Understanding MOSIP: What the Modular Open-Source Identity Platform Is and How It Is Used

by Biometric Update

BIOMETRIC UPDATE.COM

Executive Summary

MOSIP (Modular Open Source Identity Platform) is an initiative designed to help countries build functional digital identity systems, such as national ID programs, without the risk of vendor lock-in. It combines a modular, open-source software core with a growing ecosystem of technology providers and partners that support implementation and service development.

The United Nations has set a target of achieving "legal identity for all, including birth registration" by 2030 under Sustainable Development Goal 16, which links identity to peace, justice and strong public institutions. MOSIP can help countries use legal identity to achieve the intended benefits of SDG 16 by enabling public institutions to deliver services to beneficiaries.

MOSIP implementations vary widely across countries. Some, such as Morocco, use the platform to support civil registration and social protection systems rather than a primary national ID. Others deploy specific modules to extend existing identity infrastructure, while many are building end-to-end identification and authentication systems to support public service delivery.

The platform supports processes ranging from biometric and biographic enrollment—including birth registration—to credential issuance, authentication and service access.

By using open-source software and standardized interfaces, MOSIP enables governments to select and change technology providers without being constrained by proprietary systems or biometric templates. This approach addresses the "vendor lock-in" problem identified as a major barrier—particularly for countries in the Global South—at the ID4Africa 2018 Annual General Meeting, where the initiative was first introduced.

The MOSIP platform and ecosystem continue to evolve, with new tools, features and integrations—including digital payments—added over time.

Its geographic reach is expanding, with deployments across Africa, Southeast Asia, and increasingly Latin America and the Caribbean. Hundreds of millions of people are already enrolled in MOSIP-based systems, with ongoing projects expected to extend coverage significantly in the coming years.

As deployments scale, MOSIP is increasingly shaping how countries design digital public infrastructure, linking identity with payments and service delivery in ways that influence both governance models and digital economies.

Introduction to MOSIP

MOSIP is increasingly being adopted by governments as a global framework for building digital identity systems without vendor lock-in. It provides a modular platform that can be customized and scaled to national requirements, alongside an ecosystem of partners supporting implementation and service development.

Its core objective is to give governments greater control over identity infrastructure without relying on proprietary technologies, while reducing the cost and complexity of deploying systems at national scale.

The concept behind MOSIP was influenced by India's Unique Identification Authority of India Aadhaar program, launched in 2009. Aadhaar demonstrated the potential of digital identity to expand inclusion, reduce fraud and improve access to services, but its architecture was highly customized and not designed for replication in other national contexts.

MOSIP emerged as a response to this gap. Technologists and policy experts associated with the International Institute of Information Technology Bangalore, with support from Nandan Nilekani, began developing a modular, open-source platform that could be adapted by countries seeking to build sovereign identity systems.

The platform was formally launched in 2018 and introduced as a digital public good at the 2018 ID4Africa Annual General Meeting. It has since been recognized by the Digital Public Goods Alliance as a verified digital public good, reflecting its open, reusable and standards-based approach.

MOSIP combines a core software platform with design principles for national-scale identity systems. Its modular architecture allows governments to deploy and customize components such as enrollment, credential issuance, authentication and data management, while maintaining interoperability with existing systems and international standards.

Privacy-by-design is a central feature, incorporating data minimization, consent frameworks and encryption. The platform is licensed under the Mozilla Public License 2.0, enabling

governments to avoid vendor lock-in and retain long-term control over identity infrastructure.

Initial development was supported by philanthropic funding from organizations including the Bill & Melinda Gates Foundation, Omidyar Network and Tata Trusts. Since then, MOSIP has evolved into a global initiative with deployments across multiple regions and a growing ecosystem of technology providers and system integrators.

In parallel, MOSIP has expanded its community through initiatives such as MOSIP Connect, launched in 2024, which brings together governments, technology partners and development organizations to share implementation experience and advance digital identity practices.

MOSIP is increasingly positioned as a foundational layer of digital public infrastructure, linking identity with payments, credentials and service delivery systems.

Terms and definitions

Open-source software (OSS): Software whose source code is publicly available and can be used, studied, modified and redistributed without licensing fees. OSS is typically associated with transparency, collaboration and flexibility, and allows governments to avoid vendor lock-in while maintaining control over systems.

Modular architecture: A software design approach in which a system is composed of independent components ("modules") that perform specific functions. Modules can be developed, updated or replaced without affecting the entire system, enabling scalability, interoperability and maintainability.

Legal identity: The officially recognized existence of a person under the law, typically established through civil registration (such as birth registration). It includes core attributes like name, date of birth and nationality, and underpins access to rights and services. The United Nations Sustainable Development Goal 16.9 calls for legal identity for all by 2030.

Digital identity (digital ID): The digital representation of an individual's identity, composed of attributes such as personal data and, in some cases, biometric identifiers. Digital identity enables authentication and access to services in digital environments.

National ID card: A government-issued credential that serves as proof of legal identity and, in many cases, nationality. National ID systems are often integrated with public and private services.

Digital public infrastructure (DPI): Foundational digital systems that enable service delivery and economic participation at scale. DPI typically includes digital identity, digital payments and data exchange layers, designed to be interoperable, secure and inclusive.

Civil registration: The continuous and compulsory recording of vital events such as births, deaths and marriages. It forms the basis of legal identity and supports governance, public services and population statistics.

Biometrics: Measurable biological or behavioral characteristics—such as facial features, fingerprints or iris patterns—used to verify or authenticate an individual's identity.

Biometric authentication: The process of verifying an individual's identity using biometric data. It is commonly used in digital identity systems, often alongside other authentication factors, and raises considerations around privacy, security and data protection.

e-Signet: An authentication and credential management component within the MOSIP ecosystem. It enables identity verification through standards-based login (e.g., OpenID Connect), supports multiple authentication methods including biometrics, and facilitates secure data sharing through APIs.

Inji: A digital credential wallet and verification stack in the MOSIP ecosystem. It allows users to store, share and verify identity credentials, supporting privacy-preserving data sharing and digital portability.

MOSIP Connect: An annual event organized by MOSIP that brings together governments, technology providers and development partners to share implementation experiences and advance digital identity ecosystems.

Software development kits (SDKs): Collections of tools, libraries and documentation that enable developers to build applications for specific platforms or services.

Application programming interfaces (APIs): Defined protocols that allow different software systems to communicate and exchange data. APIs are essential for integrating services within digital identity ecosystems.

Partner ecosystem: The network of technology providers, system integrators and service organizations that support MOSIP implementations. This ecosystem enables countries to deploy and operate identity systems using interoperable components from multiple vendors.

OpenCRVS: An open-source civil registration platform for recording life events such as births and deaths. It can integrate with MOSIP-based systems and is designed for secure and resilient operation, including in low-connectivity environments.

OpenG2P: A digital public infrastructure platform used to deliver social protection programs such as cash transfers. It integrates with MOSIP components to enable identity verification and beneficiary management.

Building an open ID services ecosystem from vision to sustainability

In conversation with Sanjith Sundaram, Head of Partner Ecosystem

MOSIP is essentially a piece of code – the modular core of the platform – and a university initiative, according to Head of Partner Ecosystem Sanjith Sundaram.

The International Institute of Information Technology Bangalore (IIIT-B) established MOSIP in 2018 to be a core component for Digital Public Infrastructure and hosts the initiative.

Sundaram compares MOSIP's modular approach to Lego, with standardized interfaces not only making it easy for users to build with, but also for third parties to build expansions and new components for the platform. The "Lego blocks" provided by MOSIP are the core platform and accompanying modules, like the Inji digital wallet for credential issuance.

"We create these blocks and then put them there in the GitHub for people to consume," Sundaram says.

Countries begin with an understanding of what they need to do for their population, but at widely varying starting points in terms of understanding how to build that capability.

"Everything around the code, you need some capacity," observes Sundaram.

MOSIP initiatives beyond code development are therefore geared towards building capacity. That includes for technology vendors and Systems Integrators, but even more so for governments and local partners.

Knowledge-sharing is also central to MOSIP's vision, and Sundaram lauds early adopters like Morocco, the Philippines and Ethiopia for taking the step of MOSIP adoption without the benefit of successfully completed implementations to guide them, but also as a source of trust in MOSIP for the countries that have come after.

Ensuring the mission is sustainable

MOSIP was created with initial funding from a small group of philanthropic organizations, led by the Bill and Melinda Gates Foundation (see below for further detail).

The organization is now planning for a future beyond the support of donor bodies like the Gates Foundation, which may include finding different sources of funding.

Fortunately, Sundaram says, MOSIP is well-positioned to evolve in a way that ensures its mission is sustainable.

From the perspective of MOSIP, like any ecosystem's originator, he says, "sustainability is when you are able to grow the story and progress without you explicitly putting a lot of effort into it."

The Marketplace has matured significantly. While it will continue to evolve, Sundaram says, its place is now established. "There are partners who, instead of asking why they should do this are asking 'how do we do this?'"

MOSIP is no longer actively looking for new biometric device partners – the Marketplace provides a healthy amount of market choice, and technology providers can join of their own volition to sell into the MOSIP ecosystem.

Future changes to the Marketplace will likely include new sections and compliance exercises, such as for hardware security modules (HSMs), and resources to clarify how technologies contribute to public service delivery use cases.

Sustainability can be maintained in part by shifting responsibility to the community, such as potentially for maintaining the code.

At its inception, MOSIP could not rely only on community contributions to develop its code, Sundaram explains, because the needs of implementing countries are too time-sensitive to wait for independent developers to complete commitments.

There are already a number of additional modules and extensions to the platform contributed or co-developed with the community.

The Decode hackathon for students provides mentorship for the next generation of developers in the field, and the Create competition for commercial developers can help supply technology for specific use cases, Sundaram says.

At MOSIP Connect 2026 in Rabat, Morocco, several MOSIP officials addressed the sustainability question. MOSIP Chair Prof. Debabrata Das noted that "open source" means sharing not just code, but also research.

President Prof. S. Rajagopalan noted the importance of revenue for MOSIP's commercial partners to the sustainability of the overall ecosystem. A positive sign for MOSIP's long-term sustainability is the emergence of engagements driven by Systems Integrators, the first examples of which are Tonga and Trinidad and Tobago.

MOSIP's mandate is not to convince every country in the world to do a pilot, however, Sundaram points out. The organization's long-term strategy is to encourage SIs to select MOSIP as a Digital Public Good for the benefit of their customers.

Discussions about how to ensure long-term sustainability are ongoing among MOSIP leadership. Whatever happens, MOSIP will continue to exist as a non-profit with the mandate to help countries succeed in their digital identity ambitions.

How MOSIP core and projects are funded

MOSIP's development and global expansion have been driven primarily by philanthropic and development funding since its launch in 2018. Financial support from international donors has enabled the platform to evolve from a university-led initiative into a widely adopted foundation for digital identity systems.

Key funders include the **Bill & Melinda Gates Foundation**, **Omidyar Network**, **Tata Trusts**, **Pratiksha Trust**, and the **Norwegian Agency for Development Cooperation (NORAD)**. Initial funding totaled approximately $28 million, with subsequent grants supporting ongoing development, ecosystem building and country engagement. MOSIP's annual operating budget is estimated at between $5 million and $7 million.

Recent grant commitments underline continued donor support. The Gates Foundation, for example, has two active grants to the International Institute of Information Technology Bangalore (IIIT-B) totaling more than $28 million, extending through 2028 and 2029.

This funding has enabled MOSIP to build its modular architecture, invest in research and development, and support capacity-building efforts across governments and ecosystem partners. It has also helped establish a global footprint: by the end of 2025, MOSIP reported 29 country partners, more than 161 million registered users, and over 2,500 individuals trained on the platform.

MOSIP's growth reflects a broader pattern in digital public infrastructure, where early-stage innovation is often supported by philanthropic capital before transitioning toward more distributed, market-driven models.

From donor funding to ecosystem sustainability

While donor funding has been central to MOSIP's development, the organization is actively working to reduce long-term reliance on philanthropic support.

One emerging approach is ecosystem co-creation. MOSIP has used its funding to build a network of approximately 100 commercial partners, including system integrators, technology providers

and service organizations. These partners contribute to implementation, innovation and long-term maintenance of identity systems.

MOSIP President Prof. S. Rajagopalan has emphasized that sustainability will depend on expanding this shared ownership model:

“It is very important for our long-term sustainability. You have to understand that we are a university. And for a university to sustain anything on a long-term basis, you cannot solely depend on charity and philanthropic support. So, we need to build creative capacity across the world so that even if, for some reason, things change, the system should be sustained.

“Countries interface with the people in the provision of services and that has to be sustained. So, we have to have the technology that can be sustainable for centuries. One way of doing that is to co-create not only with our commercial partners, but also with universities. We are trying to establish a centre of excellence in the Mohammed VI Polytechnic University in Morocco, near Marrakesh. We are also talking to some universities here in Addis Ababa and in Manila. The idea is we’ll jointly discuss what should be their roadmap, how they will help with ecosystem partners. We will co-create solutions with ecosystem partners, universities and governments.”

This model reflects a broader shift toward shared responsibility across governments, academia and commercial partners, aimed at ensuring that MOSIP-based systems remain operational and adaptable over the long term.

Funding digital ID implementations at country level

In parallel with funding for the core platform, many MOSIP-based identity programs are financed through development institutions and multilateral funding mechanisms.

For example, Ethiopia’s national digital ID program is supported by a $350 million World Bank-funded Digital ID for Inclusion and Services project, while Nigeria’s digital identity expansion — including migration toward a MOSIP-based system — is backed by the World Bank alongside the European Investment Bank and the Agence Française de Développement.

These funding models highlight a key distinction:

- MOSIP core platform: primarily donor-funded
- Country implementations: largely financed through development finance and government-backed programs

This dual structure has enabled MOSIP to scale globally while aligning with national digital transformation strategies and development priorities.

Risks and future outlook

Despite its success, MOSIP's funding model faces potential long-term challenges. The Bill & Melinda Gates Foundation has signaled plans to scale back aspects of its global financial inclusion support by 2030, raising questions about the future availability of large-scale philanthropic funding for digital public infrastructure.

However, MOSIP's growing ecosystem, expanding marketplace and increasing involvement of system integrators suggest a gradual transition toward a more self-sustaining model.

The long-term viability of MOSIP will depend on its ability to balance three elements:

- continued donor support in the near term
- increased commercial participation within the ecosystem
- sustained investment in country-level implementations

If successful, this model would position MOSIP not just as a donor-backed initiative, but as a durable layer of global digital infrastructure.

How does a typical MOSIP implementation happen?

MOSIP implementations follow a structured, phased approach that moves from early engagement and testing to full-scale national deployment. While country contexts vary, most implementations share a common progression: pilot, planning, procurement and rollout.

Pilot phase: testing and capacity building

MOSIP implementations typically begin with engagement between the country and MOSIP officials, after which the country signs a Memorandum of Understanding with MOSIP to carry out a pilot.

MOSIP uses a Rapid Pilot Model, which Sundaram describes as primarily a capacity-building program, like many MOSIP initiatives.

It comes at no cost to the country, with MOSIP's partner ecosystem supplying sample devices, ABIS licenses and SDKs. MOSIP leads this part of the three to four-month process, which comes with no obligation. During that time, a small sample of two or three thousand people may be registered.

This pilot is "a learning environment for everyone," Sundaram says. That includes engineers assigned by the country to learn the system with no-cost training. In most cases registrations are not considered a production deployment, Sundaram says, so the data is safely discarded after the pilot is complete.

The pilot involves very limited customization or integration efforts, so there is no role at that point for a Systems Integrator.

The complete pilot provides information on the capacity of the country, and Sundaram says "they will be in a much better position to make an informed decision on whether they should go for MOSIP, or say an entirely proprietary solution."

Thus far, most countries that have completed MOSIP pilots have continued towards production rollouts.

Planning and procurement: from pilot to program

Countries that proceed with MOSIP implementation must then source funding for the project. While the pilot process is free and MOSIP does not

receive payment for the source code or its resources, implementations require the expertise of Systems Integrators, the hardware that enables registration and the software that enables service delivery. The MOSIP Marketplace is specifically designed to assist in the decisions made during this part of the process.

The MOSIP team will also point out the characteristics that Marketplace status leaves up to countries to validate, such as biometric data quality or performance level. MOSIP advises countries to do additional validations, such as checking technology providers' prior experience and presence in global benchmarking exercises.

In some cases, Sundaram says, countries are advised to make a short list of candidate technology providers from the MOSIP Marketplace, and then conduct "a small capability test locally."

The initial pilot informs an approximate budget, and typically also informs discussions with international development bodies like the World Bank's Identification for Development (ID4D) initiative, the Inter-American Development Bank or Asian Development Bank. Some smaller-scale activities have been funded by bodies like Co-Develop, Sundaram notes.

"Bodies like ID4D have their own technical expertise as well," he adds. The country, MOSIP, and funding body can all contribute to the project.

Beyond budgeting, planning should include consideration of the appropriate technical standards and regulatory requirements.

Lessons from implementation: prioritizing use cases

A key lesson that Sundaram says comes from early implementations of MOSIP is to focus on what he calls "time-to-inclusion." While many countries establishing digital ID systems concentrate first on enrolling as much of their population as possible, Sundaram says "You should start your use-cases journey ahead of time."

Concentrating on use cases will not only give the public a real-life example of the system's benefits, it could also "help you to fine-tune your approach to the enrollment as well," according to Sundaram.

Launching use cases in parallel with early enrollment efforts can help ensure inclusive service delivery targets are quickly met, while building public trust in and acceptance of the system.

One example of this approach is seen in Sri Lanka showcasing use cases for its national digital identity even as enrollment continues.

Many of the other lessons are best explained by the countries that have learned them first-hand, Sundaram suggests. One example he gives is Ethiopia's approach to exceptions-handling during its biometrics registration process.

MOSIP standards development

MOSIP underpins its ecosystem with a structured framework of standards, specifications and compliance mechanisms designed to ensure interoperability, security and trust across implementations.

The platform defines technical specifications for its core modules while aligning with widely adopted international standards in areas such as biometrics, security, cryptography, privacy and identity protocols. These include standards such as ISO/IEC 19794 for biometric data formats, OAuth 2.0 and OpenID Connect for authentication, and emerging specifications like IEEE P3167.

Standards across MOSIP components

MOSIP's architecture incorporates both global standards and platform-specific specifications.

- **Inji**, the digital credential wallet, is built on W3C Verifiable Credentials and OpenID for Verifiable Credential Issuance (OpenID4VCI), enabling interoperable and privacy-preserving credential exchange.
- **e-Signet**, the authentication layer, relies on OAuth 2.0 and OpenID Connect Core 1.0 to support secure identity verification and login flows.

MOSIP has also developed its own specifications where needed. One example is **Claim 169**, a standard for embedding demographic and biometric data within a digitally signed QR code, registered within the IANA CBOR Web Token (CWT) registry.

Compliance and certification framework

Beyond defining standards, MOSIP enforces them through a compliance framework governing participation in its ecosystem.

Technology providers listed in the MOSIP Marketplace must meet baseline requirements covering areas such as biometric capture, data encryption and interoperability. These are initially validated through a self-certification process.

For higher assurance, MOSIP operates the **MOSIP Advanced Compliance Program (MACP)**, which introduces independent testing and certification requirements.

The program applies to key components such as:

- biometric capture devices
- automated biometric identification systems (ABIS)
- software development kits (SDKs)
- print and credential issuance solutions

MACP-certified technologies must meet defined thresholds for performance, including image quality and liveness detection.

Independent validation is carried out by MOSIP-accredited laboratories. Australia-based **BixeLab** is the first accredited testing partner, while UK-based **Ingenium Biometric Laboratories** is progressing through the accreditation pipeline.

Balancing openness and control

MOSIP's standards strategy reflects a balance between openness and governance. While the platform promotes interoperability through alignment with global standards, it also maintains control through certification and compliance requirements.

This dual approach enables countries to adopt a wide range of technologies while ensuring that systems meet consistent benchmarks for security, performance and reliability.

The MOSIP Marketplace

MOSIP manages a structured ecosystem of vendors through its online Marketplace, designed to support the customization, implementation and long-term operation of national digital identity systems.

Digital identity projects carry high technical, financial and political stakes. At the same time, governments often face a fragmented and opaque supplier landscape.

“The commercial environment can be difficult to navigate through with a traditional supply model,” says Sanjith Sundaram, Head of Partner Ecosystem at MOSIP.

The Marketplace is intended to address this challenge by creating a curated, standards-based environment where countries can identify trusted technology partners.

As of May 2026, the MOSIP Marketplace includes more than 80 technology solution providers and over 25 systems integrators. While vendors are grouped into different categories, interoperability is the common requirement across all participants.

Compliance as the entry point

Participation in the Marketplace is governed by MOSIP’s Compliance Toolkit (CTK), which enables vendors to assess whether their technologies meet MOSIP specifications.

“It’s not just that someone applies and then we grant them a place,” Sundaram says. “They have to go through a rigorous program.”

The compliance process includes:

- self-assessment against MOSIP standards
- interface-level validation
- testing of encryption, protocols and data formats

This ensures that solutions can integrate with MOSIP without requiring additional development work.

However, the CTK does not fully assess biometric performance. For this, MOSIP relies on independent, accredited testing laboratories operating under a separate compliance framework.

Structuring the vendor ecosystem

The Marketplace organizes solutions across several categories, including:

- registration devices
- authentication devices
- automated biometric identification systems (ABIS)
- biometric SDKs
- print solutions
- accredited testing laboratories

Registration devices typically support multi-modal biometric capture, while authentication devices are often modality-specific.

Devices are also classified by security level:

- **L0**: encryption occurs after data reaches the server
- **L1**: encryption occurs at the point of capture

MOSIP’s Advanced Compliance Program (MACP) adds a higher level of assurance

by requiring independent certification of biometric devices, including performance and security testing.

Australia-based **BixeLab** is the first accredited MACP laboratory and issued the first certifications in 2024, while **Ingenium Biometric Laboratories** is in the process of accreditation.

Biometix, the consultancy cousin of BixeLab, also implemented an open-source version of its BQAT (biometric quality assessment tool) for use with MOSIP. Openbq is a collection of biometric quality assessment algorithms and analysis tools.

The role of systems integrators

Systems integrators (SIs) play a central role in MOSIP implementations, but their pathway into the Marketplace differs from technology vendors.

To qualify, SIs must:

- join the MOSIP Partner Programme
- train engineers through the MOSIP Academy
- complete a successful sandbox implementation

This ensures that SIs have hands-on experience deploying MOSIP before working on national-scale projects.

MOSIP distinguishes between:

- **Technology SIs**, typically smaller or regional firms building capacity
- **Commercial SIs**, larger organizations with extensive delivery experience

According to Sundaram, the ecosystem now includes around 50 partners, ranging from local consortiums to global technology firms.

Beyond procurement: a knowledge ecosystem

The Marketplace is evolving beyond a vendor directory into a broader knowledge platform.

Future updates are expected to include:

- liveness detection and Presentation Attack Detection (PAD) requirements
- expanded compliance frameworks
- partner-led collaboration initiatives
- shared knowledge repositories

MOSIP also plans to develop the Marketplace into a “repository of use cases,” featuring real-world examples of how digital identity systems are deployed in practice.

These case-based resources are intended to help governments better understand implementation choices, including build-versus-buy decisions.

Reducing risk, enabling choice

While the Marketplace connects governments with vendors, its primary function is to reduce risk in decision-making.

“The guarantee that’s given to a country is that the partner has completed the MOSIP compliance program,” Sundaram says. “That means they don’t have to do development work to get solutions onto MOSIP.”

Understanding MOSIP integrations

When it comes to digital public infrastructure (DPI), the value lies not in individual systems, but in how they connect. Linking digital identity, payments and data exchange platforms enables seamless, secure and interoperable service delivery across both public and private sectors.

This process of connecting systems is what defines integration.

In MOSIP implementations, integration is central to unlocking real-world use cases. The platform's API-first, modular architecture allows identity systems built on MOSIP to connect with external services in areas such as healthcare, education, financial services and digital government.

Integration through modular identity components

MOSIP supports integration through its core components, particularly its authentication and credential layers.

Its OpenID-based authentication service, eSignet, enables secure identity verification, while its credential stack, Inji, supports the issuance, storage and validation of digital credentials.

Inji consists of three main components:

- **Inji Wallet** for secure credential storage
- **Inji Certify** for issuing trusted digital credentials
- **Inji Verify** for validating those credentials

Together, eSignet and Inji allow governments and service providers to implement secure login, identity verification and credential management at scale.

Peru, for example, is exploring integration between the Inji wallet and its national authentication middleware to enable identity verification across government services.

Enabling service delivery through integrations

MOSIP integrations extend beyond identity into service delivery systems.

OpenG2P, a platform for government-to-person payments, integrates with MOSIP through eSignet to enable identity verification using biometric, OTP and demographic authentication.

In Sri Lanka, this integration is already being applied in practice. An “Experience Centre” built on MOSIP and OpenG2P supports access to more than 20 public service use cases, including financial inclusion programs.

Similarly, technology providers are integrating solutions directly into the MOSIP ecosystem. When Tech5 integrated its T5-IDencode platform, it highlighted gains in efficiency, including faster ID issuance and improved lifecycle management.

Civil registration and the identity lifecycle

One of the most significant integrations is between MOSIP and OpenCRVS, an open-source civil registration system used to record life events such as births and deaths.

Through a dedicated interoperability API, OpenCRVS can directly create or update identity records in a MOSIP-based system. This allows identity to be established at birth and maintained throughout a person’s lifecycle.

Tonga is one example where civil registration is already linked to a MOSIP-based national ID system.

This approach aligns with the United Nations Legal Identity Agenda and the Sustainable Development Goal (SDG) 16.9 target of providing legal identity for all, including birth registration, by 2030.

From identity system to infrastructure layer

The integration of MOSIP with payments, civil registration and service delivery platforms enables more than just identity verification — it creates a continuous, interoperable identity ecosystem.

These integrations:

- support real-time service delivery
- enable secure data exchange
- improve efficiency and targeting of government programs
- strengthen trust through consistent identity verification

Case studies

The following case studies illustrate how countries are deploying MOSIP in different contexts, from social protection systems to national identity programs. While implementation paths vary, common themes include the importance of governance, ecosystem adoption, digital sovereignty and the ability to scale identity infrastructure into real-world services.

Morocco: MOSIP for social protection and population registry

Morocco, which hosted the 2026 edition of the MOSIP Connect event, has an interesting story with the open source identity platform. Not only was it the first country in the world to sign a Memorandum of Understanding (MoU) for a MOSIP implementation, it is also now cited among the success stories of all implementations of the platform in Africa and the world.

The MoU was signed between Morocco's Ministry of Interior and MOSIP authorities on August 27, 2018, to lay the groundwork for collaboration on the implementation of a social safety net database and a social registry based on MOSIP. This was just months after MOSIP was officially launched as a start-up initiative.

Unlike many other countries which used or are using MOSIP to build their main national ID systems, Morocco used it to build a National Population Registry (RNP), kind of a foundational repository to facilitate access to social digital services. Beyond that, the MOSIP system is also used for digital Know Your Customer (e-KYC) by some government departments for identity verification when enrolling people in social programs.

Meanwhile, Morocco's main national identity system is known as the Carte Nationale d'Identité Électronique (CNIE), a biometric smart card, managed by the Directorate General of National Security (DGSN) under the Ministry of Interior. It is mandatory for all Moroccans aged 16 and above and is used for general legal identification purposes.

Successful pilot

After a successful pilot, the country was able to scale the RNP social protection system for nationwide rollout. The pilot, according to officials, took place in a phased manner as the government wanted to ensure the effective scale-up of the system in all the parts of the country. During the pilot, for example, which started in December 2021 and ended sometime in early 2022, the enrollment component of the system was tested at nearly 1,500 citizen service centers (CSCs).

Today, the North African country's social protection delivery system is widely considered robust, in part because it is anchored in a foundational framework built on MOSIP. Thanks to the RNP which is based and run on one of MOSIP's modules, the Moroccan government issues a 10-digit unique identification number which is used to access social benefits.

Designed to complement the country's national ID card system which has been in place for many years and follows a different identity track with different legal identification purposes, the MOSIP-based RNP has proven vital in the country's push for social and economic inclusion.

"The RNP, based on MOSIP, contains two main components. The first is enrollment which facilitates registering

individuals and generating an ID, which in Morocco is called the Digital Civil Social ID (IDCS). This ID is used exclusively for social services, not for banking or telecommunications purposes," an official with the Ministry of Interior told Biometric Update in a chat on the sidelines of MOSIP Connect 2026 in Rabat.

"The other aspect is authentication, and this has to do with verifying the identity of individuals who need to benefit from social programs."

Social protection revolution

Since the nationwide rollout of the RNP system was completed in 2022, the official said they have enrolled more than 23 million people into the RNP. "Morocco's population is approximately 37 million, meaning we have covered about 62–63 percent of the total population. We have conducted roughly 17 million successful authentications and facilitated over 47 million successful data-sharing authentications with social programs and entities requiring KYC," the official explained.

Alongside the RNP, the government was also able to put in place a MOSIP-based Unified Social Register (RSU) as the second module, a system that collects social and economic data from citizens to help the government identify people who need certain social services.

"Anyone who wishes to benefit from social programs must be registered in the RSU. It is mandatory for program access, though not for the general population. Here, we work with households, whereas the RNP focuses on individuals," the official says.

Another Interior Ministry official who participated in the chat with Biometric Update clarified that to be included in the RSU, households' members must first register their biometrics and other identification data with the RNP.

The official further explained that each person has their own unique ID in the RNP. But with the RSU, the household head, after being authenticated via the RNP, can create and manage a household profile providing socioeconomic data. This process can be completed in person at a CSC center (Centre de Services aux Citoyens) in cases where the head of household is unable to complete the process online.

Once the request is validated, the RSU assigns a score that reflects the household's level of living. The social programs to which the household is registered then receive the score and determine the household eligibility (based on each program's threshold and, in some cases, on other criteria specific to the program).

"On the backend, we transmit this socio-economic data to partner institutions in Morocco such as the tax authority, water management, electricity management, and telecommunications providers," an official added. "These partners then share with us the household's actual consumption data for water, electricity, telephone, and similar utilities. Using this information, the RSU generates a verified socio-economic score for each household."

Enrollment in the RNP is not mandatory for all citizens, and enrollment in the RSU is mandatory only for those who wish to benefit from social programs.

RNP services can be accessed through a dedicated portal which offers 11 other online services that allow citizens to pre-register before visiting a CSC, track their enrollment status, manage their IDCS, view authentication history, and print their IDCS, among other functions.

One of the challenges Morocco had to deal with in the implementation of the MOSIP-based RNP and RSU systems was preparing enrollment centers. Officials said they had the task of setting up around 1,600 citizen service centres across the country within just a period of eight months.

The Interior Ministry official also spoke about the importance of training. He stated that they had to recruit and train over 5,000 staff to operate these centres through tasks like enrolling citizens, managing operations, and ensuring data quality. He said obtaining clean and accurate data also proved to be a challenge.

"When you train for the first time, you need to go back and follow them to retrain. This is something that we did in a very short period of time. So, we trained people first, and then the trainees later became trainers," he said.

More government systems on MOSIP?

Asked whether Morocco was considering integrating or migrating more government systems to MOSIP beyond the social benefits and social registry programs for households, the official said there was no such consideration for the time being because the RNP is meeting the country's needs for now.

However, he said the government is considering introducing facial recognition to the RNP for authentication. "MOSIP has developed secure authentication based on facial recognition, but this feature is available in the LTS (Long-Term Support) version of MOSIP. In Morocco, we are not yet on the LTS version. Migrating to it is a prerequisite before we can integrate secure facial authentication. This is among the key enhancements the government of Morocco is considering for implementation in the coming months," he told Biometric Update.

The MOSIP LTS version was originally released in 2022, but it has undergone several patch updates in the last few years. Codenamed the "Asymmetric Amoeba," this version was designed to provide stability for digital identity programs rolling out at scale.

"We authenticate beneficiaries using the RNP, but not yet via facial recognition. Currently, we use OTP (one-time password), which has worked effectively since launch. The next step, expected this year, is to pilot facial recognition authentication. We are actively evaluating this option," the official said.

While Morocco demonstrates how MOSIP can support targeted social protection systems alongside an existing national ID, Ethiopia represents a full-scale national identity build on the platform, with a strong emphasis on sovereignty and in-house capacity.

Ethiopia: Building a national ID system on open-source foundations

MOSIP's story in Africa cannot be told without the mention of Ethiopia. This is because the country was among those that embraced the platform early on. Since then, it has gone through various stages of success despite challenges that have stood in the way of the implementation process.

The story is straightforward. Ethiopia, a nation that has long balanced its proud historical heritage with the demands of modernity, wanted to modernize its identity system and infrastructure. It was about experimenting with how identity itself can be reimagined.

Then the idea of building the country's national identity system on an open-source platform that aligns with the government's digital transformation objectives came to mind.

A story from 2019

According to Yodahe Zemichael, Executive Director of Ethiopia's National Identity Program (NIDP), they were tasked in 2019 by the government with exploring how to build a national ID and a foundational ID project for Ethiopia.

"At that stage, there was no strict timeframe to roll out a population-scale ID system that involved tens of millions of people. Around the same time, MOSIP was still very new," Zemichael recalls in an interview with Biometric Update. MOSIP, recall, was launched in 2018.

"We happened to attend a webinar where the CTO, Architect and Chief Strategy Officer of MOSIP, presented its architecture. For us, it was a new concept but very intriguing. That's how we were first introduced to MOSIP, and after some time, we formalized the collaboration by signing an MoU," he adds.

Speaking further on why they chose MOSIP from among other options and considerations, the NIDP CEO mentioned the aspects of technology and data sovereignty, saying they were then, and still are, important principles for the Ethiopian government's digitalization efforts.

"We needed full control over the code to ensure our national ownership and security. Moreover, with open-source architecture and platform, it helped us see the high-level picture of what ID management involves, helped us think about what it takes to build an ID system, because before that, it was all shrouded in mystery, what it should look like and how we could build an ID platform for Ethiopia," he says.

"At the time, there was no MoU yet and no formal relationship. Our engineers simply went to the MOSIP GitHub, where all the modular repositories for the open-source national ID platform are available, deployed

the first sandbox, and even started refactoring it right away. That is one of the good qualities of a strong open-source platform: you can just use it. With some documentation and a solid knowledge base, you can own it and even contribute to it."

From when the MoU was eventually signed, a few other processes were completed before Ethiopia was able to fully run a MOSIP-based system.

From sandbox to full scale rollout

The process, Zemichael said, started with a sandbox. "We were not going to rely on something that we had not really tested, so we started off with laboratory testing in 2019/2020," he says.

He said while they were launching their lab tests, they demonstrated a few things, including how to customize the functionalities, localize the language, create their own deployment architecture, and prove that it was vendor-neutral with no hidden background costs or direct vendor dependencies and subscriptions.

"We were happy with the result. At the end of 2020, Fayda was re-established at the Prime Minister's Office as a project. We started slowly testing our sandbox, launching a lab-based pilot with 5,000 people registered from volunteers within civil service institutions. Then the first field pilot of 100,000 people was launched to see how we could scale organically by increasing the growth of the project," he explained.

"Currently we are on MOSIP 1.1.5 but are working on a plan to migrate to the latest stable LTS version. Our major KPIs [Key Performance Indicators] achieved to date include more than 32 million total registrations, more than 62 million eKYC requests served, and integration with 91 agencies nationally."

Beyond the success, the NIDP boss explained that they have also faced a number of challenges, from early service dependency creation, effective communication and sensitization, system integration, to the migration of millions of biometric records from legacy databases of ministries such as Revenue and Education.

"Ensuring that services are integrated early enough to drive adoption, while clearly communicating the value and use of both digital and physical credentials, remains critical," he mentions, stating that "as we move into the next phase, maintaining the right balance between interoperability and privacy, particularly in the context of data harmonization and data exchange, will be key to sustaining trust, ensuring compliance, and supporting long-term system adoption."

Zemichael added: "Operating the platform while performing system integration is a complex undertaking. Engaging a dedicated SI would have allowed us to focus exclusively on operations. However, we are currently managing both responsibilities in parallel. Currently, Fayda enrollment activities have been outsourced to telecom operators, banks, and private-sector enablers, allowing our internal teams to concentrate on platform management and deployment."

The main enrollment telecom partner is Ethio Telecom, the country's biggest telecoms services provider.

Steady progress, major targets

With over 32 million people enrolled and counting, Zemichael says they are pursuing nationwide registration and have a plan to reach 63 million enrollments by July this year. Efforts, he said, are also being made to continue integration of Fayda beyond the financial sector, which for now is being implemented in phases to strengthen KYC compliance, improve financial inclusion, and reduce fraud. The country also has a plan to reach 90 million digital IDs issued by 2030.

"We expect to create dependencies across a wider range of government and public services. At the same time, Fayda will be deeply integrated into e-government platforms, enabling secure login, eKYC, authentication, and seamless service delivery.

"The rollout of digital credential solutions such as the FaydaPass Wallet will further support online and offline identity verification and credential storage. All of this will be underpinned by the continued strengthening of legal and policy frameworks, ensuring data protection, privacy, interoperability, and trust as the system scales nationwide," he notes.

According to Zemichael, their MOSIP-based ID system squarely fits into the government's broader digital transformation strategy because it is helping them build what he termed the "Ethiopia Stack," describing it as "a sovereign digital infrastructure where payment systems and the Fayda digital ID operate seamlessly together."

"In the Digital Ethiopia 2030 strategy, Fayda is explicitly identified as the foundational Digital Public Infrastructure (DPI) necessary to achieve our four national pillars: empowering people, inclusive prosperity, universal access, and digital investment," he stated.

He reiterated the aspect of digital sovereignty, saying it is about ownership and control. "By using open-source code, we ensure that the data of more than 100 million Ethiopians remains within Ethiopian data centers and is governed strictly by Ethiopian law without vendor lock-in. This aligns with our Minister of Innovation and Technology's vision that Ethiopia must shift from being a consumer of technology to a master of its own digital destiny, which is critical for national security and economic independence."

Pioneer host of MOSIP Connect

Ethiopia was not only an early adopter of MOSIP; it also had the privilege of hosting the first edition of MOSIP Connect in March 2024, an event conceived with the aim of fostering collaboration and advancing the secure and inclusive digital ID agenda around the world.

For Zemichael, hosting the MOSIP Connect event was a watershed moment for the country and for the Fayda digital ID project. The venue of the event was the prestigious Ethiopian Skylight Hotel in Addis Ababa.

“It shifted the global perception of Ethiopia from a participant to a leader in the digital identity space. The event brought over 400 delegates and more than 50 technology partners to our doorstep. This signaled to biometric device manufacturers, system integrators, and development partners in the private sector that Ethiopia is a mature, open market, encouraging international technology providers to set up local operations and support our ecosystem directly,” he recounted.

“It also gave our local engineering team direct access to the global architects of MOSIP. Instead of just reading documentation, we were problem-solving in real time with the creators of the code. It also positioned Ethiopia as a reference point for other African nations. We were able to showcase our progress to peers from countries, fostering a spirit of South–South collaboration where we share our ‘homegrown’ adaptations on Fayda,” the official added.

MOSIP adoption recommendation

For other nations implementing digital ID systems or in the process of setting up one, Zemichael says he would gladly recommend MOSIP, but with what he calls “a strong advisory regarding capacity.”

“I recommend MOSIP to nations that value autonomy and sustainability over quick, ‘black-box’ fixes. However, open-source is ‘free to license,’ not ‘free to run.’ My advice to other leaders is that you must be willing to invest in human capital. You cannot just download MOSIP and expect it to run itself. You need a dedicated technical team to manage the deployment, security, and updates,” he said.

“If a country is willing to build internal capacity and sustainability, it offers unparalleled freedom. It allows you the flexibility to customize the system to your local context (like we did with the Amharic calendar and language) in ways that proprietary vendors often do not. We are already seeing this recommendation in action. Countries like Liberia and Zambia have signed MoUs with us to learn from our experience,” he noted.

Unlike Ethiopia’s greenfield approach, Uganda has taken a brownfield path, using MOSIP to modernize an existing national identity system while addressing legacy infrastructure constraints.

Uganda: Modernizing legacy ID systems with MOSIP

There are generally two main approaches to implementing MOSIP-based national identity programs. These are the greenfield and the brownfield systems. For Uganda, the decision from the onset was to pursue the brownfield implementation, which meant that it was only going to use MOSIP as an open-source platform to develop and modernize its existing national ID system without building anything much from scratch.

As part of the modernization drive, Uganda says it is already implementing five MOSIP modules which run different aspects of its national identity system. These include new enrollment for ID, renewals for those who have existing cards, updating and correction of information on issued ID cards, as well as issuance and lost ID replacement services.

This year, the National Identification and Registration Authority (NIRA) announced that it had migrated an estimated 28 million ID records to the MOSIP-run system, which includes data of new registrants and for renewals.

The genesis of the story

Thanks to a partnership which NIRA has with IIIT-B, MOSIP's founding institution, the country is using the open-source technology to set up a national digital ID system which it considers as the foundation for the country's digital transformation ambitions. The MOU between both parties was signed in May 2023, but initial stakeholder consultations had begun in 2022.

But how did the MOSIP-Uganda story actually start? NIRA Director General, Rosemary Kisembo, told Biometric Update in an interview that their interest in MOSIP was born when the contract of the proprietary system their national ID system ran on came to expiration. She said they needed scale and greater impact.

"Our decision to adopt MOSIP was driven by two factors, but there could be more. We had a proprietary system that was very good. I don't want to say it was a bad system; it was a very good system. However, when our contract with the vendor ran out, it became very difficult to make any changes and to scale it," Kisembo explained.

"We had some challenges. You know, a proprietary system presumes that you will always be in touch with the owner. So, when you need to do something or when you need to change something, it's a black box. They will open the black box, make the change, and give you back the black box," she added.

The NIRA executive narrated that after the MOSIP system was eventually introduced, there were several changes, including in the areas of governance, legislation, and policy, which became necessary. There was the need, she said, to make certain alignments given the nature of their environment and the kind of identity space they operate.

"The changes are going to be several. I'll give you the simplest example. Before we rolled out that new system, the birth and death registration function was in another entity. But after it was rolled out, the birth and death function was brought to NIRA," Kisembo disclosed, adding that there were many other significant changes that were going to happen so as to transform the landscape of the application as it was first thought about.

Immense customization

Kisembo said from the onset, it was thought that the MOSIP system was going to be only for citizen registration, as the idea was that only adults would register with each of them issued unique identification numbers, especially as the country was planning a mass registration and renewal exercise.

But it turned out that they also needed to enrol adults and children, and also knock off the register all names of deceased persons.

She stated that although they had some level of sovereignty with the proprietary system because the data belonged to Uganda, they needed a system through which they could more easily develop the capacity within the country to make it possible to build, operate, and maintain software and to own the intellectual property faster.

"And when we own it, we can change it when we want to change it, without any panic," the NIRA boss said, underscoring the flexibility of the MOSIP system.

Kisembo admitted that with MOSIP, they have been able to do "immense customization" with their national ID system. One aspect of customization, Kisembo noted, is their ID schema. "MOSIP out of the box has 10 fields. Our ID schema has up to 150 fields," she said.

"The second substantial one is that there were rules that MOSIP gives an ID to everybody in the geographical region. But for us, we give a specific ID to citizens based on certain rules in the constitution. Then we give a different ID to aliens based on certain rules in a certain zone," she also mentioned.

She added that in Uganda, the system has been designed in such a way that ID numbers are issued to people based on the relationship they have to the country, whether they are citizens or legal residents.

"That is what was fundamentally different. It's a big change. We added that module to determine. It's quite automated. Then we added manual verification. The logic was, if you failed the business rules in that module, someone would have to now physically look through your documentation and see how to advise you to submit a better application for the manual verification," she asserted.

ID data migration challenges

Asked how the process of migrating the ID data from the legacy system to the MOSIP-based platform was, Kisembo stated that it was never easy. But the urgency of the shift was intense because the old platform, which had been in place for 10 years, had become wanting.

“The infrastructure that was hosting the legacy environment was ailing. It was touch and go. One wrong move and we would lose all the data. So, we had to create a staging area,” she revealed.

She also mentioned that not even efforts to find spare parts to get the old system properly working again were successful, as the infrastructure had become totally “ailing.”

She went on that because of the old nature of the infrastructure and the rapidly changing technological landscape, it was challenging using modern ways of transferring the data to the staging area. As such, they needed about three months to move the data to the staging area, even before the migration started.

She added that a lot of technical complexities were involved in the process, and so its ultimate success is a technical success, but not necessarily a project one.

With the new MOSIP-based ID system in place, Kisembo said one of the expectations from Ugandans is to see a significant change in service delivery, including a decrease in turnaround time.

“From the citizen’s perspective, the question is that they want to see a reduction in turnaround time. The biggest complaint they’ve had as citizens is that it takes a long time for them to get their ID,” she noted.

“That is a question that we have not yet completed answering. So, the migration was a means to that end because we needed to move all the data to reduce the time of moving between two systems and ensure that we do not issue more than one identity to one person. But that is a technical problem. The user’s problem is how you reduce my 60, 30 days to five days, or three days, for me to get my identity document,” she said.

Migration done, but what next?

After what Kisembo described as “a very successful technical feat,” she stated that their work will continue. For one thing, she said NIRA will lay emphasis on efforts aimed at reducing the time needed to obtain an ID, and to improve customer experience. “That’s the journey that continues,” she stated.

Sierra Leone’s experience reflects a similar brownfield transition, but with a stronger focus on overcoming vendor lock-in and testing MOSIP through phased pilots before national rollout.

Sierra Leone: From vendor lock-in to open identity infrastructure

Sierra Leone is another example of a successful brownfield MOSIP implementation in Africa. Formal operations began between the two parties when they agreed to a Memorandum of Understanding (MoU) in January 2023. The agreement meant that the open-source platform would serve as the basis for modernizing the West African country's existing foundational identity infrastructure.

It is worth recalling that Sierra Leonean authorities first came across the idea of MOSIP at international digital ID events like the ID4Africa Annual General Meeting, which a team from MOSIP attends regularly. It was through exchanges during these forums that the country developed an interest in adopting a platform it could customize to its own specific needs, in a move that also aligns with its digital sovereignty desires.

Before adopting MOSIP and implementing a pilot, Sierra Leone had launched an initiative in 2016 to modernize its national identity system and make it a tool to facilitate access to a range of services from the government and the private sector. But they were soon faced with the challenges of vendor lock-in with the system provided by a commercial partner.

The Deputy Director in charge of ICT and Identity Management at Sierra Leone's National Civil Registration Authority (NCRA), Moses T.F. Vibbie, told Biometric Update in an interview that the issues they encountered included the need to pay for licenses every year, which was a major burden on the government.

"We learned about MOSIP as an open-source alternative. With MOSIP, there's no vendor lock-in and no license fees. Once implemented, it gives us full ownership as a country," Vibbie stated.

The pilot, lessons, challenges

Sierra Leone then began by conducting a pilot with the MOSIP system to test the functionality and interoperability of the platform, and how it could support their long-term goals of building a scalable and inclusive digital ID system.

"We decided to test MOSIP through a pilot to see if it could replace our existing system. The idea was to understand its features, functionalities, and modules, and then decide whether to move forward with MOSIP or continue with our current vendor-based system," the Deputy Director General disclosed.

He added: "We were able to test the platform internally with our local team, with support from MOSIP. It's not like we just adopted it; we piloted it first. For us, the pilot was very successful. Another driving force

was data sovereignty and ownership. Once implemented, the platform sits with us as a country. We take total control of our identity management infrastructure."

As Vibbie explained, they tested all modules of MOSIP that were available at the time, and given that the country was not building a new digital ID system from scratch, it was important to ensure that any new system could align with the NCRA's existing operations.

"We piloted everything, from enrollment to production of ID cards, including e-Signet. Inji wasn't available at that time, so we didn't pilot it. We had to be sure MOSIP could deliver the same results we were already getting. We are very interested in Inji now because of the credential it provides, so we plan to implement it in the future," Vibbie explained.

Implementing the pilot was a very challenging process, Vibbie said. However, the NCRA put in place a strategy aimed at providing the possibility of testing and working with a wide range of vendors for specific services.

"During the pilot, we worked with multiple biometric device manufacturers who were MOSIP partners. We tested several certified devices to avoid being limited to one vendor. The MOSIP team provided the platform and support, including capacity building. The device vendors helped ensure smooth integration, and our local NCRA team managed the pilot on the ground," the official mentioned.

"The pilot had two phases: 50 percent new enrollment and 50 percent migration from our existing system. Since we already had 93 percent coverage, we needed to test both. We wanted to see if MOSIP could work with our existing data and also handle new registrations. It worked well for both," he added.

The pilot, according to Vibbie, touched people across age groups: "We tested across different age groups and locations, including children from age five and above, something we hadn't been able to do before. With MOSIP and its partners, we lowered the fingerprint capture age from 12 to five."

Given the nature of its workflow, Vibbie said the NCRA customized MOSIP modules to match it, and this included things like form fields, data alignment, and even screen colors to match our national branding.

"We wanted the transition to be smooth for our staff and avoid retraining challenges. Most of the workflows aligned well, so we only had to tweak a few things," he said.

Vibbie says that with the pilot completed, the NCRA has been working to ensure national rollout and a full switch to the MOSIP-based system.

"We haven't fully switched yet. We completed the pilot and are now working on the national rollout. Because we have an existing system, we can't just switch overnight. We're taking time to ensure a smooth migration. But the government is committed to fully switching to MOSIP," he affirmed.

Advice for potential MOSIP adopters

Offering advice to countries that intend to adopt MOSIP, Vibbie emphasized the need for a good pilot, citing a rapid pilot option which he says is now available.

“Customization is key to aligning the platform with local workflows and processes. For countries with existing systems, vendor lock-in and license costs are real challenges. MOSIP eliminates those.”

“I really like that with MOSIP, you’re not locked into one vendor. You have options—multiple device manufacturers and system integrators. If one device fails, you can switch to another. That’s critical in the biometrics space,” Vibbie added.

He also underscored the importance of capacity building: “MOSIP encouraged us to set up a team across technical and operational levels. Our Director General was very supportive, so we built a strong internal team to manage the pilot and beyond.”

Speaking about questions some countries have about whether MOSIP is truly free, Vibbie stated: “Some countries have reached out to us with concerns about whether MOSIP is truly open source and free. They worry that costs might appear later. It’s important for MOSIP to communicate clearly that the platform itself is free, with no license fees. Implementation costs, like system integrators and biometric devices, are separate. That message needs to be clear when engaging with countries.”

It’s important to mention that even before the engagement with MOSIP for the national ID system, both parties had established high-level collaboration in the area of digital payments when MOSIP signed a deal in 2022 with OpenG2P, a digital public goods organization co-founded by the government of Sierra Leone.

With Sierra Leone’s national ID system now in place, the government has a plan to ensure universal coverage before 2030, to align with SDG target 16.9. For the government, the national ID is a major asset for the country and stands as one of the main pillars supporting the country’s digital transformation.

Today, Sierra Leoneans are able to access services across several domains in an inclusive and secure manner, thanks to a MOSIP-based national ID system that is helping the country retain its digital sovereignty, reduce long-term costs, and align with international best practices in the area of digital ID.

Sri Lanka, meanwhile, represents a newer wave of adopters, using MOSIP as part of a broader digital transformation strategy, supported by international partnerships and a strong emphasis on governance and trust from the outset.

Sri Lanka: Early-stage MOSIP rollout focused on governance and trust

Sri Lanka is in the early stages of developing its national digital ID based on MOSIP, with assistance from neighboring India.

The governments of Sri Lanka and India signed an agreement under which India will support its neighbor's digital ID implementation both financially through grants and with domestic expertise. India has already supplied hundreds of millions of Sri Lankan rupees to support the early stages of the project. A condition of the grants is the selection of an Indian firm as systems integrator.

The Sri Lankan (SL-UDI) will therefore be implemented by a "master" systems integrator chosen from among Indian firms, with a domestic managed service provider taking over the system's operation after the launch.

The advantage Sri Lanka gets from its collaboration with India on the Sri Lanka Unique Digital Identity (SL-UDI) Project is the experience that India has gained from digital ID implementations both domestically and in other countries.

These comments were made by Eng. Eranga Weeraratne, Sri Lanka's Deputy Minister of Digital Economy, in an interview with Biometric Update. India's experience in implementing massive-scale digital public infrastructure in India and other countries allows Sri Lanka to accelerate its own digital transformation, reduce corruption, and improve government service delivery while adopting reliable technologies.

"The experience of delivery in such large-scale solutions is what we are hoping to get from an Indian collaborator," Weeraratne added.

Leadership, governance and trust

The Department of Registration of Persons (DRP) is the owner and legal custodian of Sri Lanka's digital identity system, currently in development, as the mandated national authority responsible for citizen registration and identity records. GovTech Sri Lanka will provide the technical delivery and operational support -- including platform implementation, integrations, and service enablement – working closely with the Department to ensure continuity and quality of operations.

The overall program will be carried out under the supervision of the Ministry of Digital Economy, which will provide policy direction, whole-of-government coordination, standards, and oversight to ensure the system is implemented securely, responsibly, and in a manner

that protects citizens' rights while enabling digital services at scale, Deputy Minister Weeraratne said.

"Sri Lanka's biggest opportunity is to make government services as simple and reliable as modern digital services, while reducing fraud, duplication, and administrative costs," Weeraratne told Biometric Update. "Today, citizens repeatedly prove who they are across agencies using inconsistent methods, e.g. by producing certified ID/Birth certificate copies, etc., which slows services, weakens targeting of benefits, and creates room for leakages. A modern foundational digital identity is a core public digital infrastructure that can fix this once, and then allow every agency to build faster, safer services on top. This will let citizens access many public services online -- remotely, anywhere, anytime, reducing queues, travel, and paperwork while improving speed and transparency."

Currently, people in Sri Lanka must use a mix of the NIC, driving licence numbers, passport numbers, and application-specific IDs to confirm their identity for service delivery.

Sri Lanka selected MOSIP to ensure the nation can own, adapt, and govern its identity system over decades, meeting national-scale security and operational requirements without vendor lock-in, says Weeraratne. He also noted that MOSIP is a mature platform that has been developed and strengthened through multiple country deployments.

"From a risk perspective, MOSIP publishes detailed security practices and testing guidance, and we will still apply Sri Lanka-specific controls (independent security reviews, strong key management, strict access controls, audit logging, and phased rollouts with measurable security gates), because the security of any national ID depends not only on the core platform but also on how it is deployed and governed locally."

Sri Lanka is using a whole-of-government governance approach: a central program management structure, a multi-agency steering mechanism, and defined technical and legal working groups. This ensures that civil registration, immigration, public administration, social protection, finance, ICT, and security stakeholders align early on standards, operating procedures, and integration priorities – rather than discovering conflicts during implementation.

Scope, phasing and realism

Capabilities are being prioritized in the first phase of issuing digital ID. "We will execute a limited-time initial phase focused primarily on issuing Digital IDs, establishing the core enrollment, de-duplication, and secure credential issuance capabilities. Immediately after that, we will begin the re-registration of all existing National ID holders into the Digital ID system, so that Sri Lanka transitions to a single, modern identity foundation. We intend to complete the full re-registration within two years,

using a carefully planned, phased approach that prioritizes quality, inclusion, and security," The deputy minister said.

He noted that the ministry is deliberately avoiding a "big-bang" switch where citizens are forced to move overnight. "Instead, we intend to run both Digital ID and physical ID acceptance in parallel for a clearly pre-defined transition period. This protects service continuity and ensures no citizen is disadvantaged while the ecosystem adapts."

During this transition window, the focus will be on enabling all ID validation points across government and other authorized service environments to adopt Digital ID-based verification as the primary method, including operational readiness, staff training, device readiness, and secure connectivity. The goal is not only technical adoption, but also a societal shift in mindset, moving away from the need to always carry a physical card, toward a secure and convenient digital identity that can be used when needed, from anywhere, at any time.

"At the same time, we will not permit uncontrolled or premature integrations; each integration will be introduced in a governed manner with security, privacy, and performance checks before it is allowed to operate at scale," Weeraratne added.

Inclusion, security and sovereignty

Sri Lanka's government is planning assisted enrollment channels through government touchpoints and mobile units, along with structured exception workflows for citizens with limited documentation.

On data sovereignty and cyber resilience shaping early design decisions, he said that Sri Lanka's digital identity must be sovereign, resilient, and secure. Early design decisions include identity data to be collected and processed only by the officers at the Department of Registration of Persons, data hosting will be in Sri Lanka and in a data centered fully managed and controlled by GovTech Sri Lanka, involve the Data Protection Authority and SLCERT from the inception for the cybersecurity and data protection measures, strong encryption key management and restricted administrative access, segmented architecture and robust logging/auditing and disaster recovery and continuity planning as core requirements.

The most important decision that will influence the long-term success of this national identity program, Weeraratne says, is to define the trust boundaries from day one. That means providing clarity about what data is collected, who can access it, for what purposes, under what oversight, and how citizens can challenge misuse. If the trust architecture is weak, according to Weeraratne, even the best technology will fail; if it is strong, adoption will follow.

Taken together, these case studies show that while MOSIP provides a common technical foundation, outcomes depend heavily on governance choices, local capacity and the ability to translate identity infrastructure into widely used services.

Key takeaways from MOSIP implementations

- **MOSIP is being used in different ways.** Morocco applies it to social protection and registry systems, while Ethiopia uses it as the foundation for a national digital ID, and Uganda and Sierra Leone are using it to modernize legacy ID infrastructure.

- **Open-source does not mean low-effort.** Countries emphasize that MOSIP reduces vendor lock-in and licensing costs, but successful implementation still requires technical capacity, systems integration, training and long-term operational ownership.

- **Governance matters as much as technology.** The strongest implementations pair the platform with clear institutional roles, legal frameworks, privacy controls and mechanisms for oversight and redress.

- **Adoption depends on real services.** MOSIP systems gain value when linked to social protection, KYC, payments, public services and other high-demand use cases.

- **Brownfield transitions are complex.** Countries migrating from legacy systems must manage data quality, infrastructure fragility, customization and service continuity while avoiding disruption.

- **Trust boundaries are decisive.** Successful programs define early what data is collected, who can access it, for what purpose, and how misuse can be challenged.

Vendor profiles

Biometric Update strives to provide accurate information, but we must point out that our list of vendors is not comprehensive. We have selected a representative group of vendors, but the list is not exhaustive. The analysis is presented on a “best efforts” basis, and we cannot accept any liability for any errors or omissions.

If a vendor considers that we have unreasonably omitted them then there is an opportunity for them to engage with Biometric Update for inclusion in subsequent editions of this report.

The MOSIP Marketplace

marketplace.mosip.io
info@mosip.io

The MOSIP Marketplace is an online platform that enables countries to discover and engage with the technology solutions they need to build and scale their national digital ID systems. Designed as a bridge between adopting governments and ecosystem partners, the platform supports countries in making informed choices on the technologies and service providers best suited to their Digital Public Infrastructure (DPI) needs.

Building a national digital ID system often requires governments to navigate a complex landscape of vendors, integration requirements, and implementation considerations. The MOSIP Marketplace was created to simplify this process through a curated digital catalogue of solutions, bringing together commercial and non-commercial technologies — including biometric device manufacturers, software providers, and system integrators — from across the world within one accessible space.

MOSIP Marketplace provides visibility into solutions at different stages of compliance and integration with MOSIP, enabling countries to assess technologies based on deployment readiness, interoperability, and long-term digital transformation goals. To support more informed evaluation, partners on the platform are organised into categories such as:

- MOSIP Compliant: Products that have completed self-compliance exercises against MOSIP specifications.
- MOSIP Integrated: Solutions that have demonstrated interoperability with MOSIP systems.
- MOSIP SI Partners: System integrators that have undergone MOSIP-led training and capacity-building programmes.

Together, these categories help governments better understand the maturity and compatibility of available solutions while exploring the ecosystem in a transparent and unbiased manner.

By creating greater visibility into trusted technologies and providers, the MOSIP Marketplace supports countries in reducing the risks of vendor lock-in while encouraging interoperability and adherence to open standards. As part of MOSIP's broader ecosystem-driven approach, the platform also works with partners to establish compliance pathways against MOSIP specifications and advance certification programmes for biometric devices in collaboration with accredited external labs. System integrators listed on the platform are further supported through initiatives such as the MOSIP Academy, helping strengthen implementation and maintenance capabilities across different geographies.

Today, the MOSIP Marketplace continues to grow as a global ecosystem platform, featuring over 125 partners and solutions from regions including Africa, Asia Pacific, Latin America, and the Caribbean. As adoption of MOSIP-based systems expands worldwide, the platform is helping countries accelerate the development of scalable, interoperable, and country-led digital ID systems.

Integrated Biometrics

integratedbiometrics.com
info@integratedbiometrics.com
121 Broadcast Drive, Spartanburg, SC 29303
+1 864 990 3711

Integrated Biometrics (IB) delivers cutting-edge fingerprint scanners, seamless biometric system integration software, contactless fingerprint capture and comprehensive identity management beginning with infant identification solutions. The company serves customers in national ID, border security, law enforcement, infant identification, and enterprise identity systems worldwide. It is known for rugged mobility-focused hardware devices that offer exceptional image quality and reliable performance in harsh, real world conditions like dust, humidity, rain, direct sunlight and extreme temperatures, to accommodate mobile field conditions and high volume enrollment scenarios that need speed and consistency.

IB has been part of the MOSIP ecosystem from its early stages, contributing MOSIP-compliant biometric hardware used in early-stage R&D, pilots and production deployments. Its fingerprint registration and authentication devices and software are successfully used by MOSIP system integrators and solution partners to capture high quality biometric data during enrollment and authentication. The company also supplies its technology to numerous registration and authentication devices listed in the MOSIP Marketplace by its customers. IB scales through partner-led solutions, offering seamless integration into tools supporting MOSIP-based national ID, civil identity, and border management programs.

Currently, there are three MOSIP-compliant fingerprint devices listed on the MOSIP Marketplace for registration use cases – Kojak, Five-0 and Watson. Going forward, IB aims to expand device availability within the MOSIP Marketplace, and the company is also currently engaged in the MACP certification process. The modular nature of IB hardware and SDKs allows easy adaptation to evolving MOSIP requirements, policy changes, and future technical standards without redesigning entire systems.

Deployment relies on a streamlined set of components, including IB fingerprint devices, IB SDKs, approved partner applications, and MOSIP registration software. For partners, IB offers direct technical support throughout integration and deployment, documentation, integration guidance, and collaboration during testing, pilots and production rollouts. Hardware integration aligns with partner solution schedules; device integration is typically straightforward once MOSIP compliance requirements are met.

SecuGen

secugen.com
sales@secugen.com
2445 Augustine Drive Suite 150, Santa Clara, CA 95054, United States

SecuGen

SecuGen Corporation specializes in advanced optical fingerprint recognition technology, developing FBI-certified sensors, software and biometric devices that can be integrated into national ID systems. Its primary markets include information security, physical access control, national ID, telecommunications, financial services and medical records management, serving global OEMs, integrators and security-focused industries. Currently, it is beginning implementation with the Uganda National Identification and Registration Authority (NIRA), to provide trusted authentication devices for its MOSIP-based deployment.

SecuGen's L1 fingerprint authentication device, the Unity 20 MOSIP, is fully MOSIP certified, designed to fit into a MOSIP-based national ID system as a secure biometric capture point within an existing authentication flow. The device integrates with MOSIP's authentication client to verify an individual's identity for services, eKYC, field operations, border control and operator logins, onboarded and validated through SecuGen's MOSIP Management Server and Management Client.

The Unity 20 MOSIP combines environmental durability, high-quality imaging and robust throughput for strong performance in harsh physical and operational environments, making it suitable for government, industrial and outdoor use. It has an IP54 ingress rating and features a scratch-resistant optical sensor enhanced by Smart Capture and SEIR technologies, enabling it to maintain excellent image quality in low light, bright sunlight, dust, moisture, and extreme temperatures.

The Unity 20 MOSIP authentication device scales naturally: because it produces ISO 19794-4:2011 standard biometric image data, it can interoperate seamlessly with other MOSIP certified devices and backend systems. Since it relies on open standards rather than proprietary formats, the device can be deployed in mixed vendor environments, upgraded without disrupting national infrastructure, and remain compatible as MOSIP specifications evolve. This makes the hardware inherently future proof and capable of supporting population growth, new use cases, and evolving MOSIP compliance requirements. Likewise, the MOSIP Management Server also scales efficiently because it performs only lightweight MOSIP mandated control plane functions.

SecuGen supports integration partners through the full implementation process including integration with MOSIP authentication flows, testing, troubleshooting and rollout. Configuration updates, ongoing maintenance, and decommissioning of devices are also supported, to ensure that devices are consistently integrated, securely managed, and reliably maintained from deployment through end of life.

Select vendors

D

Dermalog

dermalog.com

Dermalog is a German biometrics company specializing in large-scale automated fingerprint identification systems (AFIS/ABIS), biometric enrollment platforms and border management technologies. The company has supplied biometric identity solutions for national ID, voter registration, border security and law enforcement programs in multiple regions, including Africa, Asia and Latin America.

Within the MOSIP ecosystem, Dermalog provides biometric matching and enrollment technologies that can support foundational digital identity systems and related authentication workflows. Its focus on multimodal biometrics, interoperability and large-scale identity management aligns with MOSIP's modular architecture and vendor-neutral approach, enabling governments to integrate biometric services while maintaining flexibility in system design and future procurement decisions.

H

HID Global

higlobal.com

HID Global provides identity and access management technologies spanning secure credential issuance, biometric enrollment, authentication and digital identity infrastructure. The company supports governments, enterprises and public-sector agencies with solutions ranging from physical ID cards and PKI technologies to mobile identity and citizen credential systems.

In the context of MOSIP implementations, HID Global contributes technologies that support secure identity issuance, credential management and authentication. Its experience in government identity ecosystems and interoperability standards positions the company as a potential integration partner for countries deploying MOSIP-based national ID and digital public infrastructure systems.

I

Identy.io

identy.io

Identy.io develops AI-driven biometric identity verification technologies focused on facial recognition, liveness detection and digital onboarding. The company's software supports remote identity verification use cases across sectors including fintech, digital government and telecommunications.

Within the MOSIP ecosystem, Identy.io's biometric verification and presentation attack detection capabilities can support secure enrollment and authentication workflows. Its mobile-first approach and emphasis on remote onboarding align with MOSIP's expanding focus on digital service delivery, eKYC and interoperable authentication systems.

Image Match Design

imagematch.com.tw

Image Match Design develops biometric software technologies focused on fingerprint recognition, identity verification and related security applications. The company provides biometric SDKs and matching technologies designed for integration

into government and enterprise identity systems.

In the MOSIP ecosystem, Image Match Design contributes biometric software components that can support enrollment, matching and authentication functions within modular identity deployments. Its emphasis on interoperable biometric technologies aligns with MOSIP's standards-based approach and multi-vendor ecosystem strategy.

Integrated Biometrics

integratedbiometrics.com

Integrated Biometrics develops FBI-certified fingerprint scanners and biometric software designed for national ID, border management and law enforcement applications. The company is known for rugged, lightweight biometric devices optimized for mobile enrollment and operation in demanding field conditions.

Integrated Biometrics has participated in the MOSIP ecosystem from its early stages, with MOSIP-compliant fingerprint devices supporting pilots, enrollment initiatives and production deployments. Its hardware and SDKs are integrated into solutions used by MOSIP partners and systems integrators for biometric registration and authentication workflows.

Iris ID

irisid.com

Iris ID specializes in iris recognition technologies used in identity management, access control and time-and-attendance systems. The company's biometric platforms are deployed across government, enterprise and critical infrastructure environments worldwide.

Within MOSIP-based implementations, Iris ID technologies can support multimodal biometric enrollment and authentication strategies, particularly where iris recognition is used to strengthen identity assurance and inclusion. Its standards-based biometric solutions fit within MOSIP's modular and interoperable identity architecture.

L

Laxton

laxton.com

Laxton provides biometric enrollment hardware, identity registration kits and digital identity solutions for governments and international development programs. The company's technologies are widely used in national ID, voter registration, civil registration and social protection projects.

Laxton participates in the MOSIP ecosystem through biometric enrollment devices and integrated registration solutions designed for large-scale identity deployments. Its portable enrollment kits and field-ready infrastructure support MOSIP implementations in environments where mobility, scalability and rapid deployment are important operational requirements.

R

ROC

roc.ai

ROC.ai develops computer vision and biometric recognition technologies focused on facial recognition, object recognition and AI-driven identity applications. The company provides software platforms designed for secure identity verification and analytics across public- and private-sector environments.

In the context of MOSIP, ROC's facial recognition and biometric matching technologies can support authentication, digital onboarding and identity verification workflows. Its AI-focused approach aligns with the broader evolution of MOSIP implementations toward multimodal biometrics and expanded digital service delivery use cases.

S

SecuGen

secugen.com

SecuGen develops optical fingerprint recognition technologies and biometric authentication devices for applications including national ID, financial services, healthcare and physical access control. The company supplies FBI-certified sensors, SDKs and authentication hardware used in identity verification environments worldwide.

SecuGen's MOSIP-certified Unity 20 MOSIP authentication device is designed for integration into MOSIP-based identity systems, supporting biometric authentication and eKYC workflows. The company's emphasis on standards-based interoperability and durable field-ready hardware aligns with MOSIP's modular architecture and long-term digital identity deployment objectives.

T

Thales

thalesgroup.com

Thales Group provides digital identity, biometrics and cybersecurity technologies for governments, border agencies and critical infrastructure operators worldwide. Its portfolio includes biometric enrollment, civil identity systems, passport issuance, authentication and digital security platforms.

Within the MOSIP ecosystem, Thales contributes technologies and expertise relevant to secure identity issuance, biometric verification and large-scale digital identity infrastructure. The company's experience supporting national identity and border management systems globally aligns with MOSIP's focus on scalable, interoperable and standards-based digital public infrastructure.

X

Xperix

xperix.com

Xperix develops biometric devices and identity solutions focused on fingerprint and multimodal biometric capture for government and enterprise applications. The company supplies enrollment and authentication hardware used in border management, civil ID and law enforcement environments.

In MOSIP implementations, Xperix technologies support biometric enrollment and identity verification workflows through interoperable capture devices and authentication systems. Its focus on standards compliance and scalable biometric infrastructure aligns with MOSIP's multi-vendor ecosystem and modular deployment model.

BIOMETRIC
UPDATE.COM