Testing Methodologies for
Certification of Aadhaar Authentication Devices

Centre for Development of Advanced Computing

Telephone (Head Quarters, Pune): +91-20-25704100 Fax: +91-20-25694004
Telephone (Mumbai Center): +91-22 26201606, Fax: +91-22-26232195
Website: www.cdac.in, www.cdacmumbai.in

Date: 16th July 2012, v0.9

Table of Contents

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 native product. 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].

2. Acronyms and Terms

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

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 device with different sensor/extractor combination.

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:
  - » 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:

- 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 GNDC.
- 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: Sensor–Extractor–Supplier Combination.

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 GNDC

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 UIDAI/CDAC/STQC)
- Authentication Station Setup (set up and managed by respective device suppliers)
- AUA/ASA Aggregator Network (C-DAC as AUA/ASA)
- UIDAI's GNDC Authentication Server

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:

The expected test population size#: • **Maximum: 5000** • **Minimum : 3500**	
Age Group	**Total (including Male & Female)**
5-15	10%
16-45	63%
46-65	24%
66-75	02%
Above 75	01%

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.

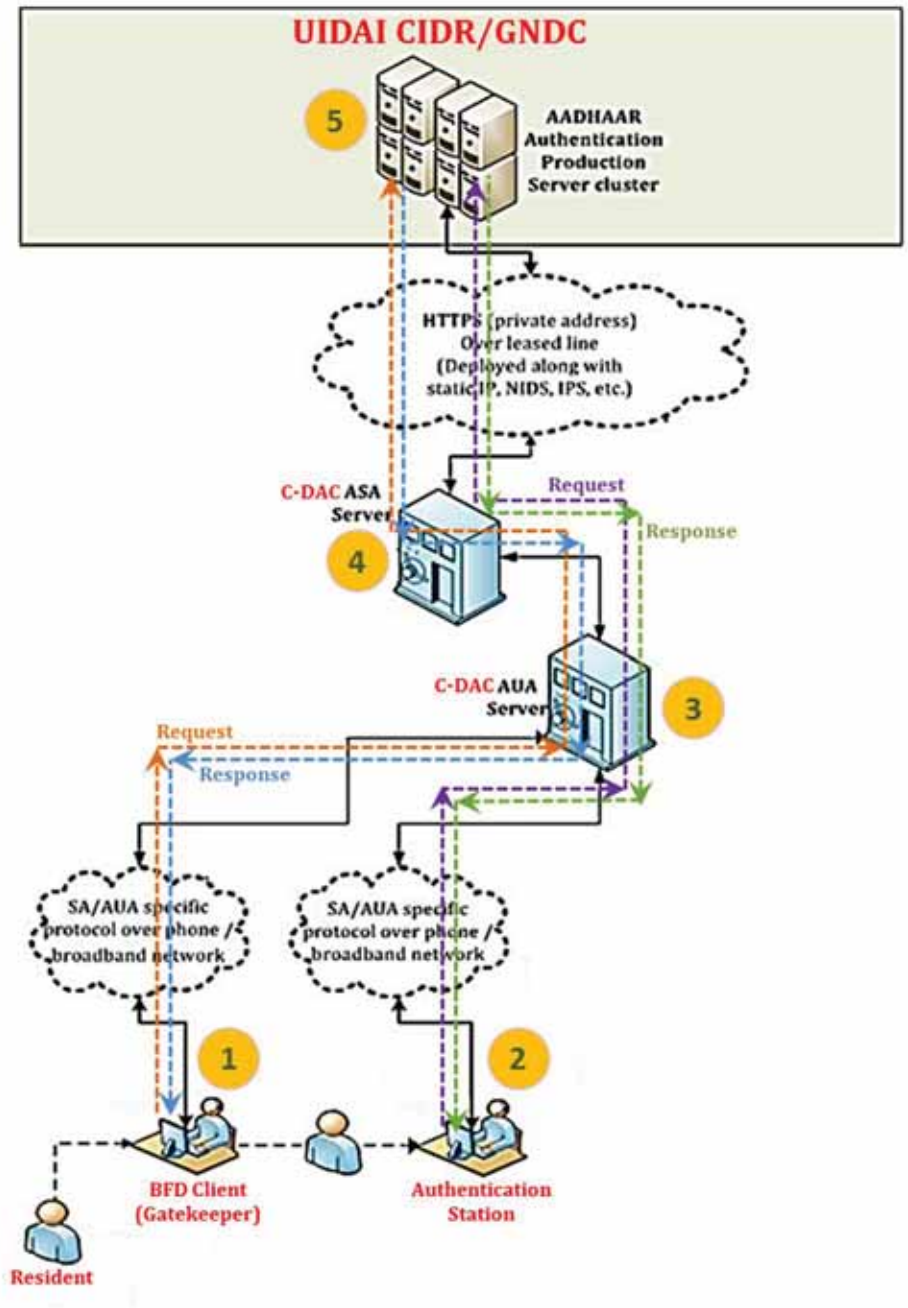


Figure 1: Aadhaar Authentication Setup for Device Certification.

6.1.2. Gatekeeper Client

To identify and reconcile the Aadhaar holders participating in the field test, C-DAC will deploy a Gatekeeper client. Before a resident is directed to an authentication station set up (described in section 6.1.3), the resident would be required to provide his/her details to the Gatekeeper client.

The Gatekeeper client may also help identify fingers that have higher probability of successful authentication. Although it is recommended that the fingers

identified by the Gatekeeper client be used for the authentication purpose by various device suppliers, the suppliers are free to consider authenticating with other fingers as deemed fit.

6.1.3. Authentication Station Setup

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 8 to 10 authentication stations (desks/halls), where each station will have multiple terminals. Each terminal may house one or more authentication devices/sensors. In all cases, each station will have every sensor-extractor-supplier combination requiring FRR testing for certification purposes.

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 or more authentication devices, where each device is 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.
  - » Barcode reader to capture and input resident's Aadhaar number.
  - » A data card. However, the suppliers are advised to keep with themselves multiple data cards (of different makes) to ensure the flawless Internet connectivity. The UIDAI-CDAC-STQC will not be responsible for any flaw/loss in Internet connectivity.

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 Aadhaar number 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 GNDC for authentication through the C-DAC's AUA/ASA network. AUA's public URL is: https://vikrant.cdacbangalore.in/authrequest/process/post

6.1.4. 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) XML data validation
  2) udc validation: udc validation against the assigned value, as udc attribute value will be assigned by C-DAC AUA.

- The error codes that may be returned by the AUA/ASA server are tabulated below:

Error Codes (defined at the C-DAC AUA/ASA for the suppliers)		
Sr.No.	**Error Code**	**Description**
1.	1201	CIDR connection timed out
2.	1202	Invalid udc
3.	1203	Invalid Auth. XML

- 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].

6.1.5. UIDAI's Authentication Server

Currently UIDAI is having two data centers (CIDR at Bangalore and GNDC at Greater Noida) from where authentication infrastructure is running.

C-DAC as AUA/ASA will connect to GNDC 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, recommendation of good fingers 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 or more participating biometric products (sensor-extractor-supplier combo).Resident provides Aadhaar Number 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.

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

3) The authentication process follows the "**Two Finger Authentication Scheme**", as explained in **Annexure C**. The maximum number of attempts per resident per product is 04. In case of the first attempt (out of four), only one FMR will be present in the PID block, whereas, in the subsequent attempts (if required), there will be two FMRs packaged in the same PID block. As per the published Authentication API Specification 1.6, POSH (Position Hint) is a mandatory attribute and ten values corresponding to ten fingers are permitted. So, finger labeling (specifying the finger position) is compulsory at the time of capture.

4) 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 either a mobile/broadband network using AUA specific protocol. The connectivity between authentication device and AUA server has to be ensured by the device supplier.

5) 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.

6) ASA server, after necessary data logging, passes the request to the UIDAI's GNDC for resident's authentication over the secured network.

7) 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.

8) One authentication packet from AUA to GNDC 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. Data Logging @ AUA/ASA

AUA/ASA will perform the information logging as per the UIDAI policies. The data that would be logged are as follows:

- **Data Logging Schema for XML Auth, Uses and Meta Tags @ AUA/ASA Server***

(Auth) **uid** *(Aadhaar number of the resident)*	(Meta) **fdc** *(fingerprint device code)*	**Auth** *(Root element of the input XML for authentication service)*						**Uses** *(This element specifies the auth. factors used by the request)*		**Meta** *(This element specifies metadata related to the device and transaction)*			
		tid	**ac**	**sa**	**ver**	**txn**	**lk**	**bio**	**bt**	**udc**	**pip**	**lot**	**lov**

- **Data Logging Schema @ AUA/ASA Server***

txn	**uid** *(Aadhaar number of the resident)*	**fdc** *(fingerprint device code)*	**Request Receipt Time**	**Request Forward Time**	**Response Receipt Time**	**Response Forward Time**	**TAT**	**AUA Request Processing Time**	**AUA Response Processing Time**

Where, TAT, AUA Request Processing Time and AUA Response Processing Time will be calculated as follows

- Turn Around Time (TAT): ***{(Response Receipt Time) – (Request Forward Time)}***
- AUA Request Processing Time: ***{(Request Forward Time) – (Request Receipt Time)}***
- AUA Response Processing Time: ***{(Response Forward Time) – (Response Receipt Time)}***

- **Data Logging Schema for Response XML @ AUA/ASA Server***

AuthRes					
txn	**code**	**ret**	**err**	**ts**	**info**

* Please refer to **Annexure A** for more details on XML data elements. Minor changes are expected in the logging schemas.

6.4. Expected Data Analysis

- **False Reject Rate (FRR) and average number of attempts for all the products at a fixed FAR.**

  Where, a product is defined as a combination of the following:
  - » Sensor make
  - » Features extractor SDK, and
  - » Supplier Profile

- **Steps for data analysis:**
  - » Design data logging schemas for the data points (to be captured) during the Testing Campaign.
  - » C-DAC (AUA/ASA team) to capture and provide data for analysis.
  - » 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 E**, **Annexure F**, **Annexure G** and **Annexure I** for details.

7. Key Roles and Responsibilities

7.1. STQC

- Specifying terms and conditions to the participating suppliers.
- Allocation of **fdc** to the participating biometric products (sensor–extractor–supplier combination).
- Supervise the biometric testing methodologies and testing campaign.
- Specifying terms and conditions to the participating suppliers.
- 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.
- Technical services at field level operations, including installation and functioning of Gatekeeper 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.
- 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.

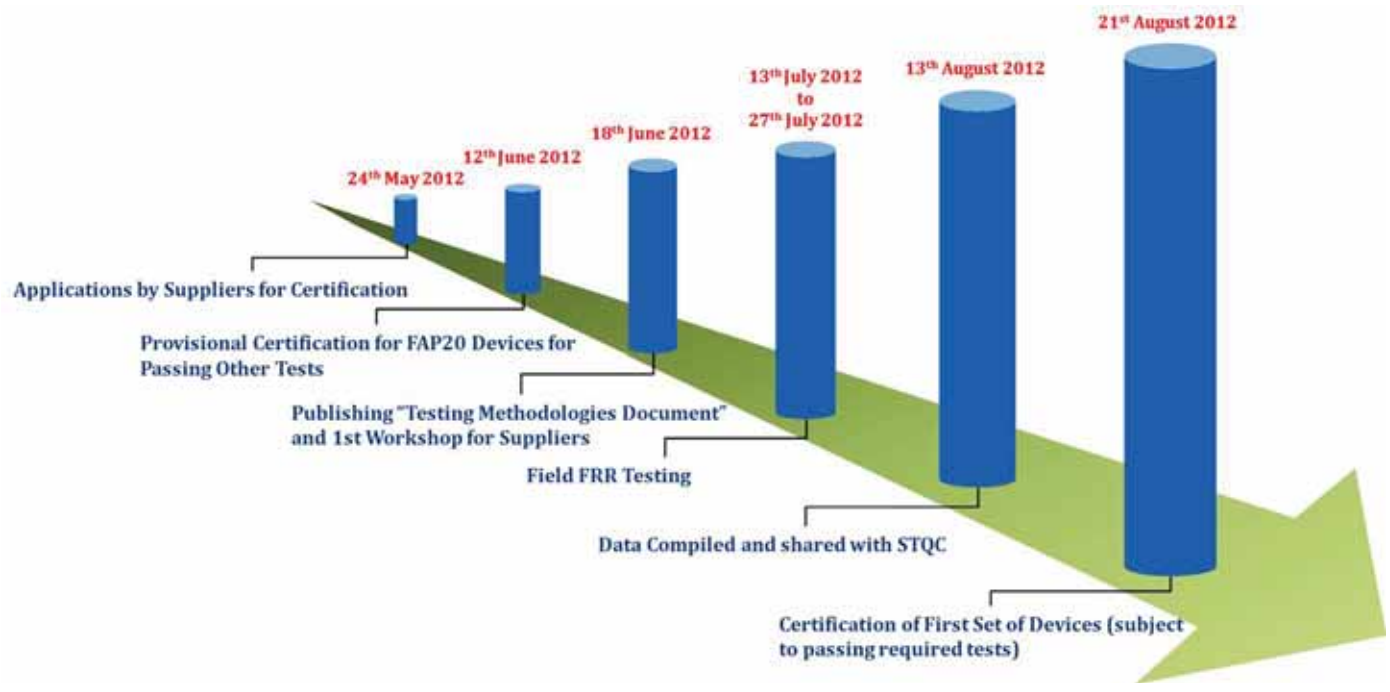
7.3. UIDAI

- Provide inputs for the field testing Project Plan and DPR.
- Provide support for monitoring field testing activities, and develop training material for the field level manpower.
- Receive data analysis and report for information & further action as may be necessary
- Liaise with local administration, provide field level manpower to manage resident mobilization, and train the field level manpower.
- Identify locations where field testing may be conducted.

7.4. Device Suppliers

- Deploy required number of authentication devices and other supporting hardware (laptop, barcode reader etc.) at assigned authentication stations (8-10)
- 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)



9. References

1) [UIDAI, Authentication API v1.6, 2012]: AADHAAR Authentication API Specification - Version 1.6
http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_6.pdf

2) [UIDAI, Role of Biometric Technology, 2012]: Role of Biometric Technology in Aadhaar Authentication (Authentication Accuracy –Report)
http://uidai.gov.in/images/role_of_biometric_technology_in_aadhaar_authentication_020412.pdf

3) [UIDAI, Authentication Model, 2012]: AADHAAR Authentication Operating Model
http://www.uidai.gov.in/images/authDoc/d3_1_operating_model_v1.pdf

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

5) [UIDAI, BDCS, 2012]: UIDAI Biometric Device Specifications (Authentication)
http://stqc.gov.in/sites/upload_files/stqc/files/New%20Revision%20_May_%201%20STQC%20UIDAI%20BDCS-03-08%20UIDAI%20Biometric%20Device%20Specifications%20_Authentication_.pdf

6) [UIDAI, Security Policy & Framework, 2011]: Aadhaar Security Policy & Framework for UIDAI Authentication – Version 1.0
http://uidai.gov.in/images/authDoc/d3_4_security_policy_framework_v1.pdf

7) [NIST, Performance of Biometric devices, 2002]: Best practices in testing and reporting performance of biometric devices, Version 2.01 By A. J. Mansfield, National Physical Laboratory and J. L. Wayman, San Jose State University. Middlesex: NPL Report CMSC 14/02.
http://fingerprint.nist.gov/minex04/minex_report.pdf

8) [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

9) [STQC, UIDAI Biometric Device Specifications, 2012]: UIDAI Biometric Device Specifications
http://stqc.gov.in/sites/upload_files/stqc/files/New%20Revision%20_May_%201%20STQC%20UIDAI%20BDCS-03-08%20UIDAI%20Biometric%20Device%20Specifications%20_Authentication_.pdf

10) [STQC, Certification, 2011]: STQC Biometric Devices Testing and Certification
http://www.stqc.gov.in/content/bio-metric-devices-testing-and-certification

10. Annexures

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:

```
<Auth uid="" tid="" ac="" sa="" ver="" txn="" lk="">
        <Uses bio="y" bt="FMR"/>
        <Meta udc="" fdc="" pip="" lot="P" lov=""/>
        <Skey ci="">encrypted and encoded session key</Skey>
        <Data>encrypted PID block</Data>
        <Hmac>SHA-256 Hash of Pid block, encrypted and then
                encoded</Hmac>
        <Signature>Digital signature of AUA</Signature>
</Auth>
```

The XML input data marked in blue color are to be sent by the supplier (from the authentication device) to the C-DAC AUA/ASA server. Rest of the input data elements will be populated at the AUA's end by the AUA.

- Description of the above mentioned data elements (to be provided by the Suppliers) are as follows:

Sr.No.	Element	Attributes	Valid Values for Field Testing	Source	Description	Max. Length & Format
1.	Auth (mandatory)	uid	Aadhaar number of the resident being authenticated	Supplier	Aadhaar number of the resident from human test population called for field testing.	Numeric string of length 12.
2.		sa	As assigned by C-DAC AUA	Supplier	Alphanumeric vendor code of size 6 will be stored in this attribute.	Alpha-numeric string of length 20
3.	Meta (mandatory)	udc	As assigned by C-DAC AUA	Supplier	Unique Device Code. This attribute value will be assigned by CDAC for all the terminal devices.	Alpha-numeric string of maximum length 20
		fdc	As assigned by STQC	Supplier	Fingerprint device code. This is a unique code provided for the fingerprint sensor-extractor-supplier combination and will be provided by STQC before start of the field testing.	Alpha-numeric string of maximum length 10

		pip	**Public IP address of the device.**	**Supplier**	All devices will be connected to the Internet and will have a public IP (if the device has a private IP and is behind a router/proxy/etc, then public IP address of the router/proxy/etc. should be set).	---
4.	**SKey** (mandatory)	**ci**	**Value of this attribute is the certificate expiration date in the format "YYYYMMDD"**	**Supplier**	Public key certificate identifier using which "skey" was encrypted. UIDAI may have multiple public keys in field at the same time.	Certificate expiration date in the format "YYYYMMDD"
5.	**Data** (mandatory)	**---**	**Encrypted & encoded Pid block**	**Supplier**	The PID block should be in the XML format.	---
6.	**Hmac** (mandatory)	**---**	**Encrypted & encoded SHA-256 hash of Pid block**	**Supplier**	Encrypted & encoded SHA-256 hash of Pid block: • After forming Pid XML, compute SHA-256 hash of Pid XML string. • Then encrypt using session key (skey). • Then encode using base-64 encoding.	---

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

<AuthRes ret="y|n" code="" txn="" err="" auaerr="" ts="" info="">

</AuthRes>

- Signature elements from UIDAI "AuthRes" are removed
- "auaerr" attribute is added in "AuthRes" element
- "auaerr" will return C-DAC AUA-ASA error code

Annexure B. Human Factors & Usability Interaction on Fingerprint Quality

Source URLs:

- http://zing.ncsl.nist.gov/biousa/docs/WP302_Theofanos.pdf
- http://zing.ncsl.nist.gov/biousa/docs/theofanos_quality_workshop_3-8-06.pdf
- http://zing.ncsl.nist.gov/biousa/docs/chi_2006_poster2.pdf

A. Human Factors and Usability Interaction on Fingerprint Quality

» Age Factor

- **Younger subjects submit higher quality prints than older subjects**

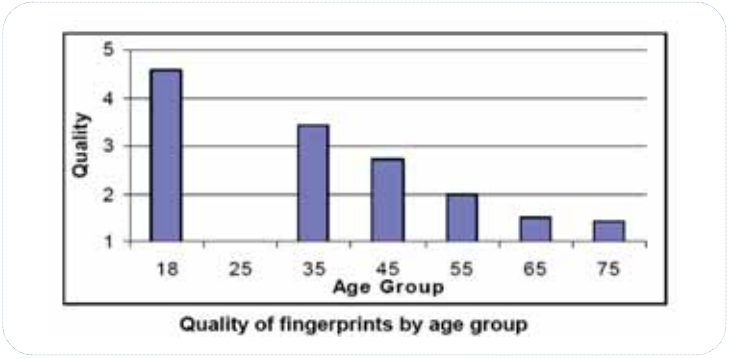


Figure 2. A quality vs age group.

» Attempts by Age Groups

- **When feedback was introduced older participants tried more times:**

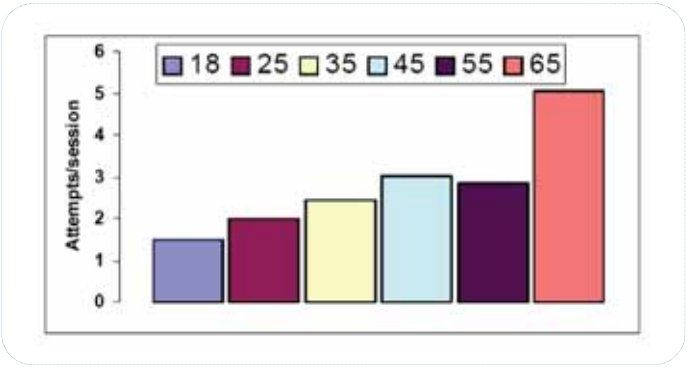


Figure 3. Attempts vs age group.

» Gender Dependency

- **Women's fingerprints, on average, are of poorer quality than men's:**

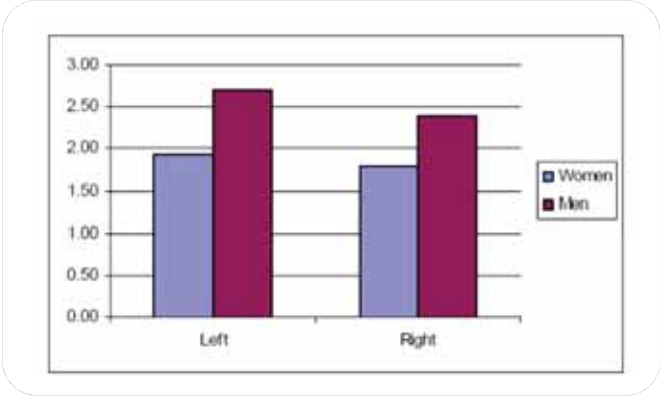


Figure 4. Quality dependency on gender.

Annexure C. Two Finger Authentication Process

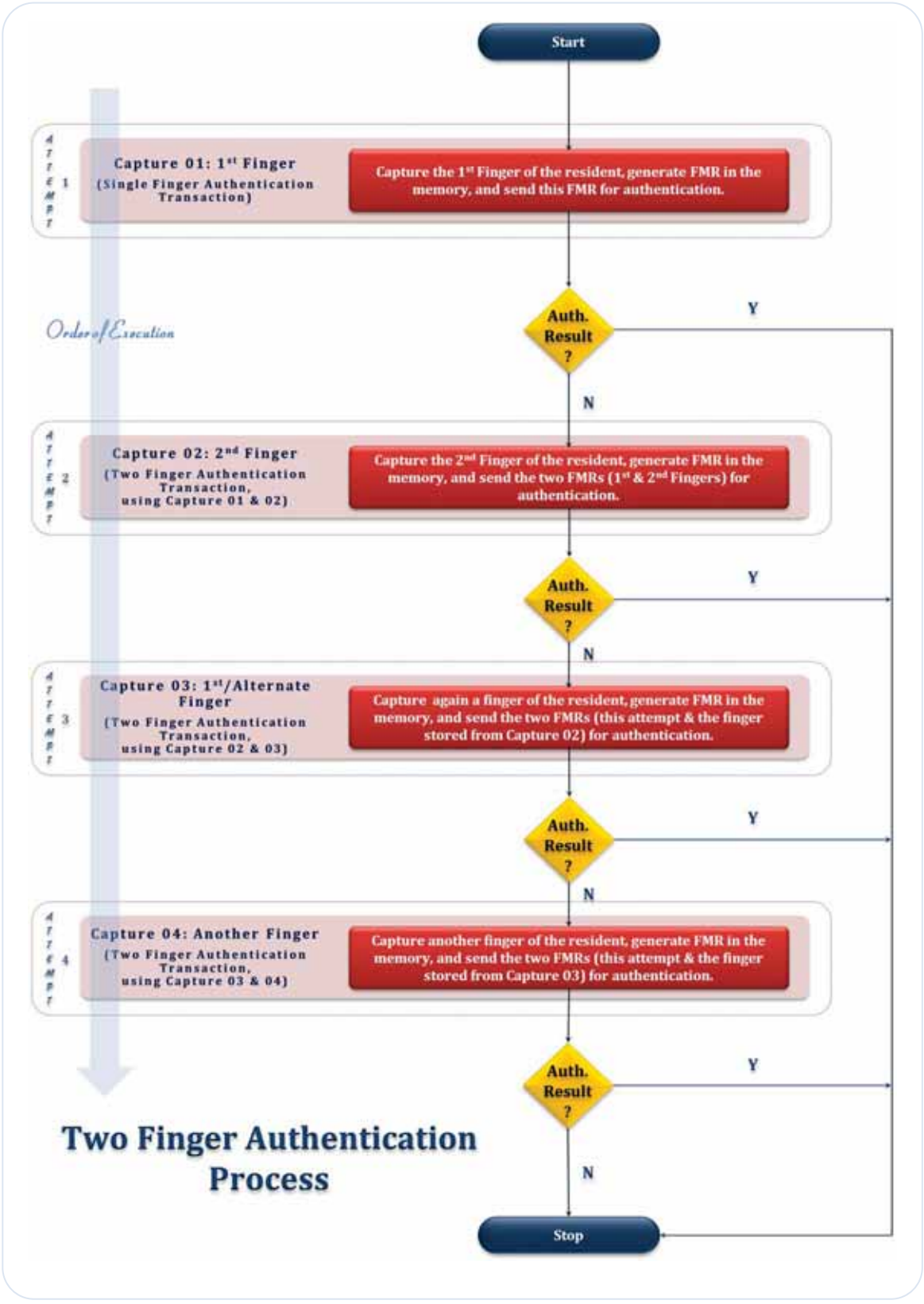


Figure 2: Two Finger Authentication Process

Annexure D. 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.

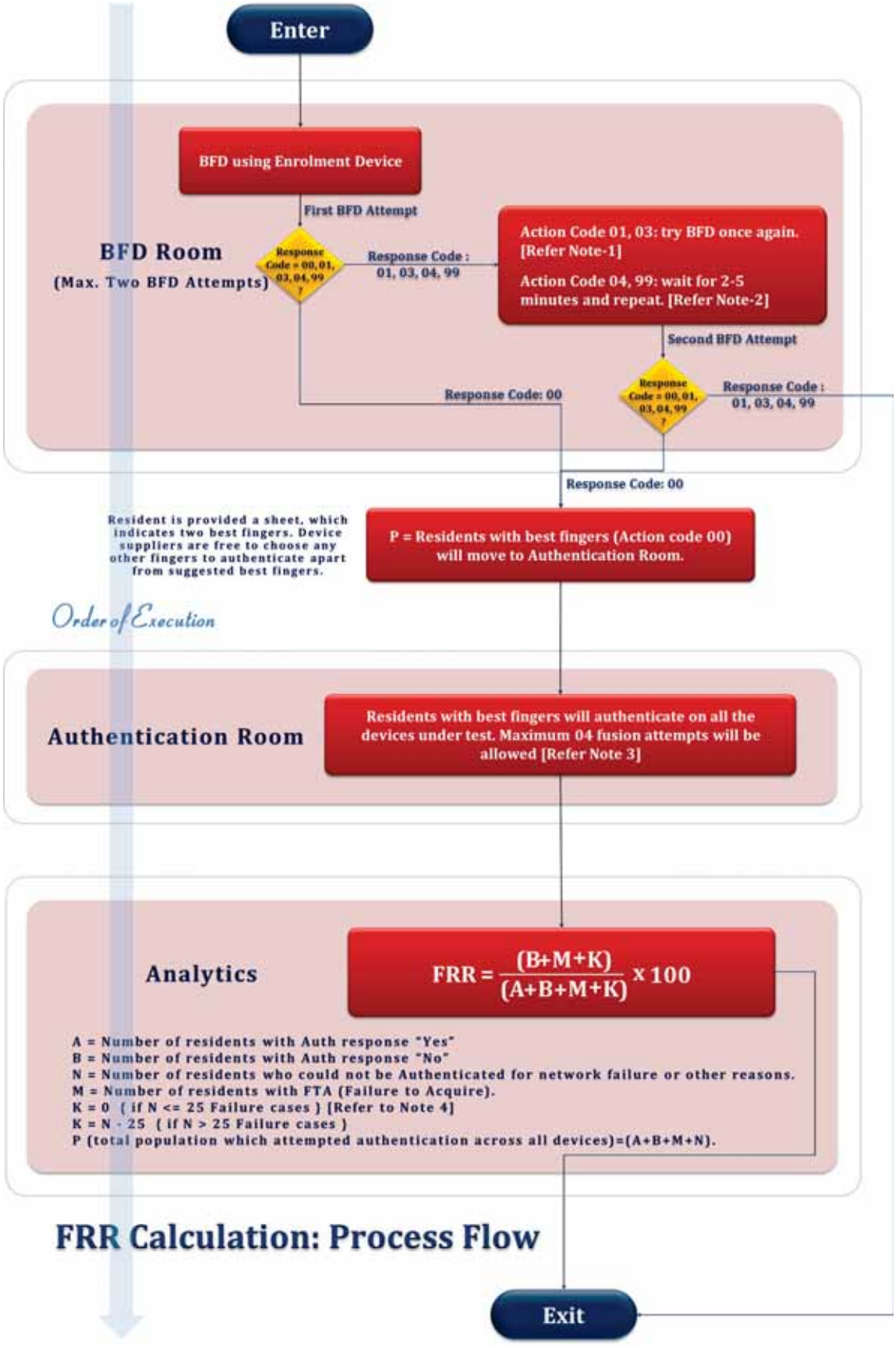
2. It is the sole responsibility of the suppliers to bring all the needed hardware, software and manpower to ensure smooth functioning of devices deployed by them.

3. The suppliers are advised to keep with themselves multiple data cards (of different makes) to ensure the flawless Internet connectivity. The UIDAI-CDAC-STQC will not be responsible for any flaw/loss in Internet connectivity.

4. 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.

5. 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 E. FRR Calculation: Process Flow



Notes

Note-1. **Action Codes 01 or 03**: BFD can be repeated for these residents second time. Attention should be paid to following factors during BFD:

a. Verify that the Aadhaar card indeed belongs to the same resident.
b. Verify the Aadhaar number being entered.
c. Sequence of capturing fingers as per the suggested order**.**

Note-2. **Action Code 04 or 99**: In case, if resident obtains action code 99, the resident is asked to wait aside for 2-5 minutes (time for on-demand fingerprint template loading from enrollment system into authentication systems) and BFD is repeated. 99 could also be a result of wrongly entered UID. Action code 04 refers to the action to check whether the Aadhaar number was entered correctly. If it was entered correctly, the resident's enrollment needs to be updated.

During BFD, even after second round, the action code returned is 01/03/04/99, such resident can't participate in the authentication exercise.

[Refer to the Best Finger Detection API document for exhaustive error codes and action codes]

Note-3. 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-4. 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-5. 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 F. 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 06 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 G. Aadhaar Numbers by Suppliers for Testing Purpose

Sr. No.	Aadhaar Number
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

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 :

Annexure H. Resident Movement: Process Flow

Resident Mobilizer at welcome table	• Resident comes to welcome table • Token & 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 • Staple consent form and BFD receipt
Resident mobilizer at STQC table	• Coordinate with runners of each floor and write station no. and serial number for the station in BFD receipt • 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 receipt)
STQC Supervisor at Auth. station	• Ensure smooth movement • Track/record exception/errors • Direct resident to the STQC table after ensuring resident authenticates on each device of the station
STQC Personnel at STQC table	• Collect the BFD receipt and consent form from resident, and file in the respective BOX file • Sign-off the token and direct the resident to gift-counter
Gift Counter Table	• Collect token from the resident • Handover Gift • Thank the resident

;

Annexure I. FRR Mock Report

Mock report and the corresponding graph are based on dummy data, meant only for gaining good understanding and clarity. Slight variation is expected in the approach.

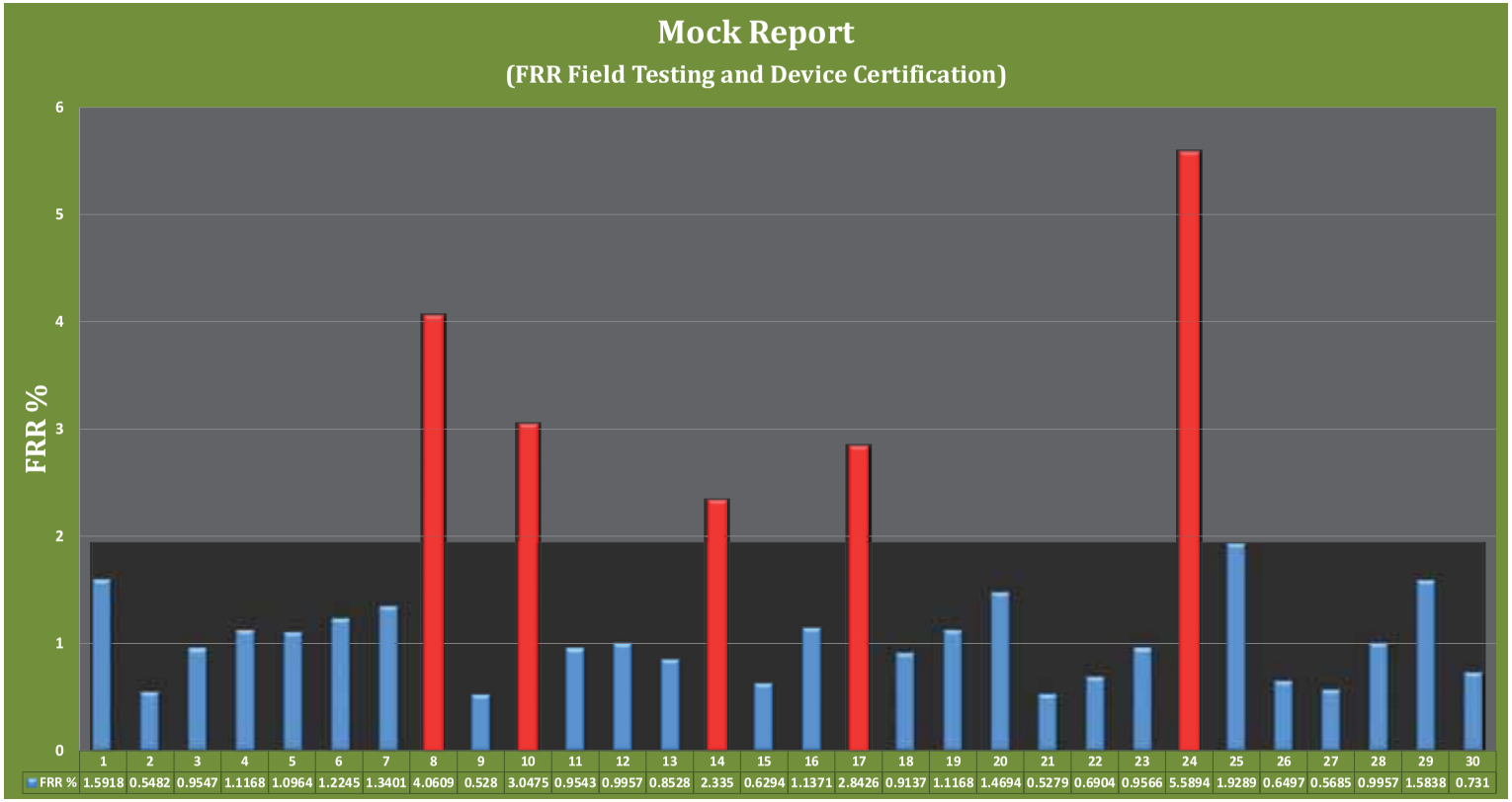
Table of Content
Back to Context

Please refer to the next page for the mock report.

FRR Field Testing Mock Report

Test Population Size arrived to the location and attempted BFD(X)	**5000**	**Symbols and Definitions -** **A: Number of residents with Auth response "Yes" .** **B: Number of residents with Auth response "No".** **N: Number of residents who could not be authenticated for network failure or other reasons .** **M: Number of residents with FTA (Failure to Acquire).** **K: K = 0 { if N <= 25 Failure Cases [refer to Note 04] } or K = N - 25 { if N > 25 Failure Cases }.**
Number of residents who failed in BFD process (Y)	**75**	**During BFD, even after second round, if the action code returned is 04, such resident can't participate in the authentication exercise.**
Total Population Size of the residents with the best fingers (Action Code 00) (P = X - Y)	**4925**	**P: Total population which attempted authentication across all devices (P = A + B + M + N).**

Sr. No.	fdc (dummy)	A	B	N	M	$FRR = \frac{(B+M+K)}{(A+B+M+K)} \times 100$	Verdict
		Auth. Result "y"	Auth. Result 300/"n"	Number of residents could not be authenticated for network failure or other reasons.	FTA Cases		
1	FDC0001001	4822	45	28	30	1.591836735	1.591836735
2	FDC0001002	4898	2	0	25	0.54822335	0.54822335
3	FDC0001003	4876	19	2	28	0.954702417	0.954702417
4	FDC0001004	4870	20	0	35	1.116751269	1.116751269
5	FDC0001005	4871	29	0	25	1.096446701	1.096446701
6	FDC0001006	4840	10	45	30	1.224489796	1.224489796
7	FDC0001007	4859	37	0	29	1.340101523	1.340101523
8	FDC0001008	4725	145	0	55	4.060913706	Device Rejected (FRR > 2%)
9	FDC0001009	4898	5	1	21	0.528025995	0.528025995
10	FDC0001010	4772	100	3	50	3.04754165	Device Rejected (FRR > 2%)
11	FDC0001011	4878	29	0	18	0.954314721	0.954314721
12	FDC0001012	4872	15	4	34	0.995732575	0.995732575
13	FDC0001013	4883	4	0	38	0.852791878	0.852791878
14	FDC0001014	4810	75	0	40	2.335025381	Device Rejected (FRR > 2%)
15	FDC0001015	4894	6	0	25	0.629441624	0.629441624
16	FDC0001016	4869	30	0	26	1.137055838	1.137055838
17	FDC0001017	4785	95	0	45	2.842639594	Device Rejected (FRR > 2%)
18	FDC0001018	4880	12	0	33	0.913705584	0.913705584
19	FDC0001019	4870	18	0	37	1.116751269	1.116751269
20	FDC0001020	4828	35	35	27	1.469387755	1.469387755
21	FDC0001021	4899	4	0	22	0.527918782	0.527918782
22	FDC0001022	4891	10	0	24	0.69035533	0.69035533
23	FDC0001023	4866	22	12	25	0.956645634	0.956645634
24	FDC0001024	4645	195	5	80	5.589430894	Device Rejected (FRR > 2%)
25	FDC0001025	4830	60	0	35	1.92893401	1.92893401
26	FDC0001026	4893	16	0	16	0.649746193	0.649746193
27	FDC0001027	4897	10	0	18	0.568527919	0.568527919
28	FDC0001028	4872	24	4	25	0.995732575	0.995732575
29	FDC0001029	4847	45	0	33	1.583756345	1.583756345
30	FDC0001030	4889	12	0	24	0.730964467	0.730964467


Mock Report
(FRR Field Testing and Device Certification)
FRR %
0
1
2
3
4
5
6
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
FRR % 1.5918 0.5482 0.9547 1.1168 1.0964 1.2245 1.3401 4.0609 0.528 3.0475 0.9543 0.9957 0.8528 2.335 0.6294 1.1371 2.8426 0.9137 1.1168 1.4694 0.5279 0.6904 0.9566 5.5894 1.9289 0.6497 0.5685 0.9957 1.5838 0.731