UNIQUE IDENTIFICATION AUTHORITY OF INDIA

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

Seeking

EXPRESSION OF INTEREST

FROM

TECHNOLOGY SOLUTION PROVIDERS AND DEVICE MANUFACTURERS

FOR PARTICIPATION IN

REGISTERED DEVICE ECOSYSTEM DEVELOPMENT AND PROOF OF CONCEPT EXERCISE

November 2016

1. Introduction and Overview

Unique Identification Authority of India (UIDAI) invites Expression of Interest (EoI) for participating in Registered Devices development and Proof of Concept exercise, from the technology solution providers and device manufacturers developing Registered devices that can be used to conduct Aadhaar enabled biometric authentication.

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 12th July, 2016 by the Government of India, under the Ministry of Electronics and Information Technology (MeitY).

Under the Aadhaar Act 2016, UIDAI is responsible for Aadhaar enrolment and authentication, including operation and management of all stages of Aadhaar life cycle, developing the policy, procedure and system for issuing Aadhaar numbers to individuals and perform authentication and also required to ensure **the security** of identity information and authentication records of individuals. The UIDAI is based on the principle that the de-duplication would be the basis of the Aadhaar approach. This would be achieved by the use of biometrics and requires high technological intervention and success. The UIDAI also believes that the verification process to get an Aadhaar should be simple and at the same time, be credible.

UIDAI and its partners have conducted various successful field studies and implemented certification processes for fingerprint and Iris authentication devices. These successes have resulted in publication of biometric device standards and associated certification processes. Subsequently, Biometric devices thus certified have contributed to increased use of Aadhaar authentication.

Over last few years, biometric authentication technology has seen many advances. Innovations in biometric authentication technologies have seen huge strides. Examples of such innovations include miniaturization resulting in integration of biometric devices into small form factor devices such as mobile phones, tablets etc. UIDAI endeavors to bring latest advances in authentication devices into the ecosystem of Aadhaar authentication. In order to provide opportunity for authentication devices ecosystem partners to test and certify their devices, UIDAI proposes to conduct field testing activities as a collaborative effort.

Several security measures are taken to ensure strong transaction security and end to end traceability for biometric devices. These biometric devices are categorized as

i. **Public Devices**: Public devices are raw biometric capture devices that provide Aadhaar compliant biometric data to the application, which, in turn encrypts the data before using for authentication purposes.

ii. **Registered Devices**: "Registered Devices" addresses the solution to eliminate the use of stored biometrics. It provides following three key features compared to public devices:

1. **Device identification** – Every device having a unique identifier allowing traceability, analytics and fraud management.

2. **Eliminating use of stored biometrics** – Biometric data is signed within the device using the device key which in turn is signed by provider key to ensure it is indeed captured from that registered device. Then the Device Driver of the device provider must form the encrypted PID block before returning to the host application.

3. **A standardized Device Driver provided by the device providers that is certified.** This device driver (exposed via an SDK/Service) encapsulates the biometric capture, any user experience while capture (such as preview), and signing and encryption of biometrics all within it.

2. Objectives and Prerequisites of the PoC

As of today, all biometric 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 10 crore authentications per day in the not too distant future. As of now Approx 107.5 crore of Aadhaar have been issued to residents of India and approx 300 crore of authentication transactions have been performed.

UIDAI has partnered with around 264 requesting entity comprised of Central/State Government and private entities to deliver various kinds of services/benefits. To deliver these benefits, biometric authentication is one of the modality to authenticate the residents. It stipulates four different types of device combinations (registered and public in discrete and integrated form factors) operating in the field for the authentication service.

UIDAI invites Expression of Interest (EOI) applications from organizations specializing in biometric devices/technology solution providers to participate in Proof of Concept (POC) exercise for Registered devices.

The organizations interested in POC shall comply to the following Levels of Device Compliance:

SDK/device drivers can be certified at 2 levels based on implementation of the signature scheme by the device provider.

i. **Level 0 Compliance –** Device security implementation has level 0 compliance if the signing of biometric is implemented within the software zone at OS level. In this case, management of private keys needs to be addressed carefully to ensure it is protected from access by users or external applications within the OS. All device providers should at a minimum obtain level 0 compliance.

ii. **Level 1 Compliance –** Device security implementation has level 1 compliance if the signing of biometric is implemented within the trust zone where other OS processes or users do not have any mechanism to obtain the private key. In this case, management of private keys needs to be fully within the trust zone. It is encouraged that device providers move towards level 1 compliance.

Selection criteria:

i. The selection of the vendors for POC will be made on the basis of readiness of the vendors and other details filled in Annex I.

ii. Selected vendors note:

   a. Post selection, vendors would be requested to participate in workshops (field visits, if any) related to POC plans, from time to time, as and when required.

   b. Vendors are requested to note that timelines for the POC may extend. If extended, information related to the same will be intimated by UIDAI to all the vendors from time to time.

3. Tentative Timelines

S.No	Milestone	Timeline
1	Publish UIDAI's invitation seeking EOI	22-11-2016
2	Last date for seeking clarifications by Partners	02-12-2016
3	Last date for submission of responses(Annexure1) by Partners	14-12-2016
4	Short listing and communicating to the Partners	23-12-2016
5	Workshop for shortlisted device partners in order to provide further details on lab testing methodologies, POC software requirements and other details.	03-01-2017
6	Last date for submission of devices, first version of SDK/driver for POC and other related information.	03-01-2017
7	i. Backend Readiness of UIDAI for the PoC ii. Completion of SDK/driver testing and tuning at UIDAI tech centre in coordination with vendor iii. Client application readiness	16-01-2017
8	PoC activity complete **Final dates will be intimated by UIDAI separately.*	31-01-2017

Annexure 1

Response Template for solutions supporting Fingerprint/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 &Official Email)	
4	(please provide a very brief overview of the product) 1. Device Type: Finger Print/Iris 2. Please specify if you are planning to submit a prototype device (non-production model). 3. Please confirm your readiness to participate in POC starting 16th January, 2017 4. Please mention if the device is a production model. Please mention if the devices are currently used in UIDAI's Authentication ecosystem.	
5	Are you willing to participate in the Proof of Concept studies by submitting required number of devices and related software? i. 4 devices / model ii. SDK/Device drivers, along with CDs iii. Integrated Authentication Client Application (Vendor should have necessary software expertise to change the SDK and client application as per the requirements during PoC) (*Vendor should also provide the necessary technical support, whether offline or online, to integrate the SDK with Auth APIs 1.6 or above*)	

6	Please include details of the technology specification of the Fingerprint/Iris. -Please confirm that the Sensor/Extractor combinations or device model is certified by STQC as qualified for usage in UIDAI's Authentication service as a public device. Please provide the device details, if a certified device is being submitted.	
7	Please specify certification Compliance Level Type i. Level 0 ii. Level 1 For compliance details on registered devices, refer the link mentioned in 'References'.	

Additional Comments, if any -

References

1. **Aadhaar Registered Devices Technical Specifications**

   https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf

2. **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

3. **UIDAI Iris Authentication Device Specification (STQC 2016)**

   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 API 1.6**

   https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_6.pdf

5. **Aadhaar Authentication API 2.0**

   https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf

6. **STQC Biometric Device Testing and Certification –Homepage**

   http://www.stqc.gov.in/content/bio-metric-devices-testing-and-certification

Contact Details

Location for submission for responses / devices:

Sanjith Sundaram

UIDAI Technology Centre,
Aadhaar Complex, NTI Layout, Tata Nagar,
Kodigehalli, Bangalore – 560092

Mail –sanjith.sundaram@uidai.net.in

Contact no. +91 9886712085

Please note: EoI responses should be sent over email as a word document; also a physical copy of the EoI response (duly signed by the official representing the organization) should be arranged to the above mentioned address for completing the EoI submission process.

Contact Persons for CLARIFICATIONS/ QUERIES:

1. **Yashwant Kumar,**
   Assistant Director General,
   Unique Identification Authority of India, Government of India (GoI),
   9th Floor, Tower II, Jeevan Bharati Building,
   Connaught Circus,
   New Delhi – 110001.
   Contact No. – 011-23462606
   Email ID – yashwant.kumar@uidai.net.in

2. **Anup Kumar,**
   Assistant Director General,
   UIDAI Technology Centre,
   Aadhaar Complex, NTI Layout, Tatanagar,
   Kodigehalli, Bangalore – 560092
   Contact No. – 080-23099203
   Email ID – anup.kumar@uidai.net.in