***Agenda:*** *Discuss and conclude on changes recommended by Sasi*

**Registration Processor**

1. *Filesystem must have permissions*.

          Both Internal File System (HDFS/CEPH) and External File System (File System in DMZ) should have permissions enabled for Upload/Fetch/Delete Files from File System.

2. *Hash Check for Encrypted Packet (RID, Hash Sequence, Packet Size, Optional Values – Anything Required for Integration, PRID)*

1. Registration Client needs to send *a Hash Sequence for the Encrypted Packet, Size of the Packet, PRID, Any Optional Attributes which would be required for Integration with External System* during Packet Meta Data Sync.
2. Whenever Registration Processor Stage fetches the Encrypted Packet they need to perform a Check Sum Validation for the Encrypted Packet against the Hashed Sequence received during Packet Metadata Sync.
3. Receiving the Packet from Reg Client.
4. Fetching the File from DMZ Zone to Store in HDFS (Secure Zone) File System.
5. Encrypt the whole Request Body for the Packet Metadata Sync Request (Same as Encryption Logic used for Packet).
6. Center ID should be passed in the Header.
7. While Receiving the Packet from Reg Client, Registration Processor can perform size validation using the Packet Size received during Packet Metadata Sync.

3. *Digital Signature of the Response received by Client (One Key Pair can be used for Whole MOSIP Application)*

1. Server Signs the response with a MOSIP Private Key.
2. Client Validates the Request using the MOSIP Public Key.

4. *Virus Scanning*

1. Virus Scanning should be done In-Memory.
2. Virus Scanning should be done before even Storing the File in the File System (even in DMZ Zone).
3. Virus Scanning should be done twice, first in Untrusted Zone and Again in Trusted Zone.
4. First Virus Scan, for the encrypted and decrypted file should be done in-memory, but it should not be unzipped as Antivirus should take care of unzipping and performing Virus Scan.
5. Second Virus Scan can be done on unzipped Files in Pre-Processing Stage (Secure Zone).
6. If Virus Scan Fails, we should not Store the file at all in MOSIP System, the Virus Scanner will store the File in Quarantine Zone. We should not worry about it.

5. *Fetching Files from DMZ to HDFS*

1. The Connector Stage (in Secure Zone) gets triggered and gets a RID.
2. The Connector Stage now performs a Check Sum Validation on the File in DMZ Zone.
3. Post Successful Validation, the Connector Stage should Pull the File from DMZ File System and Store in HDFS (in Secure Zone).

6. *OTP Validation for Officer and Supervisor (Can be part of Version 2)*

1. Registration Processor should receive a Token from Registration Client, when Officer or Supervisor authenticate the them self during Packet Creation.
2. Registration Processor validates the Token in Server and Authenticates the Officer and Supervisor.

7. *Parent or Guardian (Introducer) Biometric Validation*

          Scenario 1:

1. If RID of the Parent is not found or UIN has not been generated, then wait for Y hrs. and retry for X number of days.
2. Even if after X number of days, you don't find the Parent RID, then Perform a Bio De-Dupe for Parent's captured biometrics (*Can be taken as part of Version 2*)
   1. if match found in Bio Dedupe, generate Child's UIN.
   2. if match not found in Bio Dedupe, then reject the Child's UIN.

          Scenario 2:

a. If RID of the Parent is Processed or UIN of the Parent is received, Perform 1:1 Match,

1. if match found in 1:1 Match, generate Child's UIN.
2. if match not found in 1:1 Match, then reject the Child's UIN.

For Current Implementation,

1. For New child registration, capture one slapstick of one biometric of the Parent/Guardian
2. For UIN Update of Child, capture the UIN, Name and one slapstick of one biometric of the Parent/Guardian (It could be any Parent/guardian – Same Parent/guardian as during registration or another Parent/guardian)
3. Perform 1:1 match of the biometric captured with the biometric of the parent/guardian’s associated with the provided UIN
4. If matched - Honor Child’s UIN’s Update request
5. If not matched – Reject Child’s UIN’s Update request
6. If Parent/guardian’s RID is never received by Registration Processor, then Reject the UIN of the Resident.

8. *Manual Verification after 1:1 Biometric Match Failure*

In the event of demo dedupe potential match and bio 1:1 match failure, manual verification is not required. Such packets can be rejected.

9. *ABIS Middleware, (Not a Change...TBD with ABIS Middleware)*

* 1. For New Registration,

1. if ABIS finds 'Zero' Duplicates then go for UIN generation.
2. if ABIS finds at least 'One' Duplicate then send Packet Info with Duplicate Packet Info for Manual Verification.

b. For Update Registration,

1. if ABIS finds 'One' Duplicate then Check if the UIN Associated with the Duplicate is the UIN Present in Packet and hence Update UIN Data.
2. if ABIS finds More than 'One' Duplicate then send Packet Info with Duplicate Packet Info for Manual Verification.

10. *UIN generation*

1. For New Registration, Inserting Data in ID Database should be handled by Registration Processor.
2. For Update Registration, Updating Data in ID Database should be handled by Registration Processor.
3. ID Repository API should only perform GET/SEARCH operations.

11*. Operator and Supervisor Logins should have VIDs*

1. User ID, Password is present in LDAP.
2. Create a Mapping of User ID and VID internally and Authenticate the User.
3. Even though the mapped VID is inactive/revoked, the operator can continue with registrations
4. What happens when VID gets Expired or Changed by Operator? - TBD

12*. Blacklisted Operators and Supervisors in User Table/LDAP*

1. Add Blacklisted flag in LDAP/User table for Operator or Supervisor, if the Admin Blacklists the User.
2. If an Operator/Supervisor is found to be Black Listed in the Packet, then the Packet goes On Hold.
3. User History should be stored in MOSIP DB.

13. Adding Trained Flag for Operator or Supervisor in User Table/LDAP

Add Trained/Certified flag in LDAP/User table for Operator or Supervisor who have completed the Training for MOSIP.

14. *Use Reference ID instead of UIN,*

a. We should use UIN Reference ID instead of UIN in Registration Processor.

15*. Integration with External System and Appending /Combining the Packets*

1. Store Multiple Packets in Packet Store (DFS) for Processing.
2. The Additional Packets coming in should be as per MOSIP Standards (Pre-Decided).
3. Update Section in the Update Packet – Should have only Update Values.
4. Combination of Packet Function to Combine multiple Packets.
5. Verify the Combined packet using Check Sum.
6. This can be used for Correction Packet Integration.

*Approach for Combining Two Packets:*

1. Conventional Approach
2. Configuration Approach
3. Both (Conventional and Configuration Approach

*Conventional Approach*

In this Approach, we update the data that is the part of the New Packet.

Example:

Below is the Packet structure of two Packet, where,

1. Packet 1 is the Packet created by Registration Client.
2. Packet 2 is the Packet send by External System.
3. Packet 3 is the Combined packet.

Packet Structure:

Packet 1:

- Meta Data

- RID

- Center ID

- Machine ID

- etc.

- Demo Data

- Name – XYZ

- Gender – Male

- Age – 24

- CNIE Number

- Iris File

Packet 3:

- Meta Data

- RID

- Center ID

- Machine ID

- etc.

- Demo Data

- Name – ABC

- Gender – Male

- Age – 24

- CNIE Number

- Iris File

- Finger Print File

Packet 2:

- Meta Data

- RID

- CNIE Number

- Demo Data

- Name – ABC

- Finger Print File

*Configuration Approach*

In this Approach, we update the data based on the Configuration File Sent in the New Packet.

Example:

Below is the Packet structure of two Packet, where,

1. Packet 1 is the Packet created by Registration Client.
2. Packet 2 is the Packet send by External System with Added Values form Config File. The Config File says, Update Only Name and Finger Print File, hence in New Packet we Update Only the Name and Finger Print File.
3. Packet 3 is the Combined Packet Structure

Packet 3:

- Meta Data

- RID

- Center ID

- Machine ID

- etc.

- Demo Data

- Name – ABC

- Gender – Male

- Age – 24

- CNIE Number

- Iris File

- Finger Print File

Packet 2:

- Meta Data

- RID

- CNIE Number

- Config File

- Demo Data

- Name – ABC

- Gender – Male

- Finger Print File

- CNIE Number

- Age – 24

Packet 1:

- Meta Data

- RID

- Center ID

- Machine ID

- etc.

- Demo Data

- Name – XYZ

- Gender – Male

- Age – 24

- CNIE Number

- Iris File

*Both (Conventional and Configuration Approach)*

In this Approach, if Config File is Present then go with Configuration Approach and if Config File is Not Present then go for Conventional Approach.

TBD – The 3 Approaches needs to be Analyzed and one should be Selected for MOSIP.