सत्यमेव जयते

AADHAAR

UNIQUE IDENTIFICATION AUTHORITY OF INDIA

TECHNOLOGY CENTRE, BENGALURU
1ST FLOOR OFFICE- II, SALARPURIA TOUCHSTONE,
MARATHAHALLI SARJAPUR OUTER RING ROAD,
BENGALURU - 560103

REQUEST FOR INFORMATION

FROM
TECHNOLOGY SOLUTION PROVIDERS AND DEVICE MANUFACTURERS

FOR AADHAAR ENABLED

1. REGISTERED DEVICE SPECIFICATION
2. FINGERPRINT AND IRIS DEVICE SPECIFICATION

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.

UIDAI wishes to accelerate and scale up the adoption of Registered biometric devices with various form factors capable of Aadhaar authentication across its ecosystem. 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 Registered devices, Fingerprint devices and Iris devices are furnished as References 1, 3 and 4 respectively at the end of this document. 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 (Annexures 1, 2 and 3) for the following sections:

A. **Registered Devices Specification**
B. **Fingerprint device specification (Discrete/Integrated)**
C. **Iris device specification (Discrete/Integrated)**

[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

Unique Identification Authority of India (UIDAI) has been mandated to empower every resident of India with a Unique Identification Number (Aadhaar) and provide a digital platform to authenticate anytime anywhere. The Aadhaar will be robust enough to eliminate duplicate and fake identities, and can be verified and authenticated in an easy, electronic, 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 with more than 750 million Aadhaar generated, it is expected to cross the 1 billion mark very soon.

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 impressions (e.g., one or more fingerprints, or iris impression alone, or iris impression 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. For example, Indian banking regulations necessitating two factor authentication for financial transactions, integrated mobile devices with built-in fingerprint or iris sensors at affordable price level and adequate security from compliance to registered device specifications would make one-touch two-factor authentication secure and convenient for millions of consumers.

At present, close to one million authentication transactions are carried out every day all over India. UIDAI estimates that over a quarter of 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 750 million residents with Aadhaars 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 http://uidai.gov.in/auth

3. Registered Device Specification

As of today, all authentications are carried out using attached biometric devices called 'Public Devices'. Registered devices specification is an enhancement over the public device specification which eliminates the potential use of stored biometrics and prevents usage of a compromised device/application by mandating the captured biometrics encrypted within a secure zone before passing them on to the host application. This will ensure that the integrity and identity of the transaction are not compromised.

UIDAI is gearing up its capacity to support 100 million authentications per day in the not too distant future. It anticipates four different types of devices (registered and public in discrete and integrated form factors) operating in the field for the authentication service for a considerable period of time.

UIDAI has published Registered device specification 1.0 hosted on the UIDAI website ***(http://uidai.gov.in/images/aadhaar_registered_devices_1_0.pdf)*** and also as Reference 1 of this document.

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, finalise the specifications and determine certification process for registered device in association with STQC.

Technology solution providers and device manufacturers are requested to provide detailed inputs in the following key areas of the specifications.

1. Notes related to compliance in regards to UIDAI's Registered device specifications
2. Detailed inputs/suggestions on Registration API specification and data security.
3. Suggestions on certification process
4. Details of the product which solution provider intends to bring into the market as Registered authentication device

UIDAI is requesting the inputs in the attached format (Annexure 1) in order to speed up the processing of inputs received. In case, the solution providers are referring to more than one product/model family, they are requested to cite the references, if feasible, provide inputs separately for each of the models as applicable. Technology solution providers who are related to data security industry are most welcome to provide suggestions and comments, even if they do not foresee making products to be used for UIDAI's authentication purpose. In this case, solution providers can state their status as *'data security solution provider'* in the row marked Name and model number of product. This RFI aims to understand the state of industry and post-receiving the inputs, UIDAI through an Expression of Interest (EOI) proposes to conduct PoCs. While providing inputs, liberal supply of additional supporting materials including specification sheets as applicable will be appreciated.

4. 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 Finger print and Iris devices in 2012 and 2013 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, finalise the specifications and determine certification process in association with STQC.

The PoCs will also determine the suitability and usage characteristics of both integrated and 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 2 (Fingerprint) and Annexure 3 (Iris) to intimate the nature and availability of biometric devices.

5. Timelines

This section outlines the proposed timelines for RFI, Registered devices PoC, 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	5th February 2015
2	Closure of RFI Window – Receipt of Responses	25th February 2015
3	UIDAI's Internal Review & Closure	6th March 2015

b. Registered devices testing/certification

S. No	Milestone	Tentative Timeline
1	EOI Release	2nd April 2015
2	Closure of EOI – Receipt of Responses	20th April 2015
3	UIDAI Review / Shortlisting	30th April 2015
4	Backend Readiness of UIDAI for the PoC	May 2015
5	Registered device PoC/ Draft Certification completion	July 2015
6	Registered device final certification	October 2015

c. Iris device specification for integrated and discrete devices

S. No	Milestone	Tentative Timeline
1	Iris integrated and discrete device EOI process for Proof of Concept exercise, followed by execution of PoC	March 2015
2	Iris device specification finalization and commencing certification process	May 2015

d. Fingerprint device specification for integrated and discrete devices

S. No	Milestone	Tentative Timeline
1	Fingerprint integrated and discrete device EOI process for Proof of Concept exercise, followed by execution of PoC	March/April 2015
2	Fingerprint device specification finalization and commencing certification process	May 2015

Annexure 1

Response template for suggestions and comments related to Registered devices specification

General Details		
1	Name of Solution Provider/ Organization	
2	Contact Person's Name	
3	Contact Person's Address and Contact details (Phone & Email)	
4	Name and Model number of the product being referred to while providing information	
5	Category of the product	Discrete or Integrated (please provide a very brief overview of the product)
6	Supported Biometric	Fingerprint / Iris/ or Both. Please include brief overview of the specification of biometric component.
7	Product availability	Please provide information related to market availability if already released or if it is not yet released in the market, may please provide indicative timelines for the release.
8	Comments and Suggestions related to certification	Please provide your suggestions with respect to standards and specifications compliance of the product and provide your suggestions for certification process that can be followed.
Inputs and suggestions related to UIDAI registered device API 1.0 **Chapter 2 (Device/API Specification)**		
9	Compliance to hardware, firmware and software specification	Please provide your comments in relation to device characteristics as mentioned in the chapter 2 of the registered device specification.
Inputs and suggestions related to UIDAI registered device API 1.0 **Chapter 3 (Backend API)**		
10	Suggestions and comments on Backend API	Please provide your comments in relation to Backend APIs as mentioned in the chapter 3 of the Registered device specification.
	Other comments	
11	Comments related to overall Registered device specification	Please share overall comments related to Registered devices authentication concept as well as comments/suggestions related to specification.

Annexure 2

Response Template for integrated and discrete 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	Category of the product - Discrete or Integrated (please provide a very brief overview of the product)	
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 - Please refer to earlier PoC reports reference 8, 9 for an understanding of PoC process)	
6	Please indicate the timelines when the product is ready for Proof of Concept studies. Special emphasis is being laid on integrated devices 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[3] if relevant to the proposed device. Please use Landscape print format while providing inputs to improve readability.

[3] One can refer to existing specification (Reference 3) to get further understanding of these parameters.

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		
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
If you are providing comments related to integrated device, please provide additional comments and suggestions in relation on certification processes/standards for environment/ health/ safety/ EMC and related areas.

Annexure 3

Response Template for integrated and discrete solutions supporting Iris authentication

S. No	Parameter	Comments
1	Name of Organization	
2	Contact Person's Name	
3	Contact Person's Address and Contact details (Phone & Email)	
4	Category of the product - Discrete or Integrated (please provide a very brief overview of the product)	
5	Please include details of the technology specification of Iris component. Please include details of the technology specification of the Iris component in the format indicated below. Please provide additional information as appropriate.	
6	Are you willing to participate in 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 - Please refer to earlier PoC reports reference 8, 9 for an understanding of PoC process)	
7	Please indicate the timelines when the product is ready for Proof of Concept studies. Special emphasis is being laid on integrated devices for proof of concept studies.	

Please use Landscape print format while providing inputs to improve readability. Respondents are requested to provide information against as many relevant parameters[4] as possible.

[4] Please refer to reference item 4, for related standards to gain further understanding of meaning and context for each of these parameters

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		
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
If you are providing comments related to integrated device, please provide additional comments and suggestions in relation on certification processes/standards for environment/ health/ safety/ EMC and related areas.

References

1. Aadhaar Registered Devices - Technical Specification Version 1.0
   http://uidai.gov.in/images/aadhaar_registered_devices_1_0.pdf
2. Biometrics Standards Committee Report
   http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf
3. UIDAI Biometrics Device Specification (FP) - Authentication (STQC 2013)
   http://stqc.gov.in/sites/upload_files/stqc/files/New%20Revision%20_May_%201%20STQC%20UIDAI%20BDCS-03-08%20UIDAI%20Biometric%20Device%20Specifications%20_Authentication_.pdf
4. UIDAI Iris Authentication Device Specification (STQC)
   http://www.stqc.gov.in/sites/upload_files/stqc/files/Device_specification_BDCS_A-I_-03-07_0.pdf
5. Aadhaar Authentication Framework
   http://uidai.gov.in/images/authentication/d2_authentication_framework_v1.pdf
6. Aadhaar Authentication API 1.6
   http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_6.pdf
7. High Accuracy and Inclusive Authentication using Iris Modality
   http://uidai.gov.in/images/authDoc/iris_auth.pdf
8. Iris Authentication Accuracy - PoC Report
   http://uidai.gov.in/images/authentication/iris_poc_report_14092012.pdf
9. Role of Biometric Technology in Aadhaar Authentication
   http://uidai.gov.in/images/authentication/role_of_biometric_technology_in_aadhaar_authentication_020412.pdf
10. Authentication - Standards and Specifications
    http://uidai.gov.in/images/authentication/authentication_standards_and_specs_v1_7.pdf

Contact Details

ADDRESS:

AUTHENTICATION DIVISION,
TECHNOLOGY CENTRE- BENGALURU
1ST FLOOR OFFICE- II, SALARPURIA TOUCHSTONE,
MARATHAHALLI SARJAPUR OUTER RING ROAD,
BENGALURU – 560103 PH: +91-80-42511200

EMAIL ID:

auth.tc@uidai.net.in

ANY CLARIFICATIONS/ QUERIES:

1. SANJITH SUNDARAM
   +91-9886712085

2. SURAJ NAIR
   +91-8861303274