TERMS OF REFERENCE

for

Procurement of a consultancy firm to perform as Systems Integrator to Establish and Operationally Support the Foundational ID platform for Sri Lanka Unique Digital Identity Project

1. Introduction

1.1. The National Policy Framework (NPF) Vistas of Prosperity and Splendour is aimed at achieving a fourfold outcome of a productive citizenry, a contented family, a disciplined and just society and a prosperous nation. A Technology Based Society (Smart Nation) is one of the 10 key goals of the NPF. In that, setting up a Citizen Centric Digital Government and digitally empowered economy have been identified as a strategy to achieve the government vision.

1.2. Governments worldwide are adopting the strategy of having a Unique Digital Identity (UDI) Framework and Architecture to empower citizens within a Digital Economy and Society. It is envisioned that it could enable dramatic leaps in service quality and massive efficiency gains for governments, as well as drive financial and social inclusion to a maximum extent by providing citizens access to citizen services and benefits of healthcare, education, and other government programs.

1.3. In view of the above, the Sri Lankan Government has also given priority for a national level program for the establishment of a Unique Digital Identity Framework for Sri Lanka (SL-UDI). Therefore, the SL-UDI Framework has been defined as a foundational component with the overall Digital Government Architecture for Sri Lanka as defined by the ICTA.

1.4. ICTA is the apex ICT institution of the Government. In terms of the Information and Communication Technology Act No. 27 of 2003 (ICT Act), ICTA has been mandated to take all necessary measures to implement the Government's Policy and Action Plan in relation to ICT. In terms of Section 6 of the ICT Act, ICTA is required to assist the Cabinet of Ministers in the formulation of the National Policy on ICT and provide all information necessary for its formulation

1.5. Sri Lanka has a strong lineage in the (physical) registration and issuance of Identity Documents (including National Identity Cards). Further, the Department for Registration of Persons (DRP) has been vested with powers by the Registration of Persons Act No. 32 of 1968 to secure the identity of persons by ensuring timely registration of citizens of Sri Lanka. Therefore, the SL-UDI framework is being established in close collaboration the DRP as the key stakeholder of the project.

1.6. By now, ICTA as the implementation / execution agency of the SL-UDI project is in the process of carrying out detailed planning related to possible regulatory changes, process re-engineering, and solution implementation. Considering the SL-UDI framework is a vital element in delivering the National Policy Framework of the Government, ICTA intends to expedite the implementation of the SL-UDI through an accelerated time period.

1.7. ICTA is currently exploring the feasibility of leveraging on a Modular Open Source Identity Platform (MOSIP) with the expectation that the foundational ID solution for SL-UDI be implemented leveraging the MOSIP platform.

1.8. DRP intends to carry out the circa 16.5 million citizen registration, through circa 1,600 enrolment centers, within 1 to 2-year time period.

2. Objective of the Assignment

ICTA intends to initiate the procurement to obtain services of a Systems Integrator to assist ICTA manage the SL-UDI implementation. The Consultant is required to work closely with ICTA in order to ensure successful implementation of the Foundational ID solution envisioned by the SL-UDI.

The Consultant will be required to provide following services;

a. Supply, installation, commissioning and maintaining the software systems required to implement Digital Identity in Sri Lanka
b. To facilitate and integrate with the components/systems necessary to implement Digital Identity and its eco-system
c. To maintain the solution for the mentioned period
d. To suggest and make improvements for a smoother operation during the maintenance period
e. Use of proper technologies to assure high availability, security, performance and usability of the system
f. Provide required documentation and knowledge to implement Digital Identity in Sri Lanka

The Total duration of the assignment is 24-months including 09-months of support and maintenance will commence after the operational acceptance period

3. Scope of Work

1. The consultant is responsible for the supply, installation, commissioning and maintaining the software systems and end-to-end processes required to implement digital identity in the provided infrastructure.
2. The consultant should conduct a system requirement study of the process and review and understand the scope and functionalities required to implement it.
3. On completing the above, a Detailed Software Requirements Specification (DSRS) and a Detailed Software Technical Design (DSTD), including the proposed solution architecture document, should be submitted. Accordingly, the consultant shall prepare detailed design and solution architectures such as server architecture, network architecture, database architecture, security architecture, deployment architecture.
4. If any COTS components are proposed as a part of the proposed design, the consultant must clearly indicate the resultant commercial impact both for initial delivery and during subsequent operations in the bid submission. Further, a cost-benefit analysis should be provided to ICTA. Also, the consultant should facilitate/setup ICTA to have a tri-party agreement with Original Equipment Manufacturer (OEM) for all COTs licenses.
5. The consultant is expected to provide a comprehensive OEM warranty applicable, keep track of all warranties / AMCs & required to make all due payments for warranties / AMCs on time to the OEMs and ensure that the necessary agreements are provisioned and in force always during the tenure of the contract.
6. The consultant shall be responsible for providing annual technology support for the COTS products supplied by respective OEMs during the entire maintenance and management phase. It is mandatory for the consultant to take enterprise level annual support over the entire contract duration, at a minimum, for the COTs/software(s) provided by the SI.
7. All patches and upgrades from OEMs shall be implemented by the SI where it's subject to comprehensive and integrated testing by the consultant in order to ensure that the changes implemented in the system meet the specified requirements and do not impact any other existing functions of the system.
8. Upon obtaining approval from the committee appointed by ICTA for the above, the consultant should design and develop the solution.
9. The implementation shall span across the following stages of software development lifecycle
    i. Development and customization
    ii. System Testing/ Integration Testing/ Performance Testing
    iii. UAT
    iv. Release management
    v. Continuous Build (Continuous Integration / Continuous Deployment)
    vi. Enhancement and augmentation
    vii. Technical Support, Troubleshooting, Identification and Resolution

viii. Change and version control

ix. Patch management

x. Deploy application

xi. Offshore set-up of Development and Test Environment including required tools

xii. L1, L2 and L3 support for application including for MOSIP modules.

10. The vendor should bear the cost of the public cloud which could be used as development and staging environments under the purview of ICTA.
11. The consultant shall use MOSIP applications suite to satisfy the requirements for the core modules. The consultant shall be responsible for configuring, customizing and modifying, deploying, maintaining the MOSIP application suite to comply with given requirements.
12. The consultant shall re-assess the requirement of MOSIP components and suggest customization of the application, if any.
13. The consultant should submit all deliverables as specified in the below item '5– Final outputs, Reporting Requirements, Time Schedule for Deliverables'.
14. The consultant should obtain approval from the committee appointed by ICTA for the all deliverables.
15. ICTA intends to develop and launch the proposed solution in Twelve (12) months, followed by Three (03) months of operational acceptance. During the OAT period, system functionality, quality, and performance will be verified. The Nine (09) months of support and maintenance will commence after the operational acceptance period.
16. The consultant should implement all nonfunctional requirements (security, governance including role-based security, user lifecycle management, and complete audit-trails, etc.)
17. The consultant should study existing integrations with external organizations and carry out any enhancements needed for the proposed solution in order to provide a more comprehensive service which will be reviewed by ICTA.
18. The consultant should facilitate and carry out the integration with other systems including but not limited to ProgressiveID, National Data Exchange (NDX), Automated Biometric Identification Systems (ABIS), Card Printing Services, BiometricSDK, Biometric devices and COTs etc.
19. The consultant should evaluate mobile integrations such as Mobile Connect, native/hybrid mobile app development to facilitate digital ID services to the stakeholders.
20. The consultant should study and facilitate API integrations to external systems to facilitate Digital ID life cycle.
21. The consultant should propose the most suitable solution to securely expose data.

22. The proposed solution should be compatible with the latest technological components and best practices and which will be reviewed by ICTA and should be able to deploy into staging and production in cloud platforms provided or prescribed by ICTA.
23. The consultant should follow the proper coding standard and maintain project source code in the ICTA GIT system and upload all the relevant documents to the ICTA SCM.
24. The consultant should study and propose suitable hardware requirements (such as scanners and printers, if required) to the proposed solution and should provide the detailed specifications.
25. The proposed solution should integrate with multiple payment gateways and bank wallets proposed by the ICTA to facilitate online payments.
26. The proposed services/modules offered to the public (eService interfaces) should be available in tri-languages (Sinhala, Tamil, and English).
27. The consultant is compelled to use FOSS applications in all possible scenarios.
28. If any commercial version of the software needs to be used in the proposed solution, the consultant needs to inform ICTA in advance with proper justification of the requirement. All the licenses/subscriptions purchased should be under ICTA.
29. Adopt a proper application release procedure to release the applications to the environments during the deployment in the staging/ production environments at the cloud.
30. An issue log shall be maintained by the consultant for the errors and bugs identified in the solution as well as any changes implemented in the solution. Issue log shall be submitted to the ICTA monthly.
31. The consultant should understand and ensure the existing data volume and data complexity and provide a data migration strategy accordingly. Moreover, the data transformation strategy should follow the proper industry standards and proper control mechanisms in transforming these data to the new solution.
32. The solution should adhere to Web 2.0 concepts, open standards, and Service-oriented architecture (SOA) and industry standards.
33. The proposed solution should be browser independent and able to access with less configuration in the client workstation.
34. The consultant should carry out end-to-end security assessments prior to the solution launch and fix any issues found. Further, ICTA will conduct security assessments periodically, and the consultant should fix any vulnerability issues identified during assessments. (Prior to solution launch and during support and maintenance period).
35. The consultant should follow templates if provided by ICTA for deliverables.
36. The consultant shall comply with the independent quality assurance process, which will be carried by a team designated by the ICTA.
37. The consultant should derive the UAT test cases in collaboration with ICTA.

38. The consultant shall undertake benchmark exercise before Go-live. Validate the application and infrastructure performance benchmarks and undertake enhancement/augmentation, if required.
39. Obtain User Acceptance for the implemented solution collaboratively with the committee appointed by ICTA.
40. The consultant shall be responsible for ensuring information security including:
    i. Development of security processes and procedures
    ii. Development, documentation, implementation, and maintenance of minimum baseline security standards
    iii. Design, documentation, implementation, and maintenance of security design requirements
    iv. Supply, Procurement, deployment and commissioning as well as operations of all security tools and technologies
    v. Documenting, implementing, as well as obtaining certifications
41. The consultant shall provide necessary support and cooperation for the audit and close the findings of an audit.
42. The proposed solution should have a proper data backup plan and equip with a high availability and fault tolerance plan.
43. The consultant should provide support and maintenance services from the date of launch to the agreed time period. Moreover, the consultant should adhere to the Service Level Agreement (SLA), during the support and maintenance (S&M) phase.
44. The consultant should implement an SLA Management and Monitoring solution, configure the SLAs in the tool and enable automated monitoring and reporting of adherence to Service Levels. Manual intervention in computation of service levels should be avoided and all monitoring and measurement should be automated.
45. The consultant should develop a proper alerting mechanism to monitor system performance issues, exceptions, and system downtimes. Moreover, the proposed alerting mechanism should send an alert via SMS to designated offices by ICTA.
46. During the support and maintenance period, the consultant should attend to any issue reported and carryout configuration changes (if required) and apply relevant security patches to ensure the security of the solution and apply updates and tuning of performance, etc.
47. The Consultant should accommodate change requests (CR) after obtaining approval from the Change Control Board and as per the CR rate agreed in the contract.
48. All planned or emergency changes to any component of the system should be carried out through the approved Change Control Management process by ICTA. The consultant must always follow standard industry processes.
49. The consultant should provide proper application training and knowledge transfer all for all designated offices by ICTA regarding technical aspect.
50. The consultant should provide a training plan, considering different users, different functionalities, and the number of days, training approach, required language, etc.

51. The consultant is responsible for imparting the identified training in accordance with the training plan. The SI shall also be responsible for preparation of training materials, certificates, training aids (document, audio or video), and venues (including meals) that are required for successful completion of the training. During the training, consultant needs to provide copies of the relevant training material.
52. The consultant has to ensure that the training sessions held are effective and that the attendees would be able to carry on with their work efficiently. For this purpose, it is necessary that the effectiveness of training sessions is measured. The consultant shall prepare a feedback form that will capture necessary parameters on measuring effectiveness of the training sessions. This form will be discussed and finalized with ICTA.
53. The consultant should provide both soft and hard copies of user manuals (e.g. Printed documents and CDs). All manuals should be in tri-languages (Sinhala, Tamil, and English).
54. Adhere to ICTA project management practices
55. Participate in Project Review Committee meetings and Project management committee Meetings as a member and present the status of the project when necessary.
56. The consultant who engages with the assignment should sign a Non-Disclosure Agreement (NDA) where applicable.
57. The intellectual property rights of the solution and all artifacts in accordance with the conditions of the contract.
58. The consultant should collaboratively work with the project stakeholders (i.e. ICTA's team, management consultant, suppliers, departments, certification bodies, etc) designated or proposed by ICTA.
59. The consultant should work with the Management Consultant (MC) of the SLUDI project and accommodate the policies, procedures, recommendations and the practices proposed.
60. The consultant should facilitate & provide technical guidance to set up the registration centers.
61. The consultant should suggest and make improvements for a smoother operation during the maintenance period.
62. The following items are out of scope for the SI,
    i. Purchasing biometrics devices, BiometricSDK & ABIS
    ii. ABIS software and hardware for deduplication, Manual Adjudication System and biometric SDKs
    iii. Card personalization systems & cards delivery/shipping
    iv. Provision of network links
    v. Systems' operators and administrators
    vi. Site/Center preparation
    vii. Telecommunication costs (SMS)
    viii. Purchasing of cloud/network infrastructure

ix. Cost of operating system and virtualization software
x. Cost of project management, bug and issue tracking software
xi. Payment service provider fees (IPG)
xii. Data center infrastructure and utilities

4. Professional Staff and Engagement approach

4.1 Following key professions are required for the core team

No	Key Professional Staff
1	Project Director
2	Technical Project Manager
3	Lead Software Architect
4	Technical Lead
5	Senior Software Engineer
6	Lead Business Analyst
7	Lead UI/UX
8	Lead DevOps Engineer
9	Quality Assurance Lead
10	Lead Security Architect
11	Application trainer
12	Lead Security Architect
13	Ecosystem Specialist
14	Risk Manager

4.2 The Consultant should ensure adequate support staff to assist the Project Management Professional are assigned to this project.

5. Final outputs, Reporting Requirements, Time Schedule for Deliverables

The total project duration is 24-months including 09-months Support and Maintenance. The consultant is required to submit the following list of deliverables.

No	Deliverables	Phase	Duration
1	1.1. Solution Implementation Proposal 1.2. Detailed Software Requirement Specification (DSRS) 1.3. Implementing schedule / Project Plan 1.4. QA Test Plan 1.5. Acceptance criteria for Deliverables and UAT 1.6. Training Plan 1.7. COTs Report	Inception	Commencement + 1 ½ Months
2	2.1 Detailed Software Technical Documentation (DSTD) 2.2 Release Management Plan (including staging, production and support, and maintenance) 2.3 Data migration and integration plan 2.4 Application Prototype 2.5 Hardware requirement for the deployment	Elaboration	Commencement + 2 Months
3	3.1. Proper maintenance of source code in SCM 3.2. Test Cases and Test scripts	Construction	Commencement + 7 months
4	4.1 Solutions installation guide 4.2 User manual 4.3 Administrator manual 4.4 Updated Lanka Gate Help Desk templates (Knowledge Tree and T1 Document) 4.5 Government organization level training 4.6 Successful UAT acceptance	Transition	Commencement + 9 Months
5	5.1 Successful Operational Acceptance (OAT) 5.2 Traceability matrix 5.3 Up-to-date source code 5.4 Up-to-date documentations 5.5 Transition and Exit Management Plan	Acceptance	Commencement + 12 months
6	6.1 Monthly Support and Maintenance Report 6.2 Final S&M report should consist with comprehensive knowledge transfer documentation. 6.3 Relevant documentation updates as required.	S&M	Date of operational acceptance + 09 months

6. Facilities and Services provided by ICTA

1. Current InfoID solution documents will be provided.
2. Proper knowledge transfers of the existing systems including the relevant technical documentation.
3. Access to the ICTA Document management (SCM) system.
4. Access to staging/ production servers.
5. Arrange and facilitate the workshop/training with relevant stakeholders.
6. Access to the ICTA source code management (GIT) system.

- End-