



The Presidency
THE NATIONAL IDENTITY MANAGEMENT COMMISSION

The NIMS Strategy and Technology Document

**ESTABLISHMENT OF THE NATIONAL IDENTITY DATABASE, ISSUANCE OF UNIQUE
NATIONAL IDENTIFICATION NUMBER, ISSUANCE OF SMART CARDS AND CREATION
OF AN IDENTITY VERIFICATION AND AUTHENTICATION INFRASTRUCTURE**

August 2010

Table of Content

Executive Summary

1.	Introduction	4
1.1	Purpose and Objective of Document	4
1.2	Concern for Unique Identification of Citizens	4
1.3	Towards the Development of an Identity Sector in Nigeria	5
2.	Legal Regulatory and Institutional Framework	7
2.1	Government's Policy Thrust	7
2.2	Existing Policy and Legal Environment	7
2.3	Card Issuance and Identity Management	8
2.4	The NIMC Act No. 23 of 2007	9
2.5.	The National Identity Database (NIDB)	10
2.6	The National Identification Number (NIN)	10
2.7	The General Multi-Purpose Card (GMPC)	10
2.8	The Authentication and Verification of Identities	10
2.9	Harmonization and Integration of Identity Databases	11
3.	National Identity Management System (NIMS)	12
3.1	Concept, Design and Implementation Strategy	12
3.2	Components of the NIMS and Implementation Strategy	13
3.3	Features of the NIMS	17
3.4	Harmonization and Integration Role of NIMC	23
4.	NIMS Technology Architecture Overview	25
4.1	System Architecture Overview	25
4.2	Overview of Data Security Strategy	27
4.3	Overview of Fraud Management Strategy	30
5.	Front End Partners (FEPs) and the Enrollment Strategy	33
5.1	The FEPs and Service Implementation	33
5.2	Enrollment Process and the Issuance of the NIN	35
5.3	The National Identification Number (NIN)	37
5.4	Implementing the Use of the NIN	37
5.5	Managing the Enrollment Process to Ensure Coverage	37
5.6	Updating the NIDB	38
5.7	Other Enrollment Issues Considered	40
5.8	Smart Card Personalization and Issuance	41
6.	Back End Partners (BEPs) and the NIMS Core Value Proposition	42
6.1	The BEPs and Service Implementation	42
7.	Overview of Service Management Processes	45
7.1	The NIMS and Its Applications	45
7.2	Enrollment Application	45
7.3	The Authentication Applications	46
7.4	Biometric Solution and Provisioning	46
7.5	Verification Subsystem of Authentication Server	48
7.6	Provision of Authentication and Verification Services	48
7.7	Stakeholder/Customer Service Media	54
8.	Implementation and Risks	57
9.	Benefits of the NIMS and the NIN	60

ACRONYMS AND ABBREVIATIONS

ABIS	Automated Biometrics Identification System
AFIS	Automated Fingerprint Identification System
BEO	Back End Operations
BEPs	Back End Partners
BSP	Biometric Service Provider
CA	Concession Agreement
CADs	Card Acceptance Devices
DNCR	Department of National Civic Registration
EFCC	Economic and Financial Crime Commission
FCT	Federal Capital Territory
FE	Front End
FEPs	Front End Partners
FIRS	Federal Inland Revenue Services
FOC	Free of Charge
FRSC	Federal Road Safety Commission
GMPC/GMP Cards	General Multi Purpose Card
HIC	Harmonization and Implementation Committee
ICAO	International Civil Aviation Organization
ICPC	Independent Corrupt Practices and Other Related Offences Commission
ICPF	Integrated Card Production Facility
ID	Identity
INEC	Independent National Electoral Commission
IRCs	Identity Registration Centres
LEAs	Law Enforcement Agencies
MOCD	Match-on-Card Device
MRC	Mobile Registration Centres
MSP	Managed Service Provider
NADRA	National Database and Registration Authority
NCIR	National Civil Identity Registry
NHIS	National Health Insurance Scheme
NIDB	National Identity Database
NIMC	National Identity Management Commission
NIMS	National identity Management System
NIN	National Identification Number
NIS	Nigeria Immigration Service
NP	Nigeria Police
PPP	Public Private Partnership
PIDSP	Person Identification Service Providers
PSC	Project Steering Committee
SAGEM	SAGEM SA, France
SIM	Subscriber Identity Module
SSS	State Security Services
TSPs	Technology Service Providers

THE NATIONAL IDENTITY MANAGEMENT SYSTEM (NIMS) **TECHNOLOGY AND STRATEGY OVERVIEW**

1.0 Introduction

1.1 Purpose and Objective of Document

This document provides an overview of the concept, design, technology, benefits and implementation plan, risks and benefits of the National Identity Management System (NIMS) and Infrastructure which the National Identity Management Commission (NIMC) will put in place. This document was prepared in line with Government's approved Policy and Institutional Framework for an Identity Management System for Nigeria and was recently revised based on the provisions of the National Identity Management Commission Act No. 23 of 2007.

The contents of this document has been carefully selected to give an overview only, based on the history, development and current state of the identity sector in Nigeria, recent Government decisions on the reforms necessary in the sector, the level of implementation of the reform initiative and the challenges ahead which must be dealt with if the benefits of the NIMS are to become available to the entire Nigerian society.

1.2 Concern for Unique Identification of Citizens

Piqued by the lack of depth in the consumer credit market and the absence of a uniform system of identification in Nigeria which would particularly assist the Law Enforcement Agencies in the discharge of their responsibilities, the Federal Government, in 2005 set up a Committee to, amongst other things, advise it on appropriate steps to take to harmonize identification schemes in Nigeria.

A prominent feature of the historical development of the identity sector in Nigeria is the multiplicity of identity cards scheme. Most schemes are necessarily focused on the '*collection of personal information so that an identity card could be issued*'. This was largely due to the mistaken belief that an identity card is a conclusive proof of one's identity.

Modernization, globalization and the ever growing technology-driven knowledge economy and the complex, highly formalized nature of interaction and transactions amongst people, governments and institutions across communities, nations and continents around the world, impose a peculiar need for an acceptable means of confirming that you are dealing with whom you want to deal with. The Identity Sector has taken on a new and complex shape globally and identification schemes are now seen as a critical infrastructure for national economic development

Today 'Business Centres' across Nigeria, in response to the requirement for individuals to have a 'photo-ID', now boldly advertise 'photo ID' as one of the services they render. Unfortunately this trend only underscores the need for a paradigm shift away from 'ID card issuance' activities to 'identity management system'.

1.3 Towards the Development of an Identity Sector in Nigeria

In an effort to satisfy its identification needs, organizations in both public and private sectors, including the States, have focused on 'ID card issuance'. Recent efforts have shifted away from issuance of ordinary ID cards of different qualities to smart cards most of which do not have the corresponding verification processes. The absence of a credible National Identity Management System (NIMS) in Nigeria poses specific challenges that directly impact the lives and livelihood of every Nigerian, at home and abroad.

It will be recalled that in 2005 Government appointed a Committee¹ to advise it on how to harmonize the various identification schemes. Following Government's adoption of the Report of the Committee, a Policy for the development of an Identity Sector was approved by Government in May 2007. The Policy amongst others, provided for:

- a. The establishment by law, of a Commission to implement the identity sector reform;
- b. The Commission could partner with any organization in the private and or public sector to achieve its objective;
- c. Creation of a National Identity Database (NIDB);
- d. Issuance of Unique National Identification Number (NIN) to registered persons 16 years and above (and registration and issuance of NIN to those below the age limit);
- e. Harmonization and integration of existing identity databases in Government Agencies;
- f. Provision of data processing, storage and connectivity infrastructure;
- g. Provision of identity authentication and verification infrastructure;
- h. Introduction and deployment of a General Multipurpose Card (GMPC); and
- i. Introduction and deployment of Card Access Devices (CADs).

The primary objective of the reform agenda is to create a modern national identity management system and infrastructure that includes a secure, reliable and accessible National Identity Database (NIDB), secure identity document and identity

¹ **Committee on the Harmonization of Identification Schemes in Nigeria was set up in March 2005** by President Olusegun Obasanjo. El-rufai; Nasir, then Minister of FCT, was Chairman. The Committee submitted its Report to the President- in-Council (FEC) on March 22nd, 2006.

authentication and verification infrastructure that *enables an individual to assert his identity and around which a wide range of value proposition is built that meets* current and long term identity authentication and verification needs of Law Enforcement Agencies (LEAs), Business and Commercial Transactions in the public and private sectors in the Nigerian economy.

Aside from setting up of the NIMC and 'winding down' the former DNCR, much of the effort of the NIMC has been concentrated on developing, in partnership with the private sector and government agencies, the NIMS.

2.0. Legal, Regulatory and Institutional Framework

2.1. Government's Policy Thrust

The Committee Government set up in 2005 had proposed a Policy for the reform of the 'identity sector' in Nigeria which aimed at avoiding wastages/duplication of efforts, 'reuse' of existing investment where possible, creation of a conducive environment for the orderly development of an identity sector and to leapfrog Nigeria into the modern technology-driven identity management and assurance systems in a sustainable manner and in partnership with the private sector.

To achieve this, Government decided that the challenge of identity management and the benefits were enormous to not give the sector the deserved political support at the highest level of decision-making. To obliterate the conditions for the stunted growth of the sector, it was also decided that the sector could no longer be managed as a department under a Ministry.

These decisions in effect provided the policy² parameters for instituting a legal, regulatory and institutional framework for the orderly development of an identity sector and for the implantation of an identity management system for Nigeria.

2.2. Existing Policy and Legal Environment

There was no real attempt at providing an identity management system and infrastructure in Nigeria in the pre-colonial era, due in part to the nature of the socio-political development and cultural heritage of the various ethnic groups and nationalities that constitute the Nigerian nation- state as we know it today.

Post-independence, efforts at creating a NIMS was legislation-induced and understandably so: in the wake of efforts at implementing the various national development plans, Government Institutions and Agencies were created by law to provide specific services- the Nigeria Immigration Service (NIS), Joint Admissions and Matriculation Board (JAMB), National Health Insurance Scheme (NHIS), Federal Road Safety Commission (FRSC), Federal Inland Revenue Service (FIRS) etc- most of which required that personal information of individuals were collected before and or during the process of service delivery.

² The 'National Policy and Institutional Framework for an Identity Management System for Nigeria' was launched on January 11th, 2007. Prior to this time, a Presidential Implementation Committee, (PIC) under the Office of the Secretary to the Government of the Federation (OSGF) had begun to implement the recommendations of the Harmonization Committee which are contained in the Policy.

In some cases the process is repeated each time the service is to be delivered, a typical example being JAMB. Identities claimed were neither confirmed nor unique and an individual could have different identities in each location. Also very limited efforts were made at a uniform data collection, codification and storage to facilitate inter-agency collaboration on information sharing or management to optimize resources. In the private sector, the situation is the same with the result that an individual is obliged to provide the same set of personal information and documentation to open a Bank Account in more than one bank, for example.

The result of these activities is multiple identities, stunted growth and development of an identity sector characterized by lack of standards, varied identification schemes with isolated, disparate databases, different types of Identity Cards and an absence of any secure (trusted) means of genuinely authenticating the identity of an individual.

2.3. Card Issuance and Identity Management

A prominent feature of the historical development of the identity sector in Nigeria is the multiplicity of identity card schemes which, as earlier noted, was due to the mistaken belief that an identity card is a conclusive proof of one's identity. (See table below).

S/N	Projects/Sector	Biometrics included	Type/Number of Card issued	Year implemented
1.	INEC Electronic Voters Register	Finger prints (2x)	Paper/58.6m Plastic cards	2003
2.	NHIS Patient Cards	Finger prints (2x)	2D Bar code/>500,000	2005
3.	National ID Cards	Finger prints (6x)	2D Bar Code/>15m	2001/still ongoing
4.	FRSC	Finger prints (1x)	Mag stripe 2D Bar Code (by 2006)	1990
5.	University Students ID	No biometrics	Smart/200,000	2001
6.	ValueCard	No biometrics	Smart/1,300,000	1998
7.	PenCom National Databank	Finger prints	Smart	In-progress
8.	ECOWAS Harmonized E-Passport	Finger prints (4x)	Smart	In-progress
9.	State Governments	Some- Finger prints Others- No biometrics	2D Barcode/140,000 Others- Smart>150,000	2003/2004

Therefore it was important to effect a shift from ID card issuance to identity management.

A National Identity Management System combines a National Civil Identity Register (NCIR) or Database, a secure Identity Document and a means of accessing the Identity Database to irrefutably ascertain the identity of citizens and residents in a country. In Nigeria, the best effort so far has produced an enhanced secure system of ID Card

printing and issuance³. **It is important to note that the National Identity Card project** executed under the defunct Department of National Civic Registration (DNCR) focused mainly on ID Card printing and issuance, and less on management of identities.

2.4 The NIMC Act No. 23, 2007

The National Identity Management Commission Act is the instrument that created the legal regulatory and institutional framework for the identity sector in Nigeria including the mechanism for implementing Government's reform effort. Important sections of the Act⁴ include the following:

- a. Section 5 of the NIMC Act vests in the Commission the power and function to create, manage, maintain and operate an identity database;
- b. In Sections 1 – 13, the Commission's governance structure, functions, powers and
- c. funding mechanism was spelt out. It includes the duty to harmonize existing identity databases in government institutions, power to collaborate with public and or private sector institutions to achieve its objectives, etc⁵;
- d. Section 14- 17 established the National Identity Database, its purpose, content and eligibility to register (section 16);
- e. Section 18 -25 provides for the introduction of general multi-purpose Cards (GMPC) while Section 27 provides for the issuance of and mandatory use of the UNIQUE NATIONAL IDENTIFICATION NUMBERS (NIN) for transactions;
- f. Section 28 stipulates how unauthorized access is treated, especially in relation to transactions without a national identification number. Section 30 provides for miscellaneous offences and Section 31 provides for the Commission's power to make regulations. Section 32 repealed the National Civic Registration Act and transferred to the Commission all its assets and liabilities.

³ **In 2001 Government contracted SAGEM S.A of France (now a member of the SAFRAN Group) to deliver an Integrated Card Personalization Facility (ICPF) including personalization of 60million ID Cards (only 37.8m Cards were personalized). The contract expired in December in 2006. With advancement in technology, especially in biometrics, exclusion of over 40% of the Nigerian population, absence of a Disaster Recovery and Business Continuity Centre, no permanent arrangement for data updating and for populating the Database, no Connectivity infrastructure, no integration with other databases, very high human intervention in the data collection process and without an Authentication and Verification infrastructure, Government decided on the NIMS and to reuse, if possible the AFIS and Database from the 2001 Agreement.**

⁴ **The NIMC Act 23, 2007 and the Policy document** are available on the website of the NIMC - www.nimc.gov.ng

⁵ **The NIMC is essentially a policy focused and regulatory oriented institution.** It will enforce the provisions of the NIMC Act, issue regulations and policies consistent with the Act and prescribe the industry guidelines that will leapfrog technology deployment especially biometrics, guide enrollment, authentication and verification processes in the emerging Identity Sector in Nigeria. **However, for obvious strategic reasons the NIMC will create, operate and manage the National Identity Database and NIN issuance processes.**

2.5 *The National Identity Database*

The National Identity Database (NIDB or the Central Identity Data Repository or Register (CIDR) was created by Section 14 and Sections 15 – 17 provides for the conditions for enrollment of persons into the NIDB, which includes the age (16 years and above), legal residents, the particulars to be provided by an enrollee and the sanctions for not complying with the provisions of the Act. The Act also provides for the registration of births and deaths, an important legal provision to enable the achievement of an important strategic policy objective - full coverage.

2.6 *National Identification Number (NIN)*

Section 14(2) provides for any person in respect of whom an entry is made in the NIDB to be identified using unique and unambiguous features including the biometrics. The generation and use of a unique identification number derives from this provision. The NIN is a non-intelligent set of numbers (11) by which a registered person will be identified for life and once used can never be used again even after the person to whom it was originally assigned is dead.

2.7. *The General Multi-Purpose Card (GMPC)*

The NIMC Act provides in Section 18 for the issuance of the General Multi-purpose Card and for the contents of the Card. It also provides for the conditions under which the Card would be changed, withdrawn and or dealt with. The Section introduced for the first time a Smart card into the identity sector and makes it mandatory for each registered person to be issued one. The GMPC is targeted at achieving the policy objective of standardization, uniformity and optimization of resources and making the benefits of the NIDB to be easily deployed to card-based services.

2.8. *Authentication and Verification of Identities*

An important provision in the NIMC Act is Section 27. This section provides for the mandatory use of the NIN in specified transactions (seven in number namely ...) and also empowers the NIMC to further expand the scope of the transactions that can be covered. Whilst this provision is important for the acceptability of the scheme, the 'trust' and 'integrity' of the NIMS, and therefore the NIN, will earn its acceptability and hence the wide spread usage expected.

Accordingly the strategic intent is to provide for both 'on-line and off-line' authentication and verification infrastructure based on the dedicated network connectivity available to the NIMC. Furthermore the verification services will be rendered by the NIMC in partnership with the private sector. The NIMC partners would be required to deploy Card Acceptance/Access Devices (CADs) and a range of such

CADs will be certified for the Nigerian Market by the NIMC. The online authentication services will be supported by secure internet access for simple and graduated confirmation of identities using either biometrics and or other levels of confirmation that would become available.

2.9 Harmonization and Integration of Identity Databases

Another important provision in the NIMC Act is the provision for the NIMC to harmonize identity databases in government agencies towards ensuring that the NIN and the NIDB is fully optimized in view of scarce government resources. This would foster an orderly development of the identity sector characterized by internationally indexed standards, uniform practices and user-friendly technology solutions. To ensure this, NIMC would establish a Harmonization and Integration Implementation Committee (HIC). HIC is to ensure the standards and processes of various public and private sector institutions are ultimately in accordance with NIMC strategy and technology initiatives.

3.0. The National Identity Management System (NIMS)

3.1 Concept, Design and Implementation Strategy

Government's efforts at reforming the identity sector to allow for identity authentication and verification, through the creation of secure access to a National Identity database (NIDB), and upgrading the identity card to smart cards brought about the implementation of the **National Identity Management System (NIMS)**⁶ under the National Identity Management Commission (NIMC). The NIMS will comprise of:

- a. Registration and biometric enrollment of citizens and legal residents, for the purpose of uniquely identifying the individual and thus creating a National Identity Database and through that process (on a sustainable basis);
- b. Issue a unique National Identification Number (NIN) to the registered individuals;
- c. Issue General Multi-purpose Cards (GMPCs) (as provided for in the NIMC Act);
- d. Provide for identity authentication verification services;
- e. Provide for access and connectivity infrastructure between registration centers, central data processing center, identity verification system and backend systems;
- f. Provide for harmonization and integration of identity databases in government agencies, including providing the regulatory and institutional framework for an orderly development of the identity sector in Nigeria.

The registration and enrollment process which will be once in a life time, will result in the capture of demographic and biometric data (ten (10) fingerprints and live digital photographs and signature), and other relevant data of citizens and legal residents. Provision is made for facial recognition while fingerprint will primarily be used for verification. Also provision is made for future upgrade (in the fifth year of operation of the NIMS) for the inclusion of iris.

Various forms of registration activities and databases that currently exist will be streamlined through a process of harmonization and integration, designed to enable the 'reuse' as appropriate, of existing infrastructure, optimize resources, ensure sustainability, flexibility and scalability (based on lessons of the past) and avoid a 'single point of failure' scenario.

⁶ On March 22nd, 2006, Government, in accepting the recommendations of the Harmonization Committee it set up in 2005, noted the focus and therefore limited benefits of the Integrated Card Personalization Facility (ICPF) infrastructure built on the basis of the 2001 Agreement with SAGEM and subsequently approved the NIMS.

3.2. *Components of the NIMS and Implementation Strategy*

An important strategic approach to facilitate the implementation of the NIMS is the conceptual distinction between two connected components, namely the 'Front End Operations' (FEO) and the 'Back End Operations' (BEO), that is:

a. Front-End Operations comprising:

- i. Registration and biometric enrollment of Citizens and legal residents (Data capture/updating);
- ii. Personalization and Issuance of Smart Cards with business applications;
- iii. Deployment of Card Acceptance/Access Devices (CADs);
- iv. Citizens and legal residents' contact and support operations.

b. Back-End Operations comprising:

- i. Setup, operation and management of the National Identity Database (NIDB);
- ii. Provide for Disaster Recovery/back up and business continuity infrastructure;
- iii. Establish and maintain secured network connectivity infrastructure and communication links with relevant identity related agencies and end-users;
- iv. Provision of authentication and verification services.

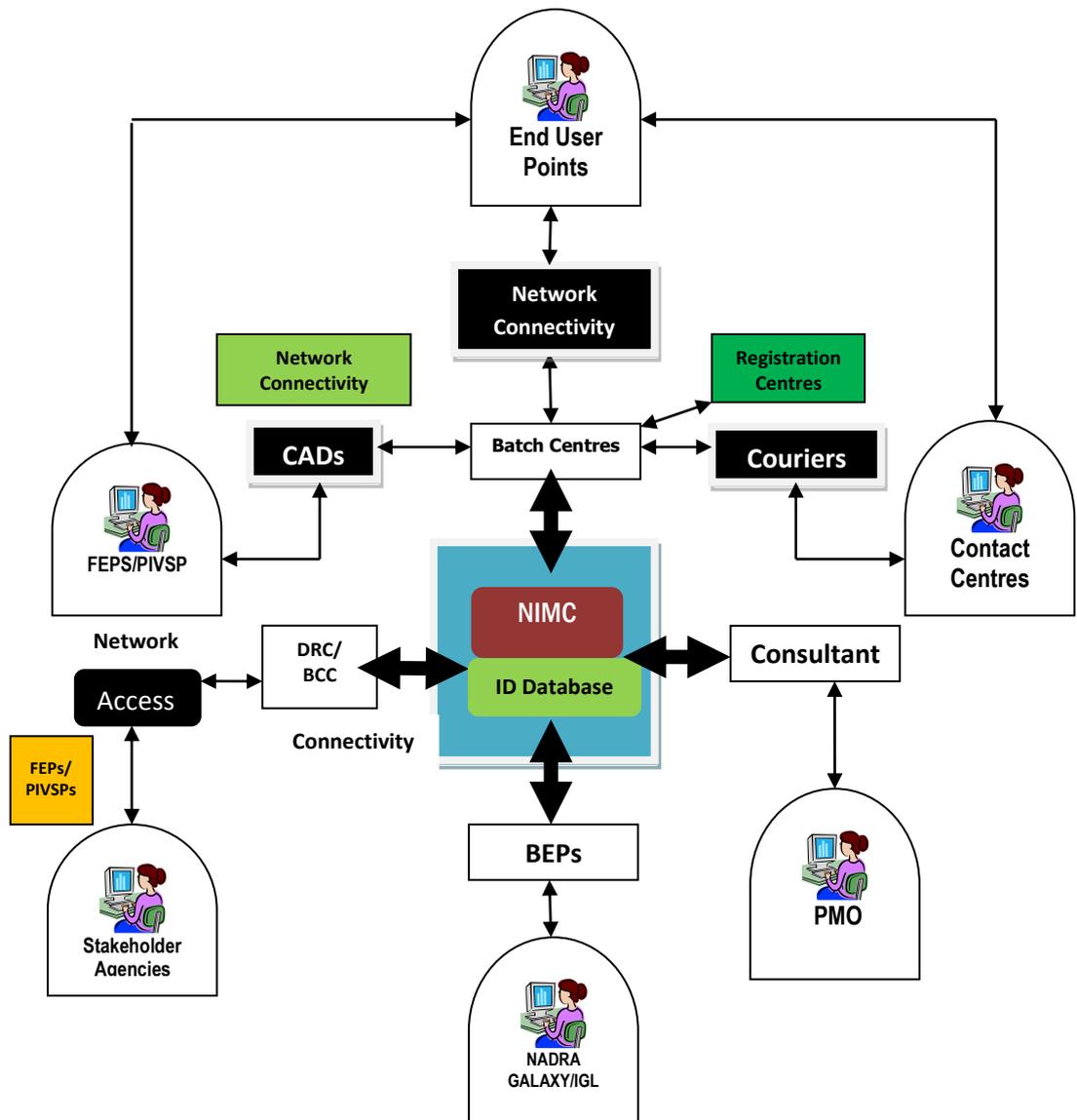
Both components will be implemented by the NIMC in collaboration with 'Front End Partners' (FEP) and approved technology service providers (designated as Back End Partners) and consultants.⁷ Upon complete roll out, the infrastructure would include:

- a. Permanent registration centres for continuous biometric and demographic data capture services;
- b. A National Identity Database and a regime of unique national identification number, (NIN);
- c. Disaster Recovery Site with provision for Business Continuity;
- d. Connectivity, Data Processing and Storage Infrastructure, Systems Integration and software development services support and maintenance capacity;
- e. Provision of authentication and verification infrastructure and commercial applications;
- f. Smart Card personalization facilities and commercial applications.

⁷ On May 16, 2007, the FEC approved the selection of two consortia, CHAMS and ONESECURECARD as NIMC partners for the FEO and Galaxy Backbone Plc, (in 2008 and later in 2009), Interglobal Ltd and NADRA as the technology service providers for the BEO. The partners have since commenced work and the NIMS Infrastructure currently being rolled out.

In the FEO, the FEPs will establish operate and maintain Identity Registration Centres (IRCs) across Nigeria in designated locations in the State Capitals and Local Government Areas⁸ under a Concession Agreement (CA) for ten (10) years. These IRCs will be permanent, temporary and or mobile centres.

The NIMS Partners and Ecosystem



⁸ The NIMC inherited properties from the defunct DNCR which it will renovate and hand over to the FEPs for use as permanent IRCs.

The NIMC will provide connectivity, processing and storage infrastructure and services at the BEO to support de-duplication, enrollment and assignment of NIN, authentication and verification as well as ensure the harmonization and integration that will deliver the digital identity platform for an economy-wide value proposition. The NIMC BEPs will provide these services as contracted Technology service providers to the NIMC.

In addition the NIMC will provide the framework and prescribe the guidelines within which the FEPs and BEPs will function including providing policy direction and leadership, and approving the technology, processes and procedures for the FEPs and BEPs under their respective contractual arrangements towards the orderly development of the identity sector in Nigeria.

As part of the framework, the NIMC will create, operate and manage the NIDB {also known as the National Civil Identity Register (NCIR)}. This NIDB as a repository of predetermined personal information of citizens and legal residents, will function as a Managed Service Provider (MSP) to implement the core NIMS value proposition (unique identification) through three functional channels – issuance of the unique national identification number (NIN)⁹, provide de-duplication processing¹⁰ and manage authentication and verification of identities¹¹.

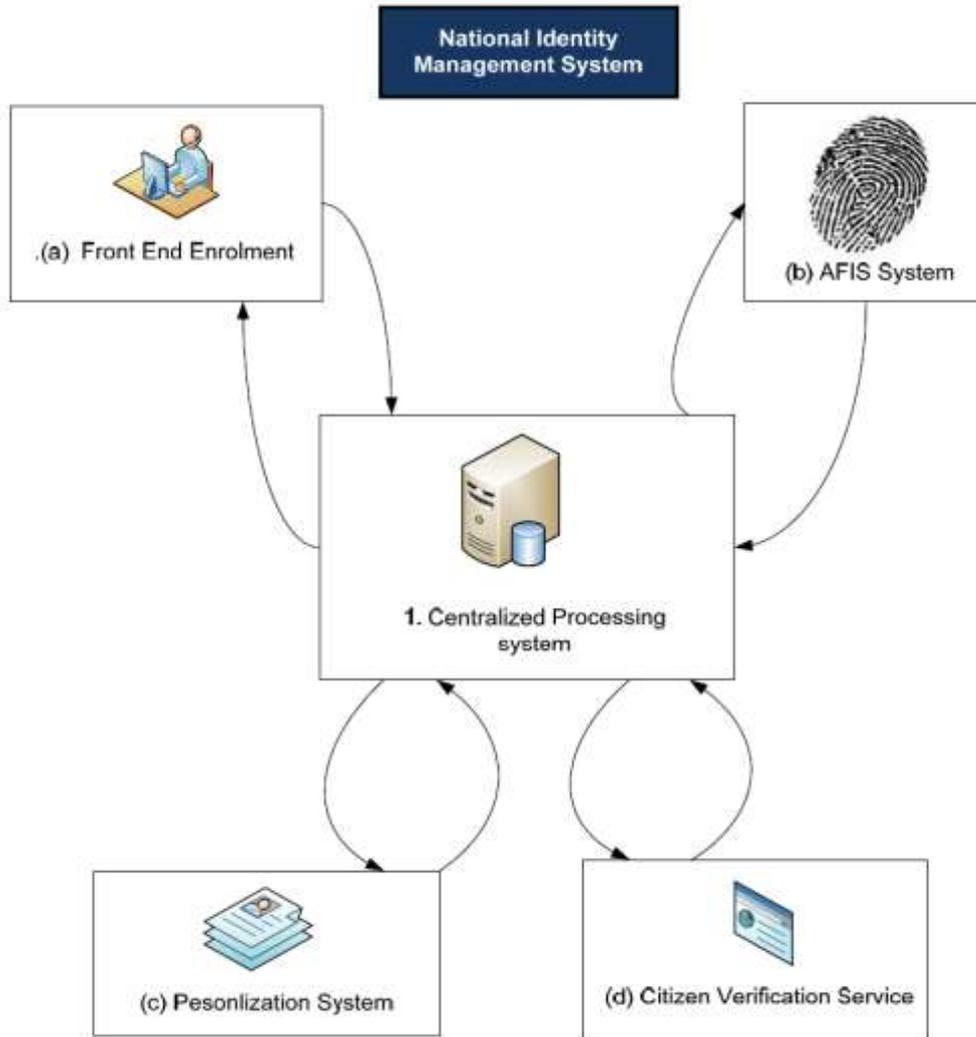
Furthermore the NIMC will provide for a dedicated fibre optic link between the central data centre and selected Government Agencies with significant data management needs so as enable co-location and foster a shared and interoperable platform.

⁹ The NIN will be a random (not intelligent) numeric that is unique to each individual.

¹⁰ The plan is to provide a redundant multimodal biometric functionality in view of the existing AFIS, providing an option or substitute. The ABIS will function as the primary de-duplication process for the NIDB under the NIMS Scheme.

¹¹ This managed service will require accredited third party off-line and on-line infrastructure support to thrive.

Overall Description of the NIMS



3.3 Features of the NIMS

a. Issuance of Unique National Identification Numbers (NIN)

The primary focus of the NIMS is the creation of a National Identity Database through the de-duplication process and subsequent issuance of a unique National Identification Number (NIN) that is linked to an individual's demographic and biometric information. The NIN is meant to guarantee an identity for the individual.¹² It will also serve as a platform for other possible beneficial uses of the NIN in terms of identity related activities and transactions. The most important aspect to note is the authentication services which will help drive non-repudiation in transactions in the public and private sectors. The NIMC Act provides for both the issuance of the NIN and certain transactions for which the use of the NIN is mandatory.

b. The NIMS provides for the Issuance of the GMPC

The NIMS provides for the issuance of the GMPC, that is a Smart Card with a processor chip. The specific technical details are contained in the relevant design document. The introduction of (and how to deal in) the GMPC is provided for in the NIMC Act (Section 18. It will facilitate off-line, match-on-card identity authentication and verification).

c. Full and Proper Coverage in the National Identity Database

In line with the National Policy and Institutional Framework for an Identity Management System for Nigeria, the plan is to ensure the registration and enrollment of citizens aged 16 years and above (and then also all those aged under 16 years). Fortunately the Act provides for the registration of legal residents, births and deaths, an important technical means of ensuring full coverage ultimately in the National Identity Database. This will ensure that the value of the NIN is wide ranging.

¹² **The NIMS is designed to provide identity and not to prove citizenship.** Legal residents are expected to present appropriate documents to establish their status. From a date and time to be specified by the NIMC, citizens and legal residents will be required to present their NIN to be entitled to certain benefits or transact certain classes of business. Non-compliance is sanctionable as provided for in the Act..

d. Proper Verification will precede Enrollment

The envisioned future state of the NIMS is full coverage in the proposed National Identity Database predicated on properly attested primary verification¹³. This will enable the NIMC ensure that initial demographic data provided by the applicants for registration and enrollment are genuine to ensure the that data collected is correct and 'clean' right from the beginning of the project so that the proposed National Identity Database (NIDB) under the NIMS would be free of duplicates/multiple identities.

e. Proper pre-enrollment verification will not hinder enrollment

The NIMC in collaboration with the FEPs will make sure that the need for a proper verification of a person prior to registration does not hinder the registration and enrollment process, in particular for those of the citizens in the rural areas and border communities¹⁴. NIMC would devise a suitable procedure and specify a list of acceptable primary source documents¹⁵ and or identity credentials by which an individual can become a 'Known citizen' before he can be enrolled.

f. No one will be turned back for not having a primary source document

As a deliberate policy, the NIMC would ensure that no one would be refused enrollment by reason of not being in possession of or able to produce any of the approved primary source documents. The NIMC would ensure the observance of standards in such a manner that they do not become a barrier to the enrollment process whilst also ensuring that the procedures help achieve total inclusion as envisaged without compromising the integrity of the National Identity Database.

¹³ Unfortunately existing identity databases in Nigeria are fraught with problems of fraud and duplicate/ghost identities. Reliance on existing identification token is therefore to achieve an interim strategic objective and this requires proper training for Registration/Enrollment Officials, proper education of applicants of the implications of falsification and the use of a wide range of demographic fraud scenarios to articulate control measures to be built into the NIMS processes. This would be done in collaboration with the NIMC partners.

¹⁴ This is particularly important given the various treaties and protocols that Nigeria is a signatory to especially the ECOWAS Treaty on Free Movement of Persons.

¹⁵ The list which would be widely publicized would be jointly developed with the NIMC partners and made available at all registration points/centres.

g. List of primary source document for pre-enrollment verification

The NIMC has developed and will make available a list of acceptable documents and or ways by which a proper verification can be conducted. This will ensure that the challenge or difficulty in establishing the primary demographic data of citizens is significantly mitigated. Most individuals do not have any form of identification, even the existing identity documents that cannot be relied upon are not generally held by citizens. In most cases it would be the first time an identification document would be issued to the individual¹⁶. The NIMC will however pay special attention to the enrollment of citizens especially in the rural areas and border communities for obvious reasons.

h. The NIMS is based on a PPP Scheme

The NIMS is based on a public-private sector partnership (PPP) scheme. A concession for an initial ten (10) year period to undertake data capture, smart card personalization and issuance and card acceptance device deployment services, require the private sector partners to establish operate, maintain and manage registration centres (mobile, temporary and permanent centres across Nigeria) which will help bring a large number of the targeted population into the Database and sustain regular data updating. It is expected that within the first thirty (30) months, one hundred million (100m) enrollments would be achieved¹⁷. There are two private sector partners whose investment and expectations have been linked to projected revenue streams based on the use of the NIN in authentication and verification services.¹⁸ The use of the NIN for authentication and verification services would be based on both on-line and off-line methods which will positively impact on service delivery in government agencies and the private sector.

¹⁶ Due to late production and an inappropriate and poorly managed distribution strategy, the ID Cards produced after the 2003 registration exercise have not been completely distributed to their owners, most of who have since relocated from their initial point of registration. Even then, the current National ID Card did not cover up to 50% of the population at that time. Logistics providers and contact centre operators would manage/facilitate the distribution of Enrollment Confirmation Slips and the Smartcard.

¹⁷ **An important departure from the past efforts is the establishment of permanent registration centres which will ensure continuous demographic and biometric capture at the convenience of the applicant** and also encourage bio-data updating while providing for a structured approach to IT up-scaling and refreshment.

¹⁸ In May 2007 two Consortia, namely CHAMS and IRISONESecureCard were appointed NIMC partners by Government.

i. Private Sector to manage the Front End Component. (Data Capture Services)

An important feature of the NIMS is that the process of enrollment has been further simplified and made more convenient and sustainable through the participation of the private sector. The FEPs will capture and process data for each enrollee under the NIMS for the issuance of the NIN. Once the data is captured, it is processed, batched and transmitted to the NIMC Data Centre. At the Data Centre the data is connected to the NIDB to perform de-duplication of personal information collected from applicants at the various Registration Centres. After this processing, a NIN will be assigned, issued and sent to the FEPs for further action (release it to the applicant and or personalize and issue a Smart Card for the applicant). The enrollment is then stored in the ABIS subsystem and the NIDB.

j. Third Parties to Support Provision of Authentication and Verification Services

The authentication services would be provided by the NIMC through various forms of partnerships with the FEPs and accredited service providers to be designated as Person Identification Service Providers (PIDSP). Accordingly the NIMC would have two sets of authentication service providers- the FEPs and the PIDSPs¹⁹. The NIMC will partner with Government Agencies (for whom dedicated fibre optic links will be established) and specific service providers for their peculiar authentication needs.

k. The NIMS will foster the Development of an Identity Sector

The NIMC has a regulatory role as well as an important 'Harmonization and Integration' role. The deployment of the NIMS as presently conceived will foster the orderly development of an identity sector in Nigeria (especially the responsibility to create, operate, regulate and manage the National Identity Database (NIDB) through which the NIN would be issued, provision of the necessary platform for continuous updating of the personal information of those enrolled in the NIDB and provision of the platform and supporting infrastructure for the authentication verification services (in collaboration with its partners).

¹⁹ **The NIMC will appoint third party service providers in addition to the FEPs as agents or licensees of the NIMC to help manage access to the NIDB for authentication and verification services** so as to ensure the achievement of wide spread usage and generate the expected revenue streams that would help sustain the scheme and 'pay back' private sector investments over the concession period. The PIDSP, will invariably 'spread the cost of deployment'.

l. NIMS provides for in-built flexibility and Industry Standards

The FEPS will be allowed significant flexibility in their processes, (within set technical standards and criteria) including card issuance, determination of fees for authentication services (mechanism will be regulated), provisioning for the authentication and verification services spectrum, and demographic and biometric data collection service regime, subject to the minimum security standards issued by the NIMC.

As part of its regulatory, harmonization and integration roles, the NIMC will provide standards to enable both the FEPs and institutions that wish to create their own Database to maintain uniformity in collection of certain demographic and biometric information, and in performing basic 'know-your-respondent' activities. These standards are to be developed and agreed under the Harmonization and Implementation Committee set up by the NIMC. It is expected that these standards will be in sync with those already issued to the FEPs as they prepare to implement the NIMS.

m. The NIMS Process will eliminate duplicates

A core component of the NIMS is the NIDB which can only be of immense value if a process of de-duplication is concluded for each unique enrollment that is in the NIDB. The system therefore is based on a 'self-cleansing mechanism which is in-built in the design, implementation and execution of the enrollment process. As an example, the registration and enrollment process provides for the FEPs to batch and submit to the NIDB at the NIMC Data Centre, applicants' data for de-duplication. The NIDB will execute a search on the key demographic fields and on the biometrics for each new enrollment. In this way duplicates in the NIDB will be eliminated.

The existing mix of multiple databases in Nigeria provides the compass for individuals to furnish different personal information to different agencies. Since de-duplication in the NIMS will ensure that citizens and legal residents have only one chance to be entered into the NIDB, it will encourage individuals to provide accurate data. This motivation will become especially powerful as access to credits, payment of different forms of benefits and entitlements and the conduct of certain transactions as specified in the NIMC Act, etc become linked to the NIN.

n. The NIDB is a Civil Register

The NIDB under the NIMS is different from and need not be confused with the 'central databases' concept under other projects of government. The NIDB is a civil register built from the process of unambiguous and unique identification of individuals by linking their demographic and biometric data to an assigned unique (non-intelligent) identification number that guarantees that the details do not appear more than once in the NIDB. As a central identity data repository (CIDR), it has the potential to meet

economy-wide value propositions of the NIMC (including supporting payment solutions and other commercial applications). It will facilitate both biometric and non-biometric specialized or function specific databases.

o. The NIMS provides for Online and Off-line Authentication

The NIMC will ensure the availability of a strong form of online authentication service as part of the NIMS. This will be in the form of 'secure graduated internet-based 'access' to the NIDB to enable comparison of demographic and biometric information of the citizens and legal resident with the record stored in the NIDB. The match-on-card option would also be available.

In line with Section 27 of the NIMC Act, and in collaboration with the FEPs and PIDSP, the NIMS will roll-out appropriate support infrastructure for the authentication (off-line and on-line) of a claimed identity, based on the use of the NIN, demographics and or biometrics across the various Government Agencies and private sector organizations.

Based on its regulatory function, the harmonization and integration mandate and through the PIDSP, the NIMC will help define and institute the necessary infrastructure and processes required to achieve optimal service level based authentication and verification services.²⁰

p. The NIMS will adopt a Privacy Policy

The NIMC will develop a privacy policy based on the outcome of a privacy impact assessment it will conduct to establish the range of privacy concerns and associated risks in the implementation of the NIMS.²¹ The NIMC hopes to achieve a balance between 'privacy risks and authentication and verification service objectives' in relation to the prescribed gamut of personal information to be collected for each enrollee. Access to the NIDB will similarly be guided by the corresponding degree of exposure to the privacy risks associated with the need for the access. Appropriate and standard indemnities would be subscribed to by enrollees at point of data capture which is consistent with the provisions of the NIMC Act.

²⁰ The initial authentication services policy provides for calibrated confirmation scheme. This will subsequently be upgraded.

²¹ In 2008, NIMC appointed a Consortia of firms to conduct a privacy impact assessment study. The outcome of the Study has been incorporated into the technology solutions of the NIMS.

q. *Full Disclosures for Overriding Public Interest*

The security and intelligence community will have access to full disclosures in the NIDB as provided for in the laws of the federation. The integration of their infrastructure with the NIMS will be designed to achieve a level of access beyond that to be granted for transaction-based verification and authentication of identities.

r. *Authentication Responses and levels of disclosure is consent-driven*

Although registration and biometric enrollment is mandatory, the NIMS process provides for confirmation of the personal information to be entered into the NIDB with the digital signature as conclusive evidence of prior consent. Also the NIMC will provide simple responses to all requests to authenticate identity through an affirmative or negative response (that is a 'Yes' or 'No' response). Further levels of access to obtain and or download full records will not be possible except in the case of security agencies and or in compliance with a lawful court order.

s. *Non-Disclosure Agreements and corresponding liability/Sanctions*

The NIMC will ensure that all Agreements and Contracts it enters into in respect of the NIMS declaratively commits parties to appropriate levels of Non-Disclosures and the strict observance of the required confidentiality in the treatment, management, access to and use of the information,(including the process of collection and treatment prior to and after it has been recorded) in the NIDB. Appropriate sanctions have been provided for in the NIMC Act for violations and non-compliance. Further delineation of liability and corresponding indemnification will be provided for in the Non-disclosure and relevant Service Level Agreements which the NIMC will enforce.

3.4 *The Harmonization and Integration Role of the NIMC*

As part of its functions, the NIMC Act provides in Section 5, and 14, for the creation of the NIDB including the harmonization and integration of existing identification databases in Government agencies. (Currently various Government Agencies/key institutions maintain disparate identity databases, going through similar processes to collect these identity data with no linkage between them thus constraining exchange of identity related data).

The NIMS provides for dedicated fibre link to specified Government Agencies. It also will connect with the national backbone infrastructure.²² There is provision for co-

²² The connectivity infrastructure for the NIMS, in part is provided by the Galaxy Backbone Plc, (GBB) a Government sponsored IT company responsible for the creation of the National IT infrastructure backbone. Aside from the dedicated VSAT network

location and fibre optic link between specified agency databases with the NIMS 'mirror database'. The harmonization and integration scheme clearly differentiates the NIMS from previous arrangements. The introduction of the unique identifier would further enhance the use of the database across agency specific databases guided by uniform standards issued by NIMC.

An important NIMC/NIMS approach is the creation of uniform standards in specific operational areas/issues. For example the demographic, biometric and verification procedures must as of necessity be standardized. Also to achieve interoperability and optimize the benefits of the NIMS, the NIMC had commissioned a harmonization and integration assessment study to determine the technical and network readiness of various government agencies. It will also develop standards and guidelines for their use towards the creation of an interoperable system with sufficient interactive window to facilitate the use of available databases by government agencies without hindrance.²³

connecting all enrollment centres at the State Headquarters of NIMC, a Disaster Recovery Centre, Business continuity infrastructure, connection of the NIMS network to the National Operating Centre of the GBB will facilitate the attainment of wider coverage and interoperability objective.

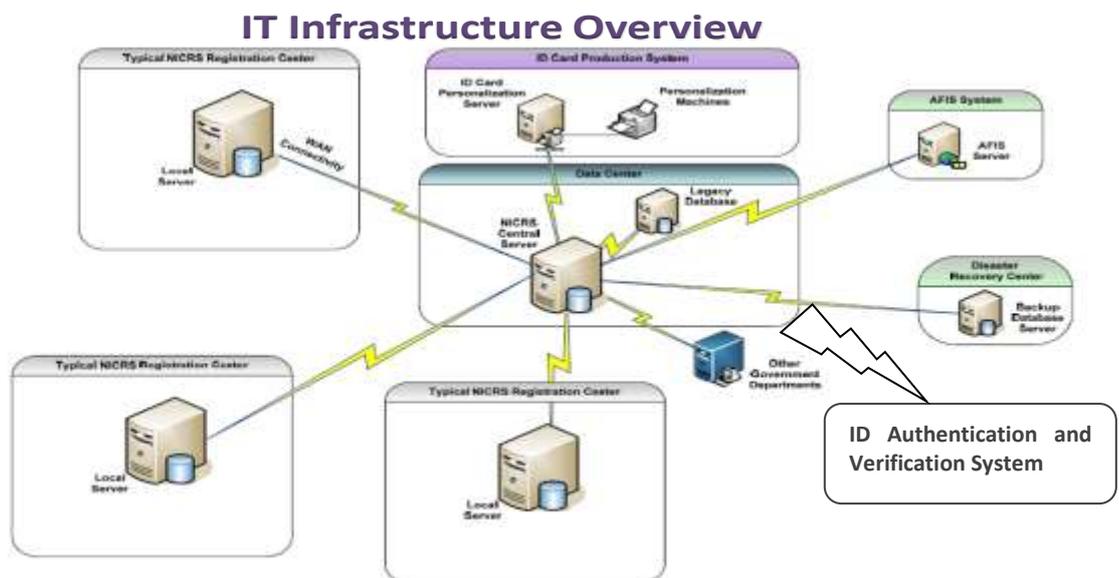
²³ **The Harmonization and Integration Implementation Committee which has membership drawn from all relevant government agencies will develop the demographic, biometric and business process policies standards and guidelines for the interoperability framework.** An important harmonization process that is currently ongoing designates the agencies as enrollment centres based on the compliance with pre-set enrollment criteria. It is expected that ultimately all such designated agencies would become enrollment partners of the NIMC.

4. NIMS Technology Architecture Overview

4.1 System Architecture Overview

The NIMS architecture is focused on the achievement of six (6) primary objectives central to the attainment of the dictum *'enroll once and be identified for life'* and these are:

- a. Ensure 'clean' and 'correct data' (demographic and biometric) collection from individuals;
- b. Ensure de-duplication process to guarantee uniqueness and integrity of database;
- c. Issuance of the NIN based on a unique non intelligent system to every enrollment in the NIDB;
- d. Focus on a sustainably high level of privacy and information security;
- e. Institute a dependable clear data verification and authentication infrastructure and service scheme; and
- f. Provide for interoperability (harmonization and integration) with other government agencies in a secure and scalable manner.



1

The important highlights of the technology architecture are described below:

- a. The NIMS (backend) Servers which is at the core of the managed services, will provide the processing of the enrollment, verification and authentication services over the network of the FEPs. The Servers are in two categories: the

primary Servers at the main Data Centre and the Servers at the Disaster Recovery/ Business Continuity Sites. They are designed to meet the demand for 1:1 and 1:N biometric de-duplication and the verification and authentication service request from end-users of the NIDB.

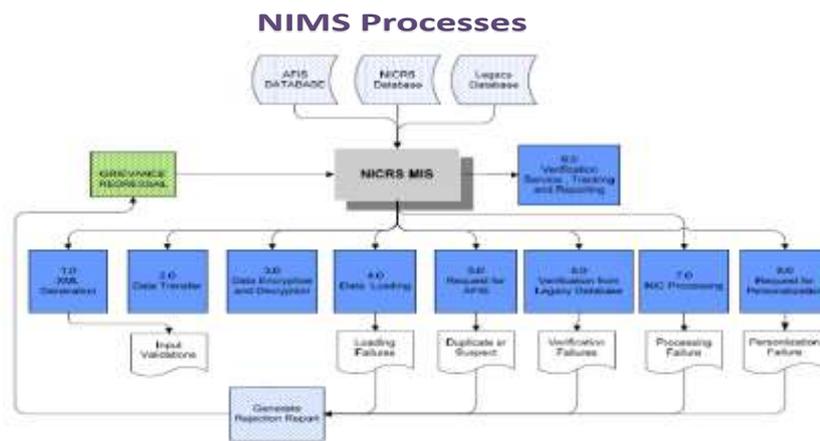
- b. The Network infrastructure provides for two sets of functionality based on the enrollment process, authentication and verification process and the Smart Card personalization process. The enrollment which will be done by the FEPs will require massive data transmittal in a single and or batched format from the IRCs where enrollments are done to the NIDB Data Centre where the de-duplication is done. It will also support the requests for identity verification from several end-user locations on-line as well as support the integrated platform for government agencies that have been harmonized with the NIDB (there is a provisioning for Contact Centres and specific logistics providers). The network includes dedicated VSAT/WAN, LAN, Internet, connected third party network infrastructure (FEPs have switch platform owners as partners) which link the State Offices of NIMC/IRCs, the NIDB and the end-users.²⁴
- c. There is a strong emphasis on the security design to secure the various components from logical and physical attacks. The security design covers both Server security (including firewall, intrusion prevention and detection systems (IDS,IPS, etc), Network security, Enrollment and End-User security(including PKI, encryption, etc).
- d. Another key component is the range of Enrollment applications. These will be provided through the FEPs and used for the capture and validation of demographic and biometric data at the various IRCs (whether or not there is internet connectivity as provision is made for batched processing) and end-user points.
- e. Another important component is the Biometric sub-system. This is used for both the enrollment process and the verification/authentication process. Provision is made for incorporation of the SAGEM AFIS as part of the 'reuse' policy of the NIMC,²⁵ such that if and when AFIS is upgraded it will provide an important service and capacity component.

²⁴ In December 2008, Government approved the implementation of the Phase I of the Network Infrastructure which covered fibre optic link to the NIDB for fourteen (14) government agencies, dedicated VSAT for the 37 State/FCT Offices of NIMC/IRCs and Disaster Recovery/Business Continuity infrastructure.

²⁵ The SAGEM AFIS is part of the existing ICPF infrastructure that has been designated for reuse, subject to upgrading and certain reconfiguration.

- f. Other subsystems include the Administrative system which covers Analytics and Reporting, Audit trailing, Fraud detection and Accounting applications. There is provision also for such administrative solutions to cover logistics and contact centre services both of which would involve third party service providers.

All these are woven into the NIMS process as represented below:



30

4.2 Overview of Data Security Strategy

a. Protecting Personal Information in the Database

The NIMC will ensure that it treats all personal information collected confidentially and securely in the process of developing the National Identity Database (NIDB). The consolidated NIDB and its harmonization and integration with other government agencies in the public domain require that a very high security arrangement is put in place especially in terms of provision of access for ‘end-user’ transactional purposes.

The history of identity management in Nigeria confirms the role of legislations in inducing the collection of personal information at various statutorily-backed institutions. These ‘silos of databases’ which often are stored in ‘files’ and cabinets’ contain significant misrepresentation are not sustainable, have limited usage and are procured at a cost both to the individual and the government agencies.

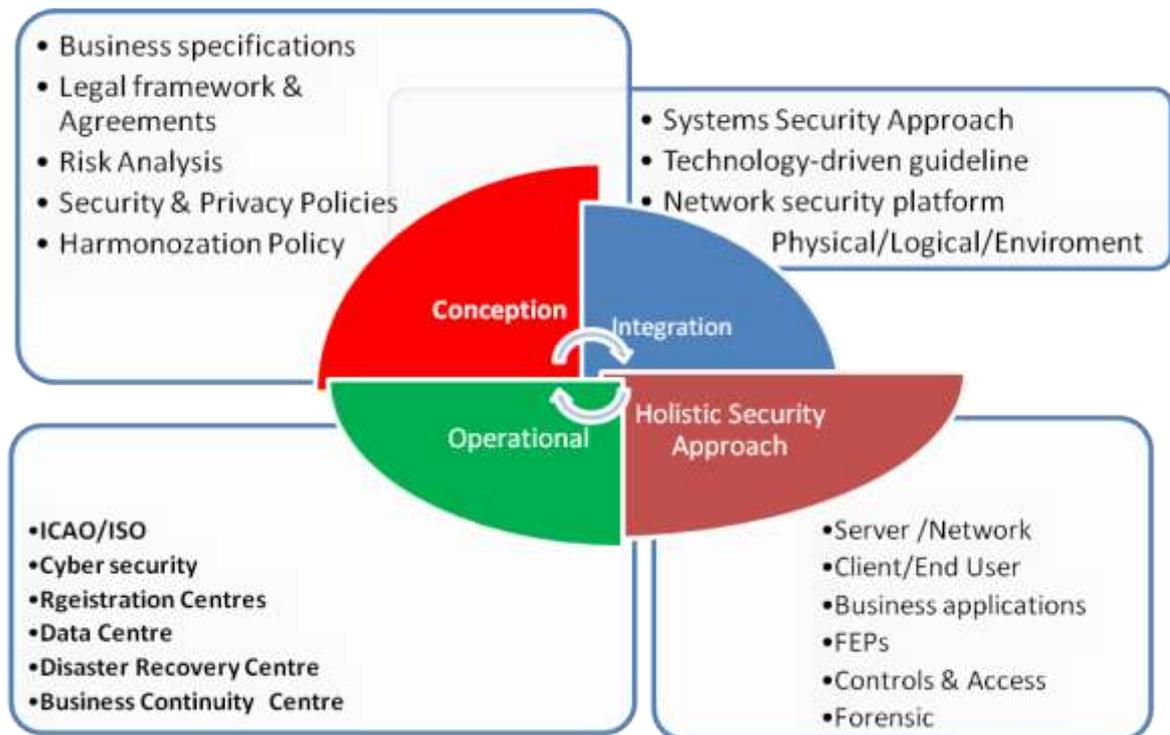
Therefore although personal information of citizens and legal residents are in one way or the other available in various forms, including biometric information, there is no secure and accessible centralized identity database, an important feature that distinguishes the NIMS from previous efforts. In most cases citizens provide these information and do not bother how they are subsequently treated and willingly provide the same information again each time the service is required and or consumed.

The 'privacy rights' are often times forgone in the quest to obtain the benefit and or value being sought. The fact that virtually the life cycle of every individual at some point requires 'registration' and such registration activities present opportunities for misrepresentation underscores the need for the development of a central identity database, a key component of the NIMS.

The NIMC Database will contain personal information of citizens and legal residents. This means that there is need for the Database to be well secured against all forms of abuse. Also the fact that the authentication and verification of the identity of citizens and residents will be done by reference to the NIMC Database further underscores the need for security and above all privacy.

b. Technology Solution for Protecting Personal Information

The NIMS under the NIMC would adopt appropriate technology to protect the privacy of individuals in a conscious response to the outcome of the privacy impact assessment study and privacy policy. In this respect a privacy policy has been developed based on the study and assessment of the privacy risks inherent in the NIMS. It is on the basis of the privacy risks that decisions on the technology solutions are taken.

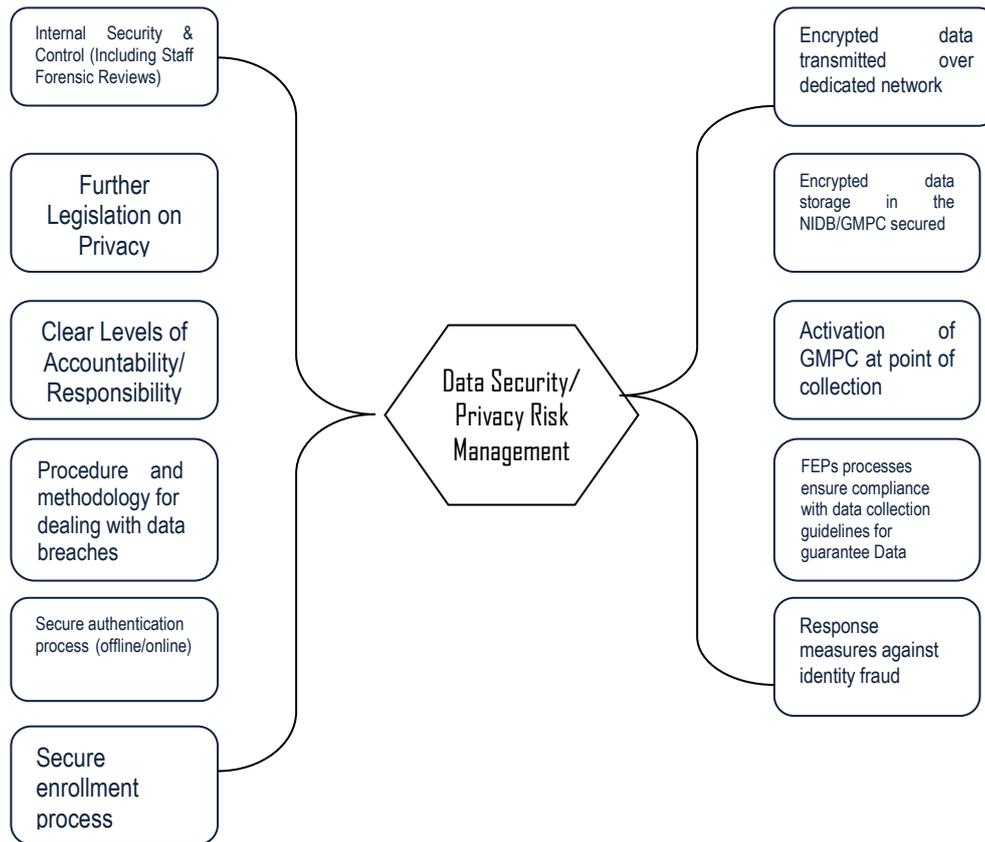


The technology and business rationale is fairly well developed: All enrollments into the Database is predicated on the concept of linking an individual's personal, identifying information to a unique national identification number as provided for in the enabling Act that set up the NIMC. This 'identity' is a verifiable identity and can be used for various transactions (with non-repudiation features which can be electronically stored) because there is an accessible, secure identity authentication and verification system in place to enable the confirmation.

The value of this 'interacting identity' is better appreciated by reference to the various uses to which the unique identification number can be put – dealings with Government Agencies, Business Entities and in particular Banking Institutions and Financial Transactions. Efforts will however be made by the NIMC to ensure that the scope of personal information is both optimal and manageable to enhance the value and facilitate privacy risk management.

In this regard the NIMC has developed a data dictionary and data modeling structure that would facilitate the use of the database in the way envisaged in Section 27 of the NIMC Act such that the database would contain the biometric information specified in the Act but with provision for future additions (from facial recognition to iris). There is provision for updating of some aspects of personal information (with historical record tracking of updating/changes). There are also some personal information fields that are not expected to change for obvious reasons, for example 'date of birth', or where the information is a key determinant for identity authentication (including sex gender which does not change), additional measures are taken to ensure a significant level of data security and stringent measures will be developed to manage implementation of changes as and when necessary.

In view of the wide range value proposition of the NIMS, the online and off-line verification and access to the database require that a strong technology-driven protection is implemented to assure individual identity. The measures adopted to ensure a high level data security is represented below:



4.3 Overview of Fraud Management Strategy

The integrity of the NIDB is a key critical success factor in the deployment of the NIMS. To achieve this two important aspects of the system require a clear policy thrust, namely the collection and processing of the data and the access and use of the data.

At the policy level, the primary objective of the NIMC is to provide a secure and accessible database and issue unique national identification numbers to enrollees in such a manner that a very high reliance is placed on the various services of the NIMC by all stakeholders. The issues of security and fraud management are therefore addressed from this perspective in the NIMS Technology.

NIMC partners (FEPs) are to comply with document security and fraud prevention and detection standards and techniques. The focus however will essentially be on the 'identity fraud' (as distinct from document fraud). This will be done by ensuring that the biometric enrollment process at the various registration centres will allow an individual's biometrics to be captured and used once in the NIDB. The high point of the management process would be that instances of false or misleading use of bio-data

would mean that the individual will live with it for life (except where tracked changes are allowed – marital status related, address related, etc).

The challenge of managing document fraud, that is, the use of misleading or forged documents to substantiate the entry of incorrect personal information, is an operational responsibility assigned to the Front End Partners (FEP). As a long term measure to strengthen the integrity of the NIDB, NIMC will focus on the adoption of enhanced security documents across various sectors of the economy over time. An appropriate starting point would be the use of security document in the issuance of secure birth and death certificates.

Given the role of the FEPs, specific fraud scenarios have been deliberately edged against in the process of implementing the global security approach described above. These include the following:

S/N	Risk edged against	Risk Management Framework
1	Where an individual presents himself/herself for enrollment into the NIDB, with no or wrong primary source document preparatory to obtaining the NIN.	Trained interviewer uses various techniques to confirm status. Limited discretion allowed and supervisory levels exist for waiver/enforcement of required document to discourage misrepresentation and yet ensure no one is turned back. If applicant is 'passed' for enrollment irregularly the verification will be queried for a second check.
2	Where an individual presents himself or herself for enrollment a second time in a different name with or without using another set of primary source document.	The on-line verification will enable the rejection of the enrollment and a report will be sent to the 'flagged details' watch list for intelligence monitoring.
3	Where an individual impersonates a deceased person with or without documents.	Trained Interviewer and or Registration Officer conduct preliminary checks using available 'Death Register' on locality. Where applicant is 'passed' for enrollment, he/she will acquire the deceased's identity for life as a change will not be possible. (In the case of females, the change in certain demographic (name) details will be possible/tracked following a predetermined process).
4	Where an individual presents himself/herself for enrollment as another existing	If the individual is 'passed' for enrollment and the existing person subsequently presents himself/herself for enrollment or gets to know

	individual.	and reports, this will trigger an inquiry and resolution process.
5	In the event that an enrollment is completed and the individual is issued with a Smart Card and subsequently presents himself or herself for a second Card in his or her name or in a second name.	Previous Card will be cancelled/deactivated and a new one issued on payment of the required fee. Action is flagged or tracked. Where the request is for a Card in a second name, request is rejected and the individual/action is put on watch list and tracked.
6	Where the de-duplication functions wrongly.	Specific verification requests can be entertained. Quality checks will also triggered to next levels of biometric verification
7	Where the individual presents himself or herself as having committed a deliberate misrepresentation of bio-data (confession).	Proper legal procedure will precede any activation of acceptable operational process to 'rest the NIN' and changes would be tracked/flagged. Systems-wide and national inquiry will be triggered.

As a deliberate security policy, the NIMS technology provides for tracking of attempts at a 'reuse' of existing biometric information for a fresh enrollment. This and similar mechanisms are part of the security architecture of the NIMS technology to address criminal tendencies, enhance the integrity of the system and ensure optimum service delivery envisaged by the NIMC under the NIMS.

5.0. Front End Partners (FEPs) and Enrollment Strategy

5.1. *The FEPs and Service Implementation*

Implementation of the NIMS is predicated on collaboration with the private sector in a Concession arrangement over a ten (10) year period (known as the Front End Partners, FEPs). The NIMC has appointed two consortia as FEPs²⁶ for the 'service implementation' defined as:

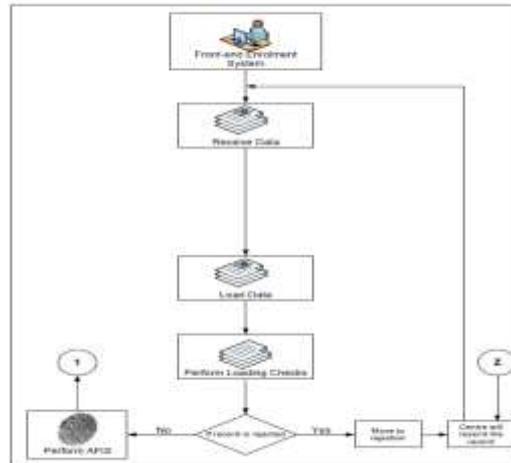
- a. Personal information data capture, (ten finger prints, face, digital signature and Iris scan);
- b. Personalization and issuance of GMPC (Smart Cards);
- c. Deployment of Card Acceptance/Access Devices (CADs); and
- d. Provision of end-user authentication and verification service infrastructure.

These four categories of services define the front end component of the NIMS.

The FEPs will implement the approved process of collection treatment and batching of personal information which is then transmitted to the NIMC Data Centre for processing and issuance of the NIN. They will implement the 'process definition' at this level, around the enrollment software provided by the NIMC and the process is subject to the approval of the NIMC.

²⁶ The FEPs are currently involved in the business of identity-related services and so have some significant experiences in the sector. They are expected to invest in the establishment and operation of IRCs across the country and in designated countries abroad, deploy card acceptance devices and issue smartcards.

Front-End Enrollment System



The NIMC certified Enrollment Application will be deployed by the FEPs and provides the basis for data capture and subsequent transmittal of the data in the required format that triggers the enrollment submission request (de-duplication etc) before the issuance of the NIN. It describes the enrollment workflow including pre-on-line enrollment, and submission processing conditions. The applications include provision for service exceptions to normal workflow, logistics arrangements covering such things as letter printing, delivery, emailing and text messaging functionality.

To ensure proper verification before enrollment, a list of acceptable primary source documents will be available in each IRC, as prescribed by the NIMC, which will be used as ‘introducing document’²⁷ Also the authentication interfaces of the existing database will be used to confirm applicants for registration and enrollment.

The FEPs are authorized to have sub-licensees as a strategy to facilitate ‘service implementation’ towards the achievement of full coverage and provision of the platform for regular updating of the NIDB. These sub-licensees report to the specific FEPs who shall be responsible for their service implementation.

Upon completion of processing the encrypted data is sent to the Card Personalization Centres managed by the FEPs for the Smart Card personalization.

²⁷ FEPs’ responsibilities are spelt out in the ‘Service Implementation’ of the Concession Agreement.

It is also the responsibility of the FEPs to activate the Cards at point of collection by the recipient whose fingerprint can activate it, as a further security measure.

5.2. *The Enrollment Process and Issuance of the NIN*

Section 18 of the NIMC Act provides for mandatory registration of citizens aged sixteen (16) years and above. The Act also provides for the registration of a citizen at birth, the issuance of a GMPC and the Unique National Identification Number. (NIN). In view of the provisions of Section 27 of the Act, together with Section 18, it is expected that citizens will be encouraged to participate in the exercise in particular, for the purpose of obtaining the NIN which is the primary objective of the registration and enrollment.²⁸ The objective therefore is to ensure that every registrable person as provided for in the Act is covered by the exercise. The NIN becomes a personal number, unique to the individual which he/she obtains at enrollment and uses for life as a dependable means of asserting his/her identity.

The enrollment process is initiated by the citizen appearing at the designated location²⁹ as provided for in Section 18 (1) of the NIMC Act to be enrolled (provide demographic data and permit his/her biometrics to be taken) with supporting document in the form of a 'primary source document'. After ascertaining that the person is suitable for enrollment, the Registration/Enrollment Officer accepts the application and the request is submitted following the process prescribed (either alone or in batches) through the FEPs' consolidation centres and dedicated network to the NIDB.

At the NIDB, a de-duplication check is run by comparing the enrollee's biometric and demographic data submitted with the existing records in the NIDB to ensure that he/she has not been enrolled before.³⁰

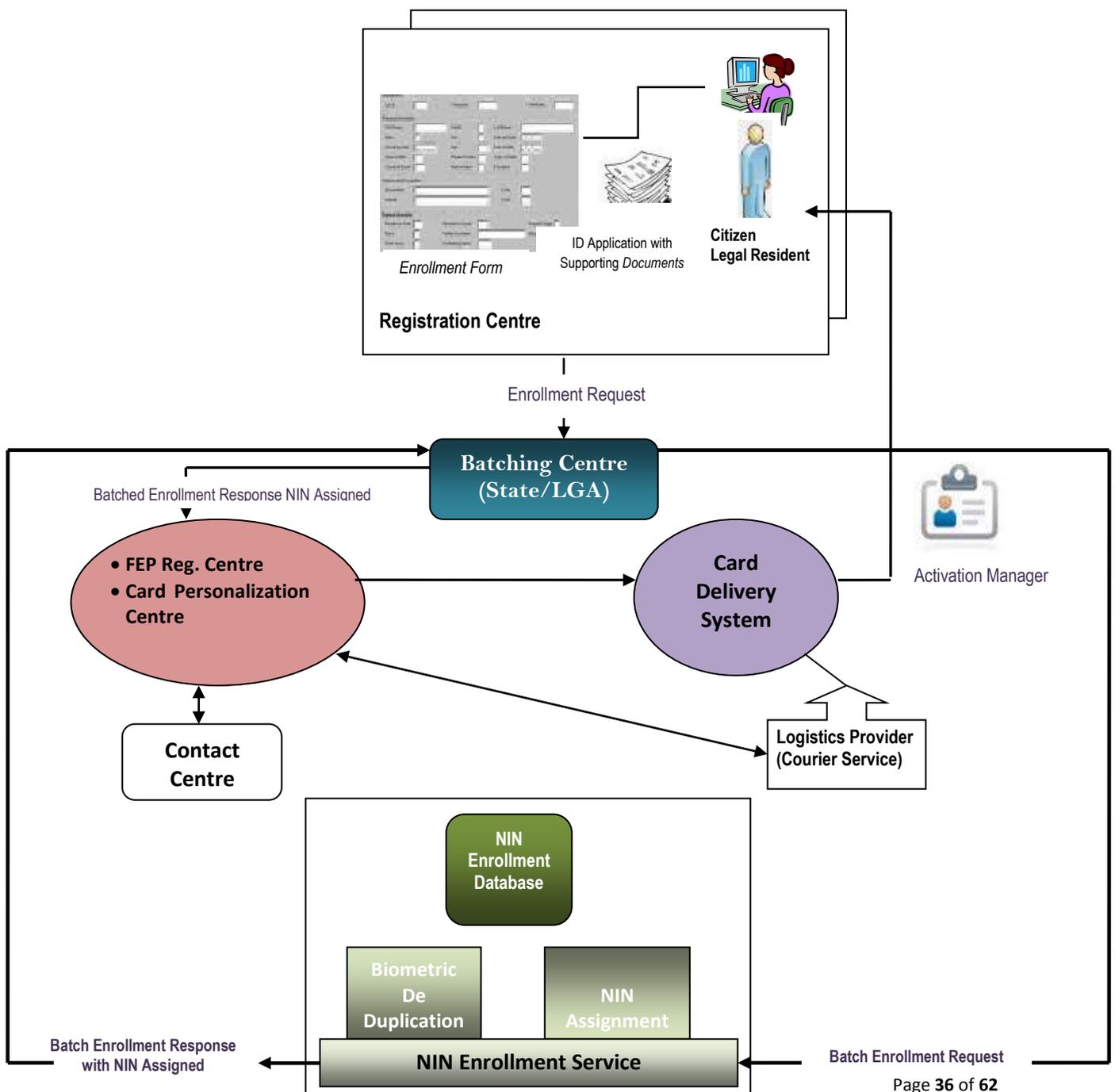
²⁸ The NIMS implementation model is predicated on the development of a national identity database or the central identity repository based on de-duplication and issuance of the NIN to each enrolled individual. This becomes the core of the digital platform required for the value proposition underlying the NIMS, one of which is the issuance of the Smart Card once the NIN is issued to an individual. The NIN is the 'glue' that will bind all databases under the harmonization and integration scheme.

²⁹ Designated locations (IRCs) are the primary responsibility of the FEPs. As part of their 'service implementation obligations they are required to set up, operate and manage IRCs across Nigeria (as mobile, temporary and or at permanent locations).

³⁰ The de-duplication and full coverage model of the NIMS ensures that those seeking to enroll more than once would be detected, stopped and tracked, it would also serve as a deterrent to falsifications. Once enrolled, even in a false name, the individual lives with it for life.

Once the process is completed a NIN is assigned and the data encrypted and sent to the FEPs Card Personalization Centre where the Smart Card is personalized and issued according to the prescribed process. The particular IRC at which the citizen (or legal resident) enrolled will receive a NIMC Response Form (NRF) containing the enrollment detail of the applicant and the NIN which confirms to the specific FEPs' IRC and the applicant that the process has been successfully completed (or not, in which case the reasons will be stated therein).

The NIN SYSTEM



5.3 The National Identification Number (NIN)

The NIN is a set of non-intelligent numbers randomly generated to provide the 'useable' component of the unambiguous and unique identification of an individual using his/her biometric and demographic data. ***The NIN is the symbol of the key deliverable of the NIMS based on the NIDB which it will use to provide authentication and verification services at enrollment and subsequent uses of the NIN.*** Once the NIN is assigned the FEP is notified as well as the applicant. The NIN is the ultimate outcome of the NIMS process encapsulated in the phrase 'ENROL ONCE AND BE IDENTIFIED FOR LIFE' It is only after this is achieved can a Smart Card be personalized and issued to a citizen or legal resident.³¹

5.4 Implementing the Use of the NIN

Enrollment under the NIMS is mandatory. Also in Section 27 of the NIMC Act Government has provided for the mandatory use of the NIN for specific transactions and from a date to be determined by the NIMC it shall become unlawful for anyone to transact in such businesses without the use of the NIN. The NIN is for the authentication and verification of the identity claimed by an individual and should be proven at the request of the individual/firm or person requiring the proof. The authentication and verification infrastructure works largely on the basis of the NIN and the Database it relates to. Accordingly, this infrastructure and the related services would be provided and managed by third parties.

5.5 Managing the Enrollment Process to Ensure Full Coverage

To ensure full coverage the FEPs are expected to establish IRCs in at least every State and Local Government Area, that is a total of eight hundred and eleven locations. Clearly this number would not be enough and the expectation is that mobile registration centres (MRC) would be established to cater for special areas and locations, like the Niger Delta Region and the hinter lands of the North.

The NIMC is conscious of the need to ensure that commercial reasons do not undermine the sound objectives of the NIMS and has therefore provided for FEPs to be able to enter into sublicensing arrangements with sub-contractors who must meet the same criteria set by the NIMC for the FEPs.

In the case of children, their biometrics will not be taken for children aged less than sixteen (16) years as provided for by law. Their enrollment will be attached to the NIN of their parents until they attain the age, at which time their biometrics will then be

³¹ With the NIN other services can be rendered even without a smart card.

taken. It is anticipated that when the Child NIN System is deployed in collaboration with the National Population Commission (NPopC), it will become a feeder system into the NIDB, allowing for total identity management from birth to death.

Another category of enrollment challenges that the NIMS has provided for concerns cultural barriers and the differently-abled persons. It is expected that by significant media and educational promotion cultural barriers would be 'broken down'.³² The challenge of facial tribal marks is an important reason why the facial recognition methodology is deferred. However it is expected that differently-abled persons will be enrolled with the disability provided for in the process.

A deliberate strategy of ensuring the full coverage of the entire population in the NIDB is the effort of the NIMC on the harmonization and Integration Policy. The policy will ensure that other government institutions that collect data do so in the manner prescribed by the NIMC for the FEPs so that with time the entire population will be covered³³.

5.6 Updating the NIDB

The NIMS enrollment process provides for the scanning and documentation of the original evidence submitted by the applicant before enrollment as this would be the basis for ensuring that falsifications can be better traced and initial proof of identification can be well managed.

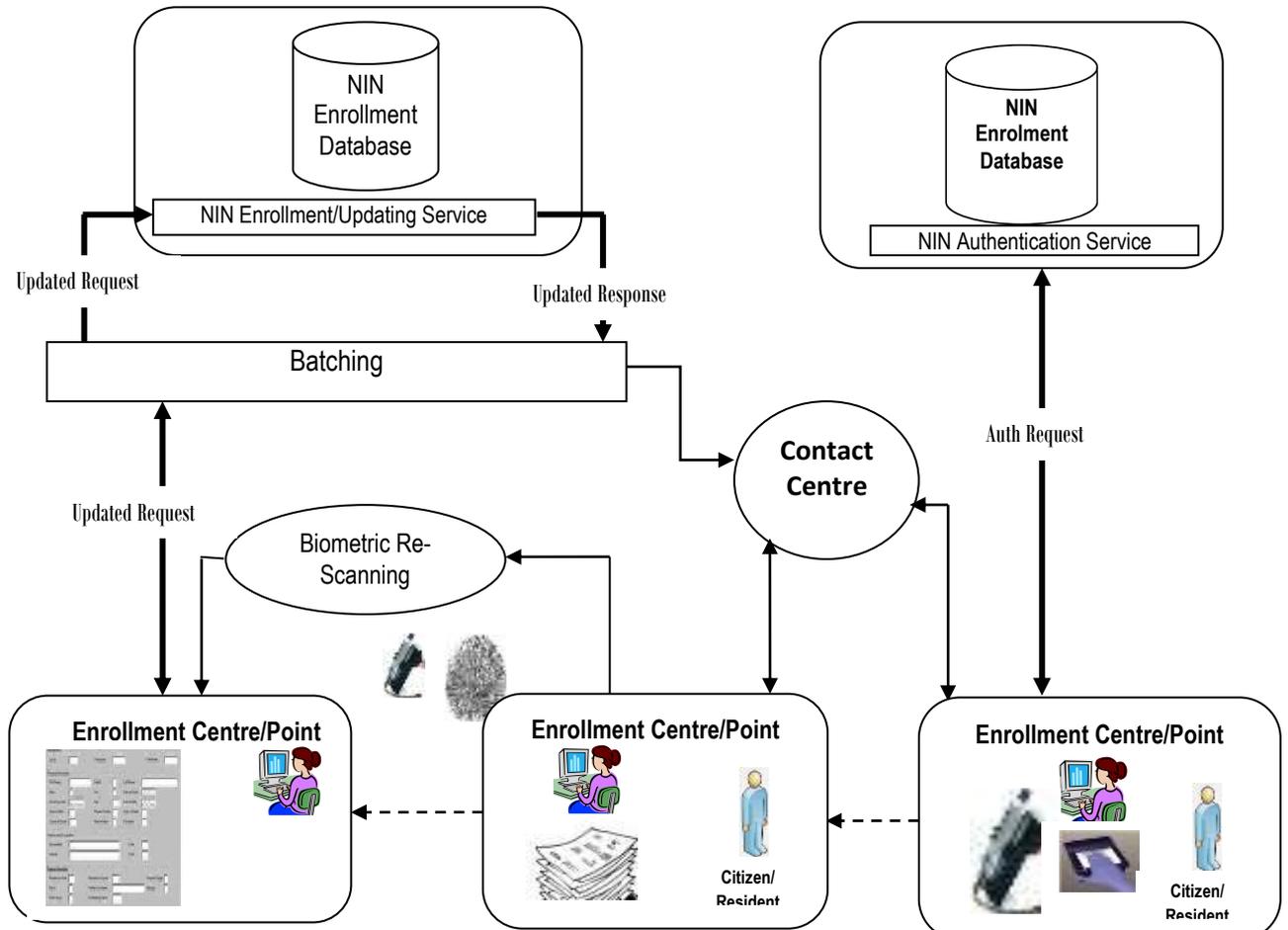
Beyond this, further updating of information in the NIDB which will be through the IRCs will be done following the prescribed procedure for information updating.³⁴ Every request for change shall be accompanied by the relevant evidential document which will be scanned and stored after which a biometric confirmation will be undertaken before the change is admitted for processing. At the completion of processing the applicant would be communicated. In the same manner as if he was enrolling for the first time. There will be provision for initiating updating of the NIDB by the individual in specific instances.

³² Section 18 (2) of the NIMC Act provides for any person having charge of any person to whom the registration issues affect, to cause such person to be brought before the NIMC for registration.

³³ These institutions include the Nigerian Communication Commission (NCC), Federal Road Safety Commission (FRSC), Federal Inland Revenue Service (FIRS), Nigerian Immigration Service (NIS), Independent National Electoral Commission (INEC), educational institutions, to mention a few.

³⁴ There are stringent criteria for updating certain demographic fields especially date of birth and sex gender. Any changes and or updates and tracked in the system including errors from the field. The biometrics will be regularly updated every five (5) years for children (from 5years up to 18years) and every ten (10) years for adults.

Updating the NIDB



3) Registration Centre will Batch and submit update request using client application

2) Applicant will submit demographic/biometric update form

1) Applicant to authenticate self

5.7 Other Enrollment Issues Considered

It is expected that the FEPs will commence pilot enrollment in the last quarter of 2010 and that within thirty months (30) from the commencement of enrollment in January of 2011, the NIDB will have one hundred million (100m) enrollments. **By that time the NIMC would have issued 100m NINs.**³⁵

There are three (3) major challenges in the enrollment process which includes the management of vital statistics (deaths and births), the speedy and professional deployment of cost effective IRCs and the dearth of skilled workforce for enrollment of biometrics especially iris scan. In this respect the NIMC has set up a special committee, following the outcome of the Harmonization Study, to work with the National Population Commission (NPopC) to develop a template for collaboration so that the automated processes of managing vital registration would become useful to the enrollment process under the NIMS.

The registration of the child at birth (and deaths) and inclusion of the NIN in the birth certificate would therefore go a long way in helping to identify the child as he grows and also in managing the NIMS process in future when the child presents himself for biometric enrollment³⁶. In this way also the attempt at full coverage is made more realistic. This issue presents a lot of challenges that the Harmonization and Integration Implementation Committee and the special committee on NPopC/NIMC will address in more detail.

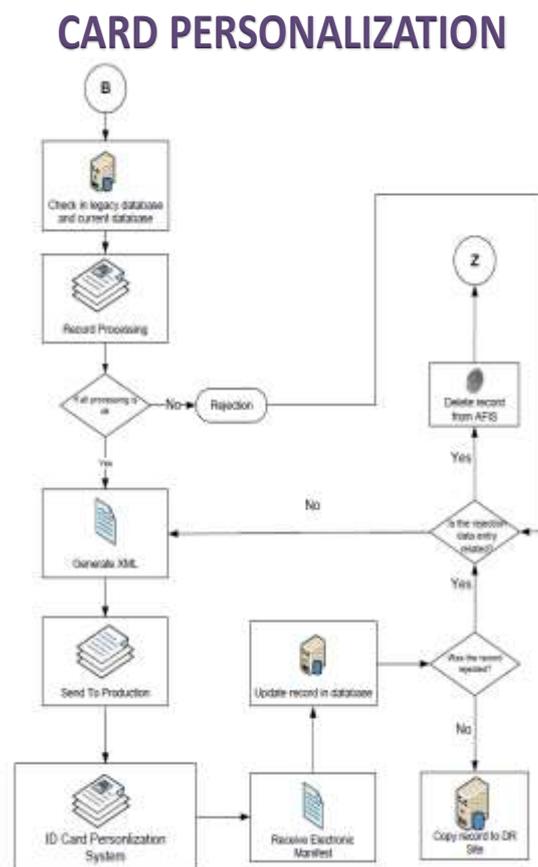
The target is that within fifty (50) months the entire Nigerian population will be covered such that only deaths and births will be focused on (and legal residents as they come in) to sustain full coverage.

³⁵ The NIMC proposes to track enrollments across the country using a GIS Internet based visual reporting system as well as the use of a third party operated contact centre to manage the application and service process as an important tool for managing the customer satisfaction measures.

³⁶ Accordingly while the child's biometrics will not be taken, since it is unstable, it is the parent's biometrics that will be used for identity authentication and verification until the prescribed age of 16 years is attained and the biometrics collected at that time (subject to a proposed amendment of the Act to allow biometric enrollment from age 5.)

5.8 Smart Card Personalization

The FEPs will personalize the Smart Cards to be issued to the enrollee using the encrypted data which is provided by the NIMC. The Smart Card will contain the prescribed demographic and biometric data prescribed by the NIMC to facilitate verification and authentication of identities as well as interoperability amongst government agencies and private sector institutions on payment solutions. The applicant is required to collect his/her Smart Card personally at which time certain functionality on the Card may be activated.³⁷



³⁷ The activation may follow a typical pattern known to Smart Card related transactions. Distribution is expected to be undertaken by logistics service providers. Currently, NIMC is exploring plans to engage courier services including NIPOST.

6.0 Back End Partners (BEPs) and the NIMS Core Value Proposition

6.1 The BEPs and Service Implementation

The initial solution proposed for the identity management system for Nigeria intended that the NIDB will be managed by the private sector with the ultimate objective of issuing GMPCs. Government realized that given the sensitive nature of the NIDB, it is both politically inexpedient and against the public interest, from a national security point of view to leave such an asset in the hands of the private sector not later than necessary.

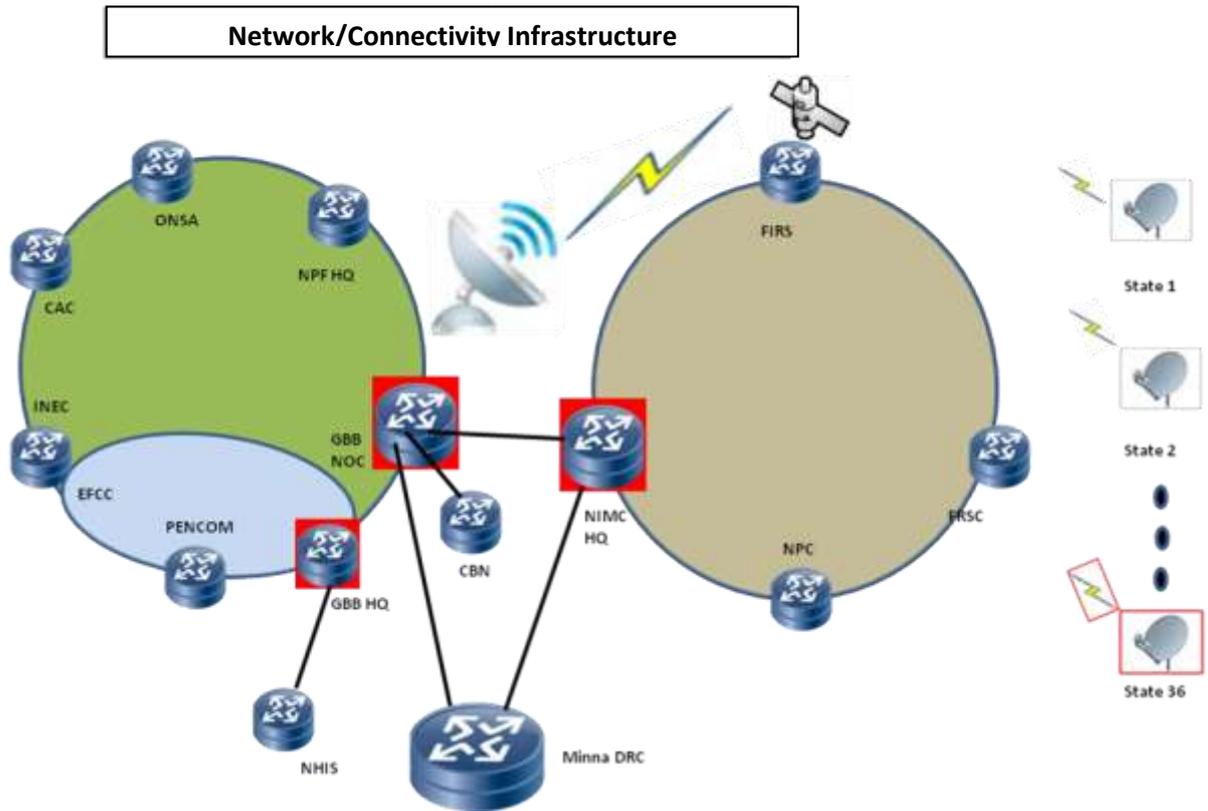
This informed Government's decision and approval in 2007, of the implementation strategy of BEO and FEO. The NIMC has three (3) back end partners who are essentially technology service providers (contractors) to render specific services as follows:

- a. **Galaxy Backbone Plc**, which is a government owned company, to provide network and connectivity infrastructure backbone most of which are dedicated, build a Disaster Recovery Centre, and host the business continuity interface for the NIMC.

The services to be provided by Galaxy include the following:

- i. The provision of dedicated Metropolitan Fibre Optic Network (with redundancy) connecting at least fourteen (14) Government establishments whose services require the authentication and verification of identities most frequently³⁸;
 - ii. Provision of a dedicated VSAT connecting the State Offices of the NIMC (which also host IRCs) to the NIDB at the Head Office including the bandwidth and maintenance services;
 - iii. The Disaster Recovery Centre and the hosting of the 'Heart Beat' and associated Business Connectivity Infrastructure
- b. **Interglobal Ltd** a local technology service provider which is an IBM partner to provide Enterprise Servers and Storage solutions for the Disaster Recovery Centre and the 'Database Mirror' and storage facilities;

³⁸ These institutions, some of which include FRSC, FIRS, CAC, NIS, ONSA, CBN, NCC, INEC, NPS, Pencom, NHIS and EFCC, have in one form or the other a database or are in the process of building one. The NIMC has encouraged the adoption of its standards to ensure seamless harmonization and integration towards interoperability.



- c. **National Database and Registration Authority (NADRA)** as Systems Integrator and provider of customized software applications and solutions³⁹. The services include the following:
- i. Provision of systems integration services for the entire system;
 - ii. Provision of web based verification service application;
 - iii. Provision of systems integration services for AFIS/ABIS, Card Personalization and other applications;
 - iv. Database setup and initial management;
 - v. Maintenance and operational support and training.

The service implementation scope for each of these technology service providers extend beyond the establishment of the process and includes maintenance management.

The NIMC is responsible through the services of these partners for the backend component of the NIMS.⁴⁰

³⁹ The NADRA will provide certain third party software from IBM, L1 Solutions and Oracle, amongst others.



⁴⁰ A Service level and operational Management Agreement will guide the relationships between NIMC and the Service Partners.

7.0 Overview of Service Management Processes

The service management processes within the NIMS aptly captures the essence of the project, its technology, architecture and the need to ensure an indigenized approach to a sustainable management of the project. The major components of the service process which are briefly discussed below, include 7.1, 7.2 to 7.6.

7.1 The NIMS and Its Applications

The NIMS Service structure consists of two main categories of applications: the core applications and the supporting applications. The former includes the enrollment and authentication applications services while the later includes the applications required for administration, reporting and analytics, fraud detection interfaces with FEPs, logistics providers and more importantly, the security management system and processes and also the proposed contact centre operators.

7.2. The Enrollment Application

NIMC certified Enrollment Application will be deployed by the FEPs and provides the basis for data capture and subsequent transmittal of the data in the required format that triggers the enrollment submission request (de-duplication etc) before the issuance of the NIN. It describes the enrollment workflow including pre-on-line enrollment, and submission processing conditions. The applications include provision for service exceptions to normal workflow, logistics arrangements covering such things as letter printing, delivery, emailing and text messaging functionality.

The NIMC through the registration process will enable the fair determination of the estimated usage (primarily for the provisioning), degree of multiple locations of deployment of authentication devices, the structure of the billing relationship, the data required for billing⁴¹, the nature and range of service platforms to be deployed by the NIMC and the planning of the service platform generally⁴².

⁴¹ The Payment collections arrangement will be the responsibility of the FEPs with the 'collecting banks' solution. The financing arrangement provides for a lien over the revenue streams and a role for the NIMC.

⁴² The NIMC will specify the BIOAPI to ensure manageable flexibility in the adoption of enrollment solutions and also accredit specific equipment for API activation and will similarly ensure the adherence to the prescribed standards.

7.3. The Authentication Applications

The Authentication Application provides the Authentication and Verification Services. This Service will allow Government Agencies, private sector organizations, the international community and Nigerian Missions abroad and other domestic or international agencies and commercial transaction processes to authenticate and verify the identity of Nigerian nationals (in real-time and off-line).

The NIMC distinguishes between the end-user institution or organization that is the 'Authenticator' that uses the NIMS platform to authenticate and verify an individual and the 'Authentication Infrastructure' which is part of the NIMS.

The Authenticator may use demographic data and/or biometric data in addition to the NIN under the prescribed authentication platform that provides him/her with the necessary assurance for the transaction. To facilitate the deployment and management of the provision of this service, all Authenticators are expected to register with the NIMC.

This service can be accessed via the web or at a 'match-on-card device point (MOCD). The typical pattern is for an authentication request to be made either a demographic, biometric, simple, multiple or advanced authentication method. Each case is adequately supported by the application. Where the NIN is submitted it is used for the 1:1 match for the individual's record, with a live scan of finger print, in the case of the MOCD, while in the case of the web based verification, it is matched against the individual's (biometric) information that is found in the NIDB at the Data Centre at the Head Office of the NIMC.

7.4 Biometric Solution and Provisioning

The biometric solution to be deployed for the NIMS will be scalable, but for the immediate and medium term requirement, is planned to accommodate up to 150million enrollments. The service will be managed by Nigerians. In view of the benefits and based on the need to incorporate existing infrastructure a multi-vendor, multi-modal biometric strategy will be adopted.

This requires the selection of a second, Biometric Solution Provider (BSP) to design, supply, install, configure, test, commission, maintain and support the biometric components of the NIMS. The short term plan is to adopt the Automated Biometric Identification System (ABIS) to run multi-modal de-duplication with mostly fingerprints and facial image (and later iris).

The components of the biometric solution include the following:

- a. Automated Biometric Identification Subsystem (ABIS), which will be used in the Enrollment Server as a biometric de-duplication solution. It will also be deployed in the Authentication Server for verification. The ABIS will maintain its own database of non-proprietary fingerprint and facial (subsequently iris) image templates for de-duplication to facilitate responses to fingerprint accompanying verification requests. The process would comply with ISO/IEC 19794-2:2005 format for fingerprint minutiae files and future standards when available.
- b. As earlier indicated a multi-modal de-duplication will be adopted with two BSPs. In view of the harmonization and integration mandate of the NIMC, the BSP will work with the NIMC to provide further specifications within ISO/IEC 19794-2:2005 to promote interoperability towards achieving the harmonization and integration objectives with stakeholder agencies and the private sector, including the financial sector.
- c. The FEPs will be required to adopt a Multimodal Software Development Kit (SDKs) in the enrollment process including manual checks for exception handling and for duplicates and an analytics module. Provision will be made for monitoring and analysis, signal detection, image selection, segmentation, image fusion, quality analysis, image pre-processing, feature extraction and comparison score generation for fingerprint, face modalities (and iris image from the year following technology-refresh under the FEPs concession Agreement).⁴³

Because of the high level of de-duplication task to be performed, the NIMS Enrollment server will utilize a multiple modal functionality biometrics– fingerprint and face photograph and iris. However only fingerprints will be used now.

In Nigeria, the common nature of most elements in the bio-data, especially first and surnames make demographic information an unsuitable for performing the filtering exercise during the de-duplication process. Furthermore to address this problem in the process, every de-duplication request will be issued a de-duplication reference number (DRN) aside from the biometric and demographic data. For every occurrence of duplicate enrollment found, the ABIS passes back the DRN of the duplicates and the scaled comparison scores upon which the duplicate finding was based. The scaled fusion score returned with each duplicate found will have a range of [0, 100], with 0 indicating the least level of similarity and 100 as the highest level of similarity. The NIMC will specify the interaction between the FEPs and it and the ABIS.

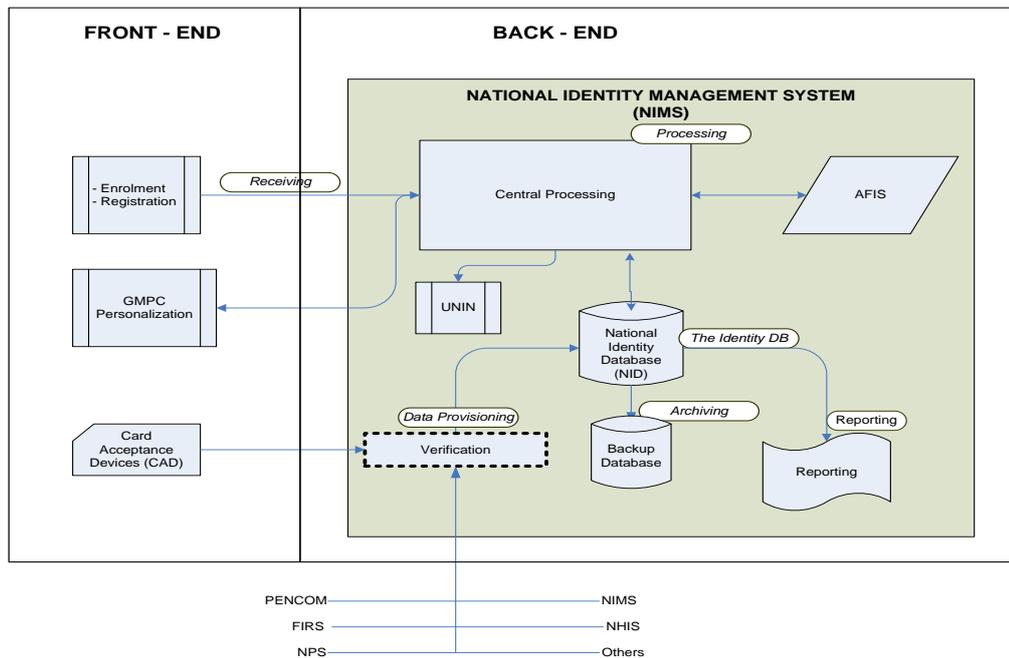
⁴³ A detailed presentation on the biometric solution is contained in a specific document for that purpose which is developed based on the agreements with the BSP.

Provision is made for routing and mediation, delivery, fault tolerance and load balancing, open standard based messaging (AMQP) using open source Rabbit MQ, transparent connectivity to analysis and system monitoring modules of NIMS applications and support of standard XML data format have all been incorporated.

7.5 Verification Subsystem of Authentication Server

The biometric verification module provides verification within the authentication server which is capable of 1:1 verification comparisons of enrolled references with incoming ISO/IEC 19794-2-compliant fingerprint, (later face and iris images and ISO/IEC 19794-2 compliant fingerprint minutiae sets without proprietary extended data.

As earlier noted, the technical architecture of the NIMS is structured to achieve the primary objective of assured data verification, de-duplication and authentication that substantially guarantees privacy in a multi-access environment. The NIN will be the anchor that will enable the attainment of this objective in the context of the service architecture below:



7.6 Provision of Authentication and Verification Services

The NIN system is Central to the NIMS and the core service of identity authentication. The NIN will be accepted to the extent that it is able to check identity theft, eliminate

incidence of duplicate and or multiple identities amongst others. The challenge therefore is to facilitate the adoption of the NIN for identity verification purposes.

To meet this challenge, the first thing is to ensure the effectiveness, efficiency and availability of the service across Nigeria.⁴⁴ The NIMC will appoint third party service providers who will vendor and manage offline and online access and use of the NIN to confirm identity within the NIN system. Through this approach, the use of the NIN can become effectively adopted at every point of transaction in both the private and public sectors.

Deploying it for specific social programmes and transactional relationships especially in the financial sector and the designated transactions identified under Section 27 of the NIMC Act will also encourage its early adoption.

The efforts of the Implementation Committee on the Harmonization and Integration of databases in the public sector will help develop a uniform platform and standard to enable the rapid adoption of the NIN.⁴⁵ It also means that access to public services can no longer be denied citizens due to an absence of a proper proof of identity.

The NIMC is the only institution authorized by law to provide the NIN and accompanying authentication service. The provision for updating the database makes the NIDB 'current' and the mandatory use of the NIN will encourage enrollment which will in turn encourage further turnout for enrollment.

The NIMS envisages various forms of authentication depending on the circumstance, and or equipment available and medium (offline and online, card, etc). The NIMC is set on making the two main categories available through third party management as follows:

- a. Offline authentication and verification of identity which is similar to the current form of identity authentication based on the Smart Card that will be issued. Here what merely happens is a photo match authentication where the photo on the Smart Card is compared physically with the Cardholder;
- b. Offline biometric authentication and verification of identity which is done by comparing the scanned fingerprint of the cardholder with the biometric stored on the Smart Card issued by the FEPs. The assurance level here is better than in the previous case and usually it is a match-on-card that is done using a CAD.

⁴⁴ In spite of the mandatory use by a provision in the NIMC Act, unless it is readily available and easy to use, the NIN will not be widely accepted.

⁴⁵ It is one thing to ensure full coverage and another to ensure the active use of the database for identity confirmation through the use of the NIN.

- c. Online authentication and verification will be provided at three (3) levels:
- i. Online biometric authentication whereby the biometric of the NIN holder and demographic and biometric details are compared with that in the NIDB;
 - ii. Online biometric authentication can also be done with only the NIN holder's demographic details being compared with the one in the NIDB; and
 - iii. The third type is where the NIN holder's biometric detail alone is used to compare with that stored in the NIDB.

The offline/online authentication service is key to the sustainability of the NIMS in the sense that the partnership with the private sector is predicated on the projected revenue streams to meet investment expectations and manage the NIMS system on an ongoing basis.

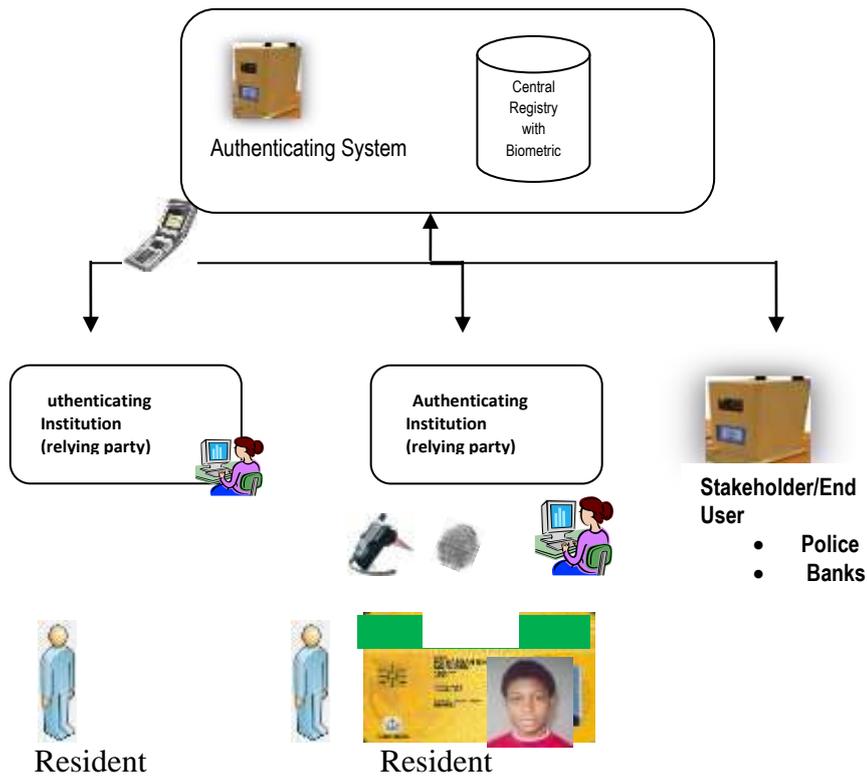
The identity confirmation service will take the form of the end user requiring the confirmation obtaining from the individual his particulars- NIN, Card, biometrics, name and a few other demographic details as may be necessary, with which the request is made and a confirmation is received in terms of a YES or NO and or matched or rejected (depending on the platform used). A fee is chargeable⁴⁶ for the service and the range of transactions over which such verification services would be utilized has already been identified in Section 27 of the NIMC Act⁴⁷.

⁴⁶ The fees structure shall be agreed with the FEPs and other service providers so as to encourage adoption and usage of the NIN and sustainability of the project.

⁴⁷ The Act provides in the same Section 27, for the expansion of the list by the NIMC and stipulates that from a date to be specified by the NIMC, the provision shall become effective with the possible sanctions that can be imposed also indicated.

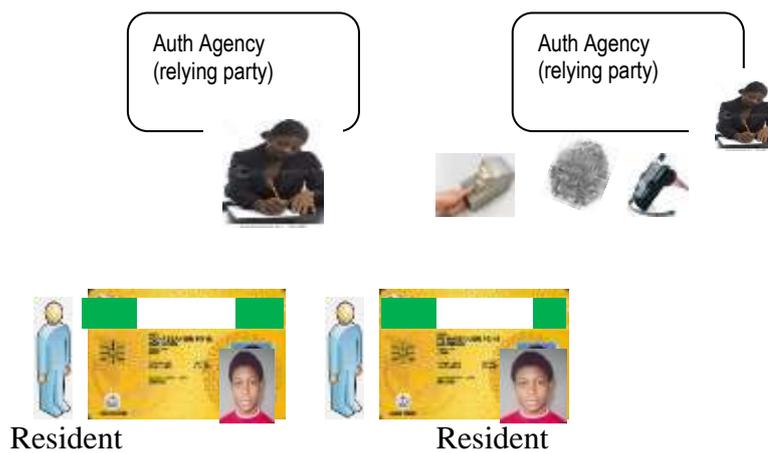
	Online		
Authentication Levels	Compare NIN and demographic data online	Compare biometric on server against finger scan	Programmatic demo/bio Authentication using APIs
Method of Authentication	Demographic Authentication	Biometric Authentication	Demo/Bio Authentication

Online Authentication Using NIN System



Offline		
Authentication Levels	Compare photo on card with card holder	Compare biometric on card with finger scan
Method of Authentication	Photo Match	Biometric Authentication

Offline Supported by CADs



Transactions already identified and the proposed fee structure includes the following:⁴⁸

S/N	Type of Transaction	Proposed Fees	End User	Remarks
1	Issuance of International Passport	N500.00	Nigerian Immigration Service	Mandatory use of the NIN.
2.	Opening of Bank accounts	N500.00	Banks and Financial Institutions	Mandatory use of NIN. Will reduce cost of KYC and cost of documenting a new account
3.	Financial transactions	N100.00	Banks and financial institutions	Mandatory use of NIN. Will reduce identity theft and identity related fraud
4.	Airline check-in	N100.00	Local and International Airlines	Required for security reasons

⁴⁸ The list is by no means exhaustive. It does not include services that would be developed around the NIN and or the Smart cards which the FEPs and other vendors might undertake.

5.	Purchase of insurance policy	N100.00	Insurance sector operators	Mandatory use of the NIN
6.	Transactions related to Land	N100.00	All relevant government agencies and institutions and those dealing in land that require it.	Mandatory use of the NIN
8.	Transactions related to the Pension Act	N100.00	Pension sector operators	Mandatory use of the NIN
9.	Credit bureau transactions	N100	Credit Bureau institutions	Mandatory use of the NIN
10.	Special payment solutions	N500.00	Financial institutions	FEPs and other vendors are free to adopt the NIN in their security framework.
11.	SIM Card Registration	N200.00	Telecomm operators, NCC and service providers in the sector	Mandatory use of the NIN
12.	Tax payment	N250.00	Tax authorities	Mandatory use of the NIN
13.	Voter's register	Free	INEC and its partners	Mandatory use of the NIN.
14.	Hotel check-in	N100.00	All duly registered hotels in Nigeria.	NIMC approve inclusion for the use of the NIN
15.	Transactions related to health insurance scheme	N250.00	All operators in the sector	Mandatory use of the NIN
16.	Accounts for Commercial transactions with chain stores and supermarkets.	N250	All credit institutions that offer credit sales.	NIMC approve inclusion for the use of the NIN
17.	Application for driver's license.	N250	Drivers License authorities	NIMC approve inclusion for the use of the NIN
18.	Diplomatic community	N150.00	All foreign missions and embassies	NIMC approve inclusion for the use of the NIN
19.	Companies incorporation and search reports on companies	N250.00	Corporate Affairs Commission and related service providers	NIMC approve inclusion for the use of the NIN
20.	Students identification and education related transactions	N200.00	Education institutions and examining bodies	NIMC approve inclusion for the use of the NIN
21.	Criminal	Free	Law enforcement	Mandatory access to

	investigations, prevention and or detection of crime		agencies	NIN/NIDB.
22.	Vehicle Registration	N250.00	Vehicle Licensing Authority	Mandatory/NIMC Approved.
23.	Card Re-Issuance	N1500	Individuals who lost their cards	It is not mandatory to have lost card reissued but payment solutions on the card makes it expedient.

The expected volume of authentication and verification requests from these sources have been projected to be in the region of one million (1m) a day. The number is expected to increase with the increasing adoption of the NIN and further enrollment of individuals into the NIDB. The revenue projections and further financial analyses underpinning the business model of the concession arrangement is contained in the respective documents.

7.7 Stakeholder/Customer Service Media

a. Stakeholder Portal

Implementation of the NIMS is based on a partnership scheme that includes several service providers, in particular, FEP. To track their activities in the sector, the stakeholder portal has been introduced to address the needs of the stakeholders, enabling them to observe, manage, analyze and perform several functions including administrative and user management functions like creation/deletion of the user records; aggregate pre-enrollment statistics (number, latency, validation issues), and aggregate enrollment statistics – number, latency, approvals, rejection reasons for the FEPs and their licensees) aggregate authentication statistics – number, latency, success / failures for authentication service providers and end-users and the tracking of individual/personal information (pre-enrollment, enrollment, and authentication).

b. Public Portal

The provision of a continuous public information sharing and management platform, which includes a grievance redress system (connected to the logistics and contact centre) and integrated into a public portal is an important innovation meant to fill a yawning gap from previous experiences and address some of the findings from the Privacy Impact Assessment study. The portal connects to roles for redressing complaints and grievances faced by citizens and legal residents in the process of enrollment and authentication. Also the public will be able to interface with the NIMC

on matters concerning the FEPs and PIDSPs as well as other stakeholders, directly and or through the contact centres.

c. FEPs System

The FEPs are expected to set up, operate and manage the IRCs⁴⁹ across Nigeria. They will perform data capture services in accordance with the concession agreement and transmit same via the dedicated network provided both by the NIMC and the FEPs. Each Registration Centre would have a complete IT infrastructure to process the data, batch and transmit to the NIMC Data Centre (for de-duplication and assignment of unique identification number) and also receive the NIN and encrypted data for the Smart Card personalization.

The IT infrastructure will enable the FEPs at both the Enrollment/Registration Centres and their National Operating Centre Control (NOCC), amongst other things, receive updates during enrollment process, upload batched demographic and biometric data and perform authentication services.

The data interface between the FEPs and the NIMC will be secured to avoid exposure to privacy risks. While it is the responsibility of the FEPs to ensure data security in compliance with NIMS standards prior to transmittal, the enrollment data flow from the NIMC Data Centre after assignment of NIN, will be encrypted to keep the confidentiality of the data being sent using the NIMC public keys.

There is a 'fraud detection' application which will be deployed to detect and reduce identity fraud including identifying and dealing with fraud scenarios like information misrepresentation, tracking multiple registration efforts by the same individual, registration for a non-existent person, or deceptive registration.

The 'administration' application will handle a wide range of administrative issues such as roles, user management, business process automation, access control and status reporting. This application will ensure that there is a trust network across both internal, for example Systems Administrators and external, for example 'Authentication Service Licensees' entities.

An 'analytics and reporting' application which provides enrollment and authentication statistics for the NIMC, its partners and the public, and which supports also a visual representation of statistics thus enabling various levels of evaluation and treatment will be available, though at an aggregate level, to protect individual identities.

⁴⁹ Prior approval is required for FEPs to establish temporary/permanent centres. The Mobile Registration Work Stations are to be supplied based on a NIMC approved technical guideline.

There is an 'information portal' which will provide administrative and information access for internal users, stakeholders, FEPs and the public.

An 'interface' application for 'Logistics' and 'contact centre' provides the platform for query and status update functionality, letter printing and delivery sending and receiving raw data, sending NIN-related data for letter printing, delivering and receiving periodic status updates on the inbound and outbound communication sending text messages and emails has been included

An important lesson from past experiences and findings of the Privacy Impact Assessment Study informed the proposal to engage logistics service providers along two basic tracks: service providers for sundry services ranging from mail delivery to transportation and contact centre service providers. The NIMC will partner with private sector operators to manage Contact Centres which will provide a central point of contact to all individuals and other entities that will partner with NIMC during the enrollment and post enrollment stages. The Contact Centres will provide services in multiple languages for citizens and other stakeholders.

The service providers for the Contact Centres will setup, operate and maintain the Contact Centres including the staff and/or agents. They will be expected to scale operations at the required pace to match volumes of interactions, provide analytics support to the NIMC, assist in driving performance improvements. They will also take end-to-end responsibility of driving resolution of queries and services, and various interactions with the stakeholders, identify and develop process models suitable for a typical Contact Centre for the NIMS. The proposed contact centre architecture overview will be based on global best.

8.0 Implementation and Risk.

An important dimension in the implementation of the NIMS is the partnership with the private sector. Also this is the first time such a partnership is being initiated and for a sector that had experienced stunted growth in the past. The challenge therefore is to deliver on the objective of the NIMS in a timely, effective, efficient and sustainable manner for the benefits of the project to impact on the governance process and economic activities decisively⁵⁰.

The major challenge and an important source of a set of risks therefore, is the level of commitment by all partners to this project to ensure timely implementation, against the history of past efforts and the need to reuse available infrastructure without slowing down implementation⁵¹.

The various implementation risks which have been identified will be addressed in the course of implementation and they include the following:

- a. Political risks. This is a major source of concern to the NIMC partners. The risk that government will reverse the policy that created the concession agreement through which private investment will be committed to the project, the risk that political support at the highest level might over time diminish, the risk that government agencies will not embrace the project and the anxiety that politicization of similar projects in the past will adversely impact public perception of the project. Closely associated with this risk is the *status quo* and *vested* interests in the existing scheme of things. Fortunately there is a political risk guarantee in place. And Government support remains exceptionally very high.
- b. Closely related to the political risk is the risk that the project cannot be sustained. The participation of the private sector in a concession arrangement which includes a technology (upgrade) refresh in the fifth year and a regime of fees for verification services are some of the strategies for ensuring sustainability.

⁵⁰ The imperative is to deliver all aspects of the project enrollment, de-duplication and authentication and verification services efficiently and sustainably.

⁵¹ The concession agreement defines the terms of private sector investment on the roll out of the NIMS. But the delivery of a sustainable NIMS is predicated on the implementation of a three-track mandate implicit in the NIMC Act: winding up of the former DNCR, setting up of the NIMC and implementation of the NIN, that is the anchor of the value proposition of the NIMS.

- c. An important element of sustainability is the extent to which the NIN is adopted. The option chosen to address the early and successful adoption of the NIN is to legislate its use in the conduct of certain transactions (Section 27 of the NIMC Act). To ensure that this does not lead to an endless obsession for an ID Card, the authentication services are to be provided both online and offline.
- d. Privacy and security risk rank high on the risk profile. Based on the privacy impact assessment study, citizens are conscious of the implications of an unbridled access to the database which can lead to infringement of individual privacy. The NIMC will therefore have to ensure that the database and access to it is not compromised.
- e. Enrollment risks have largely been taken care of by legislation in the sense that the NIN is mandatory for certain transactions and it is also mandatory once you are 16 years and above. There is provision also for registration of births and deaths and therefore the enrollment of children. The FEPs will deploy mobile enrollment kits and collaborate with local and state governments to deploy permanent enrollment centres⁵².
- f. There are other risks associated with scale of this exercise which will be undertaken by private enterprise. With a target of 100m in thirty months and a plan to cover the entire population, the massive deployment of enrollment centres, network connectivity and technology requires a huge and expanding operational and administrative capacity that needs to be well managed.
- g. Dearth of human resource in the various aspects of identity management is another source of risk. Whilst relying at this stage, on foreign experts, (even Nigerians from the Diaspora need time to adjust), NIMC contractors/vendors/partners are required to work with/train Nigerians while special training schemes will be worked out at designated training centres.
- h. The novelty of the concession arrangement in the implementation of the NIMS makes the funding an important risk factor that has been hedged against. The private sector investment require more than a political risk guarantee and yet need to take on the risk and management elements that rationalized the option to adopt a PPP in the first place. To address this risk, NIMC will lighten the significant cost items through part funding, allow a modest, optimal and scalable fee structure for verification services and provide opportunities for FEPs to deploy access to the NIDB and use of the Smart Card for other value

⁵² Based on the studies conducted, specific provisions have been made to ensure the data capturing process accommodates most of the identified challenges – specially abled, rural population, primary source documents, lack of required information, cultural barriers to enrollment, etc.

added services. Control over such a realistic stream of revenues with appropriate concessionaire equity will give Banks enough comfort to fund the project.

- i. Perhaps the most important risk when viewed against the scale of operations and dearth of human resource alone, is the technology risks. Except perhaps for the production and personalization of Smart Cards almost every technology required for this project is to be imported for the time being, including such services as systems integration and the biometric solutions. The NIN project depends on technology on a large scale- the connectivity network, the authentication and de-duplication of biometrics, storage and disaster recovery imperatives, data capture equipment etc. The NIMC will address this risk by making the right decisions as to partners and service providers in terms of the data capturing and management tools, managing obsolesce and data quality, the right biometrics and technology in the architecture and ensuring the right transaction model is achieved with the FEPs and other stakeholders.

9.0 Benefits of the NIMS and the NIN

The involvement of the private sector under a concession arrangement is meant to address this. The concession is for a ten year period. The NIMC was set up by Act No. 23 of 2007 with a mandate to issue the NIN to all citizens and legal residents in Nigeria. A key requirement of the NIN is to minimize/eliminate duplicate/multiple/ghost identity to improve the efficacy of the service delivery systems across the economy. Biometric features are selected to be the primary mechanism for ensuring this uniqueness and through this unambiguous identification of individuals who are then assigned a NIN, a unique database is created which, with a verification and authentication infrastructure, is an important social infrastructure that will address a couple of societal vices and unleash significant economic opportunities in the economy. This infrastructure is what is lacking in Nigeria today.

This is the first time in Nigeria a truly robust Identity Management Solution is being implemented with the challenge of incorporating useful infrastructure from existing Identity Card Systems that characterized efforts of the past while providing for programmes of other institutions like the FIRS, FRSC, CAC, NHIS, NIS, NPS some of whom have begun to implement large scale biometric based databases for their services.

The expectation is that as soon as the NIMS is functional, the need to collect biometric data by other government agencies would be significantly reduced if not completely eliminated. The NIMC acknowledges the need to allow a transitional period during which such already initiated programmes can be allowed to be completed with support from the NIMC to ensure the successful implementation of the harmonization and integration process,(an important mandate of the NIMC).

Our past experience at building an ID Card system was based largely on vendor dominated arrangements culminating in the turnkey contract in 2001. Therefore there is no significant expertise and or experience to depend on. The NIMS is the fulcrum of the paradigm shift from ID Card issuance to Identity Management, with no significant expertise. Yet the NIMC must be empowered to manage the NIMS and grow the identity sector in an orderly manner if the benefits of the NIMS are to be maximized, indigenous expertise and technology developed so that the sustainable development of the NIMS and the identity sector generally can be assured.

The first steps have been taken by government in terms of the legal, regulatory and institutional framework. The the creation of the NIMC and winding up of the former DNCR is a deliberate attempt to ensure a stream lined approach to the reform of the identity sector as it is. The involvement of the private sector, though quite demanding and challenging is intended to expand the sustainable scope of benefits as well as

ensure that the solution is service-oriented and capable of helping to deepen the economy.

As an instrument of identification the NIN offers a wide range of opportunities across the economy. The value proposition of the NIMS is predicated on the NIN some of which are indicated below:

- a. Financial Services Sector- The use of the NIN in the financial services sector will encourage the development of the sector generally. It will support the credit rating services, enable better management of credit administration processes and delivery of other banking and financial services, especially consumer credit, payment solutions, financial inclusion and financial benefits administration programmes. (Simplifies Know Your Customer, KYC and eliminates duplication of efforts by financial institutions in that regard) it will help foster a disciplined financial services sector.⁵³
- b. Maintenance of Law and Order through the security of lives and properties- Most criminal cases never get resolved due to multiple/duplicate/ghost identities. The increasing use of the NIN in transactions (which means repudiation is no longer possible) means it will be easier to identify the criminal – deception and identity misrepresentation/theft, the basis of advance fee fraud, etc will no longer be possible. This will enhance the work of the law enforcement agencies. It will facilitate the timely management of criminality.
- c. Governance will be enhanced through the proper identification of individuals so that for example, the taxable adults are known, social welfare programmes can be better planned, managed and the poor to whom subsidies are targeted can be reached, planning with statistics is further enhanced, etc.
- d. Political Process will be further supported. The requirement for a time frame for registration and or enrollment of eligible voters will become easier to manage with the institution of the NIN. Because the NIN will cover those who are also not eligible to vote, the requirement of a NIN for registration as a voter and or a candidate for an election will positively impact on the political process. It will reduce the time, 'proof of identity' and ascertainment of the tax and other related records of the candidate. It will provide an authentic basis for the review of Voters Register.

⁵³ In spite of the growth in the financial services sector and in particular the banking sector, Nigeria remains significantly under-banked and access to banking and other financial services remains appallingly low (total number of bank accounts is estimated to be less than 45million, which is about 30% of the current population figure of 150m. The NIN will thus mitigate the high cost of customer acquisition and reduce the cost of doing business in the financial services sector.

- e. Sundry commercial and social services. The emergence of the GSM in Nigeria revolutionized the way Nigerians do business and interact. The impact of the NIN will be more than the impact of the GSM on the socio-cultural life and interaction in Nigeria, especially at the commercial level. Various hitherto impossible transactional relationships will be made possible because you can identify who you are dealing with and the law can also do the same.
- f. The benefits of having an identity management system in place, in particular the NIN will certainly help launder Nigeria's image with significant global acceptance.