To,

All AUAs, ASAs

Sub: Upgradation of existing biometric public devices to Registered Devices

Dear Partners,

UIDAI is committed towards providing the highest quality of services in an efficient and secure manner. To enhance the security level, UIDAI has taken several security measures to ensure security of transactions and end to end traceability during the authentication process. To make it more robust and secure, UIDAI along with biometric device vendors and STQC is working on the concept of Registered Devices.

2. The key features of Registered Devices are:

a. Device identification – Every device will have a unique identifier allowing traceability, analytics and fraud management.

b. Eliminating advanced replay attacks – Biometric data is signed within the device using the provider key to ensure it is indeed captured live.

c. A standardized and certified Device Driver is to be provided by the device providers. 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. The Device Driver must form the encrypted PID block before returning to the host application.
d. There are two levels of Registered Devices named as Level 0 (software level upgrade is possible for existing public devices) and Level 1 (hardware and software level changes are required). The detailed specifications for Registered Devices are available at the link below:


3. It is expected that device vendor SDK’s would be certified as either Level 0 or Level 1 by 31st March 2017. Please contact your biometric device vendor for their schedule to support registered devices. Register device authentication backend capability will be live by 31st March 2017.

4. A decision has been taken by UIDAI that use of public devices will be discontinued and only Registered Devices will be allowed to perform Aadhaar based authentication. Therefore, you need to ensure that all biometric devices deployed for Aadhaar enabled services are upgraded to Level 0 / Level 1 Registered Device by 1st June 2017 and all future procurement of biometric devices shall from now on be as per Level 0 / Level 1 Registered Device specifications. Authentication applications will also require modification to support the registered device SDK (Level 0 / Level 1). UIDAI Authentication API 2.0 will be upgraded to only support registered device authentication. This will promote a direct upgrade from the current applications with public devices using API 1.6 to applications with registered devices using API 2.0. Accordingly, the timelines for the support for Authentication API 1.6 will be extended from 31st March 2017 to 1st June 2017. Please note that there will be no extension of this timeline and use of public devices after 1st June 2017 shall result in failed authentication transactions for which the responsibility shall be yours.

5. You may also immediately ask your device vendor to ensure upgrade of existing biometric devices to Registered Devices and provide all the required support and details for the upgrade.
6. All ASAs also need to ensure that they are able to support Auth API 2.0 which supports Registered Devices and accordingly need to prepare their system on top priority.

7. Your application development team also needs to be sensitized as changes will be required in the application and backend server to make it compatible with Registered Device and Authentication API 2.0 and would need to be tested thoroughly. Therefore, it is suggested that your technical team should be ready and get in touch with your biometric device supplier/vendor for upgradation to the latest Registered Devices specifications.

8. UIDAI is committed to ensuring that all necessary applications are upgraded on time and there is smooth transition to Registered Devices. UIDAI has already initiated workshops with all stakeholders including device providers and will continuously support entire ecosystem during this transition. In case you have any query on Registered Devices, you may kindly get in touch with UIDAI team:

Shri Yashwant Kumar, ADG yashwant.kumar@uidai.net.in
Shri Anup Kumar, ADG anup.kumar@uidai.net.in
Technical Contact Person:
Shri Rakesh Prasad rakesh.prasad@uidai.net.in
Shri Sanjith Sundaram sanjith.sundaram@uidai.net.in

9. This issues with the approval of CEO, UIDAI.

Copy for information to:
1. DG, STQC
2. Sh. Anup Kumar, ADG UIDAI
3. Sh. Pramod Varma, Chief Technology Architect, UIDAI
4. Sh. Vivek Raghavan, Chief Product Manager, UIDAI
5. All device vendors having STQC certified biometric devices
To

All AUAs / KUAs

Subject: Procurement of Registered Devices for Aadhaar authentication

Dear Partner,

Please refer to this office letter no K-11020/44/2012-UIDAI (Auth-I) dated 25th Jan 2017 wherein it was informed that with effect from 1st June 2017 authentication request will be accepted only through registered devices. In this direction, UIDAI is working closely with various device manufacturers/vendors and STQC for smooth transition to the registered device regime. UIDAI is pleased to inform that the specifications for Registered Devices (Level 0) have been published on 22nd Feb 2017 and the specifications for Level 1 will be published soon.

2. STQC will launch the registered device certification scheme on 15th March 2017 following which device of vendors will be able to get their registered devices certified from STQC as and when they are ready. On our part, UIDAI is closely working with various device vendors for development and testing of registered devices.

3. You are therefore advised that any fresh procurement of biometric device should be of registered devices only. In case, you need to procure the device before the certification of registered devices, please ensure to take an undertaking from the device vendor for upgradation to registered devices, Level 0 or Level 1 at the cost of vendor as per your functional requirements.

4. A proforma for such undertaking is enclosed for your ready reference.

Encl: As above.

(Ajai Chandra)
Assistant Director General
TO BE OBTAINED ON DEVICE VENDOR/COMPANY LETTER HEAD

UNDERTAKING

I __________________________ (Name & Designation) hereby undertake that ___ number of biometric devices are being supplied to M/s ______ (Purchaser)______ against Purchase Order No. ______________-dated ______________ for use of Aadhaar authentication.

We have seen the Registered Device specifications published by UIDAI and we are confident to get STQC certificate as per these specifications.

I __________________________ (Name & Designation) further undertake that these devices will be upgraded to Registered Devices at least Level 0 without any additional cost to M/s ______(purchaser)______ before 1st June 2017.

Date:

Name ________________________

Designation __________________

Company ______________________
F. No. K-11022/460/2016-UIDAI (Auth-II)
Unique Identification Authority of India
Government of India

9th Floor, Tower I,
Jeevan Bharati Building
Connaught Circus
New Delhi - 110001
Dated: 28.02.2017

To
All AUAs / KUAs

Subject: Instructions for providing Authentication / e-KYC services by AUA/KUA to sub-AUAs and other entities

The Aadhaar (Authentication) Regulations 2016 allow Authentication User Agencies (AUAs) to appoint Sub-AUAs for availing authentication services under Regulation number 15. Similarly under Regulation number 16, e-KYC User Agencies (KUAs) can perform e-KYC authentication on behalf of other entities. In this regard, it is necessary that these services are provided by AUAs / KUAs in such a manner which does not violate any provisions of the Aadhaar Act, 2016 and its regulations.

The AUAs/ KUAs are directed to strictly observe the following instructions while providing authentication services to Sub-AUAs or other entities:

1. The AUA / KUA shall ensure that
   
i. the client application to be used or being already used for Aadhaar authentication is developed by AUA/KUA and is digitally signed by AUA/KUA.

   ii. the client application does not store biometric data under any circumstance and biometrics /PID block is encrypted at frontend device / client level only.

   iii. the client application does not replay any authentication request with stored biometric data under any circumstance.

   iv. the client application is audited by information systems auditor(s) certified by STQC / CERT-IN and compliance audit report is submitted to UIDAI. All Sub-AUAs shall also access authentication services only through duly audited client applications.

All AUAs are required to implement the above mentioned points in their current or future authentication application as well as their sub-AUAs (if any) application at the earliest.
2. Before appointment of any sub-AUA, the AUA shall take permission from UIDAI for the appointment of such sub-AUA. The AUAs which have already appointed sub-AUA(s) also need to take permission for the same from UIDAI before 31st March 2017.

3. As per Regulation number 15(2) of Aadhaar (Authentication) Regulations, 2016, sharing of license key is prohibited in case of e-KYC authentication. The e-KYC User Agency (KUA) shall use e-KYC authentication facility in the manner as prescribed in Regulation number 16 of the said regulations.

4. AUA / KUA shall be fully responsible for the misuse and illegal sharing of the license key in production or pre-production environment of UIDAI. AUA / KUA shall not allow any other agency to perform authentication by sharing their license key. AUA / KUA shall not forward authentication request using PID block captured by unaudited application using their license key. For every sub-AUA, a separate license key shall be used.

5. In case, Authority notices misuse or illegal sharing of license key by the AUA / KUA / sub-AUA, Authority shall terminate the license of the AUA / KUA and other actions including criminal prosecution shall be taken against AUA / KUA as well as the sub-AUA and other entities as per Aadhaar Act and its Regulations.

6. AUA / KUA shall not perform any test transactions on UIDAI's production environment. Any test transaction may be performed on UIDAI's pre-production environment only.

7. In all authentication applications deployed by AUA / KUA and sub-AUA, name of AUA / KUA shall be clearly displayed to the Aadhaar number holder.

All the AUAs / KUAs are hereby required to ensure compliance of the above mentioned points and send the compliance audit report and a certificate as per attached proforma duly signed by the Chief Executive Officer or equivalent of the company by 31st March 2017. It may please be noted that failure to send audit report and the certificate by 31st March 2017 will result in immediate deactivation of license key without any further notice, and will be considered violation of the Aadhaar Act, 2016 and UIDAI shall take necessary action as per the Aadhaar Act, 2016 and may impose disincentives including termination of license of the AUA / KUA.

[Signature]
Assistant Director General
Certificate to be given by AUA / KUA

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The authentication application being used by AUA for the purpose of authentication is developed and digitally signed by AUA</td>
<td>Yes / No</td>
</tr>
<tr>
<td>2</td>
<td>The authentication application does not store and/or replay stored biometric data.</td>
<td>Yes / No</td>
</tr>
<tr>
<td>3</td>
<td>Biometrics/PID block is captured and encrypted at the front end device / client level</td>
<td>Yes / No;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Front end device / Client level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.</td>
</tr>
<tr>
<td>4</td>
<td>Sub-AUAs are using authentication services through application duly audited by the AUA</td>
<td>Name of Sub AUA: Yes / No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.</td>
</tr>
<tr>
<td>5</td>
<td>Audit of the authentication application by STQC/CERT-IN certified information system auditor(s), and audit compliance report shared with UIDAI</td>
<td>Yes / No;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Date of Audit:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Date of compliance report sent to UIDAI:</td>
</tr>
<tr>
<td>6</td>
<td>Permission from UIDAI for all sub-AUAs mentioned in point number 4 above</td>
<td>Name of Sub AUA: Date of permission</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.</td>
</tr>
<tr>
<td>7</td>
<td>Sharing of e-KYC data with other entities in compliance with Regulation number 16 of Aadhaar (Authentication) Regulations, 2016</td>
<td>Name of the entity:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.</td>
</tr>
</tbody>
</table>

It is certified that the information provided above and all its particulars have been verified by all the directors/partners/concerned officers and each one of them shall be jointly and severally liable for any discrepancy in the information supplied herein above as may be found by the Authority.

Dated:

Chief Executive Officer
Name of the Company