Unique Identification Authority of India (UIDAI)
Planning Commission, Government of India

Reference Number: K-11020/16/2012-UIDAI

INVITATION FOR EXPRESSION OF INTEREST

FOR

Participation in Iris Authentication Device Ecosystem Development

7th March 2012

Unique Identification Authority of India (UIDAI) has been set up with the mandate of providing a unique identity (Aadhaar) number to all residents of India and defining usages and applicability of Aadhaar for delivery of various services. Towards Aadhaar-enabling delivery of various services, UIDAI proposes online identity authentication. The online authentication may be done using demographic data, biometric data or OTP (One Time PIN).

For the purposes of issuing Aadhaar number, UIDAI is collecting biometric data pertaining to fingerprints and iris. For authentication services too UIDAI intends to use both types of biometrics – fingerprints and iris. Since fingerprint technology is relatively well established and quite a few organizations supply fingerprint devices, UIDAI first focussed on enabling the same for online authentication and has carried out extensive tests and studies to define specifications for fingerprint sensors required for online authentication.

UIDAI's next endeavour would be to establish an ecosystem for iris authentication. UIDAI foresees a large scale adoption of iris authentication. UIDAI would encourage a large number of players in the biometric device ecosystem to innovate and develop iris authentication sensors and extractor algorithms. Through this Expression of Interest (EOI), UIDAI invites applications from organizations specializing in biometric devices to participate in lab testing of iris authentication devices. The lab testing would be carried out at UIDAI Head Quarters at Delhi. The devices could either be production ready or under advanced stages of R&D. UIDAI may conduct further field studies based upon lab test results. The finding may be used for Iris Authentication System fine tuning and drawing device specification for device citification.

The participants would need to provide the following to UIDAI:

- Devices – 6 in numbers for each model
- Device specifications[1]
- IRIS segmentation SDK which produces output image in format JPEG 2000: Type 1, 2, 3 or 7 (previously known as Uncropped, VGA, Cropped and Cropped and Masked) compliant to ISO 19794-6
- Working Java based authentication application compliant to UIDAI's Aadhaar Authentication API Specification along with source code and support
- Device & support details as per Annexure 1

Timeline for responding to the EoI:

1. Last date for seeking clarifications – 2nd April 2012
2. Last date for submission of EOI response (Annexure 1) – 16th April 2012
3. Last date for submission of devices, SDK and authentication application – 1th May 2012

The responses of EOI may be sent either through post or in-person at following address, however clarification may be sent through email id of the officials mentioned below:

- Shri Yashwant Kumar , ADG, UIDAI, 9th Floor Tower-I, Jeevan Bharti Building, Connaught Place, New Delhi 110001: Email: yashwant.its@gmail.com
- Smt R Renuka, Deputy Director, UIDAI, 9th Floor Tower-I, Jeevan Bharti Building, Connaught Place, New Delhi 110001 : Email: rrenuka.uidai@gmail.com

[1] The vendor should ensure that the submitted devices do not cause any short term or long term health hazards to both operator and residents and are suitable for frequent repeat use.
The devices should be compliant to the basic specifications laid down in UIDAI's Biometric Committee report.

For application development references and support material, http://developer.uidai.gov.in/ may be referred.

Annexure 1 – Response Template

One such table to be filled for each model being submitted:

S. No	Parameter	Submitted device specifications	Remarks
1.	Name of Organization		
2.	Contact Person's Name		
3.	Contact Person's address & contact details (phone and email)		
Device Related:			
4.	Single or dual iris capture		
5.	Pixel resolution in pixel/mm		
6.	Capture distance		
7.	Capture volume		
8.	Contrast		
9.	Imaging wave length		
10.	Image margins		
11.	Pixel depth		
12.	Capture mode (auto, forced)		
13.	Shutter type (Global, rolling)		
14.	Frame rate		
15.	Spectral illumination curve		
16.	Spectral imager responsiveness or quantum efficiency		
17.	Geometric distortion		
18.	Signal to noise ratio		
19.	Polychromatic MTF[2] normalized by imager spectral response taking into account IR filter (both sagittal and transverse over the field of view)		
20.	Device form factor (USB based / hand held)?		
21.	Device dimension		
22.	Device IP standard (mention the IP rating)		
23.	Operating Systems supported (Windows / Linux / Android / Others) Provide details of all compatible OS		
24.	Development stage (production ready / R&D) If R&D, likely date for production readiness		
25.	Image acquisition time		
26.	Any audio / visual indication at		

[2] Defined as frequency response to sin-grayscale pattern

	device level for various events like capture etc.? If Yes, provide details		
27.	Any Liveness Detection mechanism? If Yes, provide details		
28.	Operating temperature		
29.	Storage temperature		
30.	Humidity range		
31.	ESD		
32.	Environment clearance		
33.	Safety		
34.	EMC compliance		
35.	Connectivity supported (Standard USB connectivity for PC based application, Connectivity for POS devices)		
36.	Any implementation / study done earlier for iris authentication? If yes, please attach biometric accuracy and performance report with details such as FRR/FAR results, packet size, acquisition time etc.		
37.	Any other parameter to be considered		
SDK Related:			
38.	Biometric Algorithm SDK Name		
39.	Image ISO 19794:6 compliant? (Yes/No)		
40.	Supports UNCROPPED (Type 1 and 2) image? (Yes/No) If yes, specify file size.		
41.	Supports CROPPED (image type 3) image? (Yes/No) If yes, specify file size.		
42.	Supports CROPPED AND MASKED (image type 7) image? (Yes/No) If yes, specify file size.		
43.	Any parameters for checking image quality? If Yes, provide details		
Testing Support:			
44.	No. of devices that can be provided		
45.	No. of technical manpower that can support integration & on-field troubleshooting		
46.	Mechanism for upkeep, storage, management & troubleshooting of devices on-field		