International Journal of Mechanical Engineering

IMPROVING INPUT CONTROL CONTROL BASED ON NON-CONTACT ID CARD READING TECHNOLOGY

Viloyat Abdukhalilovna Gazieva

Senior Lecturer, Department of Electronics and Radio Engineering, Tashkent University of Information Technologies

Abstract: *This article discusses ways to improve access control based on contactless id card reading technology. It's also a secure place to perform processes that one doesn't want to be exposed to the world, for example, performing a public key or private key encryption. The benefit of the smart card is that you can verify the PIN or fingerprint securely, off-line. The types and specific features based on contactless id card reading technology are covered and their specific aspects are based. In addition,. The development of contactless id card reading technology and foreign experience are covered in detail. It also provides conclusions and recommendations on ways to improve access control based on contactless id card reading technology.*

Key words: *contactless id card, reading-based technology, electronic carrier device, ID-card, biometric passport system infrastructure.*

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[1].

On the basis of the Decree of the Republic of Uzbekistan dated September 22, 2020 "On measures to introduce identification ID-cards in the Republic of Uzbekistan" from January 1, 2021, the introduction of a single system of digital identification, ie 2011 Instead of a biometric passport of the year 2006, the introduction of ID-cards as a document with an electronic device confirming the identity and citizenship of a citizen of Uzbekistan. An ID card is a plastic card document that contains a person's biographical information, digital photo, fingerprints (upon reaching the age of 16) and an electronic digital signature key certificate (upon reaching the age of 16). In world practice, this card is used not only as a certificate of identity and citizenship, but also as a bank plastic card, driver's license, public key, e-wallet [2]. Here's a step-by-step guide on how to get an ID card based on expert advice.

There are two ways to apply for an ID card:

➢ with your biometric passport, visit any department of migration and citizenship, which is convenient for you, regardless of the district in which you are registered;

➢ Electronic application through the Single interactive state services portal.

Biometric passports of the population of the Republic on the ID-card:

➢ From January 1, 2021 to December 31, 2022 on a voluntary basis;

➢ Mandatory from January 1, 2023 to December 31, 2030.

➢ From January 1, 2031, biometric passports of citizens of the Republic of Uzbekistan in 2011 will be considered invalid.

Accelerated development of the information system in the country, the widespread use of modern information and communication technologies in the provision of public services, the introduction of a single mechanism of identification in various information systems and remote services, as well as the five priorities of the Republic of Uzbekistan in 2017-2021. In order to ensure the effective implementation of the tasks set out in the State Program for the implementation of the Action Strategy in the "Year of Science, Enlightenment and Digital Economy" [3]:

1. The President of the Republic of Uzbekistan dated December 26, 2018 "On additional measures to create a system of registration and issuance of biometric passports of citizens of the Republic of Uzbekistan abroad and modernization of the biometric passport system of the Republic of Uzbekistan For information, the decision No. PQ-4079 provides for the introduction of a system of registration and issuance of identification ID-cards from 2021 instead of the biometric passport of a citizen of the Republic of Uzbekistan in 2011 on the basis of the existing infrastructure of the biometric passport system. accepted.A smart card is a safe place to store valuable information such as private keys, account numbers, passwords, or personal information.

It's also a secure place to perform processes that one doesn't want to be exposed to the world, for example, performing a public key or private key encryption.

The benefit of the smart card is that you can verify the PIN or fingerprint securely, off-line.

From left to right:

- online authentication access (with the US DoD smart badge - *military CAC*),
- secure transaction with an EMV card (with a *biometric sensor*),
- strong identification with your national ID card.

Among all radio frequency technologies, 125 kHz cards are the most vulnerable from the point of view of the above parameters. However, cards of not all standards lend themselves to such a simple hack; many modern identifiers are protected from such threats using advanced technologies. For example, protection of 13.56 MHz access cards is ensured by mutual authentication between the card and the reader, the process of which occurs in encrypted form with the generation and confirmation of the diversification key [4].

The issue of security of identification technologies is no less relevant than the analysis and assessment of the functionality and capabilities of the system at the software level. Therefore, we will consider ways to protect access cards in more detail.

Encryption DES, 3DES, AES

DES, 3DES, AES symmetric block encryption algorithms, where the same key is used for both encryption and decryption of a message, while the key length remains constant.

DES: 56 bits key length (and 8 parity bits), block size 64 bits, was a US national standard (ANSI X3.92, 1977). Modern computers are hacked by brute-force attacks in a reasonable amount of time.

Triple DES (ANSI X9.52), 3DES - triple encryption with 3 (sometimes two) different keys of 56 bits. With a high level of protection, it has a rather low performance.

AES (originally Rijndael, proposed by Joan Dieman of Proton World International and Vincent Ridgeman of Katholieke Universiteit Leuven, Belgium): variable key length up to 256 bits. AES, the new national standard for the United States, was selected from several candidates in testing because it combines simplicity and high performance.

“Rijndael has demonstrated good resistance to implementation attacks, in which a hacker attempts to decode an encrypted message by analyzing the external manifestations of the algorithm, including power consumption and execution time. Usually, the ability to resist them is provided by special coding to equalize the level of power consumption. AES can be easily defended against such attacks because it relies primarily on boolean operations. In addition, it passed all tests with smart cards and in hardware implementations perfectly. The algorithm is largely inherent in internal parallelism, which makes it easy to ensure efficient use of processor resources. " - says Richard Smith, PhD, Lead Engineer at Secure Computing Corporation [5].There are calculations showing that the energy of our entire galaxy with its optimal use is not enough to search for a 256-bit key by the brute-force method. For real tasks, 128 bits are enough.

The use of encryption algorithms DES, 3DES, AES allows you to protect access cards from unauthorized access to confidential data.

Mutual Authentication

If there is a mutual authentication algorithm, the access card, getting into the reading zone, provides the reader with its unique CSN number and a generated 16-bit random number. In response, the reader, using the Hash algorithm, creates a diversification key, which must match the key written on the card. If there is a match, the card and the reader exchange 32-bit responses, after which the reader "makes" a decision on the validity of the card. Thus, protection against repeated reproduction of information is carried out [6].

Key diversification

Key diversification is necessary in systems where access cards are used that are not sufficiently protected from cloning. As a rule, this applies to low-frequency cards of the Em-Marine standard. With the help of the software, you can configure access control, which will ensure greater reliability of the ACS.

Delimitation options [7]:

- "card - door" - access to certain rooms may be allowed only to some employees, the data of cards, which are entered in the corresponding database. Then an attacker with a duplicate access card of an office worker will not be able to enter premises with a higher level of protection;
- "card - time" - after the end of the working day, as well as on weekends and holidays, access to the territory of the enterprise and / or computer networks may be prohibited for all employees;
- "repeated passage" - such a distinction will not only prevent an intruder with a clone of the card of an employee already present at the workplace from entering the building, but will also prevent the employees themselves from letting strangers through their card;
- "Exit without entry" - with this policy, the system will not allow an intruder who entered without identification after an employee of the enterprise, but will not be able to exit using the cloned card of an employee who has already left the workplace.

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 [8]. Nwadialor [9] 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 [10] 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 crds 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 [11]. 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" [11]. 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 [12]. 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 [12].

Forms of Identification Cards

Jamie [13] 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.

Drivers 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 [14].

Methods

In Spain, Portugal, and Latin America, over 9 million university students use a Student Smart Card, developed by Banco Santander in 279 universities.

The University Card is an ID, an access card, a payment card, and a wallet.

The Algerian health program uses smart health cards for patients (here in a reader) and smart USB tokens (with a chip) for health professionals. Discover the benefits of health cards in universal health care *systems.*

Electronic IDs

An electronic ID (e-ID) card fulfills various roles: it acts as a traditional means of identification, as a travel document, and finally, as a passkey to citizen's data.

Many international regulations and standards have been established on e-ID, most of which are applied by States.

The public has become accustomed to computerized smart cards through their use in the banking system, and as a result, their reliability is no longer questioned.

National ID cards are now also being used to access an array of services that were previously difficult to synchronize.

The e-ID card (aka computerized National identity cards) can be used for identification and authentication and electronic signature. Thus, this system enables several previously complex information paths to be simplified.

It can be used as[15]:

- A representation of sovereign authority certifying that the holder is in a legitimate legal position to their national jurisdiction.
- A means for citizens to access services and exercise their rights and duties to the public authorities.
- A genuine seal of authenticity that the citizen can use to authenticate their actions regardless of the exchange formats and media used, since the data used to ensure security and trust also guarantee the legal validity of any transactions certified in this way.

Health and health insurance cards

Health cards, including a microprocessor, also act as a significant component of an IT system.

They identify the holder and their affiliation to an organization and verify their rights. These cards are widely used. Every French and German citizen has a smart card for health insurance.Unlike paper documents, which can easily be forged, these tamper-proof devices are challenging to reproduce or unlawfully manipulate[16].

2020-2021 market share forecasts

1. Telecom (SIM cards) accounts for 52% of the total market,
2. Payment and banking cards for 34%,
3. Government (eIDs and e-passports) and healthcare for 4%,
4. Device manufacturers for 5%: mobile phones, tablets, navigation devices, and other connected devices, including an embedded secure element without SIM application,
5. Others for 5%: cards issued by operators, for transport, toll or car park services; cards for pay-TV; physical and logical access cards[17].

Significant trends for 2020 and 2021 (updated)

- The device manufacturer segment (OEM) is expected to be somewhat dynamic, with a +3% growth in 2020. 2021 sales very much depend on the resilience of the market segments.
- The government and the healthcare segments are expected to grow slightly in 2020. But the pandemic has lowered the demand for new IDs and passports.
- 2021 remains uncertain; according to Eurosmart, financial services are impacted by market drops in smart credit cards, retail, and co-branded cards.
- The contactless interface has become the leading choice for financial services and governments. Covid-19 boosted contactless payments, positively impacting the contactless market.
- Lower demand for smartphones but increased need for connectivity stabilized the market in 2020. Eurosmart is forecasting a 1% growth for 2021[18].

A $21B market in 2023

According to Markets and Markets' recent research report, the smart card market value is expected to reach $21.57 billion by 2023.

Currently, smart cards and card readers account for more than 75% of the market.

The related market for software comprises management system software and databases. In addition, consulting, support, and maintenance services are also crucial.

The Asia Pacific is expected to take the largest share of the market, as reported by the same study.

- Prominent players in these markets are Gemalto (now part of THALES), Giesecke and Devrient, and IDEMIA (formerly Oberthur Technologies and Morpho), to name a few.
- Major smart card microprocessor vendors are Infineon Technologies, NXP Semiconductors, Samsung, and STMicroelectronics.
- The Mordor Intelligence market study, excluding readers and services, sizes the smart card market at USD 8.14B in 2019 and 11.50B by 2025[19].

Discussion of the results

An access card is a user ID that contains some information - a key that opens a door or access to resources. It is hard to imagine the modern world without contactless and contactless identification technologies.

Use of bank cards (magnetic stripe, EMV chip cards, contactless payments PayPass, payWave); RFID cards for transport, entertainment and loyalty programs: issuance of compulsory health insurance policy and social cards of Moscow, and, of course, physical access and logical access cards to the computer and the company's IT resources. extensive use of access cards [20].

However, “card” is a common concept because the identifier key can be in the form of a fob, a tag, a tag, and so on. Mobile phones or other devices that support NFC technology will not last long. used as an identifier [21].

Therefore, the issue of security of data transmission from the identifier to the reader is more relevant than ever. The risk of copying data from cards and cloning them is increasing every day, forcing us to take a more conscious approach to choosing technologies that provide secure identification.

Weakness of the access card

Typically, vulnerabilities are assessed by three main threats identified when working with contactless cards: data privacy, duplication of access cards, and cloning.

Insecurity of confidential information

The unreliability of confidential information, if the identifier is stored explicitly and is not protected from any reading, makes the access card and the entire system the most vulnerable, allowing attackers to access not only the object but also the data. about the cardholder. The problem is solved using DES, 3DES, AES encryption algorithms [22].

Replay

Because the same information is transmitted each time the card is read, it can be replayed to hold, record, and enter the room. Repeat protection is provided by the access card and mutual authentication of the student.

Cloning of access cards (copying)

The most common way to bypass access control is to clone the cards with a programmer without the cardholder noticing. If the information is stored on the card in an open area and is not protected from unauthorized reading (for example, on Em-Marine standard cards), the access card can be copied [23].

The intruder reads data from the card using a compact and very affordable device - a duplicator. To do this, you just need to approach the card, send a signal from the duplicator to it that simulates a reader signal, receive a response signal from the card, write it to the device memory, and then to the card slot.

However, with the help of software you can configure access control (diversification of keys), which increases the reliability of access control systems using such cards [24].

Security of access cards

Of all the radio frequency technologies, 125 kHz frequency cards are the most vulnerable in terms of the above parameters. However, not all non-standard cards deal with simple hacking, and many modern identifiers are protected from such threats using advanced technology. For example, the protection of access cards with a frequency of 13.56 MHz is provided by mutual authentication between the card and the reader, the process of which is carried out in encrypted form by creating and confirming the diversification key.

The issue of security of identification technologies is no less important than the analysis and evaluation of the capabilities and capabilities of the system at the software level. We will therefore take a closer look at ways to protect access cards [25].

DES, 3DES, AES encryption

DES, 3DES, AES symmetric block encryption algorithms, where a single key message is used to both encrypt and decrypt, while the key length remains constant.

DES: 56-bit key length (and 8-parity bits), 64-bit block size was the U.S. national standard (ANSI X3.92, 1977). Modern computers are destroyed over a period of time by incredible power attacks.

Triple DES (ANSI X9.52), 3DES - 56-bit 3 (sometimes two) three-way encryption with different keys. With a high level of protection, it has much lower performance.

AES (originally proposed by Rijndael, Joan Dieman from Proton World International and Katholieke Universiteit Leuven, Vincent Rijman, Belgium): variable switch length up to 256 bits. The new national standard for the United States is selected from several candidates in the AES test because it combines simplicity and high performance.

"Rijndael analyzed the appearance of the algorithm, including power consumption and run time, and showed good resistance to attacks trying to decode the encrypted message. Typically, the ability to resist them is provided by special coding to equalize the power consumption level. The AES can be easily protected from such attacks because it relies mainly on boolean operations. In addition, it has passed all tests excellently in smart cards and hardware applications. Richard Smith, PhD, Chief Engineer, Secure Computing Corporation.

There are calculations showing that the energy of our galaxy is not enough to search for a 256-bit key with the brute force method, if it is used optimally. 128 bits are enough for real tasks.

The use of DES, 3DES, AES encryption algorithms allows access cards to be protected from unauthorized access to confidential data.

Mutual authentication

If a reciprocal authentication algorithm is available, the access card entering the reading zone gives the reader a unique CSN number and a 16-bit random number. In response, the reader creates a diversification key that must match the key written on the card using the Hash algorithm. If compatible, the card and reader share 32-bit answers

According to the principle of action

According to the principle of operation, access cards are contact and contactless (proximity cards). Non-contact provides ease of use (no need for a line of sight and a specific position of the card), the reading distance is longer, as a rule, resistant to environmental influences and the service life is extended. However, in some cases, the contact method of reading, as well as the regular replacement of cards, increases the level of security (e.g., bank cards) [26].

According to the reading range

The reading range is also in a very wide range from 0 (contact access cards) to 300 meters (active contactless cards).

On identification technology

Depending on the identification technologies provided by the system, the following are distinguished [27]:

- access to cards using barcodes;
- magnetic stripe access cards;
- RIFD cards;
- smart cards;
- Multi-technology (including biometric) access cards.

The first two technologies are often used as additional protection on joint access cards. And the leading technology in this segment of ACS is undoubtedly RIFD (Radio Frequency Identification) - radio frequency identification.

RIFD cards

An RFID card is basically a data carrier (transponder) from which information is read and written via radio signals. RFID cards are also called RFID tags or RFID tags.

RFID tags

When talking about radio frequency identification technology in security and access control systems, it should be noted that the simplest passive RIFD tags are often used to protect goods from theft. A one-bit transponder is sufficient for this purpose, indicating that it is inside it when it enters the reading zone.

It is also possible to sew various RIFD tags in the form of capsules under the skin of pets to identify them in the access control system.

Advantages of RFID cards

Contactless access cards based on radio frequency identification technology allow quick access to the system without requiring the exact position of the tag in space. In addition, RIFD cards allow you to work in harsh environments, perform long-distance identification, and have a long lifespan.

Using modern technology, RIFD cards can contribute to the creation of two-factor identification systems (multi-tech access cards), as well as solve additional tasks if a smart card based on radio frequency identification is used.

RFID cards are divided into:

Passive RFID cards do not have their own power supply. They operate from an electric current induced in the card antenna via an electromagnetic signal from the reader. As a result, they have a minimal range, but this is sufficient for most systems. The cost of passive RFID tags is minimal.

Active RFID cards have their own power supply, which allows you to significantly increase the range, as well as use more active RFID tags in a more aggressive environment as there is improved radio signal transmission quality (where there is more noise to RF). signal), for example, in the presence of an increase in humidity (including water) or the presence of metal in the immediate vicinity (automobiles, ships and other metal structures). However, improving the technical characteristics of the work leads to an increase in the size of the RFID card, as well as a significant increase in its cost.

Semi-passive (semi-active) RFID cards, which are either battery passive or BAP. They have their own power sources, but their work is rarely (and only partially) aimed at improving the transmission of radio signals. RFID is usually done in the same way as passive RFID cards. And the power supply energy is diverted to other functions of the input card. For example, power supply of various sensors (for later downloading data through the reader), power supply of card protection systems or microchip charging on smart cards.

Conclusions

1. 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 va 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.

Literature

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:

22. Dinora Alisherovna Baratova, Khayrullo Nasrullayevich Khasanov, Ikromjon Sobirkhon Ogli Musakhonzoda, Maftuna Yuldashboy Qizi Tukhtarova, Khusniddin Fakhriddinovich Uktamov. Econometric Assessment of Factors Affecting the Development of Life Insurance in Uzbekistan. REVISTA GEINTEC-GESTAO INOVACAO E TECNOLOGIAS (Management, Innovation and Technologies) Journal. Vol. 11 No. 2 (2021). https://doi.org/10.47059/revistageintec.v11i2.1741

23. Uktamov Kh. F. and act. Improving the Use of Islamic Banking Services in Financing Investment Projects in Uzbekistan. REVISTA GEINTEC-GESTAO INOVACAO E TECNOLOGIAS (Management, Innovation and Technologies) Journal. Vol. 11 No. 2 (2021). http://www.revistageintec.net/index.php/revista/article/view/1869

24. Dinora Baratova, Khayrullo Khasanov, Ikromjon Musakhonzoda, Shokhruh Abdumuratov and Khusniddin Uktamov. The impact of the coronavirus pandemic on the insurance market of Uzbekistan and ways to develop funded life insurance. E3S Web of Conferences 296, 06028 (2021). https://www.e3sconferences.org/articles/e3sconf/abs/2021/72/e3sconf_esmgt2021_06028/e3sconf_esmgt2021_06028.html

25. Alikul Nomozovich Rakhmonov, Jamshid Sharafetdinovich Tukhtabaev, Alisher Xudayberdievich Eshbaev, Khusniddin Fakhriddinovich Uktamov, Barno Ramizitdinovna Tillaeva, Dilafruz Baymamatovna Taylakova, Bekzod Abduraxmanovich Shukurov, Magomed Abduaxat og'li Saidov. Economic And Legal System Of Elections And Characteristics Of Electoral Legislation In Germany. International Journal of Aquatic Science ISSN: 2008-8019 Vol 12, Issue 02, 2021. http://www.journal-aquaticscience.com/article_134719.html

26. Akbarovich Yadgarov, A., Khotamov, I., Fakhriddinovich Uktamov, K., Fazliddinovich Mahmudov, M., Turgunovich Yuldashev, G. and Ravshanbek Dushamboevich, N. (2021). Prospects for the Development of Agricultural Insurance System. *Alinteri Journal of Agriculture Sciences, 36*(1): 602-608. doi: 10.47059/alinteri/V36I1/AJAS21085. http://alinteridergisi.com/article/prospects-for-the-development-of-agricultural-insurance-system/

27. Tukhtabaev, J.S., Rakhmonov, A.N., Uktamov, K.F., Umurzakova, N.M., & Ilxomovich, R. (2021).Econometric Assessment of Labor Productivity in Ensuring the Economic Security of Industrial Enterprises. International Journal of Modern Agriculture, 10(1), 971-980. http://modern-journals.com/index.php/ijma/article/view/700