UNIQUE IDENTIFICATION AUTHORITY OF INDIA
Government of India (GoI)
3rd Floor, Tower II, Jeevan Bharati Building,
Connaught Circus,
New Delhi - 110001

REQUEST FOR INFORMATION

FROM

TECHNOLOGY SOLUTION PROVIDERS AND DEVICE MANUFACTURERS

FOR SPECIFICATIONS OF

1. DISCRETE FINGERPRINT DEVICE
2. FINGERPRINT SENSOR INTEGRATED IN MOBILE DEVICE
3. DISCRETE IRIS DEVICE SPECIFICATION
4. IRIS SENSOR INTEGRATED IN MOBILE DEVICE

UIDAI, 2016-17

Table of Contents

1. Introduction

Unique Identification Authority of India (UIDAI) invites Request For Information (RFI) from all technology solution providers and device manufacturers developing biometric devices (as integrated devices[1] or as discrete devices[2]) that can be used to conduct Aadhaar enabled biometric authentication.

Keeping in view the advances in biometric technology and the device industry that have taken place during the past few years, UIDAI desires to enhance its device technology and specifications in collaboration with the Industry partners with a special emphasis on the integrated devices to facilitate large scale adoption of authentication for consumer transactions.

Current specifications published and being used by UIDAI for the Fingerprint devices and Iris devices are furnished under following links:

Fingerprint Device:

http://www.stqc.gov.in/sites/upload_files/stqc/files/UIDAI-Biometric-Device-Specifications-Authentication-14-05-2012_0.pdf

Iris Device:

http://www.stqc.gov.in/sites/upload_files/stqc/files/IRIS%20Auth%20Device_specification%20issue02%20_08032016_BDCS_A-I_-03-07_0.pdf

This RFI document seeks inputs/suggestions on the possible improvements over these existing specifications and the solutions aiming to enhance the security, ease of use and the large scale adoption of authentication by Public/Private agencies and the consumers.

This document is requesting inputs and suggestions in the prescribed format (Annexure 1, Annexure 2, Annexure 3 and Annexure 4) for the following sections:

A. **Discrete Fingerprint Device Specification**

B. **Fingerprint Sensor Specification Integrated In Mobile Device**

C. **Discrete Iris Device Specification**

D. **Iris Sensor Specification Integrated In Mobile Device**

[1] 'Integrated devices' refers to devices where biometric sensor is integrated into the device package. Examples of devices in this category include, biometric sensors integrated into phone/tablet etc.

2 'Discrete devices' refers to biometric devices which need to be connected to a host device such as PC/Laptop/Micro ATM etc. as an accessory.

2. Aadhaar Authentication Overview

The Unique Identification Authority of India (UIDAI) is a statutory authority established under the provisions of the **Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act 2016")** on 12 July 2016 by the Government of India, under the Ministry of Electronics and Information Technology (MeitY). UIDAI was created with the objective to issue Unique Identification numbers (UID), named as "Aadhaar", to all residents of India that is (a) robust enough to eliminate duplicate and fake identities, and (b) can be verified and authenticated in an easy, cost-effective way.

The Aadhaar system is built on a sound strategy and a strong technology backbone and has now evolved into a vital digital identity infrastructure. It is built purely as an "*Identity Platform*" that other applications, Government and private, can take advantage of using a set of open APIs. It has reached the kind of scale that no other biometric identity system in the world has achieved so far. Currently more than 109 crore Aadhaar has been generated.

Aadhaar authentication is the process wherein Aadhaar number, along with other attributes, including biometrics, are submitted online via an API to the UIDAI for its instant verification with the information collected earlier by UIDAI during the enrolment/update process. Combination of Aadhaar number and biometrics deliver online authentication without needing a token (such as a smartcard). During biometric authentication, Authentication User Agency (AUA) collects the Aadhaar number along with one or more biometric image (e.g., one or more fingerprints, or iris image alone, or iris image along with fingerprints) which then are encrypted and sent online to Aadhaar authentication server for authenticating the resident.

The Aadhaar authentication service began as an attendant model in 2013 wherein a trained and authorized attendant operates the discrete authentication device. With the maturing of Aadhaar identity infrastructure, numerous applications are being built on the authentication platform wherein the attendant as well as the self-operated devices can be used for authentication.

At present, close to 20 million authentication transactions are carried out every day all over India. UIDAI estimates that over a million biometric devices are in use in the Ecosystem. Key ministries such as Ministry of Home Affairs (MHA), Ministry of Finance and Ministry of Rural Development (MoRD) and various State Governments have consented to adopt Aadhaar authentication / e-KYC as valid proof for establishing identity for beneficiary management and payment purposes. With more than 109 crore residents with Aadhaar now, strong endorsement from policy makers and a robust technical infrastructure, Aadhaar authentication is about to grow exponentially.

More information on Aadhaar authentication can be found at https://uidai.gov.in

3. Fingerprint and Iris Device Specification

UIDAI is planning to update its existing device specifications for Iris and Fingerprint authentication devices. UIDAI and STQC published the last revision of specification for Fingerprint and Iris devices in 2012 and 2016 respectively. There are two main drivers to consider revisiting the specification with an objective to revise them.

1. Advances and updates to biometric standards since the last publication of UIDAI/STQC authentication device standards.

2. Emergence of new category of handheld devices where biometric sensor is natively in the consumer devices. This movement has begun to put biometric devices in the hands of consumer and has popularized use of biometric for day to day transactions.

UIDAI desires to seek inputs /suggestions on the possible improvements over these existing specifications and the solutions, identify partners with shortlisted devices, conduct PoCs with enhanced specifications in real world environment, finalize the specifications and determine certification process in association with STQC.

The PoCs will also determine the suitability and usage characteristics of discrete devices for UIDAI Authentication Services. Interested entities may actively participate in these PoCs by submitting their devices and being a part of the PoC team. Interest in PoC participation will be determined through an Expression of Interest (EOI) process. Based on the PoC results, UIDAI will work along with its certification partner towards refining and publishing the final specifications and certification procedure.

Biometric device manufacturers may respond to Annexure 1 (discrete fingerprint device) and Annexure 3 (discrete iris device) to intimate the nature and availability of biometric devices.

4. Mobile Device with Integrated Fingerprint and Iris Sensors

Now-a-days, smart phones and tablets also need special protection, as their users increasingly carry out sensitive activities via their mobile devices. Compact optical biometric sensors for iris scanning are coming on as the biometric identification method of choice.

A new field of application has now opened for biometrics when unlocking mobile devices. Such a protection becomes necessary as more and more people handle sensitive matters such as banking, purchases or their professional communications over smart phones or tablets. Many manufacturers view biometrics as a secure and convenient alternative to complex passwords.

Biometric sensors detect certain characteristics and compare them with previously stored patterns of the authorized person. A measure of their effectiveness is to make the risk as low as possible that non-authorized persons can gain access (false acceptance), and to enable a low rejection rate of authorized persons (false rejection).

Biometric technology will enable users to access services remotely by embedding Aadhaar fingerprint/iris-biometric authentication capabilities in mobile or tablet. This alignment will provide a more secure authentication and verification process and help the country transition away from traditional authentication processes.

The easy-to-use biometric technology, incorporated in mobile/tablet, will help India spread its Digital India vision of providing technology so that every citizen of the country can have access to financial inclusion benefits. The solution will support government benefit programs and enable banks and financial institutions to streamline the process of an individual's authentication, regardless of language and literacy barriers. It will provide cashless and paperless services in various applications such as banking, e-Governance services such as passport, taxation, healthcare and education.

The PoCs will determine the suitability and usage characteristics of mobile devices with integrated fingerprint and iris devices for UIDAI Authentication Services. Interested entities may actively participate in these PoCs by submitting their devices and being a part of the PoC team. Interest in PoC participation will be determined through an Expression of Interest (EOI) process. Based on the PoC results, UIDAI will work along with its certification partner towards refining and publishing the final specifications and certification procedure.

Mobile device manufacturers may respond to Annexure 2 (Integrated Fingerprint device) and Annexure 4 (Integrated Iris device) to intimate the nature and availability of mobile devices.

5. Timelines

This section outlines the timelines for RFI, Iris and Fingerprint devices PoC. These timelines are provided for planning purposes only and are indicative in nature.

a. RFI

S. No	Milestone	Timeline
1	RFI Release	12th January, 2017
2	Closure of RFI Window – Receipt of Responses	1st February, 2017
3	UIDAI's Internal Review & Closure	10th February, 2017

b. Discrete Iris device specification

S. No	Milestone	Tentative Timeline
1	Iris discrete device EOI process for Proof of Concept exercise, followed by execution of POC	February, 2017
2	Iris device specification finalization and commencing certification process	March, 2017

c. Discrete Fingerprint device specification

S. No	Milestone	Tentative Timeline
1	Fingerprint discrete device EOI process for Proof of Concept exercise, followed by execution of POC	February, 2017
2	Fingerprint device specification finalization and commencing certification process	March, 2017

d. Specification of fingerprint and iris sensor integrated in mobile device

S. No	Milestone	Tentative Timeline
1	Fingerprint and iris sensor integrated in mobile device EOI process for Proof of Concept exercise, followed by execution of POC	February, 2017
2	Fingerprint and iris sensor integrated in mobile device specification finalization and commencing certification process	March, 2017

Annexure 1

Response Template For Solutions Supporting Fingerprint Authentication

S. No	Parameter	Comments
1	Name of the Organization	
2	Contact Person's Name	
3	Contact Person's Address and Contact details (Phone & Email)	
4	Are you willing to participate in the Proof of Concept studies by submitting required number of devices and related software? (PoC will be initiated and informed via Expression of Interest post-completion of RFI process)	
5	Please indicate the timelines when the product is ready for Proof of Concept studies.	
6	Please include details of the technology specification of the Fingerprint component in the format indicated below. Please provide additional information as appropriate. Respondents are requested to provide information against as many parameters as possible.	

Respondents are requested to provide their existing specifications and comments against each of the parameters if relevant to the proposed device. Please use Landscape print format while providing inputs to improve readability.

S.No.	Parameters	Respondent's Specification	Respondent's Comments
1	Platen Area		
2	Image quality		
3	Extractor Quality		
4	NFIQ Quality Software		
5	Resolution		
6	Grey scale/ Image type		
7	**Extractor & Image Template Standard –** ISO 19794-2 for fingerprint minutiae template and ISO 19794-4 for Fingerprint Image Template. **(Yes/No)**		
8	Maximum Acquisition time (Placement to Template)		
9	Audio/Visual indication of Acquisition process		
10	Liveness Detection		
11	Latent detection		
12	Platen material		
Operating temperature, humidity, Environmental, health, safety standards. Please provide information in as many areas as feasible.			
13	Preferred Operating Temperature		
14	Preferred Storage Temperature		
15	Preferred Humidity		
16	ESD		
17	Environment, health standards		
18	Safety		
19	EMC compliance		
20	Operating system environment		
21	Connectivity options		

Additional Comments if any

Annexure 2

Response Template For Mobile Device With Integrated Fingerprint Sensor

S. No	Parameter	Comments
1	Name of the Organization	
2	Contact Person's Name	
3	Contact Person's Address and Contact details (Phone & Email)	
4	Mobile Device Make and Model	
5	Are you willing to participate in the Proof of Concept studies by submitting required number of devices and related software? (PoC will be initiated and informed via Expression of Interest post-completion of RFI process)	
6	Please indicate the timelines when the product is ready for Proof of Concept studies.	
7	Please include details of the technology specification of the Fingerprint component in the format indicated below. Please provide additional information as appropriate. Respondents are requested to provide information against as many parameters as possible.	

Respondents are requested to provide their existing specifications and comments against each of the parameters if relevant to the proposed device. Please use Landscape print format while providing inputs to improve readability.

Mobile Device Specification

S.No.	Parameters	Respondent's Specification	Respondent's Comments
1	Screen Size of Mobile Device		
2	Platform – OS		
3	Location of Integrated Fingerprint device (Rear/Front)		

Fingerprint Sensor (integrated in mobile device) Specification

S.No.	Parameters	Respondent's Specification	Respondent's Comments
1	Platen Area		
2	Image quality		
3	Extractor Quality		
4	NFIQ Quality Software		
5	Resolution		
6	Grey scale/ Image type		
7	**Extractor & Image Template Standard –** ISO 19794-2 for fingerprint minutiae template and ISO 19794-4 for Fingerprint Image Template. **(Yes/No)**		
8	Maximum Acquisition time (Placement to Template)		
9	Audio/Visual indication of Acquisition process		
10	Liveness Detection		
11	Latent detection		
12	Platen material		
Operating temperature, humidity, Environmental, health, safety standards. Please provide information in as many areas as feasible.			
13	Preferred Operating Temperature		
14	Preferred Storage Temperature		

15	Preferred Humidity		
16	ESD		
17	Environment, health standards		
18	Safety		
19	EMC compliance		

Additional Comments if any

Annexure 3

Response Template For Solutions Supporting Iris Authentication

S. No	Parameter	Comments
1	Name of the Organization	
2	Contact Person's Name	
3	Contact Person's Address and Contact details (Phone & Email)	
4	Are you willing to participate in the Proof of Concept studies by submitting required number of devices and related software? (PoC will be initiated and informed via Expression of Interest post-completion of RFI process)	
5	Please indicate the timelines when the product is ready for Proof of Concept studies.	
6	Please include details of the technology specification of the Iris component in the format indicated below. Please provide additional information as appropriate. Respondents are requested to provide information against as many parameters as possible.	

Respondents are requested to provide their existing specifications and comments against each of the parameters if relevant to the proposed device. Please use Landscape print format while providing inputs to improve readability.

S. No	Device Characteristics	Respondent's Specification	Respondent's Comments
1	**Functional**		
1.1	Spatial Resolution		
1.2	Pixel Resolution		
1.3	Image Margins		
1.4	Imaging Wavelength		
1.5	Spectral Spread		
1.6	Pixel Depth		
1.7	Sensor Signal to Noise Ratio		
1.8	Scan Type		
1.9	**Output Image** IMAGE_TYPE_CROPPED_AND_MASKED with JPEG2000 compression; needs to comply with the ISO standard for Iris Image Record (IIR) i.e. ISO/IEC: 19794-6:2011, Section 6.1, 6.4		
1.10	Contrast		
1.11	Optical Distortion		
1.12	Noise		
1.13	Capture time		
1.14	Operating temperature		
2	**Safety**		
3	**Occupational Health-Safety**		
4	**Electromagnetic compatibility**		
5	**Software API**		
6	**Connectivity (How does sensor connect to device)**		
7	**Operating System Support**		

Additional Comments if any

Annexure 4

Response Template For Mobile Device With Integrated Iris Sensor

S. No	Parameter	Comments
1	Name of the Organization	
2	Contact Person's Name	
3	Contact Person's Address and Contact details (Phone & Email)	
4	Mobile Device Make and Model	
5	Are you willing to participate in the Proof of Concept studies by submitting required number of devices and related software? (PoC will be initiated and informed via Expression of Interest post-completion of RFI process)	
6	Please indicate the timelines when the product is ready for Proof of Concept studies.	
7	Please include details of the technology specification of the Iris component in the format indicated below. Please provide additional information as appropriate. Respondents are requested to provide information against as many parameters as possible.	

Respondents are requested to provide their existing specifications and comments against each of the parameters if relevant to the proposed device. Please use Landscape print format while providing inputs to improve readability.

Mobile Device Specification

S.No.	Parameters	Respondent's Specification	Respondent's Comments
1	Screen Size of Mobile Device		
2	Platform – OS		
3	Location of Integrated Iris device (Rear/Front)		

Iris Sensor (integrated in mobile device) Specification

S. No	Device Characteristics	Respondent's Specification	Respondent's Comments
1	**Functional**		
1.1	Spatial Resolution		
1.2	Pixel Resolution		
1.3	Image Margins		
1.4	Imaging Wavelength		
1.5	Spectral Spread		
1.6	Pixel Depth		
1.7	Sensor Signal to Noise Ratio		
1.8	Scan Type		
1.9	**Output Image** IMAGE_TYPE_CROPPED_AND_MASKED with JPEG2000 compression; needs to comply with the ISO standard for Iris Image Record (IIR) i.e. ISO/IEC: 19794-6:2011, Section 6.1, 6.4		
1.10	Contrast		
1.11	Optical Distortion		
1.12	Noise		
1.13	Capture time		

1.14	Operating temperature		
2	**Safety**		
3	**Occupational Health-Safety**		
4	**Electromagnetic compatibility**		
5	**Software API**		

Additional Comments if any

References

1. Biometrics Standards Committee Report
   http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf

2. UIDAI Biometrics Device Specification (FP) - Authentication (STQC 2013)
   http://www.stqc.gov.in/sites/upload_files/stqc/files/UIDAI-Biometric-Device-Specifications-Authentication-14-05-2012_0.pdf

3. UIDAI Iris Authentication Device Specification (STQC)
   http://www.stqc.gov.in/sites/upload_files/stqc/files/IRIS%20Auth%20Device_specification%20issue02%20_08032016_BDCS_A-I_-03-07_0.pdf

4. Aadhaar Authentication Framework
   https://authportal.uidai.gov.in/static/d2_authentication_framework_v1.pdf

5. Aadhaar Authentication API 1.6
   https://authportal.uidai.gov.in/static/aadhaar_authentication_api_1_6.pdf

6. High Accuracy and Inclusive Authentication using Iris Modality
   http://uidai.gov.in/images/authDoc/iris_auth.pdf

7. Role of Biometric Technology in Aadhaar Authentication
   http://uidai.gov.in/images/authentication/role_of_biometric_technology_in_aadhaar_authentication_020412.pdf

8. Authentication - Standards and Specifications
   http://uidai.gov.in/images/authentication/authentication_standards_and_specs_v1_7.pdf

Contact Details (To send responses)

1. **Yashwant Kumar,**

   Assistant Director General,

   Unique Identification Authority of India, Government of India (GoI),

   9th Floor, Tower I, Jeevan Bharati Building,

   Connaught Circus, New Delhi – 110001.

   Contact No. – 011-23462606

   Email ID – yashwant.kumar@uidai.net.in

2. **Hari Om Aggarwal,**

   Deputy Director,

   Unique Identification Authority of India, Government of India (GoI),

   9th Floor, Tower I, Jeevan Bharati Building,

   Connaught Circus, New Delhi – 110001.

   Contact No. – 011-23462617

   Email ID – hari.aggarwal@uidai.net.in

3. **Sachin Kumar Syal,**

   Senior Analyst (PMU),

   Unique Identification Authority of India, Government of India (GoI),

   9th Floor, Tower I, Jeevan Bharati Building,

   Connaught Circus, New Delhi – 110001.

   Contact No. – 8826417067

   Email ID – sachin.syal@uidai.net.in