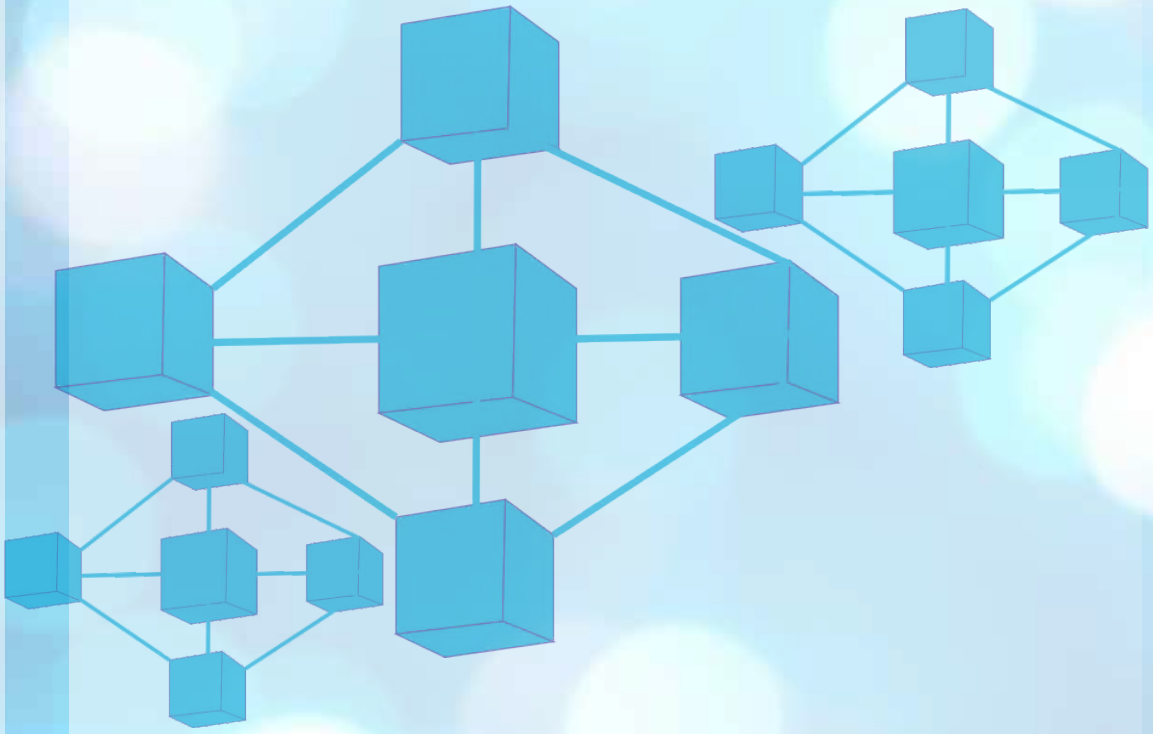
National Identity Management Commission

Providing assured identity
Established by Act No. 23 of 2007

Harmonization and Integration Policy



Published by
The Research & Strategy Unit
Office of the Director General/CEO
National Identity Management Commission
11, Sokode Crescent, Off Dalaba Street
Zone 5 Wuse
P.M.B. 18, Garki, Abuja, Nigeria.

Telephone: +234 (0) 9 6726456-7
Website: www.nimc.gov.ng
Email: publications@nimc.gov.ng

For
The Harmonization and Integration Implementation Committee,
National Identity Management Commission (NIMC)

Table of Content

Abbreviations & Acronyms

ABIS	Automated Biometrics Identification System
AMTS	Advanced Management and Technology Solution
AFIS	Automated Fingerprint Identification System
ASP	Application Service Provider
CAC	Corporate Affairs Commission
CBN	Central Bank of Nigeria
DMZ	Demilitarized Zone
DNS	Domain Name Services
DNCR	Department of National Civic Registration
EFCC	Economic and Financial Crimes Commission
FIRS	Federal Inland Revenue Service
FRSC	Federal Road Safety Corps
GMPC	General Multi-Purpose Card
HIAS	Harmonization and Integration Assessment Study
HIIC	Harmonization and Integration Implementation Committee
ICT	Information and Communication Technology
ID	Identity
INEC	Independent National Electoral Commission
IP	Internet Protocol
ISO	International Standards Organization
JTB	Joint Tax Board
MOD	Ministry of Defence
NCC	Nigeria Communication Commission
NEEDS	National Economic Empowerment and Development Strategies
NHIS	National Health Insurance Scheme
NID	National Identity Database
NIN	National Identification Number
NIMC	National Identity Management Commission
NIMS	National Identity Management System
NIS	Nigeria Immigration Service
NPC	National Population Commission
NPF	Nigerian Police Force
NPS	Nigerian Prison Services
ONSA	Office of the National Security Adviser
PENCOM	National Pensions Commission
PII	Personally Identifiable Information
PIV	Person Identification Verification
PVC	Poly Vinyl Chloride
SSS	State Security Services
SQL	Structured Query Language
UTIN	Universal Tax Identification Number
UUID	Universally Unique Identifier
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extended Markup Language

1.0 Introduction

One of the major constraints to economic development in Nigeria is the dearth of data useful to economic planning. This is in addition to the unfortunate inability of a great nation like Nigeria to develop a national system of identity management, which could serve its current needs and meet future expectations, as technology expands the frontiers of identity management.

Of central concern to Government has been the huge expenditure incurred annually by its agencies in the repeated conduct of registration and, recently, biometric enrollment activities, when it can be effectively served by a centralized system. It is partly the need for the streamlining of such activities, and the need to foster the orderly development of an infrastructure that would drive e-governance, that led Government recently to undertake major reviews of its policy initiatives in certain areas, including the identity management sector.

Major outcomes of the review exercise were the establishment of a company to address the lack of a national information and communication technology infrastructure backbone (Galaxy Backbone Plc); and the need to reform the identity sector in Nigeria which led to the creation (by Act No. 23 of 2007) of the National Identity Management Commission (NIMC). The NIMC, in addition to creating a National Identity Management System and Infrastructure, is also responsible for the harmonization and integration of databases in government institutions in Nigeria (Part III section 5 (a) of the NIMC Act, 2007).

In this document, an important aspect of the outcome of the review process is presented - the Harmonization and Integration Policy for the National Identity Management System for Nigeria. The policy provides a basis for the development of a framework for the implementation of the mandate of the NIMC in the areas of identity infrastructure, database, access, integration and management, uniform standards and methods for the collection, treatment, storage / retrieval, and use/management of demographic and biometric data in government agencies and by extension, in the private sector.

2.0 Background

Since independence, Nigeria has always recognized the need to create a system of identity management for her citizens and legal residents using demographic data. A major attempt was initiated with the enactment of the law which created, in 1978, the Department of National Civic Registration (DNCR). The DNCR was charged with registering and issuing a National Identity Card to every citizen of Nigeria aged 18

years and above. Government's primary objective then was to create a system of national identity card issuance in the belief that this would help sort out the growing concerns about the correct identity of individuals, serve as an effective tool for controlling illegal immigration, provide a basis for reliably validating other civic documents like drivers license, travel passports, etc.

However, the implementation of the programme was soon characterized by uncertainties and failed contracts which impaired its full implementation, until when Government in 2001 decided to award another contract to Messers Sagem, S.A. France, which, in 2003, carried out the demographic and biometric data capture in Nigeria of over fifty-two million (52 million) citizens over a period of six (6) weeks. Ironically only about thirty seven million (37 million) were complete records.

This project, which was specifically for the delivery of an integrated card personalization facility, registration of sixty (60) million Nigerians and issuance of sixty (60) million ID Cards, was concluded in 2006. Two important objectives of identity management were however not achieved – harmonization of identity-related databases in government agencies and the development of an identity management system for Nigeria. There was no provision for an effective means of information update and no access infrastructure at all to enable identity authentication and verification. This in part informed Government's decision to review the various identification schemes in Nigeria. More importantly, the review was also part of efforts to achieve the development goals of The National Economic Empowerment and Development Strategies (NEEDS).

In 2005 Government established a Harmonization Committee to advise it on how various government (and private sector) initiatives on identification systems can be harmonized, in view of the limited benefits of its Identity Card personalization facility under the SAGEM project.

The Committee, amongst other things, proposed a national policy and institutional framework for a national identity management system for the country. The policy included the establishment of the National Identity Management Commission (NIMC), as the primary legal, institutional, supervisory, and regulatory framework to drive the reform initiative in the identity sector. To effect this policy, NIMC Act No. 23 of 2007, which repealed the National Civic Registration Act of 1978 and established NIMC, was enacted.

The NIMC's mandate includes, among other things, winding up of the former Department for National Civic Registration (DNCR), the implementation of a National Identity Management System (NIMS) for Nigeria and the setting up of the

NIMC itself as a regulatory, institutional and legislative organization that will drive the orderly development of the identity sector in Nigeria.

The NIMS combines a National Identity Database (also known as a Central Identity Repository or Register, CIDR), a chip-based, secure identity card, and a network of access and means to irrefutably prove or assert the identity of an individual. The most important thing about the NIMS is that it will provide a Universal Identification Infrastructure for the entire country. This will help bring real and recognizable benefits to the Government, each of us - individually and collectively, and also for legal residents in Nigeria.

Under the NIMS functional responsibilities, the NIMC Act provides for, amongst other things, the Commission to create, operate and manage a national identity database, assign unique identification numbers to citizens and legal residents, harmonize and integrate various existing identification databases in government agencies, provide secure communication links to the database, and partner with any public and or private sector organization for the achievement of its objectives of instituting an identity management system for Nigeria.

The current efforts of the NIMC at establishing the NIMS has now made it possible for the proposed harmonization and integration of databases in government agencies and, more importantly, the creation of shared infrastructure for secure and reliable authentication and verification of an individual's identity, based on a uniform, standard and globally comparable industry practice.

3.0 The Environment and Scope of the Harmonization and Integration Policy

The 2005 Harmonization Committee set up by Government noted that various Government Agencies/key institutions maintain disparate identity databases. Even though they go through similar processes to collect these identity data, there exists no linkage between these agencies in accessing or exchanging such related data. In some of these institutions, the process of data collection, treatment and storage is not automated, while in others - though semi or fully automated it does not provide for any form of consolidation and security protocol as to confer any integrity and or foster any reliance on the database.

The proposed national identity database, a key component of the ongoing implementation of the NIMS, will serve as a central source of identity data to be used in identity verification and authentication, and will be connected to various other identity database in key institutions in Nigeria through the unique National Identification Number (NIN). It will also enable the streamlining of various registration and enrollment activities (standardize, eliminate duplication, etc) in government agencies, by introducing common standards and practices towards

creating and fostering the orderly development of an identity sector in Nigeria.

The strategic approach towards the achievement of the harmonization objectives remains the effective and seamless integration and harmonization of existing databases, processes and procedures, and infrastructure into a single identity management system and infrastructure, including the provision of an authentication and verification service across the public and private sectors.

In order to jumpstart the harmonization scheme, key partners from the public sector have been identified and include the following:

i. Independent National Electoral Commission – Voters Register
ii. National Health Insurance Scheme – Health Insurance Owners
iii. National Population Commission – Census, Birth/Death Registry
iv. National Pension Commission – National Data Bank
v. Nigeria Immigration Service – International Passports
vi. Federal Road Safety Commission – Drivers Licenses
vii. Federal Inland Revenue Service – Tax Payers Database (UTIN)
viii. Department of National Civic Registration – National Identity Cards.
ix. Nigeria Communication Commission (NCC) –SIM Card Register,
x. The Nigerian Police Force (NPF)
xi. Nigerian Prison Services (NPS)
xii. Joint Tax Board (JTB)
xiii. Corporate Affairs Commission (CAC)
xiv. Economic and Financial Crimes Commission (EFCC)
xv. Central Bank of Nigeria (CBN)
xvi. State Security Services
xviii. Office of the National Security Adviser

Based on its mandate as provided for in the Act, the NIMC in 2008 undertook a Harmonization and Integration assessment study which formed the basis of the Harmonization and Integration Policy. It subsequently inaugurated a Committee on the implementation of the Harmonization and Integration policy.

4.0 The Harmonization and Integration Policy

4.1 Policy Direction

The national policy direction is to establish harmonized and seamlessly integrated NIMS which is anchored on the unique NIN, and which connects the various institutional databases under a single platform. The NIMS, which includes a National Identity Database (NID) that supports a system for uniquely authenticating and

verifying the identity of every individual and legal resident in Nigeria, is designed to guarantee identity only - an important denominator in the service and functions of all institutions of government and the private sector. The NIMS also provides for the issuance of a Smart Card.

4.2 Policy Thrust

The major thrust of the NIMC policy on harmonization and integration is as follows:

i. Harmonization of existing identification schemes which are compatible with the National Identity Database in such a manner as to enable the institutions leverage on the benefits of a national identity database.
ii. Facilitate the adoption and use of the NIN to be issued by the NIMC as part of the NIMS.
iii. Provide a standardized access to the National Identity Database.
iv. Institute a sustainable and extendable interface that will facilitate the integration and interoperability of new and existing identity databases, with a centralized national identity management infrastructure, including a unified user management platform.
v. Establish a system interface, essentially a contract, between any stakeholder-system and the NIMS that defines the obligations of the stakeholder-system based on the enabling legislation and service mandates, business policies and system functionality. This may or may not require direct intervention in the data collection, maintenance, or management functions of any stakeholder-system, but it would provide the necessary safeguards for citizens' privacy and information security, as well as operational efficiencies and minimum standards for interoperability.
vi. Establish a financial model that will enable long term sustainability of the NIMS.

4.3 Policy Objectives

The overall policy objective is the promotion of an enabling legal, operational, technological and infrastructural environment for the sustainable development of NIMS, that utilizes a biometric-linked NIN to create a single, uniform, standard process for personal information, shared infrastructure for common services, as well as a common verification and authentication system, towards efficient deployment of resources and rendering of services across the economy. The government's policy objectives would remain focused on the need to identify identity eco-systems, technology solutions, business practices and procedures, laws and policies that would ensure the attainment of the following harmonization and integration objectives:

1. Development of a data format for streamlining enrollment, de-duplication and authentication processes, storage and database management process;
2. Set technical standards and technological solution specifications and procedures to guide processes and procedures for utilization of the unique identifier and the national identity database;
3. Enable a single point of access to, and common platform for utilizing, the identity data so as to guarantee identity across various segments of the economy;
4. Institute behavioral and cultural change through real-time online availability of essential identity data;
5. Create a platform for data sharing, authentication and verification of identities;
6. Provide a basis for development of common standards on demographic and biometric policies and processes for the sustainable and orderly development of the identity sector in Nigeria;
7. Create a platform to enable enforcement of legal and business rules governing the use of NIN and biometrics information in the country;
8. Achieve significant reduction in the cost of governance through the integration and interoperability of government identity databases across various agencies and departments;
9. Enhance the quality of service delivery in the public and private sector by providing shared technology solutions that offer opportunities for a wide range of service offerings;
10. Safeguard public order and assist in the enforcement of law and order while preserving the privacy of individuals and enhancing the security of identity related information;
11. Support the common identity needs of government and the private sector; and
12. Enforce global best practices in the process of selecting and adopting appropriate technologies and solution providers, and in the general administration of the NIMS.

4.4 Policy Targets

The context for the implementation of the harmonization and integration objective of the NIMC is the NIMS. The Harmonization and Integration Committee will drive the implementation of the policy to achieve the following targets:

i. Establish the guidelines and parameters for the technological solutions and

specifications towards the achievement of the harmonization and integration mandate of the NIMC;

ii. Help set up a platform for the adoption of technology solutions and related technological devices compatible with the objectives of the harmonization and integration objectives of the NIMC within 18 months of the implementation of this policy;

iii. Establish the unique identification number which shall be adopted by all the stakeholder agencies within twenty-four months from the adoption of the Policy;

iv. Establish both on-line access and off-line verification to the national identity database, as appropriate, for all stakeholder agencies within 12 months of the implementation of this policy;

v. Set demographic, biometric and business policies and processes for the establishment of a digital platform that would facilitate data exchange, access to the national identity database, and help sustain the orderly development of an identity sector in Nigeria within 24 months of the implementation of this policy;

vi. Provide a platform for other public and private sector electronic services and devices to be adopted and or incorporated as part of the harmonization and integration eco-system within 24 months of the implementation of this policy;

vii. Provide a secure and operationally efficient system for continuous registration and enrollment of individuals across the country within 24 months of the implementation of this policy.

4.5 Policy Strategies

The primary strategy for achieving the objectives and targets of the harmonization and integration policy revolves around a clear design, and development and implementation of a framework for successfully implementing the NIMS as proposed. As intended, NIMS will impact all aspects of Nigerian life; integrate and simplify existing means of identification through creating a central National Identity Database; provide a platform for data sharing and exchange; and support a coordinated, technology-driven, resource optimizing, public service delivery scheme that is citizen orientated and fraud-free. The following strategies amongst others would be employed:

i. The government would continue to provide the political, legislative and financial direction and support required by NIMC to achieve its mandate as specified in the NIMC Act.No.23 of 2007;
ii. The NIMC would adopt a strategy for creating awareness amongst key public and private sector institutions on the need for and requirements of harmonization and integration in the identity sector in Nigeria;
iii. Build consensus amongst key stakeholders on the harmonization and integration approach;
iv. Foster a buy-in by stakeholders in the identity management ecosystem;
v. Identify and document constraints to harmonization so as to induce clarity in the resolution mechanism;
vi. Build the required capacity to sustain an integrated identity management system, amongst others;
vii. Government would continue to appropriately fund the development of the ICT backbone infrastructure to support the establishment of the NIMS and the NIDB, including creating the enabling environment for the meaningful participation of the private sector in the deployment of appropriate technology and identity management solutions in Nigeria;
viii. Review extant laws as well as the mandates of stakeholder agencies and introduce required and necessary legislation;
ix. Stakeholder agencies shall review, renovate and replace and or upgrade ICT infrastructure facilities in their various institutions as initial steps towards the implementation of NIMS;
x. Implement the provisions of the NIMC Act as it relates to citizen and legal resident registration and enrollment, use of national identification number and deployment of card acceptance devices and smart cards.

5.0 Legal Framework

To guarantee an appropriate legal, institutional, regulatory and supervisory framework for the achievement of the proposed harmonization and integration, there is need for an appropriate legal framework as well as mandates. The NIMC through the appropriate legislative processes would initiate the review of existing legislation and, where necessary, submit new bills to the National Assembly for consideration and enactment. In the meantime, it is necessary to quickly submit to the National Assembly two proposed legislation: Cybercrime Bill and Privacy Bill.

5.1 Existing Legislation

Various institutions that come under the harmonization and integration scheme have been established under a specific legislation including, amongst others, the following:

i. The NIMC Act No. 23 of 2007

ii. Nigeria Immigration Act of 1963

iii. National Population Act No. 23 of 1989

iv. The National Health Insurance Scheme Act No. 35 of 1999

v. The Federal Inland Revenue Service Act No. 13 of 2007

vi. Births and Deaths (Compulsory Registration) Act of 1953

vii. The Pension Reform Act of 2004

viii. The Electoral Act of 2010

vi. The Federal Road Safety Act of 2007

ix. The Nigerian Communications Commission Act of 2003

x. The Nigerian Police Act of 1974

xi. The Nigerian Prison Act of 1972

xii. Joint Tax Board Act of 2004

xiii. The Corporate Affairs Commission Act No. 1 of 1990

xiv. The Economic and Financial Crimes Act No. 1 of 2004

xv. The Central Bank of Nigeria Act of 1958 (as amended by the 2007 Act)

The objective of the harmonization and integration process is not to stop the functions of the institutions and the necessary database they have to maintain, but rather to streamline the way and manner in which they manage identity related data to create a synergy based on the use of the NIN, which the NIMC is statutorily mandated to issue to all citizens and legal residents in Nigeria.

Accordingly, in the execution of their mandate under the harmonization platform, more attention is given to interoperability and the need to ensure that this is sustained based on a common standard.

6.0 Operational Framework

The NIMS presents the core infrastructure and framework upon which the harmonization would operate. This is based on the fact that the most common factor to all stakeholders in the harmonization platform is the requirement of a 'proven identity' to operate or function. The NIMS infrastructure represents the platform in which identity management sub-systems and applications as components are coordinated. To ensure a functional identity management in a fashion that will find general acceptance with all stakeholders and users, NIMC and the relevant stakeholders will be guided and must achieve a sync based on the policies that guide the functional components of the harmonization process. This will help to define the identity management protocols that enable the transmission of desired communications across common platforms and shared infrastructure, as well as stakeholder related systems.

To achieve the harmonization objective and thus facilitate e-government and public sector applications, the NIMS, which is designed to uniquely authenticate the identity of all individuals and provide a national identity database and an authentication/verification infrastructure, will be central to the harmonization process.

6.1 Harmonized Integrated National Identity Database (NID)

Under the NIMS, the NIMC would create, operate and manage the NID, which will serve as a central source of identity verification and authentication. The verification infrastructure shall be available to the stakeholders. The NID is based on the use of fingerprint biometrics to uniquely and unambiguously identify each individual and thereafter issue a unique identification number to each verified individual, which would be common across the other databases. Through this scheme, other databases would become harmonized with the NID to achieve an integrated identity database system.

6.2.1 The Harmonization and Integration Implementation Committee (HIIC)

The Harmonization and Integration Implementation Committee (HIIC) would be set up under the auspices of the NIMC to facilitate a coordinated implementation of the harmonization and integration mandate of the NIMC. The responsibilities of the HIIC would include the following:

i. Review, update and publish the Federal Guidelines and Business Process (Handbook) for Harmonization and Integration of Identity Management in the public sector;

ii. Develop and recommend appropriate policies and mechanisms for effective

public awareness/sensitization campaign, capacity building and technology transfer;

iii. Co-ordinate workshops, conferences and seminars for developing consensus on related issues;

iv. Develop and recommend for approval policies and technical specifications necessary and sufficient for achieving the harmonization objectives as enunciated in this policy document;

v. Monitor the implementation of the harmonization process; and

vi. Co-opt ad hoc resources to facilitate the committee's and subcommittee's work.

6.2.2 The Federal Guidelines for Harmonized Identity Management

To achieve the harmonization and integration objectives, the policy envisages the development of a set of rules, guidelines and policies which will enable stakeholder institutions develop processes and procedures. Though localized in the institutions, these rules/guidelines would be based on uniform standard technical specifications on the basic components of the digital identity management process, created by the use of the NIN under the NIMS. The following areas would be covered by the 'Federal Guidelines for Harmonized Identity Management System' in the public sector:

i. Enrollment into NIMS core database;
ii. Registration into member specific database;
iii. Issuance and use of the National Identification Number (NIN);
iv. Card specifications;
v. Card reader specifications;
vi. 10-print scanner specifications;
vii. Thumb-print scanner specifications;
viii. Data format;
ix. Identity authentication and verification process,
x. Interoperability procedure and processes,
xi. Network access and security specifications,
xii. Connectivity specifications,
xiii. Data processing and storage specifications,
xiv. Rules enforceability procedures,
xv. Penalty and cure procedures, and
xvi. Procedures for revising the guidelines.

6.3 National Identification Number (NIN)

Section 14(2) of the NIMC Act 2007 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) randomly generated 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. By the provisions of Section 18 of the NIMC Act [mandatory registration of citizens aged sixteen (16) years and above] and Section 27 (mandatory use of the NIN in specified transactions), the harmonization process would be further enhanced.

The enrollment process which is initiated by the citizen appearing at the designated location as provided for in Section 18 (1) of the NIMC Act (provide demographic data and permit his/her biometrics to be taken) would ensure that personal information is collected in a manner consistent with the harmonization objectives and thus reduce the need for such activities to be repeated by other stakeholders.

Within 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. This process ensures further that the database will serve the primary objective of the harmonization process.

6.4 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 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 which would be provided and managed by third parties would be available to stakeholders under the harmonization platform to guarantee identity of the individuals they are dealing with it thus provides a basis for the stakeholders to hold their statutory database on the same individual without any fear of contradiction.

Consequently the NIMS requires that all third parties wishing to leverage on the benefits of the authentication and verification infrastructure would meet minimum

technical specifications to guarantee access to and utilization of facilities.

Since the enrollment process is to ensure a secure unique identity database which all stakeholders would have access to, the primary responsibility for this, under the harmonization platform, has been ceded to the NIMC under the NIMS framework (even though other institutions wishing to capture biometric and demographic data could still do so provided they keep to the NIMS standards and technical specifications).

An important provision under the NIMS is the proposed arrangement for the creation of a nexus between births and deaths register and the NIN issuance. The NIMC and National Population Commission would determine the processes and procedure for ensuring the integrity of the enumeration at birth process, including methods to reconcile hospital birth records with birth registrations, and information provided to NIMC and National Population Commission.

6.5 National Identification Card (General Multipurpose Card)

Under the NIMS, there is provision for the issuance of the General Multi-purpose Cards (Smart Cards). Following Government's decision, the Smart Card will replace the current National Identity Cards issued under the previous Identification Cards scheme.

The technical specification to enable interoperability with the NIMS and the use of the NIN would be given by the NIMC and adopted by the harmonization platform. Whilst the Smart Card would now be the minimum specification in terms of the card type, further security measures and features (contact, contactless, chip memory capacity, PKI, etc) will be specified by the NIMC under the NIMS, with sufficient flexibility to enable the stakeholders under the harmonization platform to achieve interoperability and seamless integration.

6.6 Security

The NIMS is predicated on linking an individual's personal information to the NIN, thus creating an identity in a transaction context that is reliable and can be verified. To ensure that the integrity of the data is not compromised in the course of access for purposes of authentication, the NIMS has provided for the following security needs to be optimally met and sustained:

a. Development of a data security procedure and an Information Technology policy;
b. Built in process that responds to identity fraud;
c. Secure enrollment and authentication process;

d. Internal content security and control so that human interference is eliminated and other forms of interference can be tracked;
e. Investigation mechanism for every form of data breach;
f. Development of a privacy policy and the use of existing secrecy laws to enhance the checks against privacy breaches;
g. Inbuilt sanctions, accountability and deterrence mechanism.

These security protocols and others that may be decided upon by the stakeholders would help to ensure the harmonization platform is secure enough to deliver on the expected goals.

To enforce security, all NIMS-related applications must adhere to the rules established to control access and protect the privacy of identity information. Security measures should assist in preventing unauthorized use of data, and protect against loss, tampering and destruction. The NIMS must be capable of including or interfacing with standards-conformant security services, to ensure that any Principal (user, organization, device, application, component, or object) accessing the system or its data is appropriately authenticated, authorized and audited in conformance with established policies. The NIMS should support Chains of Trust for authentication authorization and privilege management, either internally or by interfacing with relevant external services.

6.7 Authentication

The generalized criteria for authentication should include:

i. The system should authenticate principals prior to accessing an NIMS application or data.

ii. The system should prevent access to NIMS applications or data by all non-authenticated principals.

iii. The system should provide the ability to implement a Chain of Trust agreement.

iv. The system should authenticate principals using username/password and at least one of the following authentication mechanisms: digital certificate, a secure token, or biometrics.

6.8 Authorization

The generalized criteria for authorization should include:

i. The NIMS should provide an ability to create and update sets of access-control permissions granted to principals.

ii. The NIMS should conform to function for the purpose of recording all authorization actions.

iii. The NIMS should provide the security administrators the ability to grant authorizations to principals according to scope of practice, organizational policy, or established legal framework.

iv. The NIMS may define context for the purpose of principal authorization based on identity, role, work assignment, present condition, location, and event and condition.

v. The NIMS should also define context based on legal requirements or emergency conditions.

6.9 Access Control

The generalized criteria for access should include:

i. The NIMS should meet the Authentication criteria established herein.

ii. The NIMC should define system and data access rules.

iii. The NIMC should enforce system and data access rules for all NIMS resources at component, application and user levels, whether local or remote.

6.10 Non-Repudiation

The generalized criteria for non-repudiation should include:

i. The NIMS should time stamp initial entry, modification, or exchange of data, and identify the actor or principal taking the action as required by users' scope of practice, NIMC policy, or established legal framework.

ii. The NIMS should provide additional non-repudiation functionalities where required by users' scope of practice, NIMC policy, or established legal framework.

iii. The NIMS should conform to criteria for Information Attestation defined herein to ensure the integrity of data exchange, and thus prevent repudiation of data origination or receipt.

6.11 Secure Data Exchange

The generalized criteria for secure data exchange should include:

· The NIMS should secure all modes of identity data exchange.

- The NIMS should conform to the criteria for Secure Data Routing established herein.
- The NIMS may provide the ability to obfuscate data.
- The NIMS should encrypt and decrypt identity data that is exchanged over all links.
- The NIMS should support standards-based encryption mechanisms when encryption is used for secure data exchange.

6.12 Secure Data Routing

The generalized criteria for secure data routing should include:

i. The NIMS should automatically route electronically exchanged identity data only from and to known sources and destinations, and only over secure networks.

ii. The NIMS should route electronically exchanged identity data only to and from authenticated sources and destinations.

iii. The NIMS should comply with the criteria for Auditable Records to provide audit information about additions and changes to the status of destinations and sources.

6.13 Information Attestation

The generalized criteria for information attestation should include:

i. The NIMS should conform to the criteria for Authentication established herein.

ii. The NIMS should conform to the criteria for Authorization established herein.

iii. The NIMS should provide the ability to associate any attestable content added or changed to an identity record with the content's author, for example, by conforming to the criteria for Auditable Records established herein.

iv. The NIMS should provide for attestation of attestable identity record content by the content's author.

v. The NIMS should indicate the status of attestable data which has not been attested.

vi. The NIMS may provide for attestation of identity record content by properly authenticated and authorized users different from the author, as required by users' scope of practice, NIMC policy, or the extant legal framework.

vii. The NIMS may use digital signatures as the means for attestation.

6.14 Privacy and Confidentiality

The generalized criteria for assuring privacy and confidentiality should include:

i. The NIMS should provide the ability to fully comply with the requirements for individual privacy and confidentiality in accordance with a user's scope of practice, established policy, or the established legal framework.

ii. The NIMS should conform to the criteria for Authentication.

iii. The NIMS should conform to the criteria for Authorization.

iv. The NIMS should conform to the criteria for Access Control.

v. The NIMS should conform to the criteria for Non-Repudiation.

vi. The NIMS should conform to the criteria for Secure Data Exchange.

vii. The NIMS should conform to the criteria for Auditable Records.

viii. The NIMS should maintain varying levels of confidentiality in accordance with users' scope of practice, established policy, or extant laws.

ix. The NIMS should provide the ability to mask parts of the electronic identity record from disclosure according to scope of practice, organizational policy or law.

x. The system should provide the ability to override a mask in emergency or other specific situations according to scope of practice, established policy, or extant laws.

6.15 Information Management

Since identity information will typically be available on a variety of NIMS applications, the system must provide the ability to access, manage, and verify the

accuracy and completeness of identity information, maintain the integrity and reliability of the data, and provide the ability to audit the use of and access to identity information.

6.15.1 Data Retention and Destruction

The generalized criteria for data retention and destruction should include:

i. The NIMS should store and retrieve identity record data and documents for the legally prescribed time.

ii. The NIMS should retain inbound data or documents related to identity record as originally received (unaltered, inclusive of the method in which they were received) for the prescribed time in accordance with users' scope of practice, established policy, or extant laws.

iii. The NIMS should retain the content of inbound identity data as originally received for the legally prescribed time.

iv. The NIMS should have the ability to retrieve both the information and data on the transaction or business context within which that information was obtained.

v. The NIMS should have the ability to retrieve all the elements included in the definition of a legal identity record.

vi. The NIMS should identify specific identity data/records for destruction, review and confirm destruction before it occurs.

vii. The NIMS may destroy identity data and records so that all traces are irrecoverably removed according to policy and legal retentions periods.

viii. The NIMS should pass along record destruction date information (if any) along with existing data when providing records to another entity.

6.15.2 Auditable Records

The generalized criteria for auditable records include:

i. The NIMS should provide audit capabilities for recording access and usage of systems, data, and organizational resources.

ii. The NIMS should conform to the criteria for Authentication.

iii. The NIMS should provide audit capabilities indicating the time stamp for an object or data creation.

iv. The system should provide audit capabilities indicating the time stamp for data modification, extraction, exchange, view and deletion, in accordance with users' scope of practice, established policy, or extant laws.

v. The NIMS should provide audit capabilities indicating the author of a change, the viewer of a data set, and the data value before a change, in accordance with users' scope of practice, established policy, or extant laws.

vi. The NIMS may provide audit capabilities to capture system events at the hardware and software architecture level.

vii. The NIMS should conform to the criteria for Access Control to limit access to audit record information to appropriate entities, in accordance with users' scope of practice, established policy, or extant laws.

viii. The NIMS should generate an audit report as provided for herein.

ix. The NIMS should provide the ability to view change history for a particular record or data set, in accordance with users' scope of practice, established policy, or extant laws.

x. The NIMS should record system maintenance events for loading new versions of, or changes to, the system; loading new versions of codes and knowledge bases; creating and restoring of backup; archiving any data and re-activating or restoring an archived identity record; entering into and exiting from the system; and remotely accessing connections, including those for system support and maintenance activities.

xi. The NIMS should record changes to the date and time wherever the system allows this to be done.

xii. The NIMS should record and report audit information using a standards-based audit record format.

6.15.3 Extraction of Identity Information

The generalized criteria for extraction of identity information should include;

i. The NIMS should provide the ability to extract identity record information.

ii. The NIMS should conform to the criteria for Secure Data Exchange and provide secure data exchange capabilities.

iii. The NIMS should provide the ability to de-identify extracted information.

iv. The NIMS should conform to the criteria for Interchange Standards to enable data extraction in standard-based formats.

v. The NIMS should provide the ability to perform extraction operations across the complete data set that constitutes the identity record of an individual within the system.

vi. The NIMS may provide the ability to perform extraction operations whose output fully chronicles the identity history.

vii. The NIMS should provide the ability to extract data for administrative, research, quality analysis and national and local planning purposes.

6.15.4 Storage of Identity Data

Structured identity record information is divided into discrete fields, and may be enumerated, numeric, or codified. Context may determine whether or not data are unstructured.

i. The NIMS should be able to capture, update, and retrieve structured identity record information as part of the identity record.

ii. The NIMS should conform to the criteria for data retention and destruction and have the ability to de-activate, render obsolete, or destroy structured identity record information.

iii. The NIMS should provide the ability to report structured identity record information.

iv. The NIMS may track structured identity record information over time.

v. The NIMS should provide the ability to retrieve each item of structured identity record information discretely within context.

vi. The NIMS should provide the ability to append structured identity record information to the original structured identity record information.

6.16 Standards: Terminologies and Interoperability

The NIMS should support terminology standards and services to enable semantic interoperability defined by the consistency of human and machine interpretation of shared data and reports. Such standards should include the capture and support of consistent data for templates and decision support logic. Terminology standards pertain to concepts, representations, synonyms, relationships and computable (machine readable) definitions. Terminology services provide a common way for managing and retrieving these items.

Semantic interoperability requires standard terminologies combined with a formal standard information model. A terminology provides semantic and computable identity to its concepts. Terminologies are use-case dependent and may or may not be realm dependent. Formal standard terminology models enable common semantic representations by describing relationships that exist between concepts within a terminology or in different terminologies. The use of standard terminologies is greatly enhanced with the ability to perform hierarchical inference searches across coded concepts. Hierarchical inference will enable searches to be conducted across sets of coded concepts stored in the NIMS.

6.16.1 Standard Terminologies

The generalized criteria for standard terminologies should include:

i. The NIMS should use standard terminologies to communicate with other systems internal or external to the NIMS.

ii. The NIMS should validate that terms and coded data are presented in a current and standard terminology.

iii. The NIMS should exchange identity data using formal standard information models and standard terminologies.

iv. The NIMS should use hierarchical inference searches e.g., subsumption across coded terminology concepts that were expressed using standard terminology models.

v. The NIMS should use a terminology service, internal or external to the NIMS, or if no standard terminology model is available, to provide a formal explicit terminology model.

vi. The NIMS should have the ability to use different versions of terminology standards to update terminology standards, and to relate modified concepts in

the different versions of a terminology standard to allow preservation of interpretations over time.

vii. The NIMS should be able to interoperate with systems that use known different versions of a terminology standard.

viii. The NIMS should be able to retire deprecated versions of standard terminologies and codes while maintaining obsolescent code sets.

6.16.2 Interoperability Standards

The generalized criteria for interoperability standards should include:

i. The NIMS should seamlessly perform interchange operations with legacy systems and other systems that adhere to recognized interchange standards.

ii. The NIMS should exchange data using an explicit and formal information model and standard coded terminology.

iii. The NIMS should use different versions of interchange standards. Changing (reconfiguring) the way that data is transmitted as an interchange standard should evolve over time and in accordance with transaction and business needs.

iv. The NIMS should interoperate with other systems that use known earlier versions of an interoperability standard.

v. The NIMS may provide the ability to update, customize, inactivate, or destroy access privilege rules and their components.

vi. The NIMS may provide the ability to route notifications and tasks based on system triggers.

7.0 Technical Requirements

The conceptual framework and design for the NIMS envisages the following characteristics:

i. User-centricity.
ii. Privacy protection.
iii. Scalability.
iv. Flexibility.
v. Open interoperability.

The conceptual architecture should embody the above characteristics and satisfy the identity requirements of current stakeholders. Focus on user-centricity, while not an entirely new concept, will differentiate it from many other identity architectures which focus on large central software applications or administration bureaucracies. This identity management architecture has the advantages of meeting the identity requirements of NIMC and helping safeguard the privacy of stakeholders and citizens.

7.1 Gateway for Exchanging Identity Data

The technical approach to harmonization should consider the ability of each stakeholder to collect, manage, and safeguard identity databases, and their ability to exchange accurate information quickly and efficiently with other stakeholders. The exchange of data is essential to effective development of Nigeria's National Identity Initiatives.

Acknowledging the lack of or limited resources, expertise, and capacity within most of the stakeholder agencies, NIMC should be charged with management and support of Centralized ID Gateway System to assist the member stakeholders in identity information retrieval and verification process. It is recommended that NIMS become the de facto central database.

7.2 NIMC Identity Gateway

The following principles and guidelines will govern the function and operation of the NIMC identity gateway:

i. Stakeholder membership only: The NIMC gateway shall only be available to member stakeholders who have subscribed and met the necessary requirements established by NIMC. In addition to the member stakeholders, NIMC should license private sector companies through which non-member stakeholders can access the database.

ii. 24/7 system (Virtual Private Network): Access to the NIMC central database should be through VPN (and preferable through direct fibre optics connections). NIMC should ensure that access to the database is available 24 hours per day and 7 days a week.

iii. NIMC ID Getaway monitoring expert group: Access to the database should be monitored on regular basis to ensure the integrity of the overall system. Any illegal access should be promptly reported to any stakeholder whose data may have been compromised.

a. Central database: NIMC ID Gateway Principles
   i. ID matching capacity should be available to all member stakeholders,
   ii. Member stakeholders should retain their own data,
   iii. Central database should not contain any nominal data,
   iv. Central database should be able to sustain 1000 hits per second, and
   v. Hit validation and billing should be outsourced to a third party.

b. Privacy protection and confidentiality: The NIMC Act regarding strengthening Freedom, Security and Justice in Nigeria specifies the duties of the Government to protect the identities of citizens. Accesses to the database will therefore be segmented.

7.3 Services to be Offered by NIMC Identity Gateway System

Initially, core services will focus on electronic fingerprint submissions for enrollment and verification. Verification requests will originate from live-scan terminals or card scanners at the stakeholder level. If identification is made, an identification response ID will be transmitted back to the stakeholder that initiated the identification request. If identification is not made, the candidate would be directed to a NIMC registration centre for stakeholders belonging to class A services (security-sensitive services). For stakeholders belonging to class B (non- security-sensitive services), a temporary National Identification will be created. Conceptually, the services that should be offered by NIMC ID Gateway System include:

i. Thumbprint and ten-print services:
   a. Electronic fingerprint identification;
   b. Submissions fingerprint investigative searches;
   c. Electronic disposition submissions (future capability); and
   d. Best practices for the exchange of 1, 2, 3, 4, 5, 6, 7, 8, 9, or 10-print identification services.

ii. Latent services:
   a. Electronic latent submissions;
   b. Latent searches;
   c. Latent image maintenance requests; and
   d. Best practices for the exchange of latent identification services.

iii. Image Services:
   a. Requests for images;
   b. Electronic requests to upgrade fingerprint images; and
   c. Requests for records of fingerprint features to accompany images.

iv. Photo Services:
   a. Subject photo request; and
   b. Subject photo append, upgrade or delete.

v. Other Biometric Services (Future Capability as new technologies become available).

7.4 Automated Data Exchanges – General Principle

Data exchange requires comparable data. Stakeholder wishing to participate in use of biometrics data for purposes of person identification must conform to NIMC standards. The following minimum basic demographic information should be collected:

I. Surname, First Name, Middle Name, Maiden Name and Other Names.
ii. Date of birth
iii. Place of birth
iv. Nationality
v. Religion
vi. Age
vii. Gender
viii. Ethnicity
ix. Permanent address
x. State of origin
xi. Local government of origin
xii. Two-Thumbprint or Ten-print
xiii. Height
xiv. Color of hair
xv. Color of eyes
xvi. Complexion
xvii. Passport Photograph (Colour, Head-to-Shoulder)

An individual can be properly indentified in NIMC database upon submission of the 17 items listed above. Other information may be collected as necessary to enable the stakeholder determine the nature and type of services to be provided. The collection of the data need not be in any particular order since the XML header will indentify the data fields being submitted to NIMC for verification.

i. Indirect access to information upon request: The ability of the various agencies to query and receive results from the NIMC central database is crucial. This function is an integral part of the database. NIMC should ensure that when the data listed above is submitted in the manner

specified in the XML packet, it can provide an answer in the form of Yes/No within a reasonable period of time.

ii. Direct access to the databases of another member stakeholder: The ability of one stakeholder to access information collected by another stakeholder, as the law may permit, is crucial for an effective and efficient ID system. The NIMC central database should be expanded to hold ancillary data points.

iii. Access to information of another member stakeholder through a central index on a hit-no-hit basis: The ability for one stakeholder to access information collected by another member stakeholder through this mode may require that value (monetary or other) be assigned to the stakeholder that collected the data. Two classifications are recommended for determining if access should be classified as hit or no-hit based on the type and nature of the access. Access classified as hit should be chargeable (assigned a monetary value). In all cases relating to identification services deemed as basic rights of the citizen, such access should be classified as no-hit.

iv. The creation or extended use of central NIMC databases: In order to harmonise the collection, use, and control of the identity databases of the various stakeholders, NIMC should allow the various stakeholder agencies to use the data in the National Identity Database (the Central Database).

7.5 Image Quality and Fingerprint Capture Device Specifications

The following specifications apply to fingerprint capture devices which scan and capture at least a single fingerprint in digital, softcopy form. They represent criteria for insuring that the image quality of such devices is sufficient for the intended applications. These specifications also pertain to fingerprint authentication and verification within the NIMC database. All specifications are to be in conformity with global best practice as represented in the NSIT, IEEI and ICAO Standards.

The fingerprint capture device used by any stakeholder must be capable of producing images which exhibit 1) good geometric fidelity, 2) sharpness, 3) detail rendition, and 4) low noise characteristics. The images must be the original representations of the input fingerprints, without alterations or enhancements.

7.5.1 Suggested International Standards (Interpol)

The image quality requirements described below are considered the minimum

standard by several international agencies, including Interpol. The finger print capture devices should be tested to ensure that they meet the requirements in normal-operating-mode, with the following possible exceptions:

i. If the device has a strong anti-spoofing feature, of a type whereby only live fingerprints will produce an image, then this feature needs to be switched-off or bypassed in the target test mode of operation.

ii. If the device's normal output is not a monochrome gray scale image (e.g., it is a binary image, minutia feature set, or color image), then the monochrome gray scale image needs to be accessed and output in the test mode of operation.

iii. Other normal-operating-mode features of the device that are similar or analogous to (1) and (2) above may need to be disengaged.

The following are some of the basic requirements for the single finger capture device. The requirements described below are considered the minimum standard by various international agencies including Interpol.

7.5.2 Fingerprint Image Quality

i. The fingerprint capture device should provide fingerprint image quality which is high enough to support the intended applications of Personal Identification Verification.

ii. The image quality will be assessed against the requirements specified by applying visual and quantitative measurements to test live scans captured on the given device. These test live scans shall consist of:

   a. a set of 20 fingers, nominally acquired from 10 different subjects or a set of 2 fingers per subject (preferably left/right index finger)

   b. a set of 5 index finger repeat captures from the same hand of a single subject.

iii. All of these test live scans shall be supplied for assessment in 8 bits per pixel, monochrome (grayscale), uncompressed format.

8.0 Capacity Issues

The Federal Government should provide NIMC with the resources (financial, human, equipment and other resources) and capacity building training and workshops necessary and required to build its capacities to meet its respective mandates regarding harmonization of the various existing national identification schemes.

The Federal Government should provide the stakeholder agencies with the resources (financial, human, equipment and other resources) and capacity building training and workshops necessary and required to build their capacities to collect, manage, and safeguard biometric data in accordance with internationally accepted standards.

The HIC should develop and implement a certification program for third party companies that provide biometrics data management and administration services for stakeholder agencies.

NIMC should establish a professional training centre to provide capacity building support to both private and public sector stakeholders. The training will focus on subject matters and skills that include finger-printing, data collection and management, privacy and security, networks, etc.

NIMC should continue to thoroughly educate the stakeholder agencies, as well as the citizenry, on the benefits of a harmonized National Identity Management System.

National Identity Management Commission
11, Sokode Crescent, Off Dalaba Street
Zone 5 Wuse
P.M.B. 18, Garki, Abuja Nigeria.