National Identification Issues and the Solution using Smart Card Technology

Agwah C. Benjamin[1], Agbaraji C. Emmanuel[2] (Corresponding Author), Ezetoha Franklin[3]
[1, 2]Department of Electrical and Electronic Engineering, Federal Polytechnic Nekede, Owerri, Imo State, Nigeria
[3]Department of Electrical and Electronic Engineering, Federal Polytechnic Oko, Anambra State, Nigeria

***Abstract*-The insecurity situation in the country has drawn a lot of attention in all the sectors involving human activity because of the terrific increase and the gravy consequences of insecurity to lives, property and the economy of the nation. Different types of identifications have been introduced ranging from national Identity (ID) Card, driver's licenses, to workers ID Cards, however these have not helped to address the issue of insecurity, fraud and other vises for which purpose they were introduced due to the ease by which they can be manipulated and faked. Smart card technology is an advanced technology which makes use of high level intelligence to address the vulnerability issues suffered by other methods of identification. This paper presents the solution to the national identification by using smart card technology. This technology comprises of a microchip embedded plastic card, reader, and central data base which houses the data of every registered individual in the country. The two types of smart card technology were reviewed and the contact type was chosen to be deployed for the national ID card because of its durability and lower cost of implementation and management. From the review it was confirmed that the smart card technology has the capabilities to address the problems of national identification.**

Keywords-Data base; ID Car; Microchip; National Identification; Reader; Smart Card

I. INTRODUCTION

The rate of crime is tremendously increasing everyday globally in different fields of life resulting to human insecurity, frauds, counterfeiting, robbery, cyber crimes and a whole lot of other vices in the society. Unfortunately, the developing nations are recording the greater percentage of this crime due to lack of the facilities needed to check illegal immigrants, impersonation, and other lapses in human identification. The national identity card was introduced in Nigeria and many other nations to help address the issue of human identification in other to solve the problem of insecurity and other vices, but due to the simple nature of the existing ID card, it became very easy to manipulate and print the ID card carelessly without any extra means of confirmation and authentication.

According to Yazeed [1], the National ID card is one of the official cards which can prove who you are, and can also show unique human identities. Many countries, such as Saudi Arabia and Germany, force their citizens to carry their identity card with them all the time, while a number of other counties, for example Austria and Finland use the resident identity card as one options that can be used as proof of identity. On the other hand, numerous of countries do not have a National identity card, for instance the United Kingdom and the United states. The September 11 terrorist attacks changed the world, governments and many people became more and more concerned about their security. A number of countries have considered or are considering again their approach to a form of ID card. Since the 9-11 attacks the majority of national polls showed that approximately two-thirds of the American public was in favor of a U.S National identity card. In most developing nations, there have been a set of different identification methods, for example national ID card, driver's license, voter's card, Medical card, worker's ID cards, etc. The national ID card was authorized by the federal government of Nigeria as a method of identifying its citizens nationally and it took a lot of time and money to complete the process of registration and collection. It has its own data file which is not referenced for confirmation or authentication of any holder of the ID card. The voter's card and the driver's license also took a similar step and have no automatic referencing central system to confirm the authenticity of their holders. However, because of these lapses in authentication, an ID card may bear another person's picture with a different name or place of residence. The fake name may also be used to register a telecommunication Subscriber Identity Module (SIM) card with other fake information due to the fact that the country lacks a central data base which should contain the personal data of every individual dwelling in the country. With the cheap and ordinary nature of the currently used ID card, it has been very easy to produce fake ID cards with different names and other personal information as the user wants it since the ID card is made with plastic card and the personal details printed on it without any complex structure. Unfortunately, the user of such ID card cannot be traced or monitored to confirm the authenticity of the Card.

With the growing technology, the government of every nation seeks to deploy the state-of-the-art methods to combat crime and other vices in the country. A smart card, typically a type of chip card, is a plastic card that contains an embedded computer chip, either a memory or microprocessor type that stores and transacts data. This data is usually associated with either value, information, or both and is stored and processed within the card's chip. The card data is transacted via a reader that is part of a computing system. Systems that are enhanced with smart cards are in use today throughout several key applications, including healthcare, banking, entertainment, and transportation. All applications can benefit from the added features and security that smart cards provide. Markets that

have been traditionally served by other machine readable card technologies, such as barcode and magnetic stripe, are converting to smart cards as the calculated return on investment is revisited by each card issuer year after year [2].

II. LITERATURE REVIEW

National security is the requirement to maintain the survival of the state through the use of economic power, diplomacy, power projection and political power [3]. Nwadialor [4] stated that, for some time now, the problem of insecurity which used to be one of the lowest in the hierarchy of social problems facing this country seems to have assumed alarming proportions since the end of the Nigerian civil war which ended in 1970. During the pre-colonial and colonial era, insecurity was merely handled by the Federal government utilizing the ministry of Internal Affairs , the Nigerian Police Force [N.P.F] , The Nigeria Prison, the Immigration service and the Customs, all of which annual budgets was among the least in the exclusive list . There were also local security men recruited by the native authorities, some of whom were attached to the customary court that were called different names like 'Danduka' or 'Courtma'. Since the past decade, government expenditure and security has walloped a life chunk of the Federal, State and local budgets in the name of security votes and other related sub-heads. It would appear that unemployment is one of the strongest push factors.

Margaret [5] suggested that a national identity card is a portable document, typically a plasticized card with digitally-embedded information, that someone is required or encouraged to carry as a means of confirming their identity. Since the World Trade Center tragedy of September 11, 2001, many countries have discussed issuing national identity cards as a way to distinguish terrorists from the law-abiding population. The government of the U.K. has discussed going in the direction of a national identity card that will use one or more biometric techniques such as iris or fingerprint recognition to confirm the identity of a card holder. The controversial plan would include developing a national database of basic personal information. Many people fear that a national identify card would compromise an individual's right to privacy and lead to the misuse of governmental power. The U.S. and Canada are among countries where a national identify card has been discussed but, so far, not seriously advocated by the government. A number of so-called Third World countries require their citizens to carry some kind of national identity card. Today, airlines and banks require some sort of identity authentication. Typically, a driver's license, passport, or other card with your name and an embedded photo was sufficient but nowadays it is not.

According to a 1996 document by Privacy International, around 100 countries had compulsory identity cards [6]. The card must be shown on demand by authorized personnel under specified circumstances. Often alternative proof of identity, such as a driver's license, is acceptable. Privacy International said that "virtually no common law country has a card" [6]. The term "compulsory" may have different meanings and implications in different countries. Possession of a card may only become compulsory at a certain age. There may be a penalty for not carrying a card or other legally valid identification (a passport, for foreigners); in some cases a person may be detained until identity is proved. Random checks are rare, except in police states [7]. In countries of the European Union, a national identity card complying to certain standards can in most cases be used by European citizens as a travel document in place of a passport. An exception is that a Swedish national identity card is not usable when travelling from Sweden to a non-Schengen country [7].

Forms of Identification Cards

Jamie [8] suggested that there are several forms of identification cards. Most forms of legal identification will have your full legal name printed on it. Some will have your picture on it so you can drive and travel. Your identification card will prove your identity. You will need an identification card to get a loan and apply for a credit card. The most common forms of identification cards are a driver's license, birth certificate, Social Security card, green card and passport.

Driver's License: You need a driver's license to operate a motor vehicle. Many jobs require that you have a driver's license. Some places that will ask for your driver's license are banks when withdrawing money or cashing check, and nightclubs. Your driver's license is the No. 1 form of identification.

Social Security Card: A Social Security card usually is issued during childhood or when you become a citizen of the United States. The card includes your unique Social Security number (a nine-digit federal identification number) and your name. When you apply for any type of credit such as a home loan, purchasing a car or applying for a credit card, this is the form of identification you will give. New employers also frequently require a copy of your card on file.

Picture Identification: Anyone can obtain a picture ID from their state's motor vehicle bureau. It will have all the basic information that your driver's license has, without giving you the legal ability to drive.

Birth Certificate: For natural-born citizens, your birth certificate proves your citizenship. This document, which includes your name, birth date, birth location and the names of your parents, is required to obtain a Social Security card, passport and driver's license.

Passport: A passport is also a form of picture ID required for travel outside of the United States. You can use a passport in lieu of a birth certificate if needed. A passport serves as one of the most widely accepted forms of identification.

Green Card: A green card allows foreign-born residents to live freely in the United States as permanent residents. A green card will allow you to get a driver's license, passport

and a Social Security card. This is treated the same as a birth certificate.

Security Issues of ID Cards

ID cards have a number of vulnerabilities as with many new technologies which need to be considered. However, identity national cards need more concerned and intention because it helps to fight against insecurity and other vices among the citizens and immigrants in the country. The following are some of the National identity card's issues:

Human error: a number of experts say human error is the biggest threat to ID card schemes vulnerability. The potential threat can appear at any moment where the scheme of identification card is interacted. It is a big challenge to ensure that all personal information is entered correctly, furthermore; there has to be a tool in the system that allows the modification of database entries when a user of the identity card changes their address or other information. Installing incorrect cardholder's data at any stage of the enrollment process is likely to create many problems of the bearer of the ID card. According to press story in the Guardian newspaper, a foreign woman could not travel for more than a month because she received incorrect information on her identity card which enforced her to send her ID card and passport to the responsible institution (UK Borders Agency) to solve the problem [9]. Human error may inadvertently restrict the freedom of an individual, cause distress and might breach information security. It can also cause delay in issuing ID cards and waste government money [10].

Forged identity and counterfeit cards: the traditional ID card, which is still being used in a number of counties, is easier clone than the "smart" National identity card. A threat may come from the lack of security features or conventional materials on the ID cards which do not match the requirement of accredited security printers. The fake identity card can be misused by teenagers to purchase alcohol, cigarettes or any unauthorized products, or even by terrorist to enter a country illegally.

Falsification of content: an attacker exploits the vulnerability of the electronic ID card's system to change the citizens' data. The consequences are various and depend upon an attacker's motives, for example it could be used to take revenge on a particular person.

Man in the middle attacks: As a result of lack of National ID card system security, an attacker might intercept communication between the identity card and server. The attacker stands between the two victims and then he will be able to access the sensitive data of a card holder.

Skimming attacks: the threat comes from creating a clandestine connection to the ID card in order to obtain data. An attacker can use a hidden, small machine like a reading device which is able to skim the information from "smart" identity cards and misuse the information [11].

Centralization of Database storing: in spite of giving hackers an obvious target to concentrate on by storing citizens' data in one place, hackers are intelligent enough to discover the weak aspects of their victim(s) before they attack. Hackers can observe the data for illicit purposes or to corrupt the identity card system.

Abuse by Authorized individual: people are already concerned about misuse of their information by criminals. However, a greater, threat is if such misused comes from authorized people such as the police or employers who deal with the citizens' database. They might use this information to stalk, threaten people, take revenge or settle scores.

Decrypting Data: There is small possibility of decrypting the biometric card's data when a secret key is known. For instance, hackers can interfere with the data stored on chips and also monitor data flows using probing pins. This enables them to steal private keys and to access private data [11].

Theft or loss of the ID Cards: if the identity card has been stolen or lost it put a lot of pressure on both the government and bearer especially in the case of traditional ID cards which have more information on them than "smart" ID Cards. For example, the traditional Saudis identity cards used to contain sensitive information such as the card holders' full name, an identification number, address and the telephone number, but such information is now hidden in the new bio-metric ID cards.

Smart Card Technology

Marie-Pier [12] opined that although smart card is not new. However, it is gaining new access into the market for many purposes such as payments and identification. Smart card technology provides more secured means of protecting personal information for identification and business transactions to fight fraud, fake, impersonation and other national security vises which have been the challenges and vulnerabilities of other methods of national identification.

The first patent was published in 1968 by Dethloff and Gryrupp, two German inventors, who developed the concept of a plastic card containing a microchip [13]. In 1970, the Japanese followed the lead of the Germans and registered a patent for their own version of the smart card [14]. At the end of 1970, Motorola developed the first secure single chip micro controller, which is used by the French banking system to improve security in transactions. However, it is since 1990 that the use of the smart card has become significant, with the exponential growth of the internet and the increased sophistication of mobile communication technologies [15].

Computer-chip cards are replacing magnetic-stripe cards in nearly all developed countries in the world [16] especially in payment and identification uses. Smart cards are devices designed to store and in most cases process data [12]. They are very portable (the size of a credit card) and durable, which makes them suitable for many applications involving

identification, authorization and payment. Since the invention of the card in the 1970s, the technology has evolved and many features have been added to the original concept [13].

According to Stephen [17] smart cards can provide non-repudiation, since the cards are designed to prevent the private key from being removed from the card, copied or replicated. It is portable, and when combined with a biometric such as finger scanning, the device becomes a very unique device that offers a substantially higher level of security and can still be transported in a wallet. This technology can offer the ability for personalization. The design or artwork on the cards can be uniquely prepared for internal use as in an enterprise, hospital systems or universities as an ID, a bank credit or debit card, or as a card that also offers a limited stored value which can be used for miscellaneous fees such as parking permits, cafeteria areas, and for other small purchases. These cards would typically have the university logo artwork. Post issuance personalization can include a photo and personal data stored on the chip in addition to keys/certificates and other necessary access privileges for e-mail, physical access to buildings and rooms as well as network access.

John [18] opined that, depending on the type of access and the required controls, the card can be used in different ways. The simplest case is when card itself provides the access. This is becoming more common with hotels. A PIN number might also be used with the card to enable an application to access a password or other information stored on the card. This implementation is sometimes used to help reduce the number of passwords a user has to remember. Multiple passwords can be stored on the card and unlocked with a single PIN number. The card can also store public and/or private encryption keys that it will use to digitally sign and/or encrypt messages.

Smart cards can be used for multiple purposes. Multi-Function Cards allow the same card to be used for multiple applications. These cards normally have a processor that includes not only the basic security provided for storage and retrieval of information, but also the ability to support customer defined applications. Most cards also provide support for built in cryptography functionality. These cards are becoming fairly common on college campuses where they are used for identification cards, physical access control, network access control, cafeteria cards, etc. The common access card (CAC) being issued by the DoD is also a multi-function card [18].

Hardware Features of Smart Card

The smart card has the following hardware features [12]:

- The card can be equipped with memory only (a memory card) or with memory and a small microprocessor to execute programmed tasks.
- Smart card technology can be contact-based or contactless. A contact card (usually a memory card) is placed in direct contact with the reader and a contactless card communicates with the reader by high frequency waves similar to Radio Frequency Identification (RFID). A contactless smart card uses a short-range radio frequency identification chip (also known as Near Field Communication (NFC) technology) to transfer data via radio waves when the consumer places the card within 4 inches or 10 centimeters of the reader [19]. The energy needed is provided by the electromagnetic field provided by the reader. The contactless smart card is an RFID technology specialization.
- The data on the card can either be encrypted or not. The triple data encryption standard (3DES) is often used to encrypt data.
- The amount of memory on the card can vary depending on the application. Blythe [15] opined that 2 and 4kb is sufficient to store financial data, personal data and transaction history. Nowadays, more than 64kb memory space is available.

In contact smart card, a microchip is embedded within slices of plastic with an open surface to provide direct contact with the PINs of the electronic smart card reader. While in the contactless smart card, the microchip can be completely embedded within the plastic card and it can be visible or not depending on the application. Contactless smart card has small antenna system which connects the smart card and the reader wirelessly.

However, the contactless smart card requires a special communication medium such the RFID for communication between the card and the reader, therefore it will be more expensive to implement and maintain. John [18] suggested that the cost of the contactless Smart Cards has prevented them from becoming widely popular, since these do not represent a significant market share and most of the security implications are the same as contact smart cards. The structural nature of contactless smart card makes it even more delicate to be handled roughly.

III. SMART CARD FOR NATIONAL IDENTIFICATION

Contact smart card technology is proposed to be deployed for the national ID card in this work because it is cheaper to be implemented and managed compared with the contactless smart card since it requires no special communication medium such as RFID to communicate with the reader. Secondly, it has more durable nature to be handled by the public users than the contactless type which has antenna systems etc. Smart card technology comprises of the computer-chip card, the reader and the database system. There are three players in this technology as illustrated in figure 1; the authorized users, the reader and the government which houses and controls the central data base which contains the personal information of the users in the country. The government will register the authorized users of the ID card, produce and issue the cards to the owners for use. It will be the duty of the government to monitor the registration of the users and production of the ID card.

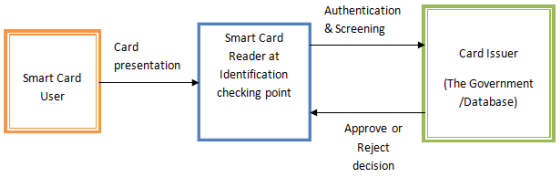

Figure 1: The block diagram of key elements of smart ID card technology

Smart Card: The smart card is the programmed plastic card with a microchip which can be programmed with the identity information of a person. Personal information details of a person may include user full names and address, passport photograph, finger print, Identity Number (IN), Next of kin, Date of birth, Local Government Area (LGA), State of Origin, Nationality etc as the case may be.

Central Database: The database system is the computer systems which houses the personal data of every citizen of the country or any authorized user of the ID card living in the country. It is a central database system which is controlled strictly by the government of the country. The personal data is gathered through the process of a strictly supervised registration process of every person living in the country that is eligible to possess the ID card.

Reader: The smart card reader is an electronic device connected directly to the central database system which can read the card with reference to the personal detail data stored in the central database and display the information stored in the card and the one stored in the database on a screen for comparison. Smart card readers function by using security software, network interfaces to banks accounts, e-mail accounts, company servers and in this case national central database servers, which validate the user to his/her application by using the users private key or digital certificate, which never leave the card. Only the card user can access the private key by using a two-factor authentication. The reader will be able to automatically detect any disparity between the information stored in the card microchip and the one in the database bearing the name and ID number with photo and finger print. This device should be located at the various points where ID cards are checked such as banks, hospitals, schools, conferences, etc. for access or other verifications.

The Network: The network connects every card reader at any location in the country to the central database system through wireless medium as illustrated in figure 2. Every institution or establishment where individual identification is checked will be expected to install smart card reader and connect it to the national network.

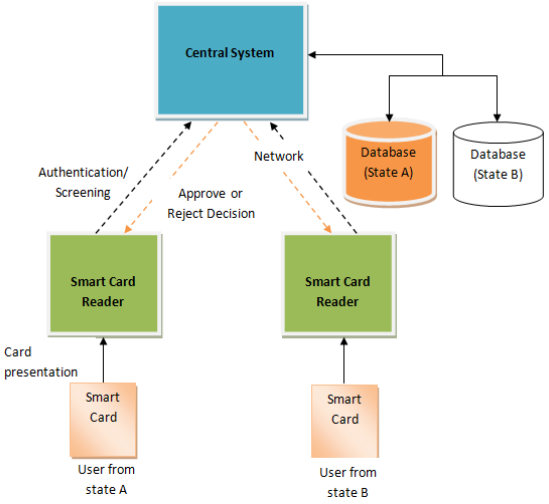

Figure: The national ID smart card architecture

Smart Card And Identity Management

A smart card can be used to securely hold user identity information, and to provide two-factor or three factor authentication. Smart card technology enables distributed and federated applications in lieu of a central database of all user identity and other personal information. The use of smart cards and federated data with standard based protocols would allow academic institutions, medical practitioners, the police, telecommunication and other government agencies to have access to data across multiple data stores with an assurance that:

a) The smart card user identity is authenticated;

b) The records of a user retrieved will be analyzed for approval if it matches with the data in the chip or rejected if there is mismatch; and

c) Only the agencies registered under the government and have need of the data have access to the central database.

In the case of user data access, proper security controls and restrictions must also be implemented around the applications, databases, and environments that house the electronic data. Smart cards can be effective in supporting numerous organizational programs in the country such as SIM card registration, voter's card registration, healthcare applications and many more, with or without a unique identifier. Smart cards can serve as a secure way to aggregate multiple identifiers across many different systems or organizations, linking them all on the smart card [20] data housing facilities.

Advantages of Smart ID Cards

According to Richard [16] cards with an imbedded computer chip have many more capabilities than magnetic-stripe cards. Computer-chip cards are much harder to counterfeit, can protect information stored on the chip more effectively, and can defend against unauthorized intrusions. A computer-chip card can use encryption to protect sensitive data, can authenticate messages that it receives, and can send messages to issuers that enable the issuers to authenticate transactions more reliably than they can with magnetic stripe cards. Smart cards also can modify data on

application for security purposes. The capacity of the smart card to encrypt data makes possible a process of "dynamic data authentication".

The smart card is capable of providing memory space to contain information needed for other types of identification; therefore it can be used for multiple purposes such as driver's license, voter ID, medical ID and many more. With these features and capabilities, the smart ID card technology will help the citizens to solve the problem of wasting money in processing different ID cards used by different agencies under the same government of a country.

IV. CHALLENGES OF SMART ID CARD

Flaws in Design/Implementation: By far, the most serious problem for smart cards is the attacks that exploit vulnerabilities caused by poor design or implementation of a card or system. These vulnerabilities tend to be easier to exploit, replicate [21], and therefore share among the hacker community [18]. However, proper supervision and examination for the smart card production and distribution will help to solve this problem.

Poor or bad network facilities: Poor network has been one of the major impediments of most technologies such as the Automated Teller Machine (ATM) that use wireless network especially in the developing nations. This problem can cause delay in ID card check at the checking points thereby disrupting somebody's activities. However, this problem can be solves and avoided by regular maintenance of the network facilities and installation of new and proper devices if old ones get bad.

Power supply: The problem of power supply is another major problem facing Information and Communication Technology (ICT) generally especially in the developing countries. Since the smart card technology will depend on the power supply for the network facilities and the computer systems, the incessant epileptic power supply being experienced in most developing nations will definitely become a great challenge to the technology.

Lack of trained staff: Smart card is a technology that needs trained personnel for its operations and management for maximum efficiency. Lack of trained staff could be a challenge because it demands some level of expertise especially at the reader point and database management.

Government policies: One of the major challenges of ICT in the developing nations is lack of proper government policies and the smart card technology will not be different. The government should make and implement policies to support the full deployment of smart card technology to address the problems of insecurity that has become a major challenge to the national development in most countries.
Nonetheless, proper general awareness should be made to enlighten the users of the national ID card on the use of the smart card and how to handle the card to avoid damaging or misplacing the plastic card.

V. CONCLUSION AND RECOMMENDATIONS

Smart cards use embedded microchips to electronically store data which is read by a reader. The technology can be contact-based or contactless. In a contact-based, the user inserts the card into the contact reader and the chip embedded in the card makes physical contact with the reader, transmitting data from the chip to the reader and writing information back to the chip. In contrast, a contactless smart card uses a short-range radio frequency identification chip known as NFC technology to transfer data via radio waves when the user places the card within 4 inches or 10 centimeters of the reader. Contact smart card technology is proposed in this work to be used for national ID card because it is more durable and cheaper to implement and manage.

Deploying smart card technology for national identification will require three elements: plastic card with a microchip (smart card), reader and a database. From the review, it was observed that the features and capabilities of the smart card technology will help to address the security issues especially in the national identification.

There should be strict monitoring of user registration, production and the issuance of the ID card. The database should be controlled and managed strictly and made more intelligent with face and finger print analyzer software so that it will be able to detect an authorized user with double or more number of registrations.

REFERENCES

[1] A. Yazeed. "National ID Cards", International Journal of Computing Science and Information Technology, 2013, Vol.1 (02) 44 – 48
[2] "Smartcard Overview", 2013, http://www.smartcardbasics.com/
[3] "National Security", http://en.wikipedia.org/wiki/National_security
[4] E. Nwadialor, "Nigeria and Security Challenges", 2011, http://www.vanguardngr.com/2011/12/nigeria-and-security-challenges/
[5] R. Margaret. "National Identity Card", 2010, http://searchsecurity.techtarget.com/definition/national-identity-card
[6] "List of National Identity Card Polies by Countries", http://en.wikipedia.org/wiki/List_of_national_identity_card_policies_by_country#cite_note-privacy-international
[7] "Countries with Compulsory Identity Cards" http://en.wikipedia.org/wiki/List_of_national_identity_card_policies_by_country
[8] P. Jamie. "Types of Identification Cards", 2014, http://www.ehow.com/list_7258957_types-identification-cards.html
[9] H. Porter. "The horror of the ID card system", Guardian Newspaper, 2009, http://www.guardian.co.uk/commentisfree/2009/feb/04/idcards-biometrics
[10] A. Siddhartha. "National e-ID card schemes: A European overview", Inf. Secure Tech. Rep., 13, 2, (2008), 46-53, DOI=10.1016/j.istr.2008.08.002 http://dx.doi.org/10.1016/j.istr.2008.08.002
[11] I. Naumann and G. Hogben. "Privacy Features of European eID Card Specifications", The European Net-work and information Security Agency (ENISA), 2009, http://www.enisa.europa.eu/act/it/eid/eid-cards-en

[12] P. Marie-Pier. “Smart Card Data in Public Transit Planning: A Review”, Interuniversity Research Centre on Enterprise Networks Logistics and Transportation (CIRRELT), 2009
[13] M. Shelfer and J.D. Procaccino. “Smart Card Evolution, Communication of the ACM”, 2002, 47(7), pp 83-88
[14] N.O. Attoh-Okine and L.D. Shen. “Security Issues of Emerging Smart Card Fare Collection”, In: IEEE Vehicle Navigation and Information Systems Conference, Proceedings, Sixth International VNIS, A Ride into the Future, 1995, pp 523-526
[15] P. Blythe. “Improving Public Transport Ticketing Through Smart Cards”, Proceedings of the Institute of Civil Engineers, Municipal Engineer, 2004, Vol. 157, pp. 47-54
[16] J.S. Richard. “The U.S. Adoption of Computer-Chip Payment Cards: Implications for Payment Fraud”, Federal Reserve Bank of Kansas City, 2012
[17] T.I. Stephen. “Identity Protection and Smart Card Adoption in America”, SANS Institute, InfoSec Reading Room, Assignment Version 1.4b, 2003
[18] A. John. “Smart Cards: How Secured are they” SANS Institute, InfoSec Reading Room, 2002
[19] Q. Nasreen. “The Contactless Wave: A Case Study in Transit Payments”, Emerging Payments Industry Briefing, Federal Reserve Bank of Boston, 2008
[20] Smart Card Alliance. “Getting to Meaningful Use and Beyond: How Smart Card Technology Can Support Meaningful Use of Electronic Health Records”, A Smart Card Alliance Healthcare Council Publication, 191 Clarksville Rd. Princeton Junction, NJ 08550
[21] J. Glave. "Pirates Cash In on Weak Chips" Wired News May 22, 1998 URL: http://www.wired.com/news/technology/0,1282,12459,00.html