Dec 12, 2012

Roadmap For The Development Of A Centralized Demographic Database

Paper Submitted by Dr Baba J Adamu

Technical Ad-hoc Committee headed by the

SSA (ICT) Office of the Vice President

Dr Baba J Adamu

Background

Nigerian Government is currently undergoing a paradigm shift regarding the use of information technologies in the public sector. Electronic identity management is one element in this planned transformation of the sector with identity management framework being a key enabler in the government's *Transformational Government Enabled by Technology* strategy.

Identity is "*a collection of attributes which helps to distinguish one entity from another*". This is what makes identity a key component in numerous economic, social and political transactions. Being able to link identities to their owner and the effective and secure handling of personal data are essential to numerous different interactions. To this end, infrastructures are developed to group, administer and store data about specific groups of people, such as citizens, customers etc. These infrastructures are Identity Management systems (IMS). The goal is to have Identity Assurance (IdA) in the use of such a system in an electronic environment. This document highlights key policy requirement in developing and implementing a secure identity management framework. The focus here is on creating a roadmap to actualize the implementation of the centralized demographic database, towards the 2016 Census and the development of an enhanced vital Identity Assurance (IdA) registration system on the basis of a methodology recognized and accepted by all stakeholders.

Stakeholders

The proposed centralized demographic database is understood to mean: **"…an electronic register of all Nigerian citizens,"** with the following government agencies represented as stakeholders and being producers, or users of population-related data, notable of which are:

a. **National Population Commission (NPopC)** – with prime responsibility for the national census and population projection and policy

b. **National Identity Management Commission (NIMC)** – with responsibility for managing the national identification scheme.
c. **National Immigration Service** (NIS) – with responsibility for issuing passports and recording the movement of Nigerians and foreigners entering or leaving the country.
d. **National Bureau of Statistics (NBS)** – conducting surveys to inform about socio-economic and living conditions in Nigeria
e. **Others** including the Federal Inland Revenue Service, the Federal Road Safety Corps, National Health Insurance Scheme, Joint Admissions and Matriculation Board, security agencies, EFCC etc. each of which produces or utilizes population data for its specific purposes.

The Roadmap Strategy Process

Strategy: does it mean tactics, long-term goals, or Good Intentions" (We'll do this and that…), or a wish list like this: "Our strategy is to provide leading-edge, world-class products by capitalizing on …etc.!" Our Roadmap strategy is designed to communicate a vision for national and individual security through provision of personal identity, and accurate population register (demographic database); encourage collaborative reflection and action based on competing alternatives, to develop a secure and integrated infrastructure enabling data access and exchange, short and precise.

Developing this roadmap has three major uses:

1. It helps reach a consensus to share, collaborate and create standard data among stakeholders; and a set of NEEDS and the technologies required to satisfy those needs; a system based on the integration of a Distributed Databases.
2. It provides a mechanism to help forecast technology developments and adoption of Grid Computing architectures (scalability) and

3. It provides a framework to help plan and coordinate technology developments that will match short-term and long-term goals with specific technology solutions to help meet those goals.

The Roadmap is a dynamic, 'living' map, which will continue to suggest specific actions towards a digital society in which citizen-centered identity management is based on robust identity assurance.

Together, we need to:

- **Recognize the key role of Identity**: we need to stimulate full integration of identity management and assurance into the Transformational Government strategy, as key enabling mechanisms for improved, electronic public service provision;
- **Build in Identity Assurance** (**IdA) from the outset**: develop a robust identity assurance framework, including technological safeguards, socio-economic safeguards, legal and regulatory safeguards including enforcement mechanisms, to support identity management from its inception, based on a clear, comprehensive, coherent and user-centric vision for identity management;
- **Focus on the user**: promote usage transparency and user-control as central elements of identity management, in order to encourage trust and confidence on the system;
- **Keep stakeholders informed**: provide timely, accurate and unambiguous information on identity management and assurance, to allow for educated and inclusive multi-stakeholder engagement;
- **Research to strengthen IdA-ability**: promote research to support the development of identity management and assurance solutions for which robust, thorough evidence is required;

- **Collaborate to make it work**: establish strong links between government agencies and IT service suppliers, in order to ensure timely, efficient, effective delivery
- **Think global**: engage with identity management and assurance developments at the international level, with particular focus on cooperation, exchange of best practice and expertise, and the development of interoperable systems at the international level.

IN THE SHORT-TERM, BY 2016

Where are we now?

The demographic database and national identity scheme were unsuccessful in the past largely due to lack of harmony and collaboration of the stakeholder agencies. Each agency that generates data wants to have the right to manage, retain and administer it. The way forward as we move toward 2016 is how individual agencies can decide what information they want to make available to other agencies and law enforcement, while retaining ownership of the data and improve their big data efforts.

While existing statutes confer on the National Population Commission (NPopC) official responsibility to manage demographic data in Nigeria especially as regards the population census, National Identity Management Commission (NIMC) is charged with responsibility for managing the national identification scheme and National Immigration Service (NIS) to issue passports and record movement in and out of Nigerians etc. It is generally agreed that NIMC and the National Population Commission should work together and exchange template and system architecture in order to establish an authentic verified centralized database for the country with a single service-point window and data-sharing architecture provided by Ministry of Communications Technology in partnership with Galaxy backbone. Most have argued that presently in Nigeria, It is not enough to collect data from census enumeration or survey, it is important that

before this information is stored in the centralized database of the country there should be a second level or even third level verification of this data to ensure their authenticity before being stored in the centralized database.

In the light of the above, it is hereby recommended in the short term to:

1. Audit all existing demographic data of various agencies to identify identical data which would be collated in the centralized database.
2. Create a centralized Demographic Database System based on the integration of a Distributed Database but that the coordinator of the centralized database should be predicated on the outcome of an evaluation of the existing capacities of agencies involved in data gathering.
3. Develop reference architecture of the framework to be adopted for the integration of existing databases in the centralized system (NIMC and the National Population Commission to work together in this regard).
4. Develop data Standards and determine data that would be shared among various agencies back by law.
5. Create a unique Personal Identification Number (PIN) algorithm, usually 12-digit for every Nigerian citizen that will identify him/her. The number will be stored in the proposed centralized database and linked to the basic demographics and biometric information (NIMC and the National Population Commission to work together in this regard).
6. Determine the best Identity Management systems (IMS) by all stakeholders

Social and Economic Dimension

The social and economic dimensions of Identity Management systems (IMS) are closely entwined and hard to map out as they encompass a large variety of issues. The issue of public trust, for example, has both social and economic implications and is a recurrent concern amongst people involved in developing solutions and services around IMS, both in the public and the private sectors.

Public trust in the security and reliability of an IMS is critical to its success, which can have important economic implications, particularly for businesses. Without a foundation of trust, acceptance and use of the services and processes facilitated by IMS in the public and the private sectors may not reach optimal levels. Conversely, promoting confidence in the identity management framework can contribute to the creation of new commercial opportunities for the business sector and the expansion of existing ones. Whereas both security and (commercial) convenience are attractive options, these advantages should be balanced with the requirement for privacy. There is a trade-off involved, and it is very important that this trade-off is recognized and discussed.

Technical Dimension

The specific technical architecture of an IMS has enormous implications for society. IMS architectures respond to different requirements and approaches to management. They can be centralized and managed by the organization or institution implementing it, or decentralized and user-controlled. They often prioritize certain types of interactions and interfaces, in particular administration to administration (A2A), administration to business (A2B) or administration to citizen (A2C). They may or may not utilize ‘trusted third parties’ for authentication processes. Where they involve electronic identity (eID) or smart cards, they can include different kinds and combinations of biometric data, have different lengths of validity, and incorporate chips with diverse information and applications.

The specific objectives of a system to manage identity create the need for appropriate, fit-for-purpose technologies. Clearly elucidating the objectives early on ensures that the development and deployment of technology will be much more effective and less prone to problems. When considering a national IMS system with obligatory participation, for example, requirements are different from those of more limited systems based on voluntary participation. Also, technologies for enhancing privacy protection of personal data (such as privacy

enhancing technologies or PET) are much less effective and often more complex when added as an “add-on” to an IMS rather than incorporated from the project’s inception.

LONG-TERM GOALS, AFTER 2016 CENSUS

This long-term plan elaborates, in particular:

- Objectives and principles that need to be taken into account for the implementation of a functioning computerized demographic database taking into account legal framework.

Principles for Demographic Database

A demographic database is a system that stores records of personal information of all citizens and non-citizens residing on the territory of a nation that meet the requirement for registration as set out in the relevant legal framework. The data stored in the database is registered in a unique, uniform and transparent way, based on documentary evidence certifying vital life events. Registration is unique and uniform in determining *what kind* of information is stored and *how* information is stored in the population register, and transparent in a manner that ensures citizens’ trust in the nation’s handling of their personal data. Multiple uses of stored personal data by other agencies ensure that all public administration institutions perform their tasks using the same information coming from the population register (demographic database).

A demographic database provides benefits to the entire nation’s public administration by allowing it access to legally valid personal information required to improve services and provide quality products to citizens in all policy areas, i.e., health, labour, justice, education, welfare, property ownership, driver licenses and emergency services, etc. In return, citizens are provided with quicker and better-quality services.

In order to establish a database that delivers these benefits, it is important to adopt a high performance universal inter-operability database with the following objectives and principles, which are considered common practice in most countries with a functioning electronic population registration system (database).

Two main objectives should be achieved to run an efficient population register. First, it requires that for each individual residing on the territory should be only one file in the register containing his/her personal information: "***one person-one file."*** Secondly, for the purpose of providing access to the data for individuals and other agencies, it is necessary to create conditions for the subsequent multiple use of registered data by electronic means: "***register once - multiple use of information"***. The solution gives: **universality, uniqueness, permanence, measurability, acceptability, scalability, dependability** and **security** on a centralized data warehouse enterprise wide approach**.** This standard format is in line with international Best Practices.

Establishing the first objective for running a demographic database should ensure that a person is only registered once in the database, and any duplication of data should be prevented. Once the "***one person, one file"*** objective is ensured, only then does the second objective, "***register once - multiple use of information",*** become important. The use of personal information stored in a population register by public institutions (as defined by law) should ensure optimal use of personal data within the public administration and within the framework of data protection and other legal safeguards. The first objective ensures data quality; the second objective ensures the proper use of data by all public institutions, thus leading to an improvement in state services.

The need for information sharing

The need for information sharing will endure as the complexity of the national security threat environment demands situational awareness and participation by partners across the spectrum. This Information Sharing will give security

operatives the capability to ensure law enforcement remains relevant to this process in a manner consistent with national security and applicable legal standards relating to privacy and civil liberties.

A centralized demographic database requires the adherence to, among others, the following main principles:

- *Based on a chosen administrative division (and territorial bodies), personal information is collected, verified and registered at the level of the local authorities*

Registered information is communicated electronically to and maintained at the central level. The local level is responsible and accountable for the collection, verification and registration of citizens. The maintenance of registered data, or the responsibility and accountability for the data quality of the population registration system, is done at the central level (through verification to avoid duplication).

- *Registration and maintenance of data is based on a sound legal framework.*

A population registration system must be based on well-developed laws, bylaws, and instructions and procedures.

- *Uniform registration should provide that registration is performed in the same way by every local office, ideally based on a computerized system.*

Uniformity in collecting, verifying and registering citizens' civil status data at the local level is essential to ensuring data accuracy. This means that clear procedures for the registration of place of residence and civil status events should be in place. Relevant local authorities need to be trained on the registration procedures and to apply them in a uniform manner. The uniformity of the population registration data collection, updating, verification and registration

procedures should be validated by a software platform that runs the Population Register. Uniformity will be controlled by means of system log files and audit trails, based on performance indicators presented through regular information updates to the management of the Population Register.

- *The registration of a person is comprised of a comprehensive set of data.*

In order to create conditions for the registration of vital life events in a person's life cycle, every person is represented by a personal file in the population register. Each file is composed of relevant data divided into a number of categories. The number of categories depends on the choice made as to which type of information will be registered. A category can contain only current data or current and historical data. Some categories of personal information in the population register should be mandatory components of a personal file.

- *Data stored in the population register consists of complete, correct and up-to date data, as well as historical data (historical data is created by the system automatically after every update of personal data).*

The data in the Population Register should be complete (all citizens and resident non-citizens should be registered), correct (registered data without misspellings, etc.) and up-to-date (reflecting the persons current civil status and residence).

- *The registration of a person should provide the person with a legal identity.*

Complete, correct and up-to-date data in the Population Register should contain legally valid data for the citizen establishing their legal identity before the state. Therefore, registered personal data need to accurately reflect a person's unique civil status and the person's place of residence (address).

- *Upon birth-registration by local authorities, the Personal Identification Number (PIN) is automatically issued by the population registration system.*

The citizen's PIN represents the unique personal identifier, which is required to make an unambiguous identification of a person in the population register when providing services; Birth registration should automatically lead to the issuance of a PIN by the population registration system according to the same algorithm unanimously agreed by all stakeholders.

- *Registration authorities should be trained regularly on the legal framework and the operation of the computerized population-registration system.*

To maintain the uniformity of registration data, as well as data accuracy, it is essential that registration authorities are regularly trained on population registration legislation, instructions and procedures, as well as on the computerized platform that is running the population register.

- *Data accuracy should be safeguarded by procedures and enforced through a cycle of systematic and continuous audits.*

To further ensure data accuracy, legal obligations and registration processes at the local level, a system for regular auditing of local offices should be put in place.

- *Other public agencies/institutions are granted access to personal information in the population register, provided that those institutions are authorized to do so by law.*

If the data accuracy of a population register is sufficiently ensured through staff training, uniform registration and audited processes, then the civil status data can be distributed to authorized third parties for the purpose of providing services.

- *Products (such as passports, ID-cards, certificates, voter lists and statistics) will only be produced on the basis of information stored in the population register.*

Services provided by the state that require the use of personal data for the production of passports, ID-cards, certificates, voter lists, and statistics should make mandatory use of personal identity data stored only in the Population Register.

Next to the objectives and principles of population registration, proper planning needs to precede the implementation of the register. In that context, it is essential that the following are clearly set out:

- A vision on the future of Population Registration (What is the goal?)
- Understanding the power of information, i.e., how to achieve and maintain data quality, how to establish data protection and how to raise awareness among the general public. (How to manage and maintain)

Responsibilities and Operational Capacities of the Stakeholders

Administration

Ministry of Communications Technology	• Establishing of 'single window' service point • Establishing data-sharing architecture in accordance with the law.
National Population Commission (NPopC)	• Establishing a functioning Population Registration system • Births, marriage, deaths registration
National Identity Management Commission (NIMC)	• Responsible for issuing and managing the national identification scheme.

National Immigration Service (NIS)	• Responsible for issuing passports and recording the movement of Nigerians and foreigners entering or leaving the country.
National Bureau of Statistics (NBS)	• Conducts surveys to inform about socio-economic and living conditions in Nigeria
Federal Road Safety Corps	• Responsible for the application and issuance of driver licenses and vehicle registration
Galaxy Backbone	• Responsible for the maintaining of IT systems on the instructions of the MofCT

IMPLEMENTATION REQUIREMENTS

Legal Framework

The legal framework defines the relevance of population registration in the context of other tasks to improve collaboration and sharing of data. The population register will not only store information on citizens but will also provide access to registered information to authorized users to enable them to perform their tasks. Therefore, while the NPocC determines the manner in which information will be processed in the system, procedures for data processing should be based on provisions elaborated in the legal framework.

Information Management

The Population Registration system should only have a central storage system to which other agencies or local offices log in via web-services (fully secured). The local offices will obtain access to the main system via the Internet (web-services) and will be able to access all information. However, they can only update information concerning their own area of responsibility. Other information is available only for viewing.

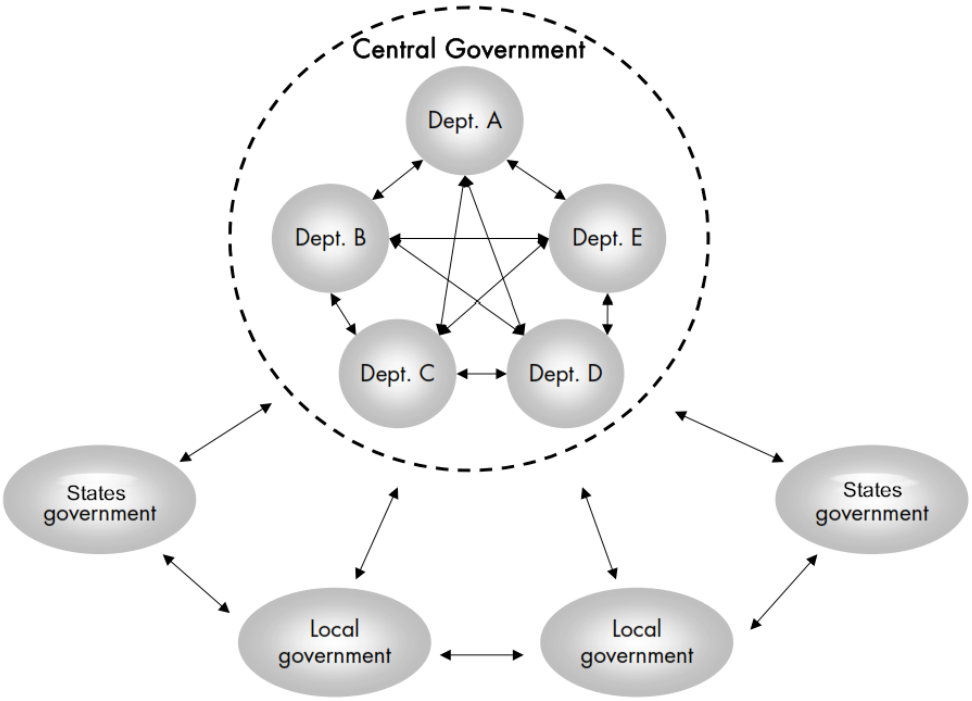
Web-services provide the advantage of eliminating the need to control local databases, as only one database stores the entire data. In addition, software updates only need to be installed at the central level and become immediately available to all local offices. Maintenance and control of the system will be done at the central level only.

Control mechanisms can be put in place more easily by providing maintenance when the data is stored centrally. It needs to be emphasized, however, that the functioning of the population register without local databases in place relies heavily on the availability of a data-transfer network. In the instances where the network connection is off, the system will cease to deliver services. Government should, however, invest in ensuring permanent connectivity.

If the population register is maintained centrally, this also requires that there is a back-up mechanism in place, provided via the data-recovery center in case of a breakdown of the main population-register database. This data recovery center needs to be located at a different location than the central database to allow data recovery in case of serious damage to or destruction of the premises that host the population-register database.

Network coverage

It is essential to establish a data-transfer network to transfer data from the local to the central level, and vice-versa. The assessment identified two issues that would need to be available: implementation for a data-transfer network and connectivity in remote parts of the country. Ideally, fiber optic cable is needed to connect the central database and offices at the local level, but some geography maybe impossible to establish such a link, which calls for using Satellite communications.



Pathways of Information Sharing in Government

In terms of short-term network requirements for population registration, it would be useful to consider a mixed solution that would incorporate secured hardwire network, satellite and, perhaps, mobile teams to establish conditions for data transfer. It is important to establish nationwide connection coverage since, in the instances when data transfer is done on a partly automatic and partly manual basis (optical discs, flash drives or similar), it brings with it high risks to data

accuracy, as discs might get lost or forgotten to be merged with the central database. Consequently, manually delivered civil status data will not provide for the storage of up-to-date information in the population register.

A satellite network can be considered as a possibility for the establishment of a secured network for data transmission, and should be considered, in any case, in rural areas as terrestrial links would be hard to establish. The establishment of a satellite network in rural areas can be done relatively quickly (in 2 or 3 months or less). It is considered the most secure way of transmitting data from the local to the central level, with the use of central hub connectivity.

Best practice for user control of electronic identity

Project allows users to administer and control their personal information online, which can later be accessed by the public and private sector organizations involved in the scheme. In this way, user control and data sharing are combined, promoting trust and acceptance by all stakeholders, citizens in particular. The scheme's central tenet is that of 'self-administering consent'. An additional advantage is that people choose their own service level by giving explicit consent to use of their personal data for specific purposes, which means that legal constraints are explicitly met.

There are three main arguments that plead for explicit citizen acceptance of data sharing of their personal information:

1. Consent – even if it is not always required by law;
2. Visibility – who wants to/has access to a person's data; and
3. Security – that the information is only used for legitimate purposes.

These are essential for the creation and maintenance of trust and collaboration between stakeholders in the scheme.

Awareness Raising, Education and Open Debate

Awareness is essential to any identity management project. Inadequate public information and awareness of privacy rights and of the objectives, requirements and implications of proposed identity management frameworks can negatively affect open debate around and acceptance of the scheme. The provision of timely, clear and definitive information to all stakeholders must be an integral part of the project from its inception. It can help ensure that misconceptions are minimized, and promote favorable reception of the policy. A multi-stakeholder debate will allow the unveiling of those areas of conflict that need to be addressed through appropriate actions and policy measures. This is also pertinent to the development of a multi-stakeholder identity assurance framework.

Conclusion

With this Report, I have provided a Roadmap for implementation in the short and long term centralized demographic database for the county.