Team,

Yesterday we met Vivek Raghavan (current chief manager of UIDAI) and got a lot of things clarified on Biometrics and registration processor. Here is the summary (Resham & Romila, please add if I have missed out anything). Please read through them and see if it requires any change in current implementation or needs to be accommodated in future stories. Please reach out to me for clarifications.

I will put out MOSIP Biometrics specs in github wiki soon and send out a reference.

**Registration client**

* Biometrics data captured in the client must be packaged in CBEFF format before it is sent to server
* CBEFF format is ISO/IEC 19785 – 3
* Within the CBEFF data package
  + Finger print image record (FIR) should be in ISO/IEC 19794 -4
  + Iris image record (IIR) should be in ISO/IEC 19794 – 6
  + Face Image data (FID)should be in ISO/IEC 19794 – 5
  + Face data capture should be in ICAO standard
* Jmrtd (<https://github.com/E3V3A/JMRTD/tree/master/jmrtd>) is a java library that will help in constructing the data package
* MOSIP needs to define limits on image size for face. Especially the size of the photo in width x height in mm and

**Registration Processor**

* AADHAR sends FP, IRIS and Face images to ABIS for de-duplication. Guess is, ABIS uses Face only in the case of a match found
* Only HTTP URL’s of images are sent to ABIS. So, all images should be stored in HTTP accessible format
* In case of a match found by ABIS, a 1:1 match against the candidate list is done using an SDK. The 1:1 match is a slow process but is more accurate. Based on the result of 1:1 match it is either sent to manual verification or rejected
* Do a virus scan before and after decryption of packet
* GPS validation will check if the GPS co-ordinates captured is within a range and within the co-ordinates of the country

**ID Authentication**

* Finger Print authentication is against ISO/IEC 19794 -2 (ISO template a.k.a minutiae) data only. Future release can do authentication on FP image i.e., ISO/IEC 19794 -4 format
* Finger Print authentication i.e., 1:1 match against the ISO template is done by a 3rd party SDK only. AADHAAR does not have code to do this match. MOSIP will also stick to this option
* IRIS authentication is against image as per ISO/IEC 19794 – 6 spec
* IRIS 1:1 match is done by a 3rd party SDK and not within AADHAAR. MOSIP will also have to follow the same. The SDK’s for 1:1 match for FP and IRIS will usually be different
* AADHAAR does not do Face authentication as of now. They are doing POC’s using ML algorithms. So, will be keep Face authentication for later versions of MOSIP and is out of scope for v1

**ID Repository API**

* After UIN is generated, ISO template as per 19794 – 4 is generated for the Finger Print and stored in the ID repo DB. The template generation is by a 3rd party SDK

**Pre-Registration**

* Rethink the design of storing documents. Docs can be stored in DFS during pre-registration and URL’s provided for read-only access. This might be rework, but I think it is good to do the refactoring now than later.

**General principles**

* Packet stored in server will be read only and never modified
* Refer to documents and biometric images as URL’s at all places in the server and never store them in DB

Regards,

Shravan