GOVERNMENT OF JAMAICA
OFFICE OF THE PRIME MINISTER

Planned Implementation of a National Identification System for Jamaica

CONCEPT NOTE

April 13, 2017

PREPARED BY
Bernard Morvant
Subject Matter Expert Identity
Javier Preciozzi
ICT Consultant

TABLE OF CONTENTS

PROJECT SYNOPSIS

Project Title:	Implementation of a National Identification System for Jamaica Assistance
Project ID:	
Project starting date:	June 20, 2016
Project end date:	June 30, 2017

Document Title	NIDS Implementation / Concept Notes
Purpose	The Consultant Team has been engaged to support the Design and Development of the ICT Architecture for the Implementation of a National Identification System (NIDS) for Jamaica. This report represents the functional and technical concept notes for the NIDS Implementation that includes: • Target project governance and human organization • NIDS use cases • High Level Illustrative NIDS Process Flow • Biometrics requirements • System architecture • Security guidelines • Identity framework and Interoperability This report has to be considered as a support document for the tender technical specifications of the procurement preparation phase.

DOCUMENT REVISIONS

Document Revision	Date	Description
0.1	September 09, 2016	Internal Working Draft
1.0	September 21, 2016	Final Draft
1.1	April 13,2017	Updated Version

1. EXECUTIVE SUMMARY

The concept of a National Registration System for Jamaica has been discussed since the 1970's and its introduction was one of the recommendations made in 1994 by the then Electoral Advisory Committee. The concept is that each person, from birth, should be issued with a unique number, which would be used when transacting business. Over the years, the concept has evolved into a national identification system (NIDS). The NIDS would provide for a unique, reliable, verifiable and secure way of authenticating an individual's identity. It would also facilitate the establishment of a database with secure authorized access and the issuance of a national identification number and an identity card to all citizens and persons ordinarily resident in Jamaica.
Furthermore, a bill draft was prepared and had gone through a review process by the cabinet and has been sent to the Parliament for review. Existing legislation, such as those governing the activities of the Registrar General's Department (RGD), Electoral Office of Jamaica (EOJ), Tax Administration of Jamaica (TAJ), the Passport Immigration and Citizenship Agency (PICA) and the National Insurance Scheme (NIS), speak to identity management as it relates to the specific functions of 'its parent' Agency and are referenced in the draft bill to make sure any necessary update once the NIDS bill is passed will be automatically performed.

The Government is therefore seeking to establish a NIDS, which will see the institution of a unique, reliable and secure method of authenticating an individual's identity. Each person registered under the NIDS will be issued with a National Identification Number (NIN), which will be their unique identifier in the system. Information captured through registration for a NIN will be stored in a secure National Civil and Biometric Database (NCBD). The use of the NIN as the primary key will enable interconnectivity of the NIDS database and all records within existing GOJ databases. Therefore, the development and implementation of a NIDS will require modifications to existing GOJ databases in order to accommodate the use of the NIN in this way.
The establishment of a NIDS will contribute to the achievement of key 'Vision 2030' goals, including effective social protection, security and safety, effective governance, an enabling business environment, a technology-enabled society and improved national competitiveness. The National Identification System is also aligned to the strategic areas of the Medium Term Socio-Economic Policy Framework (2015 – 2018), namely, Development and Protection of Human Capital, National Security and Justice, Economic Stability and Competitiveness and Employment.

The proposed implementation of the National Identification System for Jamaica will, *inter alia*:

1. Issue each citizen or persons ordinarily resident in Jamaica, a lifetime unique national identification number (NIN) from birth.
2. Establish a reliable database of Jamaican citizens and other individuals, ordinarily resident in Jamaica with an NIN as the primary key/identifier of a person in the system.
3. Issue each citizen or person ordinarily resident with a multipurpose smart identification card that will be used across multiple agencies to access services and benefits. The multi-purpose unique common identifier smart card will be used for schools, PATH, NHF, NIS, to access services in the hospitals and could eventually replace the TRN and possibly the voter's ID.
4. The system will provide an effective and convenient system of ID verification and authentication using photos and fingerprints thereby reducing the possibility of persons having multiple identities.
5. Improved governance and management of national, social, economic and security programs.
6. Strengthening of immigration and border control arrangements.
7. Cost takeout and improved precision in the delivery of government services through the streamlining of business processes and a reduction in fraud and abuse.
8. Guarantee there is 1 and only 1 unique and verifiable identification per person.

Central to NIDS is a unique National Identification Number (NIN) that is assigned to eligible participants. To maintain system integrity and trust, a NIN is only issued once an application has been vetted and approved. The NIN is assigned permanently to the enrollee, providing a consistent and persistent means of identification throughout government and the private sector.

Applicants will enroll in NIDS either at a dedicated enrollment center or at a mobile enrollment station (for example, mobile stations can support enrollment of the elderly or infirm, enrollment in schools and/or enrollment in hospital maternity wards). Enrollment can occur as soon as birth or at any age thereafter. An application for NIDS enrollment is independently vetted for authenticity and uniqueness, including authentication of proof-of-identity documents provided. Once approved, the applicant is issued a NIN, an ID card may be produced, and the card can then be used to assert identity with both government and private sector stakeholders. Authorized stakeholders can use the NIDS online Identity Verification Service (IVS) to verify identity. The IVS is operated as fee-for-service to provide revenue that will help support and sustain NIDS.

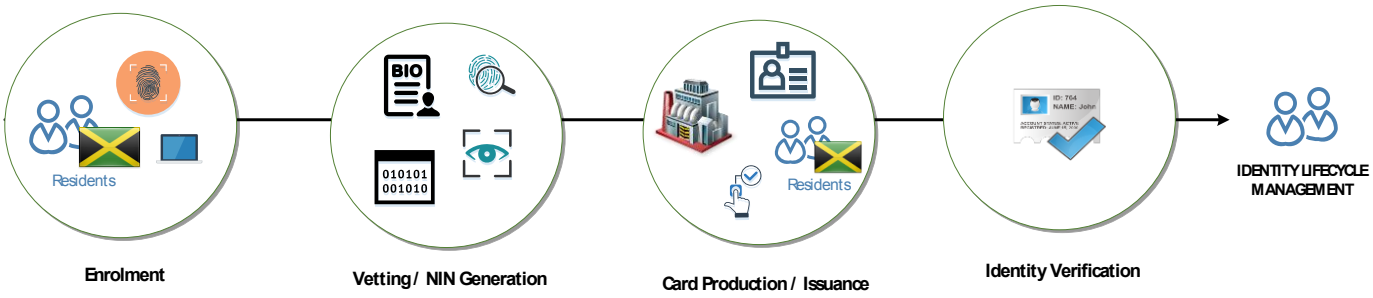

Figure 1: NIDS workflow process overview

2. NIDS IMPLEMENTATION

2.1. GOVERNANCE & OPERATIONAL DECISIONS

NIDS is a multi-components project with many interrelated dependencies and coordination considerations.

While Jamaica has experience with ICT identity systems for specific applications, including incorporating biometrics it is recommended after evaluation of the different options to manage NIDS from a single entity standpoint with a recommendation of an approach based on a transformed RGD and named National Identification and Registration Authority (NIRA) reporting to the Office of the Prime Minister. In order to best leverage existing and future capabilities on foundational identity (RGD database and NIDS database), it is recommended to manage the implementation of NIDS by managing and coordinating the major functional roles (enrollment, vetting, card production and identity verification) within the division of civil identification of NIRA .

The cooperation of identified operating organizations such as e GOV Jamaica for the hosting of the NIRA systems and Jamaica Post for the card production centre hosting and their commitment to participate, must be confirmed and formalized at the earliest.

NIRA shall have overall responsibility for NIDS operation, maintenance, storage and protection of personal data. Entities supporting individual functions (such as enrollment, etc.) should operate under formal agreement with the division of civil identification of NIRA and Service Level Agreements (SLAs) should be established to define the required performance to ensure efficient, effective operation.

There are decisions to be made as the project progresses that do not directly impact the initial implementation critical path, other identity verification process with other MDA's beyond the initial one with the Ministry of Labour and Social Security for PATH.

Operating Entities Assumptions

Where to locate / operate the Core Identity Management Systems & Networking?

Recommendation: eGovJA; has depth and experience of operating and maintaining sensitive ICT systems, including meeting high uptime and reliability requirements with established ICT Security Polices; has an established secure data processing center environment for hosting ICT servers and network

equipment; has responsibility for maintaining and enhancing the Government network. A dedicated team should be established within eGovJA based on the proposal of e GOV Jamaica and MoU signed between the two parties

Where to locate the Biometrics System(s) (ABIS)?

Recommendation: Co-locate the ABIS at eGovJA with the other NIDS core server equipment. Enrollment of biometrics will be performed elsewhere (at the enrollment locations); would operate according to an MOU with the NIDS system owner. Maintain ABIS original data in a separated database from the NIDS biographic and demographic data.

Where to situate / operate enrollment centers?

Recommendation : Use the existing RGD Offices in the hospitals for the registration of the new born ; 160 + locations island-wide provide convenience to stakeholders; NIRA will cooperate with JAMAICA POST to take advantage of the infrastructure of the existing Jamaica Post which will be upgraded in 43 sites around the country ; while the experience of Jamaica Post is limited in this type of operations , it has the experience of managing processes in a secure protocol certified by the International Postal Organization; Also Jamaica Post is in the process of upgrading their services by installing automated countertop terminals to facilitate their business .

Where to locate / operate Vetting?

For consideration: Best practice is to not operate multiple functions of an identity system under a single authority (department) to prevent collusion through separation of duties; therefore a specific department for identity vetting will be created and located at Jamaica Post Central Building .

Where to locate / operate Card Production?

For consideration: cards are only authorized for Production once applications are vetted and card production requests are generated. EOJ, PICA, FLA and TAJ all have secure credential production experience; however, the scenario which is selected at this

point in time is to locate the card production operations in the central building of Jamaica Post as it is a secure facility with a vault and co located with the shipment department for shipment and transfer of the cards to the activation sites (enrolment location)..

Where to Issue cards (delivery to the enrollee)?

For consideration: Jamaica Post local offices; known convenient location for enrollee to return to for card pickup; in-person card issuance allows verification of the biometric on the card; assures delivery of the card to the correct enrollee;

Where to locate and operate the off-site failover and disaster recovery capabilities?

For consideration: Evaluation of other critical systems such as supported by eGovJA to baseline potential disaster recovery and failover location. Emphasis on verification system for failover operations should be considered (as is revenue generating).

The Following figure is illustrating the high level organization and the communication workflow overview as it should be in the context of the NIDS project:

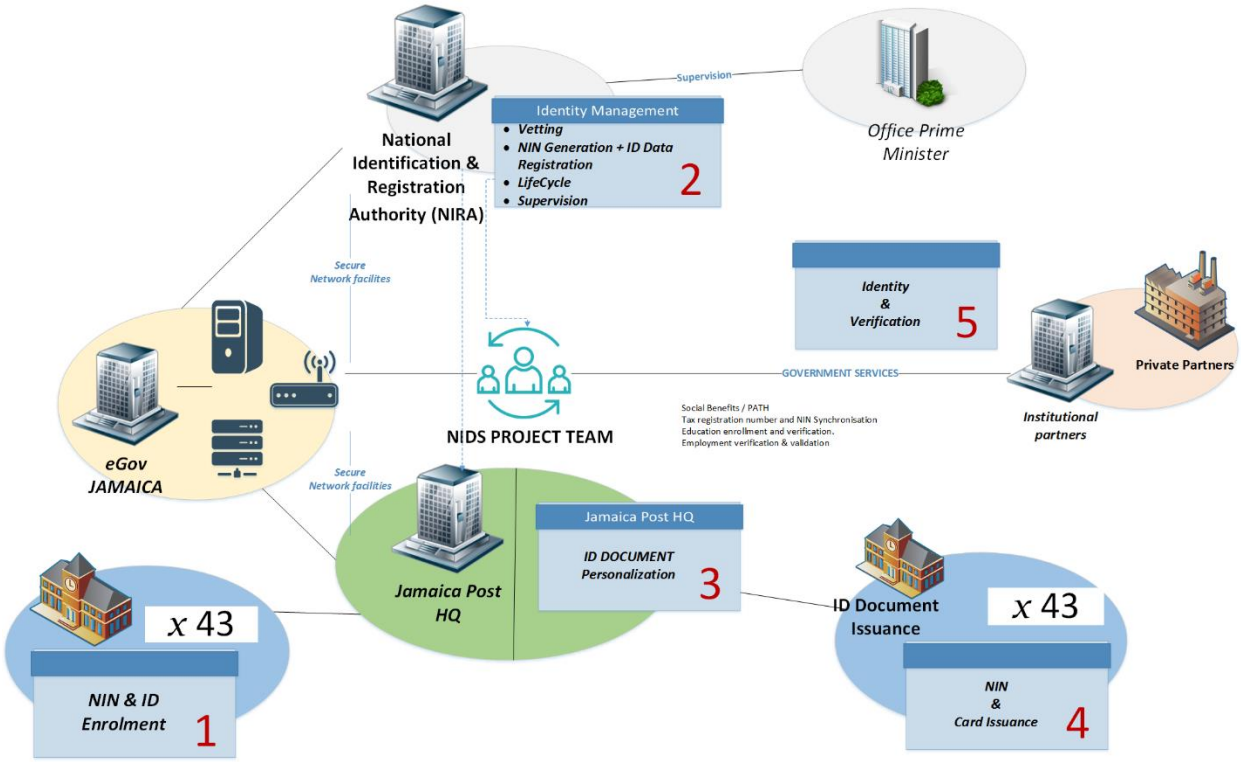

Figure 2: NIDS organization and communication workflow overview

In addition to this target of the institutional organization, the NIDS program is also relying on a strong human organization structured mainly around the following actors:

1. **NIN & ID Enrolment**
   - Local supervisor
   - Enrolment agent
   - Issuance agent
   - Receptionist agent

2. **Identity management**
   - Central supervisor
   - Vetting manager
   - ID data application manager
   - Central production manager
   - Help desk support manager
   - Vetting agent
   - Help desk support agent
   - System administrator
   - IT manager
   - Security officer
   - Administrative and process support

3. **Card production center**
   - Production manager
   - Production agent
   - Stock manager
   - Quality agent

Note: *To guarantee the continuity and consistency of the NIDS project team we assume here that NIRA will take over from the NIDS project team and will be in charge of the hiring and the staffing of all the human resources for the central activities and the system deployment assistance.*

2.2. NIDS USE CASES

A number of high priority/immediate use cases for NIDS with significant benefits and ROI to stakeholders have been identified. These include:

- Streamlining the provisioning and delivery of government services, including:
  - Social Benefits (pensions, welfare assistance, PATH grants, etc.) including eligibility determination.
  - Healthcare – eligibility and delivery.
  - Tax registration and payments.
  - Licensing (including firearms).
  - Voter registration and verification.
  - Education enrollment and verification.
  - Employment verification & validation.
- Reducing duplication of effort in managing separate identity systems (and updates thereof) across stakeholders.
- Lowering the total cost for managing identity via a common service.
- Facilitating data sharing between organizations.
- Support for online financial transactions (tax payments, etc.) including e-transactions.
- Reducing identity fraud and abuse.
- Providing a more efficient and effective means for “proof of life” verification.
- Reducing the risks to issue multiple passports (and other travel documents) to individuals.
- Improved identity accuracy, auditability and transparency.
- Preventing crime.

Initial priority areas-of-use for NIDS should be considered with a view to promoting high adoption rates that lead to an accelerated ROI.

3. HIGH LEVEL ILLUSTRATIVE NIDS PROCESS FLOW

The following figure is illustrating the process flow that will be handled by the NIDS system that could be divided as follows:

- Person biographic and biometric enrolment retrieving the birth data directly from the RGD database
- Central Consolidation of ID card applications and verification
- Person Registration and NIN generation
- National ID Document personalization
- Final ID card Issuance (delivery and activation)

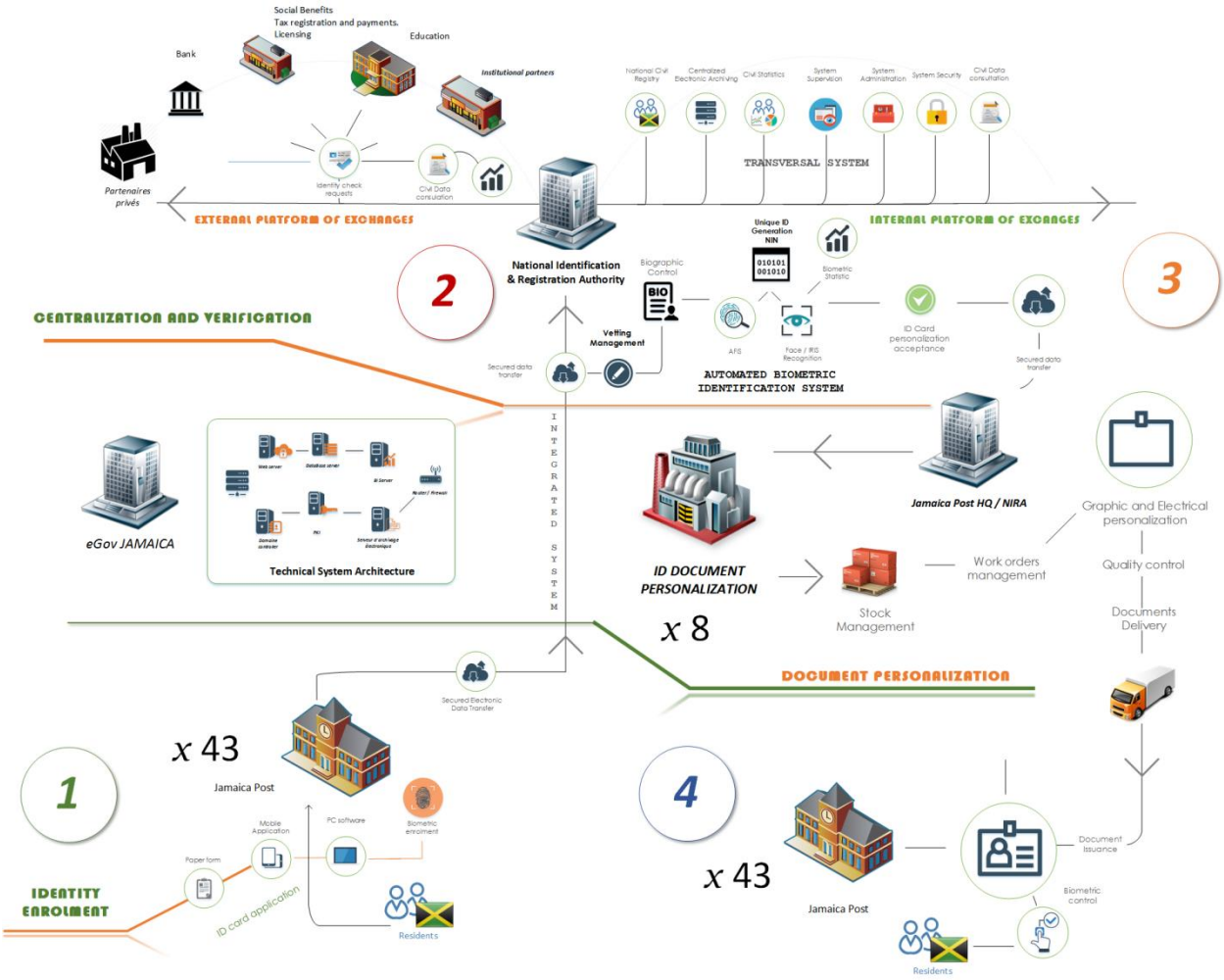

Figure 3: NIDS process flow representation

3.1. NATIONAL IDENTITY NUMBER (NIN)

The NIN is a 9-digit unique numeric number issued to each enrollee in the NIDS system and shall conclusively resolve an identity. The format provides maximum compatibility with legacy systems that were designed to support a NIN.

The NIDS system shall support the creation, issuance and life cycle management of the NIN. The number generation process implemented shall guarantee and assure uniqueness; protect and maintain an individual's privacy; be transparent; and allow full 100% auditability and reconciliation to mitigate fraud and identity theft.

3.1.1. FORMAT

The proposed format for the NIN is based on current best-practices applied to the context of existing identity frameworks. Further, this approach allows the NIN to co-exist with Tax Registration Numbers (TRNs), allowing a gradual phase-out of the TRN in favor of the NIN, yet also allowing TRNs to continue for corporations and individuals who would still need a taxpayer unique identifier, but would not qualify or require the use of a NIN for interactions with the Government.

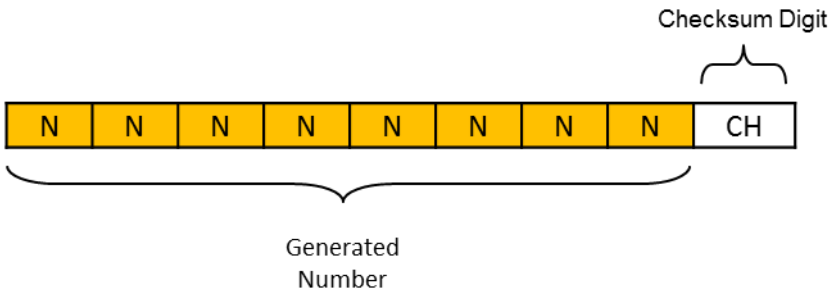

FIGURE 1: NATIONAL IDENTIFICATION NUMBER (NIN) FORMAT

NNNNNNNN	-	8-digit numeric portion Computer generated Not guessable and non-sequential
CH	-	Modulus 11 check digit Computer generated from the numeric portion and appended to the number

NINs shall be issued in the range 3xxxxxxxx to 9xxxxxxxx to leverage the existing and anticipated numbering framework. This was developed to avoid

conflict with TRNs that have been previously issued, or that may be issued in the future.

The process for generating the NIN shall exclude undesirable number sequences. Presently, the only identified undesirable number sequence is '666' but the NIDS system shall make provision to exclude other undesirable sequences if/when they are identified.

A modulus 11 check digit shall be appended at the end of the unique identifier to provide an integrity mechanism to assure the NIN is internally consistent. Use of the check digit allows a quick offline verification of the integrity of the number, and helps prevent the mis-keying of the number if it is being manually entered into a system. Note that the checksum only assures the integrity of the number; it does not assure that an identity is valid.

3.1.2. ISSUANCE

A NIN is only issued once enrolling and vetting of an application has been successfully completed. This helps ensure the integrity of the NIDS system by preventing the issuance of multiple IDs to one person. The NIN shall be unique to each individual enrolled in the NIDS system and shall remain permanently associated with their identity. In order to maintain the integrity of the system, a NIN should never be re-used.

Applications that are in process, or that require additional information to complete, shall be tracked within the NIDS system but no NIN shall be issued until the application is complete and vetting has been successfully conducted. Applications that are not vetted after a certain period of time (e.g. started, awaiting confirmatory information) should be flagged for action, and a time should be established if abandoned. Such information and statistics should be recorded and reported periodically.

Once vetted and verified, the proof-of-identity claimed documents presented as part of the enrollment process that were previously scanned and recorded should be linked with the NIN in the NIDS system. The enrollment process shall also include the intake and storage of biometrics (proposed: fingerprint and face) of the applicant. The biometrics shall be stored in a separate dedicated ABIS and also linked to the NIN.

The NIN becomes the basis for binding identity events; allowing the update of additional information, such as changes to biographic and biometric data, as relevant life events occur.

The NIN may be revoked by under specific circumstances (such as a legal determination of identity fraud, etc.). Under such circumstances, the NIN, and all data shall permanently remain in the system with its revoked status and not be eligible for future use. Such information retention is important for possible future use; e.g. to be provided to law enforcement.

NIN Issuance procedures based on age thresholds have been proposed as follows:

- For new born
- For Infants
- For Infants sub 18 years old
- For Adults

Final procedures will be documented during the development / implementation phase so that the workflow process can be developed accordingly. This work will be based on prior consulting performed and will be reviewed by a working group composed of the relevant GOJ identity experts.

3.1.3. NIN CAPACITY

The number of unique numbers using the 9-digit NIN format specified above is calculated to be approximately sixty-nine million (69,000,000). This is calculated from the total possible number combinations excluding the check digit (100,000,000) less the numbers reserved so as not to duplicate a TRN (30,000,000) and excluding undesirable number sequences (520,000+).

Rounding up the number of excluded number sequences to 1,000,000 to allow for other considerations leaves 69,000,000 usable NINs.

The current Jamaican population is presently less than 3,000,000. The current Jamaican birth rate is estimated to be not more than 50,000 per year. The proposed 9-digit NIN will therefore support 1,320 years of registration ((69,000,000 – 3,000,000)/50,000).

If the birth rate were to double, to 100,000 per year, the proposed NIN format will support 660 years of registration. If it were to quadruple, to 200,000 per year, the proposed NIN format will support 330 years of registration.

3.2. NIDS DATA REQUIREMENTS

The data architecture identifies and standardizes the data elements that are required to represent the personal information associated with an enrollee on NIDS. It defines the data elements (e.g. first name, last name, date of birth,

residential address, etc.) as well as the data element type (e.g. number, alphanumeric, date, etc.).

In an ideal world, all government systems would use standardized data architecture. Such an approach would include the following:

1. A common set of data elements
2. A common metadata specification
3. A standard data and metadata framework for interoperability (e.g. XML)

Such standardization provides consistent and standard data representation enables efficient exchange and processing between systems and removes inconsistencies/ambiguities.

3.2.1. NIDS CENTRAL CIVIL AND BIOMETRICS DATABASE

The NIDS database shall maintain and manage the identity information associated with each enrollee in the system, including links to the biometric data stored in the ABIS.

The database shall conform to accepted international standards. The data set shall consist of the core identity elements recorded during the enrollment process. This data set will be queried by the Verification Service to confirm identity.

The minimum set of data elements to be supported is summarized in the next section. The data shall be stored in the database with an electronic signature (e.g. checksum, hash, etc.) of the data record as a protection mechanism against unauthorized modification. Encryption shall be employed on key data elements in the database to ensure confidentiality of PII information. A flexible database structure and schema will be used to allow for modification/enhancement as required over time.

The database will maintain a record of associated legacy Document Identifiers, and continue to maintain them even after expiry. This will provide a complete archive and history for possible audit and/or other needs.

3.2.2. DATA FIELDS

The following table defines the proposed minimum data set to be supported by the NIDS database.

NIDS Minimum Data Set		
Field	**Description**	**Field Type**
Unique Identifier	The enrollee's unique 9 digit identifier – the NIN with calculated check digit	Numeric
Identifier Status	Valid, Suspended, Revoked, etc.	Alphanumeric
Issuing Date	Date of issuance of the NIN	Date
Enroller ID	Identifier of enrolling agent	Alphanumeric
Enrollment Date	Date of enrollment	Date
Vetting ID	Identifier of vetting agent	Alphanumeric
Vetting Date	Date of vetting	Date
Vetting Documents (multiple entries)	Image scans of the presented proof-of-identity documents. For each document, should also include the type of document and the document number/identifier.	Binary
Production ID	Identifier of production agent (if produced)	Alphanumeric
Production Date	Date of card production (if produced)	Date
Card Number	Unique card number (if produced)	Numeric
Card Type	Type of card issued e.g. standard ID card, smart card, other	Numeric or alphanumeric
Card Status	Valid, Suspended, Revoked, etc.	Alphanumeric
Expiration	Card Expiration Date	Date
Previous Cards (multiple entries)	Record of previously issued NIDS cards including card number, production ID, expiration dates and any notes	Alphanumeric
Issuing ID	Identifier of issuing agent	Alphanumeric
Issuing Date	Date of issuance	Date
Name	Stakeholder name (first, middle and last)	Alphanumeric
Title	Enrollee's title	Alphanumeric
Alias	Associated alias(es) or nicknames	Alphanumeric
Maiden Name	If applicable	Alphanumeric
Previous Name	First, middle, last	Alphanumeric
Authority	Authority for name change	Alphanumeric
Change Date	Date of Name Change	Date
Address	Present Physical Address	Alphanumeric
Email Address	Personal email address	Alphanumeric
Phone	Personal phone number	Numeric
Birth Date	Enrollee's date of birth	Date
Birth Place	Enrollee's place of birth (Town, Parish/County/State, Country)	Alphanumeric
Mother	Mother's name (or 1st Guardian)	Alphanumeric
Mother's NIN	NIN of Mother (or 1st Guardian)	Numeric

Father	Father's name (or 2nd Guardian)	Alphanumeric
Father's NIN	NIN of Father (or 2nd Guardian)	Numeric
Gender	Enrollee's gender (UN Standard classification)	Alphanumeric
Marital Status	Enrollee's marital status	Alphanumeric
Spouse Name	Name of spouse (first, middle and last)	Alphanumeric
Spouse Title	Title of spouse	Alphanumeric
Spouse Alias	Alias(es) of spouse	Alphanumeric
Citizenship	Enrollee's citizenship	Alphanumeric
Language	Enrollee's first language	Alphanumeric
Marks	Distinguishing marks	Alphanumeric
Height	Enrollee's height	Numeric
Contact	Emergency Contact information	Alphanumeric
Photo	Photograph and/or link to photograph in the ABIS (vendor to propose)	Binary and/or Alphanumeric
Photo Date	Date photograph was taken	Date
Photo ID	Identifier of agent taking the photograph	Alphanumeric
Biometric	Link to ABIS fingerprint record and other selected biometric record (iris if selected)	Alphanumeric
Biometric Date	Date biometric was captured	Date
Biometric ID	Identifier of agent capturing the biometric	Alphanumeric
Associated IDs (multiple entries)	Identifiers for associated identity numbers and document(s) (e.g. Driver's License, Health Card, etc.) including: Document type Document number Issue date Expiry date	Alphanumeric

TABLE 1: NIDS CORE DATA FIELDS

3.3. ENROLLMENT/REGISTRATION

Enrollment plays a crucial role in any identity system. The process must be sufficiently robust to ensure the validity of the information presented by a prospective enrollee, the uniqueness of each individual in the system and to minimize any opportunity for fraud. Best practices recommend a multi-step process that physically separates data entry (the gathering of information from the applicant) from the validation and adjudication of that data. This helps prevent collusive fraudulent enrollment by ensuring more than one person is involved in the process.

The enrollment process intakes biographic, demographic and biometric data from an individual and their supporting proof-of-identity claim documentation. The information gathered is then independently vetted prior to allowance of registration in the NIDS system and issuance of a unique identifying number.

Best practices recommend that enrollment is performed via an in person interview (face-to-face) with a trained, authorized enrollment agent. This process is crucial to the integrity of NIDS and in establishing and maintaining trust in the system.

Typically, enrollment is carried out at a location established by the enrolling organization as a shared co-located service within an existing facility (the local office of the Jamaica Post). Mobile enrollment stations have been used to support remote locations and also bedside registration in the maternities; and the enrollment of individuals who are unable to travel (such as the elderly or infirm). Mobile stations should have the same capabilities to intake biometric data, demographic and biographic information with the same quality and integrity of fixed enrollment locations. The NIDS framework should be able to support both fixed and mobile enrollment capability.

Enrollment Opportunities

To maximize participation in the system, consideration should be given to enrolling citizens at birth – or as soon as possible thereafter. Additional enrollment opportunities include entry to school (either upon entering school or at a pre-determined age) and enrollment at a government office when a need is first identified (e.g. applying for government services). This should be supported by multiple enrollment locations throughout the country to encourage enrollment but also by marketing/education/communication campaign.

Initial enrollment should be phased – e.g. persons reaching their 18th birthday and registering to vote for the first time, new births, etc. and at the anniversary/expiration of an existing ID credential.

There are two different scenarios for enrolment:

i) a newborn, which in general will be enrolled at hospitals at the same time he or she is registered by RGD staff in the civil registry database

ii) ii), any person older than 6 years old, where in this case the enrolment is performed at the enrolment site.

To illustrate the integration of RGD and NIDS processes, the following workflow process diagram of both processes is included, where is highlighted the relation and integration between the NIDS system and the RGD system.

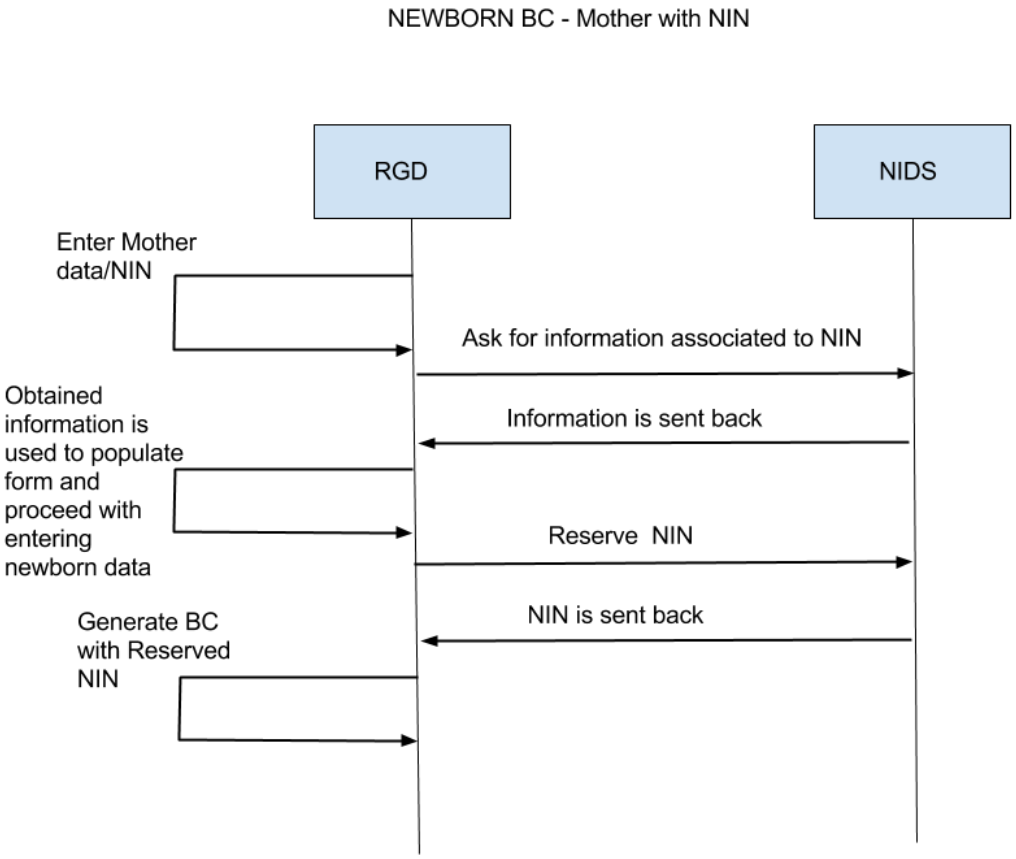

FIGURE 4- NEWBORN ENROLMENT PROCESS

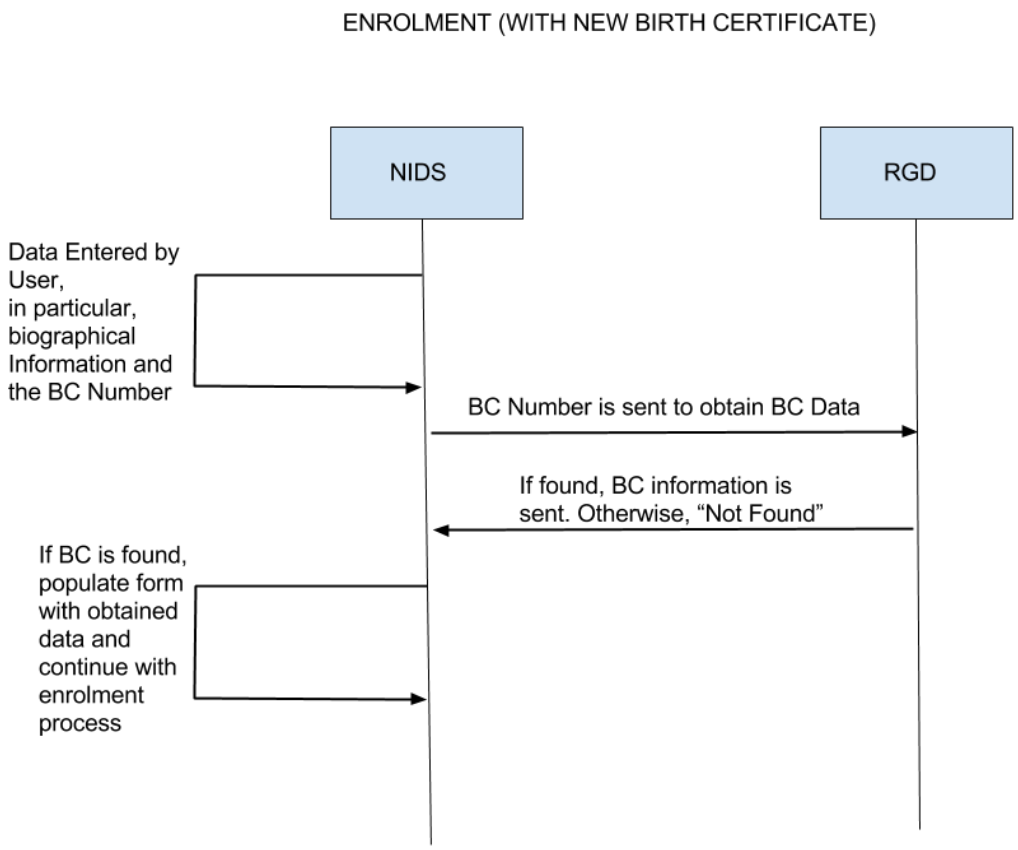

FIGURE 5 – ENROLMENT BASED ON NEW BIRTH CERTIFICATE

3.4. SCHEDULING AND PRE-REGISTRATION SYSTEM

As a complementary system to the enrolment system, we are considering scheduling and pre-registration, in order to facilitate the enrolment process. This system will be rresponsible for scheduling an appointment to perform the enrolment or renewal of the document. It will include remote/online pre-registration and in line pre-registration, while also facilitating payment processing for lost, stolen, and damaged cards (both online and in-line). Note this will be a cash-less operation so payments will have to be made via bank payments or possibly via credit/debit card.

3.5. VETTING

Vetting is a process by which the data presented by an applicant is screened for legitimacy before allowance of issuing a NIN. Once an NIN is issued an ID card may (or may not) be produced/issued. A robust vetting process helps assure the integrity of NIDS and thereby establishes trust in the system.

Applicants should be informed during enrollment that the information presented, including their biometrics, will be vetted and they should be offered an overview

of the process. Vetting includes the steps for confirmation and validation of presented biographic data. The depth of the checks will vary according to the level of and quality of the supporting materials presented.

Also during enrollment, the applicant must declare and confirm that the information given is true and complete and acknowledge that any false statement or deliberate omission may be grounds to deny the issuance of a credential, at a minimum, or may also be grounds for prosecution. This attestation must be as well captured (e.g. signing the forms) and recorded as part of the enrollment record.

Trained Vetting Officers shall adjudicate the information presented at enrollment, including biometrics, with a view to approving the applicant for acceptance into the NIDS system. The presented proof-of-identity information (including provided documentation such as birth records if not already approved during enrolment, driver's licenses, voter ID cards, etc.) should be validated against the issuing authoritative identity data sources to confirm legitimacy in case of necessity. An electronic interface is preferred where possible using either a secure electronic connection (using a NIDS system-supplied API) or via an existing verification interface (Web Portal or other). In addition, the biographic and biometric data is screened against existing enrollees in the NIDS system to prevent duplicate enrollments. The vendors should propose an API framework and format, or agree to work with the NIDS project office to define this API.

The Vetting process must be physically and operationally independent of Enrollment. Vetting must be conducted by an officer not involved in the enrollment of that individual (to prevent collusion) and vice-versa.

Experience shows that issues encountered in vetting rarely arise because of a single problem: it is usually a combination of factors that bring about potential issues and risks. It is therefore essential that the vetting process carefully in an auditable way builds a complete identity picture, so that a broad understanding of the person can be gained and all the facts verified.

3.6. CARD PRODUCTION

Once Vetting is complete and an application is approved, a NIDS ID card may be authorized for production.

To provide the greatest cost efficiency, NIDs shall use a centralized card production approach with a single facility responsible for printing. Cards shall be pre-personalized by vendor(s) who are vetted and approved for supply.

Vendor(s) will use a secure handling methodology and supply the pre-personalized stock to the central printing facility. The final personalization (including programming if a smart card) shall be carried out at the production center and the cards forwarded for issuance.

Initial cards to be issued will be standard photo ID cards with an option to issue smart cards to support digital signatures. The NIDS system will be upgradeable over time to produce, program and issue smart cards. The NIDS framework is designed to support both non-smart card and smart card based ID credentials to be used, with a migration path to smart cards in the future.

Note: *The card production process will be operated by multiples production centers that will be dispatched in 8 distinct regions. To guarantee the consistency of the data processed by each production center, all the upstream data preparation will be managed by the central site. Production centers are only processing work orders.*

3.7. CARD ISSUANCE

Following production, the NIDS ID card must be issued to the enrollee. The cards are produced at the central card production centre and securely shipped to the enrollment center for issuing to the applicant. While this has an associated level of inconvenience with the applicant being required to make a second visit to the enrollment center, it provides the added security of the card issuance being performed in-person and verified with the biometric. This assures a chain-of-trust and confirms the quality of the biometric, and that the card is not issued to anyone other than the proper applicant/recipient. Notification – such as via an email, SMS or other pre-existing best practice – to inform the applicant that their card is ready to be collected should be considered.

While Issuance is an independent process step, it is commonly performed at the same location as enrollment. This is more cost effective than establishing a separate Issuance location (the equipment needed for Issuance is already there) and typically is also convenient for the enrollee.

3.8. VERIFICATION SYSTEM

The Verification System will allow authorized stakeholders to validate and NIDS card and verify identity using the NIN and other data from the card in real time. Interface to the Verification System will be via a Web Portal or API. Authorized stakeholders are those who have established an account with the Verification Service.

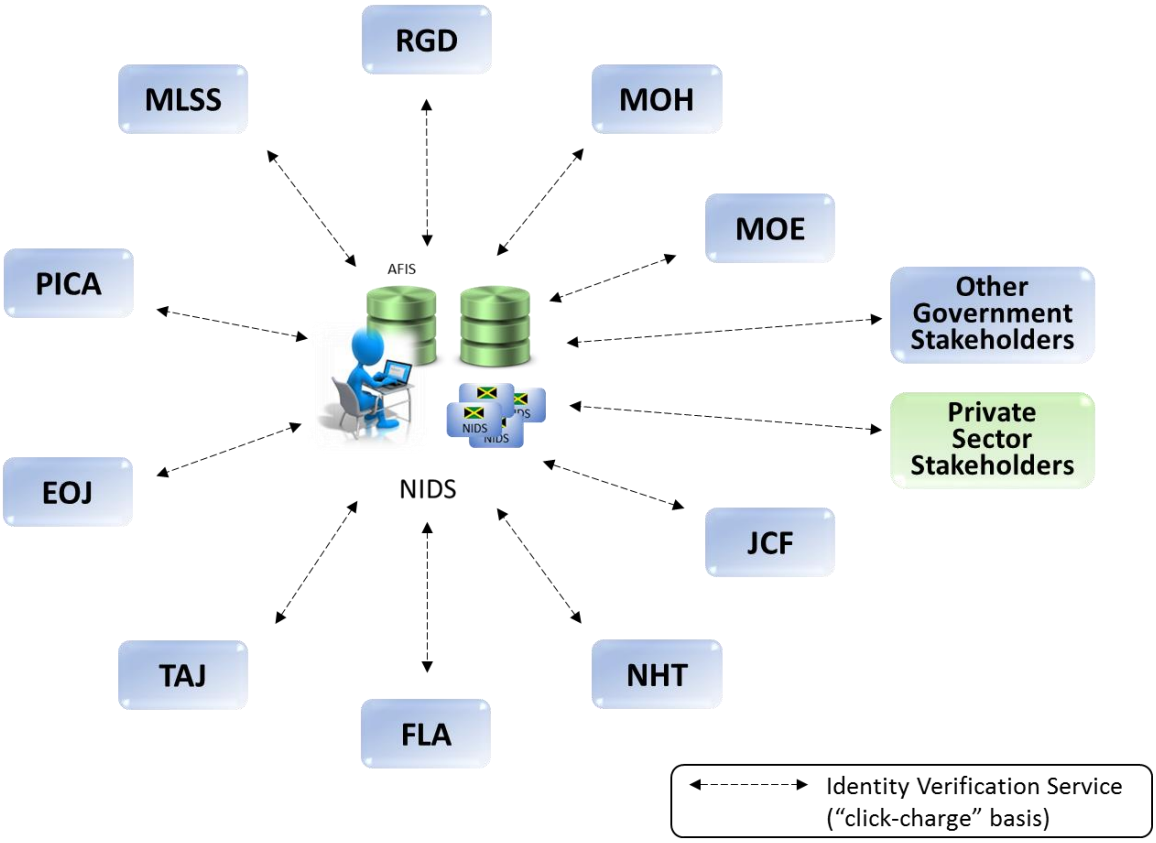

FIGURE 6: ILLUSTRATIVE IDENTITY VERIFICATION SERVICE

The Verification Service shall be established as fee-for-service (e.g. event driven click-charge), with transaction recording, billing, account management and reconciliation. Records must be auditable. Subscription and bulk pricing schedules should be developed and managed by the NIDS governance framework. Additionally, consideration and replacement fees for lost or replacement NIDS ID cards should be considered.

Note: *Verification processed will be done on a dedicated environment which will be based on the vetting ones with some additional restrictions and security features to ensure the anonymity.*

If the vendor of the system will be in charge of the software and hardware deliveries, it is important to note here that eGov Jamaica will be responsible for the hosting of the physical architecture and the definition of the security policies that will support these central activities.
eGov Jamaica will be also in charge of the support and the maintenance of the NIDS system.

3.9. IDENTITY LIFECYCLE MANAGEMENT

Key guiding principles in defining the approach to identity lifecycle management include:

- Transparency and accountability
- Increased efficiency
- Cost optimization
- Scalability and incremental expansion
- Enhanced stakeholder experience

The identity lifecycle is comprised of four basic processes: origin, use, control and retirement/archive. With respect to identity origin, the focus of most recent standards/practices focus has been on travel documents (e.g. the electronic passports based on ICAO 9303 specifications, the new generation of e-ID cards, etc.). These have focused primarily on the way the 'breeder' documents such as birth certificates are generated and as a direct consequence how such identity data are registered, validated and managed over time.
For consistency in use and control, identity management within the NIDS system framework is based around the use of a unique personal identifier (NIN) for each enrollee. Generation of the NIN serves as an anchor point for the identity lifecycle, including management of associated attributes. For transparency and accountability, once the NIN is permanently assigned to the enrolled identity it shall never be re-used or re-assigned. Authorized system users may only update attributes associated with an identity (e.g. name, address, etc.) under circumstances/conditions defined in policies, with an auditable log being maintained of all changes made.

The unique NIN identifier enables more precise maintenance and update of the identity over time; including validation and reconciliation of civil status changes (such as marriage, divorce, name change, death, etc.). The NIN also enables identity verification as a service for participating stakeholders (both in government and in private industry) and the unambiguous sharing of data across entities (where legally permissible).

The identity (and, by association, the NIN) is never deleted. Its status may become "active", "questioned", "retired", "inactive" or "revoked" but its record must unambiguously remain in the database and/or archives for transparency and future audit purposes. NINs would be expected to be never removed from the system, and their record maintained indefinitely.

Identity management is an evolving process. Processes must be adaptable and evolve on an ongoing basis as technology and environments change. The

identity management framework and infrastructure must provide the flexibility to incorporate such changes as required.

3.9.1. ID CARD LIFE CYCLE MANAGEMENT

ID card management is a subset of identity management. While an identity never expires, best practices dictate that ID cards should be issued for a finite period only. The option within the system to set the expiration date for an ID card should be fully configurable to provide the maximum flexibility in meeting different lifecycle requirements for different card types.

Cards shall have at least two unique identifiers. One is the stock number, printed on the card by the card vendor during pre-personalization; this allows tracking and auditing of inventory to prevent misuse or abuse of card stock. The second mandatory unique identifier is the UDN that is printed on the card when it is personalized. The UDN shall be linked with the NIN in the database along with its expiration date. A replacement card or renewal card will be given a new UDN and the database will be updated accordingly.

The objective of this system is also to track the life of each of the security material used to build a card (in our case just the card), starting from reception of the blank material from the supplier and ending at issuance of the document to the corresponding applicant for the duration of the card.

The NIDS system shall support independent renewal and replacement cycles for cards.

3.10. SYSTEM REPORTS & ANALYTICS TOOLS

The NIDS system must have a flexible query capability, with access control rights to protect privacy and prevent misuse or abuse. The system shall provide a number of ‘standard’ reports, pre-configured in support of key system operations such as enrollment, vetting, card production and issuance. The system shall also provide a capability to configure and customize “non-standard” reports.

An analytic tool represented by a business intelligence software (such as IBM Cognos application or any relevant open source solution like Talend software) will be also plugged into the NIDS system in order to provide statistics and dashboard on demand.

That analytic functionalities should be also proposed to the authorized stakeholders as it is illustrated into the figure n°6 located into the verification chapter.

4. BIOMETRICS REQUIREMENTS

Biometrics (fingerprint and facial), shall be enrolled for NIDS enrollees over the age of 6 years, following recommendations of the working group of identity experts of the GOJ. Facial and fingerprint biometrics are to be used and are the common best practices for large-scale ID programs. Facial recognition should be compatible with the ICAO specification for E-Passports – especially as PICA already uses facial recognition to guarantee the unicity of the applicant.

4.1.1. LESS THAN 6 YEARS

It was decided to give a NIN and a CIN starting from birth. Because until now, biometrics systems for newborn are not fully mature, the decision was to not include biometrics until 6 years old. In the case of infants less than 6 years old, no biometrics will be acquired.

4.1.2. 6 YEARS +

For persons older than 6 years old, a full biometrics enrolment will be performed. This includes the 10 fingerprints and a face image.

The major processes in NIDS associated with biometrics are:

- **Enroll** – performed during the initial in-person interview (and at renewal) with digital cameras and electronic fingerprint readers.
- **Extraction** – conversion of the raw captured data to comply with standards.
- **Comparison** – either verification with the biometric data stored or a search of the database for a match

A minimum of four fingerprints (two from each hand) is recommended for matching purposes to assert uniqueness. Finger print information shall include the enrolled digit and hand. Exception processing will be implemented for situations where fingerprints cannot be captured (e.g. loss of limb, etc.)

Biometric data should be acquired and stored in both a full image (for future new biometric matching improvements) as well as in the converted form for such as for 1:1 matching at a minimum resolution threshold as accepted by industry.

The biometric information shall be stored in an ABIS system. The ABIS system should leverage exiting know-how, experience and resources. All biometric data shall be stored in a dedicated and protected civilian database environment to ensure system integrity. The ABIS shall:

- Provide 1-to-1 (1:1) biometric authentication
- Provide a 1-to-Many (1: n) search capability.
- Conform to internationally accepted standards for biometric capture, storage and matching.
- Provide local and offsite data backup and redundancy/failover protection and disaster recovery.

4.1.3. BIOMETRICS STANDARDS

NIDS should apply the International Civil Aviation Organization (ICAO) 9303 specifications as the basis specification for both facial and fingerprint biometrics.

Other standards from the NIST (USA) also apply and will be detailed in the future technical specifications of the NIDS tender document. While There are many vendors (both hardware and software) that can support these baseline requirements that are established to provide interoperability for the resulting biometric data, the compliance to standards, the performance results to the NIST tests and the track records and references of National ID cards projects shall provide direction for the selection of biometric hardware and software vendors for NIDS.

4.1.4. AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (ABIS)

The NIDS ABIS will store and manage the biometrics (fingerprints and digital photographs) associated with system enrollees. The ABIS shall apply the ICAO9303 specifications as the basis requirements for the storage of both facial and fingerprint biometrics.

A minimum of four fingerprints (two from each hand) is recommended to increase the matching accuracy when asserting uniqueness (finger print information shall include each enrolled digit and hand).

The biometrics will be captured during enrollment and used to assist in vetting (adjudication of the presented identity to assure the applicant has not previously enrolled and was issued a NIN) and subsequent identity verification. However, subject to legal regulations/requirements, biometrics will only be enrolled for applicants over the age to be determined by the NIDS Steering Committee. If NIDS enrollment occurs before that age (e.g. at birth or upon entering school) the biometrics should be added to NIDS once the specified age is reached at the appropriate renewal point.
Another biometric identifier might be used for the identification process: decision will have to be made to retain facial or iris recognition.

All biometrics shall be enrolled and stored according to the ICAO 9303 specifications. This will provide more flexibility and options for future upgrades and enable interoperability for matching with other biometrics systems (where legally permissible). The ABIS will need to provide 1-to-1 (1:1) and 1-to-Many (1: n) match capability for both fingerprint and facial biometrics.

5. SYSTEM ARCHITECTURE

The core for the NIDS framework architecture, as illustrated in 5 below, is comprised of the enrollment, vetting, card production, issuance and verification components; each with internal and/or external network connectivity.

NIDS is an integrated system that will share the same data referential across all the sites that compose the vertical integration of the workflow process.

NIDS is also a transversal integrated system that will propose and share to the other authorized stakeholders a verified and a sustainable common set of verification services for identity management.

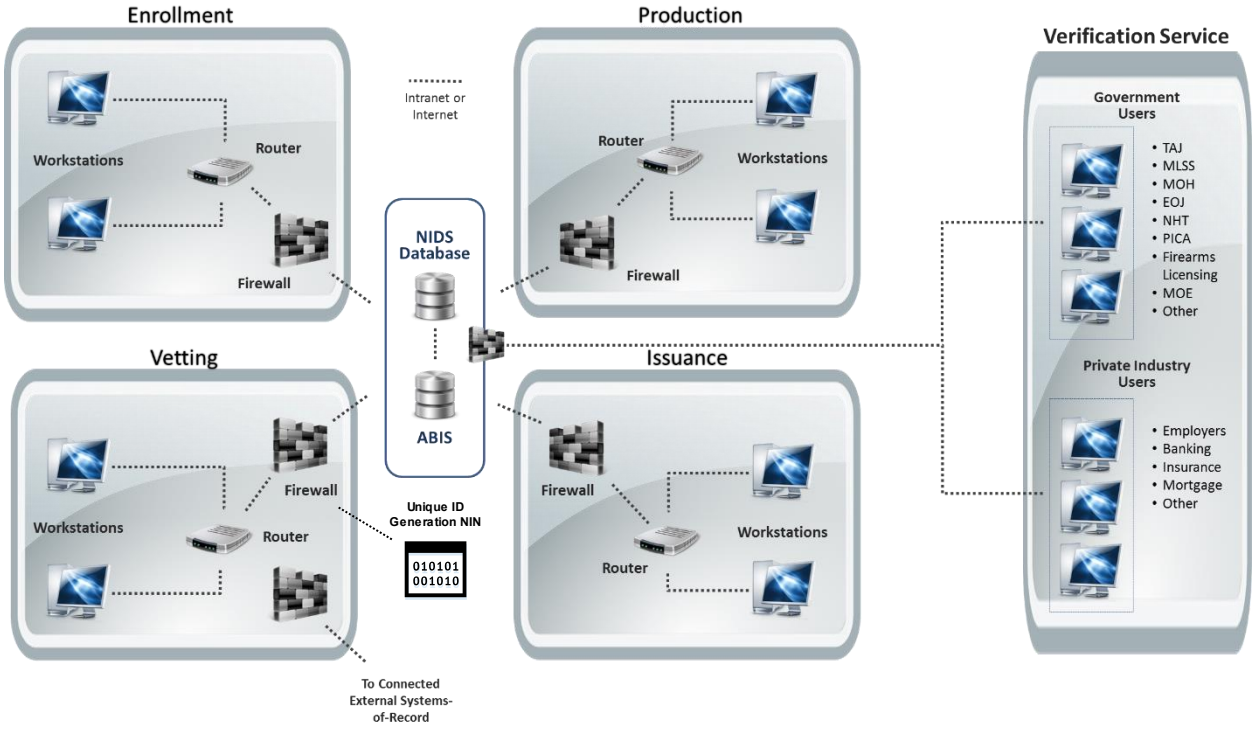

FIGURE 7: CORE NIDS FRAMEWORK ARCHITECTURE

The enrollment subsystem intakes both biographical and biometric data from applicants. It requires computer workstations, biometric readers, scanners, cameras, card readers, signature pads, receipt printers, routers and firewalls. Enrollment data is either stored and forwarded or transmitted in real time to the NIDS database and NIDS ABIS servers for further validation and vetting. It is important not to store any personally identifiable data on the local work-stations; however temporary local storage of applicant data is recommended in the case the Government Intranet network is unavailable. Regardless of the situation, the local storage of data as well as the data storage in the central NIDS system should be encrypted to protect such data to the best extent possible.

The vetting subsystem enables adjudication of enrolled applicant data. Vetting officers shall access biographical (NIDS data server) and biometric (NIDS ABIS) data and, as well, be provided interface(s) to external authoritative systems-of-record (where possible/feasible) to validate the presented information. Biometric data shall be checked to verify that a prior enrollment (even with a different name) is not already in the NIDS system. This requires computer workstations, routers and firewalls. Additional web portal and off-line enquiries shall be available to vetting officers to validate claimed identity information.

Note: *If the vendor of the system will be in charge of the software and hardware deliveries, it is important to precise here that eGov Jamaica will be responsible for the hosting of the physical architecture and the definition of the security policies that will support these central activities.*

eGov Jamaica will be also in charge of the support and the maintenance of the NIDS system.

6. SECURITY FRAMEWORK & GUIDELINES

Security Framework

The system required has two main goals:

- issue identity cards,
- provide a reference civil register database, including biometric data.

These two goals constitute a sensitive activity that engages the responsibility of the GOJ.

The integrity and reliability of the identity cards depends on security of its overall production system. To be efficient, maintainable and homogenous, large scale information system's security must be defined at top level: from organizational to technical level. This top level security is declined on system's components.

Security framework first defines requirements independent of system architecture depending on risk. This first step defines "overall security policies".

A Global Security Policy Study will be performed on the eID solution for the Government of Jamaica.

It will deliver a reference document for:

- Security integration in the IT solution
- Help in the design of user policy
- Support any future evolution of the proposed IT solution

To achieve this document, the process will be divided in 3 main steps:

- Study identified threats, risks against the IT solution and security objectives to be covered
- Meetings in order to exchange on possible security requests and potential existing problems
- Delivery of the final Global Security Policy Study.

This Study will contain chapters about:

- General Objectives
- Customer intention in terms of IT security for the deployment of the eID system in the Government of Kenya
- Limits for the risk management objectives
- Main principles, standards and legal obligations for security the GOJ in accordance with
  - local legislation
  - needs in terms of education, training and information on security
  - Service continuity management
  - Risk in case of security policy violation
- Definition of responsibility in the IT security, including incident reporting
- Reference to applicable documents

Thereafter, “Overall security policies” are declined into “Particular Security Policies” per identified subsystems and define specific security requirements.

It will generate a specific policy for enrolment workstations and will be based on the Global Security Policy Study. It will define:

- The main objectives of eID
- The access to workstations and data
- The security of the tools and communication
- Legal obligation
- Control methods (internal or external)

During the specification and development phases, data are securely stored and exchanged by integrated tools which provide integrity and confidentiality:

- Secured internal e-mail server,
- Internal content management system with security and versioning functionalities
- large data size file exchange
- Data encryption (i.e. TrueCrypt, AxCrypt).

In order to secure communications over the whole system, the following security functions are needed for the project:

- Firewall (FW),
- Intrusion Detection System (IDS),
- Virtual Private Network (VPN).

The firewall and IDS features are used in order to filter the network communications in each equipped site and in the central site.

The firewall functions are used to monitor the communications. This monitoring is used to ensure that only the communications that are compliant with the security policies are authorized. These security policies are based on:

- The different segments, i.e. Virtual Local Area Network (VLAN) and Virtual Routing and Forwarding (VRF),
- The communication from outside to inside and reciprocally.

The IDS allows inspecting the communications in order to detect anomalies in themselves. The IDS warns in case of threats such as:

- Destructive activities (Virus propagation),
- Attempt for a Denial of Service (DoS),
- Malicious interactive traffic (Trojan),
- Identity theft network (ARP spoofing, IP spoofing)
- Operation fault or application protocol (gain access and privilege escalation)

The VPN feature is used to ensure the confidentiality of communications between network sites. These functions establish an encrypted tunnel between each Registration Office and the central site.

All of these security features are based on a component of mutual security services. This component is called Unified Threat Management (UTM).

For each site that component UTM is sized according to the capabilities necessary for the treatment of potential traffic.

SECURITY GUIDELINES

All security guidelines begin with the establishment of a common set of base policies. These are foundational in setting the direction for everything that follows. These base policies should include, but not be limited to, a number of the following:

- Security Policy
- Access Control Policy
- Acceptable Use Policy
- Change Policy
- Patch/Update Policy
- Backup Policy
- Remote Access Policy

Following policy, agreed upon standards help to ensure that all stakeholders are applying the same (or stronger) practices. The standards define requirements for the use of hardware, software, technology, and security controls, thus providing a common environment for all to interact. This also promotes mutual trust by and between stakeholders.

Procedures, guidelines and best practices cover operational areas and should also include training and education. Training and education help to ensure that individuals working in security and secure environments have the latest knowledge in best practices and techniques to carry out their duties. Training and education should be continuous – not only due to turnover of employees, but to refresh the key and core concepts and elevate the awareness of the responsibility to maintain the integrity and trust of the citizens.

Compliance to policy, procedures, and guidelines is crucial as the best policies and procedures can only be effective if followed; monitoring coupled with auditing on a continual basis to help ensure compliance.

There are a number of policies which are relevant and related to the new Government of Jamaica **Protective Security Policy** which should be used as guidance for NIDS if not made mandatory.
The objectives of this new policy (in draft for discussion at this point in time) are to ensure the protection of critical assets, to include personnel, facilities, information, equipment, etc. as well as ensure business continuity.
It is recommended that the NIDS system and operations implement the Protective Security policy to guarantee the highest level of trustability which is at the core of the new identity management system

7. IDENTITY FRAMEWORK AND INTEROPERABILITY

Conformance to recognized international communication and networking standards is required across all aspects of the NIDS framework. This helps ensure interoperability and compatibility with key information systems.

Compatibility is especially important to allow the Vetting service to communicate with the issuing authorities of the baseline proof-of-identity documents (e.g. birth certificate, voter ID, driver's license, etc.) in order to facilitate fast and effective electronic adjudication of the presented documents. To that end, the identity verification service will take advantage of the existing framework developed by e GOV Jamaica.

This electronic interface is proposed to be accomplished via an Application Programming Interface (API); by conforming to standards, to be specified by the NIDS supplier. In another words, such standard API will reduce the global effort to interface other identity software and will also maximize the chance of success.

The NIN provides a common means of establishing unique identification in support of data sharing between identity systems.

Note: eGOV already has in place a service framework that facilitates the publication and administration of services. Further analysis is required to determine in which way NIRA will benefit from this framework.

8. RESOURCES REQUIRED

The identification process requires a number of roles to be covered: enrolment agent, vetting agent, etc. During the massive enrolment campaign, the number of agents will be different than the number of agents needed once most of the population is enrolled. Thus, we split our human resources required in two different scenarios:

1. Massive enrolment
2. "In Regime"

8.1. IN REGIME

The working assumptions used for the calculations are:

Parameters	
Minutes per enrolment	15
Renewal	10
Vetting	2
Quality Control	1
Issuance	2
Working hours per day	7
Working days per year	240
Jamaica total population	2,697,983.00

These parameters lead to the following production per agent/day:

Estimated production per officer/day	
Enrolment per officer/day	28
Renewal per officer/day	42
Vetting per officer/day	210

QC per officer/day	420
Issuance per officer/day	210

We have finally, the following values for new enrolments and renewal (taking into consideration an expiration of 5 years for people lower than 18 years old and 10 years for older than 18):

Estimated "In Regime" figures		
	%	Total
Renewal	15.00%	404697
Enrolment	1.80%	48564

# Enrolments per day	**# of renewal per day**	**# of enrolment officers**	**# of vetting officers**	**# of QC officers**	**# of Issuance officers**
202	**1686**	**47**	**1**	**5**	**9**

One important consideration about the enrolment agents needed is that we are assuming we can obtain a complete assignment for each agent. This is not the case since we need to distribute the agents throughout the country. Thus, the final number of enrolment agents will be in relation to the final number of sites we want to deploy in the country.

8.2. MASSIVE ENROLMENT

It was decided a massive enrolment of 3 years in which the objective is to cover 65% of the population. In this assumption, we are considering a 100% coverage of the population within 3 years since this will be the ideal situation.

	Number of applications	**Number of officers**
Year 1	899328	134
Year 2	958842	143
Year 3	1022295	152

The increase in the years 2 and 3 are related to the number of lost and stolen cards (a 6.62% was assumed, from previous experiences).