QUERY RESPONSE FOR EXPRESSION OF INTEREST (EOI)
for Participation in Authentication Registered Device Ecosystem Development
(Reference Number: K-11020/83/2013-UIDAI(AUTH-I))

Unique Identification Authority of India ("UIDAI") hereby provides response to the queries raised by some vendors against the Expression of Interest (EOI) to participate in Authentication Registered Device Ecosystem Development.

It may be noted that UIDAI, based on the request for extension of date for device submission, is proposing two cut-off dates - (i) 15th April 2014 and (ii) 31st May 2014. However, it may be understood that organization/devices submitted at the earlier cut-off date may have a natural priority in support from UIDAI to complete the lifecycle of the PoC.

Kindly note that other date i.e., last date for submission of EOI response remain the same. The important dates are mentioned once again hereunder for easy reference.

IMPORTANT DATES	
Last date for Submission of EOI response	**02nd April, 2014**
Last date for submission of devices, SDK and Authentication Application	First cut-off: **15th April, 2014** Second & last Cut-off: **31st May, 2014**

QUERY RESPONSES

Manufacturer/Supplier Entity - #1		
S.No	**Queries**	**Response**
1	1. How to do match on host? Do we need a second algorithm there? In the specs there is a provision to send unencrypted templates and images to the host for local matching and filtering should there be a need to run a verification that not the same finger is sent again but there is no way to pass back the info to the registered device implying that we need an extra algorithm running on the host. I also believe that this can be used for NFIQ as this is not discussed in the spec as part of the registered device.	If local matching is required at host level, yes, you need an SDK there. Yes, spec allows unencrypted templates corresponding to encrypted ones to be passed to host. Note that unencrypted templates cannot be used for Aadhaar auth PID block formation.
2	Please clarify why tid has to be called at each authentication transactions? If the device is embedded in the unit can this be cached?	It is not required to be called for every transaction. In memory caching is OK at host level. But, either when host is powered on or if there was some error related to this from UIDAI server, it needs to be refreshed.

3	Can we manage the secure storage in a different way? Some processors have a secure storage which is cleared for tampering but it is smaller than 512 bytes. What we propose is to store the secure data inside the device in an encrypted blob with a random key and store the random key into a secure memory which is cleared by the device in case of tampering. If tampering occurs the key is lost and the blob becomes useless.	This is not OK for UIDAI AES-256 keys and PKI private keys to be stored. They must be stored and managed within the secure area. All other data can be managed outside in encrypted fashion as you described as long as encryption and decryption is done within the secure zone. No external probe/app should be able to access the keys.
4	Should we take care of not reregistering the device or the registration system already takes care of that?	Only registration system can register the device initially before use. All AUA business applications on host need not deal with it. Note that "Reset" needs to be implemented by all AAU apps. In PoC, UIDAI will help register.
5	Please provide a list of Certification Authority from whom we need to procure the keys. Also kindly give us an idea of approximate cost of procuring such a key	CA list is published on CCA website (http://cca.gov.in) and listed as per India's IT Act.
6	Please elaborate on the public key sharing mechanism with UIDAI.	Described at high level in spec. Any specific question(s) may be addressed in upcoming proposed, workshop to be held before device submission.
7	Kindly elaborate on "Other Accuracy related certifications". Does this mean all the registered devices will undergo a fresh STQC FRR testing in the field and subsequent lab testing? Or will UIDAI put in place a process to get provisional certification of such devices?	No, it does not mean that. All it means is that registered devices certification is focused ONLY on security and compliance with spec where as sensor level accuracy certification is for biometric accuracy. Any certified biometric sensor and extraction/processing SDK can be integrated into registered devices.
8	In case of a device reset, is there a need to physically send the device back to the registration facility? Or can this be handled on the field via online update facility?	No. Reset is an API to be called from host to UIDAI server via AUA/ASA network quite like auth API.

9	Please let us know on the timelines that UIDAI expects such devices to be ready to hit the market and that there is a competitive environment. There is significant change and effort involved in developing a new product as per the specifications provided in this document. . The spec also calls for including new processes in the manufacturing of devices such as key injection and online registration. As per past experience, the time taken to manufacture a production level unit is minimum 7 months post freezing of specs After this if there is a STQC testing, we are looking at another 6 months to go through this process and get final certification. After this if there is a STQC testing, we are looking at another 6 months to go through this process and get final certification. In all, we are looking at a 12 month+ time frame before the units are certified and ready for deployment.	UIDAI expects it to hit the market by last quarter of 2014. Once the certified devices start hitting the market, UIDAI may put out a policy for deprecating the public devices and give enough time for existing investments to be used. By now, one in every two Indian residents have Aadhaar and system is expected to cover a billion people in next 2 years. Given active push in application adoption, UIDAI expects this market to continue to grow. Security being prime importance, UDIAI expects registered devices to be the de-facto in few years. Some vendors may release early and some will take time. Our expectation is that to have at least few certified devices in the market (especially for the use of financial transactions) by early 2015.
10	Please clarify should we allow Firmware updates in the field? Opening a device for field updates can be seen as a security risk and should be avoided.	No security related updates is allowed. No devices are allowed to be opened and maintained. Detail specs will follow.
11	How will the tamper resistance be tested? Is there any design guideline we should follow? Please clarify	Being worked out. Your inputs and previous experiences may be shared to ensure learnings are considered while doing this.
12	How will the secure flow from capture to extraction be tested or be validated? Kindly elaborate.	Being worked out. Your inputs and previous experiences may be shared to ensure learning's are considered while doing this.
13	How will the system be tested against external data injection?	Being worked out. Your inputs and previous experiences may be shared to ensure learning's are considered while doing this.
14	Will there be another FRR test? The current one did not specify where the algorithm had to run and we do not know which part of the current FRR extraction was done on the host or on the device. Please clarify	No. But, if a new sensor/extractor combination is to be used, they must undergo biometric sensor certification process including FRR test.
15	Where does NFIQ have to run? Can it be run on the host? Please clarify	Yes
16	Please elaborate on the proof of concept and lab testing of Authentication registered devices procedure. What tests will be carried out as a part of this process?	Entire lifecycle and usage of registered devices will be tested out and validated against UIDAI backend. At the end we also expect to finalize concrete certification scheme.
17	Can you please elaborate on Support for front end and backend server configurations	If there are any parameter tuning, setup, etc. required for the devices, it must be provided through easy to use mechanisms

18	Please clarify if UIDAI will provide slots for each applicant to get their device/s integrated with UIDAI backend? What timelines does UIDAI envisage for this exercise? This will help us in planning for resource allocation for this effort	UIDAI will inform the high level schedule and activities of the PoC in the upcoming workshop before device submission. UIDAI will work with each of the applicant in a possible time sliced method or may allot slots to each of the device. The priority and progress of PoC for each device may also depend on early submission and support by respective organization. UIDAI will provide all necessary support for this exercise. We will also create an open discussion forum dedicated to this to make discussions easier, open, and transparent.
19	Can we submit devices with non Minex certified extractor which matches rest of the specification?	Yes. For actual certification and field usage, it must be certified
20	We request UIDAI to postpone the date of submission of devices and start of POC beyond April 2014	UIDAI, based on the request for extension of date for device submission, is proposing two cut-off dates - (i)15th April 2014 and (ii) 31st May 2014. However, it may be understood that organization/devices submitted at the earlier cut-off date may have a natural priority in support from UIDAI to complete the lifecycle of the PoC.
Manufacturer/Supplier Entity - #2		
S.No	**Queries**	**Response**
1	Who would implement the application for Registration for this POC ? UID, in its specification talks about a ‘default application for laptop’ it will provide. Is it to be provided by UIDAI?	Since registration is an API, for PoC, vendors should be prepared to implement the registration app. UIDAI will register it for PoC. UIDAI will make all efforts to provide one registration app on Windows/Linux platform using Java.
2	What is the readyness of Aadhaar server to accept the Authentication, Registration & device Reset request from the Host application & by when requied details will be provided to the vendors. This will affect the capability of the vendor to submit the necessary SDK, applications by the mentioned date of 15th April.	Server readiness is expected by PoC time. Any delays from UIDAI side will be accommodated.
3	How will UIDAI manage fusion finger authentication (Since the old encrypted has to be resent) & BFDin case of Registered devices?	We are working out the mechanism to allow consecutive encrypted FMRs to be used for fusion. Suggestions are welcome.
4	Keys management shall need dedicated organization for keys creation, keys sharing, keys transport, keys signature. Manufacturer shall provide keys to UIDAI server. Then UIDAI server has to sign them before being loaded in the sensor. All this process will need dedicated tools. For this POC do we need to implement the whole process of key management ?	All you need is to upload/send a valid class II server certificate issued by a valid CA under IT Act.
5	For POC, do we need to provide public key procured from one of the approved Certification Authority in India by CCA to UIDAI. If not, is UIDAI going to provide Manufacturer Key to be used for POC?	Yes

6	What is the OS to be supported for this POC: Windows 7 ?	Windows 7 and Android 4.x
7	There is an expiry for all certificates used in the Registered device process & it is linked with the device life cycle. If any one of these certificate expired then device will stop functioning. How UIDAI propose to manage the expiry of these certificate. What will be the Manufacturer Key renewal process for devices that are on field?	Certificate is used only for registration. When UIDAI issues manufacturer key, we will ensure that key is valid for 3-4 years. There can be any number of manufacturer keys (not restricted to one). So, device vendor should buy new certificate every couple of years and create new manufacturer key for use within devices.
8	When do you plan to hold the workshop of selected vendors to explain the architecture of the POC. This should happen before submission of devices by vendors.	Yes, UIDAI will hold a workshop post clarification phase.