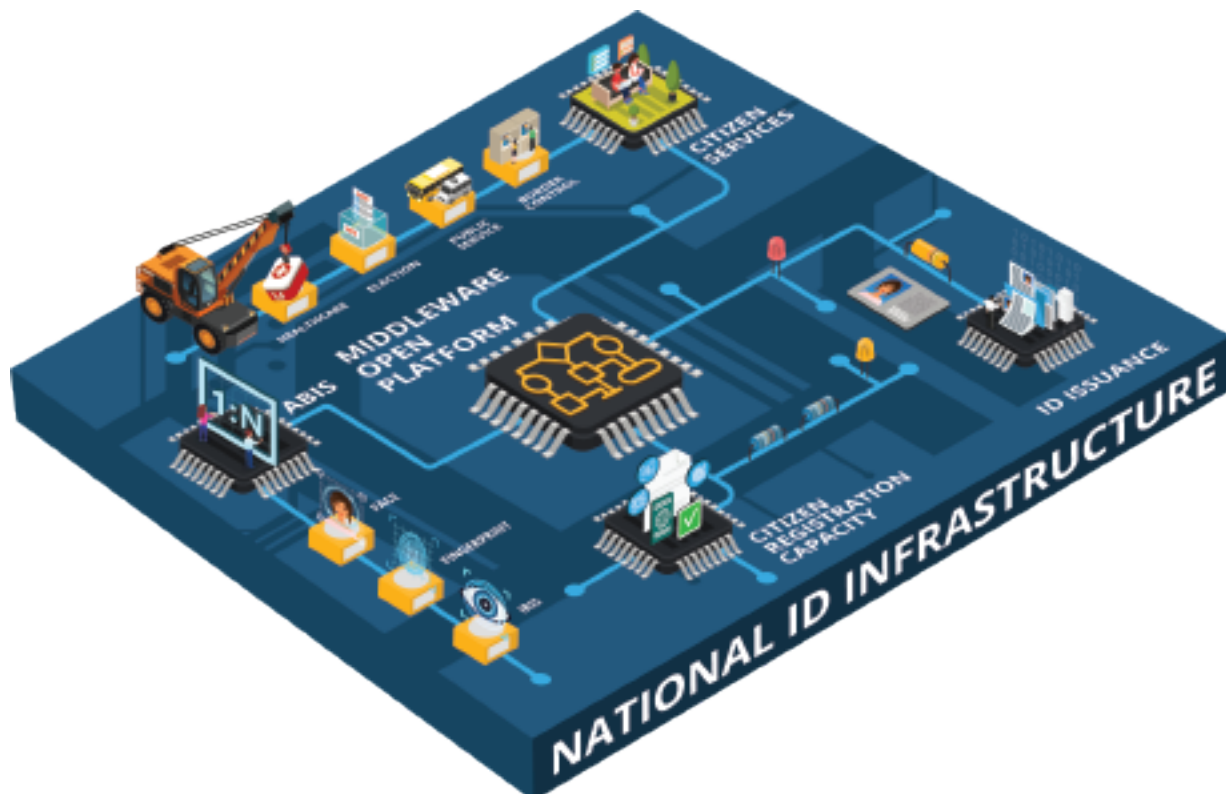


BUILDING A NATIONAL ID INFRASTRUCTURE FOR PUBLIC GOOD IN AFRICA BASED ON OPEN-SOURCE TECHNOLOGIES.

Over the last decade, virtually all industry and service sectors have transitioned to a digitalized mode for the delivery of services and the access of information. Furthermore, many governments have turned to digital ID to drive their National ID projects, resulting in greater security as well as economic and social inclusion in civil registry, and the receipt of a unique ID that facilitates the delivery of e-Government services. A properly implemented digital ID system also helps the private sector to accelerate growth of e-services, leading to economic growth through democratization of fundamental services and easy access to resources at a grassroots level.

Key to creating a foundation ID is to put the appropriate policies, regulations and technologies in place. Previously, a national ID project would typically be implemented by a single technology provider and system integrator who would build the system from scratch. However, the inexperience of the customer coupled with the absence of an appropriate legislative framework to govern the implementation often led to the project being mostly controlled by the vendor and often resulted in serious design flaws in privacy, security and scalability. The projects also often went over budget, suffered significant delays, had inherent design flaws and did not meet requirements. Furthermore, the lack of future proof designs made customers fully dependent on the technology provider and their closed systems that were difficult to expand and integrate with 3rd party solutions. Finally, these systems were rarely designed with privacy in mind, inhibiting a government's ability to make effective regulatory policies and enforce compliance.

An alternative to these limited approaches that address the aforementioned problems is an ID Management solution built on open-source platforms. In the last few years several open-source initiatives have been launched and are becoming more and more attractive to government organizations. These solutions leverage the immense experience gained from the evolution of similar large-scale programs under scrutiny of privacy and security advocates as well as overcome the technical challenges posed by the scale of the project as well as infrastructure and budget limitations. Open source platforms boast privacy and security by design and maintain scalability and modularity. They are also able to integrate with technologies and expertise from multiple vendors that complement the platform's functionality, allowing governments and institutions to benefit from best technology practices, easy compliance with regulations, and avoid issues like vendor lock-in or risk of failed execution.



MOSIP for example, an open source platform inspired by the successful evolution of advanced digital ID programs realized in Estonia, Peru and India, permits the building of an open identity management platform. Such open-source platforms offer several important benefits.

Firstly, they bring the readiness of an open infrastructure designed in accordance with privacy and security guidelines and are based on a number of ready-made components that can be implemented and tailored locally. Both the platform, and the regulatory framework to be developed in parallel, can be replicated and customized to meet a country's particular needs.

Secondly, open-source platforms include a middleware layer that represents a standardized set of functionalities, components and workflows that offer an inherent flexibility to accommodate local requirements, also making it easier for any given country to select a system integrator with specific and proven expertise to manage their identity platform. Furthermore, the substitution of one service provider for another, equally skilled, provider can be done seamlessly due to the existence of a well-known and well-documented environment. In previous implementations of National ID projects, the middleware was typically developed by the awarded ABIS provider almost as a by-product, including vital workflows and data management procedures. This often resulted in the customer not having full visibility and/or access to their own data creating an almost exclusive dependence on the vendor. By standardizing the components that relate to the key intelligence and internal workings of a National ID system, a high level of transparency and data management control can be achieved.

Implementing a comprehensive framework with the appropriate privacy and security regulations means that the solution can address concerns related to inappropriate management of personal data and data leakage, biometric irregularities, or unauthorized access and usage of personal data. This, in turn, can limit legal challenges such as those witnessed in Kenya where lawsuits were filed over the violation of rules for inclusion in the National ID system that prevented some citizens from getting access to services including healthcare, voting, and food support.

TECH5 ABIS and products from other vendors that integrate with the platform are also built using open interfaces like RestAPI's. This design not only gives governments the flexibility to change technology components without having to rebuild the entire ID system and without the need to re-register its citizens, but also avoids vendor lock-in.

Open-source ID management platforms are designed with inclusion at the center. They not only allow registration and deduplication of citizens using biometrics, but also offer utilization of a unique ID via secure authentication for various services. In this way it is ensured that every member of society is included in a system that enables their participation in social benefit programs and minimizes exclusion. The goal of any biometric engine and registration component of a National ID is to create a biometrically protected ID for every citizen. Because the registration phase of the National ID Project is the most expensive in terms of logistics and time, the approach includes capturing the three key biometrics as part of the registration process. This redundancy is necessary because if a biometric solution includes only fingerprints 10% to 20% of the population will be excluded. With the addition of Iris, the probability that any citizen will be able to be registered with at least one biometric increases to 95% - 98%. The third and most intuitive biometric, Face recognition, is also captured to complement the other two.

The inherent modularity of open-source platforms also permits customers to opt for a multi-vendor and multi-project approach. For example, in the Philippines, the project was subdivided into the provision of an ABIS deduplication system by one vendor, registration capacity such as capture devices with the appropriate software provided by a second company, and the integration of the middleware platform to be carried out by a third vendor. This approach requires careful coordination and management. The overall project management structure to ensure oversight as well as clearly defined integration points between the various levels of functionality become very critical.

For example, TECH5 has integrated with the MOSIP platform using the same integration points, and, as such, has become a building block in the overall solution. Integration with MOSIP facilitates replication of the solution for further customers, not having to address changing requirements in terms of interfaces and integration from one implementation to another. Simply put, TECH5 ABIS has become a specialized block of functionality in terms of biometric matching and deduplication, freeing us to focus on our key mission: the development and innovation of our key core technologies, iris, finger and face recognition algorithms in concert with TECH5 matching platforms. Naturally, an institution planning to deploy MOSIP still has the option to choose an ABIS from other providers.

A well implemented project can become the backbone and springboard to further layers of citizen services and functionality (technology stack) built on top of the basic ID management infrastructure. In India, for example, the Aadhaar platform was extended to house various technology stacks such as a Unified Payment Interface to facilitate money transfer, and Digilocker to retrieve, store and share verified digital documents.

Lesson to be learned: a house of services requires a solid foundation (al ID).