National Identity Management

Nimc

Commission

National Identity Management and Harmonization Committee

National Identity Management System

Handbook on Business Processes, Standards and Specifications

6th January, 2011

Version (working document)

Revision History

Revision	Date	Document Status	Participants/Comments
1.0	29 March 2010	Release	Initial release of the NIMC working document
1.0.0.1	1 April 2010	Updated Release	Second reading and review by Hon. Ken Nwabueze, added section 4 for fee
1.0.0.2	21 April 2010	Updated Release	Incorporated all the changes agreed to on the NIMHC meeting held on 12 April 2010
1.0.0.3	22nd April 2010	Update Release	Incorporated all the changes agreed to on the NIMCHC meeting held on 22nd April 2010
1.0.0.4	28th May 2010	Update Release	Incorporated all the changes agreed on the NIMC Main HC meeting held on the 25th May 2010
1.0.0.5	8th December 2010	Update Release	Incorporated the work of Biometrics sub-committee
1.0.0.6	18th December 2010	Update Release	Incorporated the work of Data and Verification sub committee
1.0.0.7	30th March 2011	Update Release	Incorporated the comments and changes of Technical Committee of NIMC Board

Change Request

CR ID	Change Request (CR) Description
CR-0001	Resolve that fees be charged based on hits or no-hits basis
CR-0002	Resolve that Early Adopters Program be implemented by NIMC
CR-0003	Resolve that the draft report be accepted and submitted to a technical writer for final draft
CR-0004	Resolve that the sub-committees of Biometrics and Data & Verifications be constituted

1 Background

Since independence, Nigeria has always recognized the need to document the identity of Nigerians and non-citizens using biographic data. An attempt to meet this need was initiated in 1978 under the Department of National Civic Registration (DNCR), which was charged with registering and issuing a National Identity Card to every citizen of Nigeria who was then 18 years or older. The government's primary objective then was to use this program as an effective tool for controlling illegal immigration, to validate other civic documents like travel passports, and to set up a reliable personal identification system for securing commercial transactions with financial institutions and the like.

There is currently no centralized national identity database and no system of National Identity Management which efficiently links public and private sector identity schemes. While the financial services sector has been most proactive in the deployment of identification schemes for delivery of its services, the schemes have differed from institution to institution within the sector. The result has been the creation of several different identification schemes and databases leading to the duplication of an individual's identity data by the various institutions offering services to that person. Government agencies also hold a number of databases with no viable integration of access or interoperability to enhance the delivery of services within these government institutions. This is despite the fact that some of these institutions have introduced smart card technology into their schemes. A reliable national system for verification and secure authentication of an individual's identity has thus not been established.

The main motivation of biometrics standards is to define requirements, formats and software specification enabling interoperability between biometric systems, especially authentication systems.

Biometric standards enable levels of interoperability. High level standards enable interoperability of data collections and storage processes.

1.1 Purpose and Scope

This Handbook is intended to provide a high-level generic biometric standards and specifications in Nigeria; one suited for anyone to gain basic knowledge and understanding the rules for use of biometric technology in National Identity Management System (NIMS).

It covers the basic functions of Enrollment, Verification, and Identification, and includes basic standards to allow only approved agencies, organizations, and entities to manage and ensure interoperability of their system with the integrated national system.

1.2 NIMC Mandate and National Identity Management System

NATIONAL IDENTITY MANAGEMENT COMMISSION ACT, 2007 ACT No. 23

AN ACT TO PROVIDE FOR THE ESTABLISHMENT OF A NATIONAL IDENTITY DATABASE AND THE NATIONAL IDENTITY MANAGEMENT COMMISSION CHARGE WITH THE RESPONSIBILITIES FOR MAINTENANCE OF THE NATIONAL DATABASE, THE REGISTRATION OF INDIVIDUALS, AND

THE ISSUANCE OF GENERAL MULTIPURPOSE IDENTITY CARDS; AND FOR RELATED MATTERS

PART II—FUNCTIONS AND POWERS OF THE COMMISSION

5. The Commission shall

(a) create, manage, maintain and operate the National Identity Database established under section 14 of this Act including the harmonization and integration of existing identification databases in government agencies and integrating them into the National identity database ;

(b) carry out the registration of citizens of Nigeria into the National Identity Database ;

(c) carry out the registration of non-citizens of Nigeria who are lawfully resident in Nigeria ;

(d) issue a General Multi-purpose Identity Card to any person registered pursuant to paragraphs (b) and (c) of this section ;

(e) collate information obtained by the Commission in pursuance of its functions under this Act and reproducing such information as may be required, from time to time ;

(f) assign a unique National Identification Number to any person registered pursuant to paragraphs (b) and (c) of this section and the National Identification Number shall be incorporated into or made compatible with other existing identity related databases or registers in respect of which information or data relating to the registered person has been registered, documented or stored ;

(g) ensure the preservation, protection, sanctity and security (including cyber-security) of any information or data collected, obtained, maintained or stored in respect of the National Identity Database ;

(h) establish and maintain secured communication links with any existing relevant identity related database or agency ;

(i) maintain secured communication links with end users in any public or private organization, agency or body including Card Acceptance Devices, Government Service Centers ;

(j) collaborate with relevant bodies and agencies in setting of standards and technical specifications for telecommunications links between organizations and for the devices utilized for such communications established or maintained pursuant to paragraphs (j) and (k) of this section ;

(k) respond to verification enquiries regarding the identification of individuals ;

(l) perform such other duties which, in the opinion of the Commission, are necessary or expedient for the discharge of its functions under this Act ;

(m)enter into any form of agreement with any private or public sector based agency or organization for the development or establishment of the Identity Management Solution or for the realization of any of its functions ;

1.3 Authority of National Identity Management and Harmonization Committee (NIMHC)

National Identity Management Commission, in discharging of its duties, on July 2009 constituted a body to be known as the National Identity Management and Harmonization Committee (NIMHC) to become the custodian for setting standards for National Identity Management System.

By the extension of the National Identity Management Commission Act, Section 5, part (j), NIMHC established rules and standards shall be binding on all subjects, agencies, organizations, and entities that are collecting, disseminating, or consuming identity data in Nigeria.

1.4 Change Control

Any financial or technical change can be brought up by any agency or member of the committee to the technical sub-committee/consultant which would be deliberated by the sub-committee and sent to the main NIMCHC for final approval. However there should be a consensus whereby the chairman would move a motion that certain changes can be made.

1.5 Contact information

1) The Director General / Chief Executive
National Identity Management Commission
11 Sokode Crescent, Off Dalaba Street
Zone 5, Wuse
P. M. B. 18, Garki – Abuja
Phone: +234-9-6726457
Fax: +234-9-5230637

E-mail: info@nimc.gov.ng
www.nimc.gov.ng

2) Director Identity Database
National Identity Management Commission
Phone: +234-9-8702329
+234-9-6726457
E-mail: aliyuaziz@aliyuaziz.com
www.nimc.gov.ng

1.6 National Identification Number (NIN)

The National Identification Number (NIN) is a 9-digit number that is unique to each Nigerian that has registered with National Identity Management Commission. The NIN is assigned to an individual at the time of the initial registration with NIMC.

NIN is associated with a single set of biometrics belonging to the subject (individual) that has been assigned the NIN. NIN is not the same as the National ID card number which may expire, discontinued, or be re-assigned.

1.6.1 NIN Assignment

Only NIMC can assign the 9-digit NIN to a subject. Once NIN is assigned to a subject, it can never be changed or altered in any form. NIN does not expire and is valid for the entire life span of the subject biometrics that it was assigned to.

1.6.2 Use of NIN

NIN shall be the basis of which the Federal, State, and Local government shall interact with a citizen of Nigeria. Each Ministry, agency, regulatory body, and entities must tie an individual to a NIN before services can be rendered to the individual.

1.7 Domain Code and Origination Identifier

Domain Code is a 6-digit number that is assigned to an agency or organization. It is fixed and unique for each entity collaborating with NIMC. The first three digits indicate the ministry or agency that oversees the entity or the regulatory body that is governing the activities of the entity. The last three digits indicate the assigned numbers for the department, commission, or agency.

For private sector entities and other none governmental agency, the first three digits shall indicate the Biometrics Service Provider (BSP) that is providing them links into NIMC Gateway.

The Origination Identifier digits are used to delineate the various locations or centers that the entity may capture and transmit data to their central hub or directly to NIMC Gateway. The mandatory origination identifier field shall contain the 6-digit number exclusive to that location. The BSP shall assign origination identifier to those entities that submit data through them.

Any submission made to the NIMC Core or Gateway shall have Domain Code and Origination Identifier contained in Type 1 or Type 14 record as in Appendix Form 2

1.8 Transaction Control Code (TCC)

Transaction Control Code is unique code assigned to each set of biometrics submitted by an enrollment agency. It shall be the primary indicator carried through the life of the subject's biometrics data to indicate the original source of the record. TCC shall always be 16-digit randomly generated code. NIMC shall assign each enrollment agency the 4-digit prefix for the TCC and the remaining 12 digits generated by the computer system.

A TCC identification number is assigned for a submission and carried through on to the response for tracing purposes. The TCC shall be generated by the system that submits the transaction. A reference identification, Transaction Control Reference (TCR), number is returned by NIMC so that the originating submission request can be identified. When an enrollment for obtaining ID cards transaction is sent to NIMC, the TCR in the response(s) will contain the TCC used in the submission. A TCC is mandatory for a submission, and a TCR is mandatory for a response. These values must be contained in the Type-1 or Type-14record as in Appendix Form 2 of the transaction.

TCC and TCR combined shall serve two purpose of

1) as evidence that an enrollment for obtaining ID cards record was successfully made and acknowledgement received for the submission,

2) as evidence that the submitting agency has lease rights to that set of biometrics.

1.9 Transaction Record Number (TRN)

Any entity that submits request to NIMC shall receive a response for their submission. The response shall include a unique record number known as Transaction Record Number (TRN). This number shall be associated with a single request in NIMC Gateway database.

TRN shall serve two purposes of

1) as evidence that a request was made and a response received for the request, 2) as evidence that PIV service was provided and in case of "HIT" shall serve as the billing code.

The submitting entity shall keep TRN as proof that NIMC provided PIV on the subject in case of issues relating to the true identity of the subject.

1.10 NIMC Core Database (Super Structure)

The NIMC Core Database, also referred to as the NIM Super Structure is the only authoritative database recognized by the Federal Government to provide Personal Identification Verification (PIV) services in Nigeria. In cases of civil or criminal proceedings, NIMC PIV shall override all other forms of identification.

1.10.1 Definition

The Core, for all intensive purposes, include the overall infrastructure put in place by NIMC for the purpose of enrollment and provision of Verification of identity services. It includes the primary and backup datacenters, AIFS database, associated network and security systems.

1.10.2 Access

Direct access to the NIMC Core by any third party shall be prohibited. All access to the system shall be through the Gateway. All access to data in NIMC Core must be predetermined, approved, and use of the data clearly stated in NIMC Data Access Form as in Form 2 above.

1.11 NIMC Gateway (data exchange engine)

The NIMC Gateway Database, also referred to as the NIMC Sub Structure is created from NIMC Core for use in providing Personal Identification Verification (PIV) services in Nigeria. It holds enough information; including fingerprint templates, to authenticate an individual based on subset of the original biometrics captured from the individual.

1.11.1 Definition

The Gateway, for all intensive purposes, includes the overall infrastructure put in place by NIMC for the purpose of verification and easy authentication of identities. It includes the primary and backup datacenters, AIFS database, and network systems. It extends into any infrastructure put in place by a NIMC certified private sector Biometrics Service Providers (BSP) for the sole purposes of providing services on behalf of NIMC.

1.11.2 Access

Direct access to the NIMC Gateway by any third party shall only be after obtaining proper credentials from NIMC. All access to the system shall be documented and each transaction record kept for billing purposes. Records of request for identify verification shall be kept for as long as it is may be mandated by law. All access to NIMC Gateway must be predetermined, approved, and use of the data clearly stated in NIMC Data Access Form as in Appendix Form 2.

1.11.3 NIMC Core vs. NIMC Gateway

The major difference between Core and Gateway can be viewed from the point of view of the main purpose each database was to serve. The Core is primarily for enrollment, long term storage, and protection of personal identities of Nigerians. The Gateway is primarily for verification, short term storage, and record keeping of transactions involving identities of Nigerians.

The Gateway is a subset of the original submission of biometrics data stored in the Core. The information contained in the Core is more detailed than what is in the Gateway. Majority of information stored in the Core are rarely used in daily type transactions. There is greater need of preserving the information in the Core by restricting physical and virtual access to the system. The Gateway on the other hand, needs to allow accessibility to ensure effective use of biometrics as means of controlling crime, enabling safe financial transactions, and promoting cooperation with international organizations.

1.12 Early Adopter Program

The early adopters program is designed to enable rapid development and deployment of effective National Identity Management System. The early adopters were picked for various reasons which were deemed necessary for development and harmonization of identity databases in Nigeria. The early adopters shall assist NIMC in an experimental way to test-run many of the systems and processes that are being implemented. The following were the early adopters

- Nigerian Communication Commission (NCC): NCC was picked for their SIM Card Registration project. This project shall serve to define the rules, provide practical experiences, and fast track the development of NIMS in the following area:
  - Mass enrollment, with an estimated 45M subjects added to NIMC database

- Federal Road Safety Commission (FRSC): FRSC was picked for their smart card, machine readable driver's license project. This project shall serve to define the rules, provide practical experiences, and fast track the development of NIMS in the following area:

  - Issuing of NIMC certified chip based smart cards that shall be used as primary form of ID card

- Central Bank of Nigeria (CBN): CBN was picked for their new licensing and regulatory of Credit Bureaus money Deposit Banks (MDBs). This project shall serve to define the rules, provide practical experiences, and fast track the development of NIMS in the following area:
  - Regulatory agency extending the use of biometrics for effective governance
- XDS Credit Bureau (XDS): XDS was picked as private sector user of identity verification services. Their inclusion can serve to define the rules, provide practical experiences and fast track the development of NIMS in the following area:
  - Private sector that is both registration organization and verification entity
  - Expend the concept of billing for verification services
- SageMetrics Nigeria Limited (SageMetrics): SageMetrics was picked as private sector Biometrics Service Provider. Their inclusion can serve to define the rules, provider practical experiences and fast track the development of NIMS in the following areas:
  - Private sector Biometrics Service Provider (BSP) to facilitate extension of verification services to entities that are not allowed to link directly to NIMC Gateway
- JTB: JTB was picked because they were the first to deploy AFIS technology with the support of Face Technology. It is expected that the ten (10) fingerprints and picture biometrics would be captured. Their inclusion can serve to define the rules, provider practical experiences and fast track the development of NIMS in the following areas:
  - Regulatory agency extending the use of biometrics for effective governance
- PENCOM: PENCOM has an AFIS implementation project. It has acquired application and it is making efforts at validating its data. Their inclusion can serve to define the rules, provider practical experiences and fast track the development of NIMS in the following areas:
  - Help facilitate verification services
- Zenith Bank Plc: Zenith bank was picked as a financial institution which widely used by Nigerians due to the leadership status in the deployment of Information and Communication Technology in the banking industry. This project shall serve to define the rules, provide practical experiences, and fast track the development of NIMS in the following area:

    - Financial sector that would help checkmate fraud

2 Process

2.1 Application process Overview

Enrollment into the NIMC Core database shall be reserved exclusively for NIMC. By statue of the laws of Federal Republic of Nigeria, it is only NIMC that shall provide enrollment services. There are exceptions where enrollment shall be temporarily delegated. However, under no circumstance shall enrollment be performed without the purview of NIMC. Enrollment may be delegated in the following cases;

- NIMC as the project manager: In cases where NIMC is appointed the project manager to manage the overall project or at least to manage the enrollment aspect of the project involving biometrics. Example of this instance is the case where NCC appointed NIMC the project manager for the SIM Card Registration (SCR) project. NIMC, in this case, may use the SCR project as an enrollment into NIMS. For a project to be used as enrollment into NIMS, it must meet the following conditions:
    - NIMC shall retain total control of the enrollment process
    - The facilities to be used as enrolment centers shall meet the minimum standards for an enrollment center as specified in NIMC Standards for Enrollment centers
    - The front-end (capturing and scanning) equipment, data transmission standards (BioAPI), and back-end (servers, AFIS) Must meet the minimum requirement specified in NIMC standards for capturing devices, datacenter, and network protocols.
- Federal Government Ministry, Department, or Agency which National Assembly act creating them explicitly authorized them to collect biometrics data for the purpose issuing of some form of an identification card. These shall include Federal Road Safety Corps, Pension Commission, Independent National Electoral Commission, and any others. It shall be noted that only NIMC is mandated by a National Assemble Act to collect and store biometrics data for the purpose of Personal Identification Verification (PIV) services. For any agency to provide enrollment services into NIMS Core, it shall meet the following conditions:
    - Use 10-print rolled or flat scanners that meet NIMC standards for enrollment process

- Harmonize their data collection form with NIMC data fields to ensure that all the fields needed for subject enrollment is captured in their form
- Take biometrics data only in cases where the subject did not provide valid National ID card (General multipurpose card ,GMPC) or that match-on-card could not be performed at the initial enrollment time
- All facilities to be used as enrolment center shall meet the minimum standards for enrollment centers as specified in NIMC standards for enrollment centers
- The front-end (capturing and scanning) equipment, data transmission standards (BioAPI), and back-end (servers, AFIS) shall meet the minimum requirement specified in NIMC standards for capturing deceives, datacenter, and network protocols.

2.2 NIMC Approvals

Regardless of organizational classification as stated in 2.2 above, approval for access into the gateway shall fall into two broad categories of:

1) Identification (enrollment)

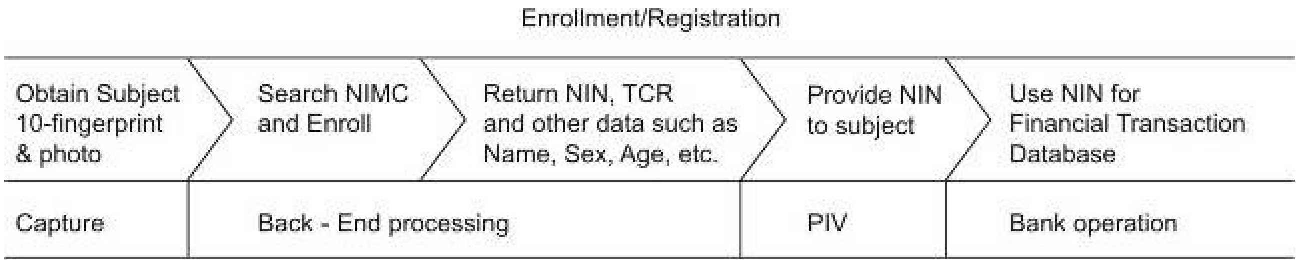
2) Verification

2.2.1 Identification (Enrollment)

The function of identification is to map a known subject to an unknown entity so as to make it known. The known subject is called the identifier (or ID) and the unknown entity is what needs identification. A basic requirement for identification is that the ID be unique by issuing National Identity Number (NIN) to subject (individual). IDs are going to be built out of a collection of Biometrics such that they are unique on the collective.

Identification is the capability to find, retrieve, report, change, or delete specific data without ambiguity. This applies especially to information stored in databases. In database normalization, it is the central, defining function to the discipline. An example of how it would work using the financial system is illustrated in Figure A

Example: Figure A


Enrollment/Registration
Obtain Subject 10-fingerprint & photo
Search NIMC and Enroll
Return NIN, TCR and other data such as Name, Sex, Age, etc.
Provide NIN to subject
Use NIN for Financial Transaction Database
Capture
Back - End processing
PIV
Bank operation

2.2.2 Verification

Verification shall always be done through the Web Services, except in special cases as determined by NIMC.
Web services are typically application programming interfaces (API) or web APIs that can be accessed over a network, such as the Internet, and executed on a remote system hosting the requested services.

In common usage the term refers to clients and servers that communicate over the Hypertext Transfer Protocol (HTTP) protocol used on the web. Such services tend to fall into one of two camps: Big Web Services and restful Web Services.

Access to NIMC Gateway for verification purpose requires use of card acceptance devices only.

Step 1: Complete NIMC Access Form, the form shall have

- The organizations name, address, and contact information
- The organizations selected Biometrics Service Provider (if any) and technical consultants (if any)
- The type of access required for by the organization
- The data fields that are required by NIMC and the information and format of data fields to be returned by NIMC
- If application is accepted, NIMC will assign the applicant their unique fixed 6-digit Transaction Control Code (TCC) and format for the variable 4-digit origination identify.

Step 2: Complete NIMC Technical Certification Form as in Appendix Form 4 and 5, the form shall address

- Network devices and protocol to use in accessing data. It is the responsibility of the organization (or their BSP) to ensure that the devices and protocols meet and exceed NIMC minimum standards as in Appendix C

Step 3: Complete NIMC Business and Process Certification Form as in Appendix Form 7, the form shall address

- Process for collection and storage of data
- Process for training, human capacity, and operators involved in the verification process
- Other business rules, SLAs, and performance targets

Step 4: Sign NIMC Gateway Access Agreement Form as in Appendix Form 9, the agreement shall address

- Terms and conditions of access to the Gateway

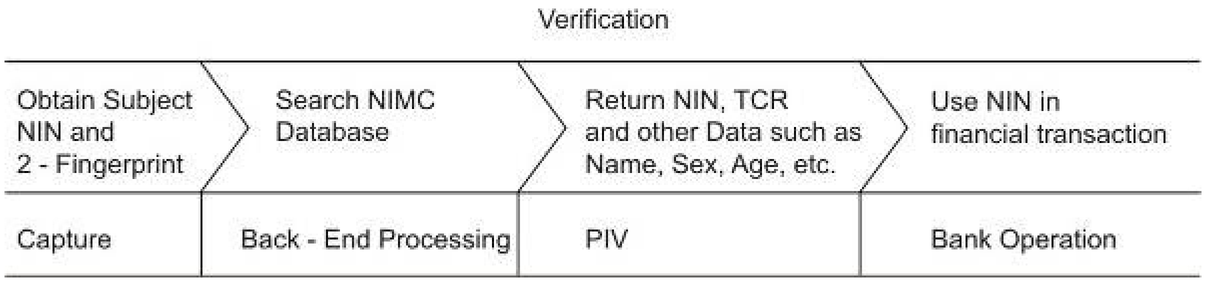
- Applicable fees charged by NIMC, accounting procedures, and method for account reconciliations and any fee that will be paid by the subject
- Warranties and other contractual obligations which must be included in the end-user application/form signed by the subject

Step 5: Testing and pilot phase as defined in section 2.5.1

Step 5: Deployment and monitoring as defined in section 2.5.2

An example of how it would work using the financial system is illustrated in figure B below.

Example: **FIGURE B**


Verification
Obtain Subject NIN and 2 - Fingerprint
Search NIMC Database
Return NIN, TCR and other Data such as Name, Sex, Age, etc.
Use NIN in financial transaction
Capture
Back - End Processing
PIV
Bank Operation

2.3 Rejections and remedies

2.3.1 Definition of Rejections

Rejection means to turn somebody down, to decide not to give somebody something asked or applied for such as access to Data.

NIMC may in cases where it has determined that the applicant is not qualified based on NIMC applicable standards, reject the application to use biometrics services. There are cases where NIMC shall not grant a request for access

- It cannot be determined the actual reason why an organization is seeking to have access to biometrics data
- The applicant has failed to demonstrate that it has met all the NIMC standards for accessing National Identity Management System
- The applicant previously violated NIMC acts and standards
- The applicant, parent organization, regulatory agency, or affiliate is not in financial good standings with NIMC.

2.3.2 Definition of Remedies

Remedies are a legal means of enforcing a right or of providing redress. It is also a way of putting something right or getting rid of something undesirable. NIMC shall create an agreement form which would include remedies for any defaulter for any organization that wishes to have access to NIMC Biometric Data.

2.4 Pilot / testing, deployment, and monitoring

2.4.1 Pilot phase

The pilot phase consist of testing for connectivity, data exchange, verification request, verification response, error handling procedures, billing and reconciliation, network access and security, and shut down procedures.

2.4.2 Deployment phase

The deployment phase shall only commence after execution of NIMC Gateway Access Agreement and after successful completion of the pilot phase. The deployment can be rolled out in phases, to the needs of the applicant.

2.4.3 Continuous performance monitoring

The goal of this project is to harmonize the data of all government agencies and citizens of Nigerians in order to provide operators with access to improved information to identify individuals more efficiently and reduce other operating costs. One approach to improving the access of data, and hence facilitating their repair, is to provide continuous performance monitoring. This approach has been shown to produce practical benefits in daily operations by allowing the identification of networking problems to be solved immediately.

3 Use of Biometrics Policy Guideline

3.1 Enrollment into NIMC core database

Enrollment into the NIMC core database is function reserved exclusively for NIMC. The following guideline shall apply;

- Any agency that shall perform enrollment into the NIMC Core database must first obtain permission from NIMC. NIMC shall retain complete control of the enrollment process used by the agency
- Any agency that shall perform enrollment into the NIMC Core shall do so using the same standards as official NIMC enrollment center. Each enrollment center shall be certified by NIMC
- NIMC reserves the right to reject any enrollment data from any third party enrollment center for non-compliance.

3.1.1 Authorized Enrollment Agencies

- The agency shall obtain Transaction Control Code and Origination Identify for each center from NIMC
- The agency shall only act on behalf of NIMC. Their registration process shall include all the data fields required by NIMC as outlined in Appendix G
- The agency shall implore 10-print biometrics for capturing fingerprints as outlined in Appendix C
- The agency shall have the capability to securely store the data and transfer the data to NIMC based on the network standards outlined in Appendix J
- The agency shall have NIMC Certification for each manufacturing number and model of any device used in capturing data, processing data, and transfer of data to NIMC
- The agency shall have AFIS system capable of storing the fingerprint raw data, fingerprint record data, and fingerprint template data for a period not less than 6 months
- The agency shall retain only the template data after having transmitted the complete data to NIMC and obtain National Identify Number (NIN) for the subject submitted
- The agency shall have the subjects NIN before any services can be offered to the subject. In the event that NIMC Core is not accessible after 72 hours of attempted connection, the agency shall issue Enrollment ID to the subject and provided services based on the same.
- The Biometric Data from the registration system of the enrollment agencies would be automatically deleted from the enrollment center system 72 hours after transmitting to NIMC.
- The agency shall have the capacity to replace the Enrollment ID issued by NIMC Core as soon as NIMC Core becomes available.

3.1.2 Enrollment process flow

Any agency involved in the enrollment process shall follow these procedures. Details of the procedure are outlined in NIMC Enrollment Procedure Form. The procedural overview outlined below is a summary of processes after the agency must have complied with all NIMC standards and certification process.

1. Obtain authorization from NIMC to become an enrollment agency
2. Obtain Domain Code to identify the agency, obtain fixed 4-digit unique Transaction Control Code (TCC) for the agency, and obtain variable 4-digit Origination Identify to be used in identify each enrollment center operated by the agency. Type 1

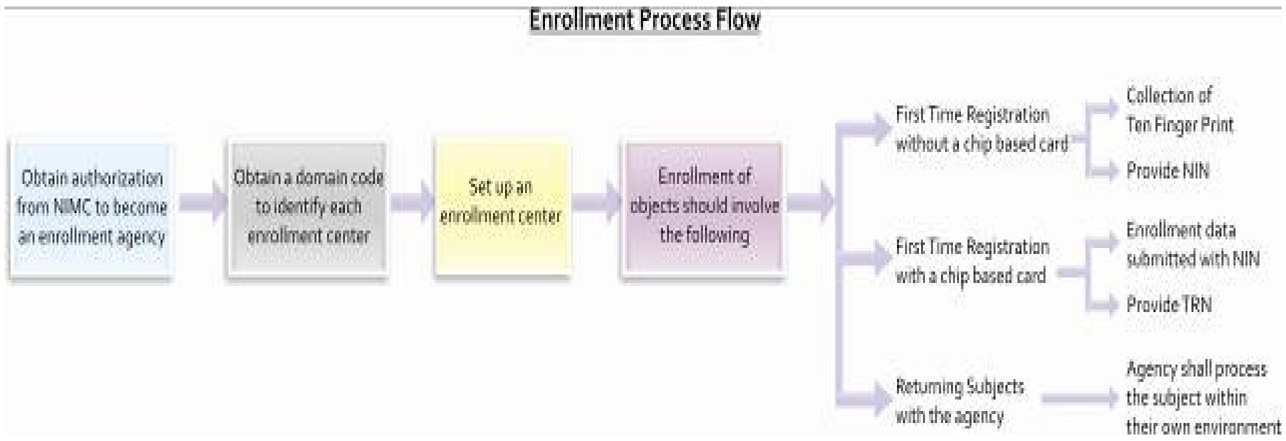
record as in appendix Form 2, submitted from any enrollment center must contain the Domain Code, TCC, and Origination Identify

3. Setup an enrollment center to include facilities for capturing fingerprints and photos (enrollment), and facilities for verification, including on match-on-card capabilities
4. Enrollment of a subject shall involve the following steps
    a. First time registration with the agency. If the subject is in possession of a NIMC certified chip based ID card with match-on-card capability, the agency will run the ID card through a card reader to identify the subject.
        i. Enrollment data shall be submitted with the subjects NIN
        ii. NIMC will run the subjects NIN and fingerprint template through the web service and immediately provide Transaction Record Number (TRN) to the enrollment agency.
        iii. NIMC shall provide a YES/NO answer and the information on NIMC Core database for those fields previously agreed to exchange within 15 minutes.
        iv. The information on NIMC Core shall supersede any information submitted by the subject. For example, if the subject first name is spelled as Chukwuemeka in NIMC Core and the subject submitted their first name as Emeka, the ID card issued by the agency (or services rendered) shall bear first name as Chukwuemeka.
    b. First time registration with the agency. If the subject is NOT in possession of a NIMC certified chip based ID card with match-on-card capability, the agency shall treat the subject as new NIMC enrollment
        i. NIMC will run the subjects 10-print fingerprint through the NIMC Core AFIS database within in real time of submission. NIMC shall perform a full scan of the database to guarantee repudiation and rule out possible duplication
        ii. If the subject exist in NIMC Core AFIS database, NIMC shall provide the subjects NIN and Transaction Record Number (TRN) to the enrollment agency within 15 minutes of finding a match
        iii. If the subject does NOT exist in NIMC Core AFIS database, NIMC shall automatically enroll the subject and issue NIN.
    c. Returning subjects with the agency. If the subject is in possession of the agency issued, NIMC certified, chip based ID card with match-on-card capability, the agency will run the ID card through a card reader to identify the subject.

i. The agency shall process the subject within their own environment. There will be no need to submit the information to NIMC except in the following cases;
   1. The subject came for renewal of the agency issued, NIMC certified, chip based card with match-on-card capabilities
   2. Their National ID card has expired
   3. The agency other internal procedures may required resubmission of data to NIMC

   For the case outlined above, the agency shall take actions outlined below
ii. NIMC shall run the subjects NIN and fingerprint template through the web service and provide Transaction Record Number (TRN) to the enrollment agency within immediately
iii. NIMC shall provide a YES/NO answer and the information on NIMC Core based on those field previously agreed
iv. If information on NIMC Core is different from the information with the agency, the agency shall update their records such that NIMC data supersede their own information. The agency shall issue an updated ID card to reflect the new information from NIMC
v. NIMC Core data shall supersede any other data submitted. The subject shall be advised to contact NIMC to correct any issue with their records before services can be offered to them

Figure C: The diagram below illustrates the process involved for enrollment


Enrollment Process Flow
Obtain authorization from NIMC to become an enrollment agency
Obtain a domain code to identify each enrollment center
Set up an enrollment center
Enrollment of objects should involve the following
First Time Registration without a chip based card
Collection of Ten Finger Print
Provide NIN
First Time Registration with a chip based card
Enrollment data submitted with NIN
Provide TRN
Returning Subjects with the agency
Agency shall process the subject within their own environment

3.1.3 Process of replacing Enrollment ID with NIN

A national identification number (NIN) would be used by the government of Nigeria as a means of tracking their citizens, permanent residents, and temporary residents for the purposes of work, taxation, government benefits, health care, and other governmentally-related functions. The number will appear on an identity card issued by a NIMC.

A citizen is issued a NIN upon enrollment when they reach a legal age (typically the age of 16) or during registration each NIMC enrollment form has an enrollment ID which would be replaced with a unique NIN upon registration of subject. Non-citizens are issued a NIN when they enter the country. This new system of replacing enrollment ID with NIN will increase the security of identity documents in order to facilitate legal, commercial, governmental and financial transactions nation-wide.

3.2 Registration into member specific database

Enrollment into the NIMC core database is function reserved exclusively for NIMC and the few agencies authorized by NIMC to do so. All others fell into the category of Registration into specific database retained at NIMC or at a NIMC authorized BSP.

Enrollment is defined as the process of enrolling a subject into the NIMC Core such that NIMC shall issue National Identity Number (NIN) to the subject. Enrollment is done once in the entire life of the subject. A subject can only be associated with a single NIN to be used for any transaction carried out with the Federal, State, and Local government, as well as with the private sector and international community.

Registration is a process of making use of Enrollment Data to extend services to enrolled members in the NIMC Core. It uses subset of enrolment data stored in the NIMC Core. The use of registration falls under the purview of NIMC. Biometrics is a double-edged sword. While it serves a very useful purpose, it can easily be misused. The application and use of biometrics for PIV is mandated in the NIMC act and therefore must be properly regulated.

The following guideline shall apply;

- Any organization that wishes to use biometrics PIV to verify and authenticate subjects must first obtain permission from NIMC. NIMC must retain complete control of the registration process used by the organization
- Any organization that shall perform registration into the NIMC Gateway, including those of BSP, shall do so using the same standards as official NIMC Registration centers
- NIMC reserves the right to reject any registration data from any third party registration center for non-compliance.

- All activities of Registration centers shall be through NIMC Gateway web service, except cases where NIMC has explicitly given permission to access the Gateway through linked fiber optics (as provided by Galaxy Backbone or any other NIMC connectivity partner)
- Records of all transactions shall be kept for a period not less than 36 months or longer as may be mandated by Federal or State laws

3.2.1 Authorized Registration Organizations

- The organization must have obtained Transaction Control Code and Origination Identify for each center from NIMC
- The organization shall only deal with subjects that have assigned NIN and must refer new subjects to NIMC enrollment centers
- The registration process shall include all the data fields required by NIMC as outlined in Appendix G
- The agency shall implore 10-print or 2-print (thumb and 1st finger) biometrics for capturing fingerprints as outlined in Appendix C
- The organization shall have card reader, with match-on-card capabilities, and BioAPI facilities
- The organization shall have the capability to securely read, send, and receive data from NIMC based on the network standards outlined in Appendix J
- The organization shall have NIMC Certification for each device used in capturing data, processing data, and transfer of data to NIMC
- The organization that must have AFIS system shall ensure that only fingerprint template is stored in their AFIS database. Storing fingerprint raw data and fingerprint record data shall be a violation of NIMC Gateway Agreement
- The organization shall retain only the NIM and Transaction Record Number (TRN) after having transmitted the complete data to NIMC and obtained a TRN for the subject submitted
- The organization shall have the subjects NIN and TRN before any services can be offered to the subject. In the event that NIMC Gateway is not accessible after 3 hours of attempted connection, the organization may issue a provisional TRN for the subject and provided services based on the same
- The organization shall have the capacity to replace the provisional TRN with the TRN issued by NIMC Gateway at the time NIMC Gateway becomes available

3.2.2 Registration process flow

Any organization involved in the registration process shall follow these procedures. Details of the procedure are outlined in NIMC Registration Procedure Appendix Form 5. The procedural overview outlined below is a summary of processes for an agency that has complied with all NIMC standards and certification process.

1. Obtain authorization from NIMC to become a Registration organization
2. Obtain Domain Code (or use a BSP Domain Code) to identify the organization, obtain fixed 6-digit unique Transaction Control Code (TCC) for the organization, and obtain variable 4-digit Origination Identify to be used in identify each registration center operated by the organization. Type 14 record as in Appendix Form 2, submitted from any registration center must contain the Domain Code, TCC, and Origination Identify.
3. Setup registration center to include facilities for verification, including match-on-card capabilities
4. Registration of a subject shall involve the following steps
    d. First time registration with the organization. If the subject is in possession of a NIMC certified chip based ID card with match-on-card capability, the organization shall run the ID card through a card reader to identify the subject.
        i. Registration data must be submitted with the subjects NIN
        ii. NIMC will run the subjects NIN and fingerprint template through the web service and provide Transaction Record Number (TRN) to the organization agency within 1 – 2 hours
        iii. NIMC shall provide a YES/NO answer and the information on NIMC Gateway based on those field previously agreed
        iv. The information on NIMC Gateway shall supersede the information submitted by the subject. For example, if the subject first name is spelled as Chukwuemeka in NIMC Gateway and the subject submitted their first name as Emeka, the organization must register the subject in their database as first name of Chukwuemeka
        v. NIMC Core data shall supersede any other data submitted. The subject shall be advised to contact NIMC to correct any issue with their records before services can be offered to them
    e. First time registration with the agency. If the subject is NOT in possession of a NIMC certified chip based ID card with match-on-card capability, the organization shall simply refer the subject to NIMC or any of the other enrolment agency to obtain an acceptable form of ID before services can be offered
    f. Returning subjects of the organization. If the subject is in possession of the organization issued form of ID and a NIMC certified chip based ID card with

match-on-card capability, the organization will run the ID card through a card reader to identify the subject.

i. The organization will process the subject within their own environment. There will be no need to submit the information to NIMC except in the following cases;
    1. The subject has been flagged during the match-on-card verification
    2. The data expiration date issued by NIMC (as indicated on the chip) for specified type of information has been reached
    3. Their National ID card number has expired
    4. The organization other internal procedures may require submission of data to NIMC

    In the cases outlined above, the agency will follow take further actions outlined below

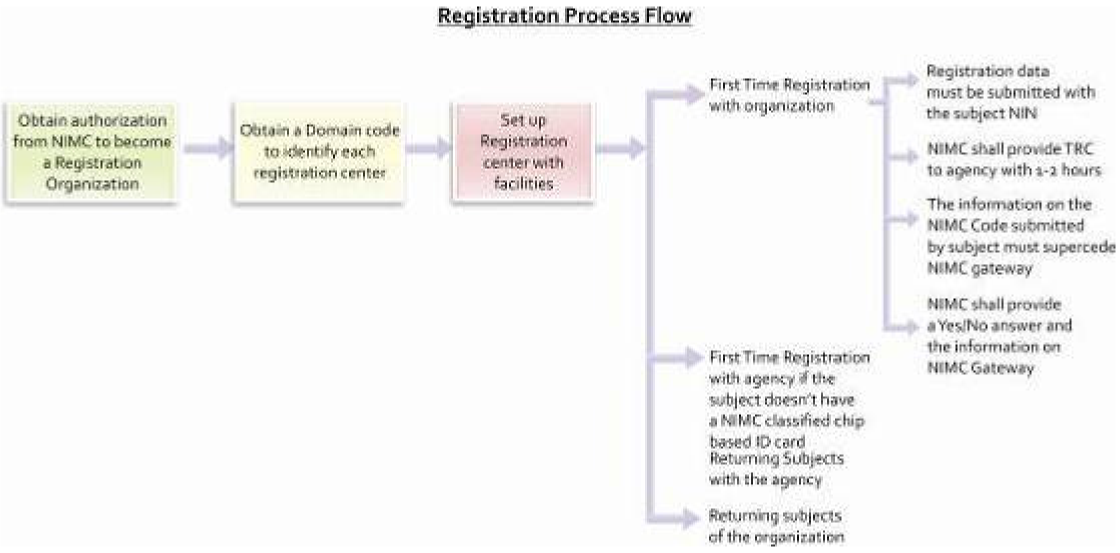
ii. NIMC shall run the subjects NIN and fingerprint template through the web service and provide Transaction Record Number (TRN) to the registration agency within 1 – 2 hours

iii. NIMC shall provide a YES/NO answer and the information on NIMC Gateway based on those field previously agreed

iv. If information on NIMC Gateway is different from the information with the organization, the organization shall update their records such that NIMC data supersede their own information. The organization shall issue an updated ID card to reflect the new information from NIMC

v. NIMC Gateway data shall supersede any other data submitted. The subject shall be advised to contact NIMC to correct any issue with their records before services can be offered to them

FIGURE D: The diagram below illustrates the process involved with registration


Registration Process Flow
Obtain authorization from NIMC to become a Registration Organization
Obtain a Domain code to identify each registration center
Set up Registration center with facilities
First Time Registration with organization
Registration data must be submitted with the subject NIN
NIMC shall provide TRC to agency with 1-2 hours
The information on the NIMC Code submitted by subject must supercede NIMC gateway
NIMC shall provide a Yes/No answer and the information on NIMC Gateway
First Time Registration with agency if the subject doesn't have a NIMC classified chip based ID card
Returning Subjects with the agency
Returning subjects of the organization

3.2.3 NIMC to provide link on their website as an option for PRE Registration

NIMC is to provide link on their website for people to register online and obtain a reference code then go to the nearest registration centre to submit the reference code; this would make the registration faster as people can go online to register.

3.3 Card type specs

Card types are classified into 3 specific cards as outlined below;

3.3.1 Primary forms of identification cards

Primary identification shall only be issued by NIMC and authorized Enrollment agencies that have meet the NIMC Card Printing certification as outlined in Appendix I. All Primary identification must meet the minimum standards outline in NIMC Card Specification as outlined in Appendix H.

Primary ID cards shall serve as the official identification documents in Nigeria. All participating stakeholders must obtain one form of primary ID from the subject before rendering any help

The card system must have the following;

- Shall be a EMV smart card, chip based with minimum of 32kb read/write storage
- Shall be JCard based and readable by all NIMC certified card reader
- The following applets shall be loaded on the card
    - E-ID Applet
    - Biometrics Applet
    - Match-on-card applet
    - Agency specific applets

3.3.2 Secondary forms of identification cards

Secondary identification shall only be issued by NIMC authorized Registration organizations that have meet the NIMC Card Printing certification as outlined in Appendix I. All Secondary forms of identification must meet the minimum standards outline in NIMC Card Specification as outlined in Appendix Figure 4.

Secondary ID cards shall serve as second form of ID in cases where primary and secondary forms of IDs are required before services can be rendered. All government benefits, financial transaction, immigration, travel, and access to major system shall require that primary form of ID be presented by the subject.

The card system shall have the following;

- Shall be a smart card, chip based with minimum of 16kb read/write storage
- Shall be JCard based and readable by all NIMC certified card reader
- The following applets must load on the card
    - E-ID Applet
    - Match-on-card applet
    - Agency specific applets

3.3.3 Other forms of identification cards

Any other forms of identification cards may be issued by participating stakeholders and various companies. Use and acceptability of these other cards shall be left to the decision of the entity accepting the card as a form of ID. The cards however shall not be used in cases where;

- The subject needs to be indentified for matters involving national security, including law enforcement, justice system, and correctional facilities
- The subject needs to be indentified for matters involving major financial transaction, including opening and operating bank accounts, granting of loans and other forms of financial instruments, and purchases of major assets

Agencies or organizations that are issuing these forms of ID cards do not require permission or supervision of NIMC. The cards shall not bear any resemblance to the type and form of NIMC approved primary or secondary forms of ID. In cases where it is determined that the card may be misconstrued as primary or secondary form of ID, the agency or organization shall be required to recall all issued cards, and to re-issue cards bearing a new design.

3.4 Card reader specs

Card reader devices are required to be present at any location needing to use Primary or Secondary form of ID cards for Person Identification Verification (PIV) services.

The card reader device can only be those make and models that has been certified by NIMC as published in Appendix C.

3.5 10-print fingerprint scanner specs

10-Print fingerprint scanner devices are required to be present at any center that shall be used as an enrollment center to process subject for possible addition into the NIMC Core database.

10-Print fingerprint scanner devices are NOT required for locations needing to use Primary or Secondary form of ID cards for Person Identification Verification (PIV) services.

The 10-print scanner device can only be those make and models that has been certified by NIMC as published in Appendix C.

Details of the standard for Biometrics, including the 10-print, facial, and Iris can be found in the reports of Biometrics sub-committee.

3.6 2-print fingerprint scanner specs

2-print fingerprint device are required at all location needing to use Primary or Secondary form of ID cards for Person Identification Verification (PIV) for the purpose of registration into the NIMC Gateway.

It is recommended that major financial institutions, airports, law enforcement agencies, retail outlets, and others procure 2-print fingerprint devices for use of Primary or Secondary form of ID cards for Person Identification verification (PIV) for the purpose of match-on-card and photo recognition applications.

2-Print fingerprint scanner devices must allow for finger printing of the thumb and index finger together as flats or rolled individually.

The 2-print scanner device can only be those make and models that has been certified by NIMC as published in Appendix C.

3.7 Data format

In other to ensure the integrity of the system, data standard format shall be adopted and followed by centers used for enrollment into the NIMC Core and registration into NIMC Gateway. The complete specification and standards for the data format is outside the subject matter of this document. Software developers developing applications to interface with any of the NIMC systems should attend NIMC Certification program as outlined in Appendix K.

3.7.1 Data categories and types

For all intensive purposes, there are three categories of data that can be exchanged with the NIMC systems, namely;

- Enrollment data formats: This format is only applicable to NIMC and those agencies certified by NIMC as authorized enrollment centers.

- Registration data formats: This format is applicable to NIMC and those organizations certified by NIMC as authorized registration location.
- Verification data formats: This format is application to NIMC web services and those agencies and organizations that have web accounts with NIMC

3.7.2 Mandatory data fields

The following are mandatory field category that must be submitted to NIMC

- Enrollment: Enrolment agencies shall collect and submit data to NIMC for all fields in NIMC Enrollment Form as in Appendix Form 1. The agency shall modify the form to include other information required by the agency.
- Registration: Registration agencies shall collect and submit the following data fields to NIMC
  - Title
  - Surname/Last Name
  - First name
  - Sex
  - Date of Birth
  - Place of Birth
  - City/LG of Birth
  - City/LG of Origin
  - Marital Status
  - Age
  - Height
  - Place of residence
  - Father's surname
  - Father's First name
  - Father's Origin LGA
  - Mother's surname
  - Mother's First name
  - Mother's Origin LGA
  - Next of Kin surname
  - Next of Kin First name
  - Next of Kin relationship to applicant
  - State of registration
  - LGA of Registration
  - Registration center
  - Ward

    - Polling Unit
- Verification: Verification entities shall collect and submit the following data fields to NIMC, along with information stored in the smart card E-ID applet.
    - Surname/Last Name as appeared on the ID Card
    - Other name as appeared on the ID Card
    - Date of Birth
    - ID card issuing agency and ID card number

  Details of data format, dictionary, standards, as well as acceptable forms of identifications, rules and process can be found in the report of the subcommittee on Data and Verification.

3.8 ID verification and retrieval process

ID verification and retrieval of data from NIMC Core or NIMC Gateway is the ultimate purpose of building the integrated National Identity Management System (database). The overall process of NIMS can be summarized into two categories of 1) Data collection (enrollment and registration) and 2) Data dissemination (verification services). Verification services are inherited in the process of enrollment and registration.

3.8.1 Basic Verification services

The stakeholders who were approved as enrollment agencies or who were approved as registration organizations are automatically approved for verification services. Verification services shall only be performed through NIMC Gateway web services via direct link or through a NIMC certified BSP. Any entity wishing to perform identity verification and authentication using NIMS must apply for access from NIMC. The process shall be as follows;

1. Obtain and complete Access Form as in Appendix Form 2 from NIMC, and obtain and complete BSP Form as in Appendix Form 10 from your selected BSP
2. Obtain Domain Code (or use a BSP Domain Code) for identifying your organization access, obtain fixed 6-digit unique Transaction Control Code (TCC) for NIMC billing reconciliation for your organization.
3. Obtain approval for the card acceptance devices you will use at your facility
4. Verification and authentication of a subject shall involve the following steps
    a. The subject must be in possession of a NIMC certified chip based ID card with match-on-card capability and must have photo picture imprinted on the card
    b. The subject will place the ID card into the card reader and place his thumb or index finger on the scanner

c. The client BioAPI will transmit the subjects print and NIN to NIMC Gateway

i. NIMC will run the subjects NIN and fingerprint template through the web service and provide Transaction Record Number (TRN) to the client within 5 – 10 minutes

g. NIMC shall provide a YES/NO answer and the information on NIMC Gateway based on those field previously agreed

h. The information on NIMC Gateway shall supersede the information submitted by the subject. For example, if the subject first name is spelled as Chukwuemeka in NIMC Gateway and the subject submitted their first name as Emeka, the client must insist the subject submit their application with first name of Chukwuemeka

3.8.2 Advanced Verification and photo image request services

Basic verification will return a result of Yes/No to confirm if the subject fingerprint minutiae matched what is in the NIMC Gateway. It will also return basic demographic data such as name, address, date and place of birth and other data fields as agreed with NIMC. Basic verification service shall not include the subject's photo images or fingerprint minutiae.

Part of the objectives for an integrated National Identity Management System (NIMS) is to save money and time for government and private sector stakeholders by not having those duplicate efforts inherit in NIMS. The procedure for facial image request shall be as follows;

1. in completing the request for basic verification services, check the option for photo image and complete the information needed for that section
2. The entity shall ensure that they have met the requirements and specifications for hardware, network, and security needed as specified in NIMC Gateway Access agreement Form as in Appendix Form 9
3. The BioAPI, for each request for verification services must specify the type of photo image to return back to the organization
4. NIMC shall issue a separate TRN for each photo image provided by NIMC.

3.8.3 Advanced Verification and fingerprint minutiae request services

Basic verification will return a result of Yes/No to confirm if the subject fingerprint minutiae matched what is in the NIMC Gateway. It will also return basic demographic information such as name, address, date and place of birth and other data fields as agreed with NIMC. A basic verification service does not include returning the subject photo images or fingerprint minutiae.

Part of objectives for an integrated National Identity Management System is to save money and time for government and private by not having them duplicate efforts inherit in NIMS. NIMC does not permit the storage of fingerprint raw images by any other entity. NIMC permits the storage of fingerprints records and minutiae. The procedure for fingerprint minutiae shall be as follows;

1. in completing the request for basic verification services, check the option for fingerprint minutiae and complete the information needed for that section
2. The entity shall ensure that they have met the requirements and specifications for hardware, network, and security needed as specified in NIMC Gateway Access Agreement form.
3. The BioAPI, for each request for verification services must specify the number of fingerprint and position of each finger to be returned back to the organization
4. NIMC shall issue a separate TRN for each finger of the subject provided by NIMC.

3.9 Interoperability procedure specs

There are numerous manufactures and supplies of biometrics systems including systems for AFIS database, fingerprint scanners, digital photos, data transmission protocols (BioAPI), system integrators, biometrics service providers, and various others. Each manufacturer will have propriety codes and procedure used in achieving various functions. In other to achieve harmony amongst the various systems, NIMC shall regulate, through product attestation and certification for each of these items.

3.9.1 Device attestation and certification process

The following shall apply;

- Participating agency, organizations, and entities may select from list of manufacture, make, and model that has been approved for use by NIMC. In cases where the entity wishes to use a provider not on NIMC list, the entity shall do the following;
  1. The entity shall submit the providers information by completing NIMC Attestation and Certification form as in Appendix Form 8 and pay the applicable fees to NIMC
  2. The manufacturer (or provider) shall submit detail technical specification data, any past testing data from any of the recognized international body/organization such as FBI, Europol, IEC, Biometrics Consortium, etc and performance data to NIMC within 30 days of receipt of application

3. NIMC shall conduct test based on NIMC specifications. Upon successful completion of the test and approval (if standards were met), NIMC will allow the entity to use the model and version approved by NIMC.

- Any new versions of the product shall be subject to recertification.

3.9.2 BioAPI and Integrators certification process

Any piece of software to be used as middleware to enable exchange or movement of biometrics data from one system to another must be regulated by NIMC through process of attestation and certification. Any company or individual consultants wishing to provide system integration services shall be approved by NIMC

- Participating agency, organizations, and entities may select from list of companies and individual consultants that has been approved for use by NIMC. In cases where the entity wishes to use a company or individual consultant not on NIMC list, the entity shall do the following;
  1. The entity shall submit the company's information by completing NIMC Attestation and Certification form as in appendix Form 8 and pay the applicable fees to NIMC
  2. The company shall attend NIMC courses on integration and successful pass NIMC code of conduct and technical examination. The company shall subsequently register with NIMC and pay the applicable annual support fee
  3. NIMC shall, upon successful completion, issue certification and approval to allow the entity to use the company for integration

3.10 Network access and security specs

The overall network security, physical, and virtual access to the system housing biometrics data is key to integrity of the system. The network access and security can be viewed from

1) System involved in collecting and processing of raw biometrics image

2) Systems involved in process biometrics records

3) System involved in processing NIN and associated data.

3.10.1 Systems involved with raw fingerprints images

Any agency or organization that is involved in capturing, processing, or storage of raw biometrics fingerprints shall adhere to the following;

- Any staff or consultant that will have physical or virtual access to the system shall be fingerprinted by NIMC and proper identification of the subject made before such individual shall be allowed access to the system

- Any staff or consultant that will have physical or virtual access to the system shall sign confidentiality agreement, including clause authorizing NIMC to seek criminal charges against them for illegally making copies, distributing such, or selling biometrics data
- Physical access to the servers shall be through biometrics authentication
- Virtual access to the system shall require username and password,

3.10.2 Systems involved with biometrics records and templates

Any agency or organization that is involved in processing and storage of biometrics records and fingerprint templates shall adhere to the following;

- Any staff or consultant that will have physical or virtual access to the system may be fingerprinted by NIMC and proper identification made before such individual shall be allowed access to the system
- Physical access to the servers may be through biometrics authentication
- Virtual access to the system shall require username and password as in NIMC Gateway Access Form

3.10.3 Systems involved with processing and storing of NIN

Any agency or organization that is involved in processing and storage of NIN shall adhere to the following:

- Any staff or consultant that will have physical or virtual access to the system may be fingerprinted by NIMC and proper identification made before such individual shall be allowed access to the system.
- Any staff or consultant that will have physical or virtual access to the system shall sign confidentiality agreement, including clause authorizing NIMC to seek criminal charges against them for illegally use of individual's NIN.
- Physical access to the servers maybe through NIN authentication.
- Virtual access to the system shall require username and password as in NIMC Gateway Access Form.

3.11 Connectivity Specs

Connectivity to NIMC Core by any agency or organization shall be prohibited. Connectivity to NIMC Gateway shall be open based on the following activities;

3.11.1 Secured fiber links

Any agency authorized as enrollment agency shall connect to the NIMC Gateway through the secured fiber optics provided by Galaxy Backbone, except in cases where an exception has been made to use other means. The connectivity between the agency and

NIMC and the connectivity between the agency and their enrollment centers must all meet NIMC specifications for connectivity as outlined in Appendix J.

- There shall be a single connection between the agency's main hub and NIMC hub.
- The agency shall deploy in such a way that their various centers are linked to their central hub, with the central hub shall make the only connection to NIMC Gateway.
- The agency shall be responsible for making sure that the connection between their hub and their various locations is through secured channel protocol.

3.11.2 Secured VPN/Crypto tunneling

Any organization authorized as registration entity shall connect to the NIMC Gateway through secured VPN/Crypto tunneling meeting the specification outlined in NIMC Network and Security Specifications outlined in Appendix J, except in cases where an exception has been made to use other means. The connectivity between the organization and NIMC and the connectivity between the organization and their registration centers must all meet NIMC specifications for connectivity as outlined in Appendix J.

- There shall be a single connection between the organization's main hub and NIMC hub.
- The organization shall deploy in such way that their various registration centers are linked to their central hub, with their central hub making the only connection to NIMC Gateway.
- The agency shall be responsible for making sure that the connection between their hub and their various locations is through secured channel protocol.
- The organization may contract with for services of a BSP to link their site into NIMC Gateway, using a single connection on their behalf

3.11.3 Public Internet links

Any other entity shall connect to the NIMC Gateway through the web services and must use the services of BSP that has fiber links or secured VPN/Crypto tunneling meeting the specification outlined in NIMC Network and Security Specifications outlined in Appendix J, except in cases where an exception has been made to use other means. There shall be no direct connectivity between the entity and NIMC.

- There shall be a single connection between the BSP main hub and NIMC hub.
- The BSP shall have the capacity to link and manage the connectivity with the entities various points and their central hub, with the BSP making the only connection to NIMC Gateway.

- The BSP shall be responsible for making sure that the connection between their hub and their various clients have proper firewall and security appliances as specified in the NIMC Network and Security Specification

3.12 Data processing and storage specs

The collection, processing, and storage of biometrics information should be handled with care. The following must be observed;

3.12.1 Captured images for enrolment purposes

Enrollment agencies shall follow the following procedures to ensure security and integrity of the captured fingerprints and photos in their system

- Captured images raw data shall be transmitted to NIMC Core within 72 hours of capturing the images. NIMC shall issue TRN and NIN for each submitted set of captured images to the enrollment agency with 72 hours of such submission.
- The enrollment agency shall delete the captured images from their system within 72 hours of capture and upon receiving the TRN and NIN from NIMC. Under no circumstance shall any agency store the raw data in their system for a period more than 72 hours. NIMC shall store the captured raw images for perpetuity and make such available to the agency upon request.
- Any agency that has an its own AFIS with capability to process fingerprint image in other to produce the fingerprint minutiae, fingerprint records, and fingerprint template shall process the data within the 72 hours allowed. The agency shall transmit the raw data, fingerprint minutiae, fingerprint records, and fingerprint template to NIMC within 72 hours of capturing the images. NIMC shall issue TRN and NIN for each submitted set of captured images, as well as issue TRN for each fingerprint minutiae, fingerprint records, and fingerprint template submitted to NIMC. The agency shall delete the captured image and fingerprint minutiae from their system. The agency may store the fingerprint record and fingerprint template for perpetuity. NIMC shall store the captured raw images, fingerprint minutiae, fingerprint records, and fingerprint template for perpetuity and make such available to the agency upon request.
- Under no circumstance shall any agency, including NIMC, alter the original captured image. The original image must be preserved in the original format it was submitted.

3.12.2 Captured images for registration purposes

Registration organizations shall follow the following procedures to ensure security and integrity of the captured fingerprints and facials in their system

- Captured images raw data must be transmitted to NIMC Gateway within 48 hours of capturing the images. NIMC shall issue TRN for each submitted set of captured images to the registration organization within 48 hours of such submission.
- The Registration organization shall delete the captured images from their system within 48 hours of capture and upon receiving the TRN from NIMC. Under no circumstance shall any registration organization store the raw data in their system for a period more than 48 hours. NIMC shall store the captured raw images for perpetuity and make such available to the registration organization upon request.
- Registration organizations are discouraged from having their own AFIS, however any organization with their own AFIS with capability to process fingerprint image in other to produce the fingerprint minutiae, fingerprint records, and fingerprint template must process the data within the 48 hours allowed. The agency must transmit the raw data, fingerprint minutiae, fingerprint records, and fingerprint template to NIMC within 48 hours of capturing the images. NIMC shall issue TRN for each submitted set of captured images, as well as issue TRN for each fingerprint minutiae, fingerprint records, and fingerprint template submitted to NIMC. The organization must delete from their system the captured image, fingerprint minutiae, and fingerprint records from their system. The organization may store the fingerprint template for perpetuity. NIMC must store the captured raw images, fingerprint minutiae, fingerprint records, and fingerprint template for perpetuity and make the fingerprint template available to the organization upon request.
- Under no circumstance shall any organization, including NIMC, alter the original captured image. The original image must be preserved in the original format it was submitted.

3.12.3 Captured images for verification purposes

Organizations that have arrangements with NIMC to use the web services for PIV must follow the following procedures to ensure security and integrity of the captured fingerprints system

- The card acceptance device must not have the capability to store any captured images used for match-on-card purposes
- For real time verification, the device must transmit the prints without storing the image in the local device or transmit it to any other system other than that of NIMC. Upon transmission, NIMC shall issue TRN which can be stored by the organization.

3.13 Rules enforceability procedure specs

The primary purpose of standards is to ensure integrity and stability of multi-shared, multi-organizational platform. Member's interactions with the NIMC Core and NIMC Gateway shall be regulated based on the severity and potential impact to the systems integrity.

3.13.1 Level 3 infractions

Level 3 infractions are normally issues that has the potential of bringing down the overall system or cause long term damage to the integrity of the system, or will infringe on the basic human rights of the subject (or subjects) in the system. The following shall be considered Level 3 infractions and the associated actions to be taken;

- No organization or agency shall store, or distribute captured raw images of subject's fingerprints. Any member found to be engaged in such activities shall immediately have their rights and privileges revoked by NIMC. NIMC shall advise the office of NSA to take further actions. Such member can only be reconnected after meeting the requirements stipulated in section 3.14
- No organization or agency may directly transfer or exchange with another entity fingerprints raw images, minutiae, records, or template without passing it through the NIMC Gateway so as to have proper records of such transfer of biometrics. Any member found to be engaged in such activities shall immediately have their rights and privileges revoked by NIMC. Such member can only be reconnected after meeting the requirements stipulated in section 3.14

3.13.2 Level 2 infractions

Level 2 infractions are generally for using of sub-standard or uncertified devices, network protocols, procedures, and processes that are not tested and approved. Integrity of the overall system can only be ensured when members adhere strictly to using only those devices that have been certified and procedure and processes that are tested. The following shall be considered Level 2 infractions and the associated actions to be taken;

- No organization or agency shall install any front-end devices including 10-print scanner, 2-print scanner, card acceptance devices, and biometrics printers that do not have NIMC certification. Any member found to use unapproved devices shall immediately have their rights and privileges revoked by NIMC. Such member may be reconnected once they have implored the proper equipments
- No organization or agency shall transmit data to NIMC Gateway using unregistered BioAPI or through an unsecured network or deviate from the procedures and process defined in the NIMC Approval form as in Appendix Form 6 and to any subsequent amendments to the form. Any member found to be engaged in such activities shall immediately have their rights and privileges revoked by NIMC. Such

member can only be reconnected after meeting the requirements stipulated in section 3.14

3.13.3 Level 1 infractions

Level 1 type infractions are generally financial transactions that may not necessarily impact the integrity of the system. However, if left unchecked shall impact the ability of NIMC to continue to maintain and support the infrastructure. The following shall be considered Level 1 infractions and the associated actions to be taken;

- Any organization or agency that did not pay their dues, service charges, and others for use of PIV shall have their privileges revoked after;
  - NIMC have notified them of their outstanding that are more than 30 days overdue
  - NIMC have sent them disconnection notice and payments were not received 30 days from date of the disconnection notice

  Such member can only be reconnected after meeting the requirements stipulated in section 3.14

3.14 Penalty and cure procedure specs

The penalty and cure for each level of infractions are administrated after NIMC must have taken the actions recommended for each fraction. NIMC shall act in a timely manner as to prevent further loss or degradation to the system. The procedures shall

- Any infractions of level 3 and level 2: Access shall only be restored after the member has taken corrective actions to the satisfactory of NIMC that such offence is unlikely to repeat.
  - If the offender is Ministry, Department, or Agency of Federal Government, they will undertake to repay NIMC any cost incurred while rectifying their infractions. It is only after concluding financial arrangements with NIMC shall they apply to NIMHC to have their privileges restored.
  - If the offender is of private sector, NGO, foreign missions, and others that are non-federal government affiliates, they shall pay in full any cost incurred while rectifying their infractions. It is only after full payment has been made with NIMC shall the offender apply to have their privileges restored.
- Any infractions of level 3 and level 2 where the offender is repeat offender, in addition to meeting the conditions stipulated above, the offender shall wait for minimum of 6 months before privileges shall be restored.
- Any infractions of level 1: Offenders shall complete their financial arrangements with NIMC before applying to have their privileges restored. In cases where they are repeat offenders, NIMC may demand that their post bank guarantees.

3.15 Publication and upgrading of the Federal Handbook

The National Identity Management and Harmonization Handbook is a set of guidelines, specifications, and recommendations with the purpose of enabling the development, adoption, and use of biometrics standards in Nigeria. It is an ongoing work that is updated on frequent basis.

The latest and most up to date can be found at www.nimchc.com

4 Transactions and fees

NIMC shall charge fees for certain services being provided. The fees shall be used for ongoing support and maintenance of the system. Agencies, organizations, and entities should evaluate their cost savings achieved by their use of NIMC Gateway. The overall principal guiding applicable fees charged shall be based on the following;

- Enrollment agencies shall not be charged any fee for submission of subject's enrollment data to NIMC. This shall be applicable to those records where the agency submitted TCC and received TCN from NIMC
- Enrollment agencies shall never be charged a fee for use of any subject biometrics that was submitted by them to NIMC. This shall be applicable for those records where the agency submitted TCC and received TCN from NIMC
- Enrollment agencies may be charged a token fee for use of a subject biometrics that was not submitted by them.
- Registration organizations shall be charged fee for registration of new subjects and for revalidation of existing subject in which NIMC shall provide TCN for their database.
- Verification entities shall be charged for any type of verification in which NIMC shall provide a TCN for their database.

4.1 Premium services

NIMC shall charge fees for the following premium services;

- Request for fingerprints records, minutiae, or template
- Request for photo images
- Request for attestation and/or certification of any device, system, or process

4.2 Hit or No-Hit

Fees shall be charged on basis of "Hit" or "no-Hit," as defined below. The definition applies to verification processes alone.

4.2.1 Hit

Any request for information contained in the NIMC database where the purpose of such request is to identify the individual through the web verification, match-on-card, manual lookup, or any other means shall constitute a hit if the following can be determined;

- The agency or entity performing the verification is charging a fee directly or indirectly to the individual or is receiving any other future numerations from the individual
- The agency or entity performing the verification will benefit from cost savings directly or indirectly, either by way of reducing processing cost or by way of other benefits

4.2.2 No-Hit

Any request for information contained in the NIMC database where the purpose of such request is to identify the individual through the web verification, match-on-card, manual lookup, or any other means shall constitute a no-hit if the following can be determined;

- The agency requesting for the information is law enforcement agency and the purpose is for prevention or prosecution of crime
- Information is requested directly by an agency for the sole purpose of Federal Government employment or appointment. In cases where the employment process was outsourced to a third, all request by the third party shall be considered a hit

4.3 Billing

Charges and fees, and mode of payment shall be negotiated between NIMC and each entity.

LIST OF APPENDIX

APPENDIX A: Committee Members List

S/NO	Name of Organization	Representatives
1.	National Identity Management Commission (NIMC)	a) Aliyu A. Aziz (Co-Chair) b) Ben Alofoje
2.	SageMetrics Nig Ltd	a) Kenneth Nwabueze (Co- Chair) b) Anyichie Adaora
3.	Independent Electoral Commission (INEC)	a) Moses Naiya b) Emmanuel Akem
4.	Economic and Financial Crime Commission (EFCC)	Bello M. T. Adamu
5.	National Office for Technology Acquisition & Promotion (NOTAP)	a) Ifeanyi N. Ebeku b) Samuel E. Ebenya
6.	Ministry of Defence (DEFENCE)	Cyril U. Agwai
7.	Department of State Security (DSS)	a) Aliyu Abubakar b) M. Ukashatu
8.	Joint Tax Board (JTB)	Ekeh Chinedu
9.	XDS CREDIT BUREAU	a) Ugbong Awah b) Zipporah Anuga (Mrs)
10.	Nigerian Communication Commission (NCC)	a) Samuel Obianke b) Olatokunboh Oyeleye
11.	Nigerian Immigration Services (NIS)	a) Epum Charles
12.	Nigerian Pension Commission (PENCOM)	a) Ekanem Aikhomu b) Kunle Odebiyi
13.	Nigerian Security Adviser (NSA)	a) M. Umar Maska b) Magani Niyomdi
14.	Corporate Affairs Commission (CAC)	Ononokpono G. B
15.	National Health Insurance Scheme (NHIS)	Modupe Ogundimu
16.	Central Bank of Nigeria (CBN)	Soji Aminu
17.	Nigerian Prison Services (PRISONS)	a) Agada F. Audu b) Garba Michael
18.	National Population Commission (NPopC)	Amos Helen O. (Mrs.)
19.	Federal Inland Revenue Services (FIRS)	Osasere J. Ehigie
20.	Federal road Safety Commission(FRSC)	Janet Adepegba
21.	Nigerian Police Service (NPS)	a) ASP Garba Michael b) DSP Agada Felix Audu
22.	SW GLOBAL	a) Martin Mirero b) Ngozi Beckley- Linos
23.	QUANTEQ	a) Dr. Fidelis Ndeh-Che b) Dolapo Olusanmokun
24.	ALTEQ	a) Shobanjo Mobolaji b) Chizoba V. C
25.	GALAXY BACKBONE	a) Amara Nwankpa b) Ogunsanya Abisola
26.	ADVANCED MANAGEMENT TECHNOLOGY SOLUTIONS (AMTS)	Dr. Steven Dike

APPENDIX B: Acronym List

AMTS	Advanced Management and Technology Solution
AFIS	Automated Fingerprint Identification System
ASP BSP	Application Service Provider Biometrics 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 Commission
GMPC	General Multi-Purpose Card
HAS	Harmonization Assessment Study
ICT	Information and Communication Technology
ID	Identification
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
NIN	National Identification Number
NIMC	National Identity Management Commission
NIMHC	National Identity Management Harmonization Committee
NIS	Nigerian Immigration Services
NPC	National Population Commission
NPF	The Nigerian Police Force
NPS	Nigerian Prison Services
NSA	National Security Adviser
PENCOM	National Pensions Commission
PII	Personally Identifiable Information
PIV	Person Identification Verification
PVC	Poly Vinyl Chloride
SSS	State Security Services
SQL TCC	Structured Query Language Transaction Control Code

TCR	Transaction Control Reference
UTIN	Universal Tax Identification Number
UUID	Universally Unique Identifier
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extended Markup Language

APPENDIX C: Approved List of Device

List of devices

S/NO	Device type	Manufacturers name	Model name	Model number	Effective date
1.	Scanners				
2.	Signature pads				
3.	Camera				
4	Card reader				

APPENDIX D: Approved List of BioAPI/ Enrollment software

List of devices

S/NO	Device type	Manufacturers name	Version name	Version number	Effective date

APPENDIX E: Approved List of BSP

S/NO	Name	Agency attached to

APPENDIX F:

Approved List of Consultant

S/NO	Name
1.	SageMetrics
2.	Quanteq
3.	Alteq
4.	Galaxy backbone
5.	Charms
6.	NADRA
7	AMTS

APPENDIX G: Data Dictionary

Refer to Data and Verification sub-committee report

APPENDIX H: National ID card Personalization Specification

S. No.	Title	Specification
1	Minimum Expected Services	The Card Personalization Center (CPC) should be capable of providing the following services: 1. Contactless Smart Card encoding and programming 2. Proximity smart card encoding and programming 3. Contact Smart Chip encoding and programming 4. Magnetic Stripe encoding 5. Composite Formulations 6. Lithographic Pre-printing 7. Hologram printing 8. Embedded UV printing 9. Micro Text capabilities 10. Variable Record Printing 11. Database Provisioning
1.	Minimum Visual Personalization	Technology employed - thermal dye sublimation method
2.	Minimum Personalized Applicant Data	FRONT SIDE: Surname, First Name, Middle Name, Previous or Maiden Name, Sex, Date of Birth, Height, Personal ID Number, Date of Expiry, Photograph and Ghost Image.
3.	Minimum Personalized Applicant Data	BACK SIDE: Town, District, Region, Address, Community, Postal Code, Postal address, Holder signature's, Serial Number of Card Production Data
4.	Minimum Secure Laminate Applications	Application of Holographic Secure laminate to protect personalized data
5.	Minimum Electronic Personalization	Personalization System is connected to the PKI module, in which all encryption keys are managed. The personal data will be digitally signed before writing on the chip. Will meet ICAO and EMV certification standards.
6.	Minimum Equipment	Data Card Central Issuance and Instant Issuance Printers Will meet ICAO and EMV certification standards
7.	Production Audit	Complete Smart Card Personalization Audit Trail system – audit trails available for card issuance, card destruction, card personalization and card delivery.
8.	Minimum Physical Security	Center will be equipped with CCTV, Biometric Access Control, Intrusion Detection and Fire Alarm systems
9.	Minimum Logical Security	Complete logical security bifurcation between administration and production networks with firewalls and network monitoring stations. Controlled environment for data preparation and production data processing.
10.	Minimum Data	PGP encryption of data. Will meet EMV and ICAO

	Transmission Capacity	certification standards
11.	Card Destruction	Performed under controlled environment employing four eye principle and strict document control.
12.	Departments	1. Administration 2. Security 3. Networking 4. Data Processing 5. Key Management 6. Data Preparation 7. Production 8. Audit Control 9. Logistics

APPENDIX I: NIMC Card printing certification

Summary of Minimum Specifications for certification

IC Card standards	**EMV2000 ver. 40, ISO 7816 and PC/SC**
IC CARD	Smart Card with 2SAM Socket
CPU	MIPS 32 bits Clocked at 96MHz
FLASH PROGRAM	**Minimum of 256 KB Flash Program ROM**
SDRAM	**Minimum of 256KB of Working RAM**
RTC	Real Time Clock (Battery Operated)
LCD	Graphics LCD Display. 128 x 64 Dots/ Icon Display E.L Back Light or LED Back Light (Option)
PIEZO BUZZER	PWM Generator
CARD READER OPERATING TEMP	**Minimum of 0 -50C**
COMPLIANCE	**CE, FCC, WHQL**
PLATFORM SUPPORT	**WINDOWS 98, ME, 2000, XP VISTA XPx64 VISTAx64 Unix**
BATTERY	Lithium ION Battery (7.2V)
MODEM	GSM/GPRS Modem Module or CDMA Modem Module
FORM FACTOR	**RS 232 or USB 2.0**
PRINTER	1. Thermal Line Printing 2. Number of dots: 384 dots 3. Resolution: 8 dots/mm 4. Printing Speed: 75mm/s
ANALOGUE TO DIGITAL CONVERTER	Minimum of Internal 6 Channel A/D
POWER SUPPLY	**Minimum of 85 to 265 Volts AC 50/60 HZ SMPS Free Voltage AC Adapter** **With o/p of at least 3v-12v**

APPENDIX J: MINIMUM REQUIREMENT FOR NETWORK STANDARDS

S. No.	Title	Specification
	Network switches	**Edge Switches** This 3 layer capable network switch should have 1. 24 Independently Managed Ports 10/100/1000MB, 2. Non-blocking ports, 3. Redundant power supplies 4. Wire speed switching 5. VLAN Capable 6. ACLs, minimum 48Gbps Switch Fabric 7. Minimum 22.5Mbps Layer 2/Layer 3 Packet Forwarding Rate 8. Redundant 1GB full duplex uplink port with 10GB uplink preferred. **Core Switches** This switch should be Layer 2 to 4 capable and have 1. 24 independently management 1000MB non-blocking ports 2. 2 redundant power supplies 3. Upto160 Gbps switch fabric bandwidth 4. Up to 65 Mpps Layer 2/Layer 3 packet forwarding rate 5. Optional dual 10 Gigabit Ethernet ports for redundant uplinks, 6. 9216 Byte maximum packet size (Jumbo Frame) 7. 8 QoS queues/port, 8. 48 Gbps per slot capacity. 9. 4096 VLANs (Port, IEEE 802.1Q, MAC-based) 10. Hardware-based ACLs.
	Routers	The modular integrated services router should be able to 1. Provide advanced security services and management capabilities. 2. The router must have built-in hardware encryption acceleration IPSec, VPN, stateful firewall protection, dynamic intrusion prevention and URL filtering support. 3. The router must be loaded with hardware and software to initiate and terminate VPN tunnels (IPSec and SSL) and serial WAN interface connections. 4. The router would be used as the edge router at this location. 5. Redundant power supply.

i) MINIMUM REQUIREMENT FOR SERVERS, STORAGE AND BACKUP DEVICES

S. No	Title	Specification
	Servers	The following are the minimum specifications for Servers depending on the Registration Centre or point of use: Network Servers (2) Messaging & Collaboration Servers (2) Database Servers (2) (Clustered) Application Servers (2) (Clustered) Antivirus Server (1) Document Server (2) Backup Servers (2) The generic characteristics are as follows 1. Midrange servers, resilient, redundant and fault- tolerant 2U rack-mounted server systems with high performing 4 socket, dual processor, 64 bit Quad Core Intel Xeon X5355 processors 2x4MB Cache, 2.66GHz, 1333MHz FSB. 2. The servers should support up to 8 GB of DDR-2 memory, up to 300GB hot pluggable SAS/SCSI hard drives, 4GB fiber channel adapters, and up to 2 Ethernet 10GB Adapters (4 ports per adapter) , Device Ports/ PCI express I/O expansion facility up to 16. 3. The servers should have up to 2 hot pluggable redundant power supplies with up to 4 redundant cooling fans. 4. Number of processors and memory should be varied depending on the needs of the particular database, antivirus, backup, operating system, messaging/collaboration software or solution proposed.
	Online Storage Devices	1. High performance storage with a modular back-up solution for critical files and data. 2. 32 Port Fibre Channel 4 Gbit/sec SAN Switch, 1U storage processor enclosure. 3. Support for up 120 (15K rpm) SCSI or SAS Drives, initial 2TB of storage, scalability to 59TB of storage capacity and

S. No	Title	Specification
		expansion slots, support 4 hot pluggable redundant power supplies with up to 4 redundant cooling fans.
	Tape Storage Device	LTO Tape Drive solution, support for unattended, automated backups, Autoloader solution that supports up to 3.2TB of native capacity, support for SCSI drives.

ii) MINIMUM REQUIREMENT FOR OPERATING SYSTEMS, SOFTWARE AND APPLICATIONS

S.No.	Title	Specification
5	**Operating System Licenses**	1. Enterprise Server Operating System Licenses; 100 user licenses. 2. OS's must be 64 bit 3. Must support multiple processors and be compatible with the servers supplied. 4. OS's must also be the latest supported version of the manufacturers products and 5. Must include all updated security patches and service packs as of the date of response.
6	**Windows Desktop Operating System**	1. Features; Hybrid kernel, Multilingual, Graphical user interface - Windows Aero, Instant Search, Windows Sidebar, enhanced security, improved navigation and search, sidebar, backup and restore center, shadow copy, speech recognition, Reliability and Performance Monitor 2. Support Platform; x86, x86-64 **3.** Licensing Policy; MS-EULA
	Windows Network Operating System	Windows Server Operating System 2003 R2 Enterprise Edition or Windows Server Operating System 2008 Enterprise Edition.
	Open Source Operating System	1. Features; Monolithic kernel with modules, Kernel programming language C; Hosted mode UML, coLinux, L4Linux, MkLinux, Itanium Linux-on-Linux, wombat 2. File System Support; FAT, NTFS, Ext2, Ext3, UFS, UFS2, HFS, HFS+, ISO 9660, UDF, NFS, 3. Hardware Supported; ATA, SATA, SCSI, USB, Fireware, PCMCIA/PC Card, AGP, Nvidia driver IA32, Nvidia driver IA64, Nvidia driver AMD64, ATI Technologies x86-64, Gigabit Ethernet, 10-gigabit Ethernet, Wireless LAN, Bluetooth, IrDA, NE2000/RTL8029, RTL8139, TCP/IP, IPv6, IPX, PPP, DHCP, Network Bridge, OpenVPN 4. Support Platform; x86 /i386 / IA-32 , x86 SMP, Xen, IA-64, x86-64 , PowerPC , PA-RISC Licensing Policy; GNU GPL/LGPL
	Oracle Enterprise Database Management	1. Oracle Database 11g Release 1 Enterprise Edition for UNIX, Linux, x64 Windows platforms With options for i. Real Application Testing ii. Advanced Compression iii. Total Recall

S.No.	Title	Specification
	System	iv. Active Data Guard v. Real Application Clusters vi. Management Packs vii. Partitioning viii. Warehouse Builder ix. OLAP x. Data Mining xi. Retail Data Model xii. Spatial xiii. Database Vault xiv. Advanced Security xv. Label Security xvi. In-Memory Database Cache. 2. Oracle Database 11*g* Release 1 Client (11.2.0.1.0) for Linux, x86-64 Windows and HP-UX, AIX Platforms. 3. Oracle Enterprise Manager 10*g* Grid Control Release 5 (10.2.0.5) for Linux, x86-64 Windows and HP-UX, AIX Platforms. 1. Oracle Secure Backup 10.3.0.1 for Linux, x64 Windows and HP-UX, AIX Platforms. 2. Oracle Secure Enterprise Search 10*g* Release 1 (10.1.8.2) for Linux, x64 Windows and HP-UX, AIX Platforms. 3. Oracle Warehouse Builder 10*g* Release 2 (10.2.0.1) For Linux, x64 Windows and HP-UX, AIX Platforms. 4. Oracle Audit Vault Server (10.2.3) for Linux, HP-UX, AIX Platforms. 5. Oracle Content Database and Oracle Records Database 10*g* Release 1 (10.2.0.0.0) for Linux, x86-64 Windows and HP-UX, AIX Platforms and Oracle Content Database 10*g* Release 1 Client for x86-64 Windows
	Enterprise Application Server	1. Support; J2EE, BPEL and Javabeans (EJBs). The APPSERVER should be able to handle all application operations between users and NIMS's backend applications and databases 2. Features; Built-in redundancy, Monitors for high-availability, High-performance distributed application services , Support for complex

S.No.	Title	Specification
		database access
	Antivirus Server licenses	1. Features; Enterprise Antivirus software. Real-time protection, detection and removal of viruses, Trojans, worms, spyware, adware, key loggers malicious tools and Auto-Dialers, Internet Worm Protection blocks viruses, spyware and worms without specific signatures, Detects and removes viruses and spyware, Blocks spyware automatically, Prevents virus-infected emails from spreading, Automatically detect and block viruses, spyware, and worms, Scans Email and instant-message and detects, removes or blocks infected attachments, Internet Worm Protection blocks viruses, spyware and worms without specific signatures, Full System Scan performs a deep scan to remove existing viruses, spyware and other threats
	Backup Software Server Licenses	1. Features; Enterprise Backup Software Server Licenses, With plug-ins for database, mail server, Total Data Protection, Mission-critical backup and storage management, Enterprise-class NAS protection, Protecting your data across the enterprise, Simplified management across multiple platforms, Fast system recovery, Faster backup and restore, High-performance disk arrays speed recovery, Simultaneous reads and writes improve performance, Automatic Client Updates, Virtual Machine Support, Heterogeneous protection, Broad connectivity, Total Datacenter compliant
	Messaging and Collaboration Software	Microsoft Office SharePoint Server 2007, Microsoft Office Communications Server 2007 R2, Office Communicator, Exchange Server 2007 SP1. OS Platform: Microsoft Windows Server 2003 R2 Enterprise Edition or Microsoft Windows Server 2008 Enterprise Edition
	Core User Applications	
	Registration and Enrolment Application (Otherwise provided by the NIMC)	1. Enterprise version with advanced multi-biometric data-mining and search system; 2. Supports fingerprint, face, and iris modalities and other biometric technologies ; 3. Should have robust performance with the ability to operate in very harsh conditions; 4. Reduced development and implementation costs; 5. Enables distribution or centralization of biometric data processing through a service-oriented architecture (SOA);

S.No.	Title	Specification
		6. Should be scalable and have built-in fault tolerance and exceptional manageability; 7. Secure management of biographic and biometric information with improved data and transaction security by enabling secure communications, digital signatures, and encryption of data at rest; 8. Should include ID management software, and a back-office system for data consolidation and safeguard; 9. Support high quality reference data; 1. Interoperable and easy to integrate with other applications ; 2. Can handle a larger number of data points during biometric authentication and compares them to an optimized reference template to reduce false rejections; 3. Software should run on J2EE compliant application server platform; 4. Employs one-to-many matching of templates against all enrolled users during enrolment to eliminate multiple identities; 5. The user database should be able to run on standard databases such as Oracle, IBM DB2, and MS-SQL; 6. Enables centralized system administration and user management; 7. Maintains transaction status records for long-term chain of custody awareness and auditing purposes; 8. Centralizes system administration and user management.
	Quality Assurance	1. Enterprise version that supports and augments quality systems 2. Enforces Configuration Management Systems. 3. Collects & Analyzes data automatically. 4. Enforces Operator Qualification Status. 5. Employ specialized logs to track completion of applications, status of complaints, requests etc. 6. Easily add or view all active, expired, incomplete or rescinded applications. 7. Application date and time stamped to provide users with real time updates to specific form status 8. Eliminates potential breaches or violations based on unsecured or misplaced paper documents 9. Incorporates trending/metrics data, risk assessment and root cause analysis to increase the overall effectiveness of quality and compliance surveillance
	Card Issuance Application	The following features are required 1. Compatible with a wide range of card printers such as Horizon etc 2. Centralized control of all card issuance and consumer selected PIN operations 1. Integrates smoothly with any TWAIN- or Video for Windows-compatible cameras, scanners and other input devices 2. Capture through TWAIN, Video for Windows or file input BMP, .JPG,

S.No.	Title	Specification
		.TIF,WMF, .TGA, .PCX image file types 3. Support for proximity smart cards, Bar code and magnetic stripe encoding capabilities 4. OS Platform: MS Windows OS 5. Supports flexible card design with text, graphics, photo and bar code fields Font sizing and colors Magnetic stripe encoding through printer fonts 6. Supports immediate issuance of new and replacement cards at any Registration in Nigeria
	Help Desk Application	1. Enterprise version with built-in connectivity for standard LDAP and Microsoft's Active Directory 2. Web Help Desk 3. Seamlessly integrates into your companys IT 4. Web interface 5. Should be equipped with cross-platform technology 6. Should have a relational Database backend and ability to interface with most DBMS 7. Should be able to prioritize help requests 8. Should enable clients access and self help Should enable E-mail submissions 9. Multi-site functionality to manage requests, assets and technicians separately for different sites in your organization 10. Should have in-built search engine 11. Access and update connected-IT equipment inventory 12. Manage both hardware and software and the clients they are assigned to 13. Build parent/child relationships between assets 14. Generate performance report for all HD requests 15. Built-in Web functionality 16. Automatic alerts and updates via email 17. Ability to generate reports and exports in spreadsheets and PDF 18. Ability to track labour and travel time and generate instant PDF quotes 1. Web-based knowledge-base system for users and technicians to search and add the troubleshooting docs

iii) MINIMUM REQUIREMENT FOR VENTILATION AND AIR CONDITIONING

E	**Ventilation and Air Conditioning**	Ventilation and Air Conditioning Systems must be installed and operational at all times in the registration centers to maintain the temperature within acceptable ranges as well as provide acceptable indoor air quality.
	Air Condition	1. Standing unit AC with 24000 BTU Equivalent cooling, Minimum cooling power of 1300 watts, Auto built-in water pump, Quiet operation

iv) MINIMUM REQUIREMNT FOR PRIMARY AND BACKUP POWER

F	**Primary and Backup Power**	Primary and Backup Power Systems should be designed to minimize service disruptions at the registration centers.
	High Voltage Transformer	1. Load Power Factor: Unity to 0.3 leading or lagging 2. Harmonic Distortion: <1% maximum added Noise Rejection (typical): 3. Common mode: -120 dB (.1Hz to 30 MHz) 4. Normal Mode: -20 dB/decade (1KHz to 10 MHz.) 5. Taps: 2-FACN @ 2.5% each, 4-FBCN @ 2.5% each 6. Electromagnetic Noise: 0.1 gauss and 1.5 ft. 7. Load rating: Continuous regardless of line/load conditions 8. Dielectric Strength: 4000 VAC. MTBF > 150000 hrs 9. Insulation: Class N, 2000C system 10. Cooling: Natural convection cooling: Full load operating temperature rise shall be less than 1150C above ambient. 11. Single point ground (SPG) shall be of copper construction with minimum thickness of ¼” x ¼”. 12. Silver plated to provide connection of lowest possible resistance to all ground wires secured to the SPG.
	Backup Generator	1. Output: 480V AC 3ph, 300KVA, 50Hz 2. John Deere Engine 3. 6 Engine Cylinders 4. Engine horse power maximum rating > 250hp 5. Sound proof, open quietness should be <= 80dB at 7 meters 6. 1000 gallon base fuel-tank 7. Over-speed protections, automatic shutdown on fault condition 8. LCD display for operation status 9. Low oil alert and low oil shutdown.
	Automatic Turnover Switch (ATS)	1. Heavy duty switch with minimum of 1200A rating 2. 50 hertz operation, 3. 3 phase minimum of 240V 4. NEMA 3R enclosure with microprocessor control panel 5. Single solenoid wire design mechanically held and electrically operated 6. Signal before transfer contacts

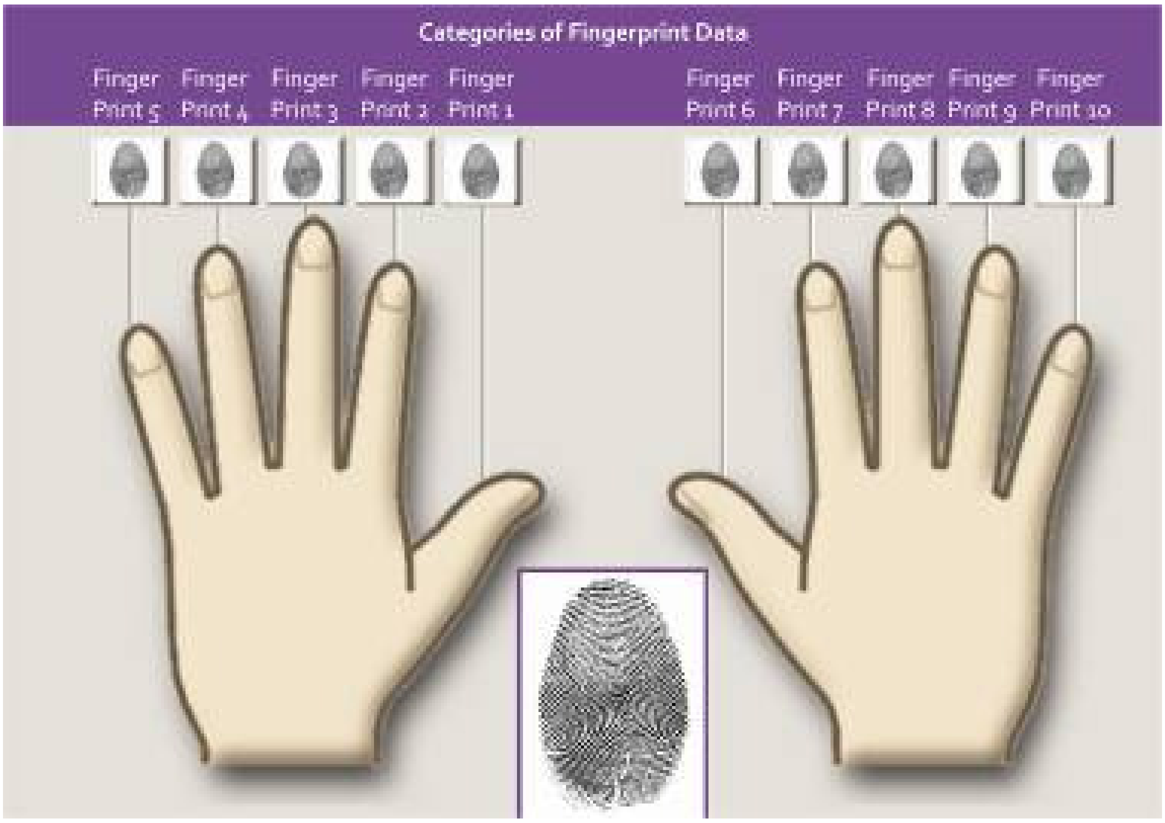
		7. UL1008 listed 8. Indicating LED's for switch position 9. Standby operation and utility 10. Manual test switch 11. Time delay bypass switch 12. Solid Neutral termination.
	Surge Protection Device (SPD)	1. Porcelain-built power surge protection device with high current greater than 1200A, 2. KEMA testing certification 3. 50 hertz rated frequency 4. CTF-D27 drop out fuse and support for applicable standards IEC282.2-2000 and ANSI/IEEE C37.41-2000.
	Automatic Voltage Regulator (AVR)	1. 250KVA output power 2. 240V 3 phase input voltage at ±5% 3. 50hertz frequency 4. 95% efficiency 5. Response speed not more than 1.5s 6. Ambient temperature range 5 – 40oC ambient 7. insulation resistance more than 2MΩ 8. Without breakdown and flashover phenomenon at overload capacity 9. 2x of rated current for 1 minute, 10. Microprocessor control with LCD display 11. Perfect automatic protection against extremely high or low voltages, Overload, over-current, or short circuit 12. Surge and lightning protection
	Uninterruptible Power Supply (UPS)	1. High performance redundant power protection 2. Scalable power and runtime suitable for datacenters. 3. Input: 3phase, 480V, 50Hz +/-3Hz (auto sensing), pf=0.99. 4. Output: 250kVA, 480V 3ph, 50Hz +/-1Hz, 5. Built-in maintenance and static bypass 6. Waveform type preferably pure sine wave. 7. Batteries: Leak-proof, Lead-Acid battery with suspended electrolyte. 8. Runtime: Full load backup time should not be less than 12hrs. 9. Recharge time: Less than 36 hours for full charge from 0% charge. 10. Full featured monitoring and alarm systems 11. LCD display for operation 12. Load bud synchronized system for use with Static Bus Transfer Switches (STS).
	Power Distribution Unit (PDU)	1. 230V output voltage 2. 1U form factor 3. 16A maximum current drawn per phase 4. IEC 320 C13 output connections 5. 230V input voltage 6. 50hertz±5% input frequency rating 7. IEC 320 C14 input connector

		8. 1.98 meters cord length 9. Maximum input current of 21A 10. load capacity >3.68KVA, EN 55024 listed
	Earthing System	1. Fault current rating of 20A 2. Simple design 3. High safety 4. Transformer neutral earthed 5. Frames of the electrical loads are connected to earth.

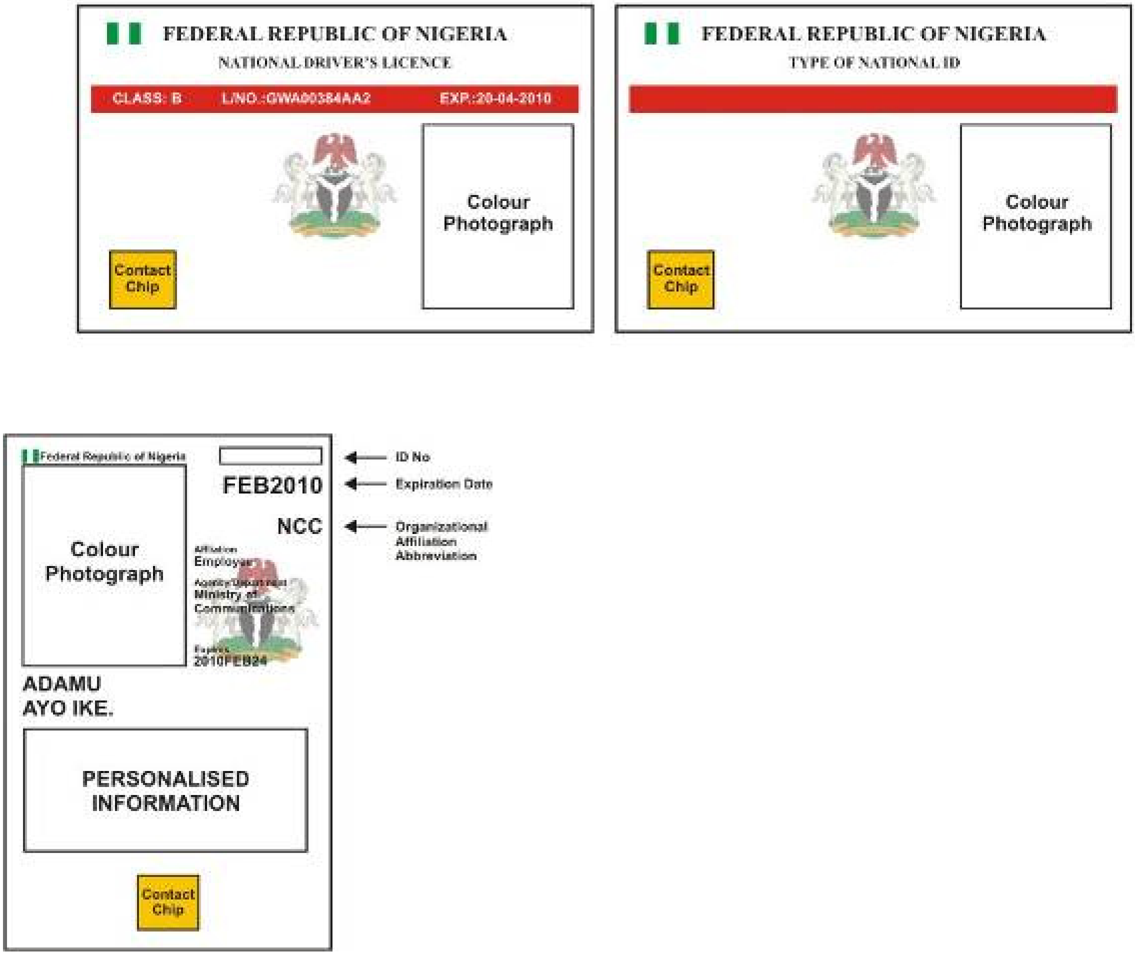
Appendix K: NIMC CERTIFICATION PROGRAM

LIST OF FIGURES

Figure 1: Categories of Fingerprint Data



Finger 4: Card specification



LIST OF FORMS

Form 1: NIMC Subject Enrollment and Request for NIN

Form 2: NIMC Request for Domain Code

NIMC ELECTRONIC DATA EXCHANGE REQUEST FORM

I. Requested Data Exchange Access (Check all that apply)

Request to: □ Add User □ Delete User □ Change User

Data Access: □ Upload □ Download □ Delete □ Rename Date: __ / __ / ____

II. Agency/Organization User Information (or BSP Contractor)

Entity Name: _____ Submitter ID(s): _____ (See 1 on instructions)

E-Mail Address: _____

Service Account Contact E-Mail Address: _____

Street Address: _____ City, State: _____

Telephone: _____ IP Address: _____

User First Name: _____ Phone: _____

User Last Name: _____ Last four of NIN: ____

Note: If this is for an automated service account, you must include a source IP address. A user name and password for the service account will be returned through the NIMC Gateway server. All individual accounts must also include a first and last name, the last four numbers of the NIN, and an email address. Any request received without this information will not be processed.

Agency/BSP Partner Authorization: (Entity point of contact *(Security Liaison)* for all Electronic Data Exchange requests)

Name: _____ Position: _____ Email Address: _____ Date: __ / __ / __

Agency/BSP Partner Technical Representative: (Entity point of contact for all technical issues)

Name: _____ Email Address: _____

III. Data Exchange Submitter Information (unless direct access, use BSP information)

Submitter Name:_____ ID Number: _____

Street Address: _____ City, State: _____

Phone: _____ FAX: _____

E-Mail Address: _____

Contact Person: _____ Phone: _____

Technical Representative: _____ Phone: _____

IV. Data Exchange Information Types / NIMC Information Owner Authorization (Check all that apply)

Name1 data to exchange: __________________ Name5 data to exchange: __________________

Name2 data to exchange: __________________ Name6 data to exchange: __________________

Name3 data to exchange: __________________ Name7 data to exchange: __________________

Name4 data to exchange: __________________

NIMC Data Owner: _____ NIMC Data Owner: _____

Note: Data Owner information to be completed by NIMC personnel

V. User Affirmation Requirement

Each individual accessing NIMC computer systems is required to read and sign an Affirmation Statement.
Fax/email all Affirmation Statements to : Attention: Data Security

Affirmation Statement: □ Attached □ On File

Note: Any new individual account requests received without an Affirmation Statement will not be processed.
Note: All password reset requests should be referred to [ ] Customer Support at [ ]

VI. NIMC ID Information (To be completed by NIMC personnel)

User ID: _____ Password: _____ Date: __ / __ / ____ Setup: ____ To Prod: __/ __ / ____

Permissions Granted: □ Upload □ Download □ Delete □ Rename

Group Name(s): _____

Form 3: NIMC Gateway Access Agreement

Form 4: NIMC Enrollment Technical Requirements

Form 6: NIMC Verification Request

Form 7: Business and process certification Form

NIMC Business and Process Certification Form

COMPANY NAME: ____

NIMC SUPPLIER CODE: _______________________

STREET: ____

TELEPHONE: ____________________________

CITY, STATE: ____

DIVISION OF: ____________________________

Persons contacted

Title____

____

____

____

____

Assessmen□ Aud□ Performed by: ______________________________________

Date: __________________

NIMC member: __________________________________ indicate your NIMC Division.

SUMMARY RESULTS

Status: GREEN□ Acceptable YELLOW□ Capable C/Actions required □RED

System not capable

Red must be checked for any finding on a No=Red question.
YELLOW or **RED** must have documented corrective actions and close out date.

If **RED** does Supplier:

a. Currently perform 100% inspection of NIMC Member defined KCs?

□Yes □ No

b. Intend to implement process certification □Yes □No (**No = RED**)

Comments:

____

____

____

____

____

____

Notes:

1. Comment sections should be utilized to reference alternate process control procedures, documents, practices and other pertinent information to address assessment questions.
2. Questions without the presence of a checkbox under the N/A column must be answered Yes or No.
3. **Alternate Process Control systems that achieve the same results will be considered acceptable.**

Process Certification System Requirement	**UTCQR-09.1**	**Yes**	**No**	**N/A**
1. Are there a defined organization structure, procedures, and documented roles & responsibilities to ensure implementation and continuous improvement of the process? Is there evidence of documented training: ▪ Management? **No = Yellow,** If responsible for Audit **No = RED** ▪ Manufacturing Engineering / Process Owner? **No = RED** ▪ Quality Auditors? **No = RED** ▪ Operators / persons performing the process? **No = RED** People in CI roles, ISO-QS-AS certified. See quality manual, procedures, W.I.'s, HR files, diplomas, certificates, and or attendance sheets from training classes completed. See control plan and or procedures for audit responsibility. **Comments:** ____ ____ ____ ______________	5.0	□ □ □ □ □	□ □ □ □ □	
2. Has the process flow map been defined? ▪ Upstream DATABSAE that must be monitored and controlled? ▪ Supplier DATABSAE that must be monitored and controlled?	5.0	□ □ □	□ □ □	□

▪ Process elements that impact NIMC member or Producer identified? **No = RED:** Work instructions / Operation sheets can be used in lieu of flowcharts. Is there a methodology for determining critical process inputs for controlling processes? **Comments:** ____ ____ ____ __________________		□	□	□
3. Does the producer have Business processes requiring process control as identified by a NIMC member? ▪ Are the requirements as defined in paragraph 5.2 met? **No = Red:** (e.g., a design, contract, purchase order, plan, schedule, instructions, delivery process etc.). **Comments:** ____ ______ ____ ______ ____ ______	4.0	□ □	□ □	□ □
4. Has Measurement System Analysis (MSA) / Gage R&R studies been performed**?** ▪ Upstream processes DATABSE? ▪ Upstream producer of DATA? ▪ Documented evidence of MSA / Gage R&R criteria? ▪ Inspection processes? **No = RED:** Audit measurement methods identified in the process map / control plan. **Comments:** ____ ______ ____ ______ ____ ______ ____ ______	5.2	□ □ □ □ □	□ □ □ □ □	□

Process Certification System Requirement	*4.4*	**Yes**	**No**	**N/A**
5. If the NIMC member has not communicated the DATA has a methodology been established for selecting processes and DATA for variability reduction based on internal measurements and or requirements? **No = RED:** (New or 1st time producer assessment **N0 = Yellow**), Prioritization rational based on customer or internal metrics, QA/CI procedures, audit/CAR findings, reaction to in-process issues, etc. **Comments:** ____ ____ ____ ____ _____________________________________	5.0	□	□	
6. Is there a monitoring system for in-process control of process DATA and NIMC member PIV? **No = RED:** Control / run charts, procedure for review, monitoring, reacting, turnbacks, at the process element / steps controlling and creating the DATA. **Comments:** ____ ____ ____ ____________________________	5.0	□	□	
7. Does the producer have procedures for controlling DATA applicable to sub-tier suppliers? **No = RED:** (New or 1st time producer assessment **N0 = Yellow**), Stated in the quality requirements, drawings, and or purchase orders. How did they flow down NIMC's requirements? **Comments:** ____ _________ ____ _________ ____ _________ ____ _________	5.0	□	□	□
8. Does the producer have a process control plan that addresses the following?	5.1	a. □	□	

a. Processes to be monitored or generic process identification. b. DATABASE description and requirement. c. PIV's settings and control method. d. Expected process capability of defined DATABASE. e. Process step where measurements are taken. f. Type of control method to be used to monitor the process and DATA. g. Subgroup size used for process control / monitoring (if required). h. Frequency of measurements / monitoring. i. Method of measurement or gauging. j. Actions required when capability levels are not maintained. k. Self Audit based on process / DATA capability cannot exceed 12 months. **No = RED:** Are elements covered by the controlling system, W.I.s, op sheets, operator check lists, tooling reference documents, measurement procedures, PM, or stand alone control plans). ***Note:*** *If the above items are available in the process operation (i.e., work instructions, manuals, etc.) they do not need to be documented in the process control plan. Alternate Process Control Plans that achieve the same results will be considered acceptable.* **Comments:** ____ ____ ____ ____ _____________________________________		b. □ c. □ d. □ e. □ f. □ g. □ h. □ i. □ j. □ k. □	□ □ □ □ □ □ □ □ □ □	□

Process Certification System Requirement	***4.5***	**Yes**	**No**	
8-1. Does the data reflect the process control plan requirements (i.e. capability)? List example part numbers and or processes audited. Example 1: Example 2: Example 3: **No = RED:** For Mfg processes, data from similar parts and features with the same tolerance produced in the same cells or machines may be used. Similar business / support processes with the same requirements can be used. Capability requirements may be less than that stated in NIMC (5.2) on upstream process PIVs and DATA (ref. Question #2) but current data must show the NIMC (5.2) capability requirements are being maintained on the NIMC member or Producer identified processes and or PIV **Comments:** ____ ____ ____ ____________	5.1	□	□	[redacted]
9. For initial audit of processes and or PIV's reported as certified that contain Variable Measured Characteristics, do they demonstrate a Cpk of 1.33 or greater for (25) consecutive observations or (30) days of output whichever is greater with no non-conformances? **No = RED:** New or 1st time producer "assessments" that cannot meet this requirement or for "audit" written concurrence from the NIMC member that the 1.33 requirement cannot be satisfied check n/a box. Examine NIMC member records. Verify the proper capability index is used (Cpk, Cpu, etc.). **Comments:** ____ ____ ____ _	5.2	□	□	□

10. For initial audit of processes and or PIV's reported as certified, that contain Attribute Measured Characteristics, do they demonstrate a minimum of (45) consecutive observations or (30) days of output whichever is greater with no non-conformances? For Business/Support processes (45) observations and/or (6) months with no non-conformances / Turn-backs that effect 100% compliance to customer requirements?	5.2	□	□	□
10-1. For sustaining, does the Mfg. Processes meet the capability requirements over the last (90) days? Does the Business or Support processes meet the capability requirements over the last (6) months? **No = RED:** New or 1st time producer "assessments" that do not meet this requirement check n/a box. N/A box cannot be used for producer audits. Examine records to verify compliance. If other criteria is used the producer must show documented approval from the responsible NIMC member. **Comments:** ____ ____ ____ ____________		□	□	□
11. Is Preventative Maintenance Plan established and being maintained? **No = RED:** Check to see if a documented maintenance schedule exists and records are available and retained. Business processes only (n/a) can be used. **Comments:** ____ ____ ____ ____ ____ ____________ ____ ____	5.2.	□	□	□
Criteria for Compliance, Control, and Continuous Improvement	***4.6***	**Yes**	**No**	

12. Periodic self-audits performed to verify controlling actions specified in the control plan are satisfied? - Is there evidence of Producer Quality Assurance system audits that include process control / certification (once every twelve months) being completed? **No = RED:** Check for self-audit, schedule, records, and results. Must be available upon request. **Comments:** ____ ____ ____ ____ ____ ____ ____ ____	5.3	□ □	□ □
13. Are the process capability records of the PIV’s available to the customer upon request? **No = RED:** Reference any NIMC member’s required reporting records. When PIV’s have not been defined by a NIMC member process capability data must be available to complete the audit. **Comments:** ____ ____ ____ ____ ____ ____ ____ ____	5.3	□	□

Form 8: NIMC ATTESTATION AND CERTIFICATION FORM

NIMC Attestation Form

National Identification Number (NIN): ________________________________

Name of Organization: ________________________________

Street: ________________________________

City, State : ________________________________

Primary Contact: ________________________________

Title: ________________________________

Phone Number: ________________________________

E-Mail Address: ________________________________

On behalf of ____,

Organization/agency Name

I hereby attest that, in consultation with the responsible Data director(s), a thorough review and assessment of all ICT Certificates has been completed, and each Database, as appropriate, is enrolled with NIMC Database and NIMC Gateway approved Proficiency Biometrics Service provider that meets regulatory requirements set forth under the NIMC Act with respect to the variety and frequency of testing for the period January 1, _______ to December 31, _______.

I further attest that, should my organization acquire a new Number and/or perform regulated testing not previously covered by this document, my organization will enroll and participate with NIMC Database and NIMC Gateway approved Proficiency Testing provider for the next scheduled proficiency testing event.

____ ____________________

Director General Date

Submit only one completed and signed Attestation Form for your organization.

Due Annually no later than January 31

Form 9: NIMC Gateway Access Agreement Form

Form 10: NIMC BSP Form