STQC Directorate

Seeking

LETTER OF INTENT

from

Authentication Biometric Device Providers

FOR PARTICIPATION IN

REGISTERED DEVICES CERTIFICATION SCHEME

27th February 2017

STQC Directorate
Ministry of Electronics & Information Technology
Electronics Niketan, 6 CGO Complex
New Delhi - 110003

1. Introduction and Overview

STQC invites Letter of Intent (LoI) for participating in the Certification Scheme for UIDAI's Registered Devices; this LoI is intended for device providers interested in obtaining certification for registered devices in accordance with the specifications published by UIDAI for Registered Devices.

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. The UIDAI also believes that the verification process to get an Aadhaar should be simple and at the same time, be credible.

Several security measures are taken to ensure strong transaction security and end to end traceability for biometric devices – both integrated[1] and discrete[2]. The registered device specification is one such measures. Starting June 1st 2017 only registered devices will be able to perform Aadhaar Authentication.

Registered Devices: "Registered Devices" addresses the solution to eliminate the use of stored biometrics. The specification for registered devices and the associated version of the authentication API are available below:

https://uidai.gov.in/images/resource/aadhaar_registered_devices_2_0_09112016.pdf

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

It provides three key additional 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 provider key to ensure it is indeed captured live. Then the Registered Device (RD) Service of

[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.

the device provider must form the encrypted PID block before returning to the host application.

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

2. Registered Devices – Objectives and Levels

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 crores authentications per day in the not too distant future. As of now Approx 111 crore of Aadhaar have been issued to residents of India and approx 300 crore of authentication transactions have been performed.

UIDAI has partnered with 300+ 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.

Registered devices (and Services) is planned to be certified at 2 levels based on implementation of the signature scheme by the device provider.

1. **Level 0 Compliance:** Device security implementation has level 0 compliance if the signing and encryption of biometric is implemented within the software zone at host OS level. In this case, management of private keys need 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.

2. **Level 1 Compliance:** Device security implementation has level 1 compliance if the signing and encryption of biometric is implemented within the Trusted Execution Environment (TEE) where host OS processes or host OS users do not have any mechanism to obtain the private key. In this case, management of private keys needs to be fully within the TEE.

Biometric device providers who are currently certified by STQC for either fingerprint or iris authentication devices are strongly encouraged to apply for at least Level 0 compliance with registered device specification. Otherwise, these devices will not be able to perform Aadhaar authentication after June 1st 2017.

Device vendors whose (fingerprint/iris) devices has already undergone accuracy certification will not need to recertify for accuracy if the "sensor and the extractor" (in case of fingerprint) and the

"sensor and KIND7 image generation" (iris) have not been changed. Device vendors where either of these have changed will need to be re-certified for accuracy.

1. LOI Submission Deliverables

Device vendors need to submit the following in the LOI

1) Device Model to be certified
    a. Whether currently certified as public device
2) OS system(s) to be certified for RD services
    a. Windows, Android, Linux
3) Compliance Level of certification

References

1. Aadhaar Registered Devices Technical Specifications: https://uidai.gov.in/images/resource/aadhaar_registered_devices_2_0_09112016.pdf

2. Aadhaar Authentication API 2.0: https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf

3. STQC Biometric Device Testing and Certification: Homepage http://www.stqc.gov.in/content/bio-metric-devices-testing-and-certification

4. 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-0308%20UIDAI%20Biometric%20Device%20Specifications%20_Authentication_.pdf

5. 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

Contact / Location Details

1. Sh. Aashish Banati	9968314724	24301361	abanati@stqc.gov.in
2. Sh. Amit Tyagi	9911270041	24301361	amittyagi@meity.gov.in

STQC Directorate,
Room No. 3061, STQC Directorate,
Electronics Niketan, 6 CGO Complex, New Delhi -110003