Approval and Issue

This document is the property of STQC Certification Services and should not be reproduced in part or full without the written consent.

Approved by **:** ____________________________
Chief Executive Officer

NOTE:

1. Management Representative is responsible for issue and distribution of this document including amendments.

2. Holder of this copy is responsible for incorporation of all the amendments and currency of the document

Amendment Record

Amendment No.	Date of Amendment	Nature of Amendment	Page Ref.

1.0 Purpose

The purpose of this document is to define procedure and criteria of certification of IRIS Authentication devices to be used for various programmes which require Aadhaar Based Authentication for service delivery.

2.0 Target Audience

The supplier of Iris authentication devices and the certification body shall follow this procedure for certification.

3.0 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 UIDAI, it is required that sufficient degree of assurance is provided that good quality of authentication devices is available to the user agencies. Testing and Certification are means to provide this confidence. This procedure facilitates the execution of Certification Process.

IRIS Authentication device Certification is required to

- Maintain quality of IRIS Authentication devices across the UIDAI eco-system for uniform resident experience
- Ensure Maximum compatibility and interoperability of devices across the application/ vendors
- Ensure Reusability of various authentication applications available across UIDAI ecosystem
- have the consolidated benchmarking of IRIS Authentication devices vis-à-vis available industry standards
- Ensure service levels and support availability

Ensure secure and transparent authentication

4.0 Background:

Aadhaar Authentication

The Unique Identification Authority of India (UIDAI) has been created with the mandate of providing a Unique Identity (Aadhaar) to all residents of India. The CIDR processes these enrolments by reduplicating them to ensure uniqueness and then issues Aadhaar numbers.

One of the mandates given to UIDAI is to define usages and applicability of Aadhaar for delivery of benefit services. The Aadhaar number, which uniquely identifies a resident, will give individuals means to clearly establish their identity to public and private agencies across the country for service delivery. UIDAI provides online authentication using the resident's demographic and biometric information to support Aadhaar-enabled delivery of services. This is done by using single finger print authentication and IRIS authentication technologies. To have confidence on the system, certification of these devices is chosen as one of the means to achieve the said objectives.

5.0 Reference documents:

ISO 19794-6; Information technology – Biometric data interchange formats – part 6: Iris Image data
NISTSP500-280; Mobile ID Device Best practice recommendation version 1.0
ISO/IEC 29794-6, Biometric sample quality – Part 6: Iris image data
UIDAI IRIS Authentication device specification

6.0 Objective:

The objective of Certification of IRIS Authentication Devices is to facilitate availability of Quality Assessed Devices to user agencies. This certification scheme provides confidence that certified devices are reliable, safe, secure and meet the requirements of UIDAI.

This objective is attained by ensuring device suppliers are certified based on their capability to supply IRIS Authentication Devices which meets the technical specification of UIDAI and suppliers have adequate support systems to ensure availability of device functionalities/services in its life cycle. This includes but not limited to training on process to operator and maintenance of devices.

Testing:

a) To verify the degree of compliance of device characteristics and specification with UIDAI requirements specification.
b) Provide opportunity for Vendors to understand defects/ nonconformance to rectify the same leading to improvement in the quality.
c) To grant certification and provide assurance to users of devices

Certification:

a) To make purchase decision easy and fast from buyer perspective as certified devices are technical compliant with UIDAI specification.

b) Reducing overall cost of demonstrating compliance, as certification is a continuous process compared to repeatedly demonstrating compliance tender wise to different buyers.

c) Enhancing Quality benchmarks systematically in a well structured way through consultative process with stakeholders.

d) To provide a platform to stakeholders in regard to “Quality” of the device.

7.0. Scope:

Scope of certification covers various type (Form factor) of IRIS Authentication Devices

8.0 Definitions and Explanations:

Supplier (Services)
The party that is responsible for placing IRIS Authentication Devices into the Indian Market and is able to ensure that Quality assessment is exercised. The supplier can also be client, vendor, channel partner, authorized agent with an legal entity in India. For the IRIS Authentication of this scheme supplier is the applicant and responsible for obtaining the certification.

Manufacturer (Product)
Legal Entity anywhere in the world that makes IRIS Authentication Devices through a process involving raw materials, components (optical, opto-electronics, electronics, embedded software etc.) or assemblies, usually on a large scale with different operations divided among different workers. They are also responsible for Quality Assurance of the produced devices including Testing of Devices as per UIDAI requirements.

Reseller: A reseller is a company or individual that purchases IRIS AUTHENTICATION Devices with the intention of reselling rather than using. A reseller’s product fulfillment based business models can include a corporate reseller, retail or direct market reseller.

Quality Assessment
The totality of measures carried out consistently and systematically, in order to ensure that IRIS Authentication Devices conforms to the UIDAI requirements of a stated specification.

Certificate of Approval

Certificate issued to the supplier after successful completion of all the tests in a control laboratory environment, demonstrating objectively that all the Quality requirements of UIDAI has been met.

Certificate of Approval is issued once adequate level of confidence is obtained about the Quality of IRIS Authentication Devices that it meets the UIDAI specifications. This confidence is based on objective assessment of laboratory test reports and documented evidence supplied by the applicant demonstrating compliance with some of the requirements. This has validity of 3 years.

Certification System

System that has its own rules of procedures and management, for carrying out certification of compliance/ conformity.

Certification Body (CB)

The body which conducts certification of compliance/conformity with respect to published UIDAI specification. STQC is the certification body for IRIS Authentication certification.

Certification Agreement

An agreement which is part of the Certification System and which details the mutual rights and obligations of the certificate holder and the Certification Body, and which includes the right to use the certificate.

Appeal

A formal expression of dissatisfaction by a party affected with a decision of a Certification Body, which is directly related to the certification status of the IRIS Authentication Devices.

Complaint

A formal expression of dissatisfaction with some matter related to a Certification Body, a certified supplier, a certified IRIS Authentication Devices or an individual.

Dispute

Expression of difference of opinion between two parties in relation to some matter related to a Certification Body, a certified supplier, a certified IRIS Authentication Devices an individual.

Minor Non-conformity

A Minor Non-conformity is an isolated procedural lapse that will not directly affect the conformance of the IRIS Authentication Devices to the applicable specification.

Major Non-conformity

A Major Non-conformity is the absence of or the in-effective implementation of one or more required system elements, or a situation, which would, on the basis of objective evidence or evaluation, affect the conformance of the IRIS Authentication Devices to applicable requirement of UIDAI.

9.0 Approval & Issue

This document has approval of the competent authority and is the property of STQC & UIDAI Govt. of India and should not be reproduced in part or full without the written consent.

10.0 Approach and Principles

Principles used for Certification

i) Device are designed and manufactured consistently as per UIDAI Specifications

ii) The device distributor in India have necessary and sufficient support infrastructure

For assessing Quality of IRIS Authentication Devices following approach is followed:

i) Control of processes of manufacturer at the manufacturer' site

- *Demonstration by an established Quality Management System for designs/development, production and supply of IRIS* Authentication *Devices as per UIDAI Specs*

ii) Control of Processes of suppliers

- *Demonstration by an established Quality Management System for Distribution. Maintenance, training and support services and supply of IRIS* Authentication *Devices)*
- Manage relationship between supplier and manufacturer(OEM) for sharing critical information

iii) Functional and Performance Testing to verify the Quality *(Demonstration through independent testing)*

11.0. Responsibilities

Device Supplier: Since Supplier is placing the devices in the Indian Market they are responsible to ensure delivery of devices as per contract and having a support system for life cycle management of the devices. Supplier is responsible to provide inputs, information and the hardware etc. as outlined in Application Form to STQC.

Supplier can sell its product to reseller under the scheme by knowing the end customer details from reseller. The serial nos. of each device will be maintained in records by reseller for supplier. Supplier will provide training and the support and knowledge transfer for troubleshooting.

Supplier shall be in agreement with reseller for back to back hardware and maintenance support and reseller is responsible and in binding to use these devices only specific to that project only. Certification body is not responsible to exercise any control to reselling activity. Supplier shall keep the record of all the devices sold to the reseller.

Golden Supplier: Under the scheme OEM shall appoint their golden supplier in India who is responsible to interact with STQC for the purpose of certification. The term golden supplier has no business connotation and term is used for operation convenience. OEM can have their own models for multiple authorized suppliers.

The term "Golden supplier" is applicable between STQC and OEM only. The golden supplier should not be allowed to claim any type of special status from certification perspective. OEM can treat him as a preferential supplier as per his own internal policy. The test report will be owned by OEM and all the test charges needs to be paid as per Indian laws and regulations act. Hence different suppliers need not get the product tested again and again.

Device Manufacturer: Device Manufacturer is responsible to provide all technical support to the supplier (Applicant) and the facilitate the certification.

STQC: STQC is responsible for certification activity and acts as certification body.

Director Test Laboratory: Director Test Laboratory is responsible for planning and managing the testing activity. Software test laboratory is responsible for conducting test on the devices and application in reliable and professional way.

12.0. Procedure

*12.1 **Pre**-requisite for Certification*

a) Supplier shall understand the Certification and Surveillance requirements, applicable charges etc. before applying to Certification Body (STQC).

b) Supplier shall prepare a technical construction file (TCF). The clarity in TCF provides confidence to the Certification Body regarding Quality of IRIS Authentication Device. The requirements of TCF are given in Annexure I.

Supplier is responsible for ensuring that device is compliant (with UIDAI specification) device, he shall provide these declarations based on test report as part of their technical construction file.

If supplier is confident regarding meeting the Certification requirement then he can apply to Certification Body (STQC). The contact details are given in the application form.

12.2 Application

a) The supplier shall fill the application as per document BDCS(A-I)-03-05and submit it to STQC along with the enclosures (1 copy TCF). Supplier shall submit the application fee as per schedule of charges. Certification Body will evaluate The Certification Body evaluates completeness of the application and TCF (Technical Construction File) preliminarily and if found satisfactory Certification Agreement – BDCS(A-I)-03-04, will be signed and informs the supplier to supply the devices (3-Number) to the designated test laboratories. At the same time CB inform the test laboratory for commencement of the test and also supplies the copy of application and test specifications to the laboratory.

b) Supplier shall submit three sets of Biometric devices along with capturing software and other essential accessories required for Image Quality tests along with a copy of TCF to Biometric Device Test Lab BDTL Mohali. Supplier shall fill Service Request Form (SRF) and submit the test & certification charges at BDTL-ETDC Mohali in advance by Demand draft only, drawn in favour of PAO,DIT payable at Chandigarh . BDTL shall inform the client Probable Date of Completion (PDC). A copy of SRF along with PDC and payment receipt shall be sent to Certification body by BDTL .

12.3 Commencement of Test

After receipt of payment and communication from Certification Body ,BDTL shall proceed for Testing as per Standard Test Plan. (Annexure-II)

The following test approach & methodology will be used:

a) 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 UIDAI.

b) The output of the biometric devices will be checked for compliance to relevant specification document provided by UIDAI.

c) The integration of Biometric device with the system will be tested through
1. Verification of compliance to relevant API standard published by UIDAI.
2. Carrying out end to end functional testing using relevant software/ a Test harness.

12.4 Inputs Required by STQC

Access to the followings information & facilities/ systems to undertake testing of IRIS Authentication devices will be required by STQC:

- Duly filled Application form along with the documents mentioned in the application form.
- Test and certification charges
- Technical construction file(TCF)
- Three Nos. of IRIS Authentication Device to be tested, software application, database , test samples, test software, test documentation, test processes and test targets as per ISO12233
- Test environment for testing of specialized parameters (if required)
- Internal test reports
- Arrangement to witness the testing at manufacturer facility, in case the in-house facility for the same is not available with STQC

Supplier would need to be directly providing the documentation to STQC, and as per the certification needs provide additional information/Test results if required.

12.5 Testing

Testing activity consist of the following task

a) Study & Understanding of the device design and configuration
b) Test Planning & Preparation
c) Test Execution
d) Test Report Preparation

STQC test lab will execute the testing as per Test Plan. In case of any non-compliance/failure STQC test lab shall inform to the certification body and stop the testing. The supplier should analyze the results and take corrective action, both at device level and at System Level. If corrections are required at Manufacture level (device level) supplier shall co-ordinate the same and inform to CB. The testing can be re-started if CB is satisfied with the analysis and corrective actions are satisfactory. CB and STQC test lab 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 at the time of Certification.

The supplier shall maintain analysis and corrective actions records which will be audited during surveillance visit.

The designated laboratory (STQC test lab) carries out the test as per supplied test specifications and following the prescribed test methods:

- Tests are conducted by testers as per defined test methodologies.
- Test results are logged and whenever a defect is found during test, the same recorded with details of observations.
- A Test Report is prepared that summarizes the test results including defects and anomalies according to their degree of severity as per defined criteria.
- The test report is submitted to the Certification Body, after the completion of tests.
- The inputs supplied (documents & IRIS Authentication device-reference sample) by the supplier and test reports are preserved by the test lab. (for 3-years)

After completion of the tests STQC test lab shall prepare the Test report in approved format and forward the detailed test report to Certification Body.
Policy of certification body in the event of the failure of the device.
In the event of the failure of the device the test lab should inform to the certification body. If failure is due to the software the supplier shall immediately take corrective/preventive actions and inform to the CB
(a) failure analysis and route cause analysis
(b) corrective and preventive actions
© action on change control/configuration control/version control of the software
If failure is due to the hardware, testing should be stopped, supplier should be informed and a fresh testing with double the number of samples should be done after (a) and (b) stated above are implemented. If any of the two samples fails the testing activity should be concluded failed.

12.6 Certification

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

a) Analyzing the test results
b) Verifying compliance to evaluation Criteria

Certification Committee will review the reports and other information holistically, and give its recommendation for Certification. Certification Committee can use a reference Checklist.
If there are technical deviations from the specifications which appears to after due recording. Members, advice of TAC may be obtained.

If be minor to all CC Members, they can consult UIDAI and/or Technical expert of TAC and if there is an agreement they can recommend for Certification there is difference of opinion in CC

The decision whether or not to certify a supplier's IRIS Authentication Devices will be taken by the Head (Certification Body) based on the recommendation of the Certification Committee. This will be on the basis of the information gathered during the certification process, evaluation of the test report and any other relevant information. Where necessary, the Certification Committee will seek expert's opinion to determine the technical basis for its decisions.

The Certification Body will not delegate authority for granting, maintaining, extending, reducing, suspending or withdrawing certification to an outside person or body without prior approval of Head (Certification Body) in each and every case.

Director Certificate Signing Authority (one from STQC and one from UIDAI) will issue the certificate after getting satisfied with the recommendation of certification committee. The certificate of approval covers:

a) The name and address of the manufacturer and supplier
b) The scope of the certification granted including brand and model no., standards and/or other normative documents to which IRIS Authentication Devices are certified
c) The effective date of certification and the term for which the certification is valid

Simultaneously, arrangements will be made to update the list of certified suppliers available at www.stqc.nic.in

Also note that the certification process is not intended to endorse one product over a competitor's product, but merely to certify that the product meets requirements of UIDAI project and that, between two products that meet requirements of UIDAI project, the STQC and UIDAI both does not recommend one over the other.

6.7 Deliverables

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

To ensure Certification remains valid, the supplier shall ensure that he meets the maintenance of Certification Requirements

13. Test and Certification Schedule:

- It will take about 4-6 weeks to complete the testing and certification after required inputs have been provided by the client to STQC.
- The charges for testing and certification will be as per the schedule of charges.(Annexure IV)
- The service tax @ 12.36% (or as applicable) shall be extra.

14. Mode of Payment:

Application, Testing, Surveillance ,evaluation & certification, annual Fee are paid in advance by Demand draft only, drawn in favour of “Pay & Accounts Officer, DIT, payable at Chandigarh ,at BDTL-ETDC Mohali.

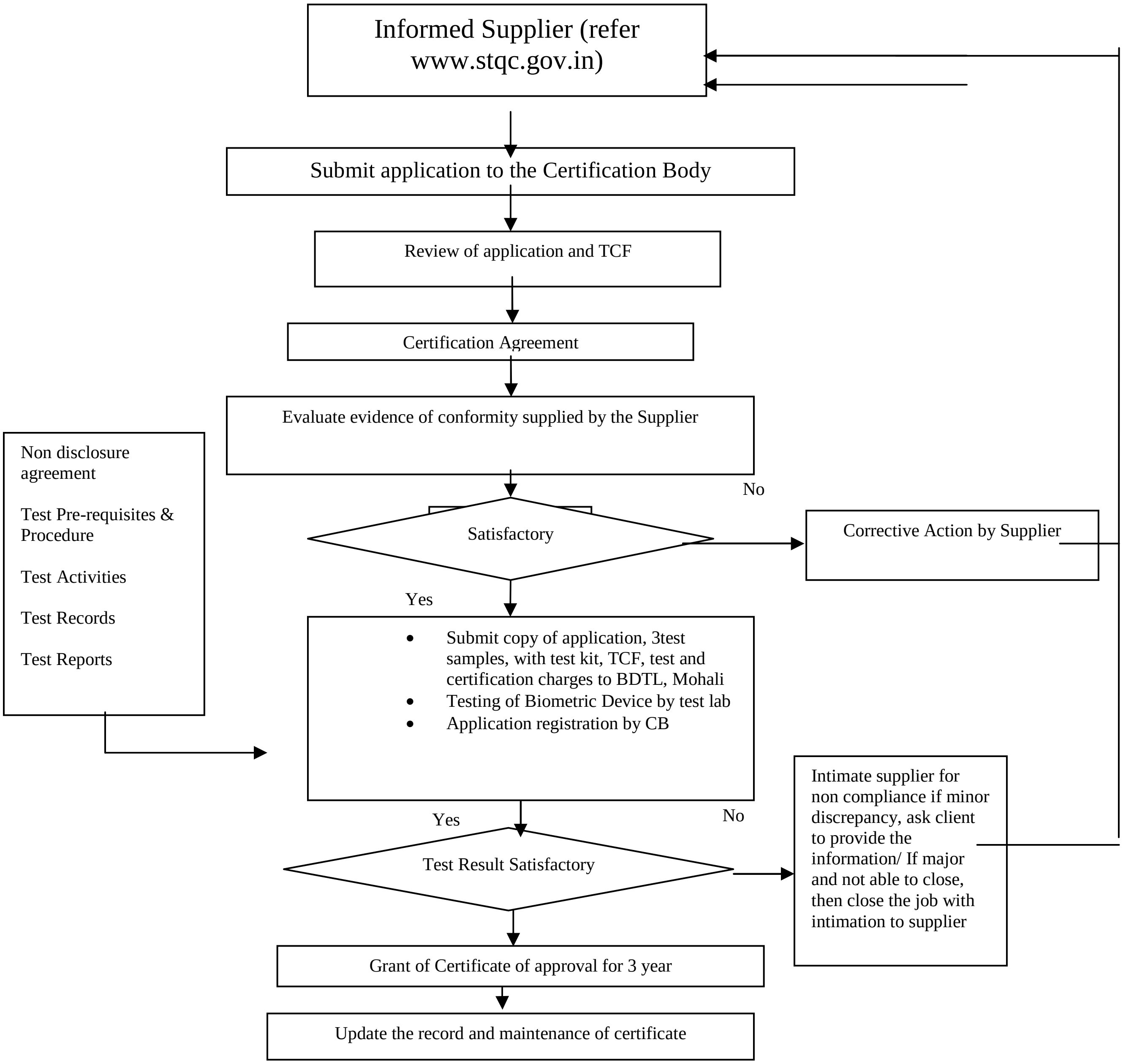
The service tax as applicable shall be paid. At present the rate is 12.36% shall be extra. The service tax No. is TMPRU 4542CST001 dated 23-04-2004.

15. Terms and Conditions:

- The payments to STQC Directorate (being Government of India organization) are exempted from TDS under section 196 of Income Tax Act.
- The client shall arrange for DUT and support environment at STQC test lab where testing will be undertaken.
- In order to complete the testing, as per schedule, client shall ensure readiness of test related documentation and timely availability of the required information.
- STQC shall ensure timely completion of test activities as per plan and submit the deliverables.

Annexure – I

Certification Process Flow Chart


Informed Supplier (refer www.stqc.gov.in)
Submit application to the Certification Body
Review of application and TCF
Certification Agreement
Evaluate evidence of conformity supplied by the Supplier
Non disclosure agreement
Test Pre-requisites & Procedure
Test Activities
Test Records
Test Reports
Satisfactory
No
Corrective Action by Supplier
Yes
• Submit copy of application, 3test samples, with test kit, TCF, test and certification charges to BDTL, Mohali
• Testing of Biometric Device by test lab
• Application registration by CB
Yes
No
Test Result Satisfactory
Intimate supplier for non compliance if minor discrepancy, ask client to provide the information/ If major and not able to close, then close the job with intimation to supplier
Grant of Certificate of approval for 3 year
Update the record and maintenance of certificate

Annexure II

(TEST PLAN SUMMARY)

(Device Sample 1)
Reference sample

Visual-Inspection
Functional Testing
Image Quality Testing
UIDAI API
ComplianceTesting
Image Quality Testing
Ergonomics

(Device Sample 2)

Visual Inspection
Functional testing
Image Quality Testing
Environmental & Durability testing
Visual Inspection
Functional testing
Image Quality testing

(Device Sample 3)

Visual Inspection
Functional Testing
Image Quality Testing
EMI/EMC Testing
*Interoperability (FRR)Testing
Visual Inspection
Functional Testing
Image Quality Testing

*FRR & Ergonomics testing can be performed at any stage after image quality testing

Annexure III

Requirements of Technical Construction File (TCF)

To create confidence in the Device Quality and to demonstrate compliance, Supplier shall maintain a technical construction file. This will require close collaborations of supplier with the manufacturer. The commercially 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 of the business of the manufacturer and supplier organisation
- Product description and reference to www…..(Provide description of the type including explanation necessary to understand the functioning of the IRIS Authentication. This may include a picture of the complete IRIS Authentication device, a description of its main components.) An additional Brochure of the chip used to ensure progressive scanning should also be provided
- IRIS Authentication Specification (may be in the form of brochure)
- Summary of Quality Control System of supplier covering following -
    - Management functions Document control/Changes to documents, Internal audit, Management review (reference of the procedure)
    - Procedure on event logging/ consolidation/Grouping e.g. organizing events based on device models, sites/installations, business processes/units, departments/ organizations/ geographic regions.

-Procedure on Corrective actions capability of setting/changing a parameter or triggering an action in the monitored device. Availability of maintenance facility – list of maintenance equipments/tools available.

- Inventory policy
- Procedure on Supply & Distribution. Record format of biometric Installations covering
    - address,
    - contact list for each organization,
    - installation type and location,
    - Device model
    - type,
    - serial number,

- Procedure on Configuration/customization Shall be able to demonstrate configuration control over various device sensor/software versions of API/DLL

- Internal test report on API/DLL compliance as per the latest API specifications released by UIDAI.
- Declaration by supplier organization regarding continues compliance on Updates, maintenance, and support as per latest APIs released by UIDAI and same are made available to the Authentication Agencies
- Procedure on training imparted to user agencies and employees of supplier organization. List of trained employees within office
- Contract agreement of supplier organization with manufacturer to provide all the relevant details, which are not commercially confidential in nature to enable him to obtain the certification and maintenance support for the devices sold in the market.
- Procedure on Exit management, for the extreme condition that the vendor decides to close the biometric business.

- List of Applicable Regulations/Standards
- Risk Assessment and/or recommended practice for the use of device

(Guidance in this regard is given below)

Severe Risk Environment

Severe risk levels imply that loss of life and/or property can result if accurate identification or verification is not made. In severe risk environments, it is plausible that inconvenience to the subject being identified or verified is secondary to the security of the situation, meaning subjects may be detained longer until the identification or verification process is completed. This assumption means that matching thresholds can be set lower (more aggressively) resulting in a returned list of potential candidates.

Moderate Risk Environments

A moderate risk environment is defined for those encounters with a subject with no or questionable identification. An officer cannot detain a subject for more than a limited amount of time without making an arrest. In this situation, it is necessary to quickly identify the subject or retain biometric information sufficient to verify the subject's identity at a later date.

Mild Risk Environments

A mild risk environment is defined for those encounters where enrollment and identification data will be used at a later date. At that time the subject would be available for comparison to the data previously retained. The results of an identification or verification should not impact anyone but the subject in question. Examples of mild enrollments include preparing for future logical or physical access control for a subject, or retaining one or more biometric images for verification in court while the subject is available. Verification examples include tracking a subject through the jail or court system using the retained biometric images. In these cases a failure to match would result in additional action to verify the subject's identity, primarily inconveniencing no one but the subject.

Certificates

- Certificate for ISO 9001:2008 (Certification for IRIS Authentication Device, Design and Development, Manufacturing and Service (Manufacturer)
- Certificate for ISO 9001:2008(Certification for IRIS Authentication Device Supply and Distribution, Training, Maintenance, and Service (Supplier/Distributor))
- Certificate of Incorporation in India (Supplier)
- IECEE-CB Certificate (IEC 62471) for eye safety, and/or with CB Test Report from recognized CTL or equivalent dual certification.
- Manufacturer authorization to supplier to place devices in Indian market. MOU to be signed between manufacturer and supplier and copy of same to be made available to certification body.

Declaration of Conformities

- Declaration to compliance with RoHS and WEEE requirements
- Declaration that supplier has a plan to make provision and comply with the notification of Government of India, Ministry of Environment and Forest regarding collection and disposal of IRIS Authentication devices/equipment at end of life applicable from May 2012.

Test Reports

- Functional Test Report
- Test report for Imaging wavelength, Spectral Spread
- USB-IF test report
- Performance Test Report in operational environment (FRR)
- EMI/EMC compliance test report
- Eye safety Compliance Test Report
- Environment/Durability compliance test report

Note: These test reports can be from any accredited test laboratory.

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
- Schematic diagram
- User manual

ABBREVIATIONS:
CB –Certification Body
BDTL- Biometric Device Test Lab
RFP- Request for proposal
UIDAI- Unique Identification Authority of India

DUT-Device under test