case study

Lessons Learned: Reflecting on MOSIP's Journey to Scale

Venkatesh Hariharan

March 2024

MOSIP is a Digital Public Good (DPG) that has gained rapid traction. Over 100 million individuals have been issued a digital ID using MOSIP, a commendable feat for a project that is just five years old. Built as an open-source solution, MOSIP is being implemented in countries as diverse as Ethiopia and the Philippines. This case study outlines the factors that led to the rapid adoption of MOSIP and the lessons that other DPGs can derive from its success.

The Modular Open Source Identity Platform (MOSIP) is a foundational identification (ID) system designed for use by national governments to provide individuals with a unique identifier that can be used to increase and improve access to critical public and private services.

In addition to its status as an open-source solution or DPG, MOSIP is an exemplar of the solutions available to build out foundational digital public infrastructure (DPI), an approach to ensuring data systems including identification, civil registry and vital statistics, payments, registries, and data exchange—are designed, deployed, and governed to benefit people. Proponents of DPI believe this approach can accelerate the attainment of the United Nations' Sustainable Development Goals (SDGs). In this paper, we examine the factors that led to the early successes of MOSIP, the challenges that lie ahead, and lessons that might benefit similar projects.

As of 20th November, 2023, 100 million digital IDs have been issued using MOSIP since its launch in 2018.[1]

Full implementations are underway in the Philippines, Ethiopia, and Morocco, while Togo, Sri Lanka, and Uganda are in advanced stages of preparation for national implementation.

Another five countries - Sierra Leone, Guinea, Burkina Faso, Madagascar, and Niger - are piloting MOSIP to create blueprints for a national rollout.

What is MOSIP?

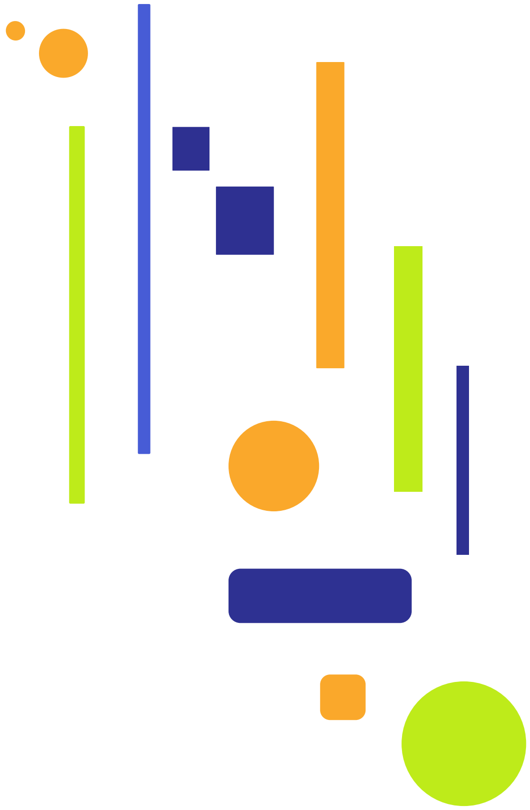
According to the World Bank, “An estimated 850 million people globally face challenges in proving who they are because they lack official proof of their identity.”[2] Without an officially sanctioned ID, people face obstacles to accessing health care, education, financial, and mobile services provided by or regulated by the state. This disconnection from public services and the formal economy can also lead to people missing out on economic opportunities—from jobs to social services and benefits.

This is why the Sustainable Development Goals include goal 16.9: “Provide legal identity for all, including birth registration.” ID4D notes that, “Identification is also a key enabler or contributor to many other SDG targets, such as financial and economic inclusion, social protection, healthcare and education for all, gender equality, child protection, agriculture, good governance, and safe and orderly migration. For these reasons, identification is widely-recognized as being instrumental to realizing the SDG promise to ‘leave no one behind.’”[3]

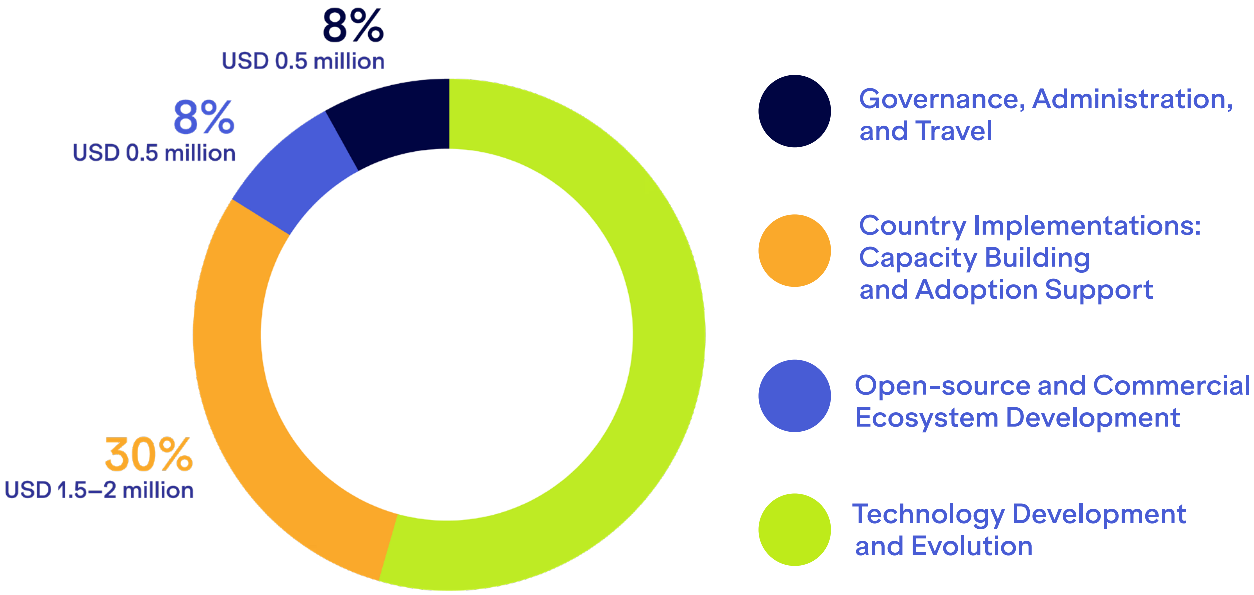
India’s Aadhaar biometric ID system, which was built in 2009, is the world’s largest ID system, with more than a billion people enrolled. It has significantly accelerated economic formalization and increased the efficiency of public service delivery. The source code for Aadhaar, however, is proprietary and owned by the Government of India, making it inaccessible for use. The success of Aadhaar prompted requests from countries around the world for a system similar to Aadhaar. Responding to this demand, a few multilateral funding agencies decided to support the building of an open, modular ID system that mimicked key design features of Aadhaar and could scale across diverse geographies—from large countries with hundreds of millions of residents to smaller countries with hundreds of thousands of residents—while leveraging the lessons learned from Aadhaar’s development and deployment.

The Bill & Melinda Gates Foundation, Tata Trust, Omidyar Networks, NORAD, and Pratiksha Trust funded the Indian Institute of Information Technology, Bangalore (IIITB), a leading educational institute in India, to build MOSIP as a digital public good (DPG) that could be used by any country to implement their own foundational ID. Like Aadhaar, MOSIP is designed to emphasize key concepts such as ensuring each person enrolled in the system is unique,[4] data minimization to mitigate potential misuse, scalability to reach the entire population including those not yet online, and affordability including financially sustainable approaches to deploying, maintaining, and improving the system.

Coined relatively recently, the term “digital public good” is defined in the UN Secretary-General’s Roadmap for Digital Cooperation as “open-source software, open data, open AI models, open standards, and open content that adhere to privacy and other applicable laws and best practices, do no harm, and help attain the SDGs.”[5] Over the last few years, an ecosystem of countries, donors, developers, NGOS, and the private sector has rallied around the idea of DPGs as a means to accelerate progress toward the digital public infrastructure (DPI) needed in countries to realize inclusive development.



After receiving an initial investment of around $28 million in grants, IIITB's annual operating budget for MOSIP today varies between $5 and $7 million. Below is a typical break down of MOSIP's annual expenditures:



> Through a series of conversations with those who conceived, designed, implemented, and funded MOSIP, this paper seeks to understand what has worked well for MOSIP, what could have been done better, and the remaining challenges to the MOSIP ecosystem.

I. Strengths

Institutional Home

MOSIP is housed inside the Indian Institute of Information Technology, Bangalore (IIITB), an academic institution that has been around since 1999 and has grown into a multidisciplinary academic institution of global repute. IIITB's leadership team has supported the MOSIP project in various ways. For example, it realized that MOSIP had to pay competitive industry-level salaries, so the project was allowed to hire staff at salaries that were higher than those of senior academics at the institute. The project has also enjoyed great support from successive directors of the institute.

Engagement Model

MOSIP entered the market at a time when many countries had been burned by the expense of purchasing and implementing proprietary software. The lack of customization and choice that can accompany the use of proprietary software (also known as "vendor lock-in") was another challenge. MOSIP was built in collaboration with the countries that signed up early, and the team provided pro-bono advisory relationships with governments, eschewing the traditional client-vendor relationships. Its source code was also made available under the Mozilla Public License 2.0 open-source license.

MOSIP built a comprehensive product after abstracting requirements from early adopters and reviewing requests for proposals (RFPs) issued by countries for building their ID systems. Since it is open source, the risk of vendor lock-in is reduced. Unlike proprietary software programs, implementation is not limited to one vendor, since multiple system integrators (SIs) are trained to implement MOSIP. Successful implementations have spurred demand, with countries now asking SIs to build ID systems on top of MOSIP.

MOSIP also engaged in no-cost pilot programs with governments as a capacity-building exercise. For example, both Togo and Sri Lanka ran MOSIP pilots before deciding to proceed with national rollouts.

The team did not attempt to pressure governments into doing national rollouts after the pilots were completed because it knew that decision-making cycles within governments are long, which helped build trust.

MOSIP also prefers that countries decide their own implementation models. Countries like Ethiopia chose to implement MOSIP through in-house teams, with support from MOSIP. Other countries chose to work with system integrators (SIs), with MOSIP supporting the countries and the SIs through knowledge transfer and training programs. MOSIP also leaves the choice of SIs to the countries and does not interfere in that process.

The MOSIP team recognizes the potential for misuse of a national ID system by a government. It has therefore drafted a Country Engagement Framework to help countries build an ID system that puts the individual's rights and needs at the center of the system. As Arun Kumar Gurumurthy, head of strategy and resourcing at MOSIP, explains, "We are very user-centric, and success for us is adoption of MOSIP and not just building a technology platform.

MOSIP advises governments and other ID issuers to consider the following aspects of the system:

- **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

This framework forms a part of the agreement that MOSIP signs with countries. Though these are not legally binding, they serve as the guiding principles for each country's engagement. It has to be recognized that just as a car maker can provide driving recommendations, but has no authority to enforce it, MOSIP can make recommendations and encode safety features into its software. However, the ultimate responsibility of good governance rests squarely with the countries implementing MOSIP.

Ecosystem: According to MOSIP's president, Prof. S Rajagopalan, there are four different ways for projects like MOSIP to be adopted widely:

- **Organic diffusion,** which is like the process of plant pollination. This is how open-source communities like Linux and Wikipedia became popular.
- **Organized diffusion,** which is the method used by companies, involves systematically expanding distribution of a product until it has wide availability.
- **Diffusion by fiat,** which is when a country imposes something on its citizens. This is how some countries distributed COVID-19 vaccines.
- **Diffusion by charity** is when something is dispersed by a charitable entity, like when oral rehydration solutions (ORS) were distributed to remedy dehydration.

MOSIP focused on organized diffusion as the best approach and built a team to pursue opportunities. For example, in 2018, the team gave a talk on MOSIP and noticed that a few people had logged in from the Philippines at 3:00 a.m. their time. MOSIP took advantage of this interest and followed up with those participants. The Philippines became one of the first countries to implement MOSIP, with 75 million digital IDs issued through MOSIP to date.

Over four years, the MOSIP team has built an ecosystem of SIs and hardware vendors through the MOSIP Partner Programme (MPP) and MOSIP Academy, but it was not easy. In the identity space, some of the top tier SIs have their own proprietary solutions. MOSIP tried to work with the top tier SIs but was met with resistance. Therefore, it decided to work with the next level of SIs, and this strategy has worked well.

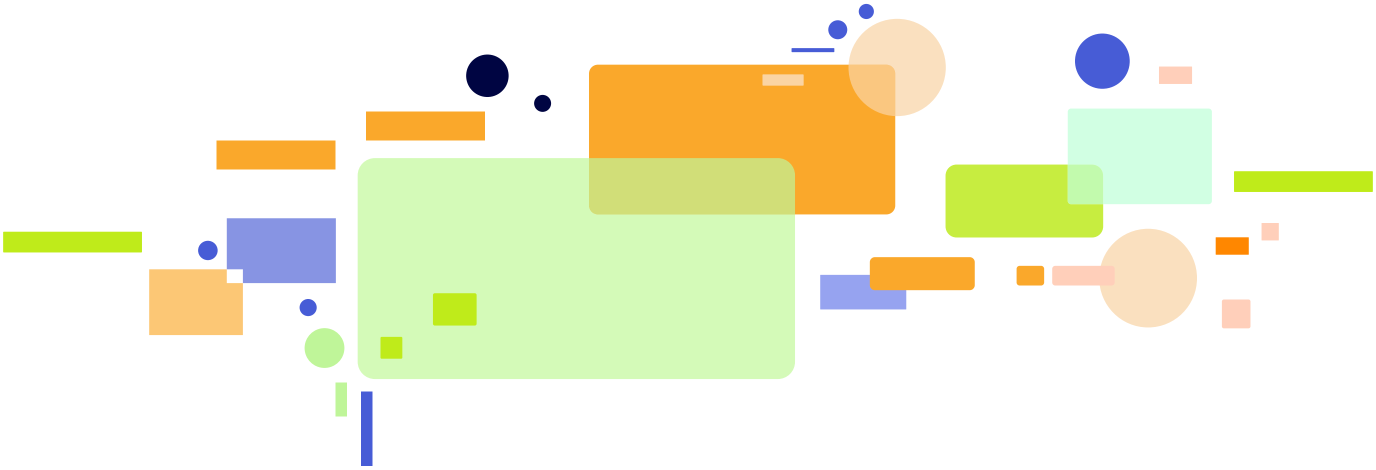
MOSIP's outreach to governments has created demand, and major SIs and technology vendors are responding to this. For example, Atos, which is a leading SI, has declared that its ID strategy in Africa will be MOSIP-based. Gemalto, an international digital security company, is about to expand its capacity on MOSIP and become an official partner. Idemia, a leading biometric ID solution provider, has also integrated its products with MOSIP, and many other SIs and device manufacturers are set to follow suit.

MOSIP has nonexclusive, equal opportunity relationships with all vendors. It is estimated that the cost of issuing an ID to an individual through MOSIP is approximately $2. Therefore, the opportunities for vendors in the MOSIP ecosystem are huge. According to a Biometric Update article, "Big deals are coming for vendors. Ethiopia has a population of 114 million, the Philippines 115 million, Morocco 37 million. A vast amount of equipment is needed not just for biometric enrolment, but at the point of service provision, whether private sector banking or government welfare."[6]

MOSIP enables its vendors through the MOSIP Partner Programme, which invites SIs to register and undergo training programs on various aspects of the platform, including deployment, customization, and maintenance. This program's objective is to create an ecosystem of SIs competent in implementing a MOSIP-based digital ID system. This improves the negotiating power of countries as it gives them a wider choice of SIs to work with and reduces the risk of vendor lock-in.

MOSIP Academy works in tandem with the MPP to enable knowledge transfer and effective technical capacity building. It is conducted through self-learning modules, classroom modules, or a combination of the two. These trainings typically take 10 to 12 weeks through a mixed-module course, including both self-training and supported classroom discussions. An understanding of the platform, its usage, and its features is essential for every SI to qualify as a MOSIP partner.

MOSIP also created the MOSIP Marketplace to help country adopters discover partners that are compliant with MOSIP. The marketplace lists details of the SIs that successfully finished the partner program, as well as devices and solutions that are under different stages of compliance. This helps adopters quickly identify the range of products and manufacturers available to them that are ready to use with MOSIP.



MOSIP has also set up the MOSIP Experience Center (MEC) at IIITB, where adopters and vendors can get an end-to-end experience of the MOSIP platform. MEC provides a space where potential adopters and users can test technologies, devices, and solutions, thus reducing the time and risk of actual implementation. MOSIP is now exploring setting up MECs in different regions to benefit countries where MOSIP is in high demand. The MECs will also serve as a space where the integration of MOSIP with other services like civil registration systems, e-sign, and electronic health records management can be tested.

Governance and Funding

The support that MOSIP received from the World Bank and its funders has been significant. MOSIP's initial project estimate was approximately $800,000, but the actual expenses in the first phase of development added up to $8 million. However, the funders were undaunted. The MOSIP team committed to having implementations in two countries in the first phase of three years but exceeded that number. Funders could see that the project could reach 360 million people in a few years and therefore continued supporting the project. MOSIP has an executive committee (EC) and a technical committee (TC) that operate independently of each other. The EC focuses on operations while the TC focuses on innovation. The TC does not take instructions from the EC, but it creates roadmaps and asks the EC for funds. MOSIP also has an international advisory board that advises on strategy. This governance structure ensures that technology decisions are not influenced by funders or business considerations and helps ensure sustainability.

MOSIP has benefited from interest in the project and advice from veteran technologists like Nandan Nilekani of Infosys and Bill Gates. Nilekani suggested that MOSIP not write a single line of code until it secured one or two clients. This ensured that MOSIP was built to real-world specifications. Gates advised that each country's design should be different and suggested that MOSIP identify 10 designs/archetypes so that a wide variety of use cases could be covered.

II. Challenges

Safeguards

Privacy is a central concern with digital ID systems. In the absence of robust checks and balances, a government-controlled digital ID system could give governments unfettered powers of surveillance. The privacy risks caused by government surveillance can be much greater than those resulting from private-sector surveillance, since governments control coercive instruments like the army, police, and tax authorities.

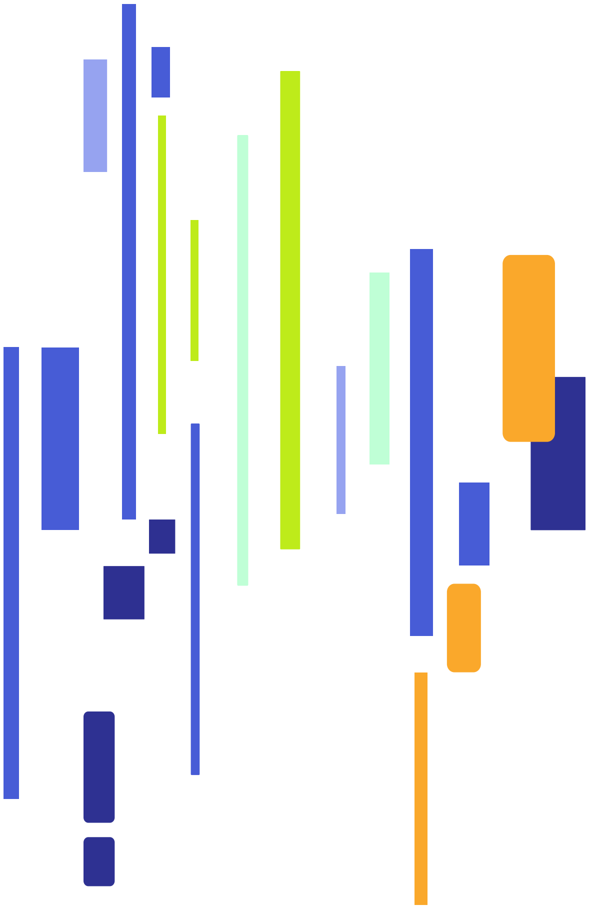
Recognizing this, funders and multilateral organizations have often grappled with whether and how to support digital ID implementations in countries that do not have privacy laws in place or have a poor record of human rights.

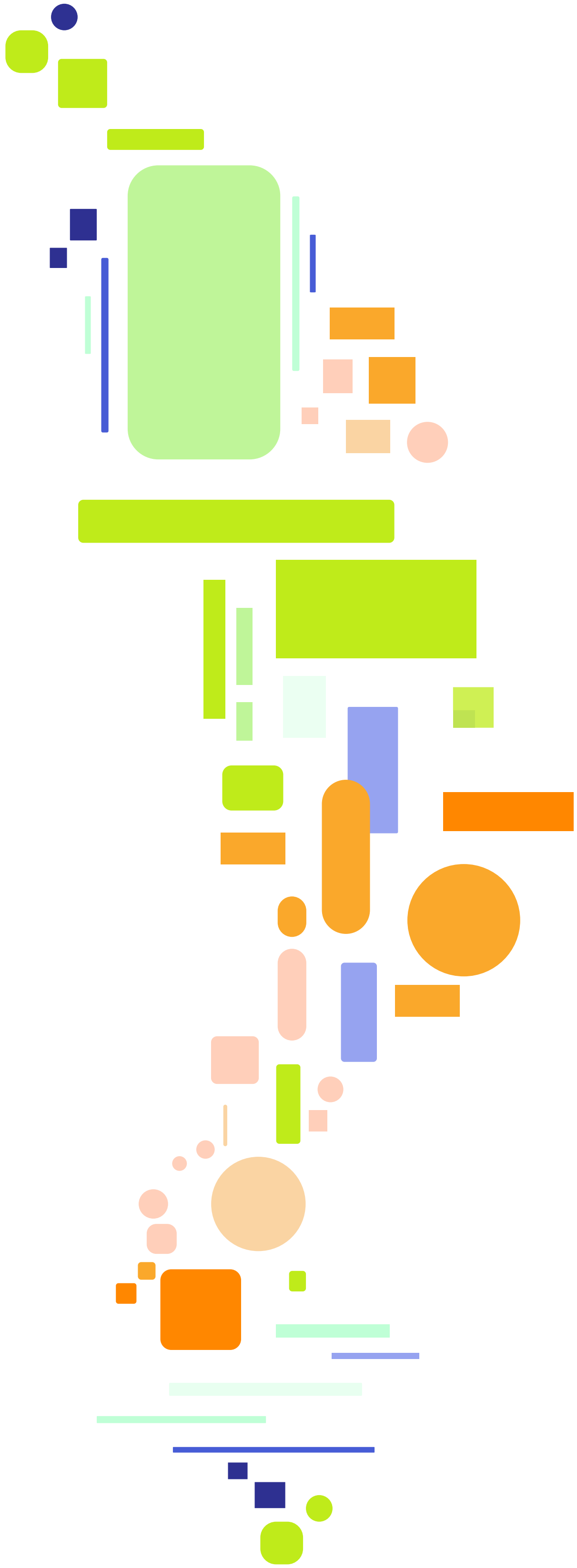
As recent events in a few democratic countries demonstrate, however, a single election can lead to a radical regime change. Therefore, it is not clear whether safeguards can be built into digital ID systems that protect the privacy of individuals from the vagaries of regime change. This challenge has led many to emphasize the need for both "privacy by design" and "privacy by policy" protections, i.e., technology design alone cannot guarantee sufficient safeguards.

Currently, MOSIP's engagement model involves signing a memorandum of understanding (MOU) with a country and working with its government to implement an ID system for its citizens. Though MOSIP plans to build applications that allow citizens to control how their data is used, disable biometrics to prevent misuse, and add many more privacy features, the fact is that governments are the central clients and operators of MOSIP deployments. In other words, citizens are dependent on the government acting in their best interests when issuing and controlling their digital identities.

MOSIP does include many privacy and security by design features that safeguard citizens' interests. For example, it allows only 1:1 searches and does not allow 1:N searches. This means that the database can be searched only against a particular ID at one time. For example, the police or another authority cannot bring a fingerprint from a crime scene and ask for it to be matched with fingerprints in the MOSIP database. It also enables zero-knowledge administration so that administrators can manage data without being able to see the actual data. But since MOSIP is open source, a government can modify the code as it wishes.

These challenges highlight the need for a wider discussion on the risks of digital public infrastructure (DPI) solutions and the safeguards that need to be built into them.





Sustainability

The sustainability of digital public goods (DPGs) is an open question in the minds of everyone in the DPG ecosystem. DPGs need market adoption, sustained resources for technology development, and an ecosystem of system integrators (SIs) who will help adopters deploy the technology on the ground.

On the market adoption front, MOSIP is doing quite well. In terms of resources, most DPGs are grant funded and have no other source of income. However, MOSIP's Rajagopalan feels that given the critical nature of digital identity solutions, governments will come forward to support MOSIP.

The obvious answer is to charge countries for using the MOSIP system. However, DPGs usually want to preserve their "trusted advisor" status and not create a vendor-client relationship by accepting money directly from adopters. An alternative funding model could be membership fees from governments and SIs that go to support DPGs. Many open-source foundations function in this manner.

DPGs like MOSIP could also benefit from building an open-source community that helps drive the development of the technology. At present, many DPG developers and funders look at open source as an afterthought. An earlier paper from the Digital Impact Alliance recommended that DPGs prioritize building an open-source community from the inception stage itself, to ensure long-term sustainability.[7]

MOSIP's Rajagopalan believes that MOSIP could have built a vendor ecosystem and open-source community programs much earlier. While the vendor ecosystem programs are now on track, the open-source efforts are still a work in progress. In the initial phase, the development of the MOSIP software was outsourced to a software services company. The resulting code was released under an open-source license, but the project lacked a community of developers who could build and enhance the MOSIP platform. Five years after inception, most of MOSIP's development is managed by the in-house team. However, open-source contributions have slowly started coming in. Countries like Ethiopia have started contributing back to the MOSIP code base, and the project team aims to increase community participation at every level of the project.

The MOSIP team's experience has been that people and organizations that have a stake in the success of MOSIP are more likely to contribute to the project. With this understanding, they have created a three-pronged strategy for building a community:

The user community:

The MOSIP team aims to convene a community of active users contributing to the project's direction, as opposed to passive consumers of the solution. Individual countries have already started to make useful contributions through code fixes, bug reports, and feature requests. The project aims to enable an organic grouping of MOSIP adopters who will share lessons and knowledge with each other, provide feedback, make feature requests, and participate in the standards-making exercise.

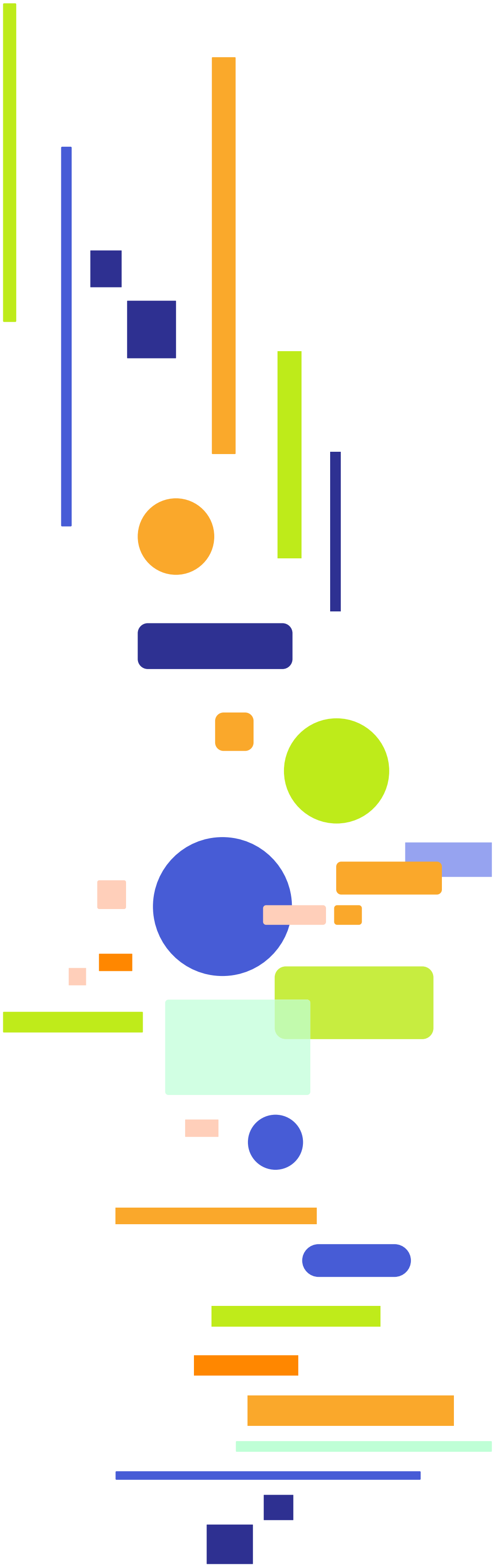
The commercial ecosystem:

MOSIP's commercial ecosystem has contributed to the project through multiple initiatives, such as review and definition of MOSIP standards and interfaces, collaborative development of an Android registration client, and participation in pilots through pro bono deployment of solutions for field testing.

Pro bono code contributions and secondment:

MOSIP's technology has benefited from a cumulative contribution of 20,000 person hours from SIs to date. These contributions have been in the form of feature development and engineering talent for code development, and there are plans to expand this program further.

Conclusion



The way the MOSIP project has scaled rapidly holds many lessons for the digital public goods (DPG) ecosystem. The shared challenges faced by DPGs are around building adoption, sustainability of the project, nurturing open-source communities, and creating a vendor ecosystem. The way the MOSIP team did pilot projects, evangelized the project at events like ID4Africa, and built confidence in the platform holds many useful lessons. The ecosystem of system integrators (SIs), hardware vendors, and independent software vendors that has been built around the MOSIP platform is another playbook worth emulating. Where the project could have been done better is in building a community of open-source contributors from the early stage of the project. Over the next few years, how the project cracks the sustainability question will be interesting to watch. Will it continue to be grant funded? Will countries that are deploying MOSIP contribute back to the core project by providing funding and development support? As MOSIP achieves nation-scale deployments, the lessons and best practices will also interest the nascent DPG ecosystem. Hopefully, this paper provides some early insights on developing and deploying a DPG that is useful to DPG developers and funders.

Acknowledgements

We thank Prof. S Rajagopalan, president of MOSIP; Sharad Sharma, co-founder of Indian Software Product Industry Round Table (iSPIRT); Arun Kumar Gurumurthy, head of strategy and resourcing at MOSIP; and Govind Shivkumar, Omidyar Network for their insights on MOSIP and the DPG sector.

Endnotes

[1] See "100 Million Registered Residents Worldwide!" at https://mosip.io/news_events/100-million-registered-residents

[2] ID4D Global Dataset: https://id4d.worldbank.org/global-dataset

[3] See, "Good ID supports multiple development goals," at https://id4d.worldbank.org/guide/good-id-supports-multiple-development-goals

[4] Ensuring uniqueness is the key task for an ID system. For example, if there are 100 individuals named John Doe, and one of them is eligible for social welfare benefits from the government, the ID system can help ensure that the benefits go to the correct John Doe. This is done by providing unique ID numbers and capturing unique identifiers like fingerprints or iris scans.

[5] UN Secretary General's Roadmap for Digital Cooperation at https://www.un.org/en/content/digital-cooperation-roadmap/

[6] "Maturing MOSIP enjoys ID4Africa limelight as it expands its partnerships and vendors flock," at https://www.biometricupdate.com/202206/maturing-mosip-enjoys-id4africa-limelight-as-it-expands-its-partnerships-and-vendors-flock

[7] Hariharan, Venkatesh, *Can We Future-Proof Digital Public Goods? Rethinking Sustainable Business Models,* Digital Impact Alliance, 2022.