Testing Methodologies for Certification of Aadhaar Authentication Devices (Fingerprint)
Table of Contents

1. Executive Summary ........................................................................................................... 3
2. Acronyms and Terms .......................................................................................................... 4
3. Introduction ......................................................................................................................... 5
   3.1. SCOPE ........................................................................................................................... 5
   3.2. PURPOSE ....................................................................................................................... 5
   3.3. OBJECTIVES ................................................................................................................ 5
4. Biometric Products Solicitation for Certification .............................................................. 6
5. Protecting the Privacy of the Volunteer Test Population ................................................ 6
6. Field FRR Testing Methodology ........................................................................................ 7
   6.1. TEST ENVIRONMENT .................................................................................................. 7
      6.1.1. Human Test Population .......................................................................................... 7
      6.1.2. Gatekeeper Client ................................................................................................. 8
      6.1.3. BFD Client ............................................................................................................. 8
      6.1.4. Authentication Station Setup ............................................................................... 9
      6.1.5. UIDAI/ASA Aggregator Network (C-DAC as AUA/ASA) .................................... 10
      6.1.6. UIDAI’s Authentication Server .............................................................................. 10
   6.2. FIELD TESTING STEPS ............................................................................................ 11
   6.3. EXPECTED DATA ANALYSIS .................................................................................... 11
7. Key Roles and Responsibilities .......................................................................................... 13
   7.1. STQC ............................................................................................................................ 13
   7.2. C-DAC .......................................................................................................................... 13
      7.2.1. Biometrics Team .................................................................................................... 13
      7.2.2. AUA/ASA Team .................................................................................................... 13
   7.3. DEVICE SUPPLIERS ................................................................................................... 13
8. High-level Milestones and Timeline (tentative) ............................................................... 14
9. References ......................................................................................................................... 15
10. Annexures ......................................................................................................................... 16
    ANNEXURE A. AUTHENTICATION REQUEST AND RESPONSE DATA FORMATS* ............. 16
    ANNEXURE B. HUMAN FACTORS & USABILITY INTERACTION ON FINGERPRINT QUALITY ......................... 18
    ANNEXURE C. TERMS AND CONDITIONS FOR SUPPLIERS .................................................. 19
    ANNEXURE D. FRR CALCULATION: PROCESS FLOW ............................................................................. 20
    ANNEXURE E. GUIDELINES FOR FTA (FAILURE TO ACQUIRE) INDICATORS .............................................. 22
    ANNEXURE F. AADHAAR NUMBERS BY SUPPLIERS FOR TESTING PURPOSE ........................................ 23
    ANNEXURE G. RESIDENT MOVEMENT: PROCESS FLOW ............................................................................. 24
1. Executive Summary

Aadhaar authentication is an online, cost effective, secure and portable authentication service. The Aadhaar authentication service delivery agencies should essentially be given confidence about the biometric authentication products that they are reliable and meet the technical specifications of UIDAI.

As part of the authentication biometric devices testing and certification procedure, all devices (sensor-extractor-supplier combination) need to prove acceptable FRR under field conditions. Such tests are to be carried out under STQC supervision, and in the test setup created by STQC. The STQC has partnered with C-DAC to carry out this test. This document details the testing procedure and methodology to be adopted for carrying out this test.

The STQC will take measures to ensure that all interested suppliers will have fair and equal opportunity to participate in the test. All products will be tested on a live authentication setup using the same human test population (having Aadhaar numbers) over a period of two-three weeks. The tests will only include genuine comparisons to determine False Reject Rates (FRRs) for each product from golden supplier* in India. Final certification by STQC would be subject to "sensor-extractor-supplier" meeting the performance objectives stated in the published STQC's biometric device specification document [STQC, UIDAI Biometric Device Specifications, 2012].

* Under the Golden Supplier Scheme, the OEMs shall appoint their respective golden suppliers in India who will be responsible for interacting with STQC for the purpose of certification.

The term golden supplier, defined as follows, has no business connotation and the term will only be used for operation convenience:

1. OEM can have their own models for multiple authorized suppliers.
2. 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 prospective. OEM can treat him as a preferential supplier as per his own internal policy.
3. 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, the different suppliers need not get the product tested again and again.
### 2. Acronyms and Terms

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>ASA</td>
<td>Authentication Service Agency</td>
</tr>
<tr>
<td>2.</td>
<td>AUA</td>
<td>Authentication User Agency</td>
</tr>
<tr>
<td>3.</td>
<td>C-DAC</td>
<td>Centre for Development of Advanced Computing</td>
</tr>
<tr>
<td>4.</td>
<td>CIDR</td>
<td>Central Identities Data Repository</td>
</tr>
<tr>
<td>5.</td>
<td>DET</td>
<td>Detection Error Tradeoff</td>
</tr>
<tr>
<td>6.</td>
<td>FAP</td>
<td>Fingerprint Acquisition Profile</td>
</tr>
<tr>
<td>7.</td>
<td>FAR</td>
<td>False Accept Rate</td>
</tr>
<tr>
<td>8.</td>
<td>FRR</td>
<td>False Reject Rate</td>
</tr>
<tr>
<td>9.</td>
<td>HMAC</td>
<td>Hash-based Message Authentication Code</td>
</tr>
<tr>
<td>10.</td>
<td>MGNREGA</td>
<td>Mahatma Gandhi National Rural Employment Guarantee Act</td>
</tr>
<tr>
<td>11.</td>
<td>OTP</td>
<td>One Time Password/PIN</td>
</tr>
<tr>
<td>12.</td>
<td>PDS</td>
<td>Public Distribution System</td>
</tr>
<tr>
<td>13.</td>
<td>PID</td>
<td>Personal Identity Data</td>
</tr>
<tr>
<td>14.</td>
<td>PII</td>
<td>Personal Identity Information (or Personally Identifiable Information)</td>
</tr>
<tr>
<td>15.</td>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>16.</td>
<td>PoC</td>
<td>Proof of Concept</td>
</tr>
<tr>
<td>17.</td>
<td>NFIQ</td>
<td>NIST Fingerprint Image Quality</td>
</tr>
<tr>
<td>18.</td>
<td>ROC</td>
<td>Receiver Operating Characteristics</td>
</tr>
<tr>
<td>19.</td>
<td>STQC</td>
<td>Standardization Testing and Quality Certification Directorate</td>
</tr>
<tr>
<td>20.</td>
<td>SSL</td>
<td>Secure Socket layer</td>
</tr>
<tr>
<td>21.</td>
<td>UIDAI</td>
<td>Unique Identification Authority of India</td>
</tr>
<tr>
<td>22.</td>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
3. Introduction

In large scale Biometric application like UIDAI, the choice of the acquisition devices is one of the most critical issues, since many, often conflicting, requirements have to be taken into account. To determine that a Biometric Device (sensor-extractor-supplier combination) is capable to meet the goal of UIDAI, in context of its performance in a “given specific operational environment” requires an understanding of the evaluation methodologies and statistics used by the biometrics community.

This procedure provides a baseline testing methodology for operational evaluation of biometric authentication devices to be used for UIDAI applications. This is done through data collection, data processing, analysis of the matching scores and decisions output by the system, without detailed knowledge of the system’s algorithms or of the underlying distribution of biometric characteristics in the population of interest. This document includes generic test plan, requirements for participating suppliers, integration of hardware and software into STQC/UIDAI/C-DAC test platform, training and guidance.

3.1. Scope

This document defines Procedure for performance testing of UIDAI biometric system in terms of false reject rate (FRR) for the purpose of ensuring conformance to UIDAI requirements, Specifies test method including recording data and results reporting. The scope covers single finger print authentication devices (from different golden suppliers).

3.2. Purpose

The purpose of this test is to find out FRR in operation environment.

3.3. Objectives

- The primary objectives of this procedure are to describe test method to:
  » standardize the test method incorporating best practices to ensure reliability and reproduction of test result with subjects of different demographic profile.
  » verify compliance with specified performance requirements.
  » avoid systematic bias due to incorrect data collection and analysis during evaluation.
  » help test engineer analyst to achieve the best possible estimate of field performance based on their evaluation.
  » understand the limits of applicability of test result and test method.

- The secondary objectives of this procedure are to:
  » provide evaluation feedback to participating suppliers/vendors enabling them to design setup for optimal performance.
  » predict performance of different suppliers/vendors.
4. Biometric Products Solicitation for Certification

Participation in the biometric testing and certification is open to all biometric suppliers. An open solicitation for biometric products compliant with Aadhaar authentication specifications is announced by STQC to include as many biometric products as possible. The schedule for the testing will periodically be posted on the STQC’s website.

Through this document, the suppliers interested in participating in the certification are apprised of the detailed implementation of the test plan in advance of the test. Participating suppliers should remain ready with their fingerprint capturing devices and software module(s) for inclusion in the biometric testing. The hardware and software to be used by the respective suppliers are evaluated as a single combined biometric product for the purpose of the test.

5. Protecting the Privacy of the Volunteer Test Population

Great lengths are taken to protect the personal information of the volunteer residents, and it is as per the published UIDAI’s Security Policy and Framework.

This test requires residents' biometrics to be captured, packaged and transmitted to UIDAI’s authentication server. It is very important that the data captured at the front end devices and applications be secured before transmitting over the network. End to end encryption of personal identity data (PID block) is necessary to ensure that data are not read, stored, or tampered with for malicious purposes. Following are the security measures for securing the resident data:

- Aadhaar number of the residents shall not be captured by device vendors during the FRR testing. Reference id will be generated (by C-DAC) which will be used by all device vendors for performing the Aadhaar authentication of residents.
- Encryption of resident data (PID block) at the time of capture using 2048 bit PKI.
- HMAC (Hmac tag) of PID block to eliminate tampering:
  Hash-based Message Authentication Code (HMAC) is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret key. As with any MAC, it is useful to simultaneously verify both the data integrity and the authenticity of a message.
- AUA license key to enable/disable specific features.
- Digitally signed AUA packet for tamper proofing and authenticity.
- No logging/storing of any PID block at device level, PID block is directly encrypted from the memory. Also, PID block is never logged/ stored at AUA/ASA level.
- Secure channel is used for transmitting data from device to AUA, AUA to ASA, and then ASA to UIDAI’s Pre-Production Sever.
- Network filter is used (white listed IPs, Certificates).
- Audits are maintained for every authentication transaction.
- Response is digitally signed for self-verification.
- Network protection and "virus/malware checks" schemes are used to ensure no rouge device or data can disrupt the service.
6. Field FRR Testing Methodology

This section describes the components of the Aadhaar authentication setup and methodologies for conducting the field FRR testing and certification of the biometric authentication products.

The high level components are as follows:
1. Authentication Frontend
2. AUA/ASA Network (C-DAC as AUA and ASA)
3. Authentication backend at UIDAI's Pre-Production Server

Test will be conducted in a real environment with a limited but actual human test population.

6.1. Test Environment

The test environment will consist of the following:
- Human Test Population
- Gatekeeper Client (station set up and managed by C-DAC)
- Best Finger Detection (BFD station setup and managed by C-DAC)
- Authentication Station Setup (set up and managed by respective device suppliers)
- AUA/ASA Aggregator Network (C-DAC as AUA/ASA)
- UIDAI's Pre-Production Server
- Exit Counter (Managed by C-DAC)

6.1.1. Human Test Population

The field test for certification of authentication devices (sensor-extractor-supplier combination) would be carried out on volunteer residents using single fingerprint devices. All products would be tested using the same human test population over a period of two weeks.

Table below presents an expected age-gender distribution* of test population:

<table>
<thead>
<tr>
<th>Age Group</th>
<th>Total (including Male &amp; Female)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10-15</td>
<td>10%</td>
</tr>
<tr>
<td>16-45</td>
<td>63%</td>
</tr>
<tr>
<td>46-65</td>
<td>24%</td>
</tr>
<tr>
<td>66-75</td>
<td>02%</td>
</tr>
<tr>
<td>Above 75</td>
<td>01%</td>
</tr>
</tbody>
</table>

# The distribution of test population may vary, but in all situation, all products would be tested over the common human test population.
* Please refer to Annexure B for reference on a study by NIST.
6.1.2. Gatekeeper Client

To identify and reconcile the Aadhaar holders participating in the field test, C-DAC will deploy a Gatekeeper client. From the Gatekeeper client the resident will go to BFD station, before he/she is directed to an authentication station set up (described in section 6.1.4), the resident would be required to provide his/her details to the Gatekeeper client.

A Random ID will be generated at gatekeeper Client against resident’s UID and resident will be handed over a printed BFD slip with new ID printed on it. Further for BFD and authentication the newly generated/printed ID on the BFD Slip will be used only.
6.1.3. BFD Client
The BFD client helps to identify fingers that have higher probability of successful authentication. Although it is recommended that the fingers identified by the BFD client be used for the authentication purpose by various device suppliers, the suppliers are free to consider authenticating with other fingers as deemed fit.

6.1.4. Authentication Station Setup
The arrangement/order of Authentication Stations should be setup (by the vendors) as per the design prepared by STQC and C-DAC on day to day basis.

The Authentication frontend components (in compliance with UIDAI standards and guidelines) will be designed and implemented by the suppliers. The XML input data that suppliers have to send to the AUA server should be as per the specification mentioned in Annexure A of this document. The suppliers would need to deploy their manpower to execute the field test for their respective devices.

There will be 05 to 06 authentication stations (desks/halls), where each station will have multiple vendor's terminal. Each station will have terminal for all the participating devices. Each terminal may house one authentication device/sensor.
Eg. Vendor X has two participating devices X1 and X2, there are 06 stations, so in total X1 device count should be 06 (1 at each station) and X2 device count should also be 06 (1 at each station).

C-DAC will be providing the internet connectivity but the suppliers are also advised to keep with themselves data card (in case required) to ensure the flawless Internet connectivity.
In order to provide a fair environment to all the participating products, the device sequence/placement in different halls would be different, so that no product suffers from unhabituated behavior of the test population.

The authentication station would consist of the following:

- Multiple terminals. Each terminal may house the following:
  - One device i.e. a single fingerprint sensor.
  - Fingerprint extractor – the software that extracts fingerprint minutiae (in compliance to ISO 19794-2:2005) from the captured image. The extractor software version should be same as what is being submitted for the certification purpose.
  - The application software, in compliance with the UIDAI's policies and specifications, to communicate and transact the data with AUA/ASA server. The xml packet being formed by the application software should be as per the specification mentioned in Annexure A of this document.

It is the sole responsibility of the suppliers to bring all the needed hardware, software and manpower to ensure smooth functioning of devices deployed by them.
The Reference ID and biometric information (such as the fingerprint minutiae) are all packaged into an Authentication packet [UIDAI, Authentication API v1.6, 2012] along with the header information and sent to the UIDAI's Pre-Production Server for authentication through the C-DAC's AUA/ASA network.
Vendor has to obtain Connector, C-DAC Aadhaar Gateway (CAG), API to integrate with client application.

The connector will validate the input parameters, generate request xml and post it to AUA server. The AUA server will accept request only from CAG and not from direct post to url.

6.1.5. **AUA/ASA Aggregator Network (C-DAC as AUA/ASA)**

C-DAC would be an aggregator and a network partner to STQC for the purpose of field FRR testing required as part of certification procedure. C-DAC will act as both AUA and ASA.

- The AUA will perform the following validations:
  1) Sub-AUA validation
  2) lk validation
  3) udc validation: udc validation against the assigned value. udc attribute value will be assigned by C-DAC AUA. Vendor has to submit the serial number of device under test for generating udc (for example: 6 devices for authentication station + 4 devices in backup).

- The error codes that may be returned by the AUA/ASA server are tabulated below:
If any errors are encountered at UIDAI’s authentication server in the authentication request, the error codes would be as defined in the UIDAI’s API document [UIDAI, Authentication API v1.6, 2012].

6.1.6. UIDAI’s Authentication Server

C-DAC as AUA/ASA will connect to the UIDAI’s Pre-Production Server (authentication infrastructure) during Biometric Testing Campaign and Products Certification.

6.2. Field Testing Steps

The field testing will be done in the following steps (refer to Figure 1):

1) Resident approaches the test location. At the test location, he/she is asked to approach to the gatekeeper client station for the attendance and generation of reference ID, recommendation of good fingers (BFD) and guidance to head towards the respective authentication station.

2) Resident approaches the authentication station. The authentication station comprises multiple terminals (laptops/workstations), where each terminal may house one participating biometric product (sensor-extractor-supplier combo). Resident provides the generated Reference ID and biometric details to terminal devices to get himself/herself authenticated. The resident would need to
authenticate himself/herself on each of the participating product (one by one) arranged along a particular authentication line.

Refer to **Annexure G** for details on **Resident Movement Plan**.

3) The authentication application software installed in the respective terminals packages the input parameters, as specified in **Annexure A**, encrypts, encodes and sends the packet to the C-DAC AUA server over network (provided by C-DAC) using AUA specific protocol.

4) AUA server, after data validation, forms the auth. XML, completes necessary data logging and then passes the request to the C-DAC ASA server over the secured network.

5) ASA server, after necessary data logging, passes the request to the UIDAI's Pre-Production Server for resident's authentication over the secured network.

6) The UIDAI authentication server returns a "yes/no" (as part of the response data) based on the match of the input parameters to the respective terminal (at the test location) through AUA/ASA server. The response XML data are logged at the AUA/ASA server.

7) One authentication packet from AUA to UIDAI's authentication server is normally about 3-4 KB including single/double fingerprint(s) and AUA digital signature. Authentication response is about 1 KB.

### 6.3. Expected Data Analysis

- **False Reject Rate (FRR) at a fixed FAR.**
  
  Where, a product is defined as a combination of the following:
  
  » Sensor make
  
  » Features extractor SDK

- **Steps for data analysis:**
  
  » C-DAC (AUA/ASA team) to capture and provide data for analysis.
  
  » C-DAC (Biometrics team) Reconciliation of BFD and Authentication data.
  
  » C-DAC (Biometrics team) to analyze the data, plot required curves, and prepare report.
  
  » STQC to review the report and give feedback.

  » C-DAC to finalize the report and present to STQC for their approval

  » Products certification by STQC (based on the approved report).

Please refer to **Annexure D**, **Annexure E** and **Annexure F** for details.
7. Key Roles and Responsibilities

7.1. STQC

- Specifying terms and conditions to the participating suppliers.
- Supervise the biometric testing methodologies and testing campaign.
- Specifying terms and conditions to the participating suppliers.
- Note the Failure to capture (FTC) cases at the field.
- Review and approval of test data analysis & reports.
- Drive testing and certification process to closure
- Certification of biometric devices for Aadhaar project.

7.2. C-DAC

7.2.1. Biometrics Team

- Coordination and preparation of the document on field testing methodologies and certification of Aadhaar authentication devices.
- Allocation of fdc and udc to the participating biometric products (sensor–extractor–supplier combination).
- Technical services at field level operations, including installation and functioning of Gatekeeper client application software.
- Generation of Reference ID.
- Installation and functioning of BFD client application software.
- Running the required post-campaign tests for data analysis and FRR calculation.
- Performing a detailed analysis of the results of the tests and graph generations.
- Drawing conclusions, and upon approval by the competent authorities, creating the final field testing report for certification of the participating products by STQC.

7.2.2. AUA/ASA Team

- Carrying out all the identified back-end AUA/ASA level development/activities.
- Data validation and errors handling at AUA/ASA Server.
- All sorts of data logging: BFD, Authentication requests and responses.
- Provide required data to C-DAC Biometrics team for data analysis
- Technical services at field level operations.

7.3. Device Suppliers

- Deploy required number of authentication devices and other supporting hardware (laptop, barcode reader etc.) at assigned authentication stations (05-06)
- Ensure end-to-end working of authentication application (including network connectivity) as per published API 1.6 and other specifications given in testing methodology document
- Deploy necessary manpower to manage the authentication operations for the respective devices
- Take necessary measures to ensure all residents directed to the specific authentication devices are able to transact
- Provide other required support to C-DAC/STQC for carrying out the test
8. High-level Milestones and Timeline (tentative)

For the Connectivity testing the vendors need to whitelist their Public IPs, get reference ids and udc generated from C-DAC.
A separate mail has been sent to all the interested vendor’s regarding this.

Figure 2: Milestones and Timelines
9. References

1) [UIDAI, Authentication API v1.6, 2012]: AADHAAR Authentication API Specification - Version 1.6

2) [UIDAI, Role of Biometric Technology, 2012]: Role of Biometric Technology in Aadhaar Authentication (Authentication Accuracy –Report)

3) [UIDAI, Authentication Model, 2012]: AADHAAR Authentication Operating Model

4) [UIDAI, BFD v1.6, 2012]: AADHAAR BEST FINGER DETECTION API Specification - Version 1.6
   http://uidai.gov.in/images/FrontPageUpdates/aadhaar_bfd_api_1_6.pdf


   http://www.npl.co.uk/upload/pdf/biometrics_bestprac_v2_1.pdf

7) [NIST, MINEX Performance and Interoperability, 2006]: MINEX Performance and Interoperability of the INCITS 378 Fingerprint Template, Supplement No. 1 Native Matching, Patrick Grother, Michael McCabe, Craig Watson, Mike Indovina, Wayne Salamon, Patricia Flanagan, Elham Tabassi, Elaine Newton, Charles Wilson, National Institute of Standards and Technology March 21, 2006

8) [STQC, UIDAI Biometric Device Specifications, 2012]: UIDAI Biometric Device Specifications

9) [STQC, Certification, 2011]: STQC Biometric Devices Testing and Certification
   http://www.stqc.gov.in/content/bio-metric-devices-testing-and-certification
Annexure A. Authentication Request and Response Data Formats*

» Aadhaar authentication during field testing will use only XML as the data format for input and output.
» The formats mentioned below are meant only for field testing and certification purposes.

* Primary source: [UIDAI Authentication API v1.6, 2012]

A1. Authentication Request Data Format: The XML input data elements are as follows:

![Diagram of Connector: Data Flow Diagram]

1. Vendor’s Frontend Application:

The Frontend Application should at least provide the following provisions:

- Should integrate the C-DAC Connector*.
- Should display the number of attempts.
- Should be able to change the environment at runtime.
- Should display txn.
- There should be provision of displaying UDC and FDC.

*C-DAC Connector has been shared with the participating Vendors.

C-DAC Connector:

C-DAC connector generates the below auth.xml and forwards it to AUA/ASA.

```xml
<Auth uid="" ac="" tid="" ver="1.6" txn="" lk="" sa=""
xmlns="http://www.uidai.gov.in/authentication/uid-auth-request/1.0">
<Uses pi="n" pa="n" pfa="n" bio="y" bt="FMR" pin="n"
otp="n"/>
<Meta udc="" pip="" fdc="" idc="" lot="" lov=""/>
<Skey ci="">encrypted and encoded session key</Skey>
<Data type="X">encrypted PID block</Data>
```
<Hmac>SHA-256 Hash of Pid block, encrypted and then Encoded</Hmac>
</Auth>

All mandatory elements as specified in Aadhaar Authentication API 1.6 should be present in request XML.

A2. Authentication Response Data Format: The XML response data elements are as follows:

<AuthRes code="" err="" info="" ret="" ts="" txn="">
   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
         <CanonicalizationMethod
            Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
         <SignatureMethod
            Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
         <Reference URI=""/>
            <Transforms>
                <Transform
                    Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            </Transforms>
         <DigestMethod
            Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
         <DigestValue></DigestValue>
      </Reference>
   </SignedInfo>
   <SignatureValue></SignatureValue>
</Signature>
</AuthRes>
Annexure B. Human Factors & Usability Interaction on Fingerprint Quality

Source URLs:
- http://zing.ncsl.nist.gov/biousa/docs/theofanos_quality_workshop_3-8-06.pdf

A. Human Factors and Usability Interaction on Fingerprint Quality

» Age Factor
- Younger subjects submit higher quality prints than older subjects

![Figure 4. A quality vs age group.](image)

» Attempts by Age Groups
- When feedback was introduced older participants tried more times:

![Figure 5. Attempts vs age group.](image)

» Gender Dependency
- Women's fingerprints, on average, are of poorer quality than men's:

![Figure 6. Quality dependency on gender.](image)
Annexure C. Terms and Conditions for Suppliers

1. The participating suppliers will have to bring their terminals, authentication devices, feature extractor, the application software (in compliance with the UIDAI’s policies and specifications) etc., to communicate and transact the data with AUA/ASA server.

2. It is the sole responsibility of the suppliers to bring all the needed hardware, software and manpower to ensure smooth functioning of devices deployed by them.

3. Data/log sheets (hard copies), as per the template provided by STQC, will be maintained for each day during the field testing. The sheets will bear the resident transactions, hardware failure (if any) and such other related details, which need to be signed by all the suppliers.

4. It is the responsibility of the suppliers to ensure all the test participants directed to a particular authentication station transact on the corresponding device deployed by the respective suppliers.
Annexure D. FRR Calculation: Process Flow

Figure 7: FRR Calculation Process Flow
Notes

Note-1. In case a particular resident authentication is not attempted by the participating supplier, supplier is required to notify the room supervisor in person. Room supervisor will categorize the error along the following two categories for that device, namely –

a. **Failure to Acquire (FTA)** – When resident fingers are not captured by the device after the repeated attempts, then the supervisor is required to make a note of the resident's Aadhaar number and make a note of it under FTA category for that particular device. Supervisor is also required to note any remarks as potential reasons for FTA.

b. **Network error or other system related errors** – When residents are not able to attempt authentication due to network or other authentication station/device related issue, the supervisor makes a note of such Aadhaar numbers under "Network and Other Errors" category for that device. These include response codes excluding y and 300.

All the FTA cases and network errors or other device related errors have to be recorded by supervisor. **In case, if any supplier fails to intimate these errors to the supervisor, all the balance cases from total population which were not recorded in the UIDAI authentication backend logs will be counted as FTA for that particular device.**

Note-2. All suppliers are provided with a grace of 25 failure cases to accommodate errors due to intermittent network or other authentication device related issues. The suppliers are requested to plan for multiple network connectivity options to accommodate variable network connectivity conditions.

Note-3. In case a particular resident leaves the authentication room midway during the device authentication process, then the resident’s Aadhaar number is eliminated for FRR calculation for all participating suppliers.
Annexure E. Guidelines for FTA (Failure to Acquire) Indicators

As deliberated in earlier workshops, FTA is an important component of FRR calculation. The decision mechanism for concluding the FTA is based on the following indicators:

**Indicator 1.** Resident is made to spend more than 03 minutes per device (in case of normal operating conditions: like network availability, etc.)

**Indicator 2.** Crowd gets built (or sequence gets blocked) at any particular device.

**Indicator 3.** More than 04 multiple attempts:
- As observed by the respective STQC supervisor
- As informed by the resident

**Indicator 4.** "Yes" response after more than 04 attempts as observed during reconciliation process: Restarting the application in-between (or after multiple attempts) during the authentication process of a resident.
## Annexure F. Aadhaar Numbers by Suppliers for Testing Purpose

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Aadhaar Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td></td>
</tr>
</tbody>
</table>

I hereby declare that I will use only the above mentioned Aadhaar numbers for testing the readiness of my applications/devices.

Supplier Name : 

Representative Name : 

Signature : 

Date : 

Date: 04th Oct 2018, v2.5
### Annexure G. Resident Movement: Process Flow

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| **Resident Mobilizer at welcome table** | • Resident comes to welcome table/Gatekeeper Client  
• BFD Slip with consent form given to the resident  
• Resident signs consent form and carries to BFD station |
| **Runner** | • Directs resident to a BFD station |
| **BFD Operators** | • Do BFD  
• Updates BFD Slip |
| **Resident mobilizer at STQC table** | • Coordinate with runners of each floor and write station no. and serial number for the station in BFD Slip  
• Explain the process to the resident  
• Direct resident to the required station no. |
| **Operators at Auth. Stations** | • Do authentication of the resident in a sequential manner  
• Sign-off in the respective device cell (on BFD Slip) |
| **STQC Supervisor at Auth. station** | • Ensure smooth movement  
• Track/record exception/errors  
• Direct resident to the STQC table after ensuring resident authenticate on each device of the station |
| **Gift Counter Table** | • Collect the BFD Slip with consent from resident, and file in the respective BOX file  
• Handover Gift  
• Thanks the Resident |