Terms of Reference
for
Development of Essential Components and Maintaining the Platform of Online Payment Service.
ICTA/GOSL/CON/QBS/2016/151

1. **Introduction;**

   In present globalized world, many economies have brought up digital commerce to facilitate governments, businesses and citizens to be able to perform digital commerce and financial transactions with efficiency, ease and low cost.

   ICTA as the apex government organization of ICT development across all sectors of the country is responsible of aligning entire country with the national policy of 'Digitization of Economy. Therefore, ICTA implements several initiatives to provide efficient and effective services to the citizens and businesses. Improvements and developments of digital infrastructure is one of the key initiative implemented towards achieving the above objective.

   ICTA will be driving revolutionary technologies such as High Speed Fiber Networks, Government Cloud, Data Centers, Common Payment Platforms, Education Portals and Social Media initiatives etc. across Sri Lanka which will transform the nation towards information Society. Infrastructure facilities are required to facilitate the on-gong initiatives until the common infrastructure facilities are implemented.

2. **Background;**

   In the rapidly evolving technological society to remain competitive, an organization must have to have comprehensive methods to reach individual target segments and provide its services to citizens in a more convenient and reliable manner. With the increasing use of internet and mobile devices, common online service and payment platform has been recognized as a key service baseline.

   ICTA in collaboration with the ministry of finance, has taken the initiative of bringing up digital commerce with ease in Sri Lanka by introducing “The Online Payment Service”. In order to streamline registration, login and financial transaction processes for citizens and corporates via Digital Instruction Providers (DIPs), it intends to develop a responsive Single Sign On (SSO) Web and Mobile based applications with administrative reporting features to facilitate online payment service in a secure scalable environment.

3. **Objective**

ICTA intends to engage a consultancy firm to design, develop and implement essential component applications and provide 6 months support and maintenance for the platform and developed essential applications upon launch.

4. **Scope of Work:**

(a) Implementation approach;

4.1 ICTA has identified number of essential component applications to be offered to online payment service. Therefore, ICTA intends to design, develop and implement proposed essential component applications. The essential component applications (Web Application and Mobile Application) scope includes;

4.1.1 An interface to the online payment service users. (Web/Mobile)
4.1.2 Web/Mobile application including the web service. Web/Mobile applications will be accessible to citizens.
4.1.3 Backend operational application (if required)
4.1.4 Development of relevant APIs to integrate with online payment service in order to expose the transaction services via Digital Instruction Providers (If required)

4.2 Web and mobile application should be integrated /configured with 3rd party tools for reporting, Single Sign On and login anomalies upon selection. (Consultant supposed to evaluate the available products/tools in the industry and propose the most suitable product based on the basic criteria given. (Refer Annex 1- Section 1,2,5)

4.3 Consultant should subscribe selected 3rd party tools on behalf of ICTA and reimburse the subscription fee monthly/annually through ICTA by providing invoices.

.

4.4 Consultant is expected to deploy multiple teams to work in parallel.

(a) Scope of Work;

4.5 Review and understand the overall architecture and design of the online payment service initiative.

4.6 Review and understand the High level functional requirements of Web application development (Refer: Annex 1- Section 3) and Mobile application development (Refer:

Annex 1- Section 4) identified for this assignment to determine the overall functional scope of the proposed essential component applications.

4.7 Review and understand the non-functional requirements of the online payment service initiative. (Refer: Annex 2- Non Functional Requirements).

4.8 Evaluate, select configure and implement suitable 3rd party tools for reporting, Single Sign On and login anomalies. (Refer Annex 1- Section 1,2,5)

4.9 On completing the above, submit a proposal comprising of the following, among others;

4.9.1 Web and Mobile Application implementing schedule
4.9.2 User acceptance criteria
4.9.3 Evaluation reports for selection of 3rd party tools for reporting, Single Sign On and login anomalies.

4.10 The above proposal should include all deliverables as specified in below item '5 – deliverables and time lines'
4.11 Consultant should provide support and maintenance for 6 months to the developed essential component applications and to the online payment service platform after the launch. (Refer Annex 3- Service Level Agreement for Support and Maintenance Services)
4.12 Selected consultant should be able to facilitate change requests (CRs) during the S & M period with the maximum ceiling days of 100 persons days. (If required)
4.13 Implement Web/Mobile Application, upon obtaining ICTA approval for the above.
4.14 Implement and integrate required APIs with online payment service which will be required to integrate with essential component applications.
4.15 Maintain project source code in the ICTA Source Code Management system (SCM).
4.16 Adopt a proper application release procedure to release the Web/mobile Application to ICTA for deployment in the staging / production environments.
4.17 Participate for Project Review Committee meeting and Project Implementation Committee (PIC) meetings as a member.
4.18 Obtain User Acceptance (UAT) for the implemented Web/Mobile Application.
4.19 Deploy into production in a Cloud Computing Platform.
4.20 Work collaboratively with ICTA throughout the tenure of the project duration.
4.21 Attending any configuration changes related to certain parameters proposed for the Web/Mobile Application.
4.22 All staff of the provider who are engaging with the assignment are required to sign a Non-Disclosure Agreement (NDA) where applicable.
4.23 Adhere to ICTA project management practices.
4.24 Support and transfer technical knowledge to ICTA IT during the period of transition.
4.25 Refer following Annexes which form a part and parcel of the Terms of Reference.

Annex 1 - High Level Functional Requirements
Annex 2 - Non Functional Requirements
Annex 3 – Service Level Agreement for Support and Maintenance Services

5. **Deliverables and time line;**

The Consultancy firm will be engaged for a period of **8 months,** in which 2 months for the designing, developing, implementing and 6 months for providing support and maintenance.

Consultancy firm is required to submit the following list of deliverables for the essential component application development and support & maintenance project for online payment service.

No	Deliverables	Phase	Duration
5.1	Successfully acceptance of following; 5.1.1 Web/Mobile Application Implementation Proposal 5.1.2 Analyze and provide System Requirement Specification. 5.1.3 DSTD (Design System Technical Documentation) 5.1.4 QATP including Acceptance criteria 5.1.5 Test Cassese 5.1.6 Evaluation reports of proposed 3rd party tools.	Inception	Commencement + 3 Weeks
5.2	Successfully acceptance of following; 5.2.1 UAT 5.2.2 Deployment Guide 5.2.3 Help Desk template for the Web/Mobile Application (Knowledge Tree and T1 Document) 5.2.4 User Manual	Construction	Commencement + 8 Weeks
5.3	Successfully acceptance of following; 5.3.1 Monthly support and maintenance Report 5.3.2 Final S&M report should consist with comprehensive knowledge transfer documentation.	Transition	Date of launch +6 Months

6. **Services and Facilities Provided by ICTA**

6.1 Documentation

- High Level Requirement/Process Document
- High Level Architecture
- Deployment Architecture
- Design Specification - API Architecture Document
- Design Specification - Data Flow Document
- Design Specification - Middleware Document

- Design Specification - Integration Document
- Design Specification - Security Standards

6.2 SLA for support and maintenance services.
6.3 Web-based access to the ICTA SCM (Software Configuration Management) system
6.4 Access to staging/ production servers.
6.5 Access to Issue Tracking System.

7. Review Committees and Review Procedures

All deliverables will be reviewed by the team appointed by ICTA.

- END –

[Annex 1] – High Level Functional Requirement

Each individual who intends to get 'Online Payment Service' services have to Sign in/Login using one of the Digital Instruction Providers (DIPs) interfaces. Since it seems to be tedious task ICTA intends to streamline this registration and login processes while developing a Web/Mobile Application with a common user interface to support Single Sign On (SSO) for Online Payment Service via Digital Instruction Providers (DIPs).

The following components should be presented in the online payment platform.

1. Single Sign On
    a. The platform should consist single sign on as a feature to access multiple applications using a single ID.
    b. A proper product should be selected and integrated into the platform to achieve the above.
    c. The product selected should be able to authenticate and authorize apps running on cloud.
    d. The product should support API-based, scalable, social-login, multifactor authentication, analytics and should operate on standard protocols.

2. Login Anomalies
    a. The platform should be able to track user activities and detect suspicious logins in real time.
    b. A proper product should be selected and integrated into the platform to achieve the above.
    c. The product should support API driven mechanism to detect anomalies where details are provided through SSO.

3. Web Application
    a. A Responsive web application should be developed where it's viewable on any computing device.
    b. The web application should utilize the above Single Sign On and Login Anomalies products to implementation where citizens are able to maintain their user profiles.
    c. This application will allow citizen's to setup their bank account for payment and list all the payments along with the other relevant information.
    d. The sensitive citizen details such as keys should be stored in a secure manner such as in a Keystore.
    e. The application will consist related features such as settings, user profile management and basic reporting.

4. Mobile
    a. The mobile application should be developed using a hybrid mobile application development platform.

b. The mobile application should consist features such as single-sign-on, user profile registration, setting up bank account, notification, transaction activity list and other related features.

5. Reporting Platform
    a. All the activities on the platform should be sent to a reporting platform in order to be analyzed in order to make decisions.
    b. The reporting platform should be implemented based on the existing big data related products.
    c. The reporting platform should support real time analytics and historical analytics as well.

6. Middleware Infrastructure
    a. The middleware infrastructure will be in place integrating stakeholders and above mentioned systems to communicate with each other without making point-to-point integrations between each party.
    b. The middleware infrastructure will be responsible for mediation, orchestration, transportation, transformation and implementing non-functional requirements.
    c. An existing platform has been implemented using a pioneer open source enterprise service bus. There may be a possibility of improving/expanding the existing platform.

[Annex 2]

Non-Functional Requirements

1. Security

1.1. User authentication and authorization

Web/mobile applications should be able to access DIPs and through public domain. Any authorization requirement should be implemented within the web/mobile application.

However, the solutions should have the provision to integrate with the online payment service middleware.

An administrative application need to be developed wherever applicable.

1.2. Confidentiality and Integrity

Developed Web/mobile application/ back end should ensure "confidentiality" and "integrity" whenever required by adhering to transport and message level security standards.

1.3. Availability

Web/Mobile application/ back end should be developed to ensure "High Availability" to remain the system available all the time. (e.g. Web applications clustering capability should be taken into consideration in the development)

1.4. Non-repudiation

Web/mobile application / back end should ensure non-repudiation.

2. Audit Facilities

Wherever applicable, an audit trail of all activities must be maintained. On a service or operation being initiated, the system should log the event, creating a basic 'audit log entry'. It should not be possible for the operation to be executed without the log entry being made.

The information recorded in the audit trail depends on the type of activity which takes place. Each service would be responsible for logging detailed information. The different types of operations are -

- Data Capture & Maintenance
- Creation of an entry / item
- Modification an item
- Deletion
- Control (or status change)

- Process execution
- Data synchronization
- Print (only selected item)
- Retrieval
- Monitor

Detail logging may be enabled or disabled for each type of operation, and/or for each business object. It should be possible to configure which attributes of a data item should be traced at the detail level. Tracing of some attributes may be considered mandatory, and they should not be turned off.

3. Backup and Contingency Planning

The main contingencies that should be considered and the training with regards to these shall be given to the relevant staff

- Equipment failure
- Physical / natural Disaster
- Messaging or communication facilities.
- Changes in operations and policy
- Sudden absence of key personnel
- Breach in Security

Automatic Backups daily, weekly and monthly should be taken. All the backup procedures and backups needs to be tested regularly for restoration.

4. Performance

Following performance criteria is provided as a guideline only. If the actual performance is falling below the stipulated figures, the Provider is to justify the reasons. However, the performance level must be accepted by the technical evaluation committee appointed by the client.

The bandwidth is assumed at 512kbps (shared) (point to point between LIX and the Department web service) with 1,000 concurrent users (50% load factor) in total.

Item	Performance
Screen Navigation: field-to-field	< 10 milliseconds
Screen Navigation: screen-to-screen	< 5 seconds
Screen Refresh	< 3 seconds
Screen list box, combo box	< 3 seconds
Screen grid – 25 rows, 10 columns	< 5 seconds
Report preview – (all reports) – initial page view (if asynchronous)	< 60 seconds in most instances. It is understood that complicated / large volume reports may require a longer period
Simple enquiry – single table, 5 fields, 3 conditions – without screen rendering	< 5 seconds for 100,000 rows
Complex enquiry – multiple joined table	< 8 seconds for 100,000 rows

(5), 10 fields, 3 conditions – without screen rendering	
Server side validations / computations	< 10 milliseconds
Client side validations / computations	< 1 millisecond
Batch processing (if any) per 100 records	< 120 seconds
Login, authentication, and verification	< 3 seconds
Daily backups (@ Dept.) – max duration	1 hour (on-line preferred)
Total Restore (@Dept) – max duration	4 hours

Annex 3

SERVICE LEVEL AGREEMENT *for* SUPPORT AND MAINTENANCE SERVICES

(i) Introduction

The aim of this agreement is to provide a basis for close co-operation between the Service Provider (name of the company) and Client (ICTA) for support and maintenance services to be provided by the Provider, thereby ensuring a timely and efficient support service is available. The objectives of this agreement are detailed below point(ii).

This agreement is contingent upon each party knowing and fulfilling their responsibilities and generating an environment conducive to the achievement and maintenance of targeted service levels.

(ii) Objectives of Service Level Agreements

- To create an environment conducive to a co-operative relationship between Client, Service Provider and Client's representatives (government organizations) to ensure the effective support of all end users.
- To define the commencement of the agreement, its initial term and the provision for reviews.
- To define in detail, the service to be delivered by each party and the level of service expected, thereby reducing the risk of misunderstandings.
- To institute a formal system of objective service level monitoring ensuring that reviews of the agreement is based on factual data.
- To provide a common understanding of service requirements/capabilities and of the principals involved in the measurement of service levels.
- To provide for all parties to the Service Level Agreement a single, easily referenced document which caters for all objectives as listed above.

(iii) Principal Period of Support (PPS) Requirements

The Principal Period of Support (PPS) is considered in 2 categories as follows;

PPS category	Duration	Applicability
PPS1	From 08:00 AM to 07:00 PM Monday to Friday.	For the essential component applications and online payment service platform related departments.

Service Provider MUST assure System Support and Maintenance Services during the above stipulated times.

(iv) On-Call Services Requirements

Provider MUST make at least ONE qualified personnel available to the Client by telephone and email for the reporting and resolution of non-conformities or other issues, defects or problems. Dedicated telephone numbers and emails should be available for reporting issues. Client will nominate the personnel who are authorized to report non-conformities or other problems with the system from the departments. Reporting of non-conformities includes requests by the Client to apply critical software updates or patches.

Table-1 shows the response priority assigned to faults according to the perceived importance of the reported situation and the required initial telephone response times for the individual priority ratings. All times indicated represent telephone response time during specified PPSs. The indicated telephone response time represents the maximum delay between a fault/request being reported and a Provider's representative contacting the Client by telephone. The purpose of this telephone contact is to notify the Client of the receipt of the fault/request and provide the Client with details of the proposed action to be taken in respect of the particular fault/request.

	Business Critical	**Non-Business Critical**
Fatal	30 minutes	45 minutes
Impaired	45 minutes	90 minutes

Table-1: Response Priority

Note:
Fatal - Total system inoperability
Impaired - Partial system inoperability
Business Critical - Unable to perform core business functions
Non-Business Critical - Able to perform limited core business functions

Provider notification can occur outside PPS time, and thus the response may occur after the next PPS begins. Furthermore, "Time to Arrive On-Site (Table-3)" starts from PPS starting time and "Time to Resolve the Problem" is PPS time starting from the actual time of arrival on site.

(v) Problem Resolution and Penalties

If problems have not been corrected within two (2) hours of the initial contact, the Provider shall send qualified maintenance personnel to the respective Client's site to take necessary actions to correct the issue reported (defect, problem or non-conformity).

If faults are not corrected within the time limits specified in the Table-2, the Client shall be entitled to a penalty payment for each hour that the Consultant fails to resolve the

fault. Maximum ceiling of penalty for a given month is 10% of the invoice amount for the month.

	Business Critical	**Non-Business Critical**
Fatal	1 Hours LKR 12,000.00	2 Hours LKR 8,000.00
Impaired	2 Hours LKR 5,000.00	5 Hours LKR 3,000.00

Table-2: Resolution Time and Penalties

The time to arrive on-site is specified in the Table-3.

	Business Critical	**Non-Business Critical**
Fatal	2 Hours	3 Hours
Impaired	3 Hours	5 Hours

Table-3: Time to arrive on-site

(vi) Service Level Monitoring

The success of Service Level Agreements depends fundamentally on the ability to meet agreed service levels and effective measuring of performance, comprehensively and accurately so that reliable information is available for both parties in agreement. Thereby a clear understanding and effective communication can be maintained between the provider and customer.

Service factors must be meaningful, measurable and monitored constantly. Actual levels of service are to be compared with agreed target levels on a regular basis by both Client and Provider. In the event of a discrepancy between actual and targeted service levels both Client and Provider are expected to identify and resolve the reason(s) for any discrepancies in close co-operation.

Compliance to SLA will be monitored via :

a. Completion of deliverables as per agreed time lines;
b. Accuracy, completeness and quality of the deliverable;
c. Issues resolution within the agreed upon time;
d. On call support within agreed upon time;

Service level monitoring will be mainly performed by Client. Provider may also monitor the level of compliance, for possible improvements. Reports will be produced as and when required and forwarded to the necessary parties.