Global Virtual Summit on Digital Identity for Refugees - Entry by MOSIP

“Design solutions for interoperable, standards based digital ID systems that include refugees?”

Introduction

Providing a secure, unique legal identity that also safeguards the rights, especially rights related to data protection and privacy of the individual, is a complex task for any government. The difficulties multiply exponentially when it comes to establishing identities of ensuring that refugees, asylum seekers, stateless persons, and other forcibly displaced persons and providing access to services across borders and organisations, most often with under extremely challenging conditions.

Under these circumstances, overcoming operational challenges often becomes the focus of conversations around identity and data sharing, at the cost of ensuring privacy and data protection. Any twenty-first century system, however, has to address both, not only in the design of the technical system, but also in the rules and processes for every partner, and public or private agency involved in handling identity-related data.

Identity verification is a central aspect of this challenge, and multipurpose, foundational ID, delinked from status under different programs, can be a way towards coordination and the development of an ecosystem of users, partners, governments and organisations that share data in a secure way while prioritising the rights of identity holders.

What is MOSIP?

The Modular Open Source Identity Platform (MOSIP) was conceived as a response to challenges of this nature. MOSIP is a technology platform which helps ID issuers, including governments and intergovernmental organisations, implement a digital, multipurpose identity system in a cost-effective way. Issuers can use MOSIP freely to build their own identity systems. MOSIP is built from the ground up as an open source solution, with open standards - adoption of the platform, as a whole, or in parts, brings flexibility and interoperability into the system.

The learnings from the implementation of identity systems around the world have been incorporated in MOSIP in order to design it with user privacy and security as central tenets from the outset. MOSIP takes care of user privacy with a consent framework that lets the user choose what to share and when. It is transparent and lets the user know what they have shared and when, and also allows the user to lock authentication features that they wish to restrict.

Anchored at the International Institute of Information Technology, Bangalore (IIIT-B) as a global public good, and funded by the Bill & Melinda Gates Foundation, Omidyar Network and Tata Trusts, MOSIP presents a different way of approaching the architecture, design and integration of large-scale systems, one that recognises foundational ID as being the basis for a range of applications and services across different systems. MOSIP-based solutions are vendor neutral and interoperable. It does one thing and does it well — empower every individual with a unique identity, which they can use to authenticate themselves at any time, and anywhere.

MOSIP consists of the following modules -

Pre-Registration

For initiating a new registration into the identity system, along with the capture of existing user data.

Registration Services

For capturing demographic and biometric details (if required) of an individual along with supporting information (proof documents & information about parent/guardian/introducer), and for packaging the information in a secure way.

Registration Processor

Registration Processor processes the data (demographic and biometric) of an individual for quality and uniqueness and then issues a Unique Identification Number (UIN). The sources of data are primarily from:

- MOSIP Registration Client
- Existing databases

ID Authentication

ID Authentication provides an API based authentication mechanism for entities to validate Individuals. ID Authentication is the primary mode for entities to validate an Individual before providing any service.

Kernel

The MOSIP kernel is a platform to build higher-level services as well as a secure sandbox. Functionally it performs or enables services such as Unique Identification Number (UIN) Generation, authorisation of various agencies with access to the system, services for the identity-holder and the administrator, etc.

What are MOSIP's technological principles?

To enable a truly open source, interoperable platform, MOSIP is based on the following architectural principles:

- MOSIP does not use proprietary or commercially licensed frameworks. Where deemed essential, such components must be encapsulated to enable their replacement if necessary (to avoid vendor lock-in)
- MOSIP must use open standards to expose its functionality (to avoid technology lock-in)
- Each MOSIP component must be independently scalable to meet varying load requirements
- MOSIP must use commodity computing hardware & software to build the platform
- Data must be encrypted in-flight and at-rest. All requests must be authenticated and authorized. Privacy of identity data is an absolute must in MOSIP
- MOSIP must follow the platform-based approach so that all common features are abstracted as reusable components and frameworks into a common layer
- MOSIP must follow API first approach and expose the business functions as RESTful services
- MOSIP must follow the following manageability principles – auditability & monitor ability of every event in the system, testability of every feature of the platform & easy upgrade ability of the platform

- MOSIP components must be loosely coupled so that they can be composed to build the identity solution according to the requirements of a ID issuer
- MOSIP must support i18n (internationalisation) capability
- All modules of MOSIP should be resilient such that the solution as a whole is fault tolerant
- The key sub-systems of MOSIP should be designed for extensibility. For example, if an external system has to be integrated for fingerprint data, it should be easy to do so.
- No business logic is applied at database level: Database will be used only to store and retrieve data.
- No specific database features to be used: Features that are common across databases which are compliant with open source standards are applied.

How does MOSIP help with establishing standards based ID systems that include refugees?

MOSIP is designed to issue foundational, multipurpose ID - a single unique identifier, which may take the form of a unique number, a mobile OTP, a smart card, a virtual token, or all of the above. It delinks the issue of identity from the issue of establishing status or access to benefits, thereby potentially assisting in implementation of ID across systems. A series of federated databases, or a central repository, could host identity related data. Other systems, such as for food distribution or health providers, would not be able to access the entirety of the database, but instead query it for the authentication of a particular individual.

Use of MOSIP does not necessitate re-enrollment in the system - MOSIP is modular and its digital authentication module, together with its data enrichment and UIN generation APIs could provide a means for digital authentication across existing systems, although a level of customisation would be required in this case. Being open source, MOSIP provides the core technologies for identity establishment, but can be used to suit different use cases and contexts.

To protect the individual’s data, the querying systems would not have access to the identity related data itself - a user could use a virtual ID or token and the only information an authenticating agency could access would be a simple ‘yes’ or ‘no’ answer to the question of whether the individual is who she claims to be. Similar data protection measures exist for offline authentication as well, through digitally signed QR codes.

It is important to note, however, that the governance and policy structures, and the people administering these systems play a far critical role in the safe and secure handling of refugee data. What we hope to introduce through this entry is new way of approaching legacy systems, that harnesses the progress in technology made in the last decade, to provide ‘Good ID’ to some of the most vulnerable people across the world.

More information is available at https://mosip.io