

**Procedure for obtaining  
Biometric Device Certification  
- Authentication/Enrolment  
(STQC/BDCS/P10)**

Issue: 01



Biometric Device Certification Scheme (BDCS)  
STQC Directorate,  
Ministry of Electronics & Information Technology (MeitY)  
Government of India



# Biometric Device Certification Scheme

P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment


Issue : 1

Date : 04-01-2021

Page : 1 of 25

## Contents

0.1	Approval and Issue.....	2
0.2	Amendment Record .....	3
1.	Background.....	4
2.	Purpose.....	4
3.	Reference Documents.....	4
4.	Target Audience.....	4
5.	Certification Context .....	4
6.	Objectives of Testing and Certification.....	5
7.	Scope of Certification.....	6
8.	Procedure.....	6
8.1.	Pre-requisite for Certification .....	6
8.2.	Application.....	6
8.3.	Inputs Required by STQC.....	6
8.4.	Commencement of Test .....	8
8.5.	Test Approach and Methodology.....	8
8.6.	Testing activities .....	8
8.7.	KEY FEATURES OF TESTING .....	9
8.8.	Certification .....	9
	Provisional Certificate .....	9
8.9.	Deliverables .....	10
9.	Test and Certification Schedule .....	10
10.	Mode of Payment.....	10
11.	ABBREVIATIONS.....	11
Annexure I	: Requirements for Technical Construction File (TCF) for Biometric Devices .....	12
1.	Authentication Device - Fingerprint Scanner.....	12
2.	Authentication Device - IRIS Scanner.....	14
3.	Enrolment Devices .....	17
Annexure-II	Test Plan (Authentication Devices - L0 and L1) .....	18
Annexure III	Certification Process Flow Chart for Authentication Device .....	20
Annexure-IV	Test Plan (Enrolment Devices).....	22
Annexure V	Certification Process Flow Chart for Enrolment Device.....	23

 STQC ॥ गुणोत्कर्षं समृद्धिः ॥	<b>Biometric Device Certification Scheme</b>	
	P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment	Issue : 1
		Date : 04-01-2021
	Page : 2 of 25	

## 0.1 Approval and Issue

This document is the property of Biometric Device Certification Scheme (BDCS) and should not be reproduced in part or full without the written consent.


**Reviewed by : Management Representative**

**Approved by : Head, BDCS**

### Note:

- Management Representative (MR) is responsible for issue and distribution of this document including amendments.
- Holder of this copy is responsible for incorporation of all the amendments and currency of the document.



	<b>Biometric Device Certification Scheme</b>	
	P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment	Issue : 1
		Date : 04-01-2021
		Page : 4 of 25

## 1. Background

Biometric Device Certification Scheme (BDCS) is operated by STQC Directorate, Ministry of Electronics and Information Technology (MeitY), Govt. of India. Under supervision of CB, the Testing Laboratories or Biometric Device Test laboratory (henceforth will be referred as BDTL) perform Testing of Biometric Device products against the requirements of UIDAI.

## 2. Purpose

Purpose of this document is to describe the Procedure for obtaining the certification of Biometric Devices including:-

- Enrolment Devices
- Authentication Devices
  - Fingerprint Scanner (Discrete)
  - IRIS Scanner (Discrete/Integrated)

## 3. Reference Documents

STQC/BDCS/D01	:	Rules and Procedures
STQC/BDCS/D08	:	Specifications
STQC/BDCS/F01	:	Application
ISO 19794-4	:	Information technology – Biometric data interchange formats – part 4: Finger Image data
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

Aadhaar Registered Devices – Technical specification, latest version

L1 traceability matrix document

Note:

Latest edition of above-mentioned standards to be referred.


*Please refer **Master List of Documents** for latest version of the documents*

## 4. Target Audience

The Supplier of authentication devices, Biometric Device Test Laboratory (BDTL) and the Certification body shall follow this procedure for certification.

## 5. 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

	<b>Biometric Device Certification Scheme</b>	
	P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment	Issue : 1
		Date : 04-01-2021
		Page : 5 of 25

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 qualities of authentication devices are 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/Kind7Generator) in their application

*Biometric Authentication device Certification is required to*


- Maintain quality of 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 Authentication devices vis-à-vis available industry standards
- Ensure service levels and support availability
- Ensure secure and transparent authentication

## 6. 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 UIDAI for UID applications.

The objectives are to verify:

1. The extent to which requirements prescribed in the relevant UIDAI specifications have been fulfilled.
2. The extent to which applicable regulations, standards and specifications set out in the applicable Quality specifications are met;
3. Provide opportunity for Vendors to understand defects/ non-conformance and rectification of the same.
4. To grant certification and provide assurance to users of devices that the certified product meets UIDAI requirements comprehensively

	<b>Biometric Device Certification Scheme</b>	
	P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment	Issue : 1
		Date : 04-01-2021
		Page : 6 of 25

## 7. Scope of Certification

The scope includes Scope of certification covers various type (Form factor) of Biometric Authentication/Enrolment Devices for UIDAI Aadhaar Ecosystem.

## 8. Procedure

### 8.1. Pre-requisite for Certification

- Supplier shall understand the Certification and Surveillance requirements, applicable charges etc. before applying to Certification Body (STQC).
- Supplier shall prepare a technical construction file (TCF). The clarity in TCF provides confidence to the Certification Body regarding Quality of Device. The requirements of TCF are given in Annexure -I.

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.

### 8.2. Application

- The supplier shall fill the application and 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 TCF (Technical Construction File) preliminarily and if found satisfactorily Certification Agreement will be signed.
- Supplier shall submit three sets of Biometric devices, Test kit for Image Quality along with a copy of TCF to Biometric Device Test Lab of STQC. Supplier shall fill Service Request Form (SRF) and submit the test charges. BDTL shall inform the supplier/vendor about Probable Date of Completion (PDC).
- In case of L1 registered biometrics device, the supplier shall ensure compliance for “clauses applicable to devices” as per L1 traceability matrix document and Aadhaar Registered Devices – Technical specifications (available on <http://stqc.gov.in/content/biometric-devices-testing-and-certification> and [www.uidai.gov.in](http://www.uidai.gov.in) website).

### 8.3. Inputs Required by STQC

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

- ~~UIDAI Requirements – Biometric device specifications compliance, API compliance documentation~~



## Biometric Device Certification Scheme

P10 –Procedure for obtaining Biometric Device Certification –Authentication/Enrolment

Issue : 1

Date : 04-01-2021

Page : 7 of 25

- UIDAI Requirements – Biometric device specifications compliance, Authentication API compliance documentation, Register Device specification compliance
- Device Documentation – Biometric device specifications brochure, Design Document, User/Operations Manual, SDK Documentation
- Technical construction file (TCF)
- Fingerprint Scanner Devices (04 No. for L1 Device and 03 No. for L0 Device) to be tested with applicable SDK, software application.
- 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
- 03 Nos. of Biometric Enrolment Devices along with SDK, API and driver software etc.
- Test environment for testing of specialized parameters (if required)
- Internal test reports of vendor
- Demonstration of devices with applicable software applications
- Compliance with L1 traceability matrix document (For L1 Device only).
- Arrangement to witness the testing at vendor’s facility, in case the in-house facility for the same is not available with STQC
- Image Quality Test Kit consisting of
  - Image capture device software
  - Image Analysis software
  - Applicable Test targets and associated jig/fixtures
  - Support tools and test procedure document

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


### • Scope of Certification

The applicant shall refine the scope of certification based on UIDAI specification and requirements, AUA’s requirement and other market needs considering the following.

Sensor extractor/kind7generator combination is certified for a specified device (Say D) at first. Once this sensor extractor combination is validated for image quality for UID 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”-

- OEM sensor extractor certified by STQC earlier for device D for UID authentication.
- OEM authorization if use of sensor extractor in the proposed device.
- Compliance with other applicable specifications as per the “intended application”
  - Example: portability in case of mobile biometric devices.
- Environmental and robustness specification as per the “intended application”
  - Example: (Operating Temp, Humidity, Drop\*, Vibration, IP)
- Functional test as per the “intended application” workflow



	<b>Biometric Device Certification Scheme</b>	
	P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment	Issue : 1
		Date : 04-01-2021
		Page : 8 of 25

#### 8.4. Commencement of Test

Certification Body (STQC) will inform the concerned testing laboratory to proceed for Testing as per Standard Test Plan. (Annexure-II)

#### 8.5. Test Approach and Methodology

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
  - i. Verification of compliance to relevant applicable API standard published by UIDAI.
  - ii. Carrying out
    1. End to end functional testing using relevant applicable software/ Test harness.
    2. Repeat functional testing for consistency of operations.

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

- Testing may be conducted in the STQC laboratory.
- External test laboratory/ client’s test facility may be used to conduct the testing (where test facilities are not available with STQC).
- Compliance may be verified by demonstration(s) of testing using client’s test facilities (where test facilities are not available with STQC).
- Compliance may be verified based on the test reports &/or certifications obtained by the client.

#### 8.6. Testing activities

Testing activity consist of the following task

	<b>Biometric Device Certification Scheme</b>	
	P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment	Issue : 1
		Date : 04-01-2021
	Page : 9 of 25	

- a. Study & Understanding of TCF documents, test reports and certifications etc.
- b. Test Planning
- c. Test Execution
- d. Test Report Preparation
- e. Release of test results/ reports for certification

## 8.7. KEY FEATURES OF TESTING

STQC lab/centres shall conduct test for Biometric Authentication/Enrolment device to verify the compliance with applicable specifications as per BDCS Scheme document “STQC/BDCS/D08-Specification”.

BDTL will execute the testing as per Test Plan. In case of any non-compliance/failure BDTL shall inform to the supplier 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/Principal Level, supplier 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 CC at the time of Certification.

The supplier 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.

## 8.8. Certification

Certification body will internally check the compliance with respect to Rules and Procedures of the scheme (STQC/BDCS/D01) 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 prepared by CB.

### Provisional Certificate

After Successful testing of biometric devices at STQC Lab or at its premises, suppliers may be given provisional certification as per procedure detailed below

- a) Instead of FRR testing, STQC will perform authentication functional test on limited subject/small sample (approx. 100) with maximum 2 failure allowed in fingerprint device and 1 failure allowed in Iris devices with same subjects. This test is to be conducted only when device is available from at least 3-5 different vendors.

	<b>Biometric Device Certification Scheme</b>	
	P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment	Issue : 1
		Date : 04-01-2021
		Page : 10 of 25

- b) Validity of the Provisional Certificate will be till Field FRR test is conducted or one year, whichever is earlier.
- c) Maximum three attempts will be permissible with each Aadhaar holder including Fail to Capture (FTC) cases.
- d) STQC will record Aadhaar number (as per applicable policy of UIDAI), Auth code, status, error code, time stamp for each transaction.
- e) Device vendor will be responsible for Authentication application development/deployment, AUA/ASA connectivity for internal FRR testing.
- f) All the other Lab tests and certification requirements (other than Field FRR test) are mandatory for Provisional Certificate.
- g) STQC will issue final Certificate after conducting Field FRR test with 5000+ test subjects.
- h) In case, any device gets failed in final field FRR testing, vendor will have to rollback all the devices deployed in the field. The related cost and loss will be borne by the concerned device vendor.

After the provisional certificate, the supplier will be eligible for empanelment. The supplier details along with status, scope and validity of certification will be published on STQC website.

### 8.9. Deliverables

On satisfactory completing all above activities and fulfilment of certification & Evaluation Criteria, CB will issue the certificate to the supplier.

BDTL is responsible for storage and maintenance of the devices and other vendor (supplier's) products (Test fixture, supplied Test Methods, Software, and Documentation etc.).

## 9. 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 and BDTL.
- The charges for testing and certification per Biometric Device will be as per applicable Guidelines of STQC schedule of charges.
- The GST shall be extra as applicable.


## 10. Mode of Payment

### Application, Certification and Testing Fee

Applicable charges are required to be paid in advance through BharatKosh ([bharatkosh.gov.in](http://bharatkosh.gov.in)) only in favour of concerned laboratory.

### Terms and Conditions


- The payments to STQC Directorate (being Government of India organization) are exempted from TDS under section 196 of Income Tax Act.

	<b>Biometric Device Certification Scheme</b>	
	P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment	Issue : 1
		Date : 04-01-2021
	Page : 11 of 25	

- The vendor 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, vendor 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.

## 11. ABBREVIATIONS

BDTL	- Biometric Device Test Lab
BDCS	- Biometric Device Certification Scheme
CB	- Certification Body
CC	- Certification Committee
DUT	-Device under test
FPS	- Fingerprint Scanner
L1 Device	- Biometric Device manufactured using Pre-Certified Hardware (PCH)
RFP	- Request for proposal
STQC	- Standardization Testing Quality and Certification Directorate
UIDAI	- Unique Identification Authority of India

	<b>Biometric Device Certification Scheme</b>	
	P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment	Issue : 1
		Date : 04-01-2021
	Page : 12 of 25	

## **Annexure I : Requirements for Technical Construction File (TCF) for Biometric Devices**

### **1. Authentication Device - Fingerprint Scanner**

To create confidence in the Device Quality, Supplier shall maintain a technical construction file. This will require close collaborations of supplier 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 (Scope should cover Biometric Device Development, Manufacturing and Service (Manufacturer))
- Certificate for ISO 9001 (Scope should cover Biometric Device Supply and Distribution, Training, Maintenance, Calibration and Services (Supplier/Distributor))
- Certificate of Incorporation in India (Supplier)
- MINEX III Certificate for extractor
- IECEE-CB Certificate (IEC 60950) for safety, enclosed with CB Test Report from recognized CTL or equivalent dual certification.
- Manufacturer authorization to supplier to place devices in Indian market

#### **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 devices/equipment at end of life applicable from March 2016 or later with relevant documents.

#### **Test Report**

- Image Quality, Test Procedure and Test Report as applicable
- EMI/EMC compliance test report
- Safety Compliance Test Report
- UIDAI API Specification Compliance / RD Test Report
- Environment/Durability compliance test report
- Performance test report of UIDAI requirements with technical rationale.
- Minex III Compliance test report for extractor


 STQC ॥ गुणोत्कर्षं समृद्धिः ॥	<b>Biometric Device Certification Scheme</b>	
	P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment	Issue : 1
		Date : 04-01-2021
	Page : 13 of 25	

**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

	<b>Biometric Device Certification Scheme</b>	
	P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment	Issue : 1
		Date : 04-01-2021
		Page : 14 of 25

## 2. Authentication Device - IRIS Scanner

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 organization
- 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



## Biometric Device Certification Scheme

P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment

Issue : 1

Date : 04-01-2021

Page : 15 of 25

- 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.

- 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.





## Biometric Device Certification Scheme

P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment

Issue : 1

Date : 04-01-2021

Page : 16 of 25

### 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 March 2016 or later with relevant documents

### 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

	<b>Biometric Device Certification Scheme</b>	
	P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment	Issue : 1
		Date : 04-01-2021
	Page : 17 of 25	

### 3. Enrolment Devices

Technical Construction File to be submitted along with the Biometric Device:

1. Documents and other inputs required for Test and Evaluation:
  - Device Documentation – Biometric Device Specifications, Design Document , User/ Operations Manual, SDK Documentation
  - Certificate for ISO 9001:2008 Certification for Biometric Device Development, Manufacturing and Service facility (Manufacturer)
  - Certificate for ISO 9001:2008 Certification for Biometric Device Supply, Training, Calibration and Maintenance etc facility (Supplier/Distributor)
  - Certificate of Incorporation in India (Supplier)
  - FBI Certificate for Image Quality of Biometric Device (Appendix F) along with Test Report
  - UL/ ANSI RP/ IEC 60825-1/ RoHS Certificate for Safety of Biometric Device along with Test Report
  - WHQL Certificate for Device Driver along with Test Report
  - Compliance Certificate for FCC Class A and Environmental Parameters along with Test Report
  - Calibration Compliance Certificate of Biometric Device
  - Manufacturers authorization (Supplier)
2. The certificate ISO 9001:2008 should clearly cover the scope of Supplier/ manufacturing organization of Biometric Device.
3. 03 Nos. of Biometric Enrolment Devices along with SDK, API and driver software etc.
4. The Test samples along with a copy of application & documents to be submitted to the assigned STQC test laboratory:

NOTE:

- All pages of the application, device documents (Biometric Device Specifications, Design Document, User/ Operations Manual, SDK Documentation etc) and all attached documents submitted by the applicant should be properly stamped and signed.
- The application should be clearly hand written or preferably typed written so as to make clearly readable.



## Biometric Device Certification Scheme

P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment

Issue : 1

Date : 04-01-2021

Page : 18 of 25

### Annexure-II Test Plan (Authentication Devices - L0 and L1)

#### Test Plan (Authentication Device - L0)

<b>(Device Sample 1)</b> Reference Sample	<b>(Device Sample 2)</b>	<b>(Device Sample 3)</b>
<ul style="list-style-type: none"> <li>- Visual-Inspection</li> <li>- Physical &amp; Dimension Testing</li> <li>- Functional Testing</li> <li>- Image Quality Testing</li> <li>- NFIQ compliance testing</li> <li>- Interoperability Testing</li> <li>- UIDAI API / RD Service Compliance Testing</li> <li>- Image Quality Testing</li> </ul> <p><i>(To be retained as Reference Device)</i></p>	<ul style="list-style-type: none"> <li>- Visual Inspection</li> <li>- Physical &amp; Dimension Testing</li> <li>- Functional Testing</li> <li>- Image Quality Testing</li> <li>- NFIQ compliance testing</li> <li>- Environmental &amp; Durability testing</li> <li>- Image Quality Testing</li> </ul>	<ul style="list-style-type: none"> <li>- Visual Inspection</li> <li>- Physical &amp; Dimension Testing</li> <li>- Functional Testing</li> <li>- Image Quality Testing</li> <li>- NFIQ compliance testing</li> <li>- Performance Testing</li> <li>- ESD Testing</li> <li>- EMI/EMC Testing</li> </ul>

Total no. of devices required For L0 Device: Three



## Biometric Device Certification Scheme

P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment

Issue : 1

Date : 04-01-2021

Page : 19 of 25

### Test Plan (Authentication Device - L1)

(Device Sample 1) Reference Sample	(Device Sample 2)	(Device Sample 3)	(Device Sample 4)
<ul style="list-style-type: none"> <li>- Visual-Inspection</li> <li>- Physical &amp; Dimension Testing</li> <li>- Functional Testing</li> <li>- Interoperability Testing</li> <li>- Image Quality Testing</li> </ul>	<ul style="list-style-type: none"> <li>- Visual Inspection</li> <li>- Physical &amp; Dimension Testing</li> <li>- Functional Testing</li> <li>- Environmental &amp; Durability testing</li> <li>- Image Quality Testing</li> </ul>	<ul style="list-style-type: none"> <li>- Visual Inspection</li> <li>- Physical &amp; Dimension Testing</li> <li>- Functional Testing</li> <li>- Performance Testing</li> <li>- ESD Testing</li> <li>- EMI/EMC Testing</li> </ul>	<ul style="list-style-type: none"> <li>- Visual Inspection</li> <li>- Physical &amp; Dimension Testing</li> <li>- UIDAI API / RD Service Compliance Testing</li> </ul> <p><b>(For L1 Device Only JTAG will be disabled and it shall be Production device)</b></p>

Total no. of devices required for L1 Device: Four

For L1 device: 4th Device will be production device and will be used for RD service testing.

For RD service certification, Vendor need to submit separate duly filled application along with Registered Device solution architecture & TCF as per clauses applicable to Device vendor under L1 traceability compliance matrix document.



# Biometric Device Certification Scheme

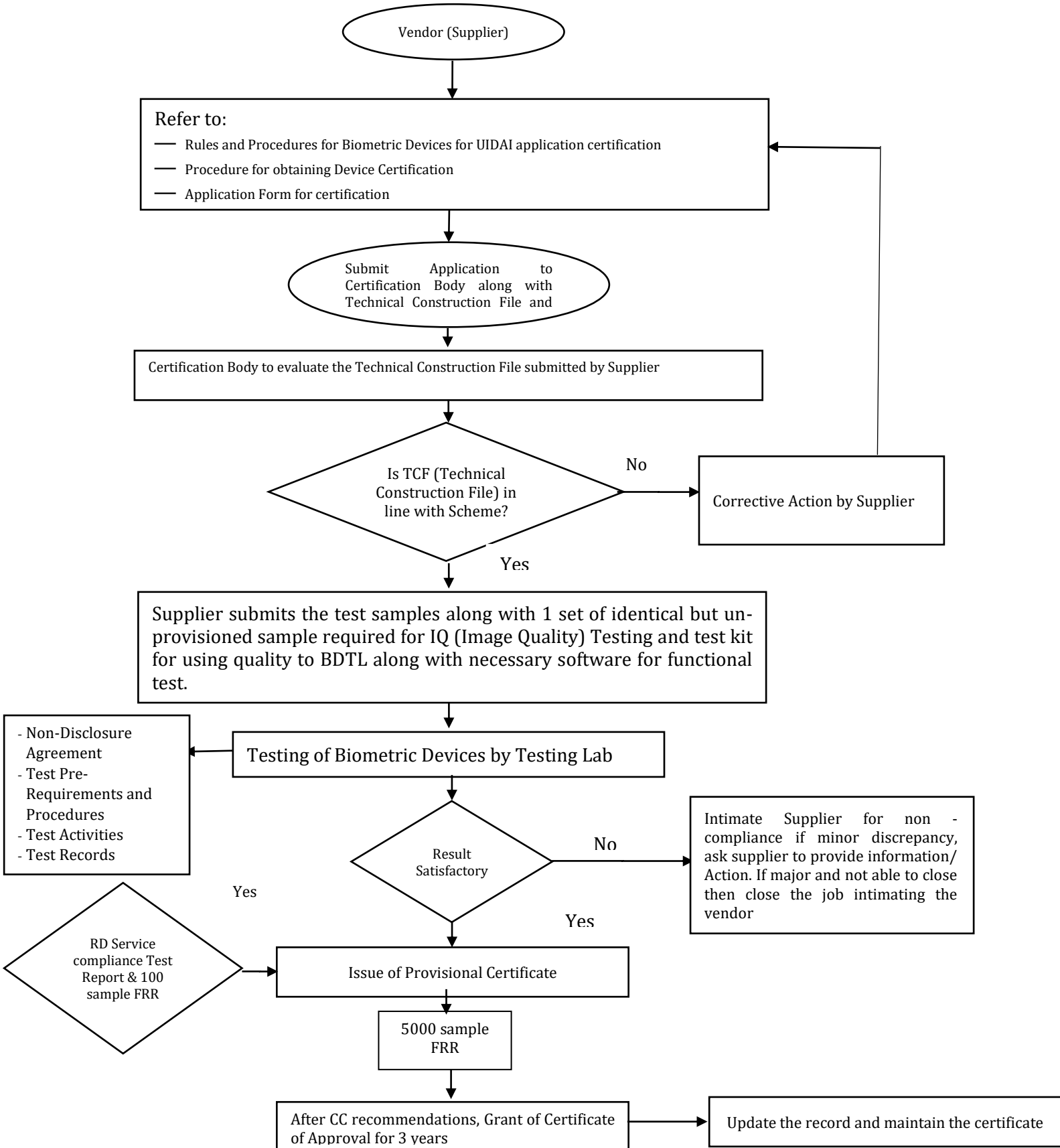
P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment


Issue : 1

Date : 04-01-2021

Page : 20 of 25

## Annexure III Certification Process Flow Chart for Authentication Device



	<b>Biometric Device Certification Scheme</b>	
	P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment	Issue : 1
		Date : 04-01-2021
	Page : 21 of 25	

#### Steps to get certification of Biometrics Devices used for UIDAI applications

1. The vendor (supplier) of the biometric device to study the scheme published at <http://stqc.gov.in/content/bio-metric-devices-testing-and-certification>.
2. Contact certification body (CB) at STQC HQ and Submit Application to Certification Body along with Technical Construction File and Certification Agreement
3. CB to evaluate the TCF submitted by vendor as per Biometric Device Certification Scheme.
4. If TCF is in line, the CB will accept the application and allocate the application reference number to be communicated to BDTL and vendor
5. On acceptance of application, the supplier will submit the devices along-with a copy of TCF and other pre-requisite software, test target etc. to BDTL, open service request form (SRF) and pay the requisite fee through BhraatKosh in favour of concerned BDTL Lab.
6. For L1 - Supplier shall submit the test samples along with 1 set of identical but un-provisioned sample required for IQ (Image Quality) Testing
7. Supplier to submit following document to CB
  - a) Certification Agreement
  - b) Test pre-requirements and procedure
  - c) Test Activities
  - d) Test Records
  - e) Test Reports
8. On receipt of reference application number and filling the SRF, BDTL starts testing of the device and on completion forward two copies of test reports to CB.
9. CB will evaluate the test result and put up the test results along with TCF to Certification Committee. On successful compliance, the Certification Committee recommends for certification of the device.
10. On completion of physical test and IQT test, 1 device forwarded to UIDAI tech centre Bangalore for RD Testing. On completion test results of RD service will be shared with CB by UIDAI HQ. CB will share the RD test reports with BDTL.
11. On successful completion of RD testing, Device testing and 100 sample FRR, the supplier may grant a provisional certificate of the biometric device.
12. The supplier must go for FRR testing using 5000 subjects on the device and after successful result of the FRR for the device, the final certificate may be granted for 3 years from original date of certification.
13. CB will update the record and maintain the certificate.



## Biometric Device Certification Scheme

P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment

Issue : 1

Date : 04-01-2021

Page : 22 of 25

### Annexure-IV Test Plan (Enrolment Devices)

#### Test Plan

<b>(Device Sample 1)</b> Reference Sample	<b>(Device Sample 2)</b>	<b>(Device Sample 3)</b>
<ul style="list-style-type: none"> <li>- Visual-Inspection</li> <li>- Physical &amp; Dimension Testing</li> <li>- Functional Testing</li> <li>- Image Quality Testing</li> <li>- NFIQ compliance testing</li> <li>- Interoperability Testing</li> <li>- UIDAI API / VDM testing</li> <li>- Image Quality Testing</li> </ul> <p><i>(To be retained as Reference Device)</i></p>	<ul style="list-style-type: none"> <li>- Visual Inspection</li> <li>- Physical &amp; Dimension Testing</li> <li>- Functional Testing</li> <li>- Image Quality Testing</li> <li>- NFIQ compliance testing</li> <li>- Environmental &amp; Durability testing</li> <li>- Image Quality Testing</li> </ul>	<ul style="list-style-type: none"> <li>- Visual Inspection</li> <li>- Physical &amp; Dimension Testing</li> <li>- Functional Testing</li> <li>- Image Quality Testing</li> <li>- NFIQ compliance testing</li> <li>- Performance Testing</li> <li>- ESD Testing</li> <li>- EMI/EMC Testing</li> </ul>

Total no. of devices required : Three



# Biometric Device Certification Scheme

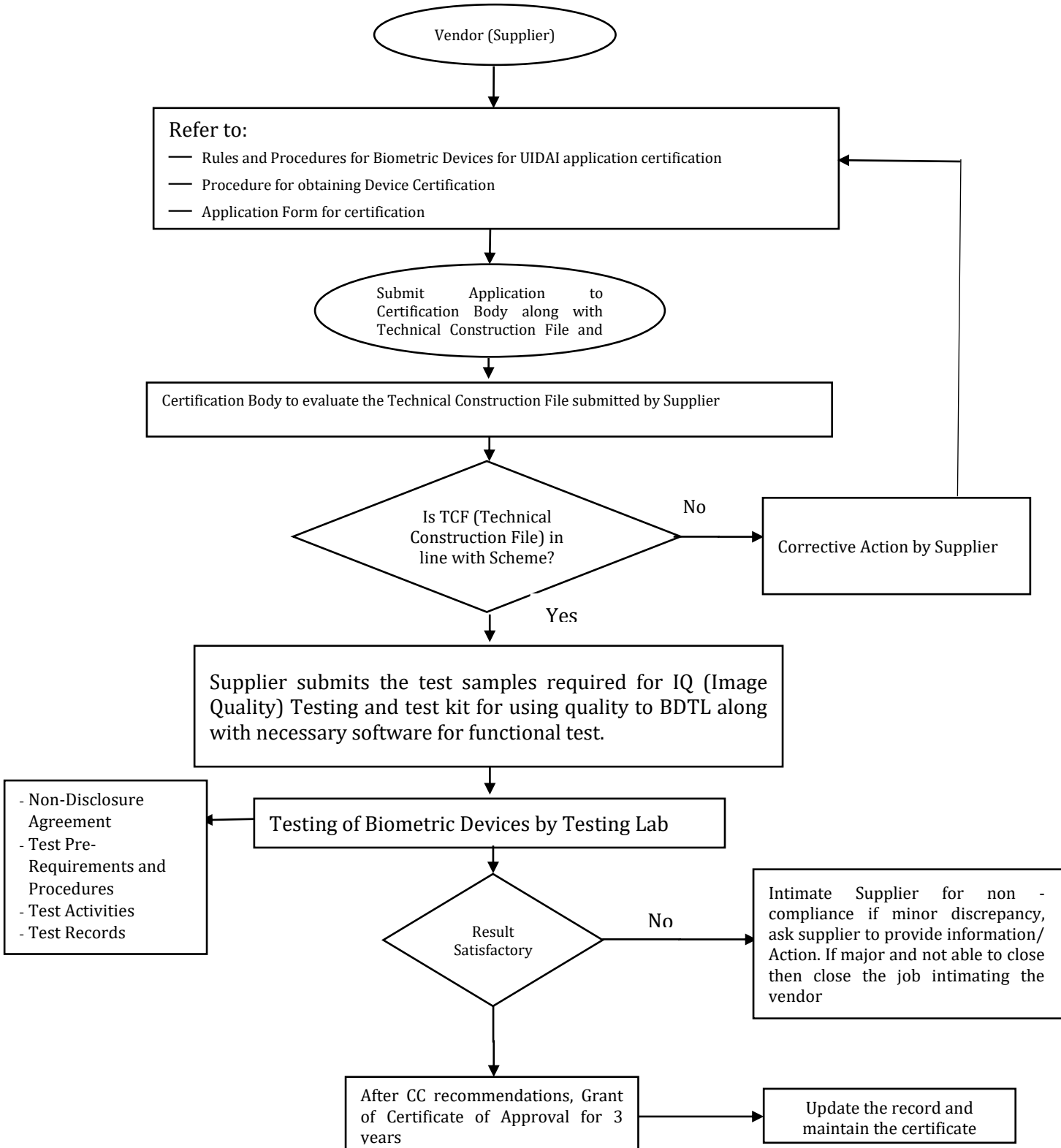
P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment

Issue : 1


Date : 04-01-2021

Page : 23 of 25

## Annexure V Certification Process Flow Chart for Enrolment Device





	<b>Biometric Device Certification Scheme</b>	
	P10 –Procedure for obtaining Biometric Device Certification –Authentication/ Enrolment	Issue : 1
		Date : 04-01-2021
	Page : 24 of 25	

#### Steps to get certification of Biometrics Devices used for UIDAI applications

1. The vendor (supplier) of the biometric device to study the scheme published at <http://stqc.gov.in/content/bio-metric-devices-testing-and-certification>.
2. Contact certification body (CB) at STQC HQ and Submit Application to Certification Body along with Technical Construction File and Certification Agreement
3. CB to evaluate the TCF submitted by vendor as per Biometric Device Certification Scheme.
4. If TCF is in line, the CB will accept the application and allocate the application reference number to be communicated to BDTL and vendor
5. On acceptance of application, the supplier will submit the devices along-with a copy of TCF and other pre-requisite software, test target etc. to BDTL, open service request form (SRF) and pay the requisite fee through BhratKosh in favour of concerned BDTL Lab.
6. Supplier to submit following document to CB
  - f) Certification Agreement
  - g) Test pre-requirements and procedure
  - h) Test Activities
  - i) Test Records
  - j) Test Reports
7. On receipt of reference application number and filling the SRF, BDTL starts testing of the device and on completion forward two copies of test reports to CB.
8. CB will evaluate the test result and put up the test results along with TCF to Certification Committee. On successful compliance, the Certification Committee recommends for certification of the device.
9. Final certificate may be granted for 3 years from original date of certification.
10. CB will update the record and maintain the certificate.

\*\*\*\*\*