket, POP, IMAP, SMTP and other standard Transport Protocol.
- Must be able to integrate with Payments Gateway, CRM, ERP and any other legacy system as required.
- Must provide message formats and protocol like JSON, XML and SOAP
- Must have to capabilities to connect with other Enterprise Messaging System, like, MSMQ, Oracle AQ or IBM WebSphere MQ.
- Should be able to connect with any data store like RDBMS, CSV, Excel, ODS, Cassandra, Google Spreadsheets, etc.
- Should be able to route, mediate and transform data and the routing support can be header based, content based, rule based and priority based.

- Should provide support for all Enterprise Integration Patterns (EIP), Database Integration, Event Publishing, Logging, Auditing and Validation.
- Must support AMQP and MQTT protocol with support for all QoS levels and retained messaging
- Must support RDBMS for scalable backend message
- Must support distributed message queues
- Must manage authentication, authorization and entitlement with ESB
- Must be able to handle 1000s of concurrent non-blocking HTTP(s) connections per server
- Must provide on-demand processing of messages
- Must be able to provide horizontal scaling via clustering with stateless server architecture
- Must ensure long-term execution stability with low resource utilization
- Must ensure load balancing for scalability and failover for high availability of service endpoints
- Must have tracing and debugging of message mediation
- Must have easy configuration of fault tolerant mediations with support for error handling
- Must provide UI or Scripting based configuration features
- Must provide comprehensive management and monitoring with a web console with enterprise level security
- Must have tracing capabilities for message mediation flows and identification of bottlenecks
- Must have operational audit, KPI and SLA monitoring and management options.

3.2 API and Service Management

For system to system communication it will be necessary to provide combined easy and managed API access with full API governance and analysis:

- System should have the ability to publish APIs/Services to a selected set of gateways in a multi-gateway environment
- System should support enforcement of government and system policies for actions like API/Service subscriptions, application creation, etc., via customizable workflows
- Manage API/Service visibility and restrict access to specific agencies or systems

- Manage API/Service lifecycle
- Ensure API/Service security by restricting API access tokens to domain/IPs, validating APIs payload contents against a schema, applying security policies to APIs authentication and authorization and provide threat protection, bot detection and token-fraud detection
- System should generate JSON web tokens for consumption by back-end servers
- System should provide developer portal to search APIs by provider, to provision the API keys, subscribe API, notification for new version of subscribed APIs and view of the API consumer analytics.
- System should have proper capabilities to manage and scale API traffic and enforces rate limiting and dynamic throttling based on usage quotas and bandwidth quotas.
- System should be horizontally scalable with easy deployment into cluster using proven routing infrastructure
- System should have high performance pass-through message routing with minimal latency
- System should provide a pluggable analytics framework for API usage, like, requests, responses, faults, throttling, subscriptions etc.
- System should track consumer analytics per API, per API version, per tiers and per consumers
- System should have configuration payment schemes to monetize API usage
- System should monitor SLA compliance for the API
- System should have provision to do the proper/required integration with SSO System

3.3 SSO and Access Management

Single sign-on is a specialized form of e-authentication that enables a user to authenticate once and gain access to the resources of multiple applications. With this property, a user logs in once and gains access to all systems without being prompted to log in again at each of them.

- Determine the business requirements
    - Identify the services to be provided online
    - Assess the risk associated with each online service
    - Define the sensitivity level for each online service
    - Identify the appropriate authentication mechanism

- Select the approach to incorporate SSO at the application level and review the e-Authentication solution.
- Must provide Single Sign-On (SSO) by using SAML2 or OpenID
- Must have SAML 2.0 or above based Single Logout, metadata profile and assertion query/request profile
- Must have OpenID connect based session management, discover and dynamic client registration
- Must provide Federated SSO via SAML2 or OpenID with external identity providers
- Must provide white label login and registration process
- Must provide Rule-based authorization support for SSO
- Must support for multi-option/multi-step authentication
    - X.509 Authentication
    - 2-factor authentication (2-FA)
    - Time-based one-time password (TOTP) based authentication
- Must provide Users and Group Management
- Must provide flexible profile management for users supporting multiple profiles per user and have the ability to link multiple user accounts to a single user
- Must support heterogeneous user stores, e.g. ApacheDS or any RDBMS
- System should support configurable password policies
- Should have account locking for invalid failed login attempts
- Should have account recovery with email and secret questions
- Should have password history validation
- Should have password pattern configuration
- Should have account locking in single and multi-tenant environments
- Should have account suspension reminders and locking of idle accounts
- System should provide multi-option/multi-step approval template based workflows for user and role management operations
- System should manage role-based access control
- Should have user friendly policy administration point
- Should have easy to integrate option with Service Bus
- Should support for SAML2 bearer grant type, JWT assertion grant type and NTLM-IWA grant type
- Should have OAuth2 token revocation support

- Should have OAuth token introspection
- Should have proper monitoring, reporting and auditing support by providing login events and session monitoring, user session termination, forced password reset and real-time security alerting for suspicious login activities and abnormal sessions based on rules

System should provide flexible deployment mechanism by supporting clustering for high availability deployment and centralized configuration management across different development environment

3.4 System Integration

- Must provide system integration service with the various e-service streams within the government sector to insure that the solution is properly architected end to end to deliver a successful implementation.
- Must ensure the service delivery based on requirement from cross-functional e-service team of various government agencies with development of integrated business processes, implementing project deliverables, with an emphasis on quality, productivity and consistency.
- Provide technical direction and control of internal and external team and provide a framework for project planning, communications, reporting and contractual activity.
- Provide required coordination between internal and external agencies for service delivery;

3.5 Change Management

- Ensure the accesses, approval, implementation and review of changes in controlled manner.
- Must facilitate and take responsibility for the overall change management process.
- Ensure that all the activities designed to implement the change as per the standards. The policies and procedures should be well defined, recognized and reviewed.
- Provide Monthly Change Summary Sheet that summarizes all CRs to understand and evaluate the changes and its future implications.
- Vendor must form a change advisory board with the inclusion of members from Client for changes that are categorized as major or significant.

- Must take necessary initiative to maintain liaise with the change requestor for business and technical queries - if any;
- Changes must be maintained and controlled through a change management system - a tool utilized for tracking and documenting all the activities (initialization, approval, update and close) related to the proposed change.

3.6 Maintenance and Support

- Must ensure the efficient and effective incident management process by providing a qualified incident management team;
- Must generate management information including KPIs and reports
- Developing and maintaining the incident management system
- Providing, developing, managing and maintaining the major incident process and associated procedures
- Submit monthly reviewing and auditing report of the incidents
- Must provide first line service desk with single point of contact for users where there is a service disruption and for some categories of request for change by following ITIL or any other widely accepted standard.
- Must provide second line service desk for incident diagnosis and resolution which cannot be achieved at the first line service desk by following ITIL or any other widely accepted standard.
- Must provide third line service desk with the inclusion of internal technical group and/or third party supplier/maintainers for network support, voice support, server support, application management, Database support etc. by following ITIL or any other widely accepted standard.
- Ensure regular backup, security and user help systems.
- Provide updated test script with pseudo-data covering all cases in test domain.

3. 7 Capacity Management and Knowledge Transfer

- The vendor shall develop a transition plan to identify the steps required to transit in to e-services by each existing product and ensure the availability of requirement and required modification;
- Develop the standard operation procedures and management of platform;

- Develop comprehensive risk matrix before launching new service in order to determine the impact;
- Identify/Assess and map required skills against available skills, develop a plan to enhance internal skills to address potential gaps and consider external skills as an option for addressing gaps;
- Train and prepare pool of SI for e-service integration. These will be a workforce of 100 master SIs trained locally or from abroad on e-Service integration and following TOGAF/WSO2 or any other well established open source e service framework;

4. Technology Specification

4.1 Technology Space

The vendor will follow the TOGAF or any other industry accepted and widely used open source based technologies, frameworks, platforms and guidelines.

- TOGAF compatible or similar open source platform to ensure enterprise level management
- Common data platform
- EService bus with 1000 multi-service request per second
- Go or Python or any other language at back-end or server side scripting layer
- API centric enterprise level design using JSON or other data delivery format.
- Micro service architecture following micro-service design approach.
- Secure interaction with Core-service and shared service using dynamic token
- API lifecycle, policy and community governance using proper analytics
- Multi-tenancy support in platform
- LDAP like OpenLDAP for user management
- Apache Maven, Apache Ant and Oracle JDK
- Enterprise Linux to host all application
- Seamless Mobile and Internet of Thing Integration
- Bootstrap, jQuery and Ajax for best UX
- MySQL or any other open source RDBMS
- MongoDB or any other Nosql database as/when required with proper justification
- Memcache, CDN or Varnish for caching and faster data delivery
- Code Version Controlling using GIT or Bitbucket in private mode
- GIT issue board or Jira or Asana for issue tracking and feature change management

- Technology and all related design/data should be open to a2i
- Notification to web and mobile with current and future OS of corresponding devices must be ensured
- Future technology change, iterative prototyping and agility in framework design are the generic expectation

4.2 Security

- The vendor should follow any of the industry standard secure development methodology such as (but not limited to) Comprehensive Lightweight Application Security Process (CLASP) by OWASP etc.
- The vendor should consider (but not limited to) common vulnerabilities such as SQL Injection, Cross Site Scripting (XSS) etc.
- Vendor will undertake responsibility for Input Validation Controls, Authorization/Authentication Control and other security controls in place in both test and production environment of application.
- The following vulnerabilities must be checked and ensured security from the beginning:
    - Cross Site Request Forgery (CRSF)
    - Cross Site Scripting (XSS)
    - Session hi-jacking
    - Session Fixation
    - SQL Injection and Code Injection
    - Input Validation/Filtering
    - Output Escaping
    - Secure File Access

5. Eligibility Criteria

The Bidder must prove that they have solid technical background and operational strength to undertake and take this work forward without any hindrances. Bidder must also have adequate technical ability, resources, human resources and processes. As such, following are defined as minimum eligibility criteria:

1. Must have Valid and up-to-date VAT, TIN, Trade license and Register of joint stock & companies (RJSC) registration.
2. Minimum 5 years of general experience in ICT business.
3. Must have 03 (three) practical experience of developing web-based enterprise solution within last 05 years.
4. Must have experience to develop fully componentized middleware platform.

5. Must have vast experience to deploy scalable system in clustered environment using Apache Ant, Maven and any LDAP system.
6. Must have capacity development experience in government and industry sector
7. Must have ITIL or similar process driven expertise
8. Must have experience to conduct ToT in e-service integration domain
9. Must have knowledge on OSGi specification.
10. Must have experience to provide platform services.
11. Firm needs to be submit last 02(two) years' financial audit reports.
12. Must have minimum amount of liquid asset in form of credit line or working capital shall be BDT 40 Lac and annual turnover shall be Tk. 100 lac.
13. Vendor needs to have at least two existing running software solution in Bangladesh in either Government or in other corporate Sector in Document management or File Management or Data Management.
14. Need to have competent full time manpower/consultants in the team that includes Project Manager, System Analyst, Business Analyst, Solution Architect, Mobile Apps Developer (iOS and Android), Web System Development Expert, Security Expert, Database Expert, UX Expert, Infrastructure Expert, Data visualization Expert, Technical Writer and dedicated Support Engineers having individual experience in relevant ICT area. Vendor will have to submit signed CV of each experts working with the company mentioning their positions.
15. Needs to have Test Environment ready with equipped devices at vendor's premise.
16. Multiple Companies having technical and legal competency for developing such Product can bid jointly but they must have legal agreement among them where one company needs to be master. Master company needs to fulfill all conditions mentioned in this ToR. Joint-venture agreement needs to have clear identification about each responsibility matrix along with IPR.