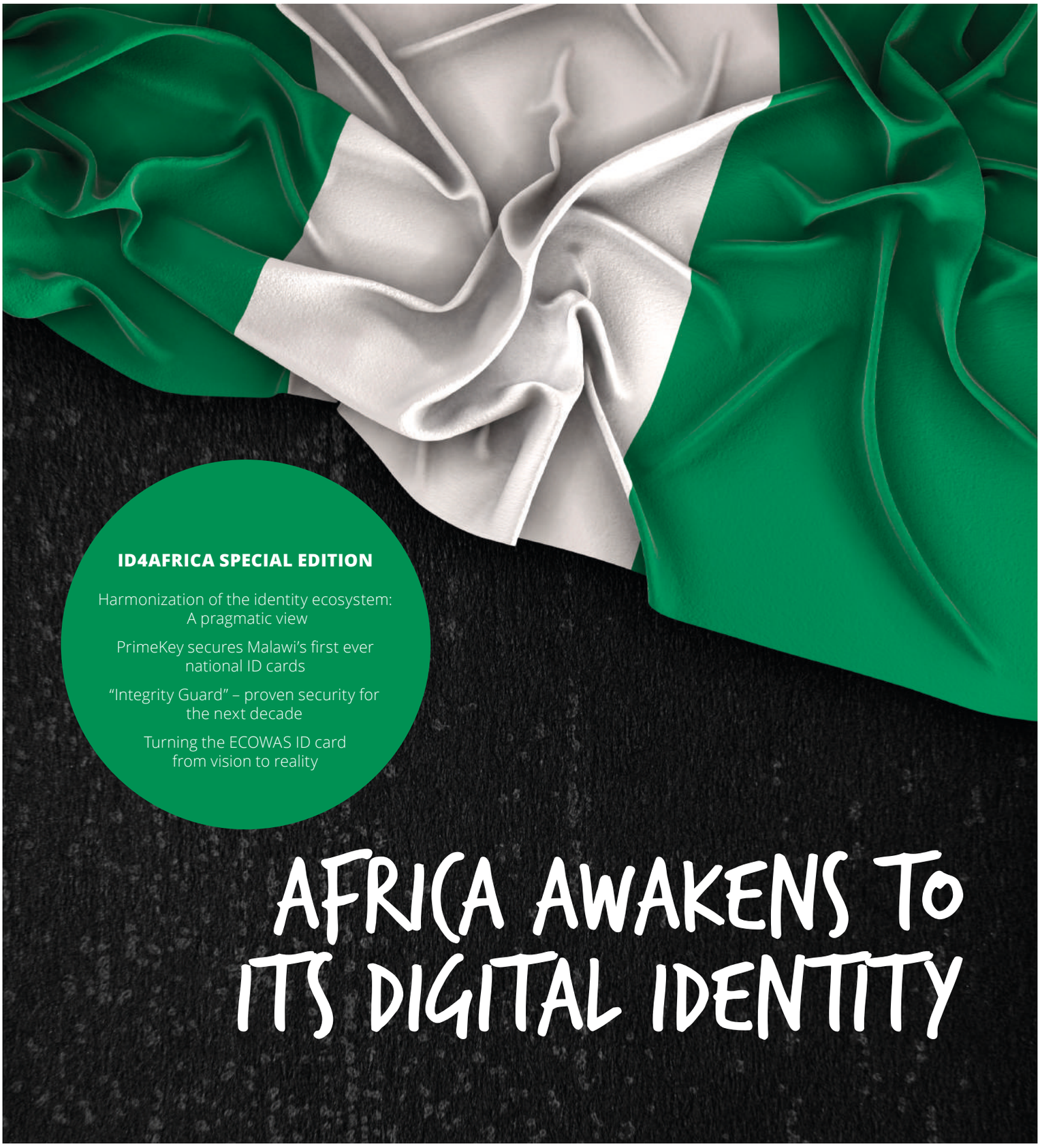
NEWS & INSIGHTS FROM THE WORLD OF ID SECURITY

APRIL 2018 | SPECIAL EDITION

The VAULT



ID4AFRICA SPECIAL EDITION

Harmonization of the identity ecosystem: A pragmatic view

PrimeKey secures Malawi's first ever national ID cards

"Integrity Guard" – proven security for the next decade

Turning the ECOWAS ID card from vision to reality

AFRICA AWAKENS TO ITS DIGITAL IDENTITY

MASKTECH

We make chips intelligent

Meet us at
• ID4Africa
• Connect:ID
• SDW

MTCOS® – ID CHIP SOLUTIONS FOR eGOVERNMENT APPLICATIONS

- High Security Operating System (MTCOS®), e.g. ePassports, eIDs, eHealth cards
- Independent worldwide supplier
- More than 65 eID-document references
- Up to EAL5+ Common Criteria certified on a unique variety of chip platforms

SecurITy made in Germany

TeleTrusT Quality Seal www.teletrust.de/tsmg

Common Criteria

MaskTech GmbH • Nordostpark 45 • 90411 Nuernberg • Germany • sales@masktech.de • www.masktech.de • +49(0) 911 95 51 49 0

Contents

Imprint

THE VAULT
Published bi-annually by Krowne Communications GmbH, Berlin.

PUBLISHER: Krowne Communications GmbH, Steve Atkins, Sächsische Straße 6, 10707 Berlin
EDITOR-IN-CHIEF: Steve Atkins
ART DIRECTOR: Lana Petersen

EDITORIAL CONTRIBUTIONS: Dr. Joseph J. Atick, Karin Trogstam, Dirk Melzer, Steve Atkins, Markus Hoffmeister
PHOTOS: ID4AFRICA, UNICEF, HID GLOBAL, ISTOCKPHOTO, MELZER MASCHINENBAU, CRYPTOVISION
PRINTING: Shanghai, China
EDITION: April 2018

AMBASSADORS for *African* IDENTITY

By Steve Atkins, Program Director, The Silicon Trust

One of the more compelling elements of the ID4Africa Movement (and there are many) is its use of what it terms 'Ambassadors' within its Ambassadors Program. Less a description of a career diplomat, more an inclusive approach to identify and recognize individuals working with Governmental roles in the various African Nations who have an understanding and hands-on role in the rolling out of citizen ID throughout their particular country.

These 29 Ambassadors, representing over 75% of sub-Saharan Africa by population, are senior-level government officials with well-defined missions to promote and manage legal identity in their countries. Having been selected based on merit and experience, they represent a growing movement of individuals who are passionate about digital identity and the positive impact its various applications have on their nation's socio-economic development. As identity experts, they volunteer their time to promote the responsible use of digital identity in Africa and act as important liaisons between ID4Africa and the institutions and identity stakeholders in their respective countries.

As Dr. Joseph Atick, Executive Chairman of the ID4Africa Movement said, "The Ambassadors' Program" is a platform for empowering African civil servants to influence and advance the identity agenda in Africa. The Ambassadors play an integral role in influencing the direction of the ID4Africa Movement, keeping us informed on issues that are pertinent to our constituent countries. They ensure that their countries' issues and concerns are part of the collective agenda of the movement and that their countries are well represented in their delegations to the ID4Africa Annual Meeting." He added, "Over the years, the level of seniority of the Ambassadors has risen, which is a testament

to the importance the member countries are attaching to their participation in the Movement."

You may be forgiven for thinking that many of these African nations demonstrate an inequality in terms of their journey towards implementation of digital identities within their countries. It is true that some nations are further advanced than others. However they share more commonality in obstacles and frustrations that need to be overcome, whatever their particular nation requirements.

It is this 'hands-on' approach that the ID4Africa Movement encourages. "If the African Nations don't own the responsibility for their digital identity implementation, then it is too easy to blame other outside instruments that may be financial or developmental in nature," Atick told me.

So what are the overriding views that these Ambassadors are sharing with the movement? What are their challenges? They are not as uncommon as you may expect.

There is an overriding frustration to find funding for such an undertaking; be it from Governmental sources or other alternatives. There is also a lack of documentation to support citizenship on one hand and a constant complaint of a 'silo' approach from agencies within these countries that bear partial responsibility for the implementation of digital identity as a whole. Ethiopian Ambassador Daniel Lishanew pointed out that in their country "There is no integration or linking between current manual paper-based registrations and other ID-based systems such as health management, driving licenses etc., that require the use of a UID number."

The sheer scope of these digital identity programs brings a lot to bear upon the technical aspects of such undertakings. Take Rwanda for example. Rwandan Ambassador, Jacques Kayisire said, "(We have) completed the implementation of Electronic National Population Registry, enrollment, production and distribution of ID Cards to all eligible citizens aged from 16 years and above. The challenge we have is to implement the under 16 years ID Cards (i.e. their biometric data capture given that the data collection is an expensive exercise – at the same time biometrics biometric of kids keeps on changing from day one to 16 years old). So the challenge is on the technical side of it and financial resources."

Tanzanian Ambassador, Alphonce Malibiche, was more upbeat, "We face a number of challenges in Tanzania – but we are not afraid of them. The challenges that I imagine many African countries share with us include inadequate connectivity and infrastructure (especially in rural and remote areas) and the absence of rich civil registration records to serve as evidence during enrollment. In addition, Tanzania is a geographically large and diverse country, which makes logistics more difficult for us than perhaps many other countries," said Malibiche, "With time, political commitment and planning, we are overcoming these challenges."

As always, however, we must not dwell purely upon the negatives. There are standout programs and implementations that have been taken on an individual country level – Malawi, for instance. "Malawi has just completed registration of 9.1 million Malawians aged 16 years and above. The figure is slightly higher than the estimated number eligible for an ID in Malawi. The ID printing and distribution is in progress. By March 2018, all registered will have a National Identity Card. Currently meetings are underway with relevant stakeholders to appreciate the usage of the card and the interface of ID database with relevant systems either in the public or private sector for appropriate data sharing within a legal framework that complies with international principles for the right to privacy and data protection," explained Malawian Ambassador, Sophie Kang'oma.

All nations agree that the ID4Africa Movement is playing a vital role in helping African nations overcome these challenges. Nigerian Ambassador, Godswill Chinemerem Ukauwa, best summed up the current situation. "In my opinion, I can say that African countries Identity Management System are characterized by lack of continuity in agenda, cynicism, inconsistency, technological backwardness, absence of digitalized identity Registration, vulnerable class, and lack of access to some rural areas, political instability that may derail existing agendas due to party interests, non-compliance to Development Agencies program, and much more. The emergence of ID4Africa has brought about the acceptance of digital identification system as a world agenda and adoption with little or no little or no complicity, and with realistic solutions to the challenges others faced in ignorance. The formation of ID4Africa in 2014 and the commencement of International Meeting from one African Country to the other are tantamount to awakening African nations from slumber as it affects digitalizing the identity of its citizenry and responsible use of identity."

Aiphonce Malibiche of Tanzania agrees, "ID4Africa plays an important role for two reasons. First, it allows practitioners and stakeholders across the continent to learn from each other, including how to overcome common challenges, trends in technology and other innovations, and what each country's

> *"The formation of ID4Africa in 2014 and the commencement of the International Meetings from one African Country to the other is tantamount to awakening African nations from slumber as it affects digitalizing the identity of its citizenry and responsible use of identity.*

plans are moving forward. Second, because no such forum on digital identification exists for the continent, ID4Africa helps us build relationships and networks, which are instrumental to continuing the knowledge exchange between the Annual Events and creates opportunities for collaboration, such as for mutual recognition of identification between countries."

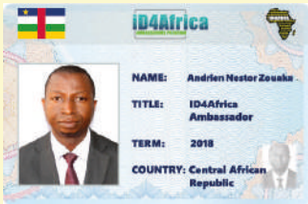
It is interesting when asking about future challenges that there appears to be a commonality in response from the various Ambassadors. Namely, that if any ID scheme is to work (interdependent of the specific African nation) there is a need for a trusted national registry that can act as a platform upon which functional systems can be based. This in turn is dependent upon a robust Internet connectivity if a particular nation is to have an efficient and cost effective identity system. Government commitment, skilled human resource especially on IT, and finances remain vital factors in contributing towards the achievement of a better digital identity system.

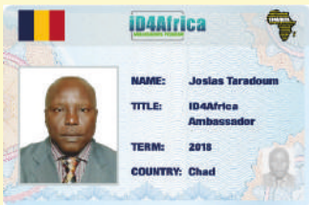
Kenyan Ambassador, Reuben Kimotho is also looking beyond immediate national ID requirements and into the future, "(There is a...) lack of mutual recognition and interoperability of national ID cards. Africa as a continent is growing and regions, including countries, are opening up its borders for cross border movement of persons and goods. We must ensure that authentication and verification services are developed to maximize on these efforts and hopefully move towards the acceptability and ownership by other government agencies of eID as a multipurpose card".

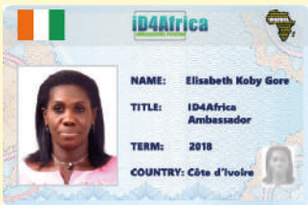
ID4Africa remains an amazing movement aimed at bringing Digital Identity to the African continent. Mohamed Ntilitt, the Ambassador for Mauritania, perhaps best summed up the Ambassadors' feelings about such a movement; " We come to the conclusion that, indeed, there is a common challenge for all African states, that of acquiring digital identity and taking ownership of it. But the way to get there is not necessarily the same. Indeed, for each country, specific factors such as context, existing identity assets, and development priorities must be taken into account in the development of a national strategy for the development of a functioning digital identity ecosystem.

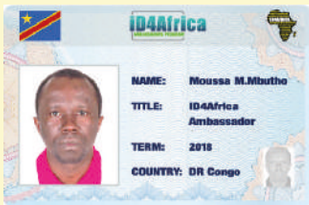
To achieve this, the ID4Africa Movement is undoubtedly a source of vital advice for governments in developing countries, as well as international organizations, to better understand the positive impact of electronic identity on social development and economic and political factors in these countries but also for user organizations and suppliers for the development of their technology roadmap and their underlying strategies." ☒

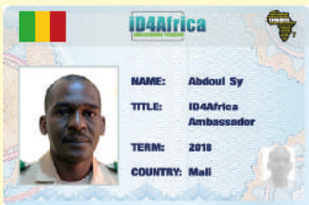
MEET THE 2018 ID4Africa *Ambassadors*

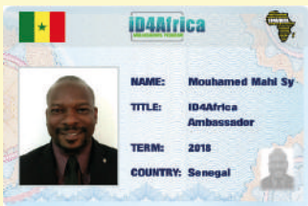


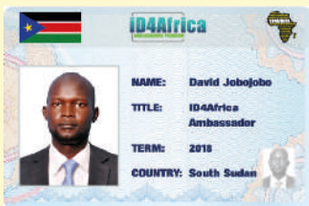












Harmonization of the IDENTITY *ECOSYSTEM*: A *pragmatic* VIEW

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 couple. Second if these databases are synchronized for life, in that when an update takes place it propagates across the ecosystem. In practice, achieving full harmonization is difficult and the road to get there may be long depending on the starting point and the country's capacity. That should not discourage 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
• Identity data • Unique Identity Numbers (UIN) • Points of contact with population • Credentials • Digital Certificates	• On-boarding • Vetting • Personalization • Issuance • Secure ID services (verification, identification)	• Privacy protection • Legal frameworks • Institutional frameworks	• Civil registers • National ID • Elections • Healthcare • Statistics • Finance • Immigration • ...	• 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

L'HARMONISATION de *l'écosystème D'IDENTITÉ*: Une VISION *pragmatique*

Par Dr. Joseph J. Atick, PDG, ID4Africa

☐ Qu'est-ce que l'harmonisation?

L'harmonisation est le thème de la réunion annuelle ID4Africa de cette année. C'est un terme qui a reçu beaucoup d'attention récemment compte tenu de la fragmentation actuelle dans les écosystèmes d'identité en Afrique. Mais qu'est-ce que cela signifie vraiment ? Et comment un pays peut-il y parvenir?

Un écosystème est harmonisé si deux conditions sont remplies. Premièrement, l'identité d'une personne réelle est unique et peut être liée à la même identité dans n'importe quelle base de données (en supposant que l'autorité légale et la protection de la vie privée sont en place). Ces répertoires de données comprennent des bases de données fondamentales telles que les registres d'état civil, les registres nationaux de la population ainsi que des registres fonctionnels répondant à des besoins sectoriels tels que les registres d'électeurs ou d'assurance maladie, pour n'en nommer que quelques-uns. Deuxièmement, si ces bases de données sont synchronisées à vie, c'est-à-dire que lorsqu'une mise à jour a lieu, elle se propage à travers l'écosystème. Dans la pratique, il est difficile de parvenir à une harmonisation complète et le chemin à parcourir peut-être long en fonction du point de départ et de la capacité du pays. Cela ne devrait décourager personne, car les mesures prises en vue de l'harmonisation peuvent avoir une valeur significative même lorsque l'harmonisation est incomplète; l'exercice n'est pas tout ou rien.

C'est quoin un écosystème d'identité?

Un écosystème d'identité est l'ensemble des composants listés dans le Tableau 1 venant de tous les secteurs et intégré pour permettre aux bénéficiaires d'affirmer leur identité unique afin de revendiquer des droits légaux, humains et administratifs. D'un point de vue administratif, un écosystème d'identité fonctionnant correctement soutient la prestation de services. Cela conduit à des gouvernements plus efficaces et plus transparents.

ACTIFS	PROCESSUS	CADRES	PARTIES PRENANTES	BÉNÉFICIAIRES
• Données d'identité • Numéro identifiant unique (NIU) • Points de contact avec la population • Titres • Certificats numériques	• Inscription • Validation • Personnalisation • Emission • Services d'identification sécurisés (vérification, identification)	• Protection de la vie privée • Cadres juridiques • Cadres institutionnels	• État civil • Identité nationale • Élections • Santé • Statistiques • Finance • Immigration • ...	• La population • Organismes publics ou privés ayant besoin de l'identité pour la prestation de services responsable

Tableau 1 L'écosystème d'identité est l'ensemble des composantes ci-dessus intégrées pour autonomiser les bénéficiaires

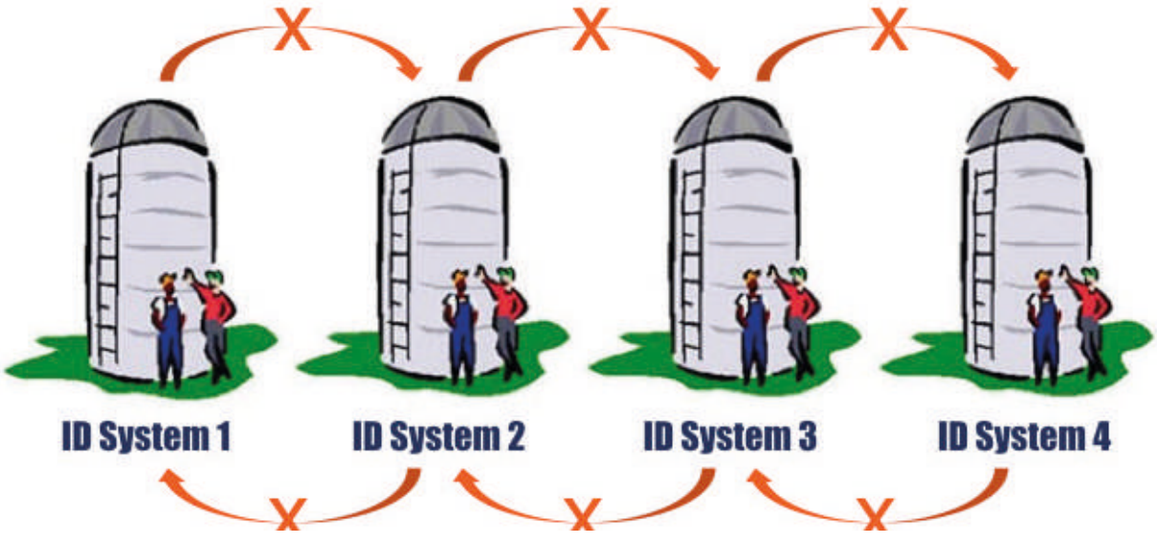


Figure 1 ID system silos dominate the current landscape of identification ecosystems in Africa.

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.

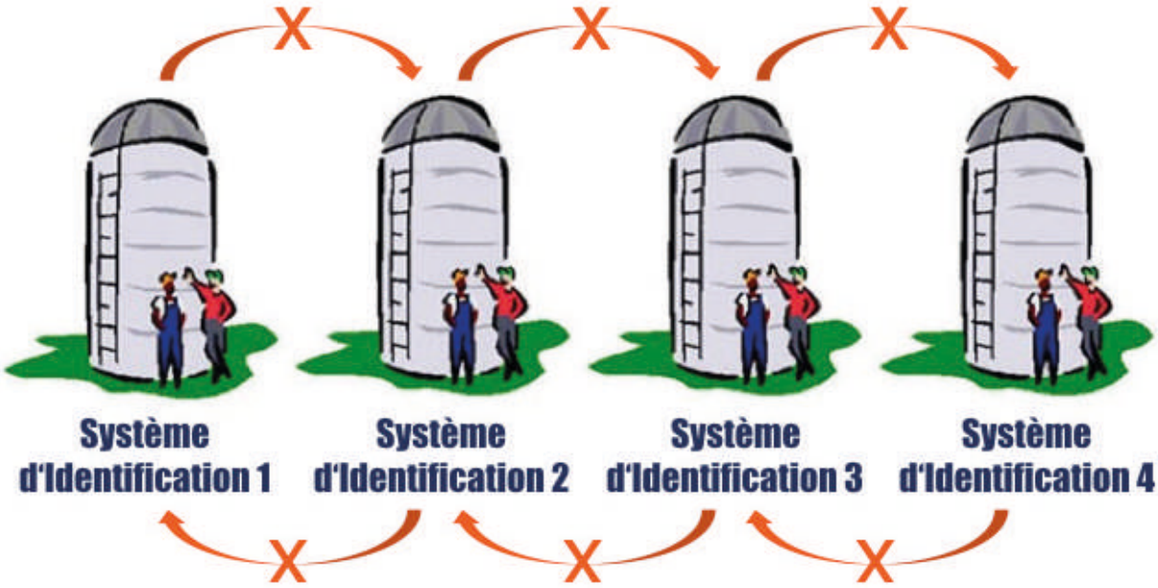


Figure 1 Les silos du système d'identification dominent le paysage actuel des écosystèmes d'identification en Afrique.

La réalité actuelle: Les silos d'identité

En l'absence d'une planification centrale ou de réglementations nationales, il est inévitable que l'écosystème identitaire d'un pays se transforme en silos (Fig. 1), ce qui est le cas dans la plupart des pays africains aujourd'hui où plusieurs systèmes d'identité prolifèrent sans lien entre eux.

> *"Alors que les Silos ont un rôle à jouer en permettant aux organisations de développer des compétences en matière d'identité ou des concepts pilotes, elles représentent finalement un obstacle sur la voie du développement d'un écosystème d'identification performant."*

L'émergence des silos d'identification est le chemin de moindre résistance pour le développement de l'écosystème. Il est plus facile de lancer un programme d'identité autonome, où une agence n'est pas contrainte par une coordination multipartite. Il représente un coût initial inférieur et une adoption plus rapide.

En conséquence, un bon nombre de ces systèmes d'identité se sont développés rapidement et sans forcément fonctionner dans le cadre d'une stratégie nationale d'identification, qui est difficile à adopter étant donné qu'une telle stratégie exigerait une volonté politique au plus haut niveau de faire pression sur les parties prenantes pour travailler ensemble.

En plus de la non-interopérabilité qui existe aujourd'hui, les systèmes eux-mêmes continuent d'avoir une faible couverture de la population, aucun numéro d'identification unique utilisé par tous, aucun modèle d'identité commun et aucun titre d'identité uniformément reconnaissable. Les conséquences sont :

- Grands défis à la prestation de services.
- Haute exclusion et désagrément élevé pour le public.
- Développement entravé (en particulier le secteur bancaire).
- Duplication des efforts et des investissements.
- Réforme du secteur civil entravée.
- Gamme limitée d'applications et de services électroniques disponible.
- Une occasion manquée de mieux servir le public.

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 country:

WORK STREAM	SUGGESTED ACTIONS
Establish the right level of supra-institutional oversight	• 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	• 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	• 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	• 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.

Appel à l'action: Une liste pragmatique

Il est clair que la situation actuelle doit changer. Les parties prenantes de l'identité dans chaque pays africain ont collectivement l'opportunité de rectifier cette situation en travaillant ensemble à l'adoption de politiques et d'actions qui orientent le pays vers l'harmonisation finale. Voici une liste de contrôle pragmatique des actions que les parties prenantes doivent considérer lorsqu'elles s'engagent à réformer les pratiques identitaires dans leur pays:

TÂCHE	ACTION SUGGÉRÉE
Établir le bon niveau d'orientation supra-institutionnelle	• Identifier les parties prenantes dans l'écosystème d'identité dans votre pays et définir leurs rôles et responsabilités. • Former un comité de pilotage technique (CPT), avec des champions représentant chaque partie prenante, rapportant au plus haut niveau politique du pays (la présidence, la primature ou le parlement). Assurer une représentation inclusive sur le CPT. • Habiliter le CPT à prendre des décisions et à prendre des mesures qui auront un impact collectif (par exemple adopter des normes, des modèles de données, etc.) • Le CPT doit être protégé des changements politiques afin d'éviter des perturbations de ses opérations à long terme.
Fixer les objectifs communs ou nationaux	• Un produit livrable important du CST doit être une stratégie nationale d'identification (SNI) qui soit adoptée par tous les intervenants et mise à jour de temps à autre. • Pour éclairer l'opérationnalisation de la SNI, effectuer d'abord un diagnostic de l'écosystème d'identité, y compris l'évaluation de la qualité des données d'identification dans tous les dépôts de tous les secteurs. • Adopter un vocabulaire commun pour la gestion d'identité et harmoniser autant que possible les processus métier qui ont un impact sur l'identité entre les secteurs (par exemple, utiliser le même type de procédure d'inscription). Convenir du modèle de données d'identité, des processus de control et de validation pour l'enregistrement et le traitement des exceptions en cas d'échec d'inscription ou de l'authentification.
Choisir la voie d'harmonisation des données	• Il s'agit d'une étape cruciale et nécessite de faire un choix éclairé sur le chemin à suivre pour l'harmonisation en fonction de ce que vous apprenez du diagnostic (voir les options pour la voie d'harmonisation ci-dessous). • S'assurer que, quelle que soit le chemin d'harmonisation choisi, des dispositions sont prises pour lier l'enregistrement d'état civil (naissance et décès) à l'identification fondatrice afin d'assurer l'intégrité de l'écosystème. • Soutenir le développement des bonnes institutions et des capacités nécessaires pour exécuter le chemin choisi. Rechercher le bon niveau de soutien politique et de financement durable pour assurer le succès.
Mettre en place les cadres juridiques et les politiques nécessaires	• Définir l'identité légale dans votre pays et préciser comment la fournir. • Établir un environnement juridique, réglementaire et d'autorisation favorable (permettant aux agences de saisir des données, etc.). • Adopter une approche basée sur les droits, avec une politique concernant les données inacceptables dans les registres d'identité. • Envisager de rendre le Numéro d'Identification Unique obligatoire pour toutes les interactions sectorielles ; assurez-vous que l'obtention de ce numéro est gratuite pour l'individu. • Adopter la politique de protection des données. • Construire un modèle de risque pour les systèmes d'identification et recommander des garanties à adopter par chaque secteur. • Réaliser des études d'impact sur les femmes et les minorités afin d'affiner la politique des systèmes d'identification pour s'assurer qu'ils sont favorables aux femmes et aux minorités.

Adopt the appropriate credential and solution strategies	• 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	• 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
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 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.

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.

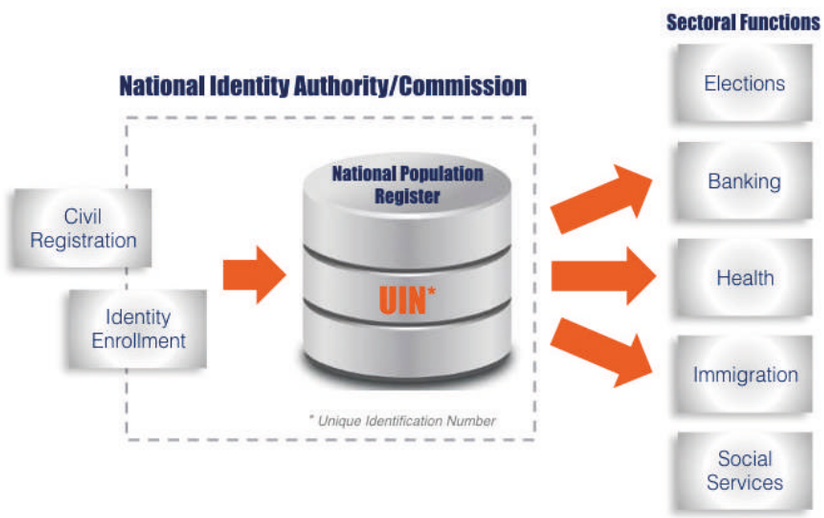


Figure 2 In this pathway, the National Identity Authority takes on a heavy task. It works to ingest civil registration data (birth records) and to enroll the adult population (presumably biometrically) on a continual basis.
The sectoral agencies insist on a UIN in order to identify the enrolles in their funcational databases.
All updates to identity need to be passed by the National Identity Authority. The model has pros and cons.

Adopter des stratégies de solution et des titres appropriées	• Adopter la migration numérique en tant que politique, mais maintenir les références et certificats physiques comme assurance (comme des reçus) contre la manipulation des documents électroniques par le gouvernement. • Permettre à chaque secteur de décider de sa stratégie en matière des titres d'identité, mais rechercher des synergies nationales entre eux (par exemple en créant une imprimerie nationale, ou des titres d'identification partagées, ou un pouvoir d'achat). • Inciter tous les secteurs à adopter une stratégie de solution basée sur des architectures standard ou ouvertes non propriétaires, avec une rentabilité, une interopérabilité, une évolutivité, une fiabilité et une disponibilité intégrées à leurs exigences. • Promouvoir des systèmes durables plutôt que des campagnes ou des solutions exceptionnels et renforcer les institutions et les capacités de gestion de l'identité de manière durable dans chaque secteur.
Promouvoir la transparence	• Encourager toutes les parties prenantes à communiquer avec le public de manière transparente et leur demander d'établir des canaux d'engagement avec la société civile et le grand public pour obtenir des commentaires, des plaintes, des réparations, etc.

Les voies d'harmonisation des données d'identité
Chemin I : Nouveau départ

Dans le cas où l'évaluation révèle qu'il n'y a pas de données de qualité suffisante dans les référentiels sectoriels, alors c'est la voie à suivre. C'est la même voie suivie avec succès en Inde, au Pakistan, en Estonie et au Pérou, pour n'en nommer que quelques-uns.

Dans ce cas, le CPT désigne une institution dans un rôle privilégié, par ex. L'Office Nationale de l'Identification (ONI) ou son équivalent (Fig. 2). L'ONI est chargé de construire et de tenir à jour un registre national de la population (RNP), qui contient les données d'identification de tous les individus dans le pays (citoyens, résidents légaux, réfugiés). Ce registre serait utilisé comme un système de base qui prend en charge tous les besoins fonctionnels de tous les autres parties prenantes sectorielles. L'ONI aurait les tâches suivantes :

- Inscrire l'ensemble de la population en utilisant le modèle de données d'identité national.
- Dédupliquer les enregistrements d'identité.
- Attribuer un numéro identifiant unique (NIU).
- Construire des services d'identité en ligne qui comprennent la vérification et l'identification.

A partir de là, les agences sectorielles relieraient leurs services à l'NIU et utiliseraient les services d'identification en ligne fournis par l'ONI pour vérifier l'identité des demandeurs potentiels de services. Rien n'empêcherait chaque agence d'enrichir les données d'identification avec des informations spécifiques au secteur (KYC: connaître votre client). En Inde, le numéro Aadhaar est maintenant requis pour tous les services gouvernementaux. Ce chemin a des avantages et des inconvénients (voir Tableau 2).

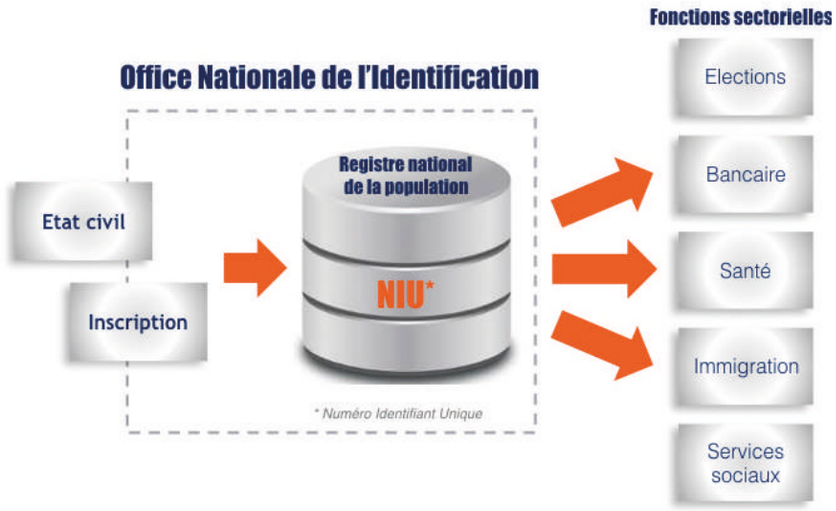


Figure 2 Dans cette voie, l'ONI assume une lourde tâche. Il fonctionne pour ingérer des données d'enregistrement civil (enregistrements de naissance) et pour inscrire la population adulte (avec la biométrie) continuellement.
Les agences sectorielles adoptent le NIU afin d'identifier les inscrits dans leurs bases de données fonctionnelles.
Toutes les mises à jour de l'identité doivent être faites par l'ONI. Ce modèle a des avantages et des inconvénients.

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
• 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	• 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).

Bien sûr, c'est l'occasion de connecter l'enregistrement d'état civil au RNP en s'assurant que les certificats de naissance sont délivrés avec l'NIU qui est généré par l'ONI et qui accompagnera l'individu du berceau à la tombe.

AVANTAGES	INCONVÉNIENTS
• Rentable à long terme. • Investissement à effet de levier: inscription une fois, utilisation en plusieurs reprises (plus facile pour la population). • Il en résulte des données d'identification plus fiables et de meilleure qualité, d'autant plus que les données sont collectées à l'aide de technologies de capture plus récentes et plus avancées qui tendent à donner des données de haute qualité. • Une véritable infrastructure pour le pays. • Pourrait être aligné avec une vision nationale (Estonie, Inde, ...). • Évite l'enregistrement multiple et la redondance. • Prend en charge de nombreux cas d'utilisation et l'innovation. • Fournit des économies d'échelleInconvénients	• Plus difficile à mettre en œuvre. • Prend longtemps pour réaliser son potentiel. Plus lent à lancer, puisqu'il n'est pas piloté par des applications immédiates. • Nécessite une volonté politique soutenue: pourrait être vulnérable aux changements de gouvernement • Nécessite un degré significatif de planification nationale, d'exécution et de centralisation. • Ne tire pas parti des points de contact avec la population détenue par d'autres parties prenantes • Pourrait être potentiellement plus coûteux au départ • Les retours de développement sont réalisés lors de l'utilisation

Tableau 2 Les avantages et inconvénients de la voie d'harmonisation où les données fraîchement saisies sont collectées par l'ONI et sont centralisées et mises à la disposition de tous les organismes sectoriels pour répondre à leurs besoins en matière d'identification fonctionnelle.

Il existe plusieurs variantes de ce modèle, où l'ONI emploie des agents afin de remédier certains des inconvénients inhérents à ce chemin vers l'harmonisation:

VARIANT	DESCRIPTION
Agents d'inscription (Enregistreurs)	Les organisations sectorielles agissent en tant qu'agents de l'ONI pour l'inscription, dit enregistreurs, voir Fig. 3. L'ONI pourrait payer les enregistreurs pour chaque nouvelle identité unique qu'ils soumettent pour l'inscription. Cette option est convaincante si les arrangements institutionnels et financiers appropriés peuvent être établis, car les agences sectorielles disposent généralement déjà d'un nombre important de points de contact avec la population qu'ils peuvent utiliser pour effectuer les inscriptions. Cela peut entraîner des économies de coûts substantielles car elle tire parti des infrastructures existantes et des fonctionnaires déjà employés. Le concept d'enregistreur ne doit pas être limité aux agences sectorielles. Cela pourrait également inclure des entreprises du secteur privé certifiées par l'ONI. L'Inde a montré que ce modèle fonctionne très bien car l'Autorité de l'identité unique de l'Inde a pu inscrire régulièrement 200 millions de personnes par an en utilisant les enregistreurs.
Agents d'attestation d'identité fédérée (AAI)	Les agences sectorielles gardent les données d'identité qu'elles recueillent sous réserve d'un modèle de données d'identité et de normes communes. Leurs données deviennent des bases de données d'identité de référence et ces organisations peuvent agir comme des agents d'attestation d'identité (AAI) de confiance qui se portent garant de l'identité de quelqu'un. Les individus peuvent choisir la banque centrale, une banque commerciale, la commission électorale ou la base de données de la carte d'identité nationale, etc., comme AAI. Le rôle de l'ONI est de fédérer tous ces référentiels. Selon les attestations des AAI, l'ONI peut attribuer des NIUs aux personnes et s'assurer qu'une personne ne reçoit qu'un seul numéro, même s'il peut être présent dans plusieurs bases de données de l'AAIs. Ce modèle de déduplication fédérée peut fonctionner techniquement mais il est plus complexe à implémenter dans le contexte du développement. Il est plus approprié dans les pays développés (par exemple Gov.uk Verify).

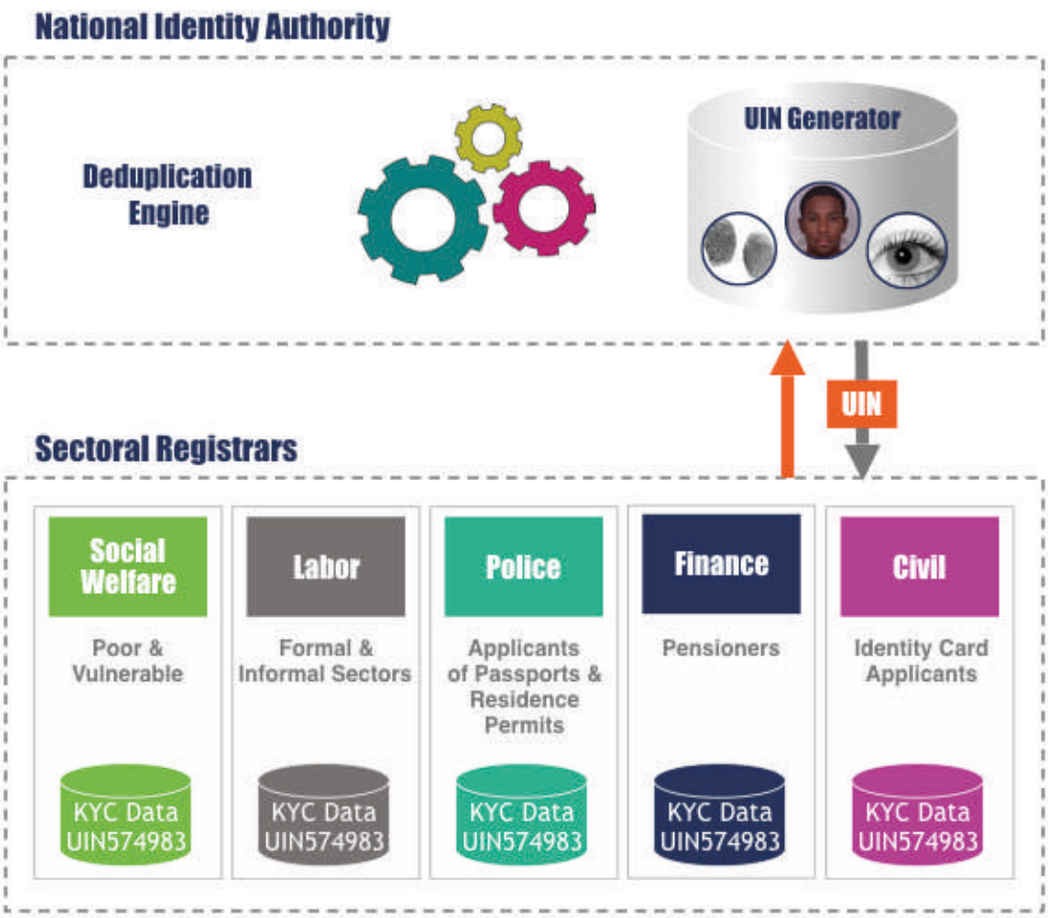


Figure 3 The Registrars: the enrollment could be sped up by leveraging the infrastructure of other organizations such as sectoral agencies or private sector, that act as registrars. NIDA maintains the back-end national identity database, deduplicates records, issues the UIN and provides online identity services that can be tapped by the sectoral agencies in order to seed their Know Your Customer (KYC) databases with the UIN.

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.

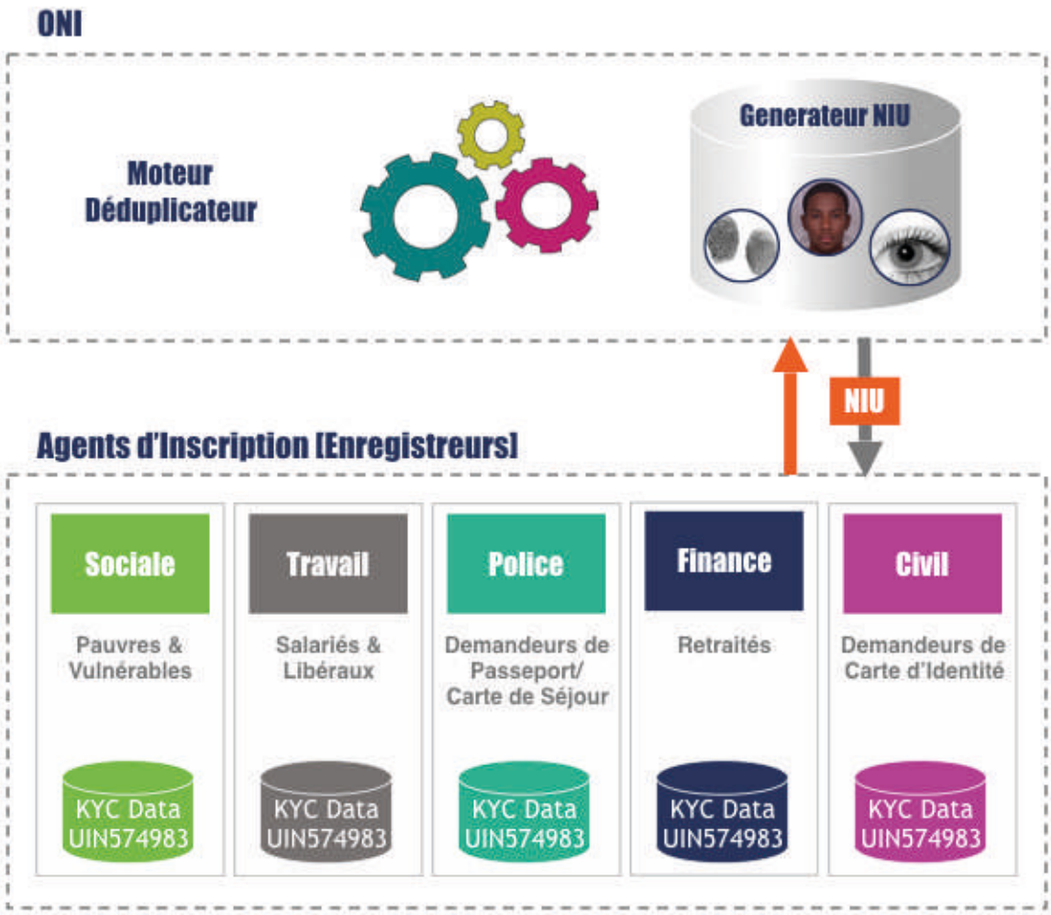


Figure 3 Les enregistreurs : l'inscription pourrait être accélérée en exploitant l'infrastructure d'autres organisations telles que les agences sectorielles ou le secteur privé, qui agissent en tant que agents d'enregistrement. L'ONI gère la base de données d'identité nationale, déduplique les enregistrements, émet l'NIU et fournit des services d'identité en ligne qui peuvent être exploités par les agences sectorielles afin de créer leurs bases de données Know Your Customer (KYC) liées au NIU.

Chemin II: Réutillisation des données existantes

Si l'évaluation menée par le CPT révèle des bases des données existantes précieuses, une analyse coûts-avantages devrait alors être effectuée pour déterminer s'il est économiquement logique de réutiliser ces données (voir Fig. 4). Ceci est un exercice d'intégration de bases de données qui n'est pas trivial mais qui est faisable en utilisant les bonnes technologies. Il s'agit d'établir une correspondance entre les mêmes identités dans différentes bases de données, même lorsque les modèles de données d'identité sont différents et la qualité des données n'est pas uniforme. Certains de ce qui est impliqué peuvent inclure :

- Utiliser les technologies de résolution des entités pour permettre d'établir des correspondances entre des enregistrements entre différentes bases de données.
- Mise en œuvre des dernières versions des systèmes d'identification biométrique automatisés (ABIS) permettant de faire correspondre des échantillons de données biométriques partiels, imparfaits ou de faible qualité. Au fil des ans, la technologie de correspondance biométrique s'est considérablement améliorée, ce qui signifie que les chances de découvrir des liens fiables sont plus élevées aujourd'hui qu'il y a cinq ans. La qualité des données reste le facteur le plus critique du succès.
- Dans la pratique, la voie choisie sera un hybride des chemins I et II où certaines données de haute qualité sont réutilisables alors que pour le reste, un nouveau départ serait nécessaire.
- Il ne suffit pas d'harmoniser à un moment donné, il faut synchroniser de façon continue. Pour ce faire, les agences sectorielles doivent s'engager à utiliser systématiquement le NIU et à reléguer toutes les mises à jour des données d'identité à l'ONI.

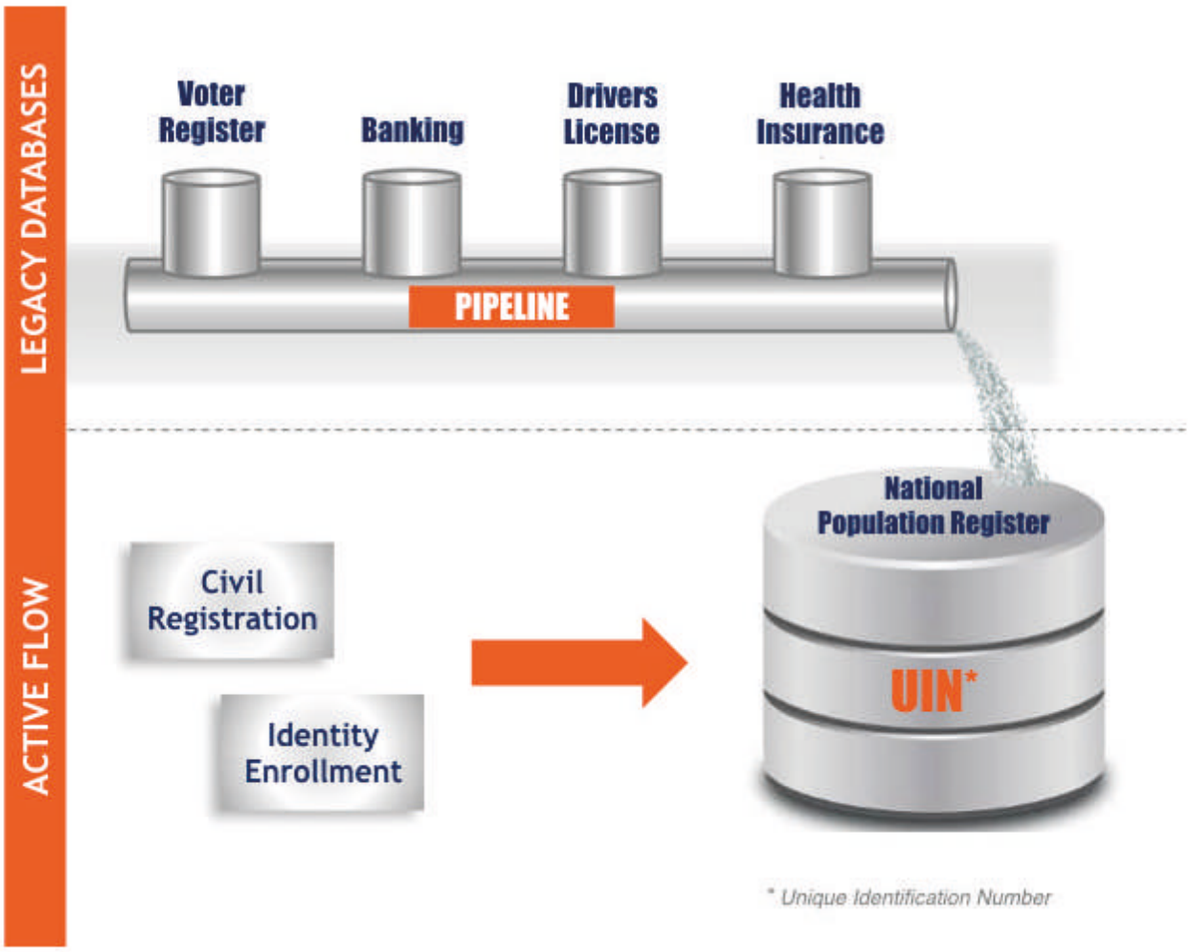


Figure 4 Harmonization of legacy databases requires a parallel exercise to civil registration and ID enrollment where the databases are consolidated, and correspondences are established using entity resolution technology before a UIN is assigned. This is a fruitful exercise only if the legacy data has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

No matter what steps are taken, it is important that identity systems developed in Africa from here on 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.

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.

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. ☒

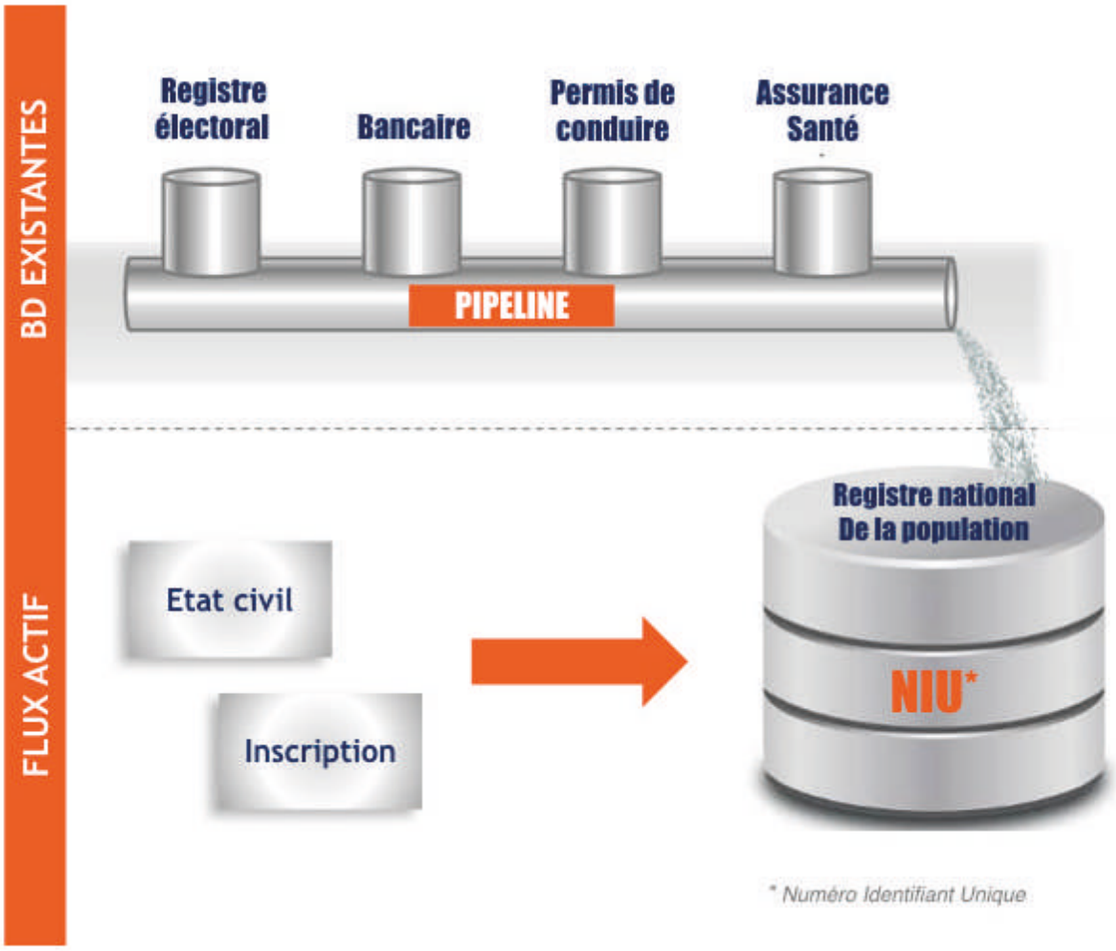


Figure 4 L'harmonisation des bases de données existantes nécessite un exercice parallèle aux enregistrements de l'état civil et les inscriptions ID où les bases de données sont consolidées et les correspondances établies à l'aide de la technologie de résolution d'entité avant l'attribution du NIU. Ceci est un exercice fructueux seulement si les données existantes ont une qualité suffisante.

Conclusions

Alors que la voie de l'harmonisation de l'écosystème identitaire dans un pays dépend des actifs identitaires et des schémas factuels propres à un pays, la plupart des pays africains, à notre avis, sont mieux servis en choisissant le premier chemin, le nouveau départ. Cela devrait s'accompagner d'une législation imposant l'utilisation du NIU pour les processus opérationnels du plus grand nombre possible d'agences sectorielles. Nous recommandons également l'utilisation de bureaux d'enregistrement (enregistreur) pour accélérer la couverture complète, ce qui devrait être l'un des principaux objectifs de toute réforme.

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.

Quelles que soient les mesures prises, il est important que les systèmes d'identité développés en Afrique respectent les normes internationales. Cela protège l'investissement du pays en évitant le verrouillage des fournisseurs et en permettant plus de flexibilité afin de répondre à tous les besoins futurs et en constante évolution. Aujourd'hui, le paysage des normes qui ont un impact

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.

sur les systèmes d'identité est très développé, comme le montre le Tableau 3. Naviguer dans cette tapisserie nécessite l'avis d'experts compétents dans le domaine des normes ISO. Nous recommandons que le comité de pilotage technique retienne les bons consultants pour cette tâche et insiste sur le fait que tout achat dans le pays doit inclure les normes applicables dans les documents de passation de marchés ou de demandes de propositions. ☒

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 **Authentication** • ISO/IEC 24761 Authentication Context for Biometrics • ISO/IEC 29115 Entity Authentication Assurance Framework	**Credential standards** • 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	

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.

Interopérabilité des dispositifs de capture ISO/IEC 19784 (BioAPI)	**Normes de données biométriques** ISO/IEC 19794 (formats d'image et de template)	**Emballage des données biométriques (CBEFF)** ISO/IEC 19785 (CBEFF = Common Biometric Exchange Format Framework - fournit une structure, des métadonnées et une sécurité communes)metadata & security)
Qualité d'échantillon biométrique ISO/IEC 29794 **Authentification** • ISO/IEC 24761 : Contexte d'authentification pour la biométrie • ISO/IEC 29115 : Cadre d'assurance de l'authentification des entités	**Normes pour les titres d'identité** • ISO/IEC 7810 to 7813 : Normes de cartes d'identité • ISO/IEC 7816 : Normes de eIDs, cartes à puce, cartes de contact • ISO/IEC 14443 : Normes de cartes sans contact • ISO/IEC 8583 : Normes pour les cartes de paiement à bande magnétique • ICAO 9303 : Normes relatives aux documents de voyage lisibles à la machine (DVLM) • Norme EMV pour les cartes de paiement (CAP-MS, DPA-Visa, EuroPay) • Spécification CEDEAO	

Tableau 3 La mosaïque complexe des normes qui doivent être respectées pour assurer un écosystème d'identité sain et harmonisé non seulement à un moment donné, mais pour toujours.

PrimeKey *secures* Malawi's FIRST *EVER* NATIONAL ID cards

By Karin Trogstam, PrimeKey

☐ Malawi has just completed registration of 9.1 million Malawians aged 16 years and above. By March 2018 all registered will have a National Identity Card. As of late 2017 Malawians were able to collect, for the first time, their very own national ID card. The ID cards are secured with digital signatures issued by SignServer and certificates from EJBCA, both products by PrimeKey.

The result is that not only can Malawians get their own ID card but also that these cards are safe from copying and tampering.

Every Malawian will get their ID on a smart card, containing their personal information. With security a top priority for the smart cards, PrimeKey has installed a Country Signing Certificate Authority (CSCA) and a Document Signer for Malawi, providing digital signatures to the millions of individual Smart Cards. This ensures that the ID of each citizen is kept secure.

The national ID initiative is founded by UNDP Malawi and delivered by SELP, in cooperation with PrimeKey. With national ID cards Malawians will no longer have problems identifying themselves to banks or other institutions, making life easier for citizens, institutions, and the government. The project is being rolled out nationally and is currently discussed on twitter under the hashtag #mymalawiID.

Chris Job, Team Leader Professional Services, who installed the PrimeKey products on site commented, "It was great to see how engaged the citizens of Malawi were in getting their first national ID card. Even farmers who lived in remote areas without electricity were motivated to go and get enrolled, which I think proves just how important this project is. It's a big step for both Malawi as a country and for its citizens and I'm happy PrimeKey could be a vital part of it." ☒

Further information can be found at www.primekey.com

"Integrity Guard" – PROVEN *security* for the *NEXT* DECADE

By Steve Atkins, Program Director, The Silicon Trust

A security chip must be able to store security-critical data – for example keys, personal data or biometric information – and be able to protect the system in a wide range of totally different application fields. Until now, companies have focused on protecting on-chip data from criminal attack by concealing it. Sensors have been used to recognize such attacks and to protect sensitive data from consequent manipulation. However these methods no longer meet the very high security requirements that exist today.

Back in 2008, to protect data more effectively, Infineon developed a completely new approach to security with "Integrity Guard". This now proven technology is based on digital security and displays two revolutionary innovations. Infineon engineers have succeeded in creating a security technology that not only encrypts the data on the security controller but can also process the data while it is encrypted. Even if malicious attackers "eavesdrop" on the data signals, they only receive encrypted, and therefore incomprehensible, information.

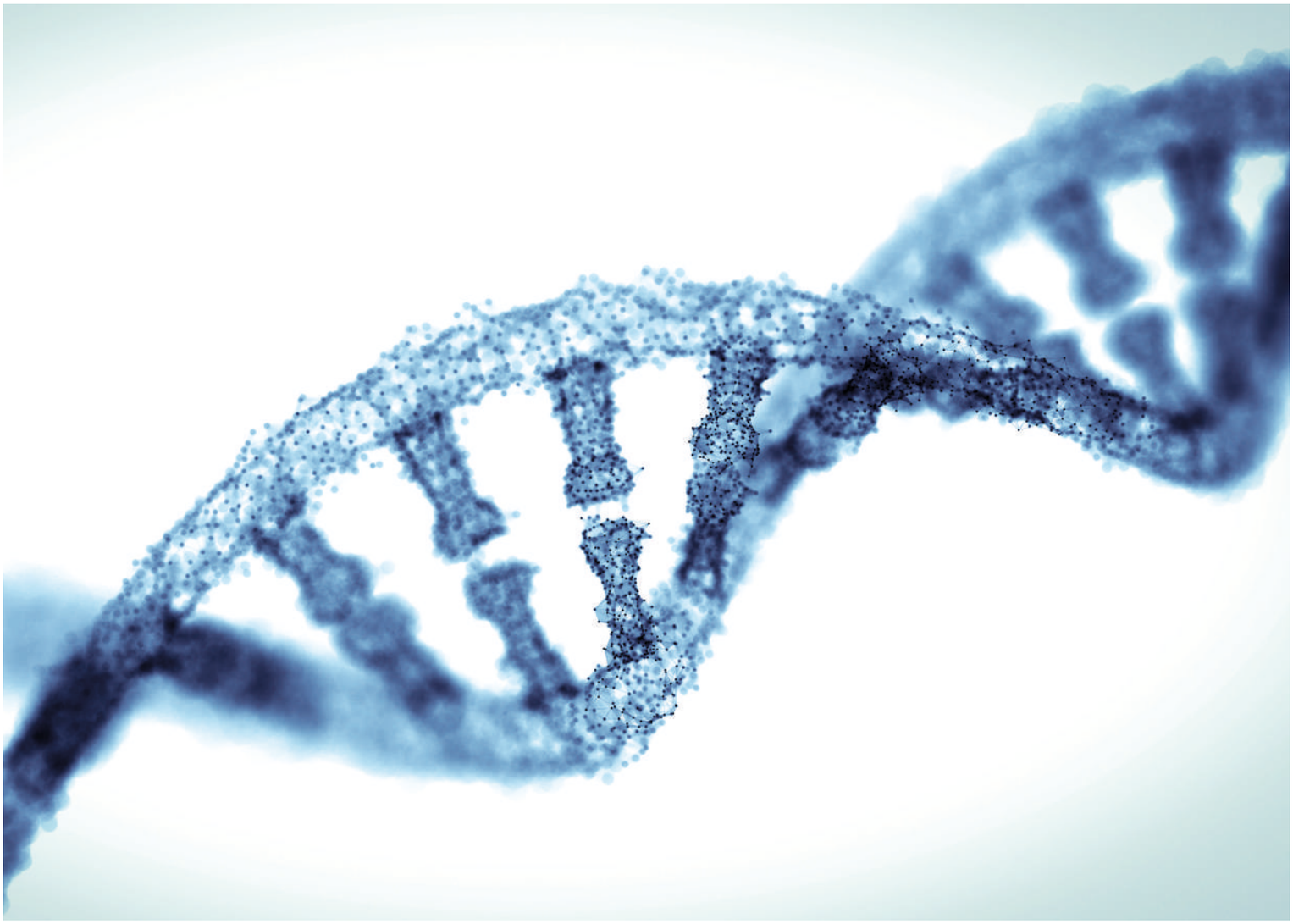
"Integrity Guard" is a security technology that has been inspired by the information storage and information processing of a living cell; the actual inspiration for the concept was the double helix of a human cell. The idea behind it is simple enough - every biological cell is comparable to a "secure computer" that must safely store and process genetic information.

The technical realization of this innovation equips controllers with robust digital mechanisms to protect secure data and to monitor security conditions. Utilizing the "Integrity Guard", the controller reacts autonomously on security threats. At the core of this self-checking design is a double CPU that performs a continuous self-check of all operations. This self-checking actually results in 'integrity protection' – hence the name "Integrity Guard".

Another key element of"Integrity Guard" is the comprehensive encryption over the whole data path, leaving no plaintext on the chip.

"Integrity Guard" encryption goes much further than conventional concepts and for the first time in chip card history even calculates with encrypted numbers in the CPU itself.

In addition to the complete encryption of the entire data path (CPUs, memories, caches and buses), these high security controllers have two CPUs and a refined error-detection system. The two units continually monitor each other, and should a unit detect that an operation has not been properly executed due to a criminal attack, it initiates the corresponding countermeasures. In this case, the chip immediately stops the ongoing processes and triggers an alarm. This makes it possible to ward off the most varied kinds of attacks.



New Digital Security features

Thanks to the totally new scope of their digital security features, controllers with “Integrity Guard” meet very high security requirements. Their robust design overcomes the disadvantages of analog security technologies. Full on-chip encryption, including encrypted calculation in the CPU itself and full error-detection capabilities over the complete core architecture provides the basis for the efficient protection of sensitive data against external attacks.

Full Error detection

“Integrity Guard” security chips are the first of their kind to be equipped with a full error detection capability for the complete data path. A dual CPU approach allows error detection even while processing – the CPUs constantly check each other to establish whether the other unit is functioning correctly. Relevant attack scenarios can be detected, whereas things that would not lead to an error are more or less ignored. Thus the risk of false alarms – a significant disadvantage in conventional solution concepts – is significantly reduced. The approach includes error detection and correction throughout the entire system.

Total encryption

The security controllers with Infineon’s “Integrity Guard” are equipped with full encryption over the complete CPU core and the memories – meaning no more plain data is left on the chip. It is the first time ever in commercial security controllers that the two CPUs have utilized fully hardware-encrypted calculation, and with different dynamic secret keys. This process is only possible because Infineon, which allows the integration of real encrypted operations, has implemented the CPUs from scratch.

Signal protection

In signal protection, the main objective is to reduce to the minimum the attractiveness of the signals for the attacker. This is done by means of full encryption. Attackers can neither manipulate nor eavesdrop on encrypted signals. Never the less, in every chip there are signals that are more important than others, so an Infineon-specific shielding, combined with secure wiring, has been developed. With this method, first all the signals are classified according to their value for the attacker. In a second step, during the design of the chip, the more interesting signals are automatically routed under less valuable lines. Subsequently, an intelligent shielding algorithm finishes the upper layers, completing the so-called I2-shield (Intelligent Implicit shield).

Towards durable security

For the challenges on the path toward durable and lasting security, a professional approach is necessary in order to evaluate the future of attacks and suitable countermeasures. When developing new product families, the planned and anticipated lifetime needs to be kept in mind. As is the case for electronic passport chips, there is often a span of ten to fifteen years between the design and end of the product's lifetime in the field.

Infineon's own security laboratories therefore focus on researching what will appear next in terms of known or even completely new attack scenarios. Localised attack methods aim at finding secret keys in the very heart of a chip – the CPU. Unencrypted CPUs make access to sensitive data easier; they can be analysed by an attacker using today's state-of-the-art methods, such as optical emission analysis or electromagnetic emanation attacks. It has been shown that conventional, scenario-specific countermeasures not only drive the cost spiral upwards, and lead to tedious security updates, but also no longer serve the requirements of applications with a high security demand.

The advantages of "Integrity Guard"

"Integrity Guard" offers a multitude of important advantages, which fully pay off in the development of secure products.

Customer-friendly security

Today, providing top-level security often means investing great effort and high costs – not only for the chip manufacturer, but also for the Operating System and application SW developers. Adding security often decreases flexibility in conventional applications or is even decreasing the performance. In Infineon's security controllers with "Integrity Guard" technology, almost all security features are automated. Infineon theorizes that because of this self-checking (automated) feature there is approximately 30% less development time taken due to less coding requirements. Once again reducing total cost of ownership.

"Customer-friendly security" means that security features are easy to use and ensure confidence along the entire value chain – from chip manufacturer and chip card manufacturer to system integrators and the customer. This customer-friendly security results in significantly lower overall costs over the product life cycle.

Designing with Integrity Guard for a secure solution reduces total cost of ownership through R&D efficiency for application development and so ensuring a shorter time to market for end customer products. Its open architecture will also accommodate future hardware extensions leaving room for expansion of products and their product life spans.

Thanks to their robust design, security chips with "Integrity Guard" technology can also be used in difficult and demanding environments. Their digital features neither have to be adjusted nor calibrated, which makes the chips even more resistant. Conditions that do not directly harm the chip itself will therefore not affect its correct functioning.

Mathematically modelled security

Error-detection codes and digital security features can be mathematically modelled. This facilitates the security evaluation and certification both internally and when performed by third parties.

Self-checking security

Security chips with "Integrity Guard" have self-controlling security mechanisms. The most important element is the comprehensive digital error detection over the complete core architecture, including memories, buses, caches, and the dual CPU.

Attack-repellent

The design of the security chips alone impedes attacks. Full encryption is used for CPU, memories, and buses, covering all stored, processed, and transferred data. These mechanisms are automated and facilitate the software implementation and use.

Accreditation and testing

Integrity Guard security technology has been evaluated by the accredited and internationally recognized TÜViT testing and certification authority.

The Federal Office for Information Security (BSI) confirmed the high security of Infineon's "Integrity Guard"-based security chips according to "Common Criteria", the internationally recognized standard for the rigorous assessment and certification of security chips. Furthermore, the security controller meets the security requirements for payment cards from EMVCo (Europay, Mastercard, Visa). More than 20 Common Criteria EAL 6+ Certificates, maintenance certificates or reassessments for security controllers based on Integrity Guard have been achieved

“Integrity Guard” is one of the world’s most advanced technologies for delivering a particularly high level of long- lasting protection for the data on chip cards.

“Integrity Guard” in end applications

Infineon´s security technology was developed for applications that require particularly high-level data security and resilience for a particularly long term of life. Important application fields for security controllers with “Integrity Guard” include governmental identification documents as well as banking and credit cards. In these fields “Integrity Guard” already today sets the technological standard for chip-based security.

Security controllers are also used increasingly in numerous networked systems such as computers, IT infrastructures, and industrial control systems as well as critical infrastructure systems such as smart grids – where “Integrity Guard” provides the basis for overall system security.

In Germany, “Integrity Guard”-based security chips are, for example, used in the electronic identity and healthcare cards as well as for contactless payment applications like the German Banking Industry Committee’s (Deutsche Kreditwirtschaft) “girocard kontaktlos” project. This project is currently one of Europe’s biggest contactless EMV payment projects.

“Integrity Guard” is one of the world’s most advanced technologies for delivering a particularly high level of long-lasting protection for the data on chip cards. Examples of the data involved in the German eHealth card with six-year validity are the insured person’s name, date of birth, gender and address as well as insurance number and insurance status. As with all “Integrity Guard”-based security microcontrollers, the data on the eHealth card is not only stored in encrypted form but also processed in encrypted form.

The inclusion of secure controllers using “Integrity Guard” means that the eHealth card is already equipped for additional applications that further raise the quality of patient care and the efficiency of treatment. With the insurance holder’s consent, additional personal data can be stored on the card, such as emergency data, essential medication, allergies, drug intolerance or indication of pregnancy.

Infineon has been supplying “Integrity Guard” technology within their family of SLE 78 security microcontrollers for the German eHealth card since 2011 and continues to supply the majority of German eHealth microcontrollers.

Infineon is the only semiconductor manufacture to supply chips to ten of the currently eleven national health card projects in Europe. Apart from German e-health cards, Infineon’s chips are also to be found in the e-health cards of Austria, Belgium, Great Britain (without Ireland), Italy, Poland, Portugal, Slovenia, Spain and Switzerland. Infineon is the global market leader in security chips for e-health cards with a 60% market share.

The security technology “Integrity Guard” deployed in the eHealth card has received multiple technological innovation awards. It won the German Industry’s Innovation Award 2010 and the security industry’s “Sesame Award” 2008 and was nominated for the “Deutscher Zukunftspreis 2012” – the German Federal President’s Award for Innovation and Technology.

“Integrity Guard” puts forward indispensable hardware security features that cannot be implemented effectively in software and gives software providers an efficient environment for truly secure, performance and feature rich applications.

Infineon will have sold more than 1.500.000.000 Mio pieces of “Integrity Guard” products by the end of March 2018.“ ☒

HIGH-END *machines* and *PRODUCTION technology* for OPERATIONAL *EXCELLENCE*

By Dirk Melzer, Melzer maschinenbau

Customers worldwide rely on MELZER's customised, high-quality production equipment 'Made in Germany'.

For more than 60 years, MELZER maschinenbau has been successfully producing customised machines and production equipment, including processing systems for smart products such as smart labels, plastic cards, e-Government solutions, and special products and labels, as well as ID cards, contactless cards, and RFID inlays. Users benefit from patented machine technology, modular processing systems, and pre-selection for the optimisation of production processes.

High quality production equipment that functions for decades

Customers around the world rely on individual solutions in combination with the unique modular design that produces high-quality products for the pharmaceutical, automotive, telecommunication, microelectronic, public transport, and printing industry. MELZER offer high quality, support, and a steady availability of spare parts for the entire life cycle of the machine – regardless how long the machines are in production.

International success with customised solutions

Being a third generation family business, MELZER develops individual production solutions together with their customers. Every machine for the production of ID documents, smart tickets, smart labels, and RFID technology is customised and exclusively 'Made in Germany'.

The MELZER specialists produce everything in-house: mechanical parts, control cabinets and software. MELZER is especially successful internationally with its innovative solutions. Long-term sales partners guarantee fast and reliable local service, and assure a continuously increasing number of satisfied customers, for example in Asia, many RFID apparel tags for the textile industry are produced with MELZER machines. Quality consciousness is growing in China, where price had been the primary concern until now. The label 'Made in Germany' is still reputable, and the machines are considered reliable, durable and economically advantageous.

Patented machine technology and pre-selection optimise production processes

MELZER uses a patented transponder selection before applying the transponder to the substrate. In mere fractions of a second, a defective transponder is being removed from the production process and replaced by a working transponder immediately. The method does not only save time and materials – it also ensures continuous product reliability. Luggage tags or endless badges, where subsequent replacement of defective products is not possible, are processed fully automated on just one machine.

MELZER developed a pioneering solution for RFID chip pre-selection. Chips are separated and tested individually, allowing the rejection of faulty units. This automatic selection

process is patented, creating a USP that saves customers money. Chips are steadily becoming more reliable, but the error rates are not yet low enough to produce without a preliminary control. Once processed, chips cannot be removed or replaced. If a manufacturer opts against pre-selection, they will have to throw away a certain percentage of the final product.

The modular design of the SL-600 enables customization as well as the future integration of new modules and functions. With a maximum of 60,000 products per hour, the Melzer MELZER SL-600 manufactures high-quality products through the worldwide patented in-line selection technology.

High volumes of up to 60,000 labels per hour

MELZER offers high-end customised machines and production equipment for RFID inlays, smart labels, ID cards, e-Government solutions, and many more applications. Customers can select from different machine options:

- The SL-1 with up to 7,000 labels per hour is well suited as an entry-level model, offering high flexibility at low investment costs, as well as the patented selection system.
- With up to 10,000 RFID labels per hour, the SL-100 is the 1-track solution.
- The multi-lane version SL-400 is well suited for the ecomonic production of large volumes of up to 40,000 RFID labels per hour. Both systems are also available as the ticket versions ST-100 and ST-400, respectively, for the production of RFID tickets or other non- adhesive products. The combination of label and ticket production is also available as single and multi-lane versions.
- With a maximum of 60,000 labels per hour, the MELZER SL-600 manufactures high-quality products. The SL-600 also offers production options for miniaturized transponders. The parallel processing of six transponder tracks creates a high production output.

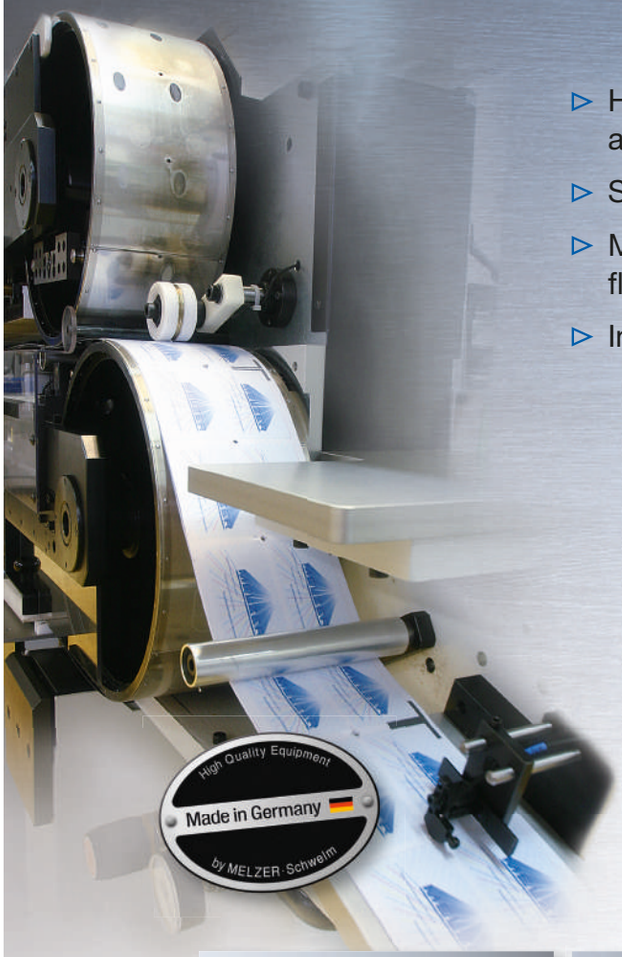
High –end and fully automated production line for ID document

Leading machine manufacturer for secure ID documents

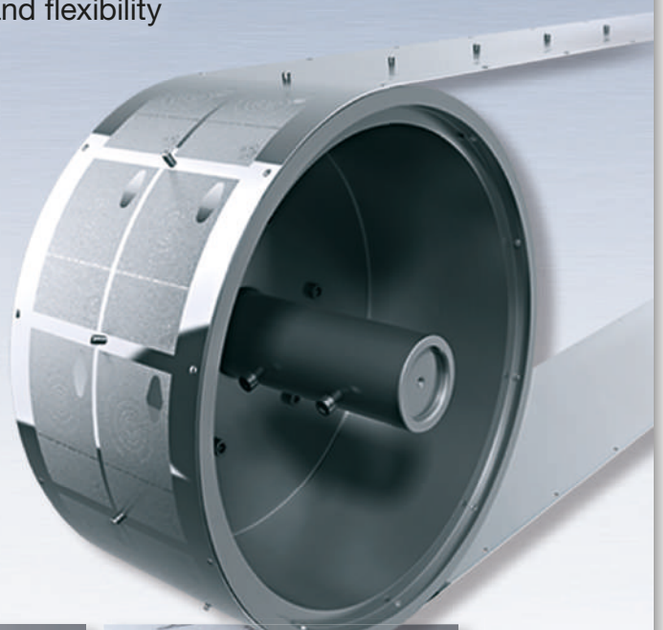
The company has turned into the leading machine manufacturer for ID and passport datapage production equipment. Production of modern credentials poses unique challenges. It includes security features such as RFID transponders, polycarbonate material, DOVIDs, transparent windows, any kind of security threads, and numerous others. These features have to be integrated into the fully automated production process – reliably, in a forgery-proof manner, and very precisely. There is a sizeable need for secure documents in order to reduce the risk of misuse and forgery. In the last ten years, the standard for secure documents has risen, and it will continue to rise. Countries all over the world wish to produce their own document instead of relying on foreign governments or companies. The MELZER modular platform enables clients to continue using this solution when they need to integrate a new security feature. The material cost of a modern biometric passport is several Euros. The reject rate is around one percent, compared to two-digit reject rates for other manufacturing processes. This means a quick ROI for the document manufacturer. ☒

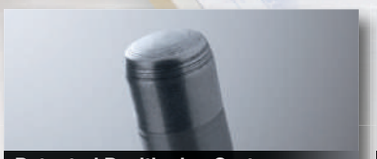
Also based on the modular system, Melzer offers the M4 line for inlay production either ID-1 or ID-3 including cover lamination based on etched, wire or printed antenna types.

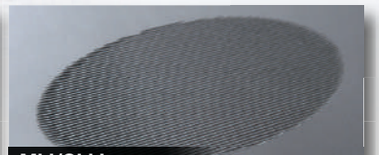
Lamination Technology for ID Documents with Security Features



- Highest automation level for maximum accuracy, security and yield rates
- Shortest lamination times
- Minimum demand of operators, floor space and energy
- Inline efficiency and flexibility

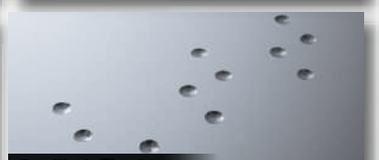


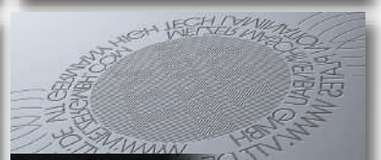

Patented Positioning System


MLI/CLI Lenses


Micro Lettering


Inlaying and raised Structures


Braille Lettering


Latent Image

INNOVATIVE MACHINERY SOLUTIONS SINCE 1956

MELZER®

Please visit us at: SDW · London, United Kingdom · Booth L27 | **14th ICAO TRIP Symposium and Exhibition** · Montreal, Canada | **TRUSTECH** · Cannes, France **more** ▷

www.melzergmbh.com

Turning the ECOWAS ID card *from* VISION to *REALITY*

By Markus Hoffmeister, cryptovision GmbH

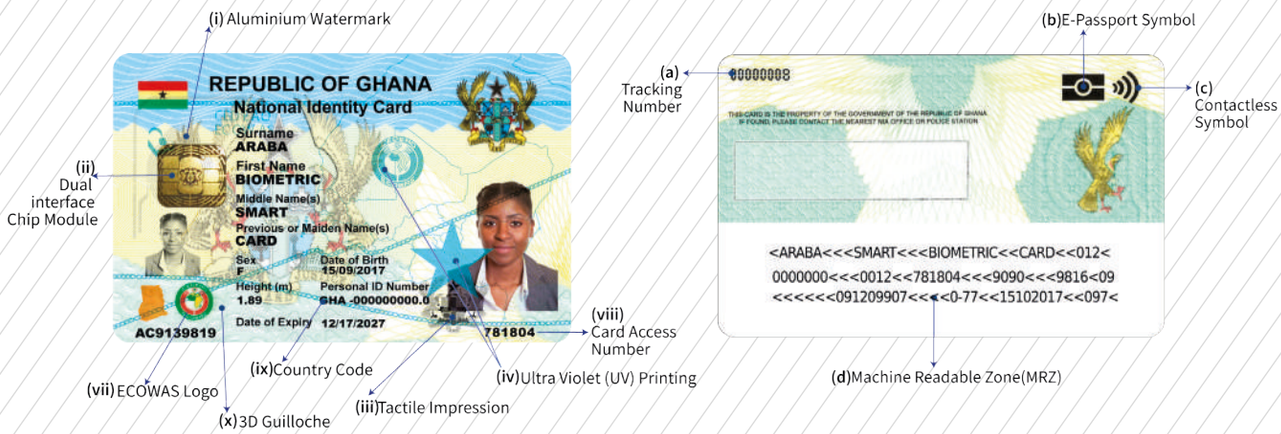
For many years, we have worked with our clients across the African continent with the aim to bring secure ID systems to the African people. Combining cryptovision's experience with European technical and regulatory standards and our customers' understanding of local requirements has been the basis of many successful projects in the region. When the Economic Community of Western Africa (ECOWAS) decided to implement a unique ID card for all its member states' citizens, cryptovision realized the huge opportunity this presented. It is because of our understanding of the European interoperability efforts, that we see the enormous relevance of the ECOWAS ID card standard for our clients in West Africa, such as Ghana and Nigeria.

☐ A West African Identification System

What is the scope of the ECOWAS ID card? It is designed to provide the maximum protection against fraud and identity theft while offering interoperability with the various national systems. The Economic Community of Western Africa (ECOWAS) consists of 15 countries whose aim it is, to promote economic and political cooperation, abolish trade restrictions, remove obstacles to the free movement of people, goods and services and the achieve harmonization between the regional policies of the member States. Passport-free travel is a complex vision and, within the ECOWAS, concerns a population of more than 300 million, a surface area of more than 5 million square kilometres, 5300 km of Atlantic coastline and 12 member states with ocean access.

Interoperability of national ID schemes is key

The nature of any national ID scheme is exactly that – its national. However, insufficient cross-border interoperability prevents citizens and businesses from benefitting from Economic Communities, such as ECOWAS. In the European Economic Area, national identity cards are issued to their citizens by the governments of all European Union members except Denmark, Ireland and the UK. Citizens holding a national identity card cannot only use it as an identification card in their home country, but also as an ICAO-standardized travel document to exercise the right of free movement in the EAA. Already in 2006, all European Union member states agreed to implement common design and minimum security standards for their perspective national ID cards, such as the size, material, ICAO-specified and machine readable biographical data as well as compliance of the electronic ID functionality with the ISO / IEC standard 144443..



Among the first ECOWAS BIC documents issued – GhanaCard

As a key vendor to the Ghanaian prime contractor Identity Management Systems (IMS), a subsidiary of Margins Group, cryptovision delivered critical components for the project, including the applications on the eID card, the backend certificate infrastructure, and middleware components used at the card issuance terminals.

The Ghanaian government has ambitious goals to issue a total of 16 million eIDs to its citizens within 12 months. The GhanaCard is a multi-application document. In addition to the primary function of identity verification, it also serves as a passport equivalent for travel within the ECOWAS sub region. Furthermore, it will enable strong two-factor authentication as a password replacement for eGovernment services online and can be used for digital signature of electronic documents. It is also suitable for financial transactions, as the plan is to enable citizens to activate the payment application after card issuance.

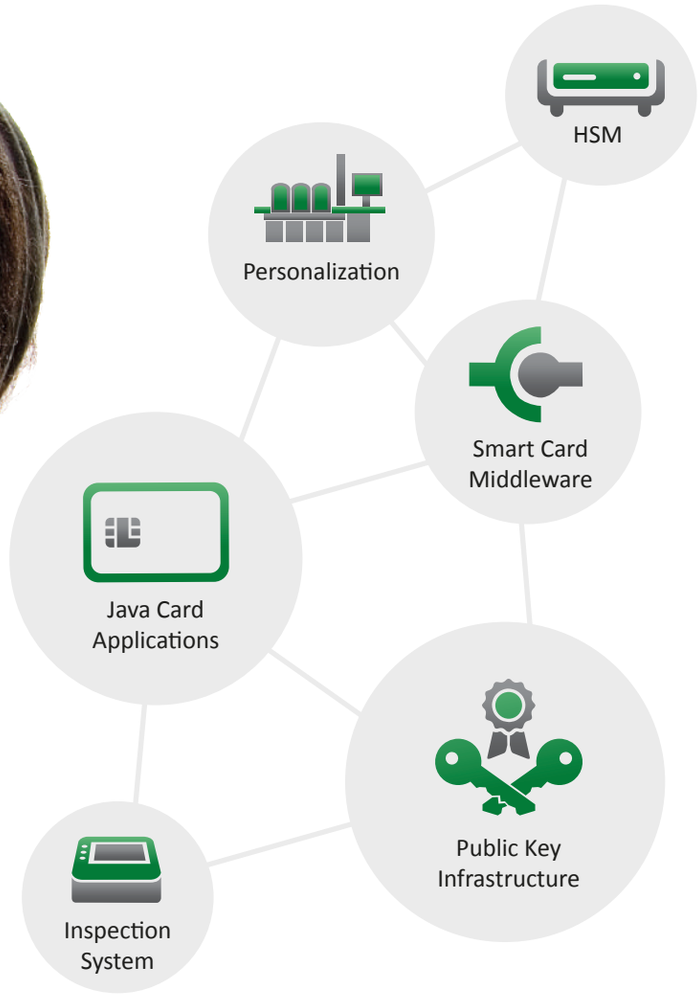
"GhanaCard card also functions as a biometric travel document that will allow holders to travel freely within in more than dozen West African countries"

To ensure the security of the GhanaCard and its infrastructure, the Ghanaian government rely on technology provided by cryptovision: For the functions on the card and also the Public Key Infrastructure (PKI), as well as the token based access to the PKI. The GhanaCard PKI, which is designed for 16 million certificate holders, ranks among the most advanced certificate management systems worldwide – incorporating several certification authorities (CAs) and multiple certificates on each card.

In terms of document security, Ghana Card is one of the few eID documents outside of the EU to feature a card verifiable, certificate-based PKI. Leveraging EAC and SAC provides one of the most secure eID documents in Africa, while still providing a simple method to access card information via the CAN. The government of Ghana is planning to use the same chip platform and ePasslet for other documents, like an electronic passport and the electronic driving license. ☒

cryptoVision

We create your eID Solution



Flexible eID solutions for enterprise and government

www.cryptovision.com

INTRODUCING THE SILICON TRUST

THE SILICON TRUST

THE INDUSTRY'S PREMIER SILICON BASED SECURITY PARTNER PROGRAM

The Silicon Trust is a well-established marketing program for smart card solutions with high visibility in the worldwide government and identification (ID) markets. With over 30 companies along the value chain, the Silicon Trust forms a strong community of likeminded companies.

THE SILICON TRUST PROGRAM FOCUSES PRIMARILY ON:

- Educating government decision makers about technical possibilities of ID systems and solutions
- Development and implementation of marketing material and educational events
- Bringing together leading players from the public and private sectors with industry and government decision makers
- Identifying the latest ID projects, programs and technical trends

EXECUTIVE COUNCIL

The Executive Council has been the steering committee of the Silicon Trust since 2008. It drives the Silicon Trust by defining the topics and directions of the program's publications, workshops and meetings.

ADVISORY BOARD

The Silicon Trust Advisory Board supports the Executive Council in defining the direction of the program in terms of public policy and scientific relevance.

SILICON TRUST PARTNERS

Partners of the Silicon Trust are a vital element of the program. The partners represent all aspects of the value chain and are international representatives of the ID industry. They all share one common goal – to create awareness, to educate and to promote the need for silicon-based security technologies.

THE 4TH ANNUAL MEETING OF THE ID4AFRICA MOVEMENT

Harmonization of Identity Schemes

Be A Part of the World's Fastest Growing Identity Marketplace

Organized by

ID4AFRICA

Hosted by

National Identity Management Commission

Platinum Sponsors

zetes
ALWAYS A GOOD ID

PWPW
POLISH SECURITY PRINTING WORKS

Premier Sponsor

IDEMIA
augmented identity

Gold Sponsor

HID

Silver Sponsors

gemalto
security to be free

GEN KEY
Identity for all

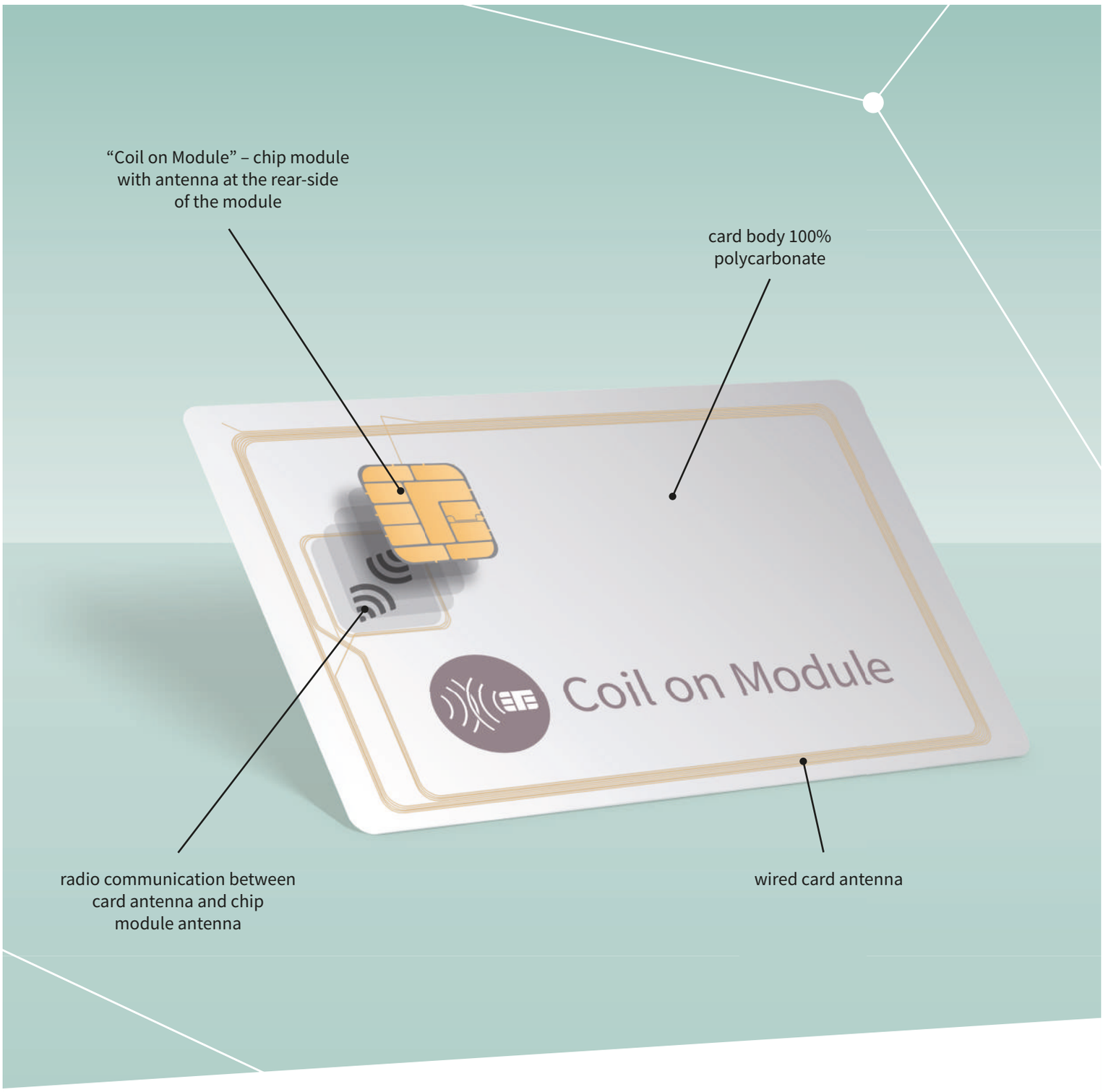
www.id4africa.com

Contact Veronica Ribeiro at
v.ribeiro@id4africa.com

Sponsorship & Exhibiting Opportunities Available!

24-26 April 2018

Abuja International Convention Center | Nigeria



Go contactless with Coil on Module (CoM)

- CoM is designed to simplify your transition from contact-based to dual-interface card production
- CoM delivers a new level of card body robustness and reliability
- CoM is THE solution for 10 years life time – essential for ID documents

www.infineon.com/CoM