OMIDYAR NETWORK INDIA

BCG BOSTON CONSULTING GROUP

MOSIP

Open Digital Ecosystem (ODE) Case Study

1. Context

Governments around the world are leveraging digital platforms to transform public service delivery. Digital Identity (ID) forms a foundational building block for any e-government digital public service delivery mechanism. According to the 2016 World Bank Identification for Development (ID4D) database, approximately 90 countries are developing digital ID systems to make disbursement of benefits more efficient.[1] Digital ID can also potentially unlock several other solutions. For example, in India, it has enabled financial institutions to offer services such as paperless instant account opening and instant credit. In Estonia, digital ID has enabled e-voting. In Ethiopia, the United Nations High Commissioner for Refugees (UNHCR) leveraged digital ID to provide humanitarian services including child protection and education to around nine lakh refugees. [2] It is evident that a digital ID solution can help promote inclusion, ensure efficiency in service delivery, and drive innovation.

While identity forms the bedrock of an efficient public service delivery system, there are several other core building blocks that need to be cemented in order to harness the true potential of such a system. Some of these include a single trusted sign-on system, a verification engine, a payments platform, a messaging platform to send notifications to users, etc. Considering that these technological needs are homogenous across countries, digital public goods anchored on open technology (open source, open standards, and open Application Programming Interfaces (APIs)) hold significant potential. They prevent the need for a country to reinvent the wheel by providing customizable building blocks for digital infrastructure and provide an opportunity to learn from other countries' experiences. Further, they are also a more cost-efficient option due to the economies of scale that they offer.

The concept of digital public goods is not novel and has already been implemented in various contexts, including health management (the open Insurance Management Information System, (OpenIMIS)), education management (Sunbird, a repository of digital resources), and financial inclusion (Mojaloop, a software for creating payment platforms). An example of a successful digital public good is open Medical Record System (OpenMRS), an open-source medical health record platform that records and analyzes patient health information to improve health care delivery, especially in resource constrained settings. Launched in 2006, OpenMRS has been implemented in over 40 countries.

In this case study, we showcase another similar attempt to create a digital public good to solve the challenge of providing digital ID, Modular Open Source Identity Platform (MOSIP).

2. Solution and Benefits

MOSIP was conceptualized to enable countries to unlock opportunities through digital ID in a cost-effective manner. It has been built as a digital public good that meets the criteria defined by Digital Public Goods Alliance[3] – facilitate vendor-independence, reusability, interoperability, and address privacy and security. Moreover, MOSIP upholds the Principles on Identification for Sustainable Development – inclusion, design, and governance to not just provide a digital ID but an identity that respects the needs and rights of an individual.[4]

It provides the following core modules that countries can configure and customize.[5]

1. **Pre-Registration**: The pre-registration portal can be used by individuals to book appointments. Individuals can provide their demographic data, upload supporting documents, and book an appointment at a suitable registration center. The resident data is shared with the selected registration center to be used during the registration process.
2. **Registration**: This module provides for the collection of an individual's demographic and biometric data along with the supporting documents. The data is packaged in a secure way cryptographically and transferred to the server in online or offline mode for processing
3. **Registration Processor**: The captured data is run through quality and duplication checks and a Unique Identification (UID) number is generated. This module also interfaces with external systems such as the Automated Biometric Information System (ABIS) to check for biometric duplication.
4. **ID Authentication**: This module allows individuals to authenticate and verify their IDs in real time. It is an API-based authentication mechanism that allows only MOSIP verified entities to validate individuals.
5. **Resident Services**: In this module, the individuals can login on the portal to access services such as lock/unlock biometrics, lock/ unlock ID, reprint UID, view authentication history, etc.
6. **Partner Management**: This module provides services to MOSIP partners and MOSIP Infrastructure Service Provider (MISP). The services include registration, policy management which allows partners to access authentication services based on a defined policy, and license key management for MISPs to send and receive authentication responses.
7. **Administration**: This is an application used by the central administration and registration center heads for configuring news or notifications according to the country, managing registration centers, machines and devices, and managing master data such as types of documents, list of holidays, list of genders, etc.

Morocco and Philippines are the first two countries in the world that are in the process of building their foundational identity systems on MOSIP, while several others in Africa and South East Asia have also expressed interest.

MOSIP has been highlighted as a model digital public good in the report of the UN Secretary-General's High-level Panel on Digital Cooperation for enabling sharing and promoting adaptability of a digital platform design across countries, as per their needs.[6]

The benefits of MOSIP to organizations, both public and private, tasked with building an identity system are listed below.

1. **Leverages existing infrastructure:** MOSIP can be built on the existing identity system of a country as the open API architecture enables backward integration. This means that countries can pursue their mission of inclusive development without having to reinvent the wheel. For example, MOSIP can leverage the existing bank identity system of a country and use it for the verification of documents.
2. **Can be customized to suit needs**: A country can customize MOSIP to suit its requirements by configuring the code and choosing the relevant modules, effectively saving time and cost. For example, countries can choose whether they would like to include biometrics as an identity attribute. This is enabled through its modular architecture.
3. **Achieves cost efficiency**: MOSIP is free for countries to build their identity systems on, relieving them of the financial burden of developing a basic digital infrastructure. Moreover, the modularity of the platform reduces the upfront cost since countries can add modules as they scale up in the future.
4. **Helps avoid vendor lock-in**: Identity systems built on proprietary technology are difficult to replace. Further, such systems find it challenging to adapt to technological and regulatory changes due to the financial and operational risks involved. Complete access to the MOSIP code along with open standards helps avoid this situation.
5. **Leverages community knowledge to continuously improve and innovate:** An open source code facilitates continuous review from a community of developers. The collective expertise can be leveraged to make the code more robust through the continuous development of new features and troubleshooting.

3. Key Features and Learnings from MOSIP

In this section, we will provide an overview of the key features of the MOSIP platform, including both the "technology" and "non-technology" aspects. These have been grouped into three primary buckets, i.e., Digital Platform, Community, and Governance.

3.1 Digital Platform

- **Open APIs, open standards, and open source to avoid vendor lock-in and enable interoperability**

  At the 2018 annual meeting of the ID4Africa Movement, a poll of the delegates identified that technology neutrality remains one of the biggest challenges in implementing national identification systems. For the successful implementation of MOSIP it is critical that a country is able to select the most relevant MOSIP modules and then build on them. Moreover, for the country to use digital ID for social benefits and other services, interoperability with civil registries, population registries, and other functional registries is imperative. To facilitate this, MOSIP follows an API first approach - a design methodology in which APIs are designed around the goals of the organization and needs of the developers, allowing developers to plug and play, and effectively build customized solutions.

  Use of open standards and open source also addresses the issues related to technology and partner dependency. Non-proprietary, freely accessible standards and source code make MOSIP agnostic to specific applications, computer language or platform. Hence, it ensures inter-changeability of products and technology. Moreover, it results in consistency among different government identity systems, facilitating interoperability and data exchange.

  While open source provides these benefits, several governments are concerned with its security (and transparency). MOSIP is helping the countries overcome this concern by building awareness around the security features of MOSIP and demonstrating use cases.

Principle 1: Be open and interoperable

MOSIP uses **'open technology'** to avoid vendor lock-in. It makes the digital ID system adaptable to regulatory and technology changes, promoting platform agility. Following an API-first approach ensures interoperability.

For example, in the countries implementing MOSIP, the system integrates with existing databases to add to the identity information being collected in accordance with the regulations established by the country.

- **Modular to suit the requirements of the country**
  MOSIP has unbundled modules which can be integrated to create a unique identification system according to the needs of the country. Hence, solutions can be easily customized, precluding the need for any re-engineering. This feature will be especially valuable to countries as it provides them with significant flexibility and an opportunity to avoid the costs and time spent on developing technology from scratch.

Principle 2: Make unbundled, extensible, and federated

MOSIP provides several modules that each enable multiple functionalities such as ID issuance, updation, authentication, and user control.

For example, Philippines is currently building their National Identity System using the ID issuance module, enabling it to collect data and issue an ID to individuals.

- **Privacy and security built into design**
  MOSIP has been designed to protect user identity and personal information by ensuring that the user is the owner of the data and enabling maximum transparency. It also ensures that the platform is protected from unauthorized access. The basic design elements built in are data encryption, access to ID repository via secured APIs, user consent framework, digital signatures, cryptographical validation of data, data anonymization, and layered technology architecture. In addition, advanced functionalities have also been built in such as 'virtual ID' that allows revocable access to limited data for one-time use, notifications and real-time data on usage to provide transparency, the ability to lock features of authentication and eKYC, and offline authentication.

3.2 Community

- **Designed for inclusion**
  MOSIP helps ensure universal coverage by providing access to the last mile individual. It offers options that work both online and offline, reducing the burden of network requirements. Offline authentication, for example, is especially relevant in resource constrained settings where network and infrastructure are poor.

- **Participatory design through partnerships with expert academics to enhance technology capabilities and through community review of open source**
  Security enhancement is one the top priorities of MOSIP considering the critical role of an ID system as a national infrastructure. Hence, MOSIP is further building its technological capabilities by partnering with top educational institutes in the United States of America (USA) and United Kingdom (UK) that have expertise in machine learning (ML) and artificial intelligence (AI). MOSIP has also appointed an International Advisory Group comprising experts from public sector and international development entities. MOSIP holds regular consultations with the experts to solicit feedback on technology and implementation aspects of the platform.

Principle 7: Drive participatory design and end-user engagement

MOSIP leverages experts from both technology institutes and countries implementing digital ID systems to seek feedback on the technology and implementation capabilities of the platform. Further, by opening the source code, MOSIP has facilitated review by the community of developers, testers, users, etc., to ensure robustness of the code.

For example, MOSIP has received feedback on GitHub regarding issues on compatibility with operating systems and inputs on the roadmap of MOSIP such as strengthening the consent and opt-out framework.

- **Co-creation by fostering an ecosystem of private companies to provide relevant services**
  MOSIP has been designed to be configurable and customizable to be relevant for any country. Hence, it is creating a community of systems integrators to build country-specific systems (includes Document Management System, ABIS, Global Positioning System (GPS) and location, and ID card printing) on top of MOSIP and implement a digital ID system in the country. The partnership approach of MOSIP follows two models. In the first model, MOSIP trains and vets service providers who are capable of building on top of MOSIP. To develop the ecosystem, MOSIP conducts workshops inviting ID solutions engineers, and biometrics and devices vendors to work hands-on on integrating with MOSIP. In the second model, countries procure their own vendors and MOSIP provides training and education, and maintenance services of the core technology. These models provide flexibility to the country while overcoming the primary barrier to developing digital ID systems, ie., a lack of technical capabilities. Going forward, MOSIP plans to automate the integration process. This will allow vendors to share test results with MOSIP online following which MOSIP can run independent tests to verify successful integration.

Principle 8: Cultivate a network of innovators

MOSIP runs workshops and events inviting vendors to build systems on top of MOSIP. The vendors are vetted and trained to build a community of systems integrators capable of integrating successfully with MOSIP.

For example, four biometric software companies have successfully integrated their ABIS with MOSIP. These systems can be used to assess the quality of biometric images of finger, iris, and face captured during registration.

- **Implementation supported by public and private partners**
  MOSIP is implemented in collaboration with public and private players. It has laid down a comprehensive structure that defines the responsibilities of each stakeholder (vendors, government, and private partners) involved in implementation. In addition, MOSIP defines a comprehensive manual for system integrators implementing the digital ID system and specifically articulates the capabilities and skills required by the implementation team. However, there have been instances when MOSIP has had to fill in the gaps because of lack of capabilities in the implementing countries. For example, they have had to customize the core platform according to the country context- a task typically done by commercial partners, to demonstrate value to the country officials. This poses a challenge to MOSIP as it is dependent on an ecosystem of government and commercial players for smooth implementation.

3.3 Governance

- **Governance mechanisms recommended by the World Bank**
  MOSIP endorses the World Bank's Principles on Identification for Sustainable Development. The World Bank has prescribed principles on governance requiring comprehensive legal and regulatory frameworks, institutions, and trust frameworks with the objective of ensuring transparency, and protecting privacy and user rights.

  MOSIP recognizes that law and technology must go hand in hand to ensure that individuals' rights and interests are protected. Hence, MOSIP proposes aligning technology with policy to ensure not just the sustainability of the system but also accountability and protection of individuals' rights. It recommends instituting robust enforcement mechanisms to govern both the technical aspects and the stakeholders involved, in developing a digital ID system.

  The governance elements recommended by MOSIP are:[7]

  - Robust data protection frameworks, including rules for limited data collection.
  - User control over data enshrined in the law, including opt-out mechanisms and notice requirements.
  - Inclusiveness, including user choice on whether to enroll or use digital ID
  - Effective grievance redressal mechanisms.
  - Widespread consultations with key stakeholders.

Principle 12: Establish and align with robust rules of engagement

In Philippines regulations have supported the pilot of the country's digital ID system (PhilSys) in 2019 with full implementation planned for 2020.

In 2018, the Philippines enacted an Act establishing the Philippine Identification System. The Act defines clear institutional accountability by appointing the Philippine Statistics Authority as the implementing agency for the planning, management, and administration of PhilSys. It also created the PhilSys Policy and Coordination Council (PSPCC) responsible for formulating policies and guidelines, including technology infrastructure, and rules of engagement for effective coordination among government departments. Further, the Act lays down rules regarding data collection, use of information, penalty for misuse, funding model, etc. In 2012, Philippines enacted the Data Privacy Act that defines rules on collecting data, processing data, and user consent. It also established the National Privacy Commission responsible for enforcing the law.[8]

The absence of a strong governance mechanism such as accountable institution, data protection regulations and frameworks, etc., poses a challenge to the implementation of MOSIP. For example, an accountable institution that lacks agency might face political pressure in the choice of the open source software. Additionally, weak regulations and grievance redressal processes create opportunities for corruption and may lead to the failure of MOSIP.

- **Suitable financial model to sustain current and future operations**
  Currently, MOSIP is funded by philanthropic foundations such as the Bill and Melinda Gates Foundation, Omidyar Network and TATA Trusts. The funds support the software development process, and implementation and trainings in countries, as MOSIP is free for countries. However, MOSIP charges businesses for trainings to keep the cost of knowledge transfer neutral. While the current funding is sustaining the operations, MOSIP is exploring innovative models for the future, both for financial and technical support. For example, large corporates often support open source projects by providing grants or a team of engineers for the maintenance of systems. In another model, the corporates that use the software for their operations sponsor the project by hiring developers to work on it full-time. MOSIP has an opportunity to build partnerships with such corporates who could become potential sponsors.

4. Conclusion

MOSIP serves as a good example of several principles of Open Digital Ecosystems (ODEs) with its open and modular technology architecture and a community of public and private partners helping countries build and implement digital ID systems. It is still in its nascence but has the potential of unlocking benefits from cross-country applications. Some considerations that can make MOSIP more impactful are:

- While the source code is open on GitHub for developers to provide feedback, MOSIP could create a more comprehensive engagement plan to **facilitate participatory design**. A cross-country network of technology experts, public sector officials, international organisations, and individuals can be built where learnings can be shared and feedback can be solicited on open forums.
- While MOSIP has recommended governance principles for countries, it has the advantage of further building out those principles based on its experience of working in different countries. A **detailed governance framework** could be immensely valuable for countries starting out to build their national ID systems.
- MOSIP can also leverage its experience in implementing digital ID programs to help countries envisage the implementation risks before developing the system. It can help countries **better understand their ecosystem** including end-users, infrastructural needs, technological capabilities, and political environment. This will enable the countries to adapt MOSIP to their requirements.
- MOSIP could **enhance marketing activities** in the target countries to improve their knowledge base. This can be done by collaborating with companies familiar with MOSIP and conducting events where potential partners can be vetted. This will enable MOSIP to conduct readiness evaluation prior to implementing in the country.
- MOSIP is funded by philanthropic foundations. Currently, these funds support the development process and trainings in countries. For businesses, MOSIP charges for trainings to keep the cost of knowledge transfer neutral. Going forward, MOSIP could explore **innovative models for both financial and technical support**. For example, large corporates often support open source projects by providing grants or a team of engineers for the maintenance of systems. MOSIP has an opportunity to build partnerships with corporates who use the software for their operations.

[1] Bhadra, S. (2019). *Five Surprisingly Consequential Decisions Governments Make About Digital Identity*. Retrieved from https://www.omidyar.com/blog/five-surprisingly-consequential-decisions-governments-make-about-digital-identity.

[2] The Engine Room. (2020). *Understanding the Lived Effects of Digital ID*. Retrieved from https://digitalid.theengineroom.org/assets/pdfs/200128_FINAL_TER_Digital_ID_Report+Annexes_English_Interactive_Edit1.pdf.

[3] Digital Public Goods Alliance. (n.d.). *Nominate*. Retrieved from https://digitalpublicgoods.net/nominate/.

[4] The World Bank. (n.d.). *Principles of Identification for Sustainable Development: Toward the Digital Age*. Retrieved from http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf.

[5] Joshi, P. (n.d.). MOSIP Architecture. Retrieved from https://github.com/mosip/documentation/wiki/MOSIP-Architecture#Modules.

[6] Digital Cooperation. (n.d.). *The Age of Digital Interdependence*. Retrieved from https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf.

[7] MOSIP, IIIT Bangalore. (2019). *Principles of Engagement*.

[8] Philippine Statistics Authority. (2017). Republic Act No. 11055. Retrieved from https://psa.gov.ph/system/files/kmcd/RA11055_PhilSys.pdf.