



HARMONIZATION OF THE IDENTITY ECOSYSTEM: A PRAGMATIC VIEW

By Dr. Joseph J. Atick, Executive Chairman, ID4Africa

WHAT IS HARMONIZATION?

Harmonization is the theme of this year's ID4Africa Annual Meeting. It is a term that has received a lot of attention recently because of the current fragmentation in the African identity ecosystems. But what does it really mean? And how can a country achieve it?

An ecosystem is said to be harmonized if two conditions are satisfied. First, the identity of a real person is unique and is linkable across all identity databases (assuming legal authority and privacy protections are in place). These repositories include foundational databases such as civil registers, national population registers as well as functional registers serving sectoral needs such as databases of voters or health insurance, to name a few. Second, if these databases are synchronized for life, such that when an update takes place it propagates across the ecosystem. In practice, achieving full harmonization is difficult and the road to getting there may be long depending on the starting point and the country's capacity. That should not be discouraging anyone because steps made towards harmonization can have significant value even when full harmonization is incomplete; the exercise is not all or nothing.



WHAT IS AN IDENTITY ECOSYSTEM?

An ID ecosystem is the ensemble of the components listed in Table 1 pooled from all sectors and integrated to empower the beneficiaries to assert their unique identity to claim legal, human, and administrative rights, while at the same time being held accountable for their individual responsibilities towards the relying parties. From an administrative perspective a properly functioning ID ecosystem supports service delivery. It leads to more efficient, effective and transparent governments.

| ASSETS | PROCESSES | FRAMEWORKS | STAKEHOLDERS | BENEFICIARIES |
|--|--|--|--|---|
| <ul style="list-style-type: none"> Identity data Unique Identity Numbers (UIN) Points of contact with population Credentials Digital Certificates | <ul style="list-style-type: none"> On-boarding Vetting Personalization Issuance Secure ID services (verification, identification) | <ul style="list-style-type: none"> Privacy protection Legal frameworks Institutional frameworks | <ul style="list-style-type: none"> Civil registers National ID Elections Healthcare Statistics Finance Immigration ... | <ul style="list-style-type: none"> The population Government or private organizations that need ID for accountable service delivery |

Table 1: The identity ecosystem is the ensemble of the above components integrated together to empower the beneficiaries

THE CURRENT REALITY: THE IDENTITY SILOS

Absent central or coordinated planning or national regulations, it is inevitable that the identity ecosystem in a country will develop into silos (Fig.1), which is the case in most African countries today, where multiple identity systems proliferate serving different functions with little link among them.

While Silos have a role to play in allowing organizations to develop ID expertise or pilot concepts, ultimately, they represent an impediment on the path of performant ID ecosystem development.

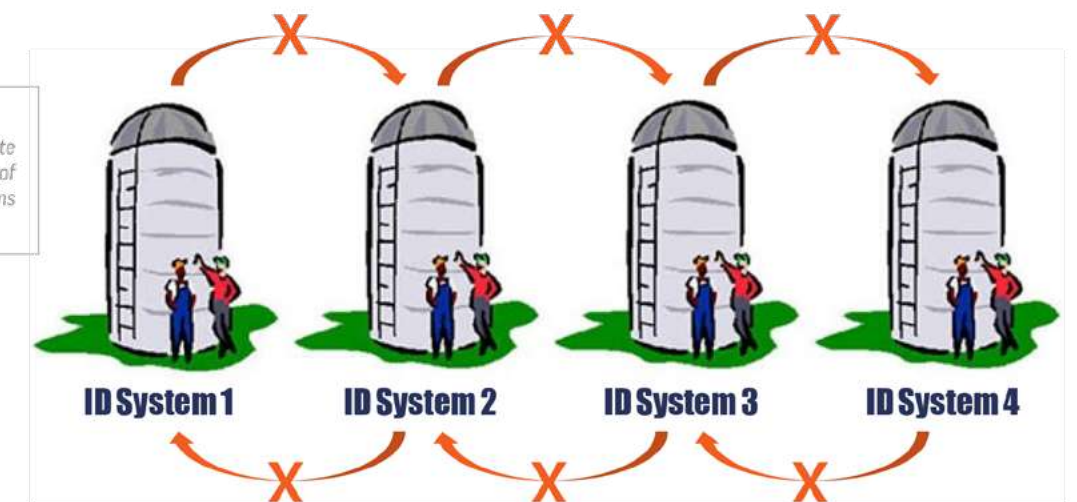
The emergence of ID silos is the path of least resistance for the development of the ecosystem. It is easier to launch an identity program standalone, where an agency is not constrained by multi-stakeholder coordination. It represents lower initial cost and faster adoption. Consequently, many of these identity systems have developed quickly and

organically without necessarily working within a national identification strategy, which is difficult to adopt given that such a strategy would require political will at the highest level to pressure the typically large number of stakeholders to cooperate.

In addition to the high degree of non-interoperability that exists today, the identity systems themselves continue to have low coverage, no Unique Identifying Number that is used by all, no common identity model and no uniformly recognizable credentials. The consequences are:

- Big challenges to service delivery.
- High exclusion & high inconvenience to the public.
- Undermined development (especially banking sector).
- Duplication of effort and investments.
- Challenged civil sector reform.
- Limited range of possible applications and e-Services.
- A missed opportunity to serve the public better.

Figure 1: ID system silos dominate the current landscape of identification ecosystems in Africa.



CALL TO ACTION: A PRAGMATIC CHECKLIST

It is clear the current situation must change. Identity stakeholders in each African country collectively have the opportunity to rectify this situation by working together to adopt policy and actions that

steer the country towards ultimate harmonization. Here is a pragmatic checklist of the actions that the stakeholders should consider as they undertake to reform the identity practices in their countries:

| WORK STREAM | SUGGESTED ACTIONS |
|--|--|
| ESTABLISH THE RIGHT LEVEL OF SUPRA-INSTITUTIONAL OVERSIGHT | <ul style="list-style-type: none"> Identify the identity stakeholders in the country and establish their roles and responsibilities. Form a Technical Steering Committee (TSC), with champions representing each stakeholder, reporting to the highest political level in the country (President's, Prime Minister's Office, or parliament). Ensure inclusive representation on the TSC. Empower the TSC to make decisions and take actions that will have collective impact (e.g. adopt standards, data models etc) The TSC needs to be shielded from political changes in order to avoid disruptions of its long term operations. |
| SET COMMON OR NATIONAL OBJECTIVES | <ul style="list-style-type: none"> An important deliverable of the TSC needs to be a National Identification Strategy (NIS) that is embraced by all the stakeholders and updated from time to time. To inform the operationalization of the NIS, conduct first a diagnostic of the identity ecosystem in the country including assessment of ID data quality across all repositories in all sectors. Adopt common vocabulary for identity management and harmonize as much as possible the business processes that impact identity across sectors (e.g. try to use the same type of enrollment procedures). Agree on the identity data model, vetting and validation processes for enrollment and exception handling for failure to enroll and failure to authenticate. |
| CHOOSE A DATA HARMONIZATION PATHWAY | <ul style="list-style-type: none"> This is a critical step and requires making an informed choice of what pathway for harmonization to take based on what you learn from the diagnostic (see the options for the harmonization pathway below). Ensure that whatever pathway is taken, provisions are made to link Civil Registration (birth and death) to foundational ID to ensure ecosystem integrity. Support the development of the right institutions and capacity needed to affect the chosen path. Seek the correct level of political support and sustainable funding to ensure success. |
| PUT IN PLACE THE NECESSARY LEGAL FRAMEWORKS AND POLICIES | <ul style="list-style-type: none"> Define legal identity and determine the process for how to provide it. Establish a supportive legal, regulatory and authorizing environment (allows agencies to capture data etc). Embrace a rights-based approach, with policy regarding unacceptable data in ID registers. Consider making the Unique Identity Number mandatory for all sectoral interactions; ensure that getting a UIN is free of charge to the individual. Adopt Data Protection policy. Build risk model for ID systems and recommend safeguards to be adopted by each sector. Conduct impact studies on women and minorities to refine ID systems policy to ensure they are pro-women and minorities. Embrace digital migration as a matter of policy, but maintain physical credentials and certificates as assurance (like receipts) against government manipulation of electronic records. |
| ADOPT THE APPROPRIATE CREDENTIAL AND SOLUTION STRATEGIES | <ul style="list-style-type: none"> Allow each sector to decide on their credentials strategy but look for national synergies among them (e.g. establishing a common secure printing facility, or shared credentials, or buying power). Urge all sectors to adopt solution strategy anchored on standards-based or open non-proprietary architectures with cost efficiency, interoperability, scalability, reliability and availability built by design into their requirements. Promote sustainable systems as opposed to one-off campaigns or solutions and build institutions and capacity for identity management in sustainable manners in each sector. |
| PROMOTE TRANSPARENCY | <ul style="list-style-type: none"> Encourage all the stakeholders to communicate with the public transparently and have them provide channels for engagement with the civil society and the general public for feedback, complaints, redress etc. |

PATHWAYS TO HARMONIZATION OF IDENTITY DATA

date a **National Population Register (NPR)**, which contains the identifying data of all individuals in the country (citizens, legal residents, refugees). This register would be used as a foundational system that supports all functional needs of all the other sectoral stakeholders.

NIDA would have the following tasks:

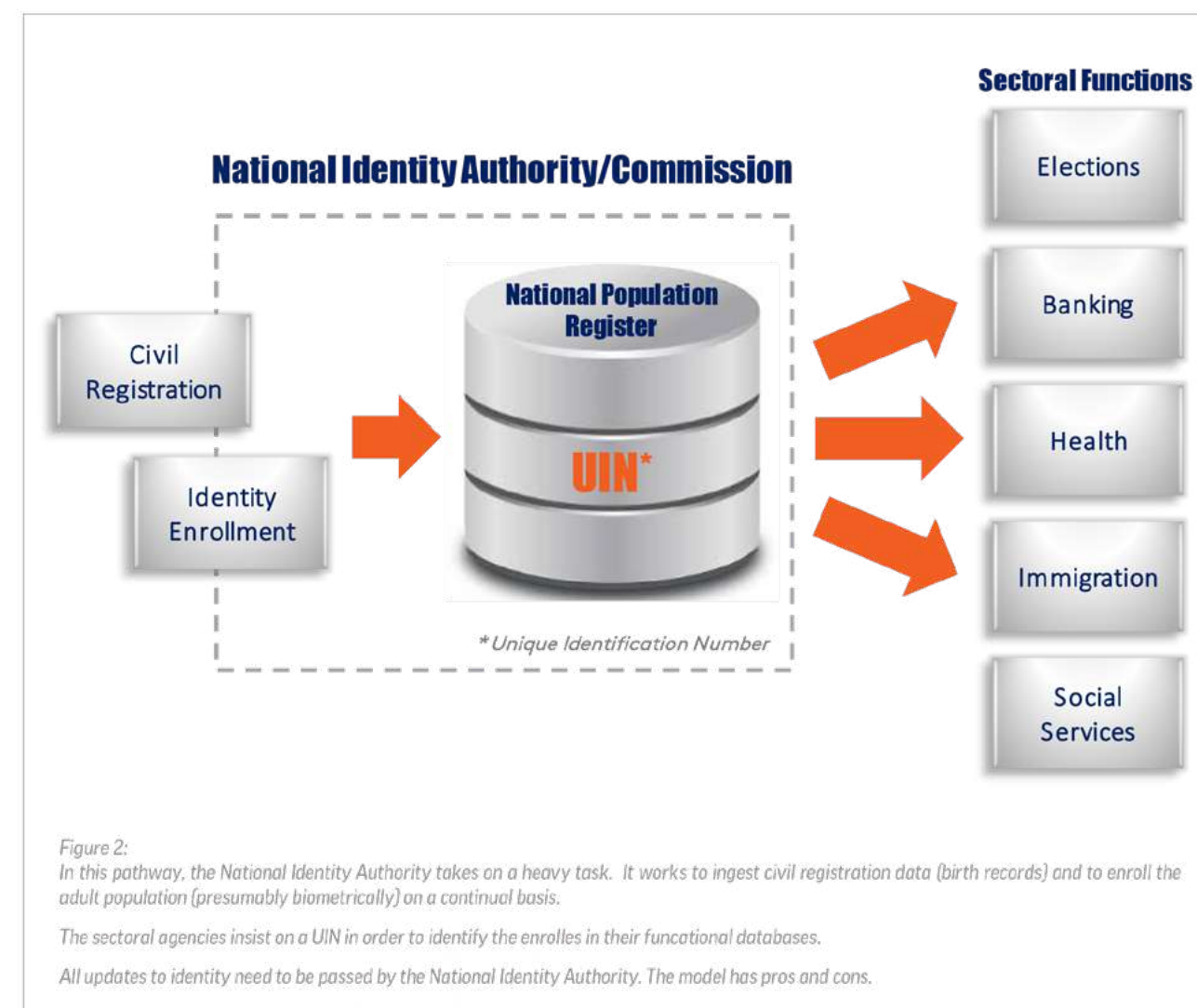
- Enroll the entire population using the national identity data model (minimal amount of data).
- Deduplicate the identity records.
- Assign a **Unique Identity Number (UIN)**.
- Build **on-line identity services** that include verification and identification.

PATHWAY I: FRESH START

In the circumstance that the assessment reveals that there is no data of sufficient quality in the sectoral repositories, then this is the pathway to take. This is the same pathway taken successfully in **India, Pakistan, Estonia and Peru**, to name a few.

In this case the TSC designates an institution in a privileged role, e.g. **National Identity Authority (NIDA)** or Commission or its equivalent (Fig.2). NIDA is tasked with building and maintaining up to

Sectoral agencies from that point on would link their services to the UIN and would use the online identity services provided by NIDA to verify the identity of potential claimants of service. Nothing would prevent each agency from enriching the identifying data with sector specific information (KYC: know your customer). In India the Aadhaar number is now required for all government services. This model has advantages and disadvantages as shown in Table 2.



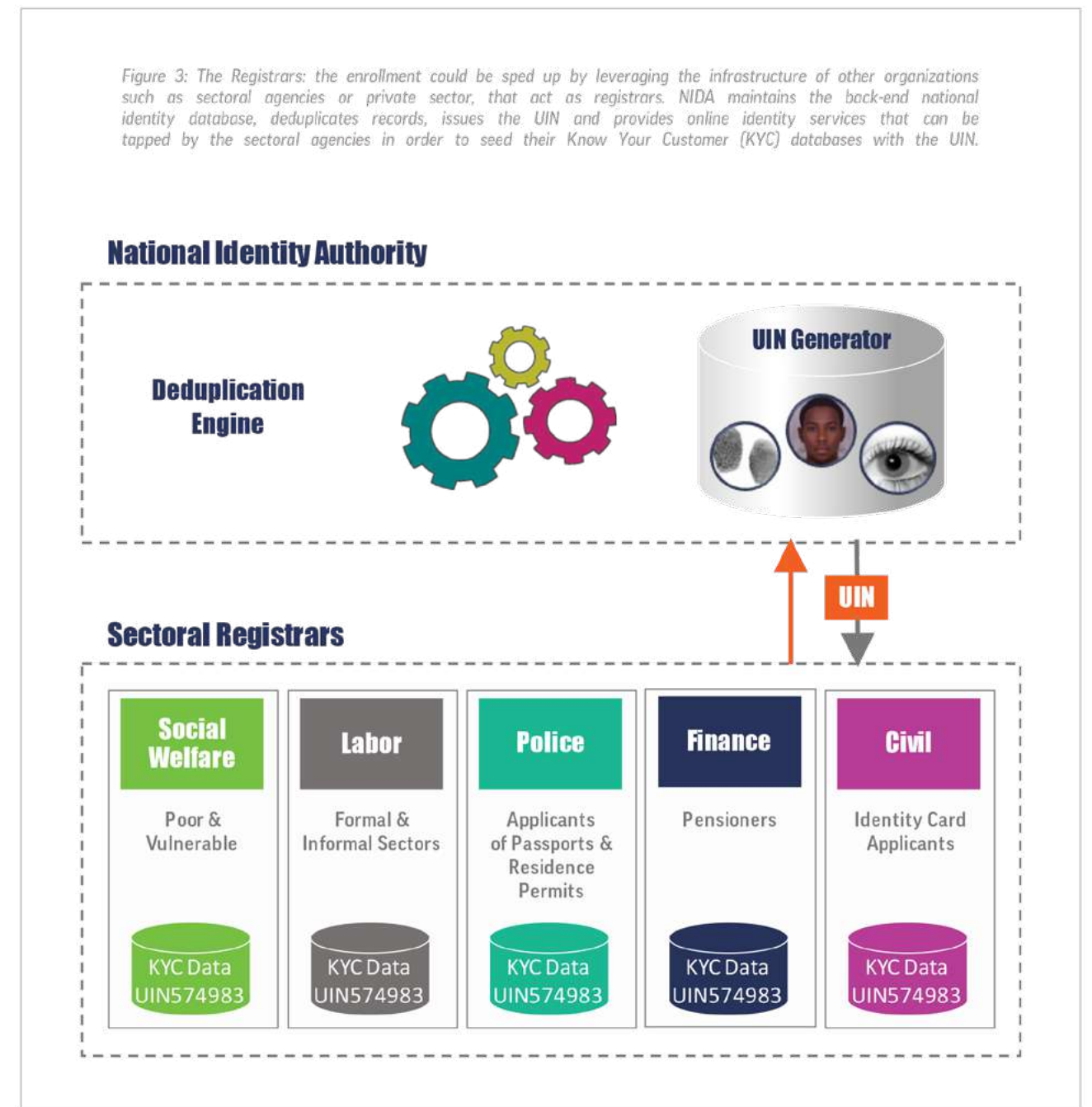
Of course, this is the opportunity to connect civil registration to the National Population Register by ensuring that birth certificates are issued with the UIN which is generated by NIDA and that the UIN will accompany the individual from cradle to grave.

| PROS | CONS |
|--|--|
| <ul style="list-style-type: none"> • Cost effective over lifetime • Leveraged investment: Enroll once use many times (easier for the population) • Results in more reliable and higher quality ID data especially since the data is collected using more recent and more advanced capture technologies which tend to give high quality data • A true infrastructure for the country • Could be aligned with a national vision (Estonia, India, ...) • Avoids multiple registration and redundancy • Supports many Use-Cases & innovation • Provides economies of scale | <ul style="list-style-type: none"> • May be ideal but hard to realize • Takes long to realize its potential. Slower to launch and take-up, since immediate applications may not drive it • Requires sustained political will: could be vulnerable to changing governments • Requires significant degree of national planning, execution & centralization • Does not leverage points of contact with the population held by other stakeholders • Could be potentially costlier initially. • Development returns are realized upon use. |

Table 2: The pros and cons of the pathway to harmonization where freshly captured data is collected by one organization (NIDA) and is centralized and made available to all sector agencies to meet their functional ID needs.

There are several variations on this model, where NIDA employs Agents in order to rectify some of the disadvantages inherent to this pathway for harmonization:

| VARIANT | DESCRIPTION |
|--|---|
| SECTORAL REGISTRATION AGENTS (REGISTRARS) | Sectoral organizations act as agents to enroll people on behalf of NIDA—so called registrars (see Fig. 3). NIDA could pay the registrars for each successful new unique identity that they submit for enrollment. This option is compelling if the right institutional and financial arrangements can be established, since the sectoral agencies normally have already significant number of points of contact with the population which they can use to perform the enrollment. This can result in substantial cost savings as it leverages existing infrastructure and civil servants. The concept of registrars does not have to be limited to sectoral agencies. It could also include private sector companies that are certified by NIDA. India has shown that this model works very well as the Unique Identity Authority of India was able to consistently enroll 200 million people per year leveraging registrars. |
| FEDERATED IDENTITY ATTESTATION AGENTS | Sectoral agencies keep the identity data that they collect subject to common identity data model and standards. Their repositories become reference identity databases and these organizations can act as trusted identity attestation agents (IAA) that vouch for someone's identity. An individual can choose the central bank, a commercial bank, the electoral commission or the national ID card database, etc., as their IAA. NIDA's role becomes to federate all these repositories and intermediate among the IAAs. Based on the IAAs attestations, it can assign UIN to individuals and ensure that a person gets only one number even when they may be present in multiple IAA databases. This federated deduplication model can work technically but it is more complex to implement within the development context. It is more appropriate in developed countries (e.g. Gov.uk Verify). |



PATHWAY II: REUSE OF LEGACY DATA

If the assessment conducted by the TSC reveals some valuable legacy identity data, then a cost benefit analysis would have to be performed to determine if it makes sense economically to reuse that data (Fig. 4). This is an exercise of integration of databases which is not trivial but is doable with the right technology. It involves establishing correspondence between the same identities across different databases even when the identity data models are different and the data quality non-uniform.

Some of what is involved may include:

- Implementing entity or identity resolution technologies to allow establishing correspondences among identity records across different databases.
- Implementing the latest versions of Automated Biometric Identification Systems (ABIS) that allow for matching partial, imperfect or low quality biometric data samples. Over the years biometric matching technology has improved

dramatically, which means that the chances of discovering reliable links are higher today than they were five years ago. Still data quality remains the most critical factor for success.

- In practice the pathway chosen will be a **hybrid of path I & II** where some high-quality data is reusable while for the rest a fresh start would be required.
- It is not enough to harmonize data at one point in time, need to synchronize on an ongoing basis. To do that, sectoral agencies must commit to using the UIN systematically and to relegate all updates to identity data to NIDA.

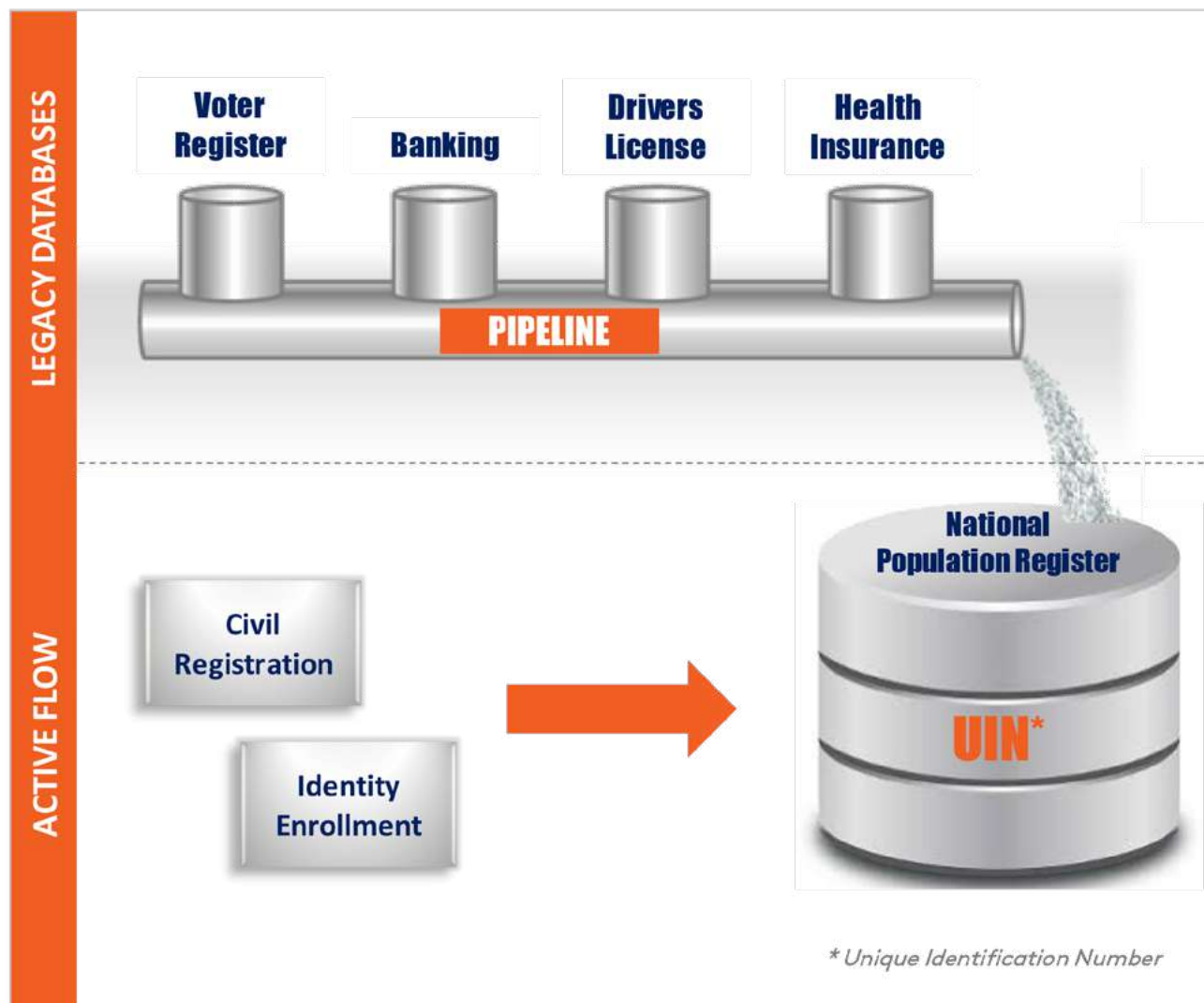


Figure 4: Harmonization of legacy databases requires a parallel exercise to civil registration and ID enrollment where the databases are consolidated, and correspondences are established using entity resolution technology before a UIN is assigned. This is a fruitful exercise only if the legacy data has sufficient quality.

CONCLUSIONS

While the path to harmonization of the identity ecosystem in a country depends on what identity assets exist and the fact patterns specific to that country, in our opinion the majority of African countries, are better off choosing Pathway I, the fresh-start path. This should be coupled with strong policy mandating the use of the unique identity number for the business processes of as many sectoral agencies as practical. We also recommend the use of registrars to accelerate achieving full coverage, which should be one of the primary goals of any reform.

We are pleased to see that Nigeria, the host of ID4Africa 2018, has embarked on this precise path. We hope to use the experience of NIMC as a successful case study in future ID4Africa Annual Meetings.

One identity for one individual for one lifetime for all sectoral needs should be the first principle driving the deliberation of any steering committee looking to reform the identity ecosystem in a country.

No matter what steps are taken, it is important that identity systems developed in Africa from this point forward adhere to international standards. This protects the country's investment by avoiding vendor lock-in and allowing more flexibility to meet all future and evolving needs. Today, the landscape of standards that impact identity systems is highly developed as can be seen from Table 3. Navigating that tapestry requires the guidance of competent experts in the domain of ISO standards. We recommend that the Technical Steering Committee retain the right consultants for this task and insist that any procurement in the country must make the applicable standards part of the requirements in any procurement or request for proposals documents.

| | | |
|--|---|---|
| Interoperability of capture devices ISO/IEC 19784 (BioAPI) | Biometric data standards ISO/IEC 19794 (image & template formats) | Packaging biometric data (CBEFF) ISO/IEC 19785 (Common Biometric Exchange Format Framework providing common structure, metadata & security) |
| Biometric sample quality ISO/IEC 29794 | Credential standards <ul style="list-style-type: none"> • ISO/IEC 7810 to 7813 ID Cards Standards • ISO/IEC 7816 eIDs, Smart Cards, Contact Cards Standards • ISO/IEC 14443 Contactless Cards Standards • ISO/IEC 8583 Standard for Payment Cards with Magnetic Stripe • ICAO 9303 Standards for Machine Readable Travel Documents (MRTDs) • EMV Standard for Payment Cards (CAP-MS, DPA-Visa, EuroPay) • ECOWAS specifications | |
| Authentication <ul style="list-style-type: none"> • ISO/IEC 24761 Authentication Context for Biometrics • ISO/IEC 29115 Entity Authentication Assurance Framework | | |

Table 3: The complex tapestry of standards that need to be adhered to in order to ensure a healthy and harmonized identity ecosystem not just at one point in time but for all times going forward.