ID4D
IDENTIFICATION FOR DEVELOPMENT

ID4D Country Diagnostic: Guinea

WORLD BANK GROUP

1818 H Street, NW, Washington, D.C., 20433
Telephone: 202-473-1000; Internet: www.worldbank.org

Cover photos: Top left by Daniel Silva; top right and bottom by Dominic Chavez/World Bank.

Contents

About ID4D

The World Bank Group's Identification for Development (ID4D) initiative uses global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification systems to achieve the Sustainable Development Goals. It operates across the World Bank Group with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, and legal, among others.

The mission of ID4D is to enable all people to access services and exercise their rights, by increasing the number of people who have an official form of identification. ID4D makes this happen through its three pillars of work: thought leadership and analytics to generate evidence and fill knowledge gaps; global platforms and convening to amplify good practices, collaborate, and raise awareness; and country and regional engagement to provide financial and technical assistance for the implementation of robust, inclusive, and responsible digital identification systems that are integrated with civil registration.

The work of ID4D is made possible with support from World Bank Group, Bill & Melinda Gates Foundation, and Omidyar Network.

To find out more about ID4D, visit worldbank.org/id4d.

Acknowledgments

This report was authored in 2016 by Jean Ferry and Marc Lixi as part of the Identification for Development (ID4D) initiative, the World Bank Group's cross-sectoral effort to support progress toward identification systems using 21st century solutions.

This report benefited greatly from the inputs by Sandrine Ouensou and PNUD as well as reviews by the World Bank Group staff, including Balakrishnan Mahadevan, Samuel Lantei Mills, and Arleen Cannata Seed under the supervision of Vyjayanti Desai.

The report would not have been possible without the insights and support by:

- His Excellency Mohamed Diare, Guinean Minister of State and Minister of Economy and Finance, who authorized this study;
- His Excellency Guilavogui Oyé, Guinean Minister of State in charge of Postal Services, Telecommunications, and Information Technologies who provided us with his complete support;
- His Excellency M. Cheick Sacko, Guinean Minister of State and Minister of Justice, Garde des Sceaux who gave us full access to his Ministry departments, and underlined the essential role of identity in the justice process;
- M. Ibrahima Camara, Principal Presidential Adviser for Public and Public Partnership who introduced us to the key actors in the identity process;
- Mr. Kaba Ibrahima, National Director of Civil Registration who brought us his perfect knowledge of the National Civil Registration in GUINEE and his vision of the future;
- Dr. Kourouma Mamady, National Director of Familial Health in Health Ministry who perfectly explained the role of the Health Ministry in the birth and death notification; and
- Mr. Cellou Diallo of WARCIP GUINEE, who gave us complete logistic support and access to his extensive address book.

Abbreviations

AFIS	Automated Fingerprint Identification System
A.N.GE.IE	Agence Nationale de la Gouvernance Electronique et de l'Informatique de l'Etat *(Guinean public agency for the management of IT solutions)*
BOT	Build Operate Transfer (a type of concession used by States to fund a project or service)
CENI	National Electoral Commission
eID	Electronic ID
EU	European Union
MATD	Ministry of Territorial Administration and Decentralization
MEF	Ministry or Economy and Finance
MFPREMA	Ministry of the Public Service, State Reform and Modernization of the Administration
Morpho	French company that delivered the system for the P.E.R.L.E Project to Guinea in 2008 (formally SAGEM)
MSPC	Ministry of Security and Civil Protection
NICT	Nouvelles Technologies de l'Information et de la Communication
NIN	National Identity Number
NIR	National Identity Register (a system developed by Waymark for managing elections and producing National Identity Cards)
NSI	National Statistics Institute
P.E.R.L.E	Project for Registration and Revision of the Electoral Role in Guinea
PPP	Public Private Partnership
SAGEM	Former name of Morpho
NIN	Numéro d'Identification Natinal (Unique ID Number)
UNDP	United Nations Development Program
UNICEF	United Nations Children's Fund
WayMark	Company that implemented the National Identity System developed by Waymark in 2012

Executive summary

Having met with most of the actors in Guinea's ITC sector, we can already share some conclusions and make a number of recommendations:

- The pilot project for the establishment of a national digital identification system must be more clearly defined;
- Clarification is required regarding the status of the project signed at the end of March 2015, for the establishment of a civil registry and the production of National Identity Cards.

Notwithstanding the solution chosen by the Guinean authorities, the terms of reference must be drafted in such a way as to ensure that:

- The needs of all sectors are duly taken into account (Justice, Health, National Education, Planning, Territorial Administration, Public Security, Transport);
- The right of all to civil registration is respected (accessibility, cost of declarations);
- Resources already invested are re-utilized;
- The system to be put in place is perfectly well organized and in conformity with an existing legal framework, or one to be defined;
- The system will be interoperable;
- The system is sustainable.

H.E Mr. Diaré, Minister of Finance, has requested World Bank support for conducting a comprehensive assessment of eID initiatives, in order to avoid launching an eID project in an uncoordinated manner. Therefore, the National Digital Identification Register, hereinafter referred to as the "Project," must constitute the backbone of all services to citizens and be a flagship project in the area of civil registration.

The most difficult phase of the Project is the initial development of the register, which must be constituted while ensuring that the rights of all citizens are respected. This may only be achieved if there is full transparency at all stages of the process and if all citizens understand the issues involved.

We recommend that a Steering Committee be put in place, in order to ensure full stakeholder involvement in the Project. This will help to avoid situations such as the current one, where the MATD is not at all involved in this ambitious Project.

1. Introduction

1.1 Purpose

As part of the preliminary study on the implementation of a national digital identification system, we have conducted an analysis of the current situation, gathering information on systems already in place or in the process of implementation, as well as the needs of the various Ministries.

This report should serve as the basis for recommendations to be made for the implementation of a national digital identification system.

1.2 Scope of the document

This document is intended for all stakeholders who have participated in this study. It could be used in the event of arbitration by the Guinean authorities in relation to the development and implementation of the Project.

1.3 References

We will, for the time being, only mention the following reference documents:

- World Bank Digital Id Tool Kit—World Bank Group—June 2014
- World Bank Report—Deploying Electronic Identity (eID) in Ebola Affected Countries—A Strategic Plan for a Fast Track Approach—February 2015

1.4 Contents

This document consists of the following chapters:

- Introduction
- Responsibilities

  Responsibility for the project
- Analysis of the current situation

  Assessment of the current situation (projects under way, actors, needs)
- Conclusion

  Recommendations for developing a solution

2. Responsibility for the project

Several Ministries currently claim responsibility for oversight of the project:

- The Ministry of Post, Telecommunications and New Technologies
- The Ministry of Security and Civil Protection
- The Ministry of Territorial Administration and Decentralization
- The Ministry of the Civil Service, State Reform and Modernization of the Administration

2.1 Ministry of Post, Telecommunications and New Technologies

Given the predominance of ICTs in the Project, the Ministry of Post, Telecommunications and New Technologies (MPTNT) should play a lead role in the design and implementation of the Project. Specifically, the MPTNT should consolidate the needs and requirements of the various stakeholders (sectorial Ministries), and propose technical standards and specifications in response to the needs of the other Ministries. The MPTNT should also play a key role in the implementation process, in order to ensure that the ICT infrastructure is adequate and used appropriately for the deployment of the future eID system (the Project).

2.2 The Ministry of Security and Civil Protection (MSPC)

The Officer in charge of Information Technologies in the Ministry has indicated that the Malaysian supplier, Multimedia Glory, was awarded the contract for the Civil Registration and National Identity Card Project. This decision was taken because the MSPC was no longer in a position to provide identity cards. The Project should be up and running before the end of May 2015. The Build Operate Transfer (BOT), which will have been signed, will guarantee that the State will have turnkey ownership of the system, without the need to provide prior financing.

2.3 The Ministry of Territorial Administration and Decentralization (MATD)

The Ministry has notified Multimedia Glory that it has been awarded the contract. The National Civil Registry Director has expressed regret that he is not involved in the Project and that it does not take into account a number of requirements regarding Civil Registration and citizens' interests.

2.4 The Ministry of the Civil Service, State Reform and Modernization of the Administration (MFPREMA)

Neither the officials of the Ministry nor of its subsidiary body, The National State Agency for Electronic Governance and Information Technology (A.N.GE.IE) have been informed of the eID projects being conducted by the Ministry of Telecommunications. Neither have they been notified of the Project for Civil Registration and National Identity Cards being conducted by the Ministry of Security and Civil Protection (MSPC). The MFPREMA insists that projects of this nature may not be implemented outside of the mandate of the National State Agency for Electronic Governance and Information Technology (A.N.GE.IE), as stipulated in decree 135, which establishes the A.N.GE.IE.

2.5 The Ministry of Economy and Finance (MEF)

The Minister of State does not know whether the Multimedia Glory contract is liable to be executed. However, he advocates close collaboration with the Ministry of Security and Civil Protection and proposes that this report include all the recommendations necessary to ensure that this project will be beneficial to all.

2.6 Conclusion on responsibilities

The responsibilities of all stakeholders must be clearly defined. The Project should be led by a single entity with a Project Manager representing the interests of all the Ministries. The Government, at the request of the Prime Minister or a Ministry with a cross-cutting portfolio, should convene all parties and disclose the conclusions of this report. This could be done at a high level workshop during the month of July, once this report has been validated.

3. Assessment of the current situation

The analysis of the current situation covered all the citizen identification projects currently underway, as well as the requirements of each Ministry.

3.1 The civil servant census project

The civil servant census project was financed by the World Bank. We met with the Head of the Civil Service and the service provider to discuss this project.

The project is a good example of collaboration between project supervision and project management. Even if difficulties have arisen, the project was never stalled. The solution put in place was satisfactory, since it helped to weed out 10,000 ghost civil servants, including 1,000 with two posts. This has led to savings of 126 billion Guinean francs per year of the State budget.

The introduction of a biometric enrollment system for new civil servants, the transfer of technology, together with the fact that Inovatech Id will maintain an ongoing presence in Guinea, should guarantee the sustainability of the system.

The implementation of the time-clock system should help eliminate even more ghost civil servants. That will leave the next important undertaking of combining the Payroll and Civil Servant Registries, which is planned for September 2016. At that time, all fictitious civil servants will be definitively struck from the books, to allow for the development of a single database.

3.1.1 Points to consider

The supplier is reliable and permanently based in Guinea. The company has not confined itself to the strict letter of the contract, its experience with the CNSS allowing it to go beyond the original Terms of Reference in order to detect an even greater number of ghost civil servants. The introduction by the banks of a system of wage freezes and thaws is a good example of cooperation between Government and the Professional Banking Association.

3.2 The electoral register

3.2.1 Versions of the register

We met with the Vice-President of the National Electoral Commission (CENI), who provided a comprehensive historical background of the CENI register. There are three versions of the system, each one of which represents a revision of the electoral lists:

- The SAGEM register, 2010 revision
- The WayMark register, 2013 revision
- The Gemalto revision of 2015

3.2.2 The SAGEM system

The first biometric voter identification system was set up in 2009, with funding from United Nations Development Program (UNDP) and the European Union (EU).

The system failed, for the following reasons:

- Poor fingerprinting techniques, due to the absence of training and support for the enumerators: out of 4,398,325 persons registered, only 3,078,020 of those registrations showed usable data based on minutiae points;[1]
- Too many loopholes in the system, with little or no monitoring of data: (i) persons under the age of 18 years were included in the lists; (ii) others were registered into the system with missing data;
- Little attention paid to constituency divisions in the publication of voters' lists.

The reliability of the register was questionable and the system needs to be developed for the third time.

3.2.3 The Waymark system

The SAGEM register was used in the Waymark system. The conditions under which the contract was awarded to this company were not absolutely transparent, thus causing doubts to be raised about the quality and level of impartiality of the system and leading to eliminate double entries in the system twice:

- Once with the use of the Waymark system based on Sonda fingerprint matching technology (Sonda is a Russian company);
- On another occasion, in Belgium, with the Zetes company.

The outcome of the second attempt was no better than the first. Overall, the operation cost approximately US$ 40 million (see UNICEF[2] report). This operation should have been completed with the printing of National Identity Cards, on the basis of the electoral register. **Today, there are 5 million unused cards, as the printing system was delivered, but has so far not been used.**

3.2.4 The Gemalto system

In light of opposition to the Waymark system, a new call to tender was launched in 2015 and the contract awarded to Gemalto to carry out the following tasks, which include:

- Migration of the data within the electoral register. No new entries should be made, nor any data eliminated during this process (there are 5,206,118 registered voters in the register);
- 2400 enrollment kits;
- Pre-loading of the kits;
- Training of 5,000 kit operators and 500 supervisors;
- Data processing and de-duplication;
- Compilation of electoral lists;
- Production of polling voter cards.

1 Characteristic features of a fingerprint, used for matching purposes.
2 UNICEF Report: Towards Universal Birth Registration in Guinea (2014).

3.2.5 Use of the CENI register as a basis for the national digital identification register

The CENI does not object to the use of the electoral register as a basis for compiling the national digital identification register. On the other hand, it does not wish to have to make a fresh revision of its lists. In other words, this means that the national register must include the entire population and that Guinean citizens under the age of 18 must be registered biometrically. A law should be enacted to provide for this process, as well as for the use of the CENI and the national digital identification registers. It also means that the information on voters' place of residence and on constituency divisions will have to be included in the national digital identification register.

3.2.6 Technical features of the CENI system

In order to complete this study, the group of experts will need to meet with the CENI technical team and be provided with the data on each voter that is stored in the system: (i) demographic data; (ii) biometric data and (iii) form of minutiae points. Once this information has been provided, our teams will be better able to identify the sources of the problems and make recommendations to the Government on a roadmap for the implementation of a national eID system (the Project). This roadmap will be described and explained in the next report.

3.3 Civil registration

3.3.1 The civil registration modernization project

A complete study,[3] financed by UNICEF in November 2013, focused on birth registration. The study made a number of recommendations, including for the establishment of a digital civil registration system, or the use of a national identity register (NIR). A brainstorming workshop, entitled **"Improvement and Modernization of the System of Civil Registration in Guinea"** was held from November 25 to 29, 2013, at the Palace of the People, with participants from MATD, UNICEF and the WHO.

Following the workshop, a modernization project was developed, to take into account political and legal considerations, as well as new international standards (see the Logical Framework for the project on the Modernization of the Civil Registration system and the Establishment of Statistics in Guinea[4]).

A 2015–2016 Action Plan was drawn up by the DNEC. It includes:

- Legal aspects (Civil Registration Code);
- Organizational and institutional aspects with the roles of the main stakeholders (DNEC, Ministries of Justice, Health, Foreign Affairs) in civil registration;
- Systems of interoperability between the various actors (Secured identity documents—MSPC, Police records—Ministry of Justice, Elections—CENI, Social Protection, Demographics—Ministry of Planning, Driving Licenses—Ministry of Transport).

The sum of one million euros has been unblocked by the European Union for financing the Action Plan. Unfortunately, the National Civil Registration Directorate (DNEC) is not in any way involved in the MSCPC

3 UNICEF Report Towards Universal Birth Registration in Guinea (2014).
4 Project on the Improvement of Civil Registration in Guinea.

project currently under way and which also pertains to the management of National Identity Cards and Civil Registration. This is not an ideal situation, as key stakeholders have not been included in the project. There is therefore a substantial risk that the project will not be effective, mainly due to a lack of involvement by relevant stakeholders and the absence of proper coordination.

3.3.2 Civil registration actors

The main actors are:

- Elected representatives from the communes;
- The Civil Registration Directorate, which has an agent in each commune to manage the registers and assist the commune-level representatives;
- The Ministry of Justice, which has several roles:
  - To emit judgments modifying civil status (divorce, adoption, rectifying of names or months and days of birth);
  - To produce supplementary judgments to replace lost birth certificates that must be entered into the registry of the commune where the person was born;
  - Numbering and initialing of registers before their distribution to commune-level civil registration offices, to ensure the authenticity of the documents;
  - Archiving and monitoring of the legal aspect of civil registration declarations;
- Guinean Embassies abroad, which perform the offices of civil registration for Guinean citizens;
- The Ministry of Planning, which should use the 4th section of the civil registration declaration for the demographic records. There are efforts under way to ensure that this 4th section is correctly used;
- The Ministry of Health, which registers births in urban areas.

3.3.3 Civil registration declarations in urban areas

Declarations in the urban areas follow the following procedure:

- Health officials record the birth or death in a ledger with counterfoils, comprising:
  - One copy for the head of the family;
  - One copy to be used for health statistics;
  - The counterfoil is kept by the health personnel.
- Declaration by the head of the family submitted to the official in charge of civil registration (civil registration officer) at the local municipality. The declaration is entered into the register, which is a booklet containing 4 leaflets:
  - One leaflet to be retained by the declarant for obtaining a birth certificate;
  - One leaflet for the clerk of the court of first instance of the commune;
  - One leaflet for the NSI (National Statistics Institute);
  - The counterfoil is kept at the commune-level civil registration office.

3.3.4 Civil registration declarations in rural areas

The procedure followed is similar to that in the urban areas, except that the declaration by the health officer is replaced by an entry in the village registry kept by the chief of the village:

- The chief enters the birth in the village registry;
- The registration is done by the civil registration officer resident in the commune, on the basis of the entry in the village registry:
  - Either by the officer making the journey to the village, carrying the civil registry;
  - Or by the village chief who journeys to the commune for the registration to be made.

Overall, this procedure is hampered by the lack of logistics and the limited number of trips made by the civil registration officer. Furthermore, there have been insufficient information campaigns on the importance of making civil registration declarations. Wide disparities exist between the rural areas and the city of Conakry (where more than 80 percent of all civil registration declarations are made). In some rural communes, the rate of declarations is less than 40 percent.

3.3.5 Civil registries

Numbered and initialed blank registries are sent to the communes. There are four types of registries:

- The registry of births;
- The marriage registry;
- The registry of deaths;
- The transcription registry (for changes following a judgment).

Apart from the great disparities between the rural sector and the city of Conakry, there are other problems worth noting:

- The lack of records for the period prior to the introduction of registries;
- Registries destroyed during the events of 2007;
- Unacceptable methods of storing and archiving registries;
- Leaflets that should be kept by the clerk of courts are not correctly filed;
- Leaflets that should be used by the NSI have not been used.

In general, it would be risky to depend solely on these documents for the recovery or reconstitution of a national civil registry. Only a general administrative census or the introduction of a system of citizen declarations could allow for the efficient and reliable reconstitution of a civil registry.

3.3.6 Supplementary judgments

The supplementary judgment is a legal provision, which states that a person's civil status may be reestablished once the original documents have been lost. Supplementary judgments are issued by the courts of first instance, through the submission of:

- A handwritten application;
- The testimony of two witnesses, with their identity cards;
- A residence certificate.

At the court of first instance visited by the team of experts, one judge is employed full time for this exercise. There are roughly 50 to 60 judgments each day and the procedure often consists of a simple administrative procedure, without the need for witnesses. The judgments are entered in a register and filed. We were unable to gain access to the archives. However, the archives in the possession of the clerk did not seem to conform to international standards observed in other countries. Files were stored in unsecured, unlit areas, with restricted space, while storage and filing methods presented real drawbacks. It was impossible to store items of proof in any logical order.

Following the judgment, the applicant should travel to the civil registration office located in his place of birth, so that the judgment may be recorded and a certified copy of the extract of the Civil Registration may be given to the applicant. Often, this formality is not observed. The supplementary judgment is often used as an easy alternative to the application for a birth certificate in one's commune of birth.

It is easy to obtain or to make a counterfeit copy of a supplementary judgment. As a result many official documents have been issued on the basis of false declarations. Some consulates refuse to accept them for visa applications. What are the options remaining for citizens of good faith, who have lost their documents and for those who are unable to obtain a copy of their birth certificate in the commune of their birth, because the civil registry has been destroyed?

3.3.7 Reconstitution of the National Civil Registry

In order to establish a Digitalized National Identification system, one cannot rely on existing civil registries or the copies stored in the registries of the courts of first instance. The recordkeeping methods are sloppy and too many documents have been either lost or destroyed. Moreover, the new digital system will need to correct existing disparities between the urban and rural communes by making access to the system available to all. Two possible solutions may be envisaged:

- A general administrative census;
- A progressive reconstitution, as the need arises.

3.3.7.1 The establishment of a digital system based on a general administrative census

The DNEC favors a general administrative census. Such a census must avoid the pitfalls of the national population census, which has proven to be very costly, while yielding disappointing results. We recommend that the administrative census be modeled off of the last census conducted by the CENI, for which specialized companies were hired. The following are the main problems associated with this option:

- Could the CENI Kits be used for conducting the census?
- Should one and could one preload the census kits with CENI files?
- What are the controls to be carried out?
- Can the National Identity Number (NIN) be issued immediately at the local level, on the basis of the information provided?
- Will the persons to be enumerated have the necessary information to allow for calculation of the NIN?
- How can one guard against enumerating people twice?
- Who should make the declaration for a juvenile (one registered parent, both registered parents, registered legal guardian)?
- What is the procedure for minors who do not live with their legal guardians?
- What is the procedure for registering juveniles and how can their identity be checked?
- What documents should be presented (National Identity Card, polling card, birth certificate)?

- What are the options for persons who are unable to provide the required documentation?
- Can the system of supplementary judgments be avoided?
- Should a digital copy of the relevant supporting document be kept in the system?

We cannot provide responses to all of these questions in this preliminary study, but they will need to be answered if the option of a general administrative census is chosen. A rapid calculation based on a time period of 15 minutes for each person enumerated for 10,000,000 persons gives us a figure of 4,200 census kits to carry out the process in a 6-month period.

3.3.7.2 Progressive implementation based on declarations

This is probably the option chosen by the MSPC project (see below). The following are the general principles of the system:

- All persons must first be registered in the system before a civil registration entry can be made;
- At the time of the first registration, an NIN is assigned to the declarant (a personal identity number, based on the individual's civil registration data);
- The NIN, as well as the biometric data of the declarant is checked each time a declaration is made.

This is a workable system, which is easier to implement than the option of the general administrative census. The disadvantage of the system is that it will take several years to cover the entire population. However, a number of actions may be undertaken to speed up the process, notably:

- Making it obligatory to use a new ID card (this does not affect persons under 18);
- Making it obligatory to have an NIN to enjoy social benefits;
- Making it obligatory to have an NIN for school enrollment.

The immediate result of these obligations is that the new system will be accessible to all.

3.3.7.3 Persons without identity documentation

There are persons with no documentation and for whom the civil registry is inaccessible, or no longer accessible. One may imagine that persons entered in the CENI registry may be issued with ID documentation. How can the NIN be granted in the specific case of a person without identity documentation? What solutions can be found for the others? What can be done for those who have never been registered in the civil registry (approximately 20 percent in urban areas, 50 percent in rural areas)? As we have seen, the system of supplementary judgments cannot solve the problem and, indeed, has even led to fraud.

3.4 The Ministry of Justice

The Ministry of Justice is a major actor in the implementation of a system of Civil Registration. It is also an important client, since all legal proceedings must be based on Civil Registration. The Ministry of Justice is also responsible for issuing criminal records, which are delivered by the court of first instance located in an individual's place of birth. As there is no centralization of information, information concerning an individual's criminal activities are not always transmitted to the clerk of the court of first instance. It is therefore quite possible for a criminal to obtain a clean criminal record.

Applications based on the National Digital Identification Registry will greatly facilitate the following activities:

- Keep track of criminal records;
- Manage registers;
- Manage files;
- Carry out digital filing;
- Manage records of accused and convicted persons.

3.5 The Ministry of Transport

The Ministry of Transport, through its National Land Transport Directorate, is conducting two projects that pertain to personal identification, and for which the National Digital Identification System could be used. They are: (i) the car registration document project; and (ii) the driving license project.

These projects are currently managed by the Ministry of Finance, as they involve the use of fiduciary documents.[5]

3.5.1 The car registration documents

The eID project only concerns the aspect of the car registration documents pertaining to private owners.

The National Land Transport Directorate is of the view that it has not been sufficiently involved in this project, which is currently under way and managed by the Treasury.

The only role of the Directorate is that of delivering the car registration document when the vehicle is put into service. Payments for car registration documents are made at the tax collection office of the Treasury, located on the premises of the Ministry of Transport.

The declarations for change of ownership are made in the offices of the Judicial Police, located in an authorized Police Station.

Personal identification is not an essential requirement for the car registration document project, but should make it easier for authenticating documents.

3.5.2 The driving license project

This project was poorly conceived and implemented, with the result that project funds have not been put to optimal use.

In 2009, following a call to tender, a Belgian company, SEMLEC, was granted a contract to develop and deliver a management application for driving licenses and car registration documents. The material was delivered in 2010, together with the secured documents, and the supplier was paid. However, it was never made operational, due to the lack of premises for housing the system. It seems that the investment has, unfortunately, been lost. It is important to learn the lessons from this failure in order to avoid the same pitfalls in the implementation of the National Electronic ID (eID) project.

5 Driving licenses and gray cards, like the vignette, or road-use sticker, are fiduciary documents.

3.6 Projects of the Ministry of Security and Civil Protection

The following MSPC projects are now under way:

- Passport, visa and Residency Permit Project—only the passport application is operational;
- Civil Registration and National Identity Cards Project—in its initial phase.

There are other MSPC projects in the pipeline, which are in the Ministry Information Technology Master Plan:

- Identification of criminals;
- Identification for security guards;
- Firearm licenses;
- Police cards.

These are all based on the Civil Registration/National Identity Card Project, and will only be implemented once the latter has become operational.

3.7 The MSPC Civil Registration and National Identity Card project

3.7.1 Status of the project

In 2010, the Malaysian Company—Multimedia Glory, submitted a proposal for the implementation of a Civil Registration system and the production of National Identity Cards. The project was put on hold but was recently reactivated to resolve the problem of the depleted stock of National Identity Cards. The team of experts received confirmation of this project in a note dated March 2015 and signed by His Excellency General Bouréma Condé, Minister of Territorial Administration and Decentralization.

However, the World Bank team was not granted access to the agreement. The only information made available was provided by Commissioner Diara, IT Manager at the MSPC and Project Leader responsible for implementing the system. The only available document pertains to the technical specifications of the Identity Cards. The team was given no other documentation concerning the project: terms of reference, the agreement signed in 2010, the implementation plan, or the specifications of the system to be developed.

3.7.2 Organization of the project

Commissioner Diara, IT Manager at the Ministry of Security and Civil Protection, is the project leader. Implementation should be gradual, beginning with the communes of Conakry. Data from existing registers will not be used, neither are there plans for conducting a biometric census. A technical note has been developed, but was not disclosed, as it is currently being validated.

3.7.3 Distribution of roles

Multimedia Glory is responsible for installing the infrastructure, the system, the system support, maintenance and logistics. The system will be entirely managed by the officers of the MSPC. A program of technology

transfer is being envisaged. The staff of the Ministry will administer the system and manage applications for the printing of National Identity Cards.

The initial enrollment will be carried out by civil registration personnel, and a National Identity Number (NIN) assigned. It will guarantee the citizen's identity and will be used to ensure that authentic documents are not issued on the strength of false declarations. For all declarations pertaining to civil registration and all legal documents issued on the basis of civil registration declarations, the NIN will be required. Payment for the documents and certificates will be made through a bank with branches in all towns throughout the country. The team received no information on planned tariffs, nor the way in which BOT revenues will be managed.

There was no information forthcoming on the way documents and ID cards will be managed. In order to block the use of falsified documents, all documents must be identified and their location traced from the moment they are received to the time they are delivered to the beneficiary.

3.7.4 Implementation planning

It appears that the material (22 servers) is currently being delivered and that the project should be operational within the three months following delivery. Implementation will be gradual and will begin in the region of Conakry, including Fourekaria and Doubreka. The notification makes reference to "phase 1" of the project. Does the contract cover the entire national territory of Guinea? And what is the timeline for the project? There has been no question of recovery or use of existing systems, nor of the phase at which the registry will be constituted.

3.7.5 General architecture

The central site is located at the MSPC, with other planned decentralized sites for enrollment. Communication will be effected with the use of e-Gov infrastructure. Client-Server applications will be used for enrollment. It is expected that all information circulated on the network will be encrypted, using an asymmetrical cryptographic system with a certificate server. The team has not been notified of any details concerning the architecture, nor has it received information on the biometric identification technology to be used. It is therefore to be hoped that the supplier will provide a document detailing the general architecture, with information on the following aspects:

- Infrastructure to be put in place;
- Use of servers;
- Operating system;
- Existing SGBD and basic blueprint;
- System protection (fire-wall, antivirus . . . etc.);
- Security system;
- Backup system;
- Business Continuity (this is indispensable for a national system—the loss of the Civil Registration registers was a disaster, the loss of the National Digital Identification system would be an even greater catastrophe);
- Access to the system and management of certificates;
- Interface and availability of information;
- Functions:
  - Civil registration declarations;
  - Applications for identity cards and civil status certificates;

- Management of secured documents (NIC, certificates);
- Biometric method used (fingerprinting, with the number of fingers, biometric portrait, etc.).

3.7.6 Technical features of the system

3.7.6.1 Capacity of the system

Details regarding the capacity of the system have not been provided to the team of experts:

- Number of citizens and volume of associated data (demographic data, biometric data);
- Number of documents required, according to the type of document;
- Flow of operations, by type and place of procedure.

3.7.6.2 Performance of the system

There was no information on biometric matching times or their level of precision (FAR and FRR), nor whether a biometric portrait would be used if fingerprints are unusable or unavailable. The name of the biometric technology provider was not given to the expert team.

3.7.6.3 System specifications

The team was not granted access to information on system specifications.

3.7.6.4 Biometric cards

Smart cards have 80k of memory space with photo, civil registration data, place of residence and printed signature, data encoded and encrypted on the card (biometric data and civil registration data). The cards are made of polycarbonate with contact (ECOWAS requirement), with many security features. The cards will be printed with a laser printer. Due to the technology used in their manufacture, these cards will be difficult to counterfeit. Nevertheless, we recommend that a factory number be printed on the card and saved on the chip.

3.7.6.5 The enrollment station

There will be 150 enrollment kits in a case that includes:

- One laptop computer (able to operate for up to 8 hours on battery power);
- One A4 scanner for scanning application documents;
- One fingerprint sensor, able to capture simultaneously the four fingers of each hand (4:4:2)—it is important that the sensor be IQS-compliant.

The case will include a high definition digital camera for the capture of facial images, per ICAO standards. It is surprising that a smart card reader has not been included, as this would make it possible to validate the delivered documents on the spot.

3.7.7 Recommendations for ensuring the success of the project

3.7.7.1 Organization

The first priority is to designate a steering organization that will include all the Ministries that have a role to play in the implementation and use of the system. This should do away with the prevailing ambiguity (regarding respective roles). This body should not be an impediment to progress, but rather act to overcome obstacles, so that the project may go forward.

3.7.7.2 Transparency

The decision to implement the project should be formalized. It is not an MSPC project, but rather a project of national interest. There can therefore be no competing project. All Ministries must collaborate and the project must be completely transparent with respect to:

- The objectives;
- Conditions of procurement contracts;
- The cost to citizens (cost of declarations, certificates and documents);
- Implementation planning.

If the conditions listed above are not observed, communication with regard to the expected outcomes of the project will be unsatisfactory, with the consequence of a poor ownership of the system and the disengagement or complete lack of involvement on the part of the main actors.

3.7.7.3 Citizen information and training

It is vitally important that citizens receive very clear updates on the project. Press campaigns will need to be organized. Operation statistics should be published, so that targeted campaigns may be carried out to correct any distortions or failure to make declarations.

3.7.7.4 Dealing with fraud

It is obvious that the system will not completely do away with fraud or the perpetrators of fraud. Each individual case of fraud must be analyzed to ascertain how the fraud was committed and corrective measures must be put in place.

3.7.7.5 Obligation to make a declaration

Some measures may be undertaken to speed up the process:

- Making it obligatory to use a new identity card (this does not apply to persons under 18);
- Making it obligatory to have an NIN in order to access social benefits;
- Making it obligatory to have an NIN for school enrollment.

These obligations mean that the new system will be accessible to all; all citizens must be able to be register whatever their current situation. However, the Civil Code and the Children's Code will need to be modified.

3.7.7.6 Specifications

In the absence of terms of reference to be studied, the project team recommends that specifications cover the following aspects:

- Infrastructure to be put in place or renewed for the central system and the local centers (buildings, network, servers);
- Methodology;
- Initialization of the system on the basis of existing data;
- Functionalities and their distribution;
- Interoperability;
- Central system; basic size, performance of biometric matchers, availability, safeguards, and outsourcing of safeguards;
- Backup systems; location and continuity service;
- Location of facilities (urban and rural communes);
- Equipment for producing secured documents performance, printing format, encoding of chips, secured printing;
- Secured documents to be produced (birth certificates, residence documents, Id cards if these are included in the project): pre-printed number, security features, printed data, biometric data;
- Management of secured documents;
- Type of equipment (fixed/mobile);
- Support staff;
- Technology transfer;
- Maintenance and support;
- Maintenance of accessory equipment;
- Maintenance of the premises;
- Number of declarations required for each type of formality (birth declarations must be free of cost)—overall daily flow, as well as daily numbers at each location;
- Expected number of applications, by type;
- Method of remuneration of the BOT.

All of these aspects must be clearly specified before the launch of the project.

3.7.7.7 Implementation

The implementation plan must also be perfectly clear and include:

- Site preparation (a prerequisite for installation of the system), which must be validated;
- Actions to be undertaken for preparing the system, with validation of the specifications, which must include:
  - Processing of declarations;
  - Processing of applications;
  - Production of documents;
  - Management of documents;

    - Administration;
    - Production statistics;
    - Financial statistics;
    - Interoperability of the system;
- Deployment of the central site, with operational and technical validation:
    - Transfer of technology;
    - Validation of installed equipment;
- Deployment of decentralized or mobile sites:
    - Systems installation;
    - Transfer of technology;
    - Validation of installed equipment;
- Support and maintenance during the life cycle of the system:
    - Validation of the support and maintenance plan;
    - Delivery of documents and materials;
    - Monitoring of dysfunctions and corrective action;
    - Monthly support and maintenance report;
    - Managing changes;
- Planning with deadlines;
- Identified risks.

3.7.7.8 Identified risks

Our team identified the following risks:

- The project does not have the support of all actors involved:

  The establishment of a steering committee should minimize this risk;
- The existing needs have not been properly analyzed and essential factors have not been taken into consideration:
    - Use of existing data or equipment;
    - System initialization;
    - Legal and organizational considerations;
    - Interoperability;

  The development of clear specifications to take account of all of these elements should eliminate these risks.
- The project is being conducted in isolation from other improvement projects underway:

  It is the task of the steering mechanism to correct this risk;
- The project is not clearly understood by the public:

  A public information policy should be implemented;
- The right of all citizens to an identity is not respected:

  The service should be made available to all and accessibility to the system guaranteed by means of a number of measures to be taken throughout the national territory;

- The cost of the service is incompatible with the rights of the citizens:

  The cost of the service should be in keeping with the economic and social reality and should not be a disincentive to making civil registration declarations;
- Civil registration staff are not properly trained:

  A training plan for officers should be implemented; the training plan should not be limited to the launching of the system but should form part of the ongoing training curriculum;
- The provider does not deliver the service as required:
  - The terms of reference should include all the services to be provided;
  - The service outputs should be audited on a regular basis by a third party (financial and technical audits);
  - The service provider should have a local representative to provide support and serve as an interface with the administration;
- The provider fails to respect the confidentiality of data (heightened risk associated with foreign service providers):

  The contract should be very clear on this point and should specify the penalties for failing to comply with the confidentiality clause; the existence of a local organization that can be held directly responsible for any leaks should attenuate this risk;
- There are glitches in the system:

  The service provider should iron out any glitches within a reasonable period of time; the timeframe can be established in a maintenance plan; penalties should be applied if the number of defects is unacceptably high;
- The system is old and should be maintained or replaced:

  Support and maintenance clauses should be included in the contract and should be applicable for the entire duration of the project, with provisions for penalties in the event of noncompliance;

  System updates should be gratis and should be included in the contract;
- The Administration is held hostage by the failure of the provider to make available all the information needed by the staff of the administration to take ownership of the system:

  The data structure should be known and the tools to manage and export the data should be provided and imparted to staff through training;
- The system does not eliminate the risks of false declarations:

  All instances of fraud detected should be evaluated and corrective measures instituted;
- System change is necessary:

  System change should be possible; the implementation of such changes should be examined on a case by case basis, taking account of the financial implications; provisions relating to system changes should be set out in the Project Plan and Maintenance Plan;
- The system is accidentally destroyed:

  A service continuity plan should be prepared and tested regularly.

3.8 The MSPC passport, visa and residence card project

3.8.1 Project description

This is a MSPC project for the implementation of a biometric system to manage passports, visas and residence cards. It has been financed by a BOT arrangement with the Malaysian company IRIS following a closed tender published in May 2013 and awarded to IRIS in November 2013.

This BOT concession includes:

- The installation of infrastructure, including the building of a central site and a backup site;
- The installation of seven regional sites with connection to the central site for the biometric enrollment of the applicants;
- The equipment of the border entry points with biometric control;
- The equipment of the main diplomatic representation for the visa management and production;
- The setting up of a centralized system to manage the demand for passports, residence permits and the production of forgery-proof documents:

  Data base management system,

  Application server,

  Automated Fingerprint Identification System (AFIS) to identify the applicants,

  Communication server,

  Passport production system,

  Residence card production system;
- The supplying of 14 decentralized enrollment systems and 6 mobile enrollment systems;
- The production of 900,000 passports in 10 years;
- The support and maintenance of system and equipment for the all duration of the contract;
- The supply of material and blank documents for the whole duration of the contract.

No general planning was given for the project.

3.8.1.1 The workflow in place for the handling of passports

It includes:

- Payment of fees (500,000 Guinean francs paid into a bank, with a numbered receipt);
- Verification of the identity of the person and authenticity of the documents produced (an essential step designed to detect scammers);
- Biometric enrollment;
- Scan of supporting documents;

- Matching;[6]
- Verification;
- Production of passports;
- Delivery.

3.8.2 Review of activities

Conakry is the only functioning center for processing passport applications that has been implemented. In almost one year, the system was able to generate a turnover of more than 36 billion Guinean Francs. Over the same period, the manual system generated a turnover of 3 billion Guinean francs. The breakdown of the turnover among the concessionaire, the State and the Project was not provided to the team.

The Guinean passport is ranked 42 in the "Power Rank," right behind the South African passport. The number of passports produced per day is classified information and may not be divulged. The waiting period for the delivery of a passport is three to four days. A report on the operation of the system is in the process of being validated by the competent authorities. The team hopes to be in a position to study the conclusions of the report, in order to prepare a road map that takes account of past and present experiences.

The registration kits for decentralized applications have been tested but have not yet been rolled out.

The Visa Residence Permit systems are also not yet up and running. Visa payment on arrival has been planned, the premises have been identified and allocated at the airport, but the system is still not yet operational.

The company that was awarded the BOT concession has not fulfilled its obligations. An amendment to fix this is currently being negotiated.

3.9 The Ministry of Planning

The Planning Ministry has carried out two functions that have an impact on the National Digital Identification Register:

- Codification;
- Demographic statistics.

3.9.1 Codification

The National Digital Identification System should be based on the classification provided by the NSI (National Statistics Institute). One problem that the NSI faces is how to match the administrative divisions handled by the MATD with the codification types of the NSI. There are two divisions:

- The administrative divisions (deconcentration): prefecture, sub-prefecture, district and sector;
- The political division (decentralization): commune (rural/urban), borough, sector.

The eID Project must take into account the codification types and be able to deal with changes. Any changes to the codification types must take into account the potential impact on the system in place.

---

6 "Matching" makes it possible to automatically compare biometric data by using the features of the data. There are two types of matching: 1:1 (authentication), and 1:n (identification). In modern, high-performance systems, 1:n matching can take just a few seconds for a database with several million persons.

3.9.2 Demographic statistics

The Ministry of Planning should have access to the registry of births, so that it can compile demographic statistics. This has not been the case for many years. The Ministry was therefore obliged to conduct a General Population Census in 2014.

In this regard, the National Statistics Institute (NSI), which was responsible for the census, ensured full transparency by placing on their website all the documents related to the census. This was an excellent initiative, which the team advises should be used in implementing a National Digital Identification System (The Project). The preliminary results have been posted on the NSI website.

The existence of a National Digital Identification Register should provide immediate access to precise demographic data, the validity of which would not be in dispute. This would require the file to be as detailed as possible in the breakdown of information by sector and for changes of residence to be handled by the system. Failing this, available statistics will be confined to place of birth, marriage or death.

3.10 The Ministry of Health

The Ministry of Health has an active role as the institution whose staff members are responsible for the registration of births and deaths and for the issue of a certificate that must be presented when making a declaration to the registry office. It is essential that they play an active part in the registration of births and deaths. It stands to reason that a statistical system that is predicated on a National Identity Number (NIN) should provide access to sound statistics on births and the causes of death.

Health personnel cannot take the place of parents for the purposes of declarations of birth. Nevertheless, one option could be to have the health personnel issue a pre-declaration, which could then be used by the parents as the basis for their declaration (date, time, gender). Consideration could also be given to enabling health personnel to issue death declarations, provided that the following questions are adequately addressed:

- Can health personnel register the death directly by using the NIN?
- Should the family confirm the registration?
- How can errors be avoided?

All these elements should be taken into account in the rollout of the National Digital Identification System.

3.11 The Ministry of Social Action and Advancement of Women and Children

We have met with the manager of the Social Safety Nets Program. This program has encountered problems in relation to the identification of persons in its two projects:

- Highly labor intensive activities (HIMO);
- Conditional Monetary Transfer (TMC).

Applications to manage these projects cannot be integrated into the eID Project. On the other hand, the establishment of a National Digital Identification System would help to confirm the identity of beneficiaries and their children. These projects should rely on the data contained in the Civil Registry declarations and make aid disbursements conditional on the authoritative identification of beneficiaries.

3.12 The Ministries of National Education

These ministries may have two roles:

- The role of trainer;
- The role of user.

3.12.1 The role of trainer

The ministry could contribute to the effective deployment of the system by:

- Raising awareness among pupils at an early age of the benefits and advantages of Civil Registry declarations;
- Strengthening information campaigns on the subject;
- Requesting parents to present a birth certificate when registering their children at school.

3.12.2 The role of user

The proper identification of students is essential for the purpose of examinations. A National Digital ID number and a digital identity would be a cardinal asset to combat exam fraud.

3.13 Local operators

We conducted this study on local operators on the understanding that the implementation of the Civil Registry Project and the National Identity Card Project had not commenced. We did so because, in our opinion, the system must be able to rely on local experience and expertise to be effectively implemented and maintained. Multimedia Glory was not represented in Guinea and we were therefore not able to meet them.

The team made contact with:

- Sabari Technology, provider of Network Solutions, Telecom IT and Electoral Assistance Support;
- Inovatech Id, Smart Card specialists and associated solutions;
- ETI provider of solution Multibio product, including Civil Registry management.

The team was not able to make contact with:

- Multimedia Glory, provider of Civil registry files;
- Gemalto, supplier of the CENI register (interviews with the systems manager of CENI were delayed, owing to the death of Mr. Yaya Kan).

3.13.1 Sabari technology

Sabari Technology has participated in all the elections between 1992 and 2013, as well as the general census and the revisions of the voting register.

In 2013, Sabari Technology revised the voting register:

- The company helped to customize the application process;
- They put together and preloaded 2,400 kits (uploading with photographs). Contrary to their recommendation, the complete list was not uploaded to the kits. This resulted in poor management of the changes of residence and accounted for the high number of duplications;

- They trained 247 supervisors, 200 trainers and 5,200 operators;
- They oversaw the logistics of ballot counting (distribution of kits and dispatch of operators, recovery of data);
- They managed the task of data de-duplication (800,000 duplications discovered);
- They published the lists (alphanumeric data and portraits);
- They printed polling cards.

3.13.2 Inovatech ID

Since 2009, Inovatech ID has been active in Guinea and on a regular basis. The company has:

- Set up the biometric file for persons insured by CNSS and produced the relevant biometric cards;
- Conducted a census of civil servants in Guinea: delivery of the system, census, biometric registration, de-duplication, file clearance, biometric point system, production of cards;
- They installed a biometric access system for restricted areas at Conakry Airport;
- They set up a biometric access system for restricted areas at the Autonomous Port of Conakry;
- They put in place a GED for paperless management and storage of land certificates for the Land Conservation Office;
- They established a staff identification system for the National Agency for Mining Infrastructure Management;
- They trained census workers for the revision of electoral lists: 500 supervisors, 5,000 census takers and 3 engineers for technical support;
- They developed a biometric card for electronic payments;
- They developed a civil registry application.

3.13.3 ETI

ETI is a provider of all kinds of solution:

- Telecom and access provider, based on its metropolitan fiber optic network and connection to the ACE project;
- Delivery of IT infrastructure;
- Delivery of complete IT solutions;
- Biometrics, through its Multibio product.

ETI's experience in the management of personal data files dates back to 1987 (civil servant survey, survey of staff members of the Ministries of National Education and Agriculture). From the end of the 1980s–beginning of the 1990s, ETI began to manage payrolls, as well as Civil Service and military personnel. At the beginning of the 1990s, the company proposed that a civil registry could be established on the basis of a centralized system. In 1993, ETI was selected together with SINORG (Deposits and Consignments Fund) to set up a civil registry in Guinea, on the basis of a centralized system. The contract was never realized.

At the beginning of the 2000s, in partnership with the City Hall Administration of Paris (AIMF), ETI submitted a proposal to manage the civil registry of the Governorate in Conakry. The system was delivered but not correctly maintained or used.

In the 2000s, the company developed numerous systems with the following administrations:

- The Civil Service;
- Ministry of Defense;
- Civil servants' payroll;
- Expenditure chains;
- Taxes.

In 2011, following its experience with international biometric solution providers, and in order to control the local market, ETI decided to develop its own product—the Multibio—with the following characteristics:

- System based on one or more types of biometrics (fingerprints, facial or iris recognition);
- System that can cover between several hundred and ten million people, based on Neurotechnology software;
- System that includes the production of secured biometric documents, passports or cards (2D barcode, smart card with or without contact);
- Complete management of documents;
- Management of persons;
- Handling of all civil registry-related applications.

3.14 Private sector clients

3.14.1 Banks

The team met with the president of the Professional Banking Association. The banks do not experience a real problem with the identification of their clients. Only 6 percent of Guineans are bankable and all banking operations are monitored with the use of identity documents.

3.14.2 Insurance companies

The mutual health insurance companies have a problem with personal identification. A secured biometric card would help them to better manage the health expenditure of their clients.

3.15 Donors

A meeting with the donors mentioned below should be organized, as they are either stakeholders in eID-related projects currently under way, or have funded other projects that are linked with the National Digital Identification Project. The donors are:

- The European Union
- World Bank
- UNDP
- ADB
- UNFPA
- UNICEF

Projects that receive international financing have a better chance of success than those whose base funding is from national sources:

- Funded projects are more firmly entrenched;
- The ongoing monitoring of the project is carried out by the donor;
- Funding is based on results.

The European Union conducts numerous aid projects that are directly related to the eID, with the following bodies:

- National police;
- The justice sector;
- Ministry of Territorial Management and Decentralization;
- The Civil Service.

The European Union was unaware of the Civil Registry and National Identity Card project managed by the MSPC and initiated by the MATD. The local project leader considers that EU financing as part of a BOT contract is out of the question. On the other hand, it is felt that there should be coordination between EU-led projects and this one. Specifically, funding had been planned for a pilot project in the forested region of the country, the aim of which was to increase the effective use of existing resources through the training of civil registration officers. If this project is confirmed, it should be carried out in coordination with the Civil Registry project.

4. Legal and regulatory aspects

The Civil Registry is governed by the Civil Code and the Children's Code, as was exhaustively analyzed in the UNICEF document on the registration of births and deaths.

The conduct of electoral censuses is governed by the Electoral Code.

The implementation of biometric registration does not pose any legal problem—there is no Law on Data Protection and Freedom of Information in Guinea.

On the other hand, the implementation of a centralized system for the management of the civil registry would require a change in the law:

- Location of registers and documents
- Use of an electronic register and issuance of certificates
- The responsibility of each actor must be clearly stipulated
  - Civil registration officer
  - Civil Service officer
  - Health workers
  - Justice sector
  - National Statistics Institute
- Interoperability
- Use of supplementary judgments and implementation of a strict regulatory framework, in respect of the following cases:
  - Civil registers have been lost and it is no longer possible to deliver certified copies (a very common occurrence);
  - A citizen's birth was not registered (less than 50 percent of all births in rural areas are registered).

In addition, a well-conceived eID system should facilitate the automatic updating of voters' lists and avoid costly revision exercises. Polling cards could be replaced by a National Identity Card. A revision of the electoral code would therefore be required.

5. Conclusion

The implementation of a National Digital Identification System is not simply a technical matter of providing the means of personal identification. Neither can it be based merely on the technical specifications of a service provider.

Consideration must be given to the legal, political, social and organizational aspects. For any solution to be envisaged there must first be a legal and institutional framework and a clear distribution of roles and responsibilities. Who will be the project leader? Who will be the project manager? How can the project be integrated into all of the reforms under way in the Guinean Administration?

The observance of the basic right of all Guinean citizens to an identity is a necessity. The National Digital Identification System should not create two classes of citizens—those who have an identity and those who do not. On the contrary, it should bridge the gap between the well-off and the poorest citizens, by making a reliable, simple and efficient system of identification available to all.

The implementation of the system by a private company could be a satisfactory solution, since this would ensure sustainability and allow the State to put in place the National Digital Identification System without having to seek funding to do so. Care must be taken to ensure that this solution does not infringe on citizens' rights and that the service provider strictly follows the specifications given. If possible, regular external audits should be conducted.

If Multimedia Glory is the chosen option, we recommend that the basic rules governing project management be adhered to. As things stand, the best one could hope for is that the National Identity Cards will be printed on the basis of CENI data. The worst case scenario is that none of the objectives of the MSPC would be achieved. We hope that the recommendations made in this document will be useful and wish every success for the project.

At any rate, responsibilities must be clearly defined, specifications clear and precise, the interests of all parties taken into account and the project conducted with full transparency.

This World Bank mission cannot continue unless these conditions are made very clear.

Annex 1: Index of documents consulted

No.	Title of Document	Date/Origin
1	Analysis and Recommendations for the Improvement of the Civil Registry in Guinea	2013 UNICEF, MATD
2	Decree 177, on the Responsibilities, Organization and Operations of the General Public Administration Inspectorate	2014 Office of the President of the Republic
3	2015 action plan of the General Civil Service Inspectorate	December 2014 MFPREMA
4	Annual Activity Report for the year 2014 of the General Public Administration Inspectorate	2014 MFPREMA
5	MFPREMA action plan 2015	2014 MFPREMA
6	Civil Servant Census Report	March 2015 MFPREMA
7	Presentation of the results of the Control of Salaries and Civil Service Personnel Project (two presentations)	March 2015 MFPREMA
8	Decree 135 on the creation of the A.N.GE.IE and its responsibilities	June 2010 Office of the President
9	Circular Letter on the Pooling of Public Administration Resources and Internet Access	July 2011 Office of the President
10	Statistics on the data of the SAGEM Electoral Register	2013 Sabari
11	PERLE Project (source of the first AFIS project for the electoral register)	2006 MATD
12	Tender for the selection of a local operator for the 2012 revision	2012 CENI
13	Tender for the first CENI biometric register	2007 UNDP
14	European Union Election Observer Mission—Final Report	September 2013 EU
15	Standard police record	May 2015 Court of 1st instance
16	Standard Supplementary Judgment Form	May 2015 Court of 1st instance
17	MATD Institutional Development Plan—Final Report	January 2015 MATD, EU
18	Funding agreement between the EU and the Republic of Guinea	February 2014 EU
19	Joint MATD/UNICEF/WHO Workshop on the Improvement and Modernization of the Civil Registry in Guinea	November 2013 DNEC
20	Definition of the project for the modernization of Civil Registry declarations	December 2013 DNEC
21	2015–2016 DNEC action plan	December 2014 DNEC
22	Executive decision 410 on the codification of communes and regions and the definition of the NIN	2014 MATD

No.	Title of Document	Date/Origin
23	ETI Biometric brochure	2013 ETI
24	Civil Code	January 1996
25	Children's Code	August 2008
26	Electoral Code	May 2007

Annex 2: List of persons interviewed

Name	Organization	Title	Reason for the visit
H.E. Mr. Guilavogui	MPTNI	Minister of State in charge of Post, Telecommunications and NIT	eID Mission
Mr. Cellou Diallo	WARCIP	Director	Organization of interviews
H.E. Mohamed Diare	MEF	Minister of State	Mission and MultiMedia Glory Project
Mr. Mamady Koulibaly	MEF	Advisor at the MEF	Mission and MultiMedia Glory Project
Mr. Condé Yamori	MATD	Secretary General	eID and MultiMedia Glory
Mr. Kaba Ibrahima	MATD	National Civil Registry Director	Civil Registry Project
Mr. Camara Jean René	Planning	Secretary General	General Census
Mr. Condé Fodé Bangaly	MATD	Inspector General	Civil Registry Project
El Hadj Ibrahima Kalil Keita	CENI	Vice-president	Voters' Register
Mountanga Drame	MEF	Social Networks IT specialist, MEF	Contribution of eID to Social Networks
H.E. Mr. Sekou Kourouma	MFPREMA	Minister	Introduction of the Mission
Camara Mohamed Sikhé	MATD	Deputy Director General—Decentralization	Legal Aspects of the eID
Conde Mamadi	Sabari Technology	Director General	Electoral Census
Taleb Latif	ETI	Director General	Biometrics and Infrastructure
Assamoi Paul	Inovatech ID	Director General	Civil Servant Census
Touré Fodé Mang	BICIGUI	Director General	Professional Banking Association
Bazzo Didier	ONRG	Technical Advisor	DGI Census and NSI Codification
Fofana Elhadj	Assembly	Legal Advisor to the President	Legal Aspects of the eID
Maitre Camara Mohamed Kofy	Justice	Chief of staff	Presentation of the eID
Camara Alpha Abdoulaye	Justice	Head of Human Resources	Legal Aspects and Role of the Civil Registry
Thuillier	Justice	Technical Advisor to the Minister	Legal Aspects and Role of the Civil Registry

Name	Organization	Title	Reason for the visit
Fofana Alseny	Justice	Chief Clerk	Supplementary judgments, police records, civil registry archives
Dr. Kourouma Mamady	Health	National Family Health Director	Birth and Death declarations by health personnel
Dia Mamadou	Transport Ministry	Chief of Staff	Gray cards and driving licenses
Camara Ahmed Camille	A.N.GE.IE	Director General	eID and Multimedia Glory
Mohamed Traoré	MFPREMA	Chief of Staff	Presentation of the Mission
Keita Ahmed Sékou	MFPREMA	Deputy Director General	Chief, civil servant census
Dr. Cissé Mahmoud	MSPC	Minister	Civil Registry and National Identity Card Project
Mr. Keita Lamine	MSPC	Air and Border Police	Pilot for biometric projects
Mr. Camara Ibrahima	President's office	Chief PPP Advisor	eID Presentation and Multimedia Glory Project
Mr. Gassama Mohamed	President's office	PPP Advisor	eID Presentation and Multimedia Glory Project
Mr. Kasas	EU	EU Representative	eID Presentation and ongoing support operations
Mr. Dangleterre	PARSS	HR Expert	eID Presentation and MSPC Projects
Mr. Kaba Ibrahima Khalil	President's office	Minister, Chief of Staff	Multimedia Glory Project
Mr. Fofana Mamadou Lamine	President's office	Legal Advisor	Problem of the Civil Registry

Country Diagnostic
Recommendations for Implementation

Contents

Tables and figures

Abbreviations

ABIS	Automated Biometric Identification System
AFIS	Automated Fingerprint Identification System
AIMF	Association Internationale des Maires Francophones *(International Association of Francophone Mayors—they supplied the Conakry Governorate with a civil register management system)*
AN.GE.I.E	Agence Nationale de la Gouvernance Electronique et de l'Informatique de l'Etat (*The State National Digital Governance and Information Technology Agency)*
BOT	Build Operate Transfer *(a concession to finance, design, construct, and operate a facility)*
CENI	Commission Electorale Nationale (National Electoral Commission)
CNI	Carte Nationale d'Identité (National Identity Card)
CNSS	Caisse Nationale de Sécurité Sociale (National Social Security Organism)
ECOWAS	Economic Community of West African States
eID	Electronic ID *(Numerical Identification System—Name of the system to be implemented)*
FAR	False Acceptance Rate *(Measures the rate of false identifications made by a biometric identification system)*
FRR	False Rejection Rate *(Measures the rate of not identified persons in a biometric identification system)*
FRVT	Face Recognition Vendor Test *(Test organized by NIST to measure Face Recognition Technology)*
GPS	Global Positioning System *(System of geo-localization that can be integrated in a mobile system)*
INS	Institut National de la Statistique (National Statistical Institute)
HIT	Positive result after matching fingerprints
IT	Information Technology
MATD	Ministère de l'Administration du Territoire et de la Décentralisation *(Ministry of Land Development and Decentralization)*
MEF	Ministère de l'Economie et des Finances *(Ministry of Finances)*
MFPREMA	Ministère de la Fonction publique, Réforme de l'Etat et Modernisation de l'Administration *(The Ministry of Civil Service, Reform of the State and Modernization of the Administration)*
MINEX	Minutia Interoperability Exchange *(Tests organized by NIST to measure the interoperability between AFIS providers)*

Morpho	A French company that supplied the system for the PERLE project in Guinée in 2008 (formerly SAGEM)
MSPC	Ministère de la Sécurité et de la Protection Civile *(Ministry of Security in charge of providing ID Cards and passports)*
NIN	Numéro d'Identité Nationale *(National Identity Number)*
NIR	National Identity Register *(System developed by Waymark to manage the elections and produce ID Cards in Guinée)*
NIST	National Institute of Standards and Technology
No HIT	Negative Result Comparison
P.E.R.L.E	Projet d'Enrôlement et de Révision de la Liste Electorale (Project for registration and revision of the Electoral Role in Guinée)
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PPP	Partenariat Public Privé (Public-Private Sector Partnership)
SAGEM	*Previous Name of Morpho—company that delivered the first biometric Identification system to the electoral commission*
TIC	Technologies de l'Information et de la Communication *(Information and Communication Technologies)*
UE	Union Européenne (European Union)
WayMark	*The company that implemented in 2012 the National Identification System developed by WayMark*

Summary

The implementation of Guinea's National eID Digital Identification System in Guinea represents a unique opportunity for its development by providing its citizens with a reliable identification system that could be a support for all the services offered to citizens—the Registry Office, Health, Justice, Education, Public Security, Welfare Agencies, New Information Technologies, voter lists.

The success of such a project requires:

- the establishment of a steering organ representing all stakeholders;
- full transparency and commitment of all stakeholders to the scope and implementation strategy;
- a legal, institutional and economic framework to be defined that respects citizens' rights and ensures the sustainability of the system;
- determination of the services offered by the system and their integration into the existing processes;
- a technical framework for the solution that has to be implemented;
- a realistic approach that takes into account the investments already made;
- a public body which manages the operational system and has the means for its management;
- financing that ensures ownership of the system and its operation and sustainability;
- an audit institution that ensures that the service provided by the system conforms to the anticipated service and that it is properly managed;
- the appointment of a Project Director who reports to the steering body and coordinates all activities from the start of activities to the implementation stage of the operational system.

1. Introduction

Object

This document presents the roadmap for the establishment of a National eID Digital Identification File in Guinea.

It is a follow-up to the Analysis of the Existing on Digital Identification in Guinea and makes recommendations on how to implement the system.

Scope of the document

This document is intended for all stakeholders, and can serve as a basis in the arbitration process conducted by the Guinean authorities on the definition and implementation of the project.

References

The following documents have been used as reference:

- The World Bank Digital ID Tool Kit—World Bank Group—June 2014
- The World Bank Report—Deploying Electronic Identity in Ebola Affected Countries—A Strategic Plan for a Fast Track Approach—February 2015
- The National eID Digital Identification—An Analysis of the Current Situation—World Bank Group—Version 1, June 2015

Contents

This document contains the following chapters:

- Introduction
- Role and objectives which defined the main objectives of the system and associated issues and the stakeholders
- Identity management—principles and associated workflows
- Development of the Digital Identity Project eID—Prerequisites and development strategy
- Implementation Plan—schedule and associated tasks

2. eID in Guinea—Role and objectives

Objectives

The right to an Official Identity is a basic right that every Guinean citizen is entitled to. The establishment of a National eID Digital Identification System based on biometric identification must guarantee that right by:

- being universal—every citizen must have a digital identity;
- guaranteeing the user's identity through biometrics;
- being accessible to all at all times;
- being at the service of the citizen;
- guaranteeing the future and promoting the economy;
- The success of this project is a national issue and a fundamental factor of progress. It can only be guaranteed if the following elements are considered:
  - Privacy and data security;
  - Reliability and performance of the system;
  - Integration into the existing administrative processes;
  - Cost for the citizen;
  - Training and information to all;
  - Sustainability of the system.

Issues at stake

The role in good governance

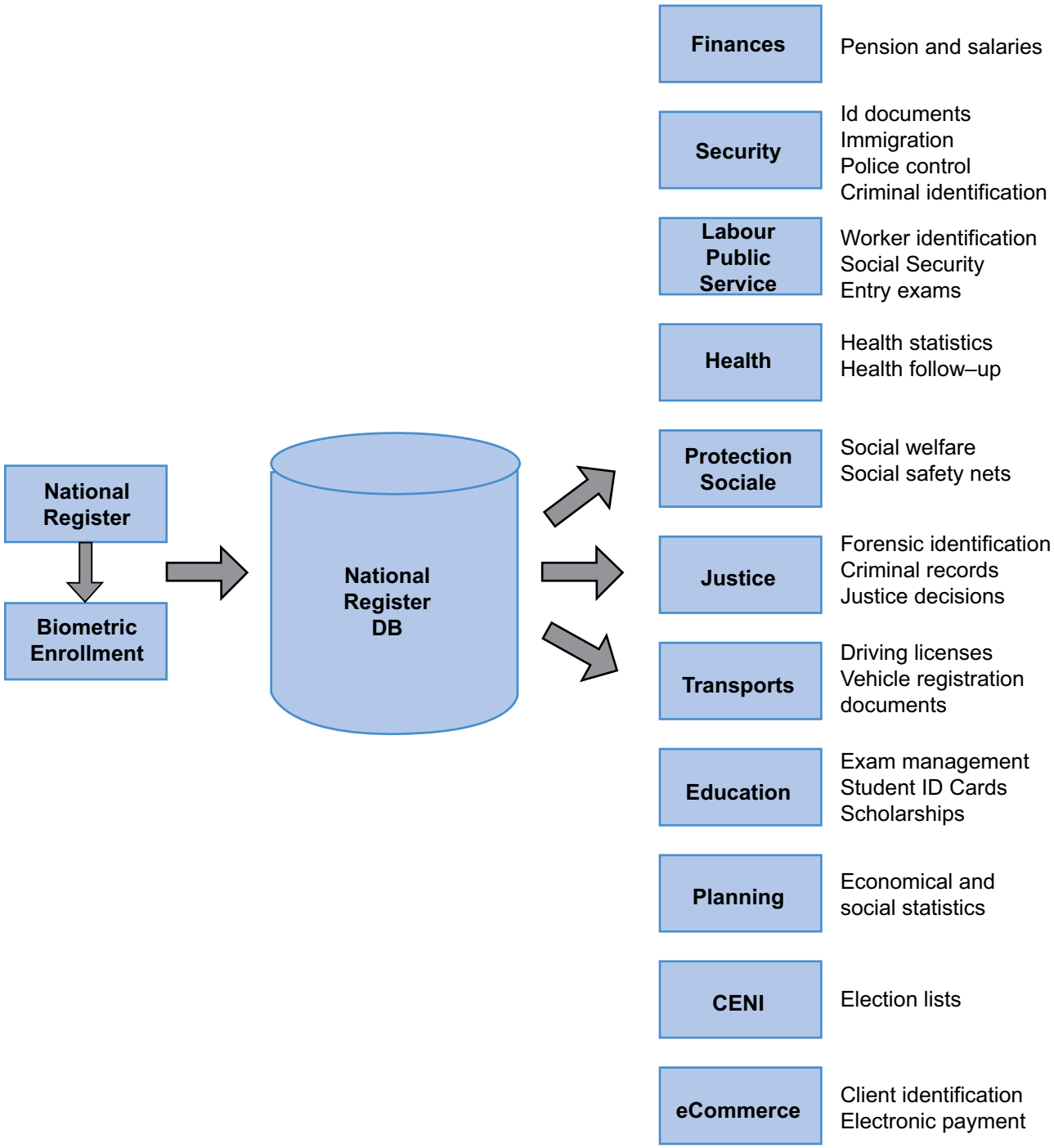
Good governance means ensuring an efficient service to the citizen at lower cost. This objective can be achieved through eID by providing services based on a reliable and unique identification of citizens by limiting all frauds related to impersonation or false identity.

eID should help reduce investments by factoring the costs and improving the efficiency of public services by ensuring system interoperability.

Role in the development of the economy

eID should promote the development of digital economics by providing the companies with a digital ID that makes transactions more reliable by securing the identity of the different actors.

Figure 1: Role of the eID



The stakeholders

Ministry of Posts, Telecommunications and New Information Technologies

Given the predominance of ICT Projects, the Ministry of Posts, Telecommunications and New Information Technologies (MPTNT) should play a leading role in the design and implementation of the Project. In particular, the MPTNT must consolidate the demands and needs of different stakeholders (sector ministries), and propose technical standards and specifications that meet the needs of other ministries.

The MPTNT must also be closely involved in the implementation to ensure that ICT facilities are adequate and used suitably for the future deployment of the eID system (the Project).

- The effectiveness of the system and the solutions to be implemented will depend in particular on:
  - The mobile network coverage throughout the country;
  - The level of progress of the eGov Project (Government Network Project to cover all prefectures);
  - The establishment of a public key infrastructure (PKI) service that is essential to data security in the context of the new technologies;
  - The implementation of online payment for the payment of duties.

The Ministry of Finance (MEF)

It is interested on several counts:

- It is the guarantor of the financial solution put in place to implement the system and ensure its sustainability.
- It manages the pay of employees and pensioners of the State. As such, it is interested in the identity of such persons and in a functional and effective eID that would allow it to improve the functioning of such services.
- It manages the Social Nets. The establishment of a system based on the identification of beneficiaries would significantly increase the distribution of aid.
- Under the General Tax Directorate, a general census of private sector businesses is under way; these companies are sole ownership companies and identification of the entrepreneurs is a key aspect of the establishment of a fair and efficient tax system.

Ministry of Land Development and Decentralization (MATD)

The National Civil Status Directorate secures the identity of the citizen. As such, it must play a key role as both a provider of information via the registration of vital events and keeping the civil registers, as a client:

- Biometric identification during the biometric enrollment of citizens;
- Biometric authentication of the declarant when recording statements of birth, marriage and death.

To date the Civil Status is poor and unreliable:

- Many civil status registers have been destroyed;
- The number of births declared is inadequate (less than 50% in some rural areas and less than 80% in the urban areas);[1]
- The death is not reported (less than 6%);
- The Transcript registers are not updated due to the misuse of the supplementary judgments.

The eID should ponder over this situation and implement procedures to take into account people who have no civil status and ensure regular registration of new births and deaths.

The Ministry of Health

- There are many ways the Ministry of Health can benefit from the eID:
  - Registration of births and deaths by healthcare personnel. Proper recording of these events is essential for the operation of the Civil Status and eID; technical solutions can be found, but the problem is not just technical; there is the need to educate and stimulate the health personnel;
  - Health statistics and epidemiological alerts; these statistics are an immediate by product of the registration of deaths and their causes; they can be refined, if a medical monitoring application is implemented;
  - Medical care of children; if children are properly registered at birth in the eID, it will not be difficult to implement applications based on the eID to ensure medical care;
  - Identification of patients: the eID should help identify patients in a secure and efficient way.

The Ministry of Justice

The Ministry of Justice is a major player in the consideration of acts of identity change. The implementation of the eID is expected to help to automatically re-transcribe these decisions.

A way must be found to replace the complementary judgments. The eID must address safely and efficiently the cases of persons who have lost their identity and avoid the proliferation of illegal documents.

Finally, the Ministry of Justice should be able to effectively use the eID for:

- Identification of the accused;
- Registration of court decisions;
- Sentence management;
- Management of criminal records.

The Ministry of Security and Civil Protection

- Most applications to be implemented by the Department are based on the identification of persons:
  - Identity document management—Passports, Residency permits, Identity cards;
  - Visa management;
  - Border controls;
  - Management of criminal records;

1 Analysis and recommendations pertaining to the improvement of the Civil Status in Guinea—CRC4D November 2013.

- Identity checks;
- Crime solving.

The ministry has already set up its own biometric system for the management of passports, visas and resident permits, and it is now implementing a solution for the National Identity Cards.

Despite all precautions, cases of fraud were uncovered. The merger with the National Identity Register (NIR) would highlight some of the fraud and the use of the eID for both Passports and the National Identity Cards would secure the identity of applicants.

The Civil Service Ministry

This Ministry is involved in several respects:

- The Ministry in charge of the ANGE.IE, a public body responsible for the coordination of the Administration's major IT projects of the administration as well as the design and implementation of Guinea's electronic systems—e-government, e-education, e-health, e-finance and e-services;
- The implementation of FUGAS (Single File for Administrative and Salary Management), based on biometric identification of civil servants:
  - Using Biometry, the Ministry has already eliminated the ghost public workers;
  - The merger with the National Identity Register is expected to complete the clearance work under way and use of the National Identity Card based on the National Identity Number will streamline procedures by securing the identity of the officials and government contractual workers nationwide.

The Ministry of Technical Education, Vocational Training, Employment and Labor

- The Ministry is interested in the implementation of the eID for several reasons:
  - It is the Ministry in charge of the NSSF that implemented a social security card based on a biometric identification system;
  - It is responsible for management of work permits.

The Ministry of Social Welfare, Women's Promotion and Childhood

The Ministry is interested in eID for the customized monitoring of its programs. Through its social workers, it could actively participate in the awareness campaign on the reporting of deaths and births essential for the correct operation of the eID.

The Ministry of Pre-University Education and Literacy

This Ministry could play a double role by:

- Ensuring that the children enrolled in the schools have been declared and that they have a National Identity Number;
- Promoting the National Identity Number and the benefits of reporting as part of civic education.

This Ministry could benefit from the eID to conduct the monitoring of the schooling of children on an individual basis. For example, a mobile application could be implemented that would record at every enrollment the school and the class of the child.

Another application could allow registration for the exams and recording of the results.

The Ministry of Higher Education and Scientific Research

This Ministry can take full advantage of the eID in the following areas:

- Management of enrollments with authentication of the students and monitoring of their schooling;
- Production of student cards based on the National Identity Number, giving access to the various services related to student life (library, sports, university cafeteria, . . .);
- University course management;
- Management of scholarships.

The Ministry of Foreign Affairs

It acts as civil registrar for Guineans born abroad. As such, it holds the civil registers for expatriate Guineans. It must take an active role in the updating of the National Identity Register.

The Ministry of Defense

It conducted a biometric census of its staff. eID should enable it to properly identify young recruits.

The Electoral Commission (CENI)

This organization plays an essential role since it would provide the voter file as the basis for the eID. In exchange, the eID could help establish a permanent revision system based on reporting and the biometric enrollment before the age of majority.

In this context the electoral law should be reviewed.

Part or all of the investments of the CENI could be re-used with a permanent deployment of equipment that would be made available to the civil status staff for the ongoing enrollment of citizens and registration of changes of address.

Such an operation imposes strong constraints on the implementation of the National Identity Register that should take into account the election schedule.

Role in the treatment of Ebola-type pandemics

Epidemiological alert

At present, the births and deaths are brought back up through the health structures that fill the counter foil book and give a copy to the family:

- the information is incomplete, to the extent that it is not the country as a whole that is covered with health posts;
- the information feedback is very slow and may take weeks (too late to treat an epidemiological alert);
- the analysis can be carried out only after consolidation of the results.

The eID is expected to help record all births and all deaths with their cause and thus have an instant analysis of the causes of death.

For this system to be effective it is necessary that these reports of death are systematic and promptly addressed, even when the death takes place outside a medical facility.

For this purpose, two birth and death registration applications can be implemented as part of the eID:

- an application on Smartphone for the regions covered by the mobile phone network (90% coverage);
- an application accessible via the Internet for sites connected to the eGov network (Coverage rate and planning).

The eID should help to easily implement such solutions. We hope that in the near future Guinea will be fully covered, ensuring the immediate registration of all births and deaths with their attendant causes.

Technology does not solve everything. The human factor must be taken into account and the implementation of the eID must be matched with a training and information campaign that should make everyone understand the importance of the issue.

Entry and exit of the contaminated areas

As we control the international movements, the eID could easily be used to control local travel by setting up a Smartphone application.

The police posted at the boundaries of contaminated areas would be equipped with Smartphones. The control application would instantly register in the eID the passage with national identity number that is on the National Identity or travel document for children without an ID card.

The movement would automatically be registered in a database linked to eID, the location of the control point being made automatically by GPS.

In the event of the migrant being infected, the eID is expected to help to know the course taken by the contaminated person and the location of those around him/her and to establish new security barriers.

We can't in that case use the fingerprint which requires a physical contact with the fingerprint sensor. Facial recognition can be used. It is less reliable, but easily implemented with a Smartphone and should allow a first level of identification.

Monitoring international travels

Biometrics is already being used in the context of border controls in many countries bordering Guinea.

With the eID, people travelling from abroad will be identified at the time of visa checks for non ECOWAS nationals or control for ECOWAS citizens. If they hold documents that meet the ECOWAS requirements, the enrollment becomes easy and can be automated; should the opposite occur, an enrollment should be effected; to reduce the layover time, enrollment could be limited to countries at risk.

For outbound passengers, in case the local movement control application is in place, it will be easy to consult the movements to ensure that the person has not visited areas or countries at risk.

Identification and monitoring of people at risk in the context of an epidemic

This mainly concerns health staff and people close to the patient, including children. This staff may consist of nationals or expatriates.

One can't in this case use biometric identification that requires contact with the fingerprint sensor.

The technologies based on the iris or on fingerprinting without contact would avoid the contact and would make biometric identification even more secure. The contactless fingerprint scanners are still expensive, but they may be limited to patients, their families and caregivers.

3. Identity management

Registration and controls

Control is essential because it ensures the level of trust we can have in the system. Most frauds are related to inadequate controls.

The basic principle is that all events related to the identity are recorded in the system from birth to death and their recording is reinforced by the authentication of the submitter.

We propose here some work flows that will ensure these principles.

Birth registration

As is currently the case, the operation will be conducted in 2 stages:

- Registration of birth by medical staff or village chief:

  Either directly using a mobile phone application for the areas covered by the telephone network;

  Or a posteriori by the civil register officer, using the village record book or medical record book for declarations for areas not covered by the telephone network;

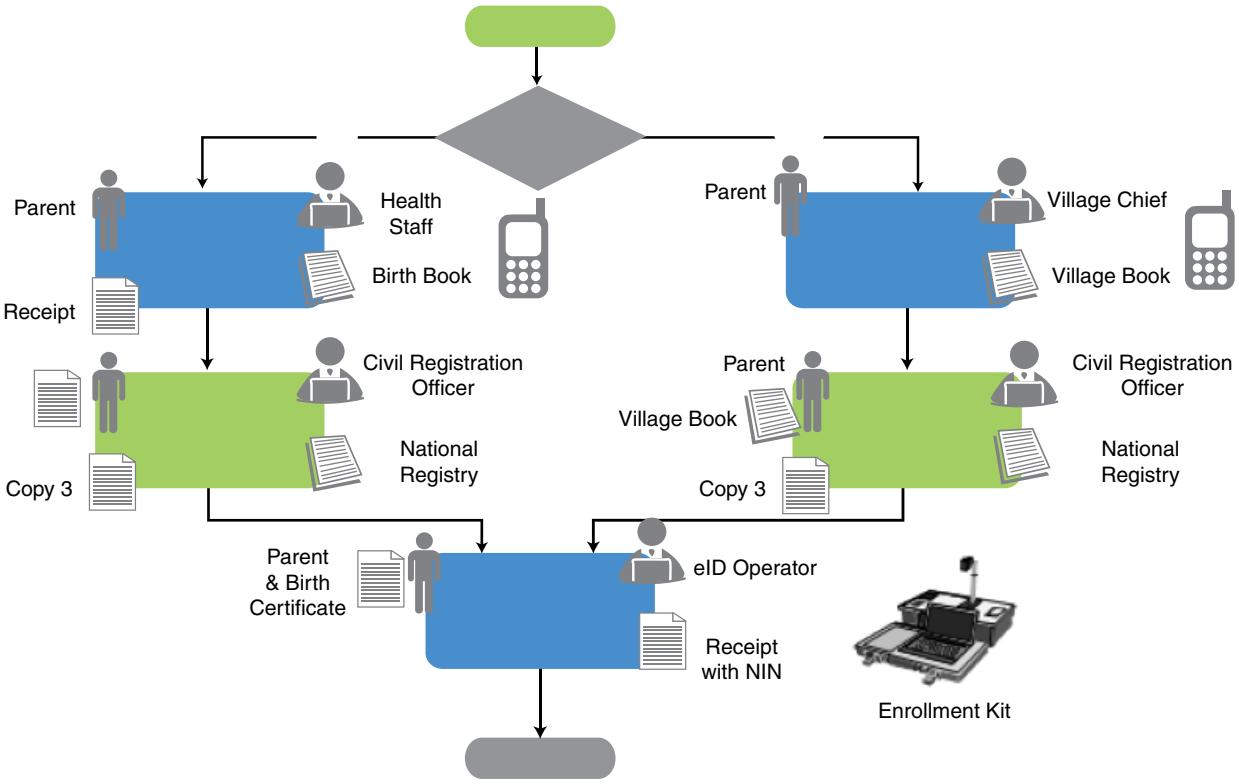
  Nowadays this step is not properly managed; very often the health staff does not issue any document to parents; we recommend incentives linked to the declaration of births at the registry office;
- The declaration of birth at the Civil Register Office made by the parent(s) to the municipality registry office:

  The statement must correspond with the birth recorded by the health staff or the village chief;

  The newborn is registered in the system;

  A receipt with the national identity number is given to the parent—the receipt concerned is not a birth certificate, but it can be used to obtain the certificate.

Figure 2: The Birth Registration Process



We have described this process by trying to follow the procedures which are currently in place and subject of pilot operations.

Before implementing this process, we must ask the following key questions:

- Is the birth registration by the village chief or the health personnel realistic?
- Isn't the process an obstacle to universal birth registration?
- Should a connection be established with the parents while recording their National Identity Number (NIN) if it is known?
- In this case should the parents be authenticated?

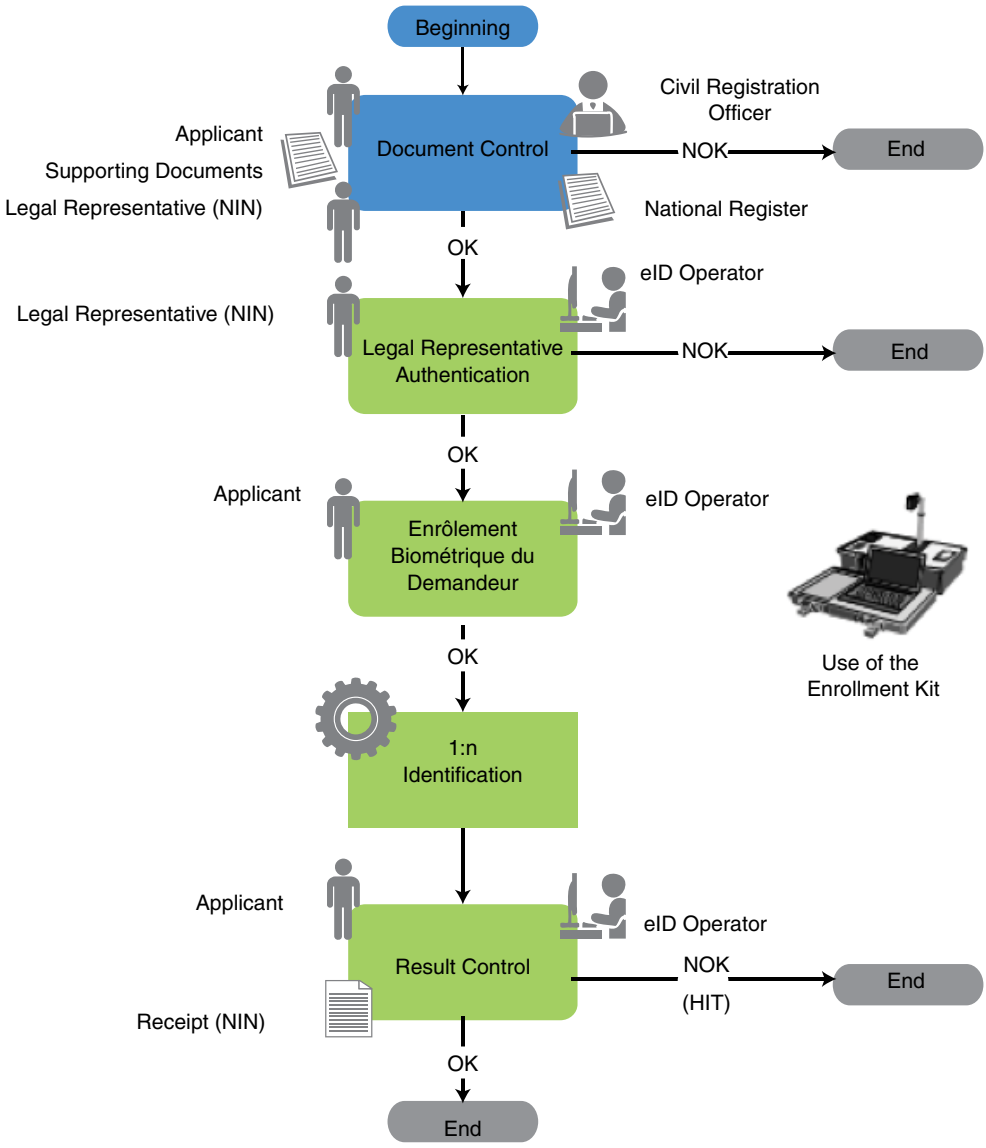
Registration in the eID of unregistered juveniles with a civil status

This applies to all those born before the introduction of the eID and who are not included in the national identity register. They must be registered in the system to get a NIN—a prerequisite for obtaining any identity document.

This registration must be done by the staff of the Registry Office of the person's birthplace.

The applicant must be accompanied by his legal representative with his identity and his birth documents.

Figure 3: Registration of a Minor without a NIN



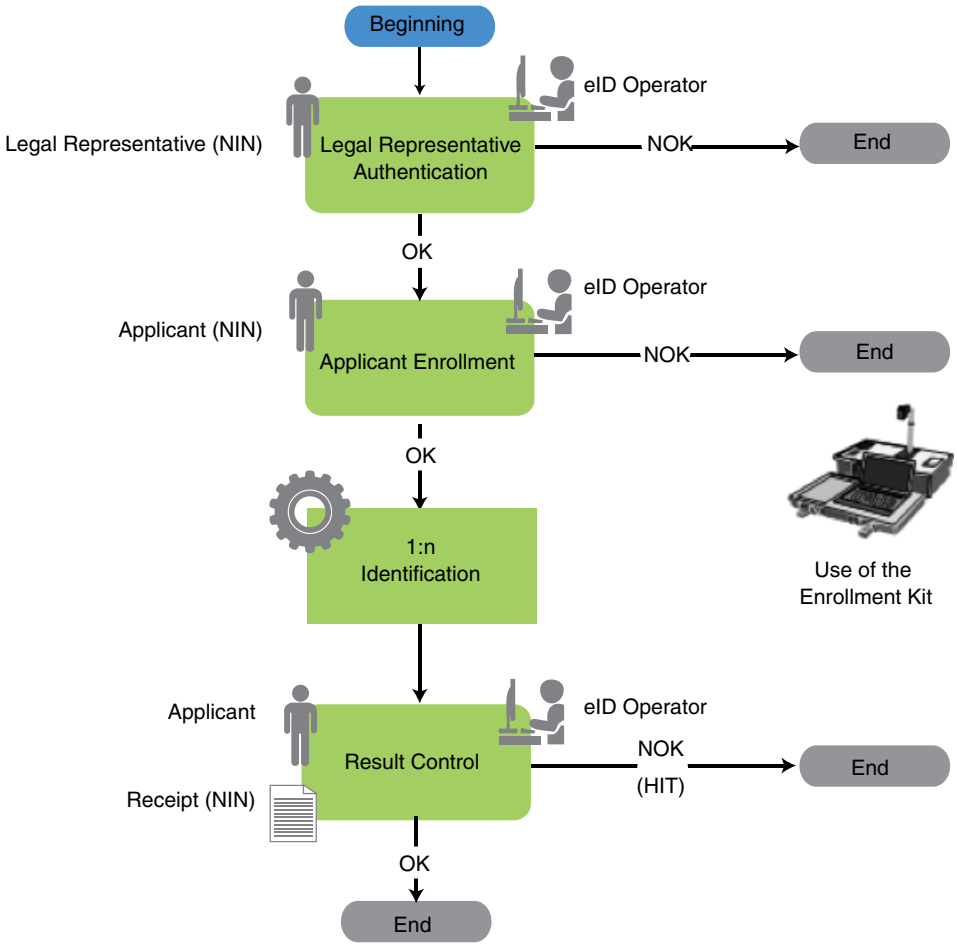
The following operations must be carried out:

- Civil Registry Control based on the documents presented;
- Biometric authentication of the legal representative;
- Registration in the system of the biometric data;
- Production of a receipt with the National Identity Number.

Initial biometric enrollment of minors in possession of a National Identity Number

This applies to young people not in possession of any identity document but already have a national identity number either at birth registration or upon request.

Figure 4: Enrollment of a Minor with NIN



This must be carried out before the delivery of the first identity documents. It must be done as close as possible to the applicant's place of residence. For this, it is desirable that all municipalities be equipped with the means to do so. This is essential and should not be the occasion for false identities based on theft of identity. This is why we recommend the presence and authentication of the legal representative during this operation.

The following operations must be performed:

- Biometric authentication of the legal representative;
- Applicant enrollment:

  Control of the applicant based on his National Identity Number; the system data matches with the presented documents; if that is not the case, the application is rejected;

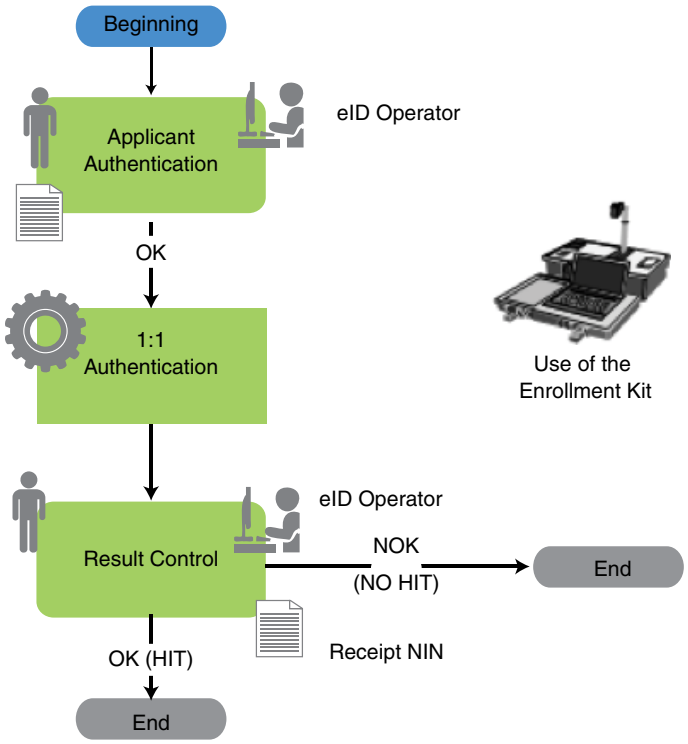
  Capture of biometric data and identification request sent to Central Site;
- Biometric identification of the applicant (research 1:n):

  Matching 1:n is performed;

  In case of no match, the biometric data is recorded in the system;

  The results are sent to the operator;

Figure 5: Application for a NIN



- Control of search results by the operator:

  In case of match result two cases can be envisaged:

  - The system data matches with the applicant data—biometric enrollment had been previously performed—a receipt can be given to the applicant;
  - The biographic data does not match with the applicant data—this is probably a fraud attempt; an investigation should be conducted—the decision will be taken after the investigation.

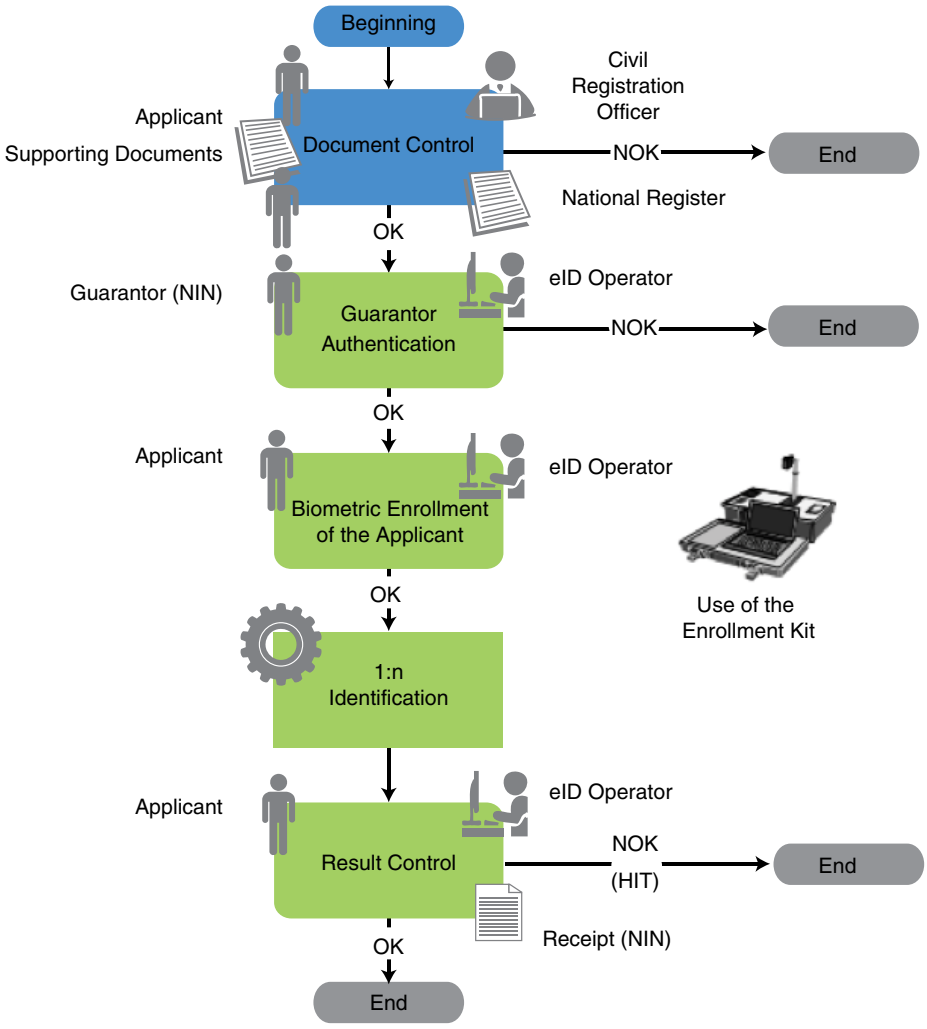
  In case of no match, a receipt can be given to the applicant; the receipt will help the applicant to obtain ID documents.

Adults registered in the electoral roll

The level of confidence in the electoral register allows us to assume that citizens registered in this file were correctly identified. A National Identity Number will be assigned during system initialization.

- They may request this number from the Registry Office by presenting their polling card;
- The person is authenticated biometrically;
- A receipt is issued with the National Identity Number.

Figure 6: Adult Unregistered in the System



Registration of an adult unregistered in the eID and having a civil status

This applies to adult citizens not registered in the electoral roll.

This registration must be done by staff of the Registry Office of the birthplace. It is mandatory in order to obtain a national ID number and is a prerequisite for obtaining any identity document.

The applicant must bring along his birth certificate and be accompanied by a guarantor in possession of a NIN and his identity documents.

The following procedure should be followed:

- Controlling the civil status register based on the documents presented;
- Guarantor authentication;
- Registration of the applicant's biometric data;
- Biometric enrollment of the applicant;

- Identification of the applicant (comparison 1:n):
  - The person is already known and the biographic or biometric data does not match with the application:

    The application is rejected;

    This is probably a fraud attempt and an investigation should be carried out to resolve the issue;
  - The person is unknown:

    A National Identity Number is allocated;

    The person is registered in the eID;

    A receipt is issued to the applicant.

Control by the Registry Office and authentication of the guarantor do not fully guarantee against attempts at fraud. This risk can be reduced by informing all stakeholders of penalties in case of attempted fraud. Any proven fraud must be severely punished and published in order to deter potential fraudsters.

Registration of persons without civil status

This applies to all persons, whether adults or minors, for whom the Register does not exist and have no documents showing their civil status. A supplementary judgment must be issued that should not be considered as a civil status document. It must be first recorded in the transcript register of the place of birth under the responsibility of the local registrar. As happens in other countries, the judgment is stapled to the register and registration can be done only in the presence of a witness.

This is not the procedure being currently applied and the law must be amended accordingly.

Hence, the procedure for those with a civil status may be followed.

Registration of the changes of address

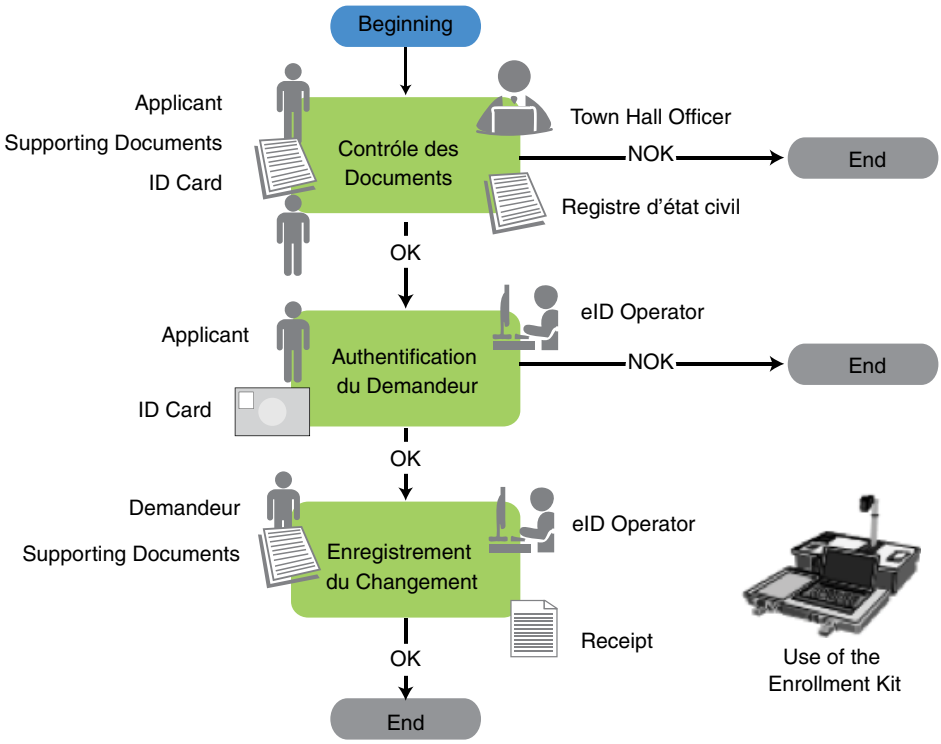
This is important for the review of the electoral lists. This also allows for accurate population statistics on migration.

The applicant comes along with his supporting documents (National Identity Card and Certificate of residence).

The following operations should be performed:

- Document control;
- Authentication of applicant;
- Registration of change of address.

Figure 7: Change of Address



Production of identity documents

This concerns the birth certificates, National Identity Cards, Certificates for secure use of mobile applications or the Internet.

They should be based on the National Identity Register to give them a good level of reliability.

Birth certificates

They are produced on demand by the Civil Registry officials and are based on the civil status registers. We recommend that these documents be produced after the registration of the declaration in the eID on the secure and numbered paper. It must include, in addition to civil status data, the National Identity Number. This document is the only proof of identity for minors who do not yet have a National Identity Card.

The eID should help obtain a copy thereof easily.

The National Identity Card

The MSPC has chosen to produce ID cards with smart cards to authenticate with the data that is on the chip. We do not think that the solution is satisfactory for:

- Lack of involvement of the stakeholders;
- The processes that help ensure a good level of trust are not defined;

- The investments already made are not taken into consideration (Electoral roll, Cards and WayMark production system);
- The choice of the National Identity Number does not take into account the situation of civil registers;
- The terms of the implementation are not defined;
- The implementation of the ECOWAS card planned for 2016 is not taken into account.

We recommend limiting investments using the card stock that was purchased as part of the Waymark project pending the establishment of the ECOWAS identity card which will be launched in 2016 and which we hope will take into account all eID related constraints:

- Document identification;
- Printing of civil status data and portrait according to ICAO standards;
- Encoding on the chip of vital data, portraiture and templates associated with the fingerprint allowing for authentication of the bearer.

At first, the identity card must contain the National Identity Number, biographical identity data and photograph in a 2D bar code with the minutiae of one or more fingers that would allow for bearer authentication.

A National Identity Card project which would not rely on eID would question the basis of eID and would cast doubts on the validity of the documents.

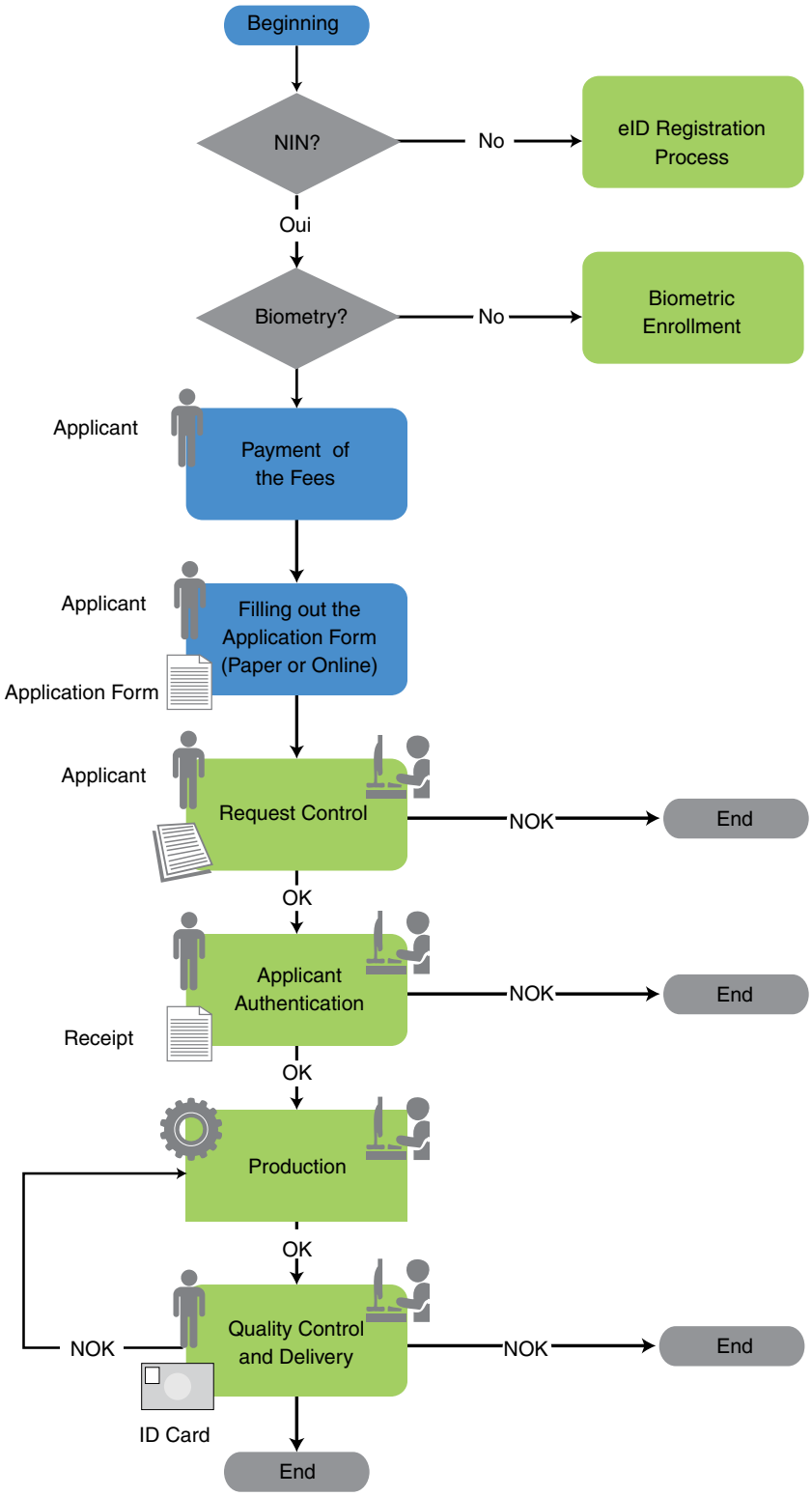
The prerequisite for obtaining a card is that the applicant be registered biometrically in the eID:

- He has an NIN either because he was in the Electoral Commission file or because he was biometrically registered in the eID;
- He can be authenticated with his biometric data stored in the eID.

We strongly recommend control of the quality of the document produced at the time of the issuance ensuring that it can be used to authenticate the applicant.

The applicant authentication when applying for the National Identity Card significantly reduces the risk of collusion during enrollment or processing of card ID request as there is need for the fraudster to get on his side the enrollment officer, the card ID data entry operator and the document issuing staff.

Figure 8: The Identity Card Issuing Process



The certificates

As part of the eGov and a digital saving that the eID will permit, we strongly recommend the implementation or use of a Public Key Infrastructure with a Certification Authority and Registration Authority.

Mobile identity

This applies to both individuals and government officials who need to use mobile applications in the context of their work. eID should provide them with a mobile identification system that guarantees the security of their transactions.

Three solutions:

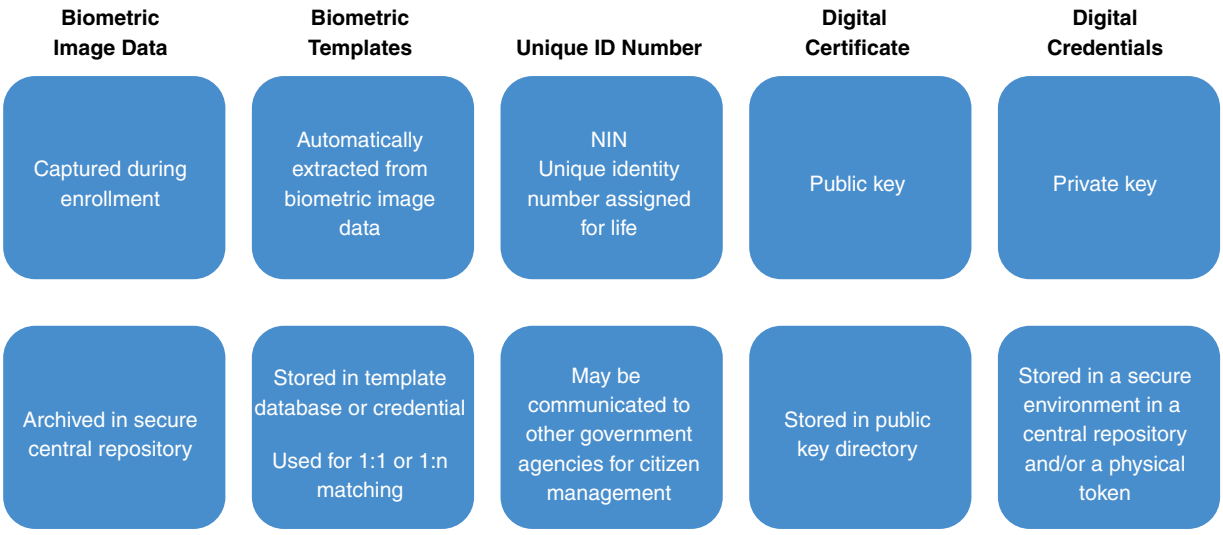
- Using a PIN associated with the NIN for transactions that are made from a mobile device—useful when there is no biometric authentication means available;
- Using a certificate, required for online authentication;
- Biometric authentication requires the means to enter the person's biometric data to be authenticated (fingerprint sensor or high definition camera for facial recognition).

Identity guaranteeing data storage

These data can be stored at several levels according to their type and usage:

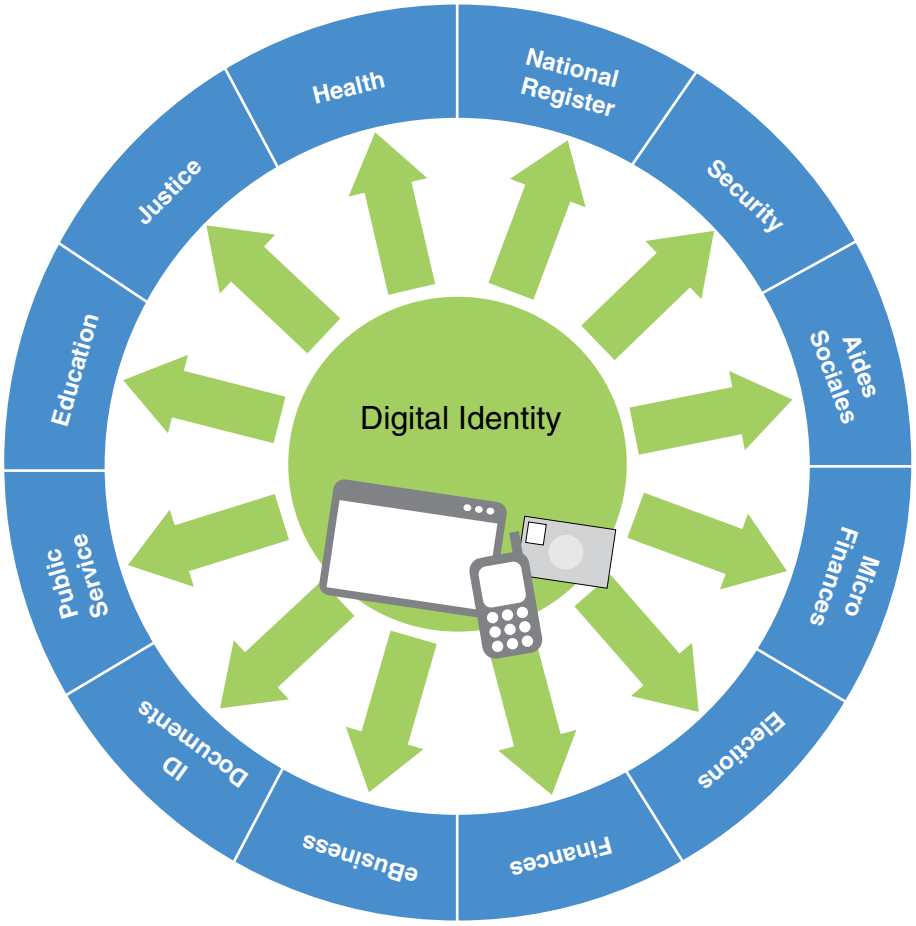
- Biometric data images;
- Biometric templates;
- National Identity Number (authentication);
- Public key—a key given to a user that can be used to authenticate and decrypt data from a reliable transmitter;
- Private Key—key given to the transmitter to encrypt data.

Figure 9: Identity Guaranteeing Data



The use of eID

Figure 10: eID Use



Public Sector

- National register
- ID documents
- Driving licenses
- Security
- Health
- Justice
- Education
- Social protection
- Elections
- Finances (pensions, taxes, salaries)

Private Sector

- eBusiness
- Electronic payment
- Insurance

The implementation of eID would be a real development tool in effectively fighting against fraud, protecting the weakest and securing all with an identity.

Fight against fraud

The first use of the eID is the fight against the multiple identity related frauds and the eID effectively helps to fight against these consisting of:

- The use of false documents:

  Any use of the eID for document production is centralized in the eID with the references of the document produced. Using a false document is immediately identified by consulting the base;
- The use of genuine forged documents:

  A cursory comparison of the eID base and document data reveals the fraud;

- The use of genuine documents based on false statements:

  Registration in the eID right from the statement of birth prevents from making false statements that would alter the identity;
- Use of stolen documents or identity theft:

  The biometric authentication feature related to the document or available online eliminates this risk.

Production of identity-based documents

In addition to identity documents, eID allows the production of numerous documents based on identity:

- Passports:

  There is already a passport production system. It is now based on a document control and on an interview of the applicant. Identification with the National Identity Register would allow more effective controls than they are now;

  We recommend that in this context, the applicant's passport file be updated to take into account the National Identity Number;

  A biometric reconciliation of the file of passports applicants with the eID will help detect fraud that had not been noticed when producing the passport;
- Driving license:

  The system to put in place can be based on the eID for authentication of applicants and therefore does not require AFIS for its implementation;

  This link with the eID will help fight effectively against the trafficking of false driving permits;
- Registration certificates for vehicles belonging to persons;
- School and student ID cards:

  eID could be effectively used for the production of these documents in order to avoid the risk of fraud in the examinations;
- Social security cards;
- Gun permits;
- Police cards;
- Guard service card;
- Insurance card;
- Civil servant's card;
- Retail card for informal trade that would help ensure that the trade is allowed and has fulfilled all tax obligations.

Justice

Identification of individuals is a foundation of justice; many uses can be envisaged:

- Identification of persons subject to trial (authentication);
- Consideration of court decisions based on reliable National Identity Number (authentication);
- Identification of accused persons (identification);
- Management of convictions (authentication);

- Management of a central police record based on the National Identity Number:

  Registration of new convictions pose no problem. The reconstruction of the history seems almost impossible:

  - The history is scattered over different court offices;
  - Establishing the link between past court decisions and eID seems to us problematic.

Elections

eID should help avoid the costly review of electoral lists based on the National Population Registry which is up to date at any time.

Eventually, if the generated ID cards are based on this file and are put into general use, the identity card would replace the voter card.

Whatever the solution adopted, the electoral law should be revised to allow the compilation of lists from the eID.

Moreover, the registration on the lists is based on the place of residence; this means that changes of residence should be handled in the system.

Identity control

In this field there are multiple applications. They are all based on the authentication feature of the eID. We only mention the main ones:

- Identification of civil servants;
- Identification of pensioners;
- Identification of social insurance contributors;
- Identification of welfare beneficiaries;
- Declaration of residence:

  The change of residence can be handled by the system; it could be complemented by a mobile application that would be made available to the neighborhood chief or village head;
- Health control;
- Border control;
- Police identity check;
- Land Registry;
- Taxation of the informal sector could be based on the trader's identification with the presentation of a card enabling him to practice his trade;
- Authentication for all online transactions, based on the certificate.

Implementation of social and economic statistics

The more applications associated with the system, the more it will be able to provide reliable socioeconomic statistics.

At an initial stage, based solely on the statements of birth and death, the system must provide reliable and rapid demographic and health statistics.

Management of social assistance

Identification of people in need of help is essential.

The eID should help:

- Check on the beneficiary's identity;
- Make sure the recipient does not receive several times the same assistance by registering in multiple assistance programs;
- Ensure that the family is effectively registered and that it fulfills its obligations;
- Ensure that the benefits are paid to recipients.

Microfinance

Microfinance is a key factor of development and of improving the status of women.

The biometric authentication of the beneficiary should facilitate the implementation of loans by ensuring reliably the identity of the beneficiary, and based on that identity, a transaction history that allows the granting of new loans.

Implementation of online services based on online digital identification

This concerns both the public sector and the private sector.

Online services must be able to rely on an irrefutable identification of the beneficiary. The implementation of the eID is expected to develop this type of application.

One of the first applications is electronic payment services essential to the proper development of online commerce.

Insurance companies and mutual health associations

This concerns both the public and private sectors managing health expenditure.

It is essential for this activity to control the identity of the beneficiary to ensure the beneficiary's rights.

Pensions

A biometric check of pensioners would help ensure that they are still alive. Biometric tablets could be used for this control. This control is a way to fight against the non-reporting of deaths.

4. Development of the digital identity project eID

Prerequisites

The implementation of a digital identification system is a complex process that requires the full commitment of stakeholders.

This commitment cannot be granted unless:

- the population to be identified is fully defined (citizens, foreign residents and visitors);
- the perimeter of use is validated by case studies covering the key aspects:

  Registration of births,

  Identification of persons without identity,

  Taking into account court decisions,

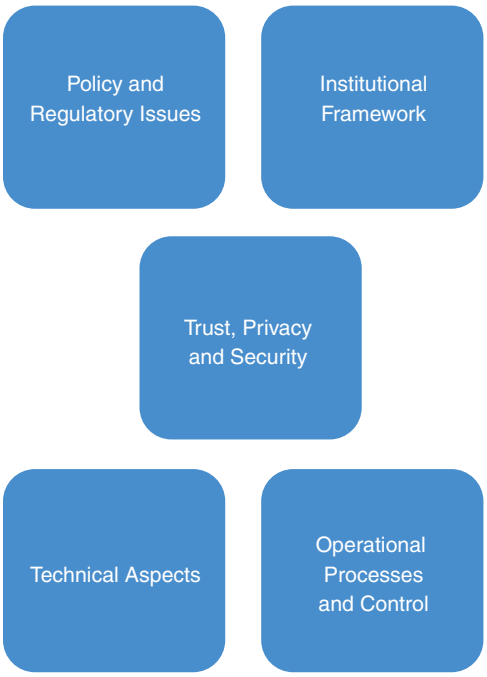
  Production of identity documents,

  Use in the context of social nets,

  Processing of the electoral rolls,

  Digital economy;
- The strategy is approved by the stakeholders;
- The implementation solutions issues are understood by all and have unanimous support for all its aspects:
  - Legal and regulatory;
  - Institutional;
  - Trust, confidentiality and security;
  - Technical aspects;
  - Operational and control.

Figure 11: Different Aspects of the Implementation



The approach and strategy

In Guinea, the approach consisted in developing systems based on sectoral needs:

- The biometric identification of the military;
- The biometric identification of civil servants (MFPREMA);
- The social insurance contributors file (NSSF);
- Passports, Residence permits, visas (MSCP);
- The electoral register (CENI)—the most advanced system that takes account of all the Guineans of voting age; it has been subjected to numerous audits, checks and updates that confer on it a good level of reliability.

This approach is costly; it complicates the enrollment formalities for the citizen and does not help share data easily and improve the level of trust in the system.

Implementation of the eID should help limit the costs and capitalize the investments already made by:

- Using the Electoral Register as a base for National Identification Register;
- Using the investments made for reviews of electoral rolls to set up enrollment services;
- Using the Foreign Residents File of the MSCP as a base for foreign residents;
- Updating the existing files with the eID identifier, the NIN (the eID managed Unique National Identity Number).

The legal and regulatory aspects

Providing a legal framework for eID is important; we should make sure that by ensuring the right of citizens, the eID is not put into question.

Data managed by the eID

Currently there is no law on the management and use of digital data in Guinea. The law should help control the data that will be managed by the eID:

- National Identity Number;
- Biographic data;
- Biometric data;
- Record of updates and uses.

Confidentiality and security of digital data

The National Digital Identification Register covers all citizens and may include confidential data affecting privacy.

The legislation must specify the context in which these data may be used and by whom as well as the penalty associated with any use thereof outside this context.

The law should state that all safety measures provided by technology should be taken against the loss of data or accidental or unauthorized dissemination of such data, with penalties applicable to any fraudsters.

Scrutiny right

Digital Identification can manage numerous data about a person. The law should enable the citizens to know all the data attached to their person that are handled by the eID.

Right to oblivion

The data relating to a citizen cannot be kept indefinitely. The law should specify for each data type how long they can be kept in the system.

Birth and death registration

Registration of births (Articles 157–165 of the Civil Code) and deaths (Articles 166 and 167 of the Civil Code) must be reviewed for consideration of the recording in the eID by specifying:

- Responsibility of the medical staff and/or the village chief;
- Responsibility of the family;
- Responsibility of the Registrar;
- Responsibility of the civil registry officers.

Identity data updating rules

The law should specify that a change in the Civil Status can be applied in the eID only after registration in the civil register. The court decision can in no way replace a Birth Certificate to conform the birth or transcription register.

Management of undeclared persons

The supplementary judgment as used currently should be cancelled.

The law should precise that a supplementary judgement cannot replace a Birth Certificate. To be applicable, supplementary judgement must be registered in the civil register of transcripts of the beneficiary's place of birth under the responsibility of the registrar.

Requirement of a National Identity Number

The National Identity Number must be mandatory for all and can be automatically assigned upon registration in the eID.

Its form and method of attribution must be defined by law.

Using the electoral register

The latest revision of the electoral register must be used to initialize the National Identity Register. This use must be authorized by law.

Biometric enrollment

The law must allow the use of biometrics as a means of identification.

Using the eID

The scope of use of the eID should be specified by law:

- Use by government services;
- Use by the private sector as a server of digital identity.

Access to data

The law should specify who should have access to the data and under what conditions:

- Access to identity data;
- Access to the biometric data (fingerprints, portrait);
- Access to the history data;
- Access to the statistical data;
- Access to the identification and authentication functions.

Updating the electoral rolls

The electoral list revision may be carried out as and when the biometric registration and recording of the statements of residence are taking place. One can imagine that the lists are based on the status of the eID on 31 December of the year preceding the election. This induces a change in the electoral law.

Penalties applicable to false identity witnesses

It is important to have a legal deterrent for identity frauds defining the penalties applicable to the fraudsters and their accomplices.

Cyber crime

Cyber crime must be legally defined and punishable by law. It relates to:

- The use of a false digital identity;
- A breach into the computer systems;
- Alteration and falsification of digital data;
- Destruction or sabotage of information systems.

The institutional aspects

The National Identity Agency

The implementation of such a project requires the establishment of a champion who will be dedicated to this project and will represent the interests of all in all its stages. We recommend using the A.N.GE.IE or the creation of a National Identity Agency (whatever the solution we shall refer later in the document to the National Identity Agency).There are several possible scenarios:

- A public institution under the Presidency;
- A public institution under a Board of Directors representing stakeholders;
- A public institution under a Ministry.

In all cases, the institution must be financially self-supporting with a source of revenue related to user-fee services. This income should help it maintain the system and pay off the initial investment.

The role of the National Identity Agency

The institutional role of this institution is defined in the table below. As an option we have included the production of National Identity Cards.

The National Agency for identification may be limited to Back Office operations.

The Front Office operations will be carried out by public servants who are in contact with the citizens or the operators managed by the provider:

- Registration of births and deaths—Health Personnel or Village Chief;
- Recording of declarations of birth—Civil Register Staff;
- Biometric enrollment—Civil Register Staff;

- Management of identity documents:
  - National Identity Cards—police officers;
  - Acts of birth or certified copies—Civil Register Staff;
- Record of changes of residence—municipal official or Civil Register Staff and/or Police Personnel.

Table 1. Institutional Role of the National Agency of Identification

	Institutional Role	Tasks
Collection	**Data Registration**	▪ Establishes enrollment centers around the country (fixed, temporary and mobile) ▪ Educates and mobilizes the population ▪ Trains and motivates the operators ▪ Ensures the maintenance and servicing of equipment ▪ Centralizes the collected data
Store	**Central Repository**	**Central System:** ▪ Establishes, owns and operates the National Register of Identity ▪ Ensures the uniqueness of the identified persons, either by elimination of duplicates during the system initialization, or by a systematic identification after a biometric enrollment ▪ Assigns a unique number to identity (NIN) that secures an identity for life ▪ Secures and protects the stored data ▪ Updates the identity data when this is required **Standards:** ▪ Defines the standard for enrollment (type of data, controls, quality) ▪ Defines the pathway for total enrollment covering ▪ Establishes the standard for identity vetting (links with Civil Registry, birth and death declarations) ▪ Certifies the registrars and monitors their work ▪ Sets the standard for ICT infrastructure required to secure access the National Identity Register for the purpose of Identity verification
Used	**Birth Certificates**	▪ Manages the stock of security paper ▪ Receives requests ▪ Authenticates the requester using the eID ▪ Prints the document
	National Identity Card (MSPC)	▪ Manages the stock of ID cards ▪ Receives requests ▪ Check the documents ▪ Authenticates the requester using the eID ▪ Custom and printed the cards ▪ Issued the cards by controlling their quality

	Institutional Role	Tasks
Used	**Identity Provider**	▪ Manages the system that allows you to distribute the functions of identification and authentication ▪ Promotes the system and ensures the developments which allow you to extend the service
	Managing Certificates	Public Key Infrastructure: ▪ Certification Authority ▪ Registration Authority ▪ Authority of deposit

Links with other institutions

We recommend to include in the eID all the applications that ensure the identity and location of citizens. Other data and applications will be managed by each institution, the link which between applications is done through the National Identity Number and standard interface to be defined.

The institutional governance of the agency

The functioning of the agency must be perfectly controlled. We recommend to the establishment a multilayer organization based on a set of committees.

Figure 12: Interoperability

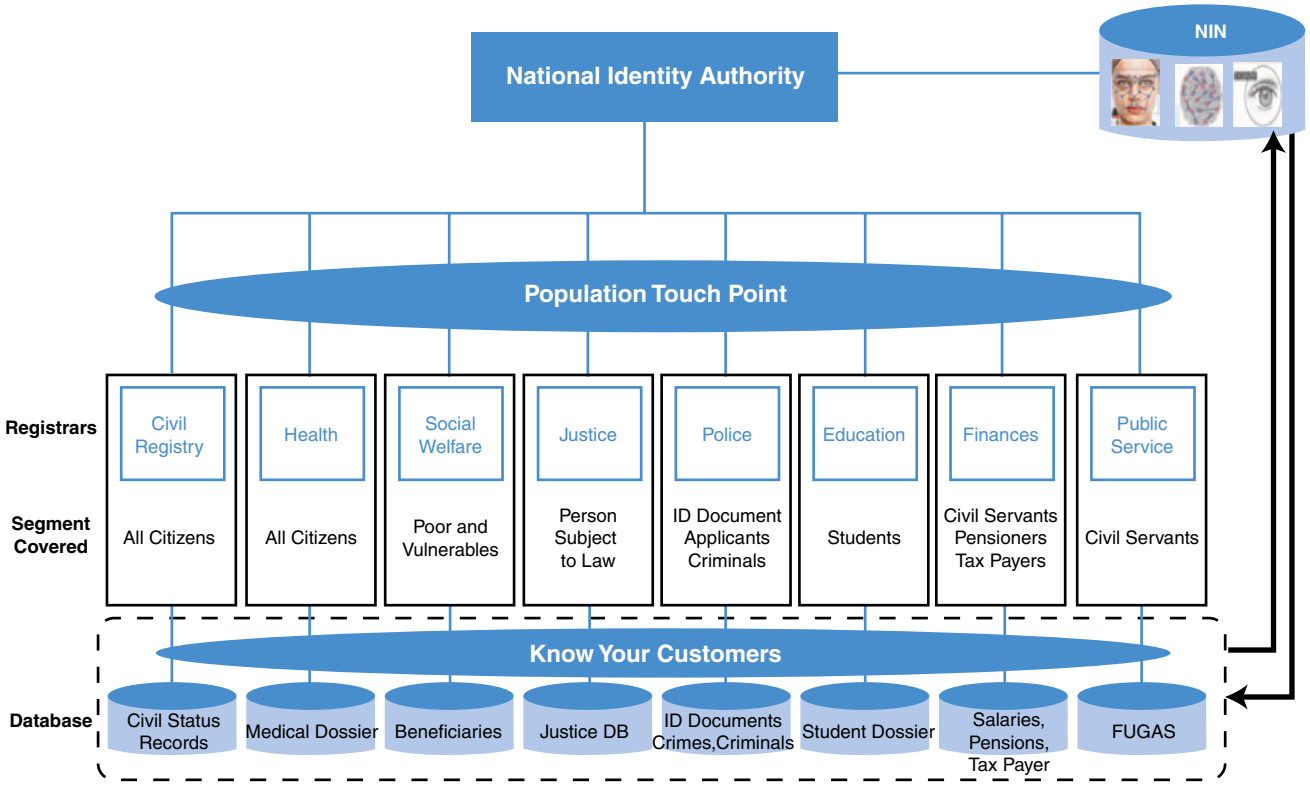
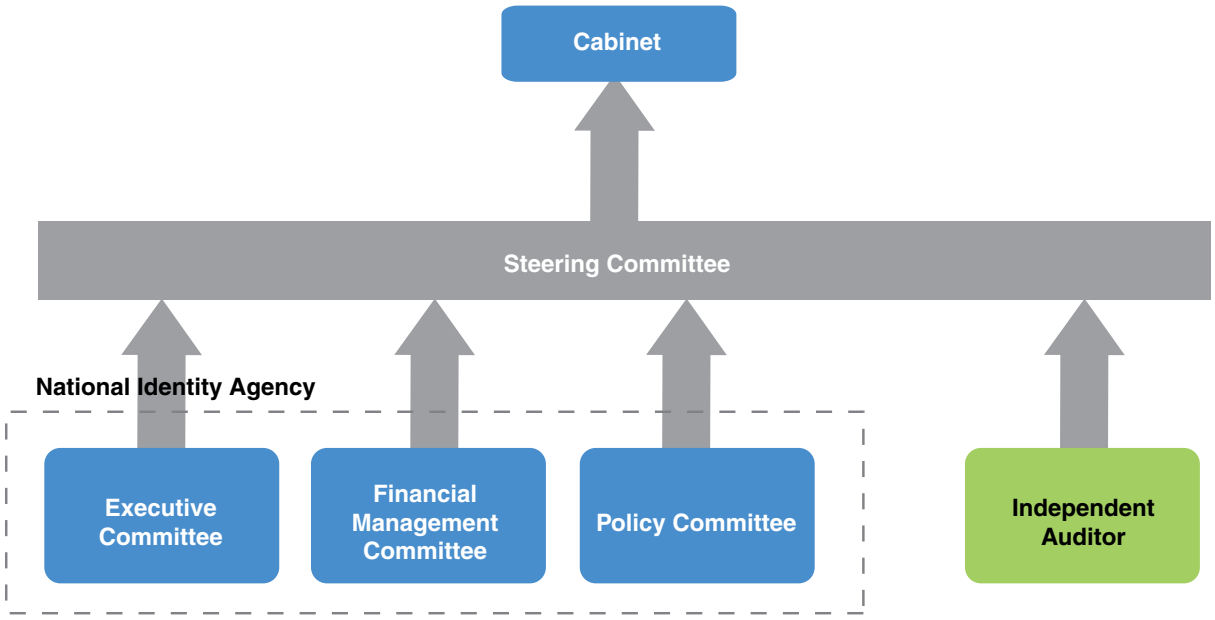


Figure 13: Governance Structure of the Agency of Identity



The steering committee

It meets regularly on a basis to be defined or on request of the chairman or of one of its members:

- It represents all the stakeholders;
- He reviewed the reports from the other committees;
- It takes decisions;
- He can ask for audits;
- He is accountable to the Government or to the President.

The executive committee

It meets regularly or at the request of the Director of the Agency or at the request of the Steering Committee. He is accountable to the Steering Committee:

- It insures of the good management of the agency;
- It prepares and follows the budget;
- It directs, coordinates and controls the activity of employees of the agency.

The financial committee

It is composed of members of the steering committee and meets regularly:

- It approves the budget of the agency and follows its execution;
- It approved the accounts;
- It ensures that the revenues are properly distributed.

The orientation committee

It is composed of members of the steering committee and meets regularly:

- It ensures that the Agency correctly ensured its mission;
- It assesses the risks;
- It proposes new orientations.

Independent auditor

Companies or Agencies that are mandated by the Steering Committee to make audits:

- Security;
- Management and accounting;
- Technical;
- Quality.

Private public partnership

The implementation of a Public-private partnership should help to ensure the sustainability of the system.

It can be done in 3 ways:

- Concession:

  This is the solution that has been considered for the project National Identity Card; if this choice is made, there is no longer a problem of funding. In return, it must ensure that:

  - The system is correctly integrated in the existing structures and interoperability is ensured;
  - The institutional and legal framework is perfectly defined;
  - Guinea remains master of its system;
  - The data that must be confidential are not used by the vendor;
  - The contribution of investment already made is taken into account and is deducted from the share which goes to the concessionary company;
  - The system remains adaptive;
- Participation in the establishment of a consortium of operators:

  Our prior study has not shown that the private sector was prepared to participate in this way; with the development of the digital economy, this could change and would provide an additional financing and the assurance of a better management;
- Subcontracting of services:
  - For the support and maintenance, this is absolutely mandatory and should be part of the contract for implementation of the system with the guarantee that the solution provider is installed in Guinea in a sustainable manner; the service must not be sub-treated locally, but executed by a local subsidiary of the supplier;
  - In the same way, the supplier could provide the staff for the use and administration of the system. This would guarantee a good use of the system and a maintenance guaranteeing the sustainability of the system; it must avoid reproducing the experience which has been made with the equipment of the AIMF (hardware supplied in the Governorate of Conakry for the management of Civil Status by the French Association of Mayors and which have fallen into disuse).

The technical aspects

The functional perimeter

The technical solution depends totally on the functions integrated in eID. They are summarized in the below table.

Table 2. Operational Scope

Function	Benefits	Disadvantages	Recommendations
Registration of births and deaths (optional)	▪ It is placed as close to the people as possible ▪ It allows to raise the level of trust by making it possible to follow the process from birth to death ▪ It allows to keep health statistics	▪ Additional work for health personnel ▪ Staff recording births must be equipped with recording tools (Smartphone or biometric tablet) ▪ May not be universally applicable (energy problems and telephone network coverage) ▪ Staff training and level	▪ We recommend that this function be implemented and integrated into the eID system ▪ In case this function cannot be implemented at birth, it should be made using traditional means (village booklet, book of statements)
Declaration of births and deaths	▪ Allows to link the eID to the Registry Office right after the declaration of birth	▪ Induces a separate operation for the biometric registration	▪ Parents must be authenticated (possible if the National ID is biometric or if there is network connection)
Biometric registration of young people before they reach the age of maturity	▪ Used to complete digital identity before issuing an identity document and automatic enrollment on the electoral rolls	▪ A formality that is new to Guineans. It requires the authentication of a parent or a legal guardian	▪ Can be performed by the Registry Office staff of the place of residence for the municipalities with a connection
Registration of adults	▪ Allows to record an unidentified person removing the abuses of auxiliary judgments	▪ A formality new to the Guineans ▪ Requires authentication of a guarantor ▪ Must be done in the municipality of birth to check the register of transcripts	▪ Must be done by the Registry Office staff of the place of residence

Function	Benefits	Disadvantages	Recommendations
Registration of change of residence	▪ Used to centralize information on population migration ▪ Helps to automatically update the electoral roll ▪ Serves to fight against the misuse of certificates of residence	▪ Does not stand in lieu of the residence certificate	▪ The person making the statement must be subjected to biometric authentication
Production of secure birth certificates (optional)	▪ This would be an immediate tangible benefit of the eID	▪ Secure Document Management to be added ▪ The infrastructure is more costly	▪ Limit this feature to the prefectures

The general infrastructure

The general infrastructure is totally dependent on the environment and operations to be performed at each type of site as summarized in the table below.

Table 3. Distribution of Equipment

Site	Operations	Environment	Equipment
Main site	▪ Data management ▪ Administration ▪ Comparison 1:n and comparisons 1:1 ▪ IPK structure	▪ Secured premises ▪ Access to eGov ▪ Access to Telecom services provided by the operators ▪ Direct optic fiber connection to the backup site	▪ Access control ▪ Generator ▪ UPS ▪ Air-conditioning ▪ Fire alarm and extinguishers ▪ AFIS/ABIS ▪ SGBD Server ▪ 10 terabyte storage rack ▪ Application server ▪ Communication server ▪ Outsourcing and backup management

(continued)

Table 3. Continued

Site	Operations	Environment	Equipment
Backup site **(Central site mirror)**	▪ Data management ▪ Administration ▪ Comparison 1:n and comparisons 1:1 ▪ IPK structure	▪ Secured premises ▪ Access to eGov ▪ Access to operator-supplied Telecom services ▪ Direct optic fiber connection to backup site ▪ Uninterruptible power supply	▪ Access control ▪ Generator ▪ UPS ▪ Air-conditioning ▪ Fire alarm and extinguishers ▪ AFIS/ABIS ▪ SGBD Server ▪ Application server ▪ Communication server ▪ Outsourcing and backup management
Prefectures	▪ Processing of applications for NIC ▪ Printing of birth certificates or copies	▪ Air-conditioned office ▪ Premises conditioning close to civil registers ▪ Access to eGov and/ or telephony operators desirable. ▪ Uninterruptible power supply	▪ Solar panel ▪ UPS ▪ Air-conditioning ▪ Enrollment kits connected to the central site ▪ Secure printer ▪ Safe
Police stations	▪ Handling of NIC applications ▪ NIC production	▪ Premises for registration of applications ▪ Premises for the productions of cards	▪ Solar cell panel ▪ UPS ▪ Air-conditioning ▪ Enrollment kits connected to the central site ▪ NIC printers ▪ Strong safe
Municipalities	▪ Registration of births (health personnel) ▪ Statement of births (Registry Office) ▪ Biometric enrollment (Registry Office) ▪ Notification of residency (Police/Registry Office) ▪ Declaration of deaths (Health personnel)	▪ Air-conditioned premises close to the civil status registers ▪ Access to eGov and/or phone operators desirable ▪ Uninterruptible power supply	▪ Solar panel ▪ Air-conditioning ▪ Enrollment kits connected to the central site ▪ Hardened biometric tablets ▪ Printer

Site	Operations	Environment	Equipment
Villages/ neighborhoods	▪ Registration of births (Health personnel/village head) ▪ Registration of deaths (Health personnel/village head)	▪ Access to a phone operator ▪ Electric power to charge the mobile phone	▪ Solar cell panel ▪ Hardened biometric tablets ▪ Counterfoil book (health or village)

The sizing parameters

The architecture of the proposed system must ensure that it is scalable:

- Base size (at least 15 million people);
- Daily flow of processed data (2,100 registered births, 2,100 births reported, 2,100 biometric records, 2,100 1:n searches, 720 deaths and 10,000 1:1 searches per day—the system must be able to develop by simple reconfiguration and adding hardware;
- Less than 10 seconds response time for a request for 1:1 comparison in the central system;
- On average 10 seconds or 1 minute maximum response time for a request for 1:1 comparison;
- The number of terminals connected simultaneously should be about 500 (we counted 1 kit by rural municipality and 3 kits by urban municipality, 12 training and stand-by kits).

These figures are scalable and depend on the use that will be made of the system. The system capacity can be increased by simply configuring and adding hardware. The system should not be dependent on a single supplier or a single technology. For this, we must ensure that the system supplied is neutral in relation to the provider and in relation to the technology.

The World Bank recommends a number of requirements to be included in the terms of reference that will help meet these criteria (see table below).

Table 4. Requirements for Suppliers

Requirement	Description
Scalability and open architecture	The solution must be built from modules or subsystems running specific tasks and having an open interface based with Service Oriented Architecture (SOA). The modules are specialized services that are easy to orchestrate in a global solution using a standard integration and upgradable architecture. **Applicable standards:** ▪ All communications between modules must follow safety and interface standards as defined in the ISO/IEC 7498 norms
Off-the-Shelf Components (COTS), scalability, reliability, availability	▪ The hardware and IT platform must be based on off-the-shelf modules; this includes servers, storage equipment and all communication (ICT) components ▪ Scalability: The system must be designed to achieve national coverage scheduled in the next 15 years simply by adding hardware and software ▪ Reliability: The system must be reliable with a high level of performance without interruptions due to malfunction ▪ Coverage: The system should cover urban and rural municipalities ▪ The supplier must ensure that each component can be obtained from two different dealers
Certification of biometric capture equipment	The biometric capture equipment must be certified for the quality of captured images and must have a standard interface to ensure plug-and-play interchangeability. **Applicable certifications:** ▪ US FBI Annex F for the 5:5:2 captors or their equivalent, the US NIST Profile 60 ▪ US NIST PIV for 1 finger capturing **Interfaces:** The Bio API ISO family (ISO/IEC 19784, 19785, 24702, 24708, 29141) standards
Biometric and identity data format	▪ Identity data must be consistent with internationally accepted standards for data exchange ▪ No portion of the data should have a proprietary format and all data must be accessible through standard protocols without provider intervention (read, search, export) ▪ The fingerprints must be stored as images in gray scale using the WSQ factor 15 compression ▪ The portraits comply with ICAO (ISO/IEC 19794) standard ▪ The portraits are stored in Jpeg format or jpeg2000 with a compression of a 20 to 24 ratio. They must be stored in raw format.

The selection of the biometrics provider

What characterizes the quality of a biometric search system is its accuracy, which is measured by the false acceptance rate (FAR) and false rejection rate (FRR). These rates are calculated for different suppliers in NIST organized benchmarks (MINEX, IREX and FRVT).

We must ensure that the provider is serious and that he participated in these tests. He needs not be the best, but he must offer correct results.

At any rate, the supplier must secure:

- A FAR and FRR for all types of research (1:n, 1:1);
- A response time (often providers give a number of comparisons per second and will not commit themselves to a response time).

We must also ensure that the supplier guarantees the treatment of juveniles. The systematic registration of juveniles is not planned but exceptional circumstances may require us to do so:

- Health crisis;
- Juvenile travel documents.

The National Identity Number

The national number is a key component of eID as it allows identifying the citizens and ensuring interoperability between all the systems that handle the citizens. It may not be based on the civil registry number as proposed in the draft National Identity Card/Civil Registry project:

- It is not universal because it is not systematically recorded in the Birth Certificates;
- There may be a doubt about the register ID in case of a registration in the transcript civil registry;
- The records of people born before independence are not available; a number of records have been lost;
- This number does not guarantee uniqueness unless the centenarians are automatically removed from the system.

We believe that the NIN should be assigned automatically by the system, either at birth registration by the medical staff, or at the time of the declaration of birth at the registry office.

A significant number based on the date and place of birth is appealing, but how does one do that to have it hold in 15 digits? We offer the following proposal TSMAAJJJCCCnnnRK:

- T = Guinean or Foreigner (1 or 2);
- S = Gender (F or M);
- M = Millennium (1 or 2);
- AA = 2 last digits of the year of birth;
- JJJ = day of the year;
- CCC = Municipality code conforms to the INS or country ISO code for Guineans born abroad or foreigners;
- nnn = order number;
- R = Region code (1 to 9 for Guineans born in Guinea, 0 for Guineans born abroad);
- K = control key.

This is only a proposal. The NIN number is essential and must be defined as early as possible in the life of the project.

Here are the requirements:

- It must be unique;
- It identifies the person for life;
- It must be universal and covers all the persons handled in the eID;
- It must have a maximum length of 15 characters + a key letter;
- It must be assigned automatically by the system, even if the recording is done offline.

There are several ways to tackle the problem of offline attribution:

- A NIN based on the identification of the registration system. This solution is risky because it is related to the configuration of the local system and a configuration error can have very serious consequences;
- The use of a temporary number related to the municipality code and the date and time of the recording RCCCAAAAMMJJhhmmssccK:
  - R = Region;
  - CCC = Municipality or country code;
  - AAAAMMJJ = Registration date (AAAA = Year, MM = Month, JJ = Day);
  - hhmmssccc = Registration time (hh = hour of registration, mm = minute of registration, ss = seconds, ccc = hundredth of a second);

  The probability of having a duplicate is very low for a municipality with 3 kits. The probability of collision is <1/100,000) and the consequences are less serious than that of a duplicate NIN—the system can deal with this risk by processing the exception;
- Assigning a NIN when recording in the central system. If the registrant has not received its registration, the number will be searched by a query about the town, date and time of birth. It ensures unicity but it means that the NIN cannot be attributed when the terminal is not connected and a temporary identifier must be given.

This operation is very delicate and all possible scenarios must be considered when specifying the system:

- The place of birth is covered or not covered by a network to enable registration of the birth;
- The Municipality where the declaration is made may or may not be connected to the central system.

System initialization

Two solutions are possible:

- The general census;
- The use of the Electoral Commission file and a gradual construction of a comprehensive file based on declarations.

The general census

We rejected the idea of a general census.

It is too costly to realize especially if we must rebuild all the missing civil registers.

It requires:

- the participation of magistrates for those who do not have identity through the organization of public hearings;
- the involvement of the registry office;
- cooperation of the general public;
- organizing a census with over 5,000 agents and 5,000 kits—this is a much more difficult operation to organize that an electoral census or an economic census;
- at least 6 months of census during which the crucial issue of birth registration is not resolved;
- risks of errors or drift over time are huge.

In addition, this lies beyond the eID task limited to person identity. In case this option is chosen, we advocate a progressive approach:

- Using an existing system as the base (CENI or eID);
- Registration of new declaration with printing of the certificates on security paper—this guarantees the future;
- Registration upon request of the former documents with issuance of a secured copy, for people producing the originals after checking the relevant register—this makes possible rebuilding the past records.

Initialize the eID using the Electoral Commission Database

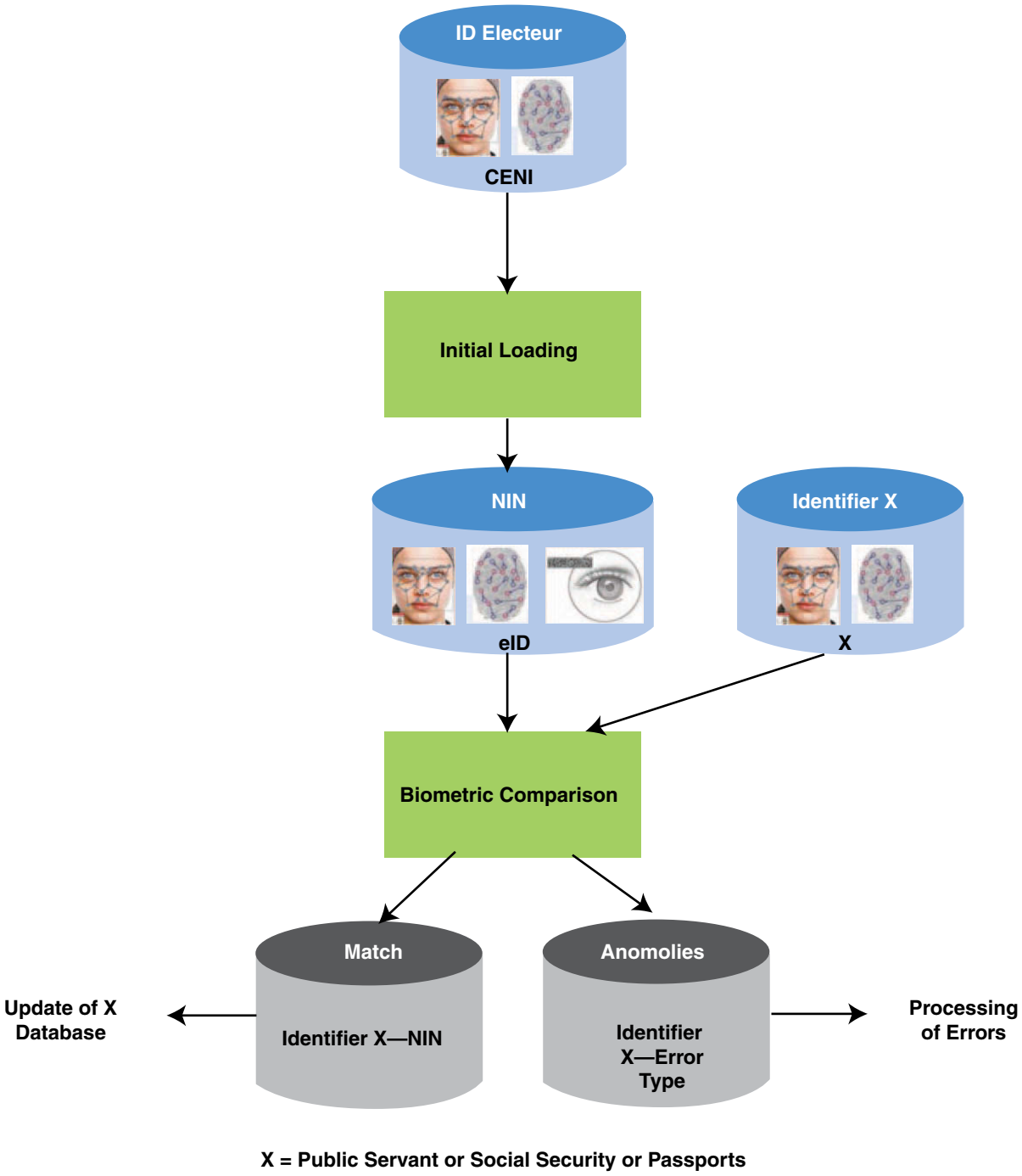
This is the solution we recommend for the following reasons:

- Over 90% of adults are recorded in the Electoral Commission Database with a good degree of reliance on the data;
- Celerity in the implementation—the only prerequisites are linked to time required for the installation of the system;
- As soon as the system is operational, the newborn infants can be registered in the eID; the only prerequisites are:
  - The system has been delivered and installed;
  - The data migration has been effected;
  - Staff training and recruitment have been completed;

  Concerning initialization, we recommend the use of the Electoral Commission data to initialize the eID data with:
  - a NIN computed using the birth date and birth location contained in the Electoral Commission database;
  - the demographic data of the Electoral Commission Database;
  - the voter identifier;
  - the biometric data;
  - the templates might have to be re-extracted during migration (coding), the NFIQ quality must be assessed for fingerprints and the ICAO quality for portraits; this will give a good idea of the quality of the initial base; the citizen with poor quality portrait or fingerprint can be marked to force a biometric re-enrollment at their next visit to eID;

  The eID file can then be compared to other existing biometric files. This comparison will provide a list of errors to be processed and a list of correspondence to update the existing files with the NIN.

Figure 14: Initialization and Updating of Existing Databases



Existing file update

This initialization is an opportunity to validate the existing biometric files (passports, civil servants, Social Security).

The comparison can be done at any level (demographic/biometric data). A list of differences would be generated for each file.

A commission must make a decision on each encountered error (a process similar to the one that was implemented by the Public Service Ministry) with the following possible conclusions:

- the person is not enrolled in the eID, he must obtain a NIN and get registered;
- an error to be corrected either in the eID or the compared file;
- a case of fraud—the fraudster to be sued to court;

The Social Security, Civil Service, Pay Department and Passport files must be updated with the NIN (a field to be added to the existing files).

Interoperability

Link with the Civil Registry

The registry office plays a key role, since any operation affecting the identity of a person must be registered in a civil registry before registration in the eID. Any update of eID must refer to the registry identification.

- Must we record in the system the civil registries to avoid transcription errors when registering the birth declarations?
- Should the data stored in the eID be checked?
- Can we show the NIN in the birth certificate if the option of producing the birth certificates by the eID system is chosen?
- Is it possible to re-transcript the NIN in the civil registry after eID registration?

  From a practical standpoint, this could be useful, as the NIN could be officially transmitted to the person concerned. But would this be legal? What would happen in the event of a transcription error?

The link with the health system

We have given preference to registration of the births in the eID before declaring them at the Registry but this depends on:

- Phone coverage;
- Training of health staff and village heads;
- Motivation.

The system could assign a provisional number upon the registration of birth and send an SMS to those concerned. As the use of mobile is not yet universal, this might be the source of problems.

In any case, we must be able to establish a link between birth registration and the declaration at Registry Office.

Once the NIN is assigned, the health system will use this number to monitor a citizen's health throughout his life until the suggestion of death.

The link with existing systems

The NIN must be used universally.

For all systems that deal with people, this requires a modification of existing systems and recording of the NIN in the system.

We have seen the approach that was recommended for existing biometric files (the Electoral System, the Civil Service system, the passport system, and the Social Security System); biometrics can help do the reconciliation and make that link effective.

For others, it should be considered case by case.

In all instances a citizen may apply for a NIN either from his voting card ID, or from the provisional number, or after a 1:n search in the eID.

New services

The eID should provide standard interfaces for all types of request:

- Identification;
- Biometric authentication;
- Application for a certificate;
- PIN based identity control;
- Certificate based identity control.

Trust, privacy and security

Trust

Trust is based on a set of requirements summarized in the table below.

Table 5. Trust-Related Requirements

Requirement	Response
Data integrity	The solution should be such as to ensure that data is correctly acquired and cannot be altered or manipulated during transmission. **Measures to take:** ▪ Controls during capture—finger and portrait quality is automatically controlled during capture. The system must calculate the NFIQ note and ICAO compliance for portraits. The system must ensure that there is no reverse or double hand. The 4:4:2 entry limits the number of fraudulent practices than could be done on the fingers. ▪ Statistics are kept on the quality for detecting operators who do not do their job properly and address the problem. ▪ Any transfer of data should be encrypted (USB key or network transmission (https). ▪ The operators do not have access to the local databases. ▪ All transactions are signed and composted. ▪ At the time of delivery of the document, quality control should be effected to check that the recipient can be biometrically authenticated using the document. ▪ The accuracy of matching must be guaranteed by the MINEX benchmarks. The Civil Registry data matching against data from the eID will give a good idea of the system accuracy (FAR and FRR).

Requirement	Response
Reliable documents and certificates	▪ Documents that are very difficult to copy. The documents are numbered and their use is monitored: identity papers including biometric data that allow to authenticate a person. ▪ Asymmetric encryption and certificate management in a public key infrastructure.
Secure Identity	▪ 1:1 authentication with False Identification rate <100,000 (very difficult to prove)
Fight against fraud	▪ Registration at birth ▪ All operations are traced ▪ Recording of vital data modifying events are entered by the eID staff and validated by the Registry Office personnel ▪ Identification of the guilty in cases of proven fraud (the system identifies those responsible) and severe deterring action (imprisonment and heavy fine)
Data protection and security	▪ The data usage rules perfectly defined and applied to the system ▪ Material security of data centers (access control, intruder alarms) ▪ Security against hacking ▪ Systematic data encryption during the transfer ▪ Access to the system is monitored and limited to authorized persons only ▪ Systematic control of persons (identity, use of mobile phones, laptops, USB keys) ▪ Safety rules clearly defined and fully applied

Protection of privacy

The system contains data that are private in nature and misuse of them may worry the citizen:

- The enrollment data:

  This is private data and some people may be anxious at the thought of this data being made public;

  This data is strictly private and persons handling them are required to be licensed and know their duty of restraint. Any breach of this rule shall be punished by law (see legal framework to be put in place);

  As the kits operate in connected or disconnected mode, they must contain local databases. Several precautions must be taken to prevent such data from being the subject of piracy:

  - Encrypting of the local database;
  - Operation in kiosk mode (no access to the system for operators);
  - During maintenance with return to the supplier, the maintenance procedure should help ensure that the supplier does not have access to the data in the local database.

  This data can be pirated during transmission; all data should be encrypted regardless of the transmission mode (asymmetric encryption).
- Central database with data from the entire population:
  - The central database must be especially protected against malicious intrusions;
  - Accreditation required for all persons accessing the central site;
  - Very strict security policy (minimum length password with regular changes);

- Prohibition to have unapproved equipment connected;
- Encryption of data exchanged with other parties;
- Encryption of central base data;
- Installation of a DMZ.

- The widespread use of the NIN allows access to many records belonging to one person (the objective). In particular, consultation of the records helps to establish links that may infringe on privacy. Two basic rights must make this intrusion acceptable:
  - The right to inspect—a person must be able to know all the data stored in the system regarding his NIN on simple request;
  - The right to oblivion—data must be erased from the system depending on their nature.

Security

The system security is based on a number of basic principles that are covered by the ISO/IEC 7498-2 Standard.

- Authentication:

  For stations with fingerprint capture equipment, access to the station will be protected by a biometric login ensuring operator authentication and limiting the functions to which he will have access depending on his profile;
- Authentication of all data transmitted through the network or file transfer will be guaranteed by an electronic signature linked to the data.
- Access rights:
  - The system must be based on a control of access rights which, depending on the user's profile, allows them access to different features:
    - Birth registration;
    - Registration of birth statements;
    - Biometric enrollment;
    - Recording of address changes;
    - Demographic statistics, health, data quality, system operation;
    - Consultation;
    - Administration.
- Data integrity:

  A number of mechanisms should be implemented to ensure data integrity:
  - Data encryption using private keys;
  - Data confidentiality;
  - No repudiation.

The financial aspects

System acquisition cost

Three scenarios are possible:

- The system does not include the production of documents;
- The system includes the production of national identity;
- The systems includes the production of birth certificates.

System acquisition cost without the document production

It is assumed that the premises are available and only need fitting:

- Central site and Administration;
- Backup site;
- A secure space is available in each municipality to install the enrollment kit with its solar panel.

The cost of acquisition covers the following items:

- Central site layout:
  - Offices (2):
    Furniture,
    Air-conditioning,
    UPS,
    Regular power supply,
    Network wiring (2 outlets);
  - Administrator's office:
    2 desks with chairs,
    Air-conditioning,
    UPS,
    Regular power supply,
    Network wiring (4 outlets), connected to the central system,
    2 PC,
    2 black and white laser printers,
    Access control;
  - Training room (10 posts):
    Furniture (12 tables and chairs),
    Air-conditioning,
    UPS,
    Regular power supply,
    Network wiring (12 outlets) connected to the training system,
    Projection screen,

Video projector (1),
10 training kits;

- Meeting room (10 persons):
  Furniture (10 tables and chairs),
  Air-conditioning,
  UPS,
  Regular power supply,
  Network wiring (2 outlets),
  Projection screen,
  Video projector (1);
- Data center:
  Access control,
  Raised floor,
  Fire alarm and extinguishers,
  System-controlled air-conditioning,
  System controlled UPS (30 KVA),
  Generator (40 KVA);
- Engine room equipment:
  Database management system with a 10 terabyte storage rack,
  Backup system with backup robot data outsourcing,
  Application server,
  Communication server,
  Mail server,
  ABIS,
  Public Key Infrastructure;

- Licenses associated with the COTS and the system;
- Services associated with the implementation (generally estimated at 10,000 hours):
  - Project management,
  - System specification,
  - System customization,
  - Integration and testing,
  - Installation and configuration,
  - Migration,
  - Validation and acceptance tests,
  - Training,
  - Deployment,
  - Start-up support.

National Identity Card production—cost of acquisition

- The costs to be included are, for each item, licensing costs, the piloting system and the printer. Fitting out of premises and furniture;
- Antitheft cabinet for storing blank cards and cards waiting to be delivered;
- Application recording and card production kit;
- Printing system;
- Installation and testing;
- Acceptance.

Birth certificate production—cost of acquisition

The costs to be included for each item are the license, the piloting system and the printer:

- Fitting out of the premises and furniture;
- Safe for storing blank cards and cards waiting to be delivered;
- Printing system;
- Installation and testing;
- Acceptance.

Operating costs

There are 3 possible scenarios:

- The system does not include the production of documents;
- The system includes production of National Identity Cards;
- The system includes the production of birth certificates.

Operating costs excluding the production of documents

Here are only included the costs directly related to operations not including the agency running costs:

- System management:

  Initially, the only customer is the administration; in this context, two system administrators must be provided who will monitor the system and perform administrative tasks during business hours; eventually the administration and supervision will be provided on a 7d/7d. 24h/24h basis. This can only be considered if the service expands. In this case, such a service would require five system administrators;
- Central system maintenance and support:

  Will be ensured by the system supplier. We assumed that the service consist of 8 hours per working day with two hours response time;

  The same observation applies to the administrators, this service should eventually be extended to 24 hours a day/7 days a week.

- Local sites maintenance and support:

  This concerns mainly the support and maintenance of kits and mobile applications;

  The supplier must have an open support service to business hours 5d/5d. . . . This service must answer the calls within 2 hours and resolve a fault that need repair within 24 business hours after the call. This means the supplier should have backup stocks in the prefectures with a person ready to intervene.
- Use of the kits:

  We recommend subcontracting the operation of the kits to the supplier. This is the guarantee of the proper use of the system. This means that the supplier must provide 400 operators with supervisors in each prefecture.

Cost of production of National Identity Cards

In the event that the production of the National Identity Card would be the responsibility of the agency, the cost should include:

- The supply of cards:
  - The supplier shall provide cards to each of the production sites;
- The cost of consumables;
- Production system maintenance and support;
- The supplier must have a service open 5 business days a week. . . . This service must answer the calls within 2 hours and resolve a fault that needs repair within 24 business hours after the call. This means the supplier should have backup stocks in the prefectures with a person ready to intervene.

Financing the operation

To be sustainable, the system must have income. This income cannot come from birth declarations that we must seek to encourage. Identity is a right for all including the poorest. We must therefore rely on the other services:

- Applications related to Identity documents for a fee (National Identity Card, driving license, birth certificates and copies of birth certificates);
- Applications for digital certificates for a fee;
- Identification and authentication for a fee;
- Generation of the revised voters' lists (number of revisions);
- Residency update applications.

We made a simulation on income only from authentications and identifications, ensuring that operations related to the registration of deaths and birth are free of charge.

This yields an annual income of 7.5 billion francs of which 2.7 billion Guinean francs relate electoral reviews.

These earnings can be easily doubled or tripled if identity document production is included.

Table 6. Returns of the Agency

Transaction	Nb./day	Rate	Income/Day	Income/Year
ID Card authentications	2,160	10,000	21,600,000	4,320,000,000
Residency authentications	500	5,000	2,500,000	500,000,000
Fee-charging authentications	0	10,000	0	0
Free authentications	4,320	0	0	0
Fee-charging Identifications	0	0	0	0
Free identifications	2,160	0	0	0
Birth registrations	2,100	0	0	0
Registration of deaths	576	0	0	0
NIC revisions	2,660	5,000	13,300,000	2,660,000,000
Total income			**37,400,000**	**7,480,000,000**

Operational processes and controls

Compliance with law

The agency shall operate in compliance with the law:

- Compliance with the fundamental right of all to an identity without preferential treatment;
- Respect for confidentiality and privacy without misuse of the data contained in the national identity register.

The agency shall ensure that these principles are respected and shall penalize heavily any breach.

To this end internal rules shall be respected and regular audits should be conducted to ensure that they are respected.

Fraud and cyber crime control

The agency shall protect itself from fraud internally and face attacks from the outside.

In this regard a number of precautions have to be taken in relation to both the employees, the suppliers and the protection of the system:

- The employees or the supplier's staff selected to work on the system must be accredited;
- Employees must be made aware of the risk and should know the penalties in case of an offence;
- The implemented procedures should limit the risk of collusion:
  - Applicants authentication;
  - The control of the documents compliance is to be carried out by independent persons;
  - Authentication when handing documents;

- Separation of roles:
  - Enrollment;
  - Check;
  - Receiving INEC applications;
  - Production;
  - Issuance;
- Every access to the system must be protected by a biometric login through which a user can use only the functions authorized by his profile;
- The system shall be protected against intrusion risk;
- The System shall be protected by a DMZ and a double firewall;
- The exchanged data shall be encrypted and signed for origin guarantee;
- Time-stamped data using checksum.

To deal with the system misuse, all decisions shall be stored in a system history that cannot be changed without this being detected by the system.

When fraud is detected, every step shall be taken to determine its origin and to ensure it does not happen again by amending the procedure and punishing the briber and the corrupt.

Service continuity

The service provided by the eID may not experience prolonged interruption. Measures must be taken to ensure continuity of service even in case of disaster.

A disaster plan should be developed which should include the return to normal.

To be effective this plan should be repeated once or twice per year without disrupting the normal operation of the system.

In all cases the system must be covered by a service contract based on a maintenance plan.

A hotline must be implemented with an escalation procedure. This shall be specified in the system maintenance plan. Global and partial unavailability rates shall be assessed and reviewed regularly with the supplier. Serviceability failure can result in penalties being imposed on the supplier.

Financial assessment and system efficiency

eID cannot operate without a sound financial footing.

eID's revenue is generated by the services provided. Therefore, the system will have to automatically generate operating statistics to assess:

- The services provided and the associated revenues:

  The produced reports shall be used:
  - by the agency's Accounting Department to reconcile with bank statements;
  - by the Finance Committee to ensure that the agency is properly funded;

- The service efficiency (response time and downtime):

  Statements produced shall be used by the administrator to ensure that the system performs properly and that the down time falls within contractual agreed limits. Failing that, penalties shall be imposed on the supplier.

Service relevance and adaptation

Measures shall be taken to ensure that the service is used and promoted properly. This is the Policy Committee's duty.

Two tools shall be provided including:

- The quality of the stored data:

  The administrator must provide statistics on the quality of stored data. If the biometric data is not correct (poor quality, number of missing fingers too large), the system will not render the service expected, and it is important to alert managers and the Steering Committee promptly so as to correct the problem at the earliest.
- Performance statistics:

  Operating statistics help to insure that the objectives in terms of the system performance are achieved:

  - Number of registered births;
  - Number of biometric enrollments;
  - Number of authentications.

If the targets are not achieved, the Directive Committee shall be informed and campaigns shall be undertaken to promote the system.

In addition, to promote the system, new services for new uses must be defined. It is the role of the Policy Committee to establish them and manage the changes.

The changes conform to the standard project cycle management:

- Budget and planning;
- Specification;
- Development;
- Acceptance;
- Commissioning.

Controls to be implemented

The agency operations and support functions

Table 7. Agency Controls

Category	Controls Description
Operational Governance	This concerns the various policies to be implemented at the agency: ▪ Information Security Policy ▪ Privacy Policy ▪ Human Resources Management Policy ▪ Information System Policy Management ▪ Disaster Plan and Business Continuity ▪ Information retention policy ▪ Communication and acknowledgement by employees of the policy
Human Resources	All employees participating in the eID shall be accredited. This includes the control of their past and the assurance that they have no criminal history.
Service Provider Control	Ensure that the service provider can deliver the requested service with all the guarantees required. ISO 9001 certification by the local representative in the areas associated with the eID constitutes a guarantee that the service can be provided locally.
Change Management	Ensure that the procedures for implementing change do exist and they do not cause a disruption of the service. In this regard, ISO/IEC 200000 standard recommendations standards for IT service management shall serve as a basis.
Audit	Regular audits shall be carried out to ensure that the law and internal policies are properly applied. The audit results shall be published to reassure the public.
Communication	Information campaigns and training for the general public shall be conducted regularly to promote the eID. The staff shall undergo regular training internally to ensure that the agency's policies in terms of confidentiality and security are understood and applied.
Security and Privacy	**Control procedures to prevent unauthorized persons entry:** ▪ Perfectly defined policy of access to the system (user profiles, limited time, password, biometric login, access to the profile dependent functions) ▪ Segregation of duties for the issuance of identity or Identity Documents for the purpose of fighting collusion ▪ Systematic logging of all operations to facilitate investigations and to limit fraud through its deterrent effect with exemplary punishment in return ▪ Consultations limited to public data

Category	Controls Description
Operational Resilience	▪ Systematic service redundancy ▪ Degraded mode in case of failure ▪ Preventive maintenance plan ▪ Regular and controlled database backup ▪ Integrated measurement of the system serviceability ▪ Setting up a disaster plan and verification of its operation

Identity management controls

Table 8. Identity Management Controls

Category	Control Description
Registration	▪ Birth records control for declarations of births ▪ Civil Status control for the issuance of NIN ▪ Parents authentication for nonregistered minors ▪ Guarantors authentication for nonregistered adults ▪ Identification following biometric registration ▪ Verification of a potential duplicate and decision making
Issuance	▪ Applicant authentication ▪ Documents check ▪ Issuance of documents ▪ Applicant authentication when handing document
Authentication	This service is the most commonly used and it is: ▪ Either offline through comparing the document biometric data with the person's data; ▪ Or online through comparing the person's data with the data of the person registered in the system and identified by his NIN.
Update	This applies to the updates for identity and address data rectification ▪ The person should be authenticated ▪ Controlled supporting documents (civil status, certificate of residence)

5. Implementation plan

Diagnosis

A diagnosis was carried out. Cf. Guinée eID—An Analysis of the Current Situation.

Establishment of a steering committee

This is the current phase.

It is aimed at:

- Identifying stakeholders;
- Defining an eID scope;
- Defining an implementation strategy;
- Appointing the Steering Committee members who shall represent all stakeholders;
- Appointing a project manager who shall coordinate all subsequent activities and who shall report to the Steering Committee.

Implementation of the legal and regulatory environment

This is a key operation because it provides the eID with a legal framework.

It is aimed at revising existing laws in order to adapt them to the new eID uses and to create a digital identity code together with its use.

This could be done in two steps:

- Preparation of draft revisions—Civil Code, Electoral Code and Children's Code—and the creation of a Digital Identity Code;
- Implementation of the amended laws.

For this step, the project will require the assistance of legal experts well conversant with the existing laws and digital identity problems.

Strategy definition

Stakeholders shall agree on the strategy to be implemented. For example:

- Using the Electoral File as a starting point with automatic NIN allocation;
- Registration of new births when the system starts and allocation of a NIN to the newborns;

- Production of birth certificates by the system;
- NIN allocation on request for the nonregistered persons in the system;
- Biometric enrollment of youth from 16;
- Production of identity cards for persons registered in the system;
- Death registration.

The above strategy ensures that eID gives everyone a right to an identity and that the system can be implemented almost immediately.

This step is conducted by the project manager and requires an active involvement of the Steering Committee. A consensus of the Steering Committee shall be required.

Setting up a project framework

A Project Manager shall be appointed and his duties properly defined:

- He is the coordinator of all the activities;
- He is responsible for planning and monitoring of activities;
- He reports to the Steering Committee.

Establishment of the institutional environment

The Institutional Environment must be defined with the participation of the various associated committees including:

- The National Identity Agency with its duties and mission;
- The Associated Committees—their composition, duties and mission.

Funding

The funding option shall be defined together with the amounts involved including the appropriation budget and the operating budget and concerns:

- The State Budget;
- Loans;
- Build Operate Transfer (BOT) Concession;
- Self-financing for the operating costs portion or government partial funding.

The project manager is the main actor of this step relating to the assessment of the implementation and operating costs. The decision on the funding options shall be based on the costs assessment. This may be the responsibility of the Finance Committee. The Steering organ shall make the final decision.

Defining the use of the system

This includes:

- The role of the eID in each of the uses;
- The definition of the main processes:
  Birth registration;
  Enrollment of 16-year old youth;
  Late registrations;
- Definition of standard interfaces to ensure interoperability.

Implementation of a communication plan

The communication plan helps to:

- promote the eID;
- ensure transparent implementation of operations (e.g., dedicated WEB site);
- allows citizens to express their opinion about the system.

The selection of a supplier

The selection of a supplier follows the usual rules including the:

- Drafting of the terms of reference
- Calling for tenders
- Opening of bids and supplier selection
- Contract

The supplier is absolutely required to have a permanent local representation which undertakes to provide the contractual services during the 15-year life of the system. This can be guaranteed in several ways:

- He already has references in Guinea
- He has established a structure in Guinea which is not an empty shell
- His services not relating to hardware providing must be done in Guinée

The system implementation

The project plan

The supplier provides a project plan including:

- Communication rules;
- A delivery schedule with a list of deliverables:
  Infrastructure;
  Acceptance testing plans;

Hardware and software;

Documentation:

- Specification;
- Installation plan;
- Acceptance testing plans;
- Training Plan;
- Deployment Plan;
- Support and Maintenance Plan;
- Operating Plan for the sites where he is in charge of operation;
- Disaster Plan;
- Administration Guide;
- User Guide (Kit, card printing, document printing);
- Diagnostics (Kit, card printing, document printing);

Training:

- eID for policymakers;
- Central Site Administration and Trouble Shooting;
- Kit End User;
- Kit Administration and Trouble Shooting;
- Printing Systems Administration and Trouble Shooting;
- Card Printing Management;
- Birth Certificate Printing Management.

Startup Support

Specifications

The supplier shall specify the provided system.

Specifications shall conform to the terms of reference and shall indicate the:

- system performance (accuracy, response time);
- details of the system architecture;
- data structure;
- workflows reflecting the process defined in the terms of reference;
- man-machine interfaces for each function;
- administration functions;
- reports and statistics;
- interfaces with external systems (protocol, message format).

The infrastructure installation

Should comply with the terms of reference and acceptance testing.

The system customization

The customized system is to comply with the acceptance testing.

Operator selection and training

The supplier shall recruit and train operators. The selected operators must be accredited and undergo a morale survey.

The system initialization

The system must be loaded with Electoral Database data.

The loaded system shall be subject to an acceptance testing which includes:

- Data control (global statistics and control of a sample);
- Data Quality Report printing;
- Authentication test on a set of a persons who have been loaded;
- Identification test on a set of a persons who have been loaded.

The Central System delivery

The Central System shall be subject to acceptance testing which will include:

- An inventory;
- An inventory of the delivered documentation;
- A comprehensive functional test;
- A test of the backup system including the simulation of a disaster and the return to normal operations.

Remote site deployment

The remote site deployment shall be based on a deployment plan.

The implementation at each individual sites includes:

- Installation;
- An inventory of the installed equipment;
- An acceptance test with a functional test;
- The site shall become operational following the signing of the acceptance test Protocol.

The system commissioning

The system shall be declared operational when the central site is installed and all remote sites are operational. The support and maintenance contract shall be implemented in accordance with the Maintenance and Support Plan to be approved.

Maintenance and support

The Administrator shall trace all incidents and their resolution in respect of the:

- Time of call
- Telephone number
- Description of the problem
- Problem analysis
- Problem resolution or workaround
- Date and time of the resolution
- Impact on the system and downtime

Maintenance meetings shall be held once a month with the supplier for the purpose of addressing problems and their impact on the system.

The meetings shall facilitate major servicing planning including changes.

Every change shall be subject to testing that will include the following:

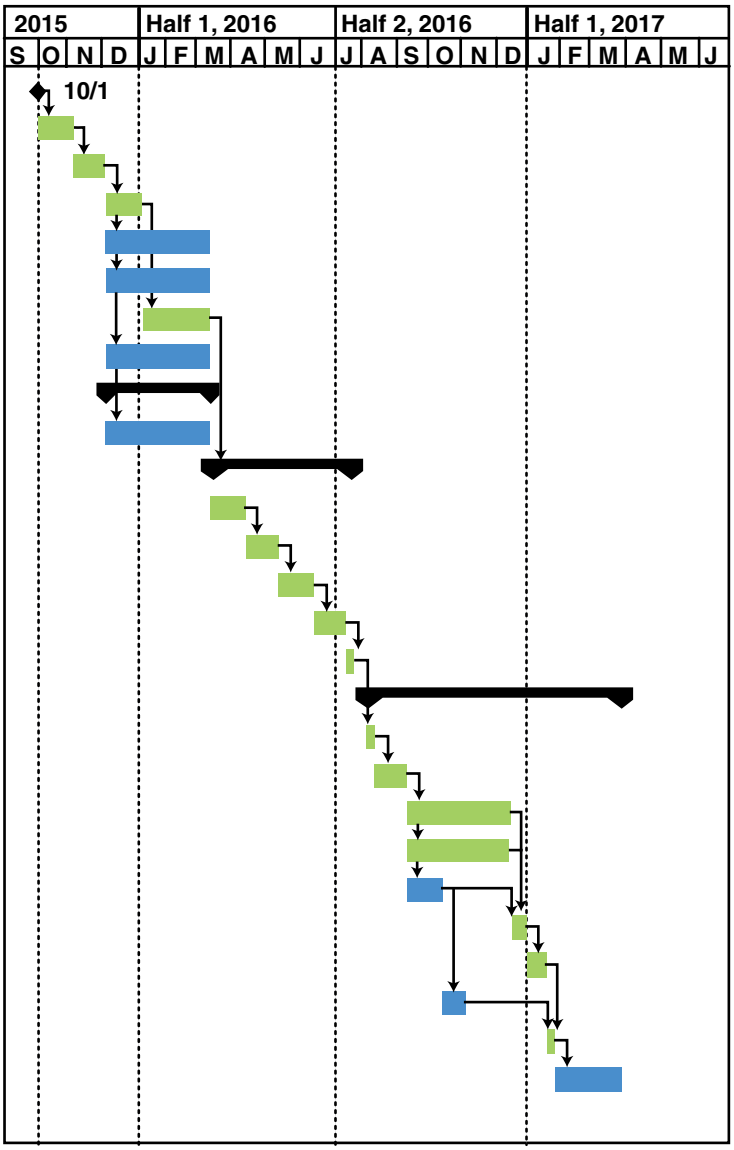
- the installation of changes;
- the adjustment or new functionality testing;
- nonregression testing.

Work schedule

Work can be planned as follows:

Figure 15: Implementation Planning

Name	Duration
TO	0 day
Steering Committee Appointment	20 day
Project Organization	20 day
Strategy Definition	20 day
Institutional Framework Definition	60 day
Project Funding	60 day
System Use	40 day
Communication Plan	60 day
Law Modification	60 day
Preparation	60 day
Provider Selection	85 day
Redaction of the Terms of Reference	20 day
Tender	20 day
Tender Responses	20 day
Processing of the Answers	20 day
Contract	5 day
Implementation	150 day
Project Plan	5 day
System Specification	20 day
Infrastructure Preparation	60 day
Personalization	60 day
Delivery	20 day
Central Installation	10 day
CENI Migration	10 day
Training	15 day
Acceptance	5 day
Deployment	**40 day**



Annex 1: Identity basic principles

Identity and trust

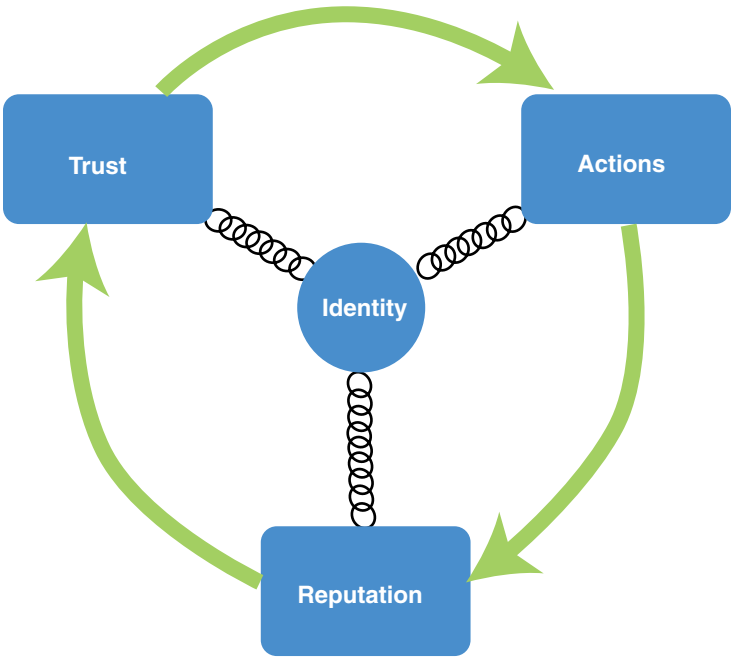
Identity is what connects a person to his reputation. Based on this reputation, confidence level is determined. The confidence level enables him to act, which in turn increases his reputation.

The data

The identity of a person is based on three types of data:

- The biographical data (Name, First Name, Date of Birth, Place of Birth, Father's Name, Mother's Name, Civil Status Number);
- The supporting documents (documents proving that the biographical data is correct);
- The biometric data (Physical appearance, Fingerprint, Iris) they allow to uniquely identify a person.

Figure 16: Identity and Trust



This dataset does not guarantee the identity of a person; and there are major risks involved at the time of registration in the system:

- A person may use false supporting documents or true false supporting documents (true documents based on false declaration);
- The recording officer does not perform the requisite checks;
- A person may use another person's data (identity theft).

For the system to be credible, it is important to ensure a maximum level of trust at the enrollment phase.

Four cases are worth considering:

- The person is registered in the system at birth:

  Registration in the eID at birth should eliminate the risk of the use of a false document. The identity theft remains a risk at the time of biometric enrollment, which cannot be done at birth. We must take for this operation every precaution to increase the level of confidence (authentication of the legal representative or guarantor);
- The person is a voter:

  He or she can be authenticated through the biometric data of the electoral roll;
- The person is not a voter; he/she has proof of identity but is not in the eID system:

  The supporting documents must be submitted in the presence of a witness (guarantor or legal representative for minors) and the witness is authenticated;
- The person is not a voter and has no supporting document:

  A court judgment or its equivalent after review of the law must be issued; the judgment shall be recorded in the register of transcripts of the birthplace—the transcript is the responsibility of the registrar and binding on him—the decision is recorded in the eID; a declaration receipt must be given; the person is registered in the eID system.

In all the cases, the image of the supporting documents that is used for the enrollment must be stored in the system; all transactions must be signed, composted and logged in the system. In the event of proven fraud, this will help identify and prosecute the fraudsters.

The identification function

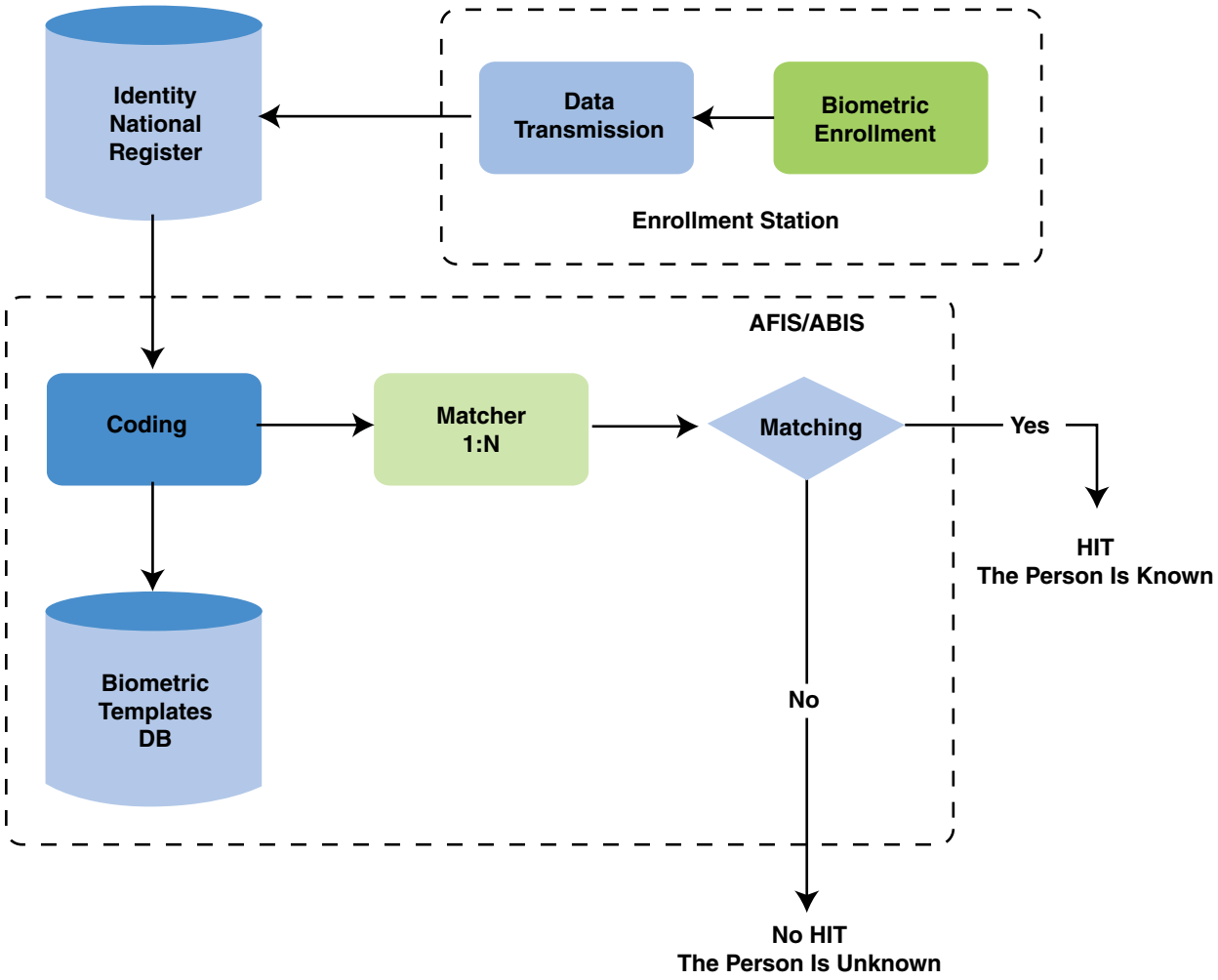
This function allows with near certainty a person's identification based on biometric data recorded in the system.

It is used during the first biometric enrollment, to ensure that the person is not already registered. The biographic data of the person to be identified is compared to the biometric data of all the persons in the database (comparison 1:n).

The probability of nonidentification (FRR—False Rejection Rate), depends on the quality of data and the performance of the technology used.

In the event that the answer is positive (HIT), the probability of false identification FAR (False Acceptance Rate) is very low; however, the result must be confirmed by an expert who, given all the data available, shall make a decision.

Figure 17: The Identification Process



The authentication function

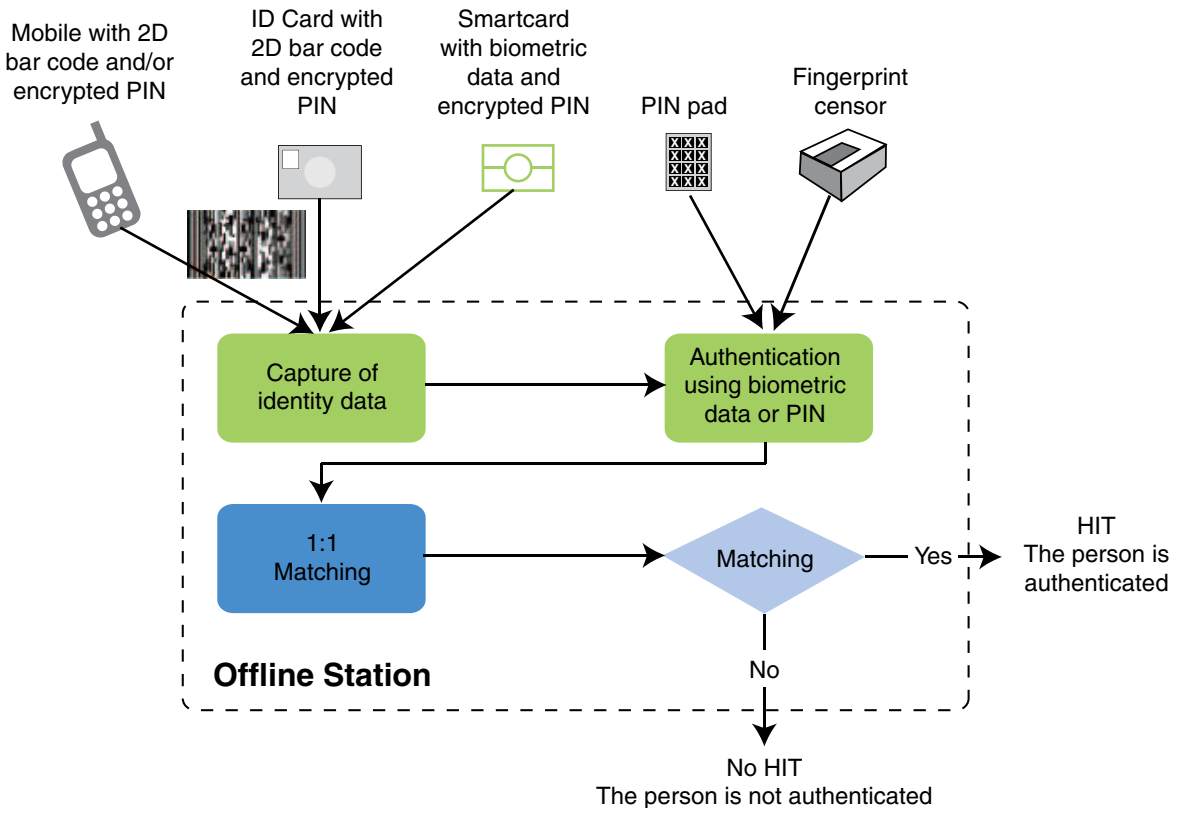
This function ensures that a person corresponds to the identity documents provided by the person to authenticate.

It is used when the person is known by the system—his identity number is known and we must ensure that it corresponds to that identity.

The biometric data of the person to be identified is used to compare the person to identify with the data of the database or those of the biometric document (comparison 1:1).

In the event of identification (HIT), the trust level must be very high. It depends on the technology provider. The rate of false HITs (false identification) must be below 1/100,000.

Figure 18: The Offline Mode—Authentication Function



In case of nonauthentication (No. HIT), the trust that we can give the result depends on the quality of the fingerprinting and the delivery procedure of the biometric document that should help ensure that the data in the biometric document is correct.

In offline mode, authentication is carried out locally using the supporting documents containing the PIN or biometric data.

In online mode, the NIN identification data and image fingerprints are sent to the central site where a 1:1 comparison is made. The result is sent back to the remote application. Another solution would be to extract the templates and make the 1:1 comparison locally—this is more difficult to implement on a mobile client and raises the issue of associated licenses.

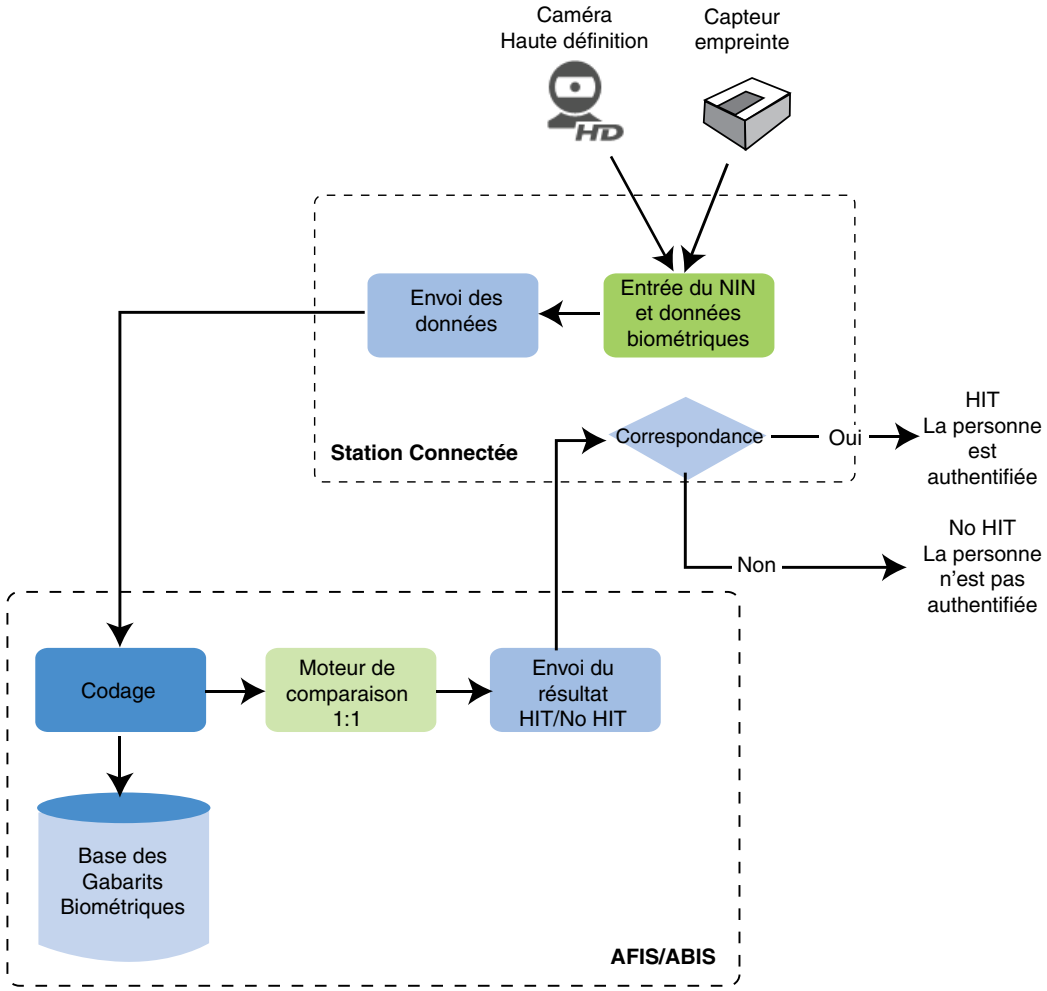
The juvenile issue

In the event of biometrics being based on the fingerprint, we must understand that the prints change in size when growing. A simple comparison of an adult fingerprint and a juvenile fingerprint will not detect a match.

If the proposed system should handle juveniles, the technology provider must take this need into account.

In general we recommend biometric enrollment to begin at the age of 16 years before issuing the first identity card.

Figure 19: The Offline Mode—Authentication Function



The problem of poor quality fingerprints

Registration of poor quality fingerprints can downgrade the overall accuracy of the system because it adds noise (a good candidate can be hidden by a multitude of false candidates).

To address this problem, we make the following recommendations:

- Make an immediate control of the quality of fingerprinting and not allow the recording of poor quality fingerprints;
- Include facial recognition in the system. This allows the system to exclude the fingerprints of very poor quality while enabling the identification or authentication of individuals with very poor quality or lack of fingerprints;
- Properly train the operators;
- Conduct regular statistics on the quality of the fingerprints in the database and those of persons with missing or too poor quality fingers recorded in the database; these statistics can be made for each operator allowing the correction of bad practices.

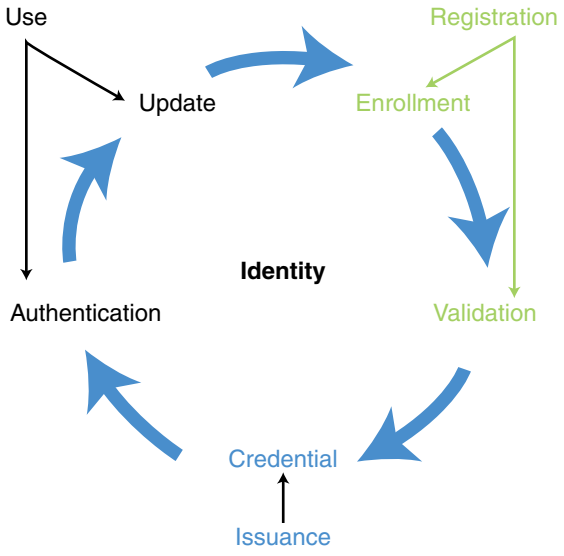
The accuracy of face recognition is poorer than that of fingerprints, but is better than recording bad fingerprints. At any rate, this should be an exceptional procedure and the operators must be properly trained so that the fingerprinting is done properly.

The identity life cycle

The identity follows a cyclical process consisting of three phases:

- Registration:
  Registration is to be done according to the following cycles:
  - Birth registration;
  - Biometric registration;
  - Update recording (court decision, application for National Identity Card);
  - Registration of deaths;
- Certification which includes:
  - Authentication of the guarantor;
  - Identification for the initial biometric enrollment (Research 1:n);
  - Control of application related documents;
  - Issuing of documents;
  - Birth certificate;
  - National Identity Card;
- Use;
- Authentication;
- Updating.

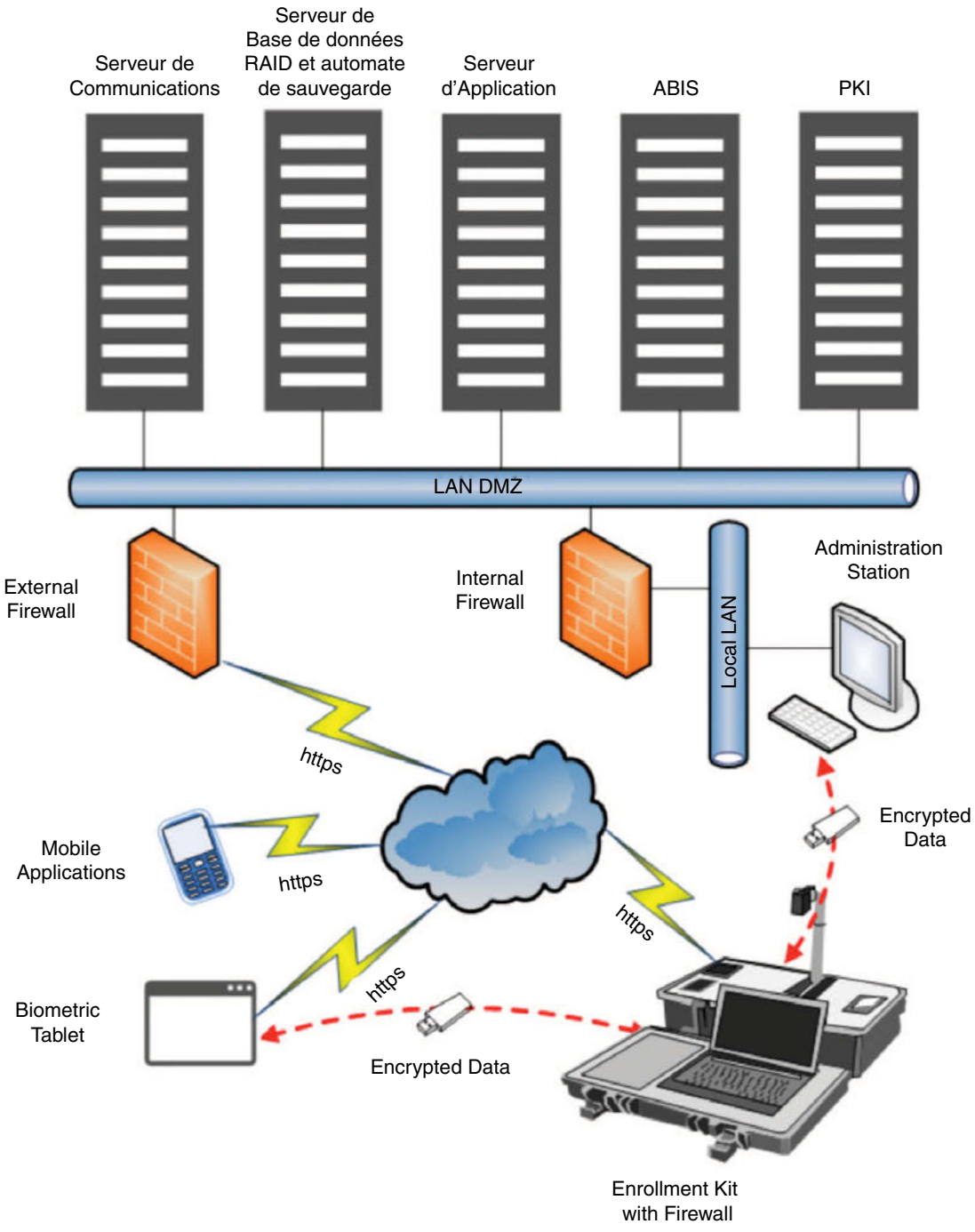
Figure 20: The Identity Cycle



Annex 2: The system architecture

The communication infrastructure

Figure 21: The Communication Infrastructure



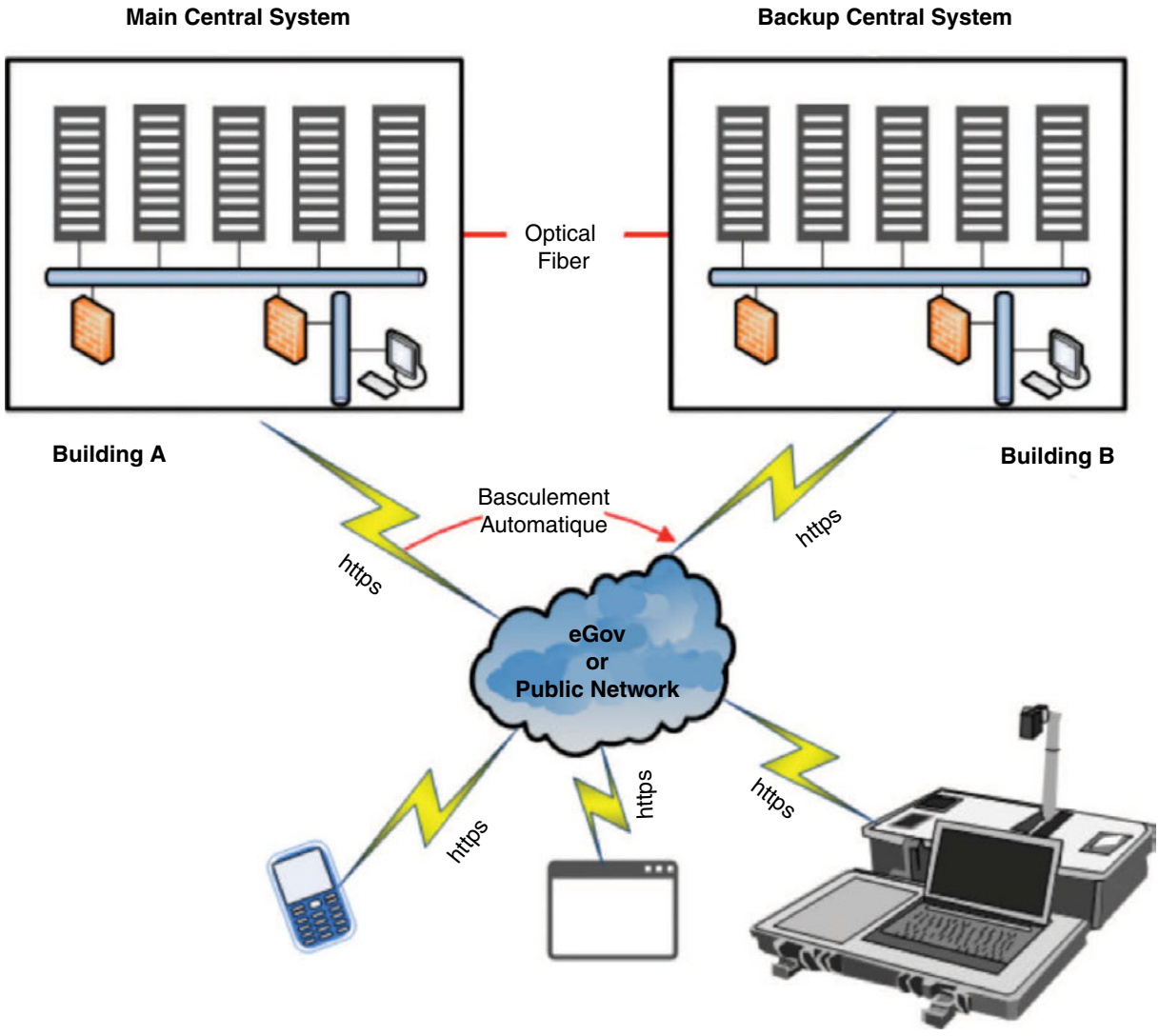
The architecture must anticipate all cases:

- The area is not covered by eGov or telephone coverage; in this case the data transfer must be by USB key containing the encrypted data;
- The area is covered by eGov or telephone operator. In this case interaction with the central system will take place using the https protocol. The kits will be fitted accordingly.

Central site and backup site

In case of disaster, treatments are switched on to the backup system, and communication with the remote sites will be done through the backup system.

Figure 22: Main Site and Backup Site



The central site

The central site may include:

- The agency offices (4) equipped with:
  - office furniture;
  - air-conditioning;
  - backup current;
  - the local network;
- A meeting room for 12 persons equipped with:
  - A meeting table with chairs;
  - Air-conditioning;
  - UPS;
  - Video projector with screen;
  - Local network;
- A training room connected to the training system with training stations connected to the training system (12 posts);
- An office for the system administrator;
- A data center that meets the ISO/IEC 27001 safety requirements and that can accommodate all of the central system servers as well as the training server;
- The site must be equipped with a generator and an uninterruptible power supply covering the needs.

The backup site would include only the backup data center and a room for the administrator with the same safety requirements.

The two sites must be connected by an optic fiber.

Servers and services in the central system

The central system must consist of:

- A database management system with automatic duplication on the backup system and export of the backups;
- A RAID array with a 10 terabytes capacity in RAID5;
- An applications server;
- A communication server capable of handling 20,000 transactions in 8 hours with 500 simultaneous connections;
- An ABIS with portrait and 10-finger fingerprints biometrics for 15 million people with a response time <10 seconds. Biometrics using the iris could be used but should not exceed 100,000 persons;
- A public key infrastructure;
- A messaging system;
- A backup active directory to manage the equipment, users and profiles;
- A management station equipped with a printer and office software;
- A training system capable of handling up to 12.

There should be enough redundancy so that the system continues to operate in degraded mode even if one of the systems fails.

The problem of redundancy can be resolved by using virtualization.

Servers and services in the backup system

The backup system is a replica of the main system with the same performance and safety requirements.

Infrastructure in the prefectures or Conakry municipalities

All equipment must be housed in clean and secure premises.

The prefectures or Conakry communes will host one or more kits. These must be connected to eGov network or via a 3G telephone operator.

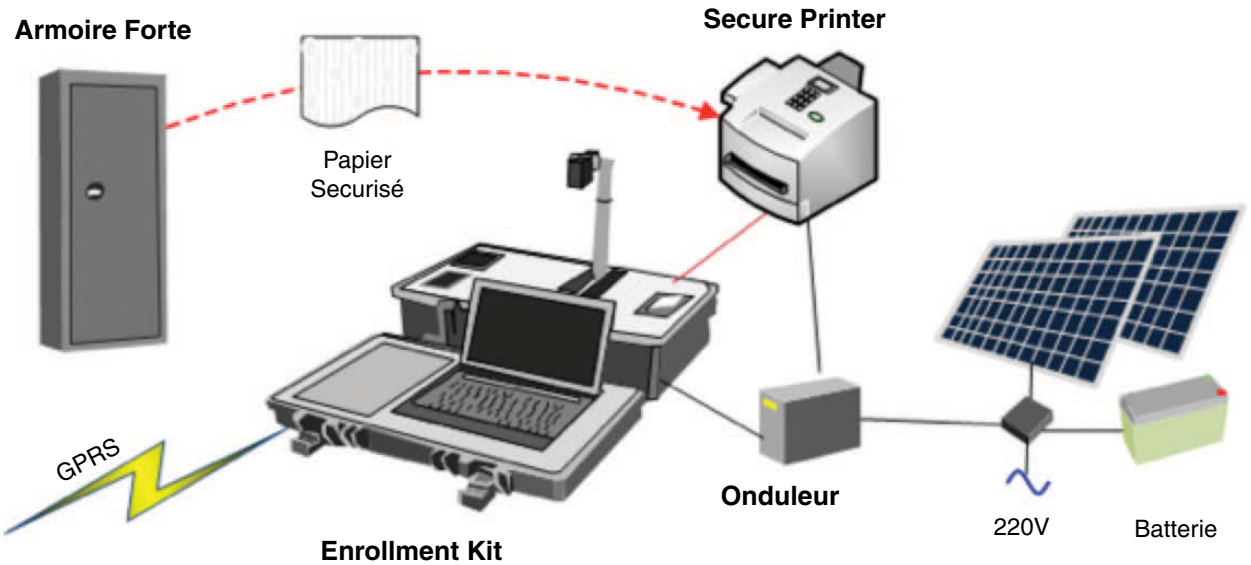
The equipment must be protected by a UPS connected to the main power supply or a battery with solar panels in case of prolonged power interruption.

If the printing of birth certificates is included in the system, the site must be equipped with a secure printer connected to the kit. The printer should have the following security features:

- Access to the printer tray protected by a lock;
- Starting a print job should be protected by a PIN;
- Secure printing:
  - Encrypting and decrypting of the data sent to the printer;
  - Anti-copying device;
  - Micro printing;
  - Special ink prohibiting modification of a document.

The security paper should be stored in an antitheft cabinet. The site manager is responsible for the management of this stock. The documents are numbered and must be registered in the system. There can be no loss or fraudulent use of a document.

Figure 23: Registration and Printing of Birth Certificates at Main Municipality Level



- Laptop
- Scanner
- Receipt Printer
- High Definition Camera
- Biometric Scanner 4:4:2
- Signature Pad
- Smart Card Reader
- Bar Code Reader
- USB Key
- GPRS (Card or Modem)

Infrastructure in rural municipalities

The municipalities will host one biometric enrollment kit. To address the energy problems, we propose setting up a solar panel to power the kits. This will remove all problems related to power generation (generator management, fuel management, current stability problems).

Figure 24: Municipality Kits

Enrollment Kit

- Laptop
- 8 Hour Battery
- Scanner
- Printer
- High Definition Camera
- Biometric Scanner 4:4:2
- Signature Pad
- Smart Card Reader
- Bar Code Reader
- USB Key
- GPRS (Card or Modem)
- GPS Localisation

National Identity Card processing infrastructure

As requested by the Ministry of Public Security, we assumed that the printing would be decentralized at the municipal police stations in Conakry and at the prefecture police stations in the interior. A centralized solution would be easier to support and maintain but more difficult to organize. Before making a final decision, the two solutions must be discussed and compared from all points of view:

- Global cost;
- Organization to implement;
- Service efficiency;
- Risks.

The equipment should be housed in clean and secure premises.

A police station may host one or more kits. It shall be connected to eGov network or via a 3G telephone operator.

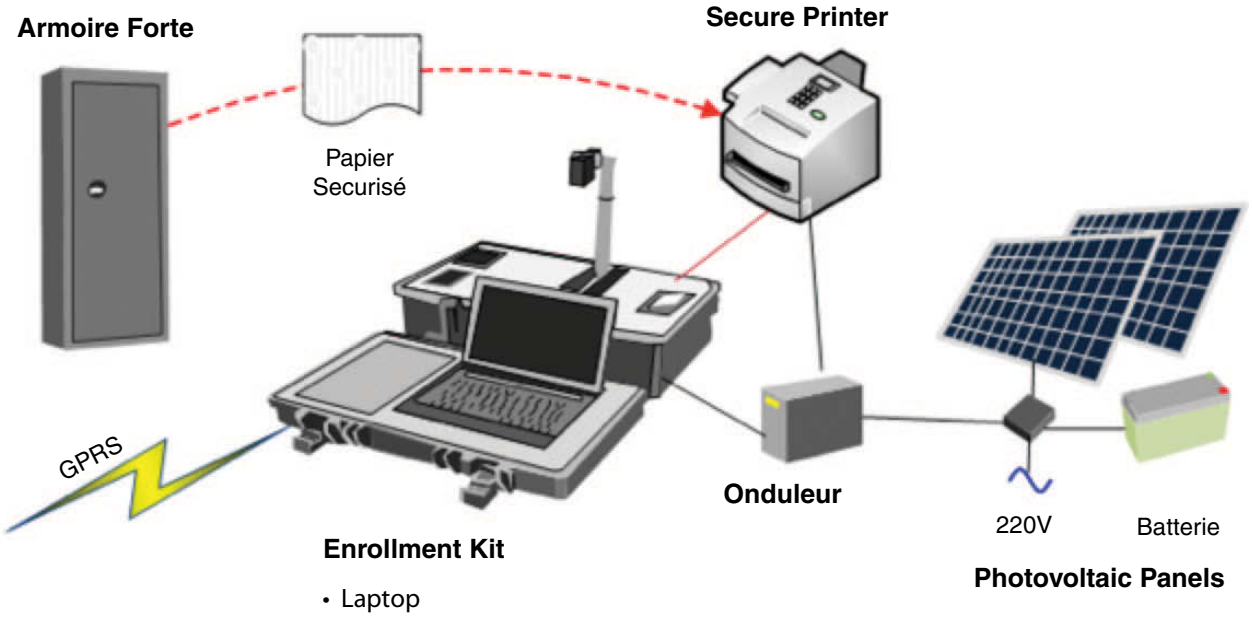
The equipment must be protected by a UPS and can be provided with batteries and solar panels in anticipation of prolonged power interruptions.

The kits must be equipped with a card reader for authentication of applicants and a 1D Bar Code Reader to capture card numbers.

The printer can be connected to a Kit or an independent station depending on the type of processing (front office or back office).

Identity cards should be stored in an antitheft cabinet. The site manager is responsible for managing the stock. The cards are numbered and must be recorded and tracked in the system. Then there can be no loss or fraudulent use of a card.

Figure 25: Enrollment and Card Production



Enrollment Kit

- Laptop
- Scanner
- Receipt Printer
- High Definition Camera
- Biometric Scanner 4:4:2
- Signature Pad
- Smart Card Reader
- Bar Code Reader
- USB Key
- GPRS (Card or Modem)

worldbank.org/id4d

ID4D
IDENTIFICATION FOR DEVELOPMENT

WORLD BANK GROUP