UIDAI

**Unique Identification Authority of India**
Planning Commission, Govt. of India (GoI),
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

# Role of Biometric Technology in Aadhaar Authentication

## KIND-7 IRIS Authentication Accuracy – PoC Report

**May 2013**

# Executive Summary

UIDAI has collected iris images of residents during enrollment, and successfully leveraged iris modality for de-duplication. As recommended in the previous PoC study on Iris feasibility for authentication, a new PoC was conducted to study the feasibility of using KIND7 iris images for on-line biometric authentication in the indian context. The findings of this study are presented in this report.

This report covers the design framework, field implementation, data collection and analysis. It interprets empirical results to assess effectiveness of iris technology, authentication processes and devices. It concludes with a set of recommendations for authentication process and device ecosystem.

Figure 1 Poster inviting residents for iris auth PoC exercise

Similar to last PoC (IRIS, 2012)Assessment of iris feasibility can be further divided into

1. Coverage: Can residents use iris with KIND7 images efficiently and conveniently for Aadhaar authentication?
2. Accuracy: How accurately can KIND7 iris image format authenticate a resident?
3. Device readiness: Are there commercially available devices capable of performing authentication using images?
4. System readiness: Is the entire authentication system ready for performing iris authentication using KIND7 images?

**Study Process**: PoC was conducted in a manner similar to the previous study (IRIS, 2012).

## Feasibility of KIND7 Iris for -line Authentication

The empirical results clearly demonstrate KIND7 iris images of size over 2.5KB is viable in Indian context for online authentication.

| Accuracy | Kind 2 | KIND7 ( Size ~1.5KB) | KIND7 (Size ~ 2.5KB) | KIND7 ( Size ~ 3.5KB) | KIND7 ( Size ~ 5KB) |
|---|---|---|---|---|---|
| True Accept rate* | *99.30%* | *97.93%* | *99.13%* | *99.53%* | *99.36%* |

*100-(FTC+FRR)

**Device Readiness**: **Six** different devices with a variety of form and function are available to form competitive vendor eco-system.

**System Readiness**: Median time for end-to-end authentication was little over **one minute** over shared internet in urban setting.

Residents with aadhaar number were asked to participate in the test. During the scenario test, each resident was authenticated on-line on nine cameras. Extensive logs were generated for off-line analysis. During the analysis, the data was first reviewed and cleansed of exceptions and anomalies. All statistics reported in this report were generated in UIDAI's Technology center in Bangalore.

Figure 2 PoC9 and PoC10 locations

**Set-up:** The PoC was conducted in urban setting at centers in East Delhi district between April 5th and April 12th 2013. The PoC centers were designed to resemble expected ground reality. The PoC was conducted in real field conditions and not in lab environment.

In scenario testing, 101663 online authentication transactions were performed by residents on a shared broadband line. The online authentications were performed on using internet connectivity offered by local internet service provider. All the cameras used in the PoC studies were obtained through an Expression of Interest (EOI) tender. In all, 131863 iris images were capture during this process.

Iris PoC was carried out using the Aadhaar authentication system described in an earlier report (IRIS, 2012).

**Results**

PoC was conducted to obtain samples that demographically represent Indian population. At the end, the samples used have a slight over representation of children (between 5 and 15 years) and women. They under-represent of seniors (above 65 years) as compared to Aadhaar enrollment data.

**Coverage**: The coverage achieved by iris authentication was high, demonstrating the potential of iris to be an inclusive modality. Out of 5,200 residents, three residents were not able to use any of the eight cameras, and 4 additional residents could not use four or more cameras. Thus, there is no inherent technical or physiological limitation to using iris for authentication.

**Accuracy:** Table 1 show the True Accept Rate (TAR) for different authentication modes with three attempts averaged over six "good" cameras when KIND7 images of 2.5KB are used The data shows that, high accuracy can be obtained using both single and dual eye cameras. In summary, False Reject Rate (FRR) of less than 0.5% is achievable with single eye cameras and little over 1% with dual eye cameras whenever two irises are matched. Note, the accept rates shown below includes rejects as well as failure to capture cases.

| Authentication Mode | Single eye camera | Dual eye camera |
|---|---|---|
| 1 attempt authentication | 95.80*% | Not Applicable |
| Multiple attempt (max 6) authentication | 99.57*% | 98.98*% |

*100-(FTC+FRR)

Table 1: True Accept Rate at FAR 1 $e^{-5}$

**Accuracy insight and conclusions:**

a) Manual inspection of iris images provided insight into the root cause of failure to capture and false rejects cases. Excessive compression and improper segmentations were identified as primary reasons for failure. High quality capture coupled with right segmentation/compression methods are key for successful authentication using KIND7.
b) The data shows that high accuracy can be obtained using both single eye and dual eye cameras. Performing up to three attempts to capture the iris improves the TAR for both single and dual iris camera. Images compressed more, benefit more from the attempts. This may be attributed to improved capture quality during second and third attempts
c) Two iris authentication shows material improvement over one iris authentication. This implies, authentication of both eyes as against any one eye of an individual shows material improvement in TAR. When 1st attempt fails, accuracy improvements are realized by trying 2nd attempt with a different eye instead of the same eye again. Hence incorporating the authentication sequence involving right eye-left eye up to three attempts for each eye is likely to result in authentication success for most residents.

**Device readiness:** The cameras are available and performing at required level. Satisfactory performance of six cameras supplied by OEMs based in several different countries will assure competitive vendor eco-system. Key variables determining effectiveness of a camera are

a. Single eye and dual eye capture: Five single eye cameras and four dual eye were tested. Both single eye and dual eye devices were found suitable for iris authentication.
b. Capture aid: As observed during previous PoC, various physical and optical aids were utilized by different cameras. Cam eras with visual indications on the camera for capture process, eye alignment, actionable feedback and capture completion were materially easier to use.
c. When KIND7 images are used for authentication, focus on capturing high quality images coupled with right segmentation and compression at the device is likely to result in higher authentication rates.

All participating camera vendors were asked to supply IRIS segmentation SDK which produces image in formats KIND 1, 2, and 7 (also known as Uncropped, VGA, Cropped and Cropped & Masked respectively) compliant to ISO 19794-6 standard, 9 of 11 device vendors provided software in compliance to API specifications published for the purpose of PoC. Software process was very similar to one followed during PoC9. In addition to providing drivers for the app, devices vendors provided support for KIND1, compressed KIND2 (15KB), KIND7 image format in compliance to ISO 2011 (ISO, 2011) specifications

Very similar to previous PoC findings, there was a difference in performance of different cameras. In each category of single and dual eye cameras, one camera was an outlier compared to median performance of the group. For example, one camera demonstrated a failure to capture (FTC) rate of about 4.28% when the median of peer cameras was below 0.5%. Some of the outliers were also judged to be more difficult to use in the field and were not considered in accuracy analysis. In all, six cameras were considered for accuracy analysis. Furthermore, by developing and providing training to use the devices, FTC rates can be reduced and ease of handling and using can be improved for all devices.

**System readiness:** The overall system behaved reliably and conveniently for both resident and operators. Two important metrics measure user friendliness of the iris based authentication.

a. Authentication time. Using Internet connectivity provided by local service provider in urban setting, median time across all devices was little over one minute. Authentication time is defined as time taken to complete full transaction including capture of two irises, local image quality check, operator review, transmission, backend processing and authentication response.
b. Round trip time: Median round trip was less than 2 seconds.

Previous PoC demonstrated that the current setup is capable of supporting sustained fingerprint authentication speeds of one million per hour. It has been demonstrated repeatedly in the literature that iris matcher is more efficient than fingerprint matcher. Therefore no independent tests were performed using iris matcher. Based on published data, it is safe to state that Aadhaar is capable of sustaining iris authentication rate of over one million per hour.

**Recommendations and next steps**

The empirical results clearly demonstrate iris authentication to be viable in Indian context with KIND7 images of size over 2.5KB. With current level of device readiness for iris capture, it is capable of achieving authentication accuracy of above 99.5% using two irises and up to three attempts. Suggestions made in this document for the vendors, once implemented, will improve the rates further. KIND7 image in addition to accuracy, provide small sized images (above 2.5KB) which will help use iris authentication over low bandwidth networks. The overall systems – network and software - have shown to meet desired requirements in real life condition. Finally, six different devices with variety of form and function are available to provide competitive vendor eco-system.

The PoC also provided a number of insights that could further improve performance of device and system. Four key improvements are

a. Capture quality, segmentation and compression are key for achieving high level of accuracy in authentication. Device vendors must strive to further improve algorithms for delivering high levels of accuracy.
b. Dual iris camera vendors can improve the capture process to reduce FTC by developing capability to capture eyes sequentially, one eye at a time. This will help improve coverage for dual iris cameras as well as improve ease of use during the capture process by improving capture efficiency.
c. Ergonomics and capture aids continue to play key role in quality and ease of use. Several ergonomic improvements in device design to aid in easier and more accurate capture. These cover visual aids for proper placement of camera and appropriate visible light source inside certain types of camera.
d. Capture and segmentation efficiency –During the PoC, the segmentation software was used on laptops. It is important to optimize the algorithms to run efficiently on small form factor devices such as POS terminals, in order to provide quick capture and segmentation for producing KIND 7.

It is recommended that UIDAI and STQC specify iris authentication device specifications and define rigorous certification process based on the findings of the report.

**Abbreviations**

| | |
|---|---|
| API | Application Programming Interface |
| ASA | Authentication Service Agency |
| AUA | Authentication User Agency |
| EOI | Expression of Interest |
| CIDR | Central Identity Data Repository |
| DET | Detection Error Tradeoff |
| NIST | National Institute of Standards and Technologies |
| IREX | Iris Exchange |
| FAR | False Accept Rate |
| FRR | False Reject Rate |
| FTC | Failure to Capture |
| IEC | Information, Education and Communication |
| KYC | Know Your Customer |
| PDS | Public Distribution System |
| PoC | Proof of Concept |
| SDK | Software Development Kit |
| STQC | Standardisation Testing and Quality Certification Directorate |
| TAR | True Accept Rate (1 – FAR) |
| UIDAI | Unique Identification Authority of India |

## Contents

## Figures

## List of tables

# 1 Aadhaar Authentication

The Unique Identification Authority of India (UIDAI) has been created with the mandate of providing a Unique Identity (Aadhaar) to all residents of India. The CIDR processes these enrolments by de-duplicating them to ensure uniqueness and then issues Aadhaar numbers. As of April 2013, nearly 300 million residents have been enrolled in Aadhaar.

One of the mandates given to UIDAI is to define usages and applicability of Aadhaar for delivery of benefit services. The Aadhaar number, which uniquely identifies a resident, will give individuals means to clearly establish their identity to public and private agencies across the country for service delivery. UIDAI provides online authentication using the resident's demographic and biometric information to support Aadhaar-enabled delivery of services.

Aadhaar Authentication is the process wherein, Aadhaar number along with the Aadhaar holder's personal identity data is securely submitted to the CIDR for matching, following which the CIDR verifies the correctness thereof on the basis of the match with the Aadhaar holder's identity information available with it. To protect resident's privacy, Aadhaar Authentication service responds only with a "Yes/No" and no Personal Identity Information (PII) is returned as part of the response.

Aadhaar Authentication supports several different types of authentication through a combination of demographic fields, biometric fields as well as other methods such as one-time-password (OTP). In case of iris, the CIDR server supports authentication of iris images compliant with ISO standard that ensures vendor neutral, open format.

For further information on Aadhaar authentication system, please refer to (UIDAI, 2012).

This study builds on previous iris authentication feasibility study (IRIS, 2012) and further analyzes the feasibility of using small sized iris images for authentication.

# 2 Objective

UIDAI has successfully leveraged iris modality in enrollment and has collected iris images of the resident during enrollment. Iris is used for biometric de-duplication.

UIDAI conducted a proof of concept exercise (PoC 9) involving IRIS technology and published the findings. The report (IRIS, 2012) concluded that up to 99.21% in case of single eye cameras and up to 99.40% of residents using dual eye cameras could be reliably authenticated. During the PoC, compressed KIND 2 images were used for authentication. KIND7, a smaller image standard (ISO, 2011) would reduce network load and was recommended for authentication by NIST in their studies[1]. The Iris biometric authentication report also recommended that online authentication use smaller size KIND 7 image format (also known as Cropped and Masked). This study will analyse the accuracy and field usage characteristics of KIND 7 images.

KIND 7 image format provides the following two benefits:

a. Image size of 2 to 5KB instead of >15KB using other formats. In a mobile network based application, it can reduce the need for high network bandwidth and improve throughput.
b. Previously published reports (P. Grother, 2009) did not detect any perceivable reduction in matching accuracy.

Second Iris Authentication Accuracy Study aims to answer the following *four* questions.

1. Readiness of the device vendor to provide interoperable iris image in KIND 7 format.
2. Authentication accuracy of different image sizes possible under KIND 7 format compared with the baseline case of KIND 2.
3. Improvement in transaction time due to reduced packet size.
4. System readiness: overall readiness of system including reliability.

The results of above goals will be used to further tune Iris Device certification specifications and determine the usage specifications of iris authentication in the field.

To achieve the goal, it is necessary to conduct rigorous field tests on sample population and to measure feasibility in four areas:

A. **Coverage** indicates the percentage of the population that is able to conveniently and efficiently utilize iris authentication. For any system to be utilized for large scale benefit delivery, ease of use and speed of verification are also key measure of the overall coverage.
B. **Accuracy** measures percentage of time, system is able to authenticate genuine resident, while rejecting attempt by imposter.
C. **System readiness** covers overall response time with particular emphasis on authentication time, network latency, reliability, stability and ease of deployment
D. **Device readiness** measures individual device's ability to perform above three factors reliably. Particular attention was given to understand different device characteristics and develop recommendation for enhancing device performance.

[1] IREX I, Performance of IRIS recognition algorithm on standard images, NIST Interagency Report 7629.

# 3 Design and Field Implementation

## 3.1 Introduction to PoC studies

There have been few studies regarding biometric authentication in the Indian field context and it was important to conduct rigorous PoC studies in order to design and configure the UIDAI authentication system. A number of such PoC studies have been carried out, each building on the learning from the previous ones. This chapter describes the design and setup for this study.


Figure 3 PoC Center at East Delhi

Continuing the methodology used in the previous study (UIDAI, 2012) (IRIS, 2012),the iris PoC tests various parameters using (ISO, 2005), which provides the following definitions:

> *Scenario evaluation is an online evaluation of end-to-end system performance in a prototype or simulated application. The utility of scenario testing stems from the inclusion of human-sensor acquisition interaction in conjunction with the enrolment and recognition processes, whose benefits include the following:*
> - *Ability to gauge impact of additional attempts and transactions.*
> - *Ability to collect throughput results for resident authentication.*

And

> *Technology evaluation is the offline evaluation of one or more devices and algorithms for the same biometric modality using a corpus of samples. The utility of technology testing stems from its separation of the human-sensor acquisition interaction and the recognition process. It allows for varying different parameters to re-run the same sample image* [ISO 19795-2, 2007].

The tests in the iris PoC have been instrumented to collect sufficient data to conduct both a specific scenario evaluation and follow on technology evaluation in future.

# 4 Background

The IRIS authentication PoC (IRIS, 2012) analysis concluded that

1. Accuracy: Table 2 shows the True Accept Rate (TAR) for different authentication modes with two attempts averaged over six "good" cameras. The data shows that high accuracy can be obtained using both single and dual eye cameras. In summary, False Reject Rate (FRR) of less than 0.5% is achievable whenever two irises are matched on single or dual eye cameras.

| Authentication Mode | Single eye camera | Dual eye camera |
|---|---|---|
| One iris authentication | 96.21% | Not Applicable |
| Two irises authentication | 99.54% | 99.73% |

Table 2: Single Eye and Dual Eye TAR at FAR = $1e^{-5}$.

2. All participating camera vendors were asked to supply IRIS segmentation SDK which produces image in formats KIND 1, 2, 3 and 7 (also known as Uncropped, VGA, Cropped and Cropped &

Masked respectively) compliant to ISO 19794-6 standard [ISO 19794-6, 2011]. The camera vendors provided predominantly only two formats, KIND 1 and KIND 2. The image size is a dominant factor in network latency for mobile networks. While this PoC used KIND 2 compressed image of size 15 KB, use of KIND 7 would have reduced it to 2 to 5KB resulting in speedier authentications.

3. **System readiness:** The overall system behaved reliably and conveniently for both resident and operators. A few cases of system failure were observed. Two important metrics measure user friendliness of the iris based authentication.
    - Authentication time. Using a GPRS based semi-rural network, median time across all devices was less than one minute. Authentication time is defined as time taken to complete full transaction including capture of two irises, local image quality check, operator review, transmission, backend processing and authentication response.
    - Round trip time. Less than a quarter of the authentication cycle was transmission and backend matching time. Median round trip was less than 10 seconds, while only 7.8% of transactions took more than 15 seconds.
4. The study recommended device vendors to support KIND 7 image.
5. The study observed several ergonomic improvements in device design to aid in easier and accurate capture. These cover visual aids for proper placement of camera and appropriate visible light source inside certain types of camera.

## 4.1 Iris Authentication Concepts

Prior to presenting the authentication accuracy results, terms used in this document are defined below.

1. Session: Visit. This PoC uses only one session. Residents, who were enrolled earlier, were matched against enrolled data. Enrolments had been carried out roughly over one year earlier.
2. Sample: User's biometric measures as output by the data capture subsystem. For e.g., face image, fingerprint image and iris image are samples.
3. Presentation: Submission of a single biometric sample on the part of a user. It may also be referred to as impression. On single eye camera, each presentation may generate one image. One presentation of two eye iris camera generates two images. In this PoC, every presentation that results in captured image is considered an attempt.
4. Attempt: Submission of one (or a sequence of) biometric samples to the system after it has passed quality check. NOTE: An attempt results in a template and can be used to generate a matching score. There is a slight difference between ISO definition of attempt and PoC attempt. PoC attempt is after quality check. A failure to acquire due to missing iris or inability to even register image on scanner does not result in an attempt.
5. False reject rate (FRR): Proportion of verification transactions with truthful claims of identity that are incorrectly denied. All data collected from the field includes an operator-set flag for the expected response (the Ground Truth). Based on this, all 'true' authentication transactions are rerun in the lab and the matching scores recorded. This allowed capture of the false reject rate for a particular threshold.
6. False accept rate (FAR): Proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed. Expected false requests are created by pairing biometric data

collected from the field with an Aadhaar number other than the original Aadhaar holder (imposter requests). A large number of these requests are rerun and matching scores recorded. This allows capture of the false accept rate for several thresholds. As many false requests as necessary are created to provide statistically significant results.

Figure 4 Iris capture using single iris camera

7. Failure-to-capture (FTC) includes:
    - Attempts where the biometric characteristic cannot be captured;
    - Attempts where the raw sample was not acquired or did not meet quality thresholds are not processed by the matching algorithm, and do not generate matching scores.
8. Transaction: Transaction time is defined as entire on-line process of capturing biometric sample, packaging it for on-line submission, communicating to the backend server (CIDR), backend server matching and receiving of the response. It begins when the resident provides his/her Aadhaar number and ends when the response is received.
9. True Accept Rate (TAR): TAR = 1 – (FRR+FTC).

## 4.2 Test Methodology

Continuing the methodology used in PoC 8 and 9, this PoC tests various parameters using ISO 19795 Biometric performance testing and reporting standards. In particular, 19795-2 (ISO, 2005) Testing Methodologies for Technology and Scenario Evaluation covers scenario based testing. The tests in this PoC have been instrumented to generate data for technology test of PoC 9 and conduct new scenario tests. This report primarily focusses on scenario test conducted during the PoC.

The reader is requested to refer to PoC 9 report [UIDAI, Iris, 2012] and ISO 19795-2 (2007) for the detailed description of technology and scenario test methodologies.

### 4.2.1 Scenario Test

The scenario testing will mimic production environment of authentication tests. The resident will be authenticated using backend biometric matching. The device vendors will provide KIND 2 and four different sizes of KIND 7 images for authentication as follows

a. KIND 2 compressed with image size to be around 15KB.
b. KIND 7 compressed with image size not to exceed 1.5KB
c. KIND 7 compressed with image size not to exceed 2.5KB.
d. KIND 7 compressed with image size not to exceed 3.5 KB
e. KIND 7 compressed with image size not to exceed 5KB.

In scenario testing, it is important to measure process parameters such as end-to-end authentication time and number of attempts. The target time for a resident to complete the entire PoC is 10 minutes. In this duration, residents are expected to conduct iris authentication across 10 devices spread over 6 stations.

The data analysis will report

1. Total authentication time for five different image sizes.
2. False reject rate (FRR) of each format at FAR of 1 in 100,000.

Figure 5 Dual Eye camera

In scenario testing, it is important to measure process parameters such as end to end transaction time and number of attempts.

Iris authentication devices come in a variety of flavours and designs. Available models were tested to determine readiness of iris authentication including compliance to ISO specifications, usability, interoperability and performance of the camera. The iris devices were tested for relative performance and to provide input into the final UIDAI iris authentication device specifications to be used for STQC certification.

### 4.2.2 Iris Capture attempts under scenario testing

Iris images were captured using maximum of 3 attempts of up to 3 presentations. All images were captured automatically by the device, without operator forcing the capture.

1. Each successful presentation resulted in image capture. Unsuccessful presentation, where the camera was unable to capture image was still counted as presentation.
2. Each captured presentation was checked for quality using SDK's quality algorithm. If the quality was below acceptable threshold, the image was captured again (i.e., second presentation). The final image was either the first image meeting quality threshold or best image among the three presentations, whichever comes first. Final image was sent to the back end for verification using the chosen mode of communication.
3. If the verification failed, the resident was asked to undergo step 1 & 2 again up to two additional attempts.
4. FTC condition would occur if no image was captured after three attempts and operator was provided an option to mark FTC against the resident Aadhaar number.

**Single eye camera**: Each presentation was defined as image of one eye. Second attempt used different eye from the first. In other words, the recommended multiple attempt sequence was right eye, left eye, right eye. The switching of eyes effectively provides "best finger" strategy for two eyes. Attempts were stopped as soon as any or both iris passed online authentication.

**Dual eye camera**: Each presentation was defined as one image of each eye (two iris images). While other aspect of process was same (3 attempts of 3 presentations each), the maximum number of images captured would be twice that of single eye camera. Dual eye camera is effectively equivalent to using two fingers for authentication in previous studies. If any eye were to pass during the authentication process the process is considered complete.

### 4.2.3 Iris Stations for scenario testing

The residents will authenticate on every iris camera station. Each authentication device undergoing the test is considered one iris station. Two iris cameras were connected to every laptop. Stations were set up in a manner which makes it convenient for the residents to move from device to device in sequence. Residents were scheduled on each station using software program (gatekeeper client) and operators transferred the resident UID numbers from one to next in a sequence for them to

cover all stations in a row. The transfers were triggered once the authentication in the station is completed. The steps followed at each station for each resident is as follows

1. The iris cameras were used in assisted mode i.e., operators were operating the camera.
2. Attempts: Image captured by the camera is considered an attempt. Every captured image will be sent for backend matching. Maximum number of attempts per resident is capped at 3 for dual eye camera and 6 for single eye camera. In other words, maximum number of iris captured and sent for matching is 6 for both single and dual eye cameras.
3. Quality check: Though Quality checking is the responsibility of the vendor and should be performed prior to providing the image to the host application, it was also done by the PoC application. In the event of quality being less than set threshold, additional attempt was conducted to capture again.
4. Image creation. The client software requested a specific type image through the API from the device. In this PoC, for each device, roughly equal number of authentications was carried out using one of the five image sizes (KIND 2 compressed + 4 types of KIND 7). To achieve equal distribution, the client software specified the image size in each instance. In one authentication (i.e. one resident at one station), only one type of image was generated and authenticated.[2]
5. Operators were trained on capture processes and importance of quality and biometric position (left iris, right iris).
6. Matching: The resident is authenticated when match occurs in any attempt. No further biometric capture is done at the station for the resident. In case of dual eye camera, both irises are sent for matching. In case of single eye camera, one iris is sent for matching per attempt.
7. FTC: Even after repeated attempts to capture the resident iris, if the device is unable to capture the iris through auto capture methods, FTC is recorded when the maximum time is reached.
8. If a resident is unable to authenticate at the station, the resident is not excluded from going to other authentication stations.
9. All residents were queued through a purpose built software program so they can authenticate at all stations. This was managed through tracking software where a resident visiting a particular station is marked as “visited” and was routed to next station in sequence. This also helped to reduce operator error while entering Aadhaar number.

[2] In PoC 9 scenario testing, one resident was authenticated on one of the eight cameras. In contrast, this PoC requires each resident to go through all cameras. However, to fully mimic real life operation, only one type of image format is created during one authentication. Assuming 5,000 residents and five possible formats, average of 1,000 residents will generate one format size per camera. It is unnecessary for the device vendor to generate all formats for each capture. The device’s authentication time will increase if it generates all formats for every capture.

### 4.2.4 PoC Client Application and Data Collection

As part of the PoC client application, to measure different variables and compare/fine-tune

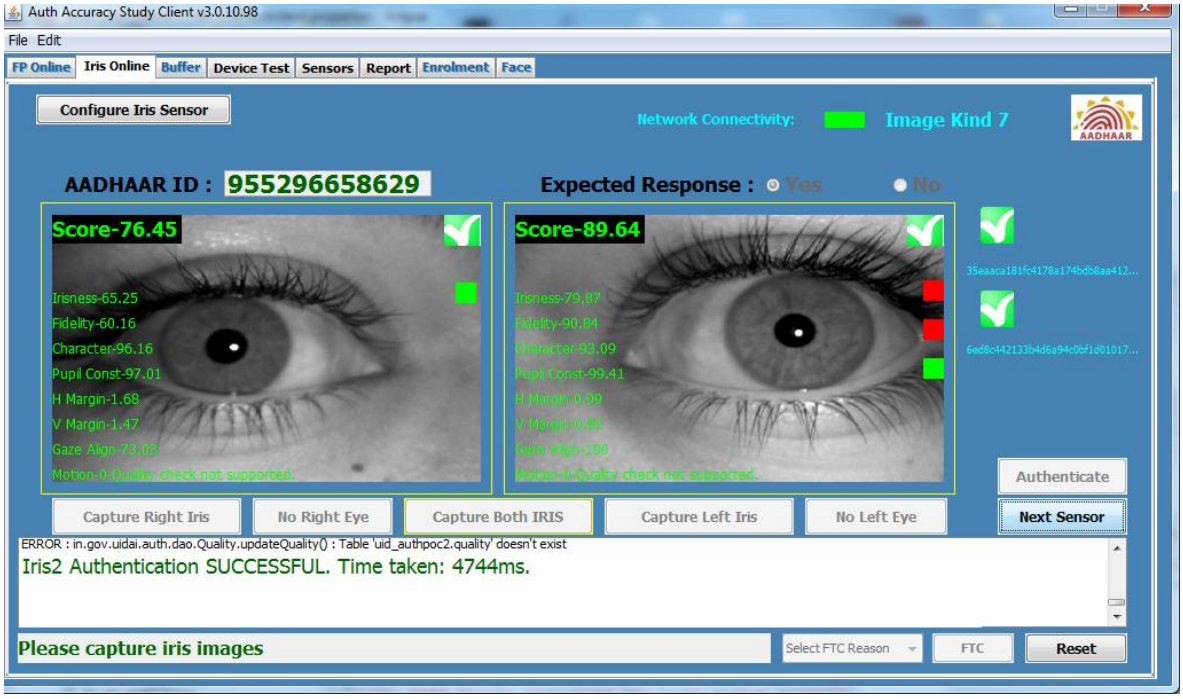


Figure 6 Screen shot of PoC client UI

performance of various SDKs, detailed logs were captured for further analysis. PoC application prominently displayed quality parameters along with captured iris.

### 4.2.5 Vendor Participation

All Iris camera vendors who participated in PoC9 participated in this study. It may be recalled that vendors participating to PoC9 were selected based on EOI. One vendor who could not prepare the device in time for PoC9 was ready this time around and participated in the study. Two vendors who had earlier participated in the study replaced their devices with modified devices based on learning from the previous PoC.

| Items | Number |
|---|---|
| EOI responses received | 11 |
| Number of models ready with H/W and S/W by due date | 9 |
| Number of vendors who provided latest updates to the devices software since PoC9 | 9 |
| Number of OEM participated | 7 |
| Devices modified based on learning's from PoC9 | 2 |

Table 3: Vendor participation statistics

### 4.2.6 Field Setup

Authentication PoC centers were designed to resemble expected ground reality. The PoC was conducted in real field conditions and not in lab environment. Some key considerations for setting up and managing the authentication stations were as follows:

- UIDAI procured all the components and standardized them across all authentication PoC stations – such as laptops, network connectivity, power backup, etc. EOI participants provided cameras and capture software. UIDAI performed initial testing and final software integration with PoC UI.
- Local internet service provider was roped into provide internet connection. This was used for connectivity in order to send authentication requests to CIDR. Wi-Fi routers were used to provide connectivity to individual authentication stations.
- Regular electrical supply available at the PoC location, backed up with UPS/ generators was used for the PoC exercise. Disruptions in the main power supply were noticed during the course of the PoC.
- Sensors were deployed across various stations to provide equal opportunity to all participating device technologies / OEMs, constrained by USB port availability.
- The key consideration was to get each resident to authenticate using all the authentication devices.
- For resident mobilization, residents were requested to participate in the Proof of Concept studies through announcements by local administration.
- Residents who participated in the PoC study were provided with token gift and takeaway apart from snacks.

## 4.3 Resident and operator communication and training

Most of the resident communication materials developed during the previous PoC was reused during this PoC with suitable translation. Additional material such as announcement banners were developed specifically for the PoC. Communication materials include materials to educate the operators and residents to conduct the process as well as do's and don'ts. Banners, Standees were placed in and around the PoC site. Operators were also trained using the same instructions.


Figure 7: IEC material used during PoC

## 4.4 Data Quality & Data Analysis

Data analysis consisted of the following steps:

- Scrutiny of logs from field
- Visually reviewing images to understand errors. Several types of errors were identified and rectified
    - Labeling errors. Wrong demographical information, wrong label of right or left eye

- Enrollment errors. Residents with extremely low quality images, imposter images and missing images. Images that could not be matched due to enrollment errors (8 residents) were identified and not considered in accuracy analysis.
- Segmentation Errors (for KIND 7) – Failed images were analyzed for issues related to segmentation while generating KIND7 images.
- Compression errors (for KIND 7) – In order to generate small sized iris images, vendors were compressing the masked and cropped image. Failed images were checked for presence of compression artifacts.

# 5 Feasibility of using iris for authentication

This section summarizes the following areas from the iris study:

- Demographics of the study participants (scenario test)
- Coverage - Resident population who were able to have their iris captured for authentication
- Accuracy - Matching accuracy using various matchers
- System readiness - Capture time, Network time related characteristics
- Devices readiness and related findings

In scenario testing, 101663 online authentication transactions were performed by residents on a local internet service. In all, 131863 iris images were capture during this process.

## 5.1 Demographic Profile

The demographic profile of participants in the iris study was compared with the profile of residents enrolled in Aadhaar – both nationally as well as within Delhi region. The comparison was done on the basis of participant age bands, as well as gender.

It was found that children in 5-15 years range were slightly over represented in the sample compared to overall Aadhaar enrolment statistics, while senior residents (66+ years) were slightly under represented. Similarly, females were over represented in the study. In contrast, earlier PoC (IRIS, 2012) had fewer children (9%), more senior residents (8%) and adults (83%) compared to PoC10. Similarly, PoC9 had more female residents (55%) and no transgender resident compared to PoC10.

The following charts show the age and gender distribution of all Aadhaar holders nationwide, in Delhi district and participants in the iris PoC.

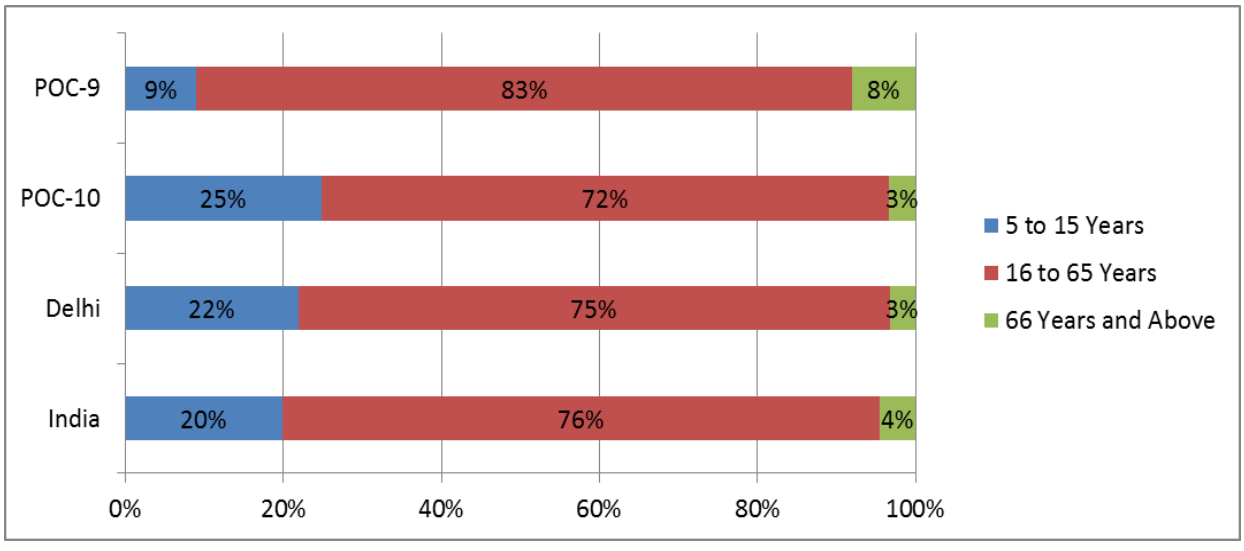


Figure 8: Age distribution of participants in study compared to Aadhaar enrolment

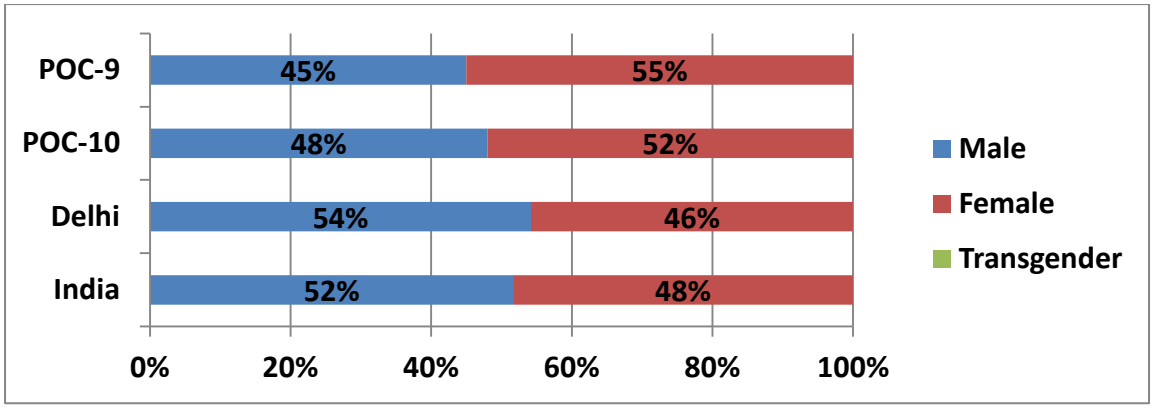


Figure 9: Gender distribution of participants in study compared to Aadhaar enrolment

## 5.2 Coverage

Coverage is primarily measured by failure to capture (FTC) rate. Since devices with different characteristics and quality were utilized, FTC rate over all devices does not accurately measure maturity of iris technology. A new metric that measures inherent technology limitation in capturing iris images in Indian context was also introduced. This measured the number of residents who could not use any device and could not use several devices.

### 5.2.1 Resident coverage across multiple devices

| Resident coverage across 7 cameras | Number of residents | % failure |
|---|---|---|
| Of the total Residents who participated | **5200** | |
| Neither eye could be captured in all cameras | **3** | **0.058%** |
| Only left eye was captured (right eye not captured) | **0** | **0.000%** |
| Only right eye was captured (left eye not captured) | **2** | **0.038%** |
| Failed iris capture on 4 or more cameras | **4** | **0.077%** |

Table 4: Failure to Capture

Two conclusions can be drawn from the statistics:

- PoC9 had reported that the coverage achieved by iris authentication was high, demonstrating the potential of iris to be an inclusive modality. There was no inherent technical or physiological limitation to using iris for authentication. PoC10 confirmed the same findings.
- The observed FTC rate of 0.077% (based on failure across 4 or more cameras - PoC9 reported 0.33%). This indicates that it should be possible for most of the residents to conveniently authenticate using iris. FTC rates were improved from PoC9 which had reported an FTC of 0.33%. However, PoC9 had larger representation of senior residents as compared national average while PoC10 had seniors residents represented more in line with local as well as national average.
- Failure in template generation and segmentation for different KINDs, if any, was included in false reject statistics. FTC was measured with respect to ability of the camera to capture KIND1 image.
- Image KIND and image size is not expected to have any impact on FTC.

### 5.2.2 Failure to Capture (FTC) by Camera

FTC rates are computed by device and can provide another perspective on the capture failure.

| Single Eye Camera | FTC | Dual Eye Camera | FTC |
|---|---|---|---|
| A | 0.09% | F | 1.41% |
| B | 0.02% | G | 0.96% |
| C | 0.04% | H | 4.53% |
| D | 1.6% | I | 0.22% |
| E | 0.13% | | |

Table 5: Camera-wise FTC

The failure to capture (FTC) of individual iris cameras varies widely by camera as shown in Table 5. When compared to median performance of peer devices, camera “D” and camera “H” performed poorly. Furthermore, poor performance of the same two cameras was observed throughout the PoC. These cameras were thus judged to be outlier. All future results, unless explicitly specified exclude these cameras.

## 5.3 Accuracy results from Scenario test

The most common measure of accuracy is True Accept Rate (TAR) and False Accept Rate (FAR). Just like coverage it is instructive to use additional measure, called resident accuracy, to understand behavior of iris technology across cameras.

All biometric matchers require FAR threshold as input to calculate matching score which is used to determine FRR. Accuracy calculations shown below are done using threshold value of 42. Based on the imposter matching, threshold of 42 correspond to FAR of about $1e^{-5}$ or 1 in 1, 00,000. PoC 10 scenario methodology was used during imposter matching. Images collected during PoC9 were used to conduct the imposter matching.

### 5.3.1 Authentication Accuracy based on Image size

Table below highlights the transaction results when different image sizes were used for authentication. The results below does not include duplicate authentication of a resident on the same device. When image size of K7 image was reduced below 1.5KB, the reject rate increased and excess compression was seen as major contributor. However, for image size of about 2.5KB and above, the accept rate was seen closer to KIND2 images (15KB). Further increasing the size beyond 3.5KB was not observed to contribute significant improvements to accept rates. Camera D and H did not operate satisfactorily because they had both usability and capture problems. Camera E's software erroneously compressed images far greater then specified sizes of 1.5, 2.5, 3.5 and 5KB respectively. All three cameras were excluded from further consideration. All data unless explicitly specified show results of remaining 6 cameras. Note that True accept rates sighted in the table considers false reject (FRR) as well as Failure to capture (FTC).

| Accuracy centric statistics | KIND 2 | KIND7 ( Size ~1.5KB) | KIND7 (Size ~ 2.5KB) | KIND7 ( Size ~ 3.5KB) | KIND7 ( Size ~ 5KB) |
|---|---|---|---|---|---|
| Total authentication transactions | **6117** | **5950** | **6125** | **6030** | **6107** |
| Authenticate with Either left or right eye | *6074* | *5827* | *6072* | *5994* | *6068* |
| **True Accept rate*** | ***99.30%*** | ***97.93%*** | ***99.13%*** | ***99.53%*** | ***99.36%*** |

* Results indicated above do not include three cameras D, E and H-* TAR =100-(FTC+FRR)

**Table 6: Transaction-wise Accuracy**

Most of the errors were attributed to excess compression of images in addition to segmentation errors while generating KIND7 images. Good quality capture coupled with correct cropping and masking operation and compression to required levels was seen to contribute to accuracy. It is important to note that resident groups which participated in various groups shown above are different from each other.

### 5.3.2 Device Accuracy

The accuracy of individual iris cameras varied widely. The FRR achieved using up to 3 attempts of both left and right iris (FAR of 1e-5) is shown in table 7 for single eye and dual eye cameras. Compared to median performance of peer groups, three cameras – D, E and H were considered to be outlier.

| Device centric statistics | KIND 2 | KIND7 ( Size ~1.5KB) | KIND7 ( Size ~ 2.5KB) | KIND7 ( Size ~ 3.5KB) | KIND7 ( Size ~ 5KB) |
|---|---|---|---|---|---|
| Single eye Cameras –A | 0.40% | 3.34% | 0.40% | 0.80% | 0.20% |
| B | 0.19% | 1.09% | 0.68% | 0.30% | 0.39% |
| C | 0.60% | 0.72% | 0.70% | 0.10% | 0.40% |
| D | 2.36% | 9.58% | 2.84% | 3.02% | 2.24% |
| E | 0.97% | 30.54% | 2.83% | 1.70% | 1.35% |
| Dual Eye Camera - F | 1.36% | 2.80% | 1.47% | 1.19% | 1.56% |
| G | 1.17% | 2.33% | 1.36% | 0.99% | 1.08% |
| H | 4.28% | 6.18% | 3.69% | 4.49% | 3.53% |
| I | 0.49% | 2.13% | 0.59% | 0.20% | 0.20% |

**Table 7: Camera wise Reject Rates**

Note that the rates shown include failure to capture for each camera.

### 5.3.3 Impact of using two irises and multiple attempts

Single eye camera captures one iris at time. The 3 “good” single eye cameras achieved a true accept rate (TAR) 97.51% in one attempt. This means that 96.21% residents can be authenticated using a single (right) iris capture using KIND 2 images and similarly 95.80% of residents could be authenticated using KIND7 images compressed to about 2.5KB using right iris. For KIND7 images (size 2.5KB), when the other (left) iris is added in matching the percentage of resident successfully authenticating improves to 99.23%, again in single attempt. Capturing both the left and right iris up to three times (three attempt) improves the TAR to 99.57% for KIND7 (size of 2.5KB).

As seen from the table below, there is a significant improvement in the TAR rate, between a single (left) iris capture and both iris capture and TAR improves further by adding more attempts.

| Single Eye Camera | Single Iris TAR | Both Iris 1st Attempt TAR | Both Iris Upto 3 Attempts TAR* |
|---|---|---|---|
| KIND 2 | 97.51% | 99.5% | 99.7% |
| KIND 7(size ~1.5KB) | 89.79% | 96.48% | 98.34% |
| KIND 7(size ~2.5KB) | 95.80% | 99.17% | 99.57% |
| KIND 7(size ~3.5KB) | 95.65% | 99.10% | 99.67% |
| KIND 7(size ~5KB) | 96.31% | 99.21% | 99.7% |

*** Up to six authentication attempts**

**Table 8: Single Eye, both eye TAR for good camera across various image sizes**

Dual eye camera captures both irises at the same time. For KIND7 (size 2.5KB), the "3" good dual iris cameras achieved a TAR of 98.36% was in the first attempt and in up to three attempts, the dual iris capture improved the TAR to 98.98%.

| Dual Eye Camera | Both Iris 1st Attempt TAR | Both Iris 3 Attempts TAR* |
|---|---|---|
| KIND 2 | 98.79%% | 98.98% |
| KIND 7(size ~1.5KB) | 94.8% | 97.6% |
| KIND 7(size ~2.5KB) | 98.36% | 98.98% |
| KIND 7(size ~3.5KB) | 98.80% | 99.2% |
| KIND 7(size ~5KB) | 98.85% | 99.05% |

- multiple attempts (max 6) authentications

**Table 9: Dual eye camera - Good Camera TAR across all image sizes**

Average number of attempts for all good cameras was little over 1. However for KIND7 images of size 1.5KB was more than other KINDs.

| Average number of attempts for successful authentication | KIND 2 | KIND7 ( Size ~1.5KB) | KIND7 ( Size ~ 2.5KB) | KIND7 ( Size ~ 3.5KB) | KIND7 ( Size ~ 5KB) |
|---|---|---|---|---|---|
| Single eye cameras – | 1.037 | 1.098 | 1.048 | 1.056 | 1.044 |
| Dual eye cameras | 1.034 | 1.13 | 1.064 | 1.053 | 1.049 |

**Table 10 Average number of attempts for successful authentication**

The data shows that high accuracy can be obtained using both single eye and dual eye cameras. Performing up to three attempts to capture the iris improves the TAR for both single and dual iris camera. When 1st attempt fails, accuracy improvements are realized by trying 2nd attempt with a different eye instead of the same eye again. Images compressed more benefit more from the attempts. This may be attributed to improved capture quality during second and third attempts. Dual iris camera's overall TAR was impacted by FTC. Treating single eye at a time during the dual capture process is likely to reduce the FTC while using dual iris camera.

### 5.3.4 Matcher Performance

Matcher was updated to support latest ISO specifications (ISO, 2011)in order to support KIND7 image formats. Matcher took about 220ms to complete the matching for most transactions. This was in line with iris KIND2 authentications as observed in the past PoC. Matcher was observed to take more time for KIND2 images as compared to KIND7 images.

**Matching time**

| KIND | Server Processing time(median, ms) |
|---|---|
| 2 | 280 |
| 7( Size < 1.5KB) | 229 |
| 7( Size < 2.5KB) | 229 |
| 7( Size < 3.5KB) | 231 |
| 7( Size < 5KB) | 233 |

Table 11 Matching time

## 5.4 System findings

Besides accuracy and coverage, the third most important factor for feasibility of iris based authentication is system level factors. These factors consist of

- Response time
- Image size used in transmission.
- Matcher speed

The response is measured with two metrics: Resident authentication time and round trip time. Resident authentication time includes time to select the device, enter the Aadhaar number, guiding the resident for correct capture procedure, completing the capture of both eyes, submitting the transaction and receiving response. Round trip time measures the last two parameters of the authentication time during which the resident is waiting for system to respond.

### 5.4.1 Resident Authentication Time

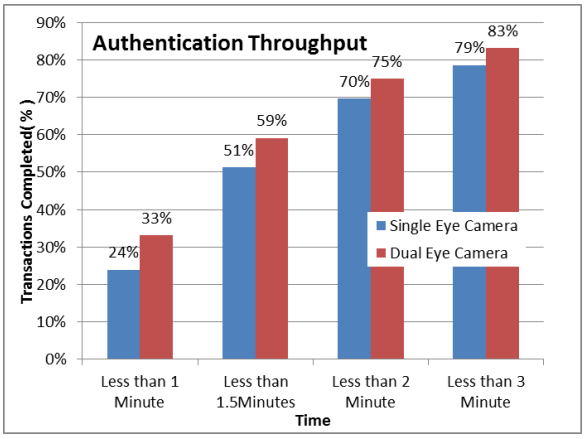


Figure 10 Authentication time

Figure 10 is a histogram of authentication time including single and dual eye cameras. About 50% of residents took more than 1.5Minutes to authenticate. This is in higher than what was observed in the previous PoC (PoC9). This could be attributed to operators starting the auth process using the gatekeeper client before the resident settled down. After Aadhaar number is entered into the tool, there was a wait for resident to settle down. Further training to operators is likely to reduce the total authentication time. In case of single eye devices, one iris is captured at a time whereas in case of dual eye device, both irises are captured at a time. Median time of dual eye capture across all dual eye cameras was 79 seconds whereas for single eye cameras it was 88 seconds. It is higher than reported times during PoC9.

Dual eye cameras were able to complete marginally higher number of authentications compared to single eye cameras.

Further training the operator could help reduce the overall authentication time and improve ease of use and throughput while using iris authentication in the field.

This time distribution also includes the time taken for repeated impressions due to failed quality or failure to capture during the first attempt.

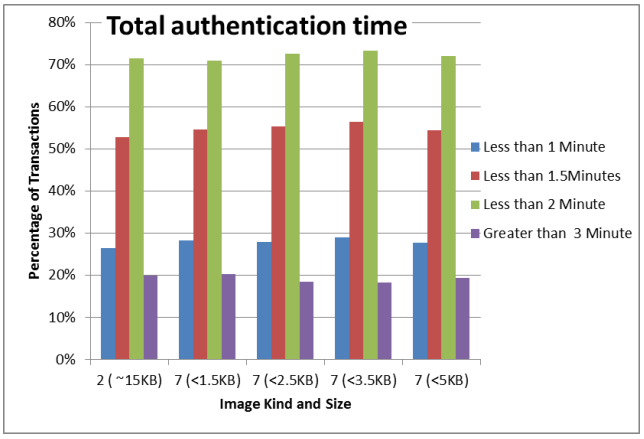


Figure 11 Total Authentication time for different image sizes

Resident Authentication time did not vary with various KIND images used during transactions. Figure 11 shows that there was no major variation when different image sizes were used during authentication transaction.

### 5.4.2 Round trip time

The histogram of round trip time for various sizes of image using the shared broadband network for authentication is shown in figure 13. Over 61% of transactions returned in less than 2 seconds, while less than 6% of transactions took more than 10 seconds.

The network performance can be further improved by smaller image sizes as discussed in the next section.

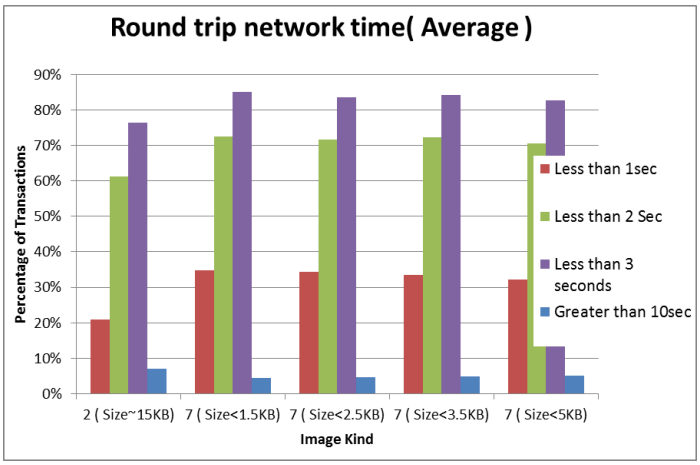


Figure 12 Round trip network time histogram

### 5.4.3 Image size

Scenario testing used KIND 2 image compressed to about 15KB using JPEG 2000 lossy compression techniques. All device vendors were able to provide usable compact formats – KIND 2 and KIND 7 (also called CROPPED and CROPPED AND MASKED).

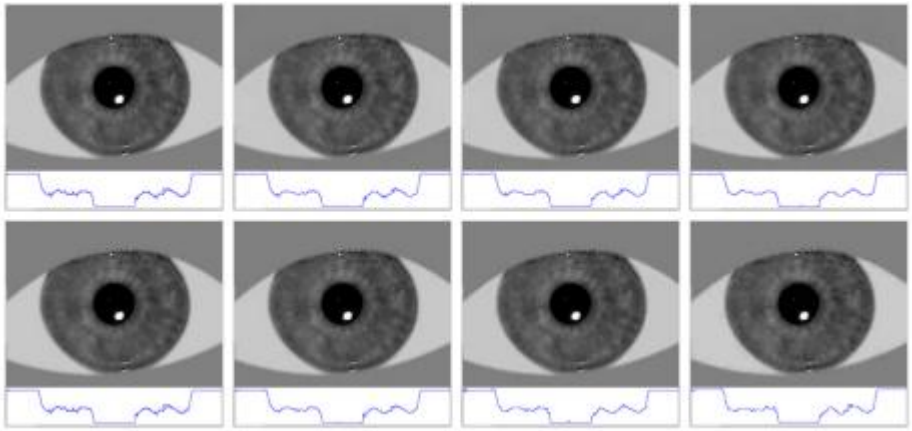

Figure 13 KIND7 Images (Ref: IREX Report)

However vendors varied in terms exact size of KIND7 images required for testing accuracy. Notably, those compressed more than required resulting in image sizes lesser than stipulated for the user group produced more rejects as compared to their peers.

The diagram below shows the image sizes used in this PoC. Refer [ISO 19794-6-2011] for further definitions of image types cited below.

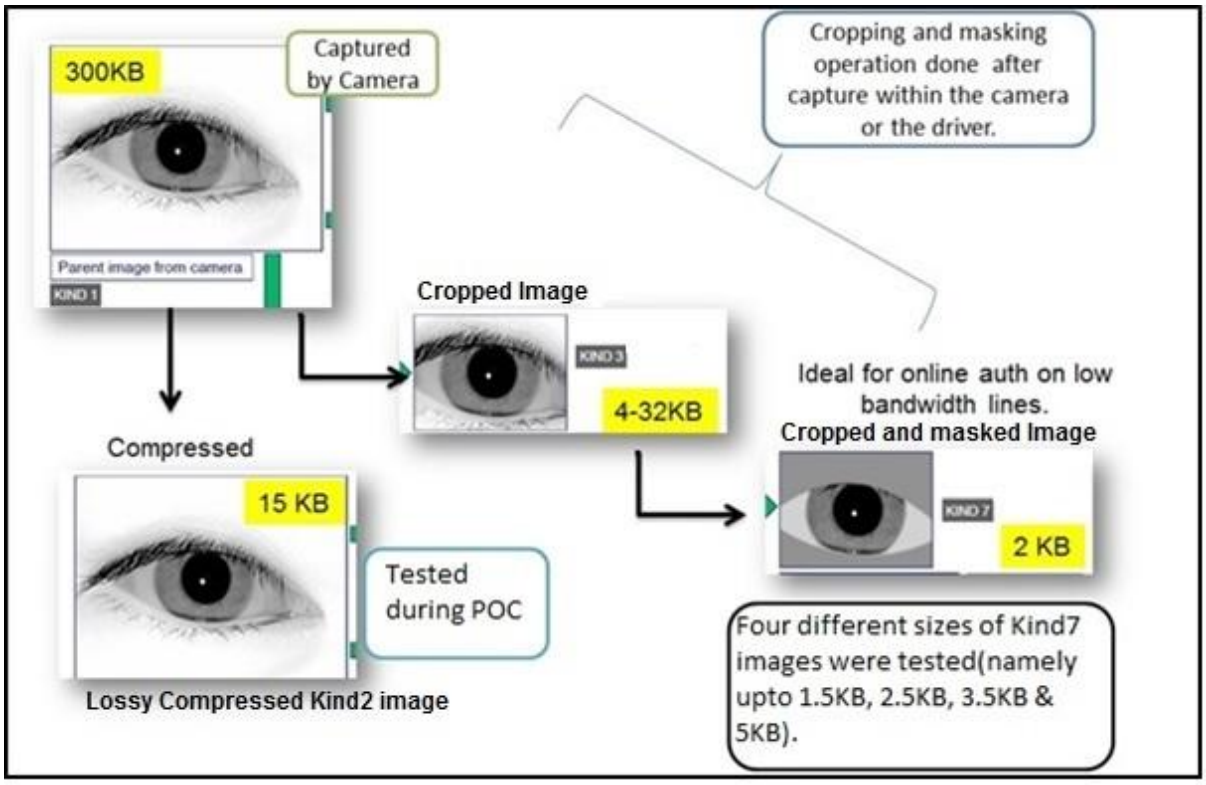


Figure 14 Image Formats

## 5.5 Devices Findings

During the PoC, Five cameras were single eye cameras and four cameras were dual eye cameras. 9 of 11 device vendors provided software in compliance to API specifications published for the purpose of PoC. Software process was very similar to one followed during PoC9. In addition to PoC9 software devices vendors provided support for KIND7 image format in compliance to ISO 2011 specifications

All the devices used during the test, were supplied with rugged casing. No breakages and malfunctioning due to packaging were reported during the PoC.

Devices supported auto capture feature. This enabled devices to automatically capture good quality iris pictures when operator held the device at the specified capture distance from the resident iris.

All devices supported various KIND7 image sizes as required by the PoC. Devices supplied the specified KIND 2 or KIND7 image when requested by the PoC application.


Figure 15 Images of residents participating during PoC

Observations related to device usage, handling process, actionable feedback was very similar to those followed during PoC9. It was observed that during the initial stages, most of the device vendors took about three weeks to achieve ISO compliance for images from the date of testing. Technology testing tool development cycle helped the device vendors to achieve compliance as well as standardize on image sizes required for PoC.

Several device vendors improved the capture algorithms to improve picture quality as well as ease of capture during the capture process. These improvements were more in the single eye category compared to dual eye device category.

Two single iris device vendors improved the device casing completely. These changes which were arrived at as learning from the previous PoC contributed to better handling and ergonomics of capture.

Single iris cameras were relatively easier to handle and capture using auto capture facility. It was observed that the training required to handle a dual iris camera is more than single eye cameras in

order to achieve better capture quality and ease of use. This point pertains to both residents and operators training. It is likely that over repeat usage, ease of use of dual iris cameras may be improve. For other relevant discussions related to single and dual iris cameras, refer to PoC9 report (IRIS, 2012)

Excessive compression (more than required to achieve the stated image size) was seen to contribute significant error rates in one camera. Compressing bad quality iris images was seen contributing more to rejects and hence higher attention being paid to capture quality is more likely to offset any compression related issues in regards to accuracy.

# 6 Observations & Recommendations

In conclusion, a set of observations derived from the analysis of the PoC results and subsequently a list of recommendations that flow from the PoC analysis are presented. These observations are pertaining to specific topics examined in this PoC only. These Observations must be seen in conjunction with observations and recommendations from previous report (IRIS, 2012) for completeness.

## 6.1 Accuracy

It was shown that KIND7 images performed favorably when the image sizes were about 2.5KB and above.

| Accuracy centric statistics | KIND 2 | KIND7 ( Size ~1.5KB) | KIND7 (Size ~ 2.5KB) | KIND7 ( Size ~ 3.5KB) | KIND7 ( Size ~ 5KB) |
|---|---|---|---|---|---|
| True Accept rate* | *99.30%* | *97.93%* | *99.13%* | *99.53%* | *99.36%* |

Table 12: True Accept Rate at FAR = 1e-5.*TAR=100-(FRR+FTC)

Operating at false accept rate of one in 100000, Iris technology also lends itself for highly secure online authentication against imposter attacks. Table 12 shows higher accuracy of authentication being achieved through KIND7 images of size 2.5KB.and above. It was observed that there is a slight degradation in performance when image size was 5KB.Specific investigations is beyond scope of the PoC.

Multiple attempts (up to three) were seen to improve the quality of authentication further.

## 6.2 Device Readiness

All vendors supplied devices with auto capture software as well as ability to support KIND7 image format as per ISO specifications.

There is a variation in authentication accuracy cameras based on capture algorithms, ergonomics and related factors. In the study, it was observed that while most cameras performed well, there were outliers with high FTC and FRR rates. Operator's difficulty in using them correlated with their poor FTC and FRR rates. This observation was in line with previous PoC findings. Improving capture algorithms/quality and ease of capture for residents and operators is key to have good accuracy.

Single eye cameras fared slightly better than dual eye cameras due to higher level of observed FTC with dual eye cameras. Dual eye cameras have the advantage of capturing both eyes simultaneously thus reducing the capture time.

Devices providing capture aids and actionable feedback help operator with faster and better quality capture. The devices which provided effective capture aids and feedback to operator regarding capture process and image quality was seen to achieve very high degree of accuracy. This observation was reinforced during this PoC as well.

It is important to emphasize that the quality of image plays an important role in ensuring authentication accuracy. Devices have incorporated quality measurements within their capture

algorithms to enable auto capture. In addition to the existing parameters, to further improve the quality of capture and minimize number of attempts, algorithms could check for gaze correctness, rotated device, upside down eyes, occlusion, focus, motion blur and special eye conditions. While generating KIND 7 images, cameras with better quality of images were seen to perform better in terms of accuracy in comparison to those with poor quality images.

Since it is expected that iris authentication be available on SFF( small form factor ) devices, capture, quality and segmentation algorithms need to be optimized to be able to provide quick capture while capturing from POS terinam.

## 6.3 System Readiness

The median time to perform end-to-end online authentication was seen about little more than one minute. This was in contrast to less than one minute observed during previous PoC. Operators scheduling the residents into the tool before the resident is ready for capture, contributed to higher authentication time. Further training to operators can reduce the overall authentication time.

It is recommended to use sizes of 2.5KB for KIND7 during the field authentication over mobile broadband networks in order to reduce the latency.

In cases where the broadband connections are available, KIND7 image formats of size over 2.5KB recommended. In cases where KIND7 image formats fail to provide successful authentication after repeated attempts, trying to authenticate with lossy compressed KIND2 images (up to 15KB) is likely to help when the rejects are due to segmentation and compression defects.

## 6.4 Recommendations

1. KIND 7 ( > 2.5KB) performs as well as KIND 2 .Hence it is recommended that KIND 7 images of 2.5KB be treated as baseline for iris authentication when KIND7 images are used.

2. One eye vs. two eyes: Two irises authentication provides significant improvement in accuracy and coverage over one iris. In case of single eye camera, it is recommended to authenticate first with one eye, and only in case of failure, the second eye be used for authentication.

3. Attempts: Up to three attempts are recommended (max of 6 authentication attempts). In line with the previous PoC results, most of the gains were observed within first two attempts. Gains with attempts were more seen with KIND7 images due to compression and segmentation issues associated with low quality images. With further attempts, chances of improvement in quality improve due to resident familiarity apart from other factors.

4. Device Certification: Stringent authentication device testing and certification is recommended to ensure high quality authentication devices are deployed for Aadhaar authentication.

5. Capture aids: Vendors should be asked to provide better capture aid for operator and residents. The study categories three types of aid: actionable feedback, visual aid and “appropriate light source to improve quality of image and finally measures to block ambient light reflections. These improvements detailed in Annexure will reduce capture time, improve accuracy and offer better user experience.

6. Capture quality: It is important to emphasize that quality of image plays important role to ensure authentication accuracy. Devices should make attempt to incorporate specific areas of quality explained in the document along with what is being already being done within the devices to ensure quality.

7. Matcher Setting: It is recommended that in order to offer better robustness and security against imposter attacks, matcher be operated at FAR of 1e-5. It has to be noted as per previous findings that iris lends itself for further security at FAR 1e-6. This flexibility can be leveraged with using iris authentication especially in areas that require even higher level security.

8. Existing matcher used during the PoC lends itself well in terms of stability and speed of matching well to offer iris authentication to wider audiences.

9. Device specification: It is recommended that STQC incorporate support for KIND 7 in the device specifications and certification processes. It is also recommended that vendors take into account learning's stated in the report to improve device accuracies.

10. Exception handling: During this PoC, like previous PoC, residents with special eye conditions had difficulty to capture during authentication. As recommended during in the previous report, residents with special eye condition should be identified using enrollment data or during first time authentication. They should be advised to use already available form of alternate authentication such as fingerprint or OTP. This will improve resident satisfaction and increase efficiency of the field operation.

11. (Restated from previous recommendation)-Multifactor authentication: Applications using biometric authentication will be diverse in nature, each requiring different level of assurance and conducted in different environment. Iris based authentication as tested is one of the several authentications methods. We recommend further studies multi-factor authentication. Biometric coupled OTP will also prove useful in many financial services and security applications. A smaller study coupled with the current study would provide data and optimized process for creating multi-factor authentication.

# 7 References

[Grother, P, 2009]: IREX Summary. By P. Grother, E. Tabassi, G. W. Quinn, W. Salamon: NIST.

[ISO 19795-2, 2007]: Biometric performance testing and reporting—Testing methodologies for technology and scenario evaluation. By International Standards Organization.

[ISO 19794-6, 2011]: Information technology -- Biometric data interchange formats -- Part 6: Iris image data. By International Standards Organization.

[UIDAI, FP, 2012]: Role of Biometric Technology in Aadhaar Authentiation - Detailed Report http://uidai.gov.in/images/role_of_biometric_technology_in_aadhaar_authentication_020412.pdf

[UIDAI, IRIS, 2012]: Role of Biometric Technology in Aadhaar Authentiation – Iris Authentication accuracy Report http://uidai.gov.in/images/**iris**_PoC_report_14092012.pdf