THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

Ministry of Technology

BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS

Volume 02 of 03 - Annexure 8: Biometric Certification

Single Stage Two Envelopes Bidding Procedure

FOR THE

PROCUREMENT OF A MASTER SYSTEM INTEGRATOR (MSI) FOR DESIGNING, DEVELOPING, SUPPLYING, DELIVERING, INSTALLATION, IMPLEMENTING, SUPPORT AND MAINTAINING THE SOFTWARE, HARDWARE AND INFRASTRUCTURE FOR SRI LANKA UNIQUE DIGITAL IDENTITY (SL-UDI) PROJECT OF GOVERNMENT OF SRI LANKA

INVITATION FOR BIDS No: **ICTA/SLUDI/IS/2022/01**

May 07, 2023

Table of Contents

8.1 Illustrative Biometric Device Certification Process

8.1.1 Purpose

Purpose of this is to describe the Procedure for obtaining the certification of Biometric Devices for SL-UDI program.

8.1.2 Target Audience

The MSI of biometric devices and the certification body (CB) shall follow this procedure for certification.

8.1.3 Certification Context

Biometric holds out the promise of increased confidence in personal authentication processes compared with traditional password and tokens. This is because of the direct link between the biometric characteristic and the individual. Measuring the quality of biometric sample is a crucial step in the collection process. Quality of sample features (data quality) that can be extracted from digitized sample depend on the image quality. Poor quality biometric image diminishes the matching performance of biometric recognition system result in false matches, false non-matches and increase search time.

To meet the objective of SL-UDI, it is required that sufficient degree of assurance is provided that good quality of biometric devices is available to the user agencies. Testing and Certification are means to provide this confidence. This procedure facilitates the execution of Certification Process. This certification is primarily focused on combination on sensor and the extractor. However, the context on the device is not lost during the certification activity covering its reliability, portability, and other relevant characteristics. The applicant shall provide the details of both the components (sensor and extractor) in their application.

8.1.4 Objectives of Testing and Certification

The key aim of testing & certification is to ensure that the Device Under Test (DUT) complies with the requirements, relevant standards, specifications including specifications released by SL-UDI. The objectives are to verify:

(i) The extent to which requirements prescribed in the relevant SL-UDI specifications have been fulfilled.

(ii) The extent to which applicable regulations, standards and specifications set out in the applicable Quality specifications are met.

(iii) Provide opportunity for Vendors to understand defects/ nonconformance and rectification of the same.

(iv) To grant certification and provide assurance to users of devices that the certified product meets SL-UDI requirements comprehensively.

(v) To conduct an operational evaluation , security evaluation and performance evaluation.

8.1.5 Scope of Work

The scope includes testing & certification of the following Devices:

(i) Single Fingerprint Image Scanners for authentication
(ii) Multiple Fingerprint Image Scanners for enrolment
(iii) Iris Image Scanner for enrolment and authentication
(iv) Multiple Iris Image Scanner for enrolment
(v) Face Scanners for enrolment and authentication
(vi) Other devices as may be included from time-to-time

8.2 Procedure

8.2.1 Pre-requisite for Certification

(i) MSI shall understand the Certification and Surveillance requirements, applicable charges etc. before applying to Certification Body.
(ii) MSI shall prepare a Technical Construction File (TCF). The clarity in TCF provide confidence to the Certification Body regarding Quality of Device. The requirements of TCF are given in Section 8.2.11.

If MSI is confident regarding meeting the Certification requirement then he can apply to Certification Body.

8.2.2 Application

(i) The MSI shall fill the application and submit it to Certification Body (CB) along with the enclosures (1 copy TCF). MSI shall submit the application fee as per schedule of charges. CB will evaluate TCF (Technical Construction File) preliminarily and if found satisfactorily Certification Agreement will be signed.
(ii) MSI shall submit three sets of Biometric devices, Test kit for Image Quality along with a copy of TCF to Biometric Device Test Lab (BDTL). They shall fill Service Request Form (SRF) and submit the test charges. BDTL shall inform the MSI Probable Date of Completion (PDC).

8.2.3 Commencement of Test

CB will inform the Head BDTL to proceed for Testing as per Standard Test Plan. Issue of Provisional Certificate TCF will be evaluated comprehensively and if found meeting the criteria let down and satisfactory completion of functional testing CB will issue the Provisional Certificate.

8.2.4 Test Approach and Methodology

The following test approach & methodology will be used:

(i) The robustness of the devices will be tested by subjecting these devices to simulated environmental conditions (climatic & durability) such as temperature, humidity, dust, etc., as specified by the requirement, relevant specification document provided by SL-UDI.

(ii) The output of the biometric devices will be checked for compliance to relevant specification document provided by SL-UDI.

(iii) The integration of Biometric device with the system will be tested through:

a) Verification of compliance to relevant API standard published by SL-UDI.

b) Carrying out end to end functional testing using relevant software/ a Test harness. Repeat functional testing for consistency of operations.

c) Quantitative Data Analysis: Carry out periodic field sample collection from vendor devices as per SL-UDI procedure for predetermined number of Subjects. Results from the study will provide quantities metrics that will be used to qualify devices. This is a very crucial procedure for ensuring consistency and interoperability. This procedure applied in particular to biometric capture devices. Data collection will be done by SL-UDI / its representative. CB will do data analysis.

In order to verify compliance to the device specifications and schedule of requirements, one or more of the followings will be used:

(i) Testing may be conducted in the CB laboratory.

(ii) External test laboratory/ MSI's test facility may be used to conduct the testing (where test facilities are not available with CB).

(iii) Compliance may be verified by demonstration(s) of testing using MSI's test facilities.

(iv) Compliance may be verified based on the test reports &/or certifications obtained by the MSI (subject to verification of test results on sample basis.

To carry out testing following shall be arranged:

(i) Test Harness would be provided by SL-UDI

(ii) During certification, complete compliance to authentication specification will be checked including compliance with API, released by SL-UDI

(iii) For authentication devices, various authentication components may need certification which adheres to relevant specifications published by SL-UDI

(iv) Certification authority has to carry out Statistical and qualitative analysis as per SL-UDI guidance.

8.2.5 Inputs Required by CB

Access to the followings information & facilities/ systems to undertake testing of DUT will be required by CB:

(i) SL-UDI Requirements – RFP Document, Biometric device specifications, API Documentation

(ii) Device Documentation – Biometric device specifications, Design Document, User/ Operations Manual, SDK Documentation

(iii) Biometric Device to be tested with SDK, software application, database & test samples.
(iv) Test environment for testing of specialized parameters (if required)
(v) Internal test reports of MSI.
(vi) Arrangement to witness the testing at MSI's facility, in case the in-house facility for the same is not available with CB.
(vii) Image Quality Test Kit consisting of:

- Image capture device software
- Analysis software
- Test target and associated fixtures
- Support tools and test procedure document

MSI would need to be directly providing the documentation to CB and as per the certification needs provide additional information/ Test results.

8.2.6 Scope of certification

The MSI shall refine the scope of certification based on SL-UDI specification and requirements, UA's requirement, ISO/IEC & ICAO standards (refer biometric standards in the Adopted Standards Section of Volume-2) and other market needs. Sensor extractor combination is certified for a specified device at first. Once this sensor extractor combination is validated for image quality for SL-UDI authentication, the certificate can be extended to other form factor devices using exactly the same sensor extractor combination subject to the following conditions being met by the new device for the "intended application".

(i) OEM sensor extractor certified by CB earlier for device D for SL-UDI authentication.
(ii) OEM authorization if use of senor extractor in the proposed device.
(iii) Compliance with other applicable specifications as per the "intended application" – example: portability in case of mobile biometric devices. (Scenario evaluation)
(iv) Environmental and robustness specification as per the "intended application" example: (Operating Temp, Humidity, Drop*, Vibration, IP)
(v) Functional test as per the "intended application" workflow. (Scenario evaluation)
(vi) Security requirements as per the SL-UDI specifications (Presentation attack testing (Liveliness))
(vii) Additional requirements as per the "intended application" (like MicroATM specs for FI)
(viii) Additional certifications for the "intended application" (like PCI for payment terminals).
(ix) Technology Evaluation – compliance to the technical requirements as per the Sl-UDI specifications.
(x) Operational evaluation – Analysis of performance problems in production SL-UDI and resolve the performance problems.

*Mainly suitable for mobile handheld devices.

"Intended application"- Financial inclusion, PDS, LPG subsidy, Telecom, and so on using SL-UDI authentication platform.

8.2.7 Testing

Testing activity consist of the following tasks:

(i) Study & Understanding
(ii) Test Planning & Preparation
(iii) Test Execution
(iv) Test Report Preparation

8.2.8 Key Features of Testing

(i) CB shall conduct test for biometric authentication device - "Sensor" output - Compliance to the ISO 19794-4 template using SL-UDI supplied test harness.

(ii) For assuring quality of sensor image output, the vendor shall:

a. Submit the PIV compliance certificate. Or
b. Manufacturer own facility test report demonstrating compliance with PIV test specifications. Or
c. Any alternative equivalent of the above with the support of technical rationale which will be reviewed and evaluated by a technical expert committee nominated by a competent authority. Or
d. Based on the test report generated by Biometric Device Test Laboratory (BDTL) of CB by testing as per the requirements of ISO 19794-4

The MSI supplied test reports and certificates may be acceptable for Provisional certificate. For certificate of approval, CB may be carrying out independent testing separately.

(iii) Technically image enhancement for certification is not acceptable. NFIQ score will be tested using SL-UDI supplied test harness. CB shall conduct the test on number of subjects (for all ten fingers). The test subjects shall have at least one finger with NFIQ score reported/observed to be with value numeric one.

(iv) CB shall conduct test for biometric authentication device - "Extractor" output –compliance to the ISO 19794-2 template.

To check the quality of biometric authentication device extractor, the following test shall be conducted:

(i) First of all only those subject samples shall be considered fit for test whose number of minutiae extracted by using the backend extractor shall be at least 16. These successful test samples shall be used with the MSI devices (DUT) & the extractor shall pass the test if it is able to extract at least 12 minutiae points. This should not include false minutiae which can adversely affect template quality (as per the ISO 19794-2, for authentication at least 12 minutiae points must match).

(ii) In order to meet the objective of SL-UDI Authentication Service where the residents get a usable & reliable service, the MSI device (sensor+ extractor combination) should be compatible with the backend of SL-UDI & shall be able to deliver an acceptance FRR and FAR the threshold value fixed by the SL-UDI.

(iii) SL-UDI shall expose a "test service" (similar to their backend in terms of extractor and matcher algorithms used), access to which shall be provided to the MSIs of biometric authentication devices on registration. The MSI's (BDTL) is expected to conduct testing on at least 1500 devices from each type samples (residents) to gain the confidence that their sensor + extractor combination is compatible with the SL-UDI backend & shall be able to deliver the desired FRR. This test may take quite some time & cannot be completed in a short duration expected for provisional certification. Thus the provisional certificate shall be granted if the above conditions get satisfied along-with the system related control checkpoints viz. ISO 9001 of Manufacturer & MSI, RoHS undertaking, Manufacturer authorization of MSI etc. The MSI is expected to provide a report for compliance to this requirement within 3 months, in order to maintain his provisional certification.

(iv) BDTL will execute the testing as per Test Plan. In case of any non-compliance/failure BDTL shall inform to the MSI and stop the testing. The MSI should analyse the results and take corrective action, both at device level and at System Level. (If corrections are required at Manufacture level/Principal Level, MSI shall co- ordinate and inform to CB. The testing can be re-started if CB is satisfied with the analysis and corrective actions are satisfactory. CB and BDTL will decide whether to start test from zero level or partial testing is adequate depending on the situation and engineering analysis of the test data. This should be recorded and presented to Certification Committee (CC) at the time of Certification. The MSI shall maintain analysis and corrective actions records which will be audited during surveillance visit. After completion of the tests BDTL shall prepare the Test report in approved format and forward the detail test report to CB.

8.2.9 Certification

Certification body will internally check the compliance with respect to Rules and Procedures of the scheme and put up to Certification Committee (CC) after:

(i) Analyzing the test results

(ii) Verifying compliance to evaluation Criteria

Certification Committee will review the reports and other information holistically, and give its recommendation for Certification. CC can use a reference Checklist.

8.2.10 Deliverables

On satisfactory completing all above activities and fulfilment of certification & Evaluation Criteria, CB will issue the final invoice and after receipt of payment issue the certificate along with the test report. The MSI should bare the payment.

BDTL is responsible for storage and maintenance of the devices and other customer MSI products (Test fixture, supplied Test Methods, Software, and Documentation etc.).

8.2.11 Requirements of Technical Construction File (TCF)

To create confidence in the Device Quality, MSI shall maintain a technical construction file. This will require close collaborations of MSI with the manufacturer. The confidential part of this file may not be revealed to the Certification Body only summary/ principles used of confidential part of the file may be informed to the Certification Body on need base. The general content of the TCF are:

General	• General description • Biometrics Device Specification (may be in the form of brochure) • Quality Control System (with special emphasis on Image Quality) • List of Applicable Regulations/Standards • Risk Assessment
Certificates	• Certificate for ISO 9001:2008 (Certification for Biometric Device Development, Manufacturing and Service (Manufacturer) • Certificate for ISO 9001:2008(Certification for Biometric Device Supply and Distribution, Training, Maintenance, Calibration and Services (MSI/Distributor)) • Certificate of Common Criteria • Certificate of Incorporation in Sri Lanka (MSI) • PIV Certificate for Image Quality for finger print Scanner • IECEE-CB Certificate (IEC 60950) for safety, enclosed with CB Test Report from recognized CTL or equivalent dual certification. • WHQL Certificate for Device Driver along with test report • Manufacturer authorization to MSI to place devices in Sri Lankan market Declaration of Conformities Declaration to compliance with Restriction of Hazardous Substances (RoHS) and Waste Electrical and Electronic Equipment Directive • (WEEE) requirements
Test Report	• Image Quality, Test Procedure and Test Report • Common Criteria certification report • EMI/EMC compliance test report • Safety Compliance Test Report • SL-UDI API Specification Compliance Test Report • Environment/Durability compliance test report • Performance test report or FAR of SL-UDI requirements with technical rationale.
Technical Information	File shall provide the necessary evidence that the design is in accordance with the relevant requirements. File shall identify the product and its specification consisting of its description in terms of: • Photographs, brochures • Technical construction drawing and Schematic diagram • User Manual

Table 1 :General content of the TCF

8.2.12 Test Plan

Test Plan

Device Sample 1

- Visual Inspection
- Physical & Dimension testing
- Interoperability Testing
- SL-UDI API Compliance Testing
- Functional Testing
- Image Quality Testing
- (To be stored for reference)
- (Scenario evaluation)
- (Presentation attack testing (Liveliness))
- Technology Evaluation
- Operational evaluation

Device Sample 2

- Visual Inspection
- Functional Testing
- Image Quality Testing
- Environmental & Durability Testing
- EMC Testing
- (Scenario evaluation)
- (Presentation attack testing (Liveliness))

Device Sample 3

- Visual Inspection
- Functional Testing
- NFIQ Compliance Testing
- Performance Testing
- (Scenario evaluation)
- (Presentation attack testing (Liveliness))
- Technology Evaluation
- Operational evaluation

8.3 Registration of Devices

The process of registration of devices is given below:

(i) **Entry of Certified Devices**: The Designated Officials of Authority (DOA) i.e. users which will act on behalf of the authority to create an entry of certified devices i.e. their make, model, type (fingerprint/iris), certificate number, date of certification, certification end date, etc.

(ii) **Renewal of Certified Devices**: The designated officials of authority (DOA) will be able to mark the renewal of existing certified devices by selecting make, model, type (fingerprint/iris) of concerned device and entering renewal details such as certificate number, date of certification, certification end date

(iii) **Suspension of Certified Devices**: The designated officials of authority (DOA) will be able to suspend the certified devices by selecting make, model, type (fingerprint/iris) and entering the suspension order number and effective date till which suspension should be valid.

(iv) **Revocation of suspension**: The suspension of the certified device should be revocable under two circumstances (i) Automatically on expiry of suspension period, (ii) Manually revoking the suspension by selecting make, model, type (fingerprint/iris) and entering the suspension revocation order number and effective date till which revocation is valid.

(v) **Registration of Devices by UAs**: On purchase of biometric device, the UA Administrator should be able to register their devices by selecting the certified device using its make and model and entering the unique serial number of the device. In case of duplicate serial number for the given make and model, the registration should not be permitted. On successful registration, a unique device code will be allocated to the registered device which should be sent along with authentication service request. At the time of suspension of certified device, any new device of the concerned make and model should not be allowed to get registered.

(vi) **Deregistration of device by UAs**: The UA Administrator should be able to deregister an already registered device. For this the UA Administrator should either provide unique device code or the make, model and serial number of the device.

(vii) **Registration of Devices by residents**: This functionality is similar to that of ‘Registration of Devices by UAs’. The resident would be required to login using NIU and OTP in the portal. At the time of suspension of certified device, any new device of the concerned make and model should not be allowed to get registered.

(viii) **Deregistration of device by residents**: This functionality is similar to that of ‘Deregistration of Devices by UAs’. The resident would be required to login using NIU and OTP in the portal.

8.4 Local Certification Lab

If a local lab is made available at the time of certification, the MSI utilize such services locally, where the rates are in par with international CB or at a lower rate.

8.5 References for BDC Process

[1] Rules and Procedures for Biometric Device Certification (Authentication) BDCS(A)-03-01), Issue-2 http://www.stqc.gov.in/sites/upload_files/stqc/files/STQC%20UIDAI%20BDCS_A_-03-01%20Rules%20and%20Procedure%20for%20Biometric%20Device%20Certification_Authentication_%2011012016%20_1.pdf

[2] Procedure for obtaining Biometric Device Certification (Authentication) (BDCS (A)-03-02) ISSUE-1 http://www.stqc.gov.in/sites/upload_files/stqc/files/STQC%20UIDAI%20BDCS-03-02%20Procedure%20for%20obtaining%20Biometric%20Device%20Certification_Authentication_.pdf

[3] Test Method and Procedures for Biometric Devices (Authentication) BDCS (A)-03-09 Issue 1 http://www.stqc.gov.in/sites/upload_files/stqc/files/STQC%20UIDAI%20BDCS-03-09%20Test%20Method%20and%20Procedures%20for%20Biometric%20Devices_Authentication_.pdf