Testing Methodologies for

Certification of Aadhaar Authentication Devices

(IRIS 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: 10th Oct. 2013, v7.0

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 (Iris Device Make & Model, and Iris Kind 7 IIR Encoder (with version number)) 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 one-two 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 the product meeting the performance objectives stated in the published STQC's biometric device specification document [BDCS(A-I)-03-07; Iris Authentication Device Specification].

* 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 of Content

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.	FAR	False Accept Rate
7.	FRR	False Reject Rate
8.	GNDC	Greater Noida Data Center
9.	HMAC	Hash-based Message Authentication Code
10.	IIR	Iris Image Record
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.	ROC	Receiver Operating Characteristics
19.	STQC	Standardization Testing and Quality Certification Directorate
20.	SSL	Secure Socket layer
21.	UIDAI	Unique Identification Authority of India
22.	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/product is capable of meeting the goals of UIDAI, in context of its performance in a "given specific operational environment" requires an understanding of the standard evaluation methodologies.

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

3.1. Scope

This document defines procedure for performance testing (only FRR (False Rejection Rate)) of participating products for Aadhaar authentication. The scope covers details on FRR estimation of iris authentication devices (from different golden suppliers), logging (at AUA/ASA) and reporting.

3.2. Purpose

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

3.3. Objectives

The primary objectives of the testing process are to:

- standardize the test methods while incorporating best practices.
- 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.
- provide end-to-end understanding to participating suppliers/vendors for designing operational setup for optimal performance during field testing.
- evaluate performance of products from 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 iris devices (and related software modules) for inclusion in the biometric testing. The hardware and software (Iris Device Make & Model, and Iris Kind 7 IIR Encoder) 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/ASA, and then to UIDAI's Production Server.
- Network filter is used (whitelisted 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. UIDAI's Authentication backend (UIDAI's 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 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 Production Server.

6.1.1. Human Test Population

The field test for certification of authentication devices would be carried out on volunteer residents using iris 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%
46-75	26%
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.

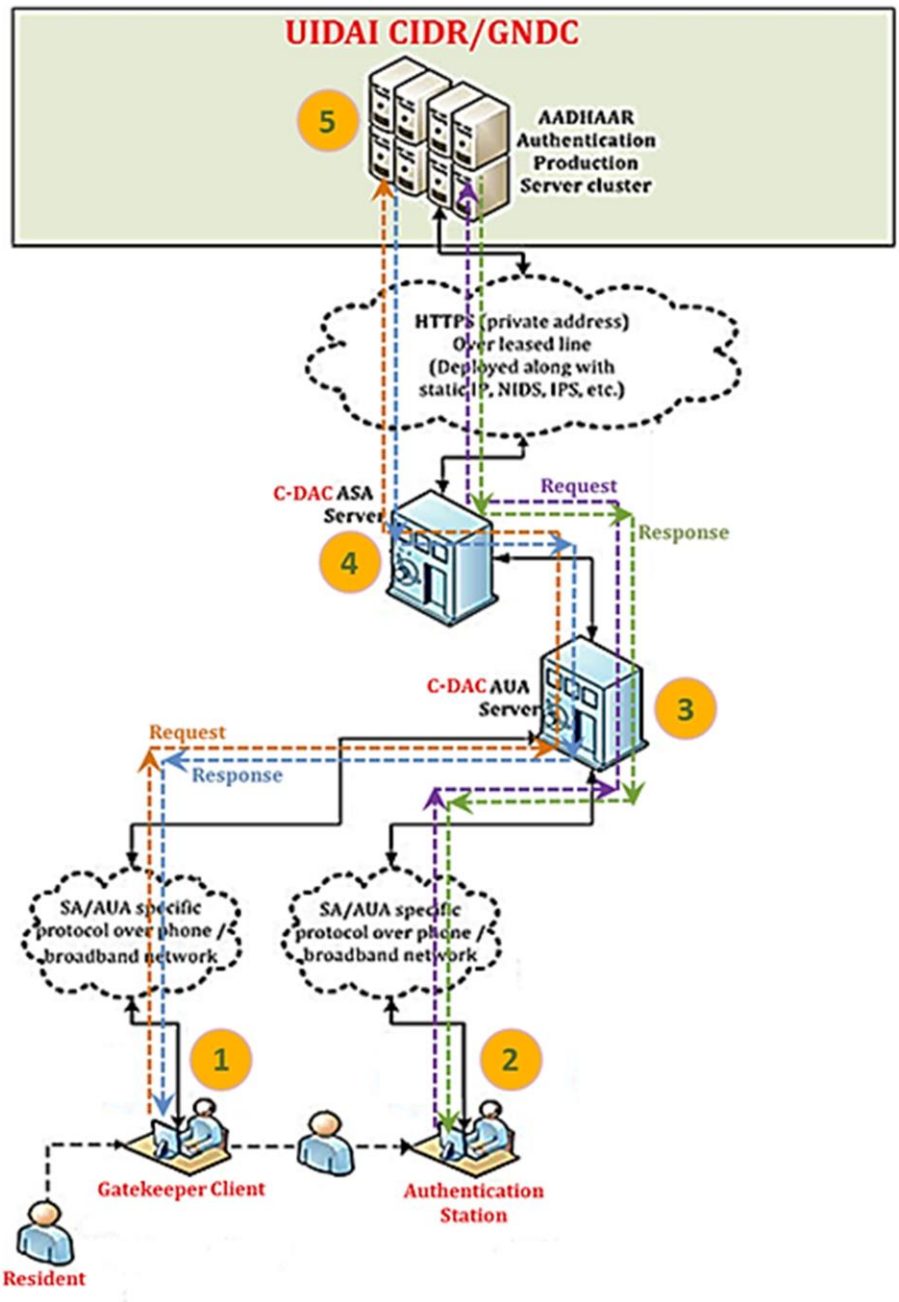


Figure 1: Aadhaar Authentication Setup for Device Certification.

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.

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 5 to 6 authentication lines/rows, where each line will have multiple terminals. Each terminal will house one authentication iris device. So, each line/row will have all the participating products that require FRR testing for certification purposes.

In order to provide a fair environment to all the participating products, the device sequence/placement in different lines would be different, so that no product suffers from unhabituated behavior of the test population.

The authentication line would consist of the following:

- Multiple terminals, where each terminal will house the following:
  - » One iris authentication device.
  - » IIR (Iris Image Record) Kind-7 Encoder – The encoder generates IIR template (in compliance to ISO/IEC 19794-6:2011) from the captured iris image.
  - » The application software (in compliance with the UIDAI's policies and specifications) communicates and transacts 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 from the Aadhaar Card.
  - » A data card. 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 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 resident's IIR template) are all packaged into an Authentication packet [UIDAI, Authentication API v1.6, 2012] along with the header information and sent to the UIDAI's Production Server for authentication through the C-DAC's AUA/ASA network.

AUA's public URL is:
https://sanchar.cdacbangalore.in/auth/0/1.0/0

(https://sanchar.cdacbangalore.in/auth/<first digit of Aadhaar number>/1.0/0)

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

C-DAC as AUA/ASA will connect to the UIDAI's 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 guidance to head towards the respective authentication line.

2) Resident approaches the authentication line. The authentication line comprises multiple terminals (laptops/workstations), where each terminal will house one participating biometric product. Resident provides Aadhaar Number and biometric details to terminal device to get himself/herself authenticated. The resident would need to authenticate himself/herself on each and every participating product (one by one) arranged along a particular authentication line.

3) The authentication process follows the "**Two-iris Authentication Scheme**". The maximum number of authentication attempts per resident per product is 03 per eye (in case of monocular/single Iris Camera). The recommended sequence is: L – R – L – R – L – R (Left Iris–Right Iris–Left Iris–Right Iris–Left Iris–Right Iris). For binocular/dual-eye Iris Cameras, only 03 authentication attempts are permitted. The recommended sequence is: LR – LR – LR (each attempt will generate two separate requests, expected to result in two separate responses). In any attempt, there will always be only one IIR that will remain present in the PID block.

   As per the published Authentication API Specification 1.6, POSH (Position Hint) is a mandatory attribute and two values corresponding to two irises (LEFT_IRIS, RIGHT_IRIS) are permitted. So, iris labeling (specifying the iris 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 Production Server 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.

Note: Every single iris authentication attempt will be checked for KIND 7 Iris Image (IIR). Any authentication attempt with IIR other than KIND 7 will be considered as noncompliant (in this context), and will strictly be treated as REJECTED (NO/NON-MATCH).

6.3. Data Logging @ AUA/ASA (w.r.t. Iris Modality)

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) **idc** *(iris 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)*	**idc** *(iris 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 Rejection 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:

  » Iris Device Make and Model

  » Iris Kind 7 IIR Encoder (with version number)

- **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.

  Please refer to **Annexure C and Annexure D** for more details on "FRR Calculation Process Flow" and "Mock Report".

  » STQC to review the report and give feedback.

  » C-DAC (Biometrics team) to finalize the report and present to STQC for their approval.

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

7. Key Roles and Responsibilities

Table of Content

7.1. STQC

- Specifying terms and conditions to the participating suppliers.
- Allocation of idc to the participating biometric products.
- 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 coordination with AUA/ASA team at the backend.
- 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 AUA/ASA back-end activities.
- Data validation and errors handling at AUA/ASA Server.
- All sorts of data logging: Authentication requests and responses.
- Provide required data to C-DAC Biometrics team for data analysis.

7.3. UIDAI

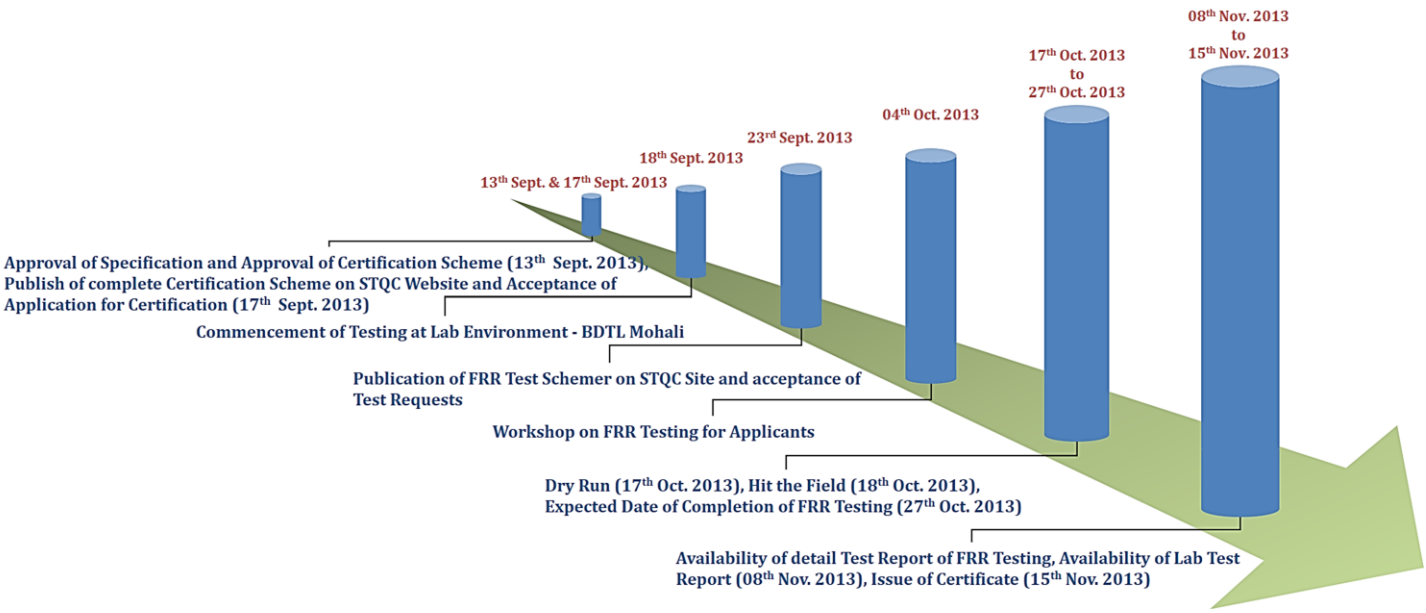
- Provide inputs for the field testing Project Plan and DPR.
- Provide support for monitoring field testing activities, and develop training material for the field level manpower.
- Receive data analysis and report for information & further action as may be necessary.
- Liaise with local administration, 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 iris authentication devices and other supporting hardware (laptop, barcode reader etc.) at assigned authentication lines.
- 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 are directed to the specific authentication devices and able to transact.
- Provide other required support to C-DAC/STQC for carrying out the test.

Note: General **terms and conditions for suppliers** are further specified in **Annexure B**, which may be revised time-to-time (and will be published in the newer versions of this document).

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, 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

5) [BDCS(A-I)-03-07] Iris Authentication Device Specification
http://www.stqc.gov.in/sites/upload_files/stqc/files/Device_specification_BDCS_A-I_-03-07_0.pdf

6) [STQC → Certification]: 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="IIR"/>
        <Meta udc="" idc="" 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
		idc	As assigned by STQC	Supplier	Iris device code. This is a unique code assigned to the product. The code will be provided by the 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. Terms and Conditions for Suppliers

1. The participating suppliers will have to bring their terminals, authentication devices, IIR encoder (and other related routines in SDK), the application software (in compliance with the UIDAI's policies and specifications) etc., to communicate and transact the data with AUA/ASA server.

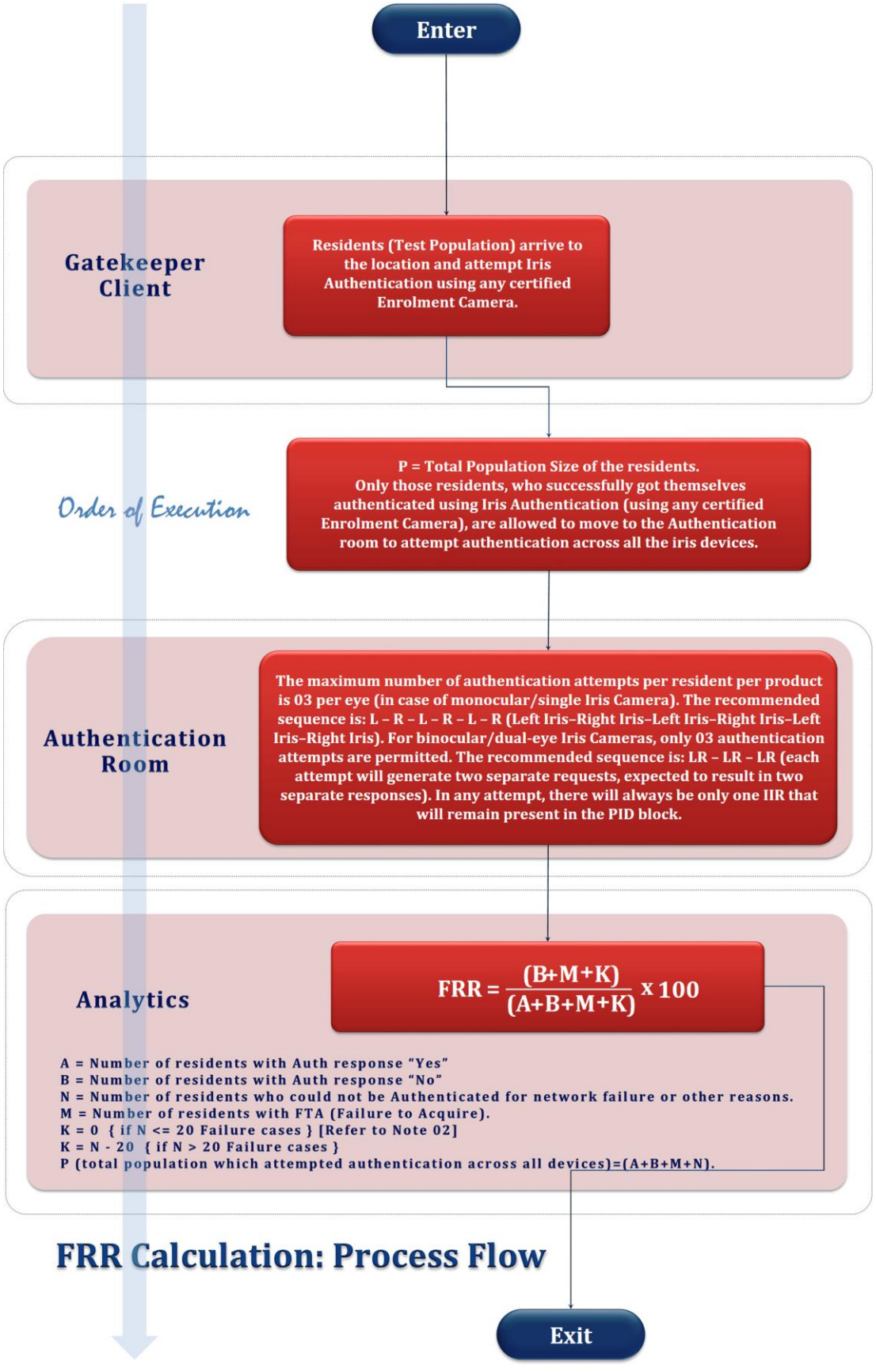
2. It is the sole responsibility of the suppliers to bring all the needed hardware, software and manpower to ensure smooth functioning of devices deployed by them.

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 line transact on the corresponding device deployed by the respective suppliers.

Annexure C. FRR Calculation: Process Flow



Notes

Note-1. In case a particular resident's iris 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's irises are not captured by the device after the repeated attempts (as per the policy in sec. 6.2 (3)), 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 20 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 D. 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 (Iris Devices)

Test Population Size arrived to the location and attempted Iris Authentication using any certified Enrolment Camera (X)	**4000**	**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 <= 20 Failure Cases [refer to Note 02] } or K = N - 20 { if N > 20 Failure Cases }.**
Number of residents who failed Iris Authentication using any certified Enrolment Camera (Y)	**75**	
Total Population Size of the residents (P = X - Y)	**3925**	**P: Total population which attempted authentication across all devices (P = A + B + M + N).**

Sr. No.	idc (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	IDC0001001	3862	15	28	20	1.101152369	Device Rejected (FRR >= 1%)
2	IDC0001002	3908	2	0	15	0.433121019	0.433121019
3	IDC0001003	3893	12	2	18	0.764720877	0.764720877
4	IDC0001004	3880	20	0	25	1.146496815	Device Rejected (FRR >= 1%)
5	IDC0001005	3881	29	0	15	1.121019108	Device Rejected (FRR >= 1%)
6	IDC0001006	3879	10	16	20	0.767459708	0.767459708
7	IDC0001007	3869	37	0	19	1.426751592	Device Rejected (FRR >= 1%)
8	IDC0001008	3865	25	0	35	1.52866242	Device Rejected (FRR >= 1%)
9	IDC0001009	3912	1	1	11	0.305810398	0.305810398
10	IDC0001010	3873	22	3	27	1.24936257	Device Rejected (FRR >= 1%)
11	IDC0001011	3888	29	0	8	0.942675159	0.942675159
12	IDC0001012	3882	15	4	24	0.994644223	0.994644223
13	IDC0001013	3893	4	0	28	0.815286624	0.815286624
14	IDC0001014	3891	14	0	20	0.866242038	0.866242038
15	IDC0001015	3904	6	0	15	0.535031847	0.535031847
16	IDC0001016	3891	18	0	16	0.866242038	0.866242038
17	IDC0001017	3877	26	0	22	1.222929936	Device Rejected (FRR >= 1%)
18	IDC0001018	3911	2	0	12	0.356687898	0.356687898
19	IDC0001019	3902	9	0	14	0.585987261	0.585987261
20	IDC0001020	3850	23	35	17	1.408450704	Device Rejected (FRR >= 1%)
21	IDC0001021	3911	2	0	12	0.356687898	0.356687898
22	IDC0001022	3901	10	0	14	0.611464968	0.611464968
23	IDC0001023	3893	5	12	15	0.51111679	0.51111679
24	IDC0001024	3876	18	5	26	1.12244898	Device Rejected (FRR >= 1%)
25	IDC0001025	3891	14	0	20	0.866242038	0.866242038
26	IDC0001026	3912	7	0	6	0.331210191	0.331210191
27	IDC0001027	3914	3	0	8	0.280254777	0.280254777
28	IDC0001028	3898	8	4	15	0.586585055	0.586585055
29	IDC0001029	3894	16	0	15	0.789808917	0.789808917
30	IDC0001030	3895	6	0	24	0.76433121	0.76433121

Notes:

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

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

b. Network error or other system related errors - When residents are not able to attempt authentication due to the network or other auth. station/device related issues, 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".

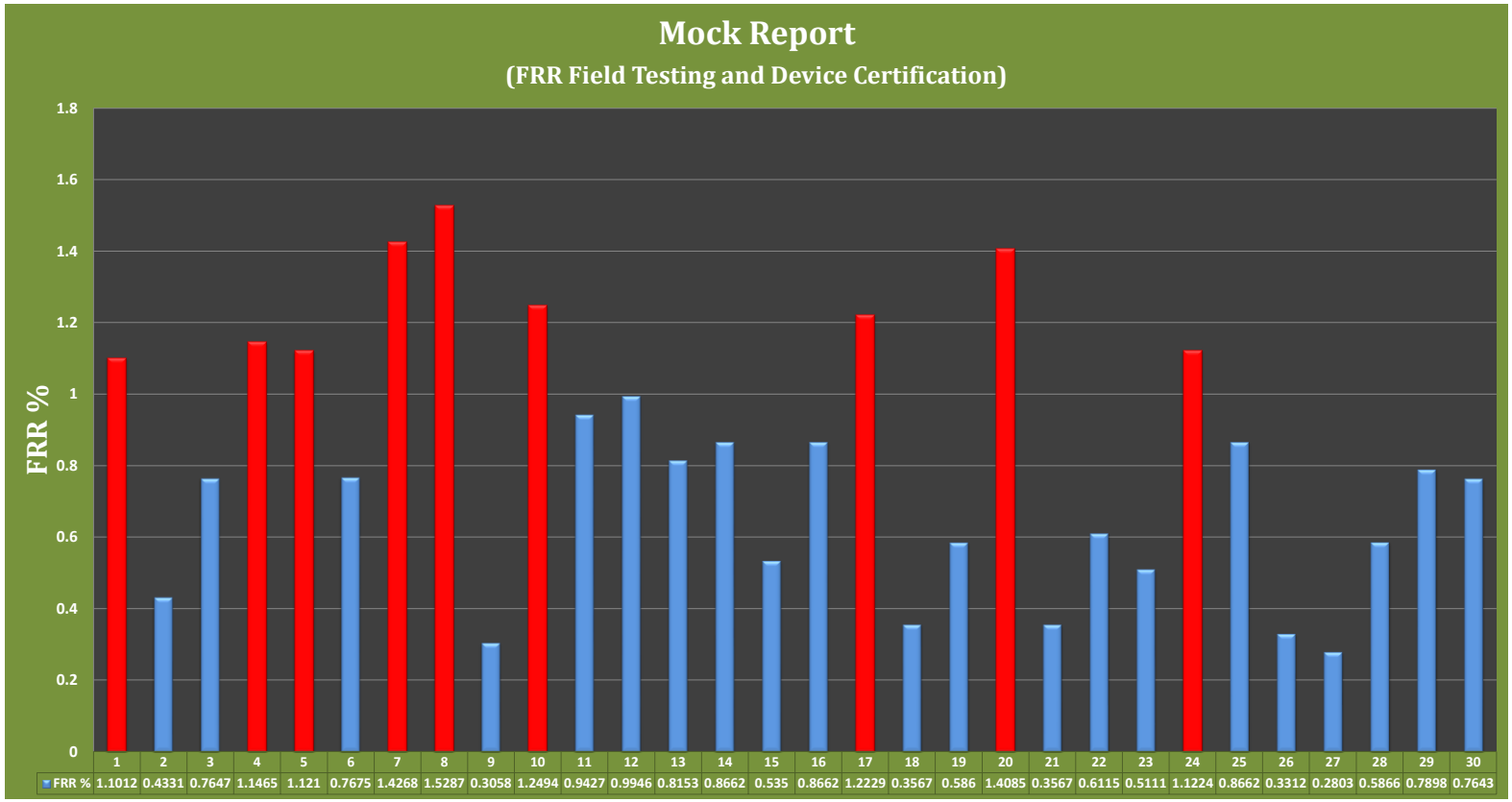
All the FTA cases and network errors or other device related errors have to be recorded by the respective supervisors. In case, if any supplier fails to intimate these errors to the supervisor, all the balance cases from total population which were not recorded in the UIDAI authentication backend logs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

Note-2: All suppliers are provided with a grace of 20 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 auth. room midway during the device authentication process, then the resident's Aadhaar number is eliminated for FRR calculation for all participating suppliers.

Mock Report

(FRR Field Testing and Device Certification)



	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 %	1.1012	0.4331	0.7647	1.1465	1.121	0.7675	1.4268	1.5287	0.3058	1.2494	0.9427	0.9946	0.8153	0.8662	0.535	0.8662	1.2229	0.3567	0.586	1.4085	0.3567	0.6115	0.5111	1.1224	0.8662	0.3312	0.2803	0.5866	0.7898	0.7643