ADRRI JOURNAL OF ENGINEERING AND TECHNOLOGY

*ADRRI JOURNALS (***www.adrri.org***)*

pISSN: 2026-674X ***ISSN-L***: 2026-674X VOL. 2,No.2(1), October, 2014

Fraud vulnerability of Kenya's National Identity Card System

Joel Cherus[1], Kageni Njagi[2], Jason Githeko[3], Joseph Siror[4]
[1]School of Science, Engineering & Technology, Kabarak University, Private Bag - 20157 Kabarak, Kenya.
[2]Institute of Postgraduate Studies and Research, Kabarak University, Private Bag - 20157 Kabarak, Kenya.
[3]Department of Computer Science, Egerton University, P.O. Box 536 Egerton 20115, Kenya.
[4]National Economic and Social Council, PO Box 62345 – 00200 Nairobi, Kenya.

[1]**Correspondence:** cheruskimeli@gmail.com, jcherus@kabarak.ac.ke

Received: 15th September, 2014 **Revised**: 20th October, 2014 **Published Online:** 30th October, 2014

URL: http://www.journals.adrri.org/

[**Cite as**: Cherus, J., Njagi, K., Githeko, J. and Siror, J. (2014). "**Fraud vulnerability of Kenya's National Identity Card System**." ADRRI Journal of Engineering and Technology, Ghana: Vol. 2, No. 2(1), Pp. 64-71, **ISSN**: 2026-674X, 30th October, 2014.]

Abstract

Modern crimes such as terrorism, money laundering and illegal immigration are majorly committed by individuals who falsify their identities by forging identification documents. One such document that is a target of forgery in Kenya is the national identity card. Research has shown that thousands of national identity cards in use today are not genuine. An understanding of the challenges that make identity card systems vulnerable to fraud may help in developing specifications for secure identification systems. This study investigated design and functional weaknesses inherent in Kenya's national identity card system and proposed potential areas for future research. A survey was carried out on Kenya's second generation identity card system. This involved interviewing system administrators and users of Civil Identification System, Automatic Fingerprint Identification System and Production System, observing processes at the field registration stations and studying relevant documentation. The survey revealed that the national identity card system is challenged by existing manual processes, outdated technology and its architectural design. It is hoped that these findings will assist relevant experts in developing effective and secure national identity card systems.

Keywords: national identity card, civil status data, biometric, identity fraud

INTRODUCTION

To date, a National Identity Card is still the most trusted document for proofing an individual's identity in Kenya. It is required during voting, purchasing property, accessing higher education or even obtaining employment (Florence et al., 2007). It is the basic document needed to obtain other identification documents such as social security cards, health insurance cards, driving licenses, passports, college identity cards, etc.

So far, extensive research has been undertaken on national identity card systems with special focus on technology infrastructure (Dettmer, 2004; Jain, 2010; Rössler, 2008), privacy (Borcea-Pfitzmann, Hansen, Liesebach, Pfitzmann, & Steinbrecher, 2006; Koops, Leenes, Meints, Van Der Meulen, & Jaquet-Chiffelle, 2009) and adoption (Heichlinger & Gallego, 2010; Loo, Yeow, & Chong, 2009; Rissanen, 2010). There is however inadequate coverage on the security challenges hindering the effectiveness of these systems. An effective identification system is supposed to (1) identify, (2) authenticate and (3) authorize the right person to the right entitlements. Research has however indicated that a lot of identity-related crimes committed today are as a result of ineffective personal identification systems. This calls for the development of personal identification systems that are resilient, secure and resistant to identity fraud. To achieve this, an investigation of the challenges making them ineffective may need to be undertaken first.

The purpose of this paper therefore is to present the challenges which contribute to the vulnerability of Kenya's national identity card system. Specifically, the identified functional and design weaknesses of the system and potential areas for future research are discussed.

Background to Identification Systems

Identification is "the act [or process] of recognizing or establishing as being a particular person" (Clarke, 1994). In small enough communities, individuals can identify each other by their physical characteristics or by name. However, in large communities, identification is complex and requires other means (Castro, 2011). Clarke (1994) suggested three basic means of identifying human beings. The first one is "knowledge-based" identification. This is where a person is recognized by demonstrating knowledge in information he/she is expected to know. Such information may include the person's surname or personal identification number. Second is "token-based" identification, whereby a person is recognized by being in possession of some item like the passport, identity card, or a driver's license. Third is "biometric" identification, which refers to a variety of identification techniques that are based on physical characteristics including the description of appearance, social behaviour, finger prints, retinal scans or DNA patterns.

The Kenya's national identification system has been token-based since its inception. It can be traced back to 1915 during the colonial period when the Native Registration Ordinance was passed. This ordinance made it compulsory for all male natives of sixteen (16) years and above to wear on their necks, a metal container that was generally referred to as the 'Kipande'. This copper plated metal contained the registration certificate of the applicant and his particulars including his fingerprint impressions. The registration certificate was meant to assist the colonial authorities in supervising and controlling the movement and recruitment of male indigenous Africans into colonial labour (Zeleza, 1992). The 'Kipande' was later changed into an identity card in form of a booklet containing the particulars and fingerprint impressions of the holder. This was later replaced with 1st Generation Identity Card. A number of weaknesses in the 1st Generation Identity Card which included illegal registration of aliens, easy manipulation, forgeries and theft, easy duplication of identity card numbers, delays in replacing lost identity cards and double registration (Florence et al., 2007) necessitated the shift to 2nd Generation Card in 1995. The 2nd Generation Card System has however experienced new challenges which have made it insecure.

METHODOLOGY

Data for this study was collected through interviews, observation and reading of relevant documentation. A purposive sampling strategy was used to strategically select the interviewees. Participants were selected based on their roles in the system. The goal was to gather information from people who have had more experience in administering and using the system. Two (2) system administrators and two (2) users of each of the following subsystems; Civil Identification System, Automatic Fingerprint Identification System and Production System were identified and subsequently interviewed.

Interviews were conducted at the National Registration Bureau central site, a place where most of the system processes have been automated. The administrators of the identification system were asked to describe the functionality of the system and its information technology infrastructure. On the other hand, users were asked to narrate their day to day interaction with the system. Both the administrators and users were also asked to identify challenges that hinder the system from being effective. Though there were no comprehensive technical and user manuals for the system, in-house developed documents were readily available.

Data from the interviews and documentation was recorded on paper. They were then categorized into issues of system architecture and system functionality. In each case, themes were developed and described accordingly.

RESULTS

The current National Identity Card System is based on a process workflow that combines manual and semi-automated processes at the field and headquarter offices respectively. The identity document produced from this system is a laminated paper-based card.

System Architecture

The Identity Card System is an integration of three systems, namely; (a) The Civil Identification System, (b) The Automatic Fingerprint Identification System (AFIS) and (c) The Production System as shown in Figure 1.

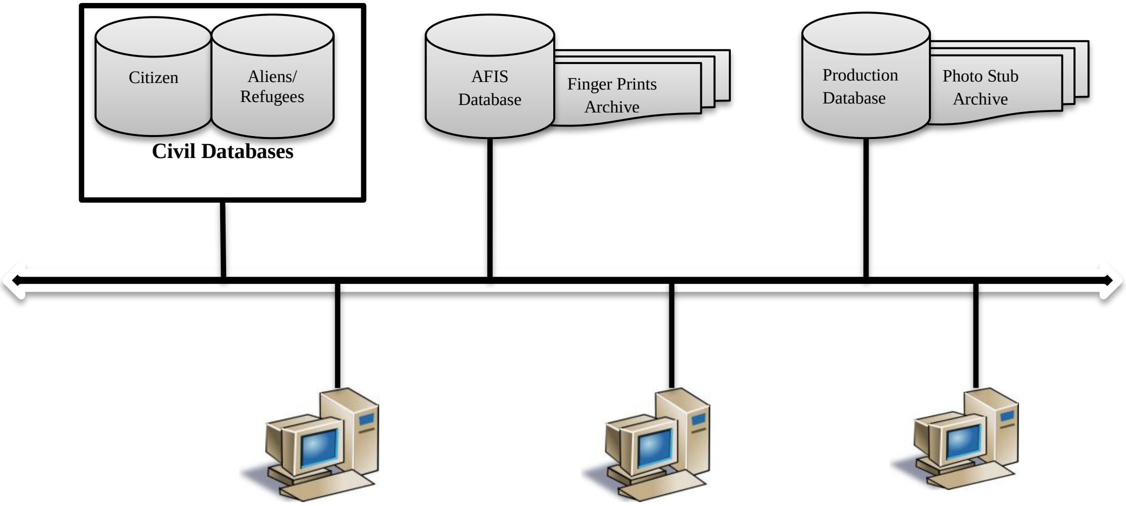

Figure 1: National Identity Card System Architecture

Subsystems

The Civil Identification System

The civil identification system is composed of two subsystems; Citizen Identification and Alien/Refugee Identification. The Citizen Identification Subsystem manages citizens' civil status data (i.e. full names, date of birth, sex, county/district/country of birth, etc.). The system generates identity card numbers for all new authentic applicants. On the other hand, the Alien/Refugee Identification Subsystem manages aliens and refugees civil status data. The records of aliens and refugees are stored in one database but are differentiated by serial numbers derived from the enrolment forms. These serial numbers are sequentially allocated in two different number ranges, one for aliens and the other for refugees. A complete application record from these subsystems is sent to AFIS for final verification.

Automatic Fingerprint Identification System (AFIS)

This system is used to capture fingerprint impressions, perform searches and archive fingerprint images. Fingerprints are scanned from applicants' paper forms. AFIS automatically verifies the authenticity of all applications against the archived fingerprints. Authentic records are confirmed to the Civil Identification System which will then be cleared for further processing. The main objective of AFIS is to detect double and illegal registrations.

The Production System

The production system is used to capture photo images, thumbprints and signatures of applicants which are then archived in Microsoft Windows folders. A reference field to the records in the archives is stored in the production database. The system prints, laminates and cuts identity cards for applicants whose records have been verified to be complete through a process known as "card personalization". They are then packed, ready for delivery.

Technology infrastructure

The identification system is connected via a bus topology network that runs on a Windows platform. It operates on client-server architecture. Civil status data is stored in relational databases and accessed through oracle-based form interfaces from client machines. Biometric data is stored in Windows folders. Data backup process is semi-automated.

System Functionality

The National Identity Card System has four main operational steps: (1) identity registration, (2) data processing and (3) Card Delivery and Collection.

Identity Registration

The registration process is manual. An applicant commences registration by presenting all the necessary supporting documents required to prove citizenship. These documents are parent(s) identity card(s), birth certificate, school leaving certificate and birth clinic card. After a positive identification is done, an applicant is authorized to apply for an identity card by filling in application forms. There are three types of application forms; form 136A, form 101 and form 136C. Form 136A is used to capture civil status data, form 101 is used to capture biometrics data (10 fingers) and form 136C which has a bar code is used to verify the issued card against the stored information.

There are six (6) types of applications that can be made:- *(i) Initial Registration / Not Previously Registered (NPR)* - An application meant for a citizen who has never been registered, and therefore his/her data does not exist in any identity system, i.e. in either the 1st or 2nd Generation Identity Card System, (ii) *Replacement of 1st Generation Identity Card* **-** An application request for the replacement of 1st Generation Identity card with the 2nd Generation Identity Card, (iii) *Change of Particulars of 2nd Generation Identity Card* **-** An application to change the particulars of an applicant as a result of marriages or change of names, (iv) *Duplicate* - An application for applicants whose identity cards are lost or mutilated, (v) *Correction on Civil Status Data* - An application request to correct errors made on civil status data for applicants, (vi) *Other Corrections* **-** An application requesting for corrections on photograph or fingerprints rejected in the previous application.

In the final stage of the registration process, the applicant is issued with a waiting card and advised on when to collect the national identity card. Completed application forms are taken to National Registration Bureau Headquarters for processing and final production of the identity card.

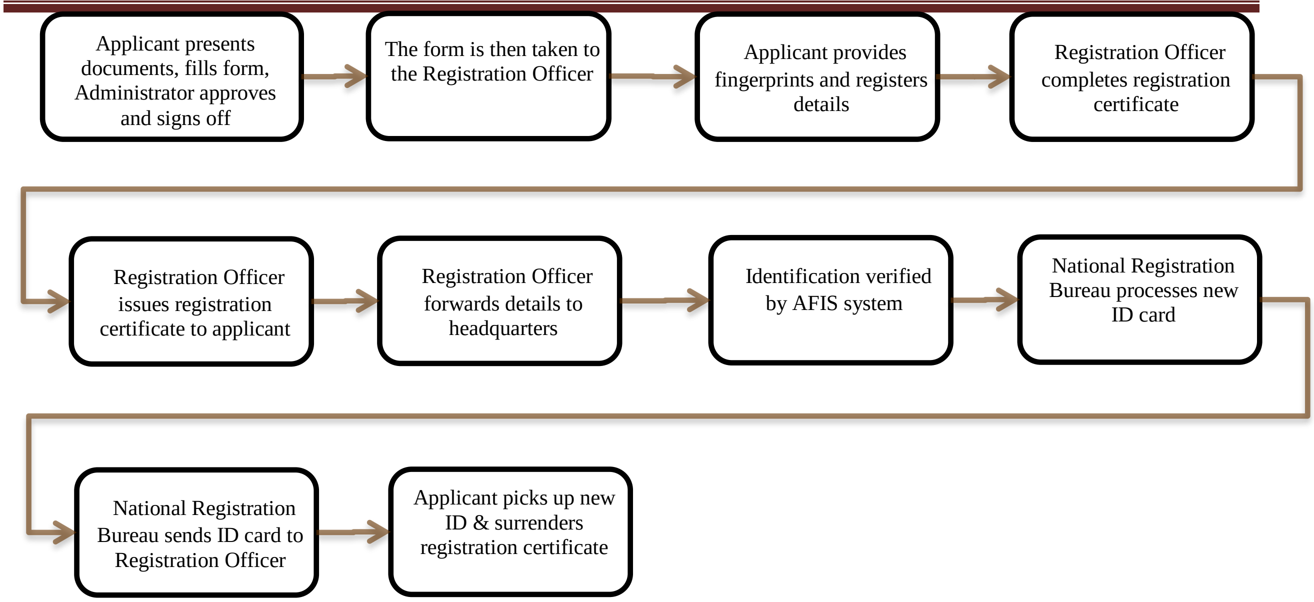
Applicant presents documents, fills form, Administrator approves and signs off
The form is then taken to the Registration Officer
Applicant provides fingerprints and registers details
Registration Officer completes registration certificate
Registration Officer issues registration certificate to applicant
Registration Officer forwards details to headquarters
Identification verified by AFIS system
National Registration Bureau processes new ID card
National Registration Bureau sends ID card to Registration Officer
Applicant picks up new ID & surrenders registration certificate

Figure 2: National Identity Card System Workflow

Data Processing

Data processing is done with the assistance of computer-based systems. The process involves data verification, validation and storage. The production process culminates with the production of identity cards that must be checked for quality before being issued to their respective owners. Quality checks are undertaken at three levels; 1) Physical damage checks, 2) Text, data, photo and fingerprint visual checks and 3) Optical Character Recognition (OCR) checks, where data printed on the machine readable zone of the card is checked for consistency with the data stored in the central database.

Card Delivery and Collection

Each production batch containing identity cards are sorted and packed according to registration offices. Packaged identity cards and rejection statements are placed in tin boxes for dispatch to the registration offices by courier service. The applicants will then be required to collect their identity cards from the field registration office.

DISCUSSIONS

The current workflow and design of the Second Generation Identity Card system presents serious security challenges. First, application for a national identity card requires that an individual presents supporting paper documents. These documents can be counterfeited easily and thus may allow illegitimate acquisition of national identity cards. Similarly, the Second Generation Identity Card itself is paper-based and thus can easily be counterfeited as well. Secondly, it is hard to verify a person's identity using the card since the information it contains cannot reliably prove one's identity. Further, there is no link between the national identity card system and other secondary identity systems such as those used in health institutions, schools, banks, social security etc. A forged birth certificate for example, can be used to apply for a national identity card, which may then be used to open a bank account. Thirdly, there are many adults especially from remote parts of the country who do not have national identity cards. Criminals including foreigners can take advantage of this gap thus acquiring the cards illegitimately.

CONCLUSION AND RECOMMENDATION

This study surveyed the Kenya's national identity card system with an intention of identifying the functional and technological weaknesses of the system. This was in relation to a growing trend in the misuse of national identity cards. The study specifically sought to identify functional and design weaknesses in the system in order to recommend potential areas for future research. The findings revealed that the system is mainly challenged by existing manual processes, outdated technology and its architectural design. In view of these, the following areas are recommended for future research: (1) Development of a framework for testing vulnerabilities and measuring the strength of identity registration systems; (2) Development of interoperable models of identification systems; and (3) Reengineering legacy identification systems in order to enhance their security.

REFERENCE

Borcea-Pfitzmann, K., Hansen, M., Liesebach, K., Pfitzmann, A., & Steinbrecher, S. (2006). What user-controlled identity management should learn from communities. *Information Security Technical Report, 11*(3), 119-128.

Castro, D. (2011). Explaining International IT Application Leadership: Electronic Identification Systems *The Information Technology & Innovation Foundation*.

Clarke, R. (1994). Human Identification in Information Systems: Management Challenges and Public Policy Issues. *Information Technology & People, 7*(4), 6-37.

Dettmer, R. (2004). Safety in numbers [biometric identification cards and database]. *IEE Review, 50*(11), 26-29.

Florence, J., Hassan, A., Carole, A., Ezra, C., James, M., Akademia, N., . . . Moses, K. (2007). An Identity Crisis? A Study on the Issuance of National Identity Cards In Kenya. Nairobi: Kenya National Commision on Human Rights.

Heichlinger, A., & Gallego, P. (2010). A new e-ID card and online authentication in Spain. *Identity in the Information Society, 3*(1), 43-64.

Jain, A. K. J. F. N., K. (2010). Fingerprint Matching. *Computer, 43*(2), 36-44.

Koops, B. J., Leenes, R., Meints, M., Van Der Meulen, N., & Jaquet-Chiffelle, D. O. (2009). A typology of identity-related crime. *Information Communication and Society, 12*(1), 1-24.

Loo, W. H., Yeow, P. H. P., & Chong, S. C. (2009). User acceptance of Malaysian government multipurpose smartcard applications. *Government Information Quarterly, 26*(2), 358-367.

Rissanen, T. (2010). Electronic identity in Finland: ID cards vs. bank IDs. *Identity in the Information Society, 3*(1), 175-194.

Rössler, T. (2008). Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government. *Computer Law &amp; Security Review, 24*(5), 447-453.

Zeleza, T. (1992). *The Colonial Labour System in Kenya*: East African Educational Publishers.