Hi All,

The demo was comprehensive and the approach to stubbing out dependencies is highly appreciated.

Here are my notes and feedback.

1. ID Repo Get method to have filters on the data attributes to be returned.

2. Anadi to clarify on eKYC ecosystem hierarchy

3. Rationalization of json formats needed. Will be covered in API Review.

4. UsageData tag - need to understand that a bit more. Part of API Review

5. Test artifacts including Comm Sync (SMS, Email Stubs) to be in place.

6. Performance design to be looked into.

7. API Review to be Scheduled.

Regards,

Ramesh

Hi All,

Please note the points discussed during the end to end demo of ID-Authentication module, for features developed until Sprint 7.

Kindly add on/update as required.

**@ Ramesh/Anadi/Krishnan/Shrikant,**

Thank you for your time and extensive review & feedback.

***Participants***:

Anadi, Ramesh, Krishnan, Shrikant, Gita, Jyoti, Gayathri ,Shravan, Romila, Gurpreet, Loganathan, Manoj, Hema, Vignesh, Athila, Resham, Techno forte team, Lalana

***Document(s) Referred***:

1. For Demo: *Enclosed deck <Sprint 7 ID-Authentication Demo.pptx> and ID Auth and repo services in QA environment*
2. For Technical Review: *GitHub*
3. For Functional Review: JIRA
4. For Testing Status: Test Strategy doc, *JIRA and eclipse*

***Action Items*:**

1. Recommendation to move Static PIN auth to v1+
   1. As considerable amount of work has already been done, IDA team decided to retain the feature as part of V1
2. TSP and UA Concept - Below clarifications are pending with client (Anadi to get back by Feb 1st  – post which tech team will modify the api specifications, followed by Tech specs review session with Ramesh/Anadi)
   1. Do we need multiple levels of TSP or should we fix it to two? If yes, how many?
   2. Who in the level is authorized to see what?
   3. Who in each level is authorized to do what?
3. Security features of auth api review session with Sasi - Anadi
4. Platform Level Terminologies for the Network provider and the Service provider raising the authentication request to be finalized – Hema/Resham based on response for point 2
5. Authentication failure due to poor quality of finger prints passed should be logged, so that it can be further used by any entity for analytics/reporting/further action (Clarification query to be added in JIRA – Hema)
6. *Testing*:
   1. Test Cases for auditing data to be added and verified - Vignesh/Athila
   2. Automation of notification scenarios to be implemented - Vignesh/Athila
   3. Biometric test data to be common to all modules  - Jyoti/Gita

***Discussion points***

1. *Demo:*
   1. *ID Repository:*
      * Discussion on retrieval of a subset of demographic attributes from the stored identity for a country – Recommendation is to add filters for the data requested
      * Security review required for table structure for ID-Repo
   2. Authentication: Recommendation to have single client which encrypts and encodes and sends Auth Request and decrypts and decodes and shows the response
   3. *Known issues:* CNIE related pending specifications to send Fingerprints to MOSIP from Morocco will impact storage of the data in ID- Repository therefore will impact ID-Authentication
   4. *Testing:*
      * Discussion on Test strategy, Test data and the Automation test process
      * No of test cases written and/run in each sprint – generated/calculated from scripts
   5. *Backlog:* Suggestion to pick up user-stories with Device/SDK dependency, and integrate when the devices are available – already on Track
2. Generic
   1. *Multifactor authentication:* SI , the Network provider and the Service provider for a country will construct the api for multifactor authentication and invoke the auth api. If multiple auth parameters are in request, MOSIP to perform an ‘AND’ on the results for each parameter and send consolidated response
   2. Authentication/eKYC policy: policies tied to UA will govern the permissible auth modes and the attributes returned in the e-KYC response
   3. Additional eKYC API if provided, will be a feature specific to GoM and not a platform requirement
3. Technical
   1. Capability to mediate the auth flow between request and response (say to introduce liveliness detection)-  supported in the ID Auth filter layer
   2. Auth API design on Scalability, Availability and Performance – Current design supports these NFR - Recommendation to scale up with respect to these requirements
   3. Component Diagram Illustration of ID Authentication

Regards,

Hema