++ Srijoni

Thanks & regards,

Resham Chugani

Business Analyst

**From:** Resham Chugani   
**Sent:** Friday, January 11, 2019 4:09 PM  
**To:** Shrikant Karwa <[shri@mosip.io](mailto:shri@mosip.io)>; Arun Gurumurthy <[arun@mosip.io](mailto:arun@mosip.io)>; Ramesh Narayanan <[ramesh@mosip.io](mailto:ramesh@mosip.io)>; Anadi Mishra <[mishra.anadi@gmail.com](mailto:mishra.anadi@gmail.com)>; Krishnan Rajagopalan <[krish@mosip.io](mailto:krish@mosip.io)>; Sanjay Jain <[snjyjn@gmail.com](mailto:snjyjn@gmail.com)>  
**Cc:** Shravan Poorigali <[Shravan.Poorigali@mindtree.com](mailto:Shravan.Poorigali@mindtree.com)>; Romila Mattu <[Romila.Mattu@mindtree.com](mailto:Romila.Mattu@mindtree.com)>; Gita Vittal Rao Phutane <[Gita.Phutane@mindtree.com](mailto:Gita.Phutane@mindtree.com)>; MOSIP BA <[Mosip.Ba@mindtree.com](mailto:Mosip.Ba@mindtree.com)>  
**Subject:** Notes from MOSIP Technology Bootcamp - 10-11Jan'19

Hi All,

Sharing key points from the two day MOSIP Technology Bootcamp.

Please add on/update as required.

Significant feedback has been highlighted.

***Day 1 - 10Jan’19***:

1. Feedback on: *Introduction of MOSIP*, presented by Sanjay Jain
   1. ID – Real, Unique and Identifiable
   2. Steve – MOSIP should consider workflow for different applicant types (EG: Different documents for Refugee etc) – This is accommodated within MOSIP by way of configuration/mapping
2. Feedback on: *Modularity & Configurability*, presented by Shravan, Mindtree
   1. ID for multiple countries – Interoperability between systems of multiple countries should be considered
   2. Monolithic vs. Hierarchical ID systems architecture
   3. Self-sovereign IDs with control to individual to decide what formulates an ID, should be the way forward
3. Address by Nandan Nilekani – UIDAI Chairman and co-founder/Non-Exec. Chairman of Infosys
   1. Key differentiators MOSIP should focus on, as compared to aadhaar
      1. Open Source ABIS vs. Aadhaar’s approach of multiple ABIS engines not exposed
      2. Online/Realtime generation of IDs vs. Aadhaar’s approach of batch process
      3. Minimalism in design should be considered to build layers over MOSIP
   2. Functional ID vs. Foundational ID
4. Feedback on: *Design Manageability and Scalability*, presented by Anadi
   1. Adam – Regularly cycle micro-services to avoid security compromise
   2. Biometric Matching – Do not discard fusion of biometrics adopting a uni-modal ABIS (Allow for multi-modal ABIS solution)
   3. Include pre-sales documentation for marketing MOSIP
   4. Ability to coordinate data exchange between multiple data authorities/sources
   5. Ease forward compatibility with future architecture and how will MOSIP handle data portability from MOSIP to other ID system
   6. Notify Country about the vision of MOSIP being a foundational ID
5. Feedback on: *Building Digital Infrastructure for Development - India Experience*, presented by Pramod Varma
   1. Aadhaar experience/challenges:
      1. India did not have a birth registry during the onset of aadhaar, and aadhaar overcame this issue by providing digital identities
      2. Best practices: Transparency, conscious trust building, civil society engagement
      3. Exception Handling in terms of biometrics – Recommend multi-modal based fusion biometrics to handle exception scenarios. Also consider OTP based authentication to sort this issue
6. *Making standards work in the real world – examples from Canada and Scotland,* addressed by Steve Pannifer
   1. Scope: Business, Legal and Technical
   2. Types of identities:
      1. Real Identity: Identification (People and Organizations)
      2. Digital Identity: Authentication (Keys)
      3. Virtual Identity: Authorization
   3. Challenges in meeting the standards:
      1. Competing stakeholders
      2. Time to build standards is not fixed, as it needs to evolve
      3. ID standards tend to focus on technicality and trust framework takes the scope completely
   4. Examples:
      1. Pan Canadian Trust Framework (PCTF) – A collaborative approach to develop a Pan-Canadian Trust Framework
         1. Definition of a *Verified Person*: Real, Identifiable and Unique within the population
      2. Scottish Govt. – Common Public Sector Approach: Aim is to test and deliver an online ID scheme
   5. Benefits of Standardization:
      1. Business: Determine acceptable solutions
      2. Legal: Reduce cost, protect citizens
      3. Technical
   6. Sources of digital identity technical standards:
      1. International Organizations
      2. National Organizations
      3. Industry Consortia
7. *Facilitating a private ecosystem around MOSIP* - Panel Discussion (Tomicah Tillemann, Edward Duffus and Shrikant Karwa)
   1. Data portability to be looked into to avoid vendor lock-in
   2. Interoperability is vital
   3. eCRVS

***Day 2 - 10Jan’19***:

1. *Aadhaar Stories: Building the World's largest identity platform,* addressed *by* Vivek Raghavan
   1. Factors MOSIP should consider to be different from/better than aadhaar:
      1. Online Registrations and UIN generation (With real time immediate deduplication and UIN generation)
      2. Mobile phones – To ascertain identities
      3. Biometric and UIN locking for authentication
      4. Machine Learning to automate processes
2. *Morocco's RNP Project: Program Status,* presented by Gov Abdelhalak Harrak
3. *Demonstration of MOSIP Platform*, presented by Resham Chugani
   1. Biometric deduplication in online mode
   2. HoF Concept - Handling family tree and family association (EG: Polygamy scenarios)
   3. Request to share the link to the visual prototypes of the functional demo (Guinea and Cote D'Ivoire)
4. *MOSIP: Design for Privacy and Security*, presented by Ramesh and Sasi, followed by panel discussion
   1. MOSIP should consider Audit transparency yet protect PII data
   2. MOSIP should go beyond encryption in terms of Security – Backend Tokenization
   3. Digital Certificate utility
   4. *Transparency and Control: What level of control does a user need to protect their privacy, while not hampering identity and verification/authentication? How to maintain transparency to build trust?* – Sandeep Shukla
      1. Provide guidelines to user community for strict auditing of eco-system partners
         1. Device management
         2. Security practices for programmers developing
      2. Cyber Security Protection - Hacking by way of patching upgrades to be looked into
   5. *Leverage Cryptography and avoid data mis-use* – Satya Lokam
      1. Data Storage: Individual should own their data, even if encrypted – MOSIP should provide control of data to an individual
         1. De-centralized identity
         2. Adopt one-way hash approach and prevent misuse of data: Data tampering and data leaks
         3. Data should be stored with keys, which an individual can control
   6. *Surveillance State – Surveillance state: Are there mechanisms to ensure privacy when multiple government and private systems deal with citizen identity? What are the policy, legal and technical measures that can be put in place to protect privacy?* – Gopinath Kanchi
      1. Alternative architecture using token to validate/authenticate an individual, without storing data
   7. *Lessons: What lessons can be incorporated from issues faced by existing identity systems across the globe?* – Ott Sarv
      1. MOSIP comes across as a data capturing platform rather than an ID platform
      2. MOSIP should provide data sharing control to the individual
      3. MOSIP should focus on MVP
5. *Advancements and Challenges in adopting Biometrics Systems* - Panel Discussion (Vivek Raghavan, Prof. Anoop Namboodiri and Anadi Mishra)
   1. Biometrics liveness detection should be dwelled upon
   2. Other modes of biometrics:
      1. DNA, Ears, Gait, Keystroke
      2. Speech can be used as a biometric above voice biometrics
   3. ABIS:
      1. Benchmarking mechanism – Leader boards of various engines to record accuracy of various parameters
      2. Privacy preserving biometrics
6. *Decentralization in Action: What Open Source, Distributed Ledgers and Digital Identity Systems Can All Learn From Each Other,* presented by Brian Behlendorf
   1. Focus on “Do-ocracy” more than meritocracy
   2. Emerging Open Source Standards: Decentralized Key Management System (DKMS), DID (De-centralized Identifier)
   3. MOSIP should focus on end user interface and biometrics integration, rather than back-end registry
   4. To ease migration, anticipate multiple foundational IDs in the architecture (Even if not in v1.0) – EG: A common foundational id being connected and mapped
7. *Open Source Ecosystem for MOSIP Panel Discussion*: Panel Discussion (Satish Mohan, Edward Duffus, Brian Behlendorf and Krishnan Rajagopalan)
8. *MOSIP Roadmap*, presented by Sanjay Jain

Thanks & regards,

Resham Chugani

Business Analyst