International Journal of Civil Engineering and Technology (IJCIET)
Volume 9, Issue 11, November 2018, pp. 1063–1071, Article ID: IJCIET_09_11_101
Available online at http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=9&IType=11
ISSN Print: 0976-6308 and ISSN Online: 0976-6316

SMART SOLUTIONS: PROTECTION NFC CARDS WITH SHIELDING PLATES

Iryna Bashynska*
Department of Accounting, Analysis and Audit, Odessa National Polytechnic University, Shevchenko av. 1, Odesa, Ukraine

Volodymyr Filippov
Department of Management named after I.P. Prodius, Odessa National Polytechnic University, Shevchenko av. 1, Odesa, Ukraine

Nadiia Novak
Department of Accounting, Analysis and Audit, Odessa National Polytechnic University, Shevchenko av. 1, Odesa, Ukraine
Corresponding Author*

ABSTRACT

In 2017 it was decided at the legislative level to introduce in the cities a system of contactless fare - an electronic ticket. This technology, among other things, involves the use of NFC cards. With the development of this technology, the issue of personal data security is becoming more acute. This technology works on radio waves, the transmission of which is hampered by water and metal. The use of water to protect the cards entails certain difficulties in implementation due to the instability of the substance, therefore, existing technologies use metal in one form or another. The article discusses the existing methods of protection NFC card, but besides advantages, these devices have several drawbacks, which is why in our opinion, they can not be implemented by the municipality as a means of protecting an electronic ticket. That's why we suggest using "NFC card with shielding protection".

Key words: electronic ticket, e-ticket, NFC, smart-city, shielding plate

Cite this Article: Iryna Bashynska, Volodymyr Filippov, Nadiia Novak, Smart Solutions: Protection NFC Cards with Shielding Plates, *International Journal of Civil Engineering and Technology (IJCIET)* 9(11), 2018, pp. 1063–1071.
http://www.iaeme.com/IJCIET/issues.asp?JType=IJCIET&VType=9&IType=11

1. INTRODUCTION

Efficient functioning of urban passenger transport is one of the most important conditions for the development of the social and industrial-economic sphere of any city [1; 2; 3]. Due to the growth and development of the city, the burden on public transport is increasing, inevitably there are problems related to the provision of transport services to the population.

Increasing the mobility of the population in the conditions of reduction of transportation possibilities leads to an increase in the filling of the salons. At the peak time, it reaches the physical limit.

Not provided not only a minimum level of comfort of passengers traveling, but levelled necessary, subject to safety during their transport. The absence of a conductor in the cabin imposes on the driver additional duties, the performance of which distracts his attention. In some cases, existing standards of work of drivers may be violated, which results in their fatigue and, consequently, increase the probability of an accident. Violation of the rules of the road and the rules of carriage of passengers, poor quality and unsafe service of the inhabitants of the city increasingly become a serious problem of the transport network of our city.

One of the principal problems in organizing the operation of public transport in the city of Odessa is the fact that the financial and economic results of the carriers' activities (especially the volume of revenues) depend on the quantitative indicators of their work – the number of passengers transported.

Under the existing conditions there is almost no real control over the actual number of carried passengers, both paid and privileged. In addition, the quality of carriers' performance is ignored – the number of trips in the section of routes, class requirements, passenger capacity of rolling stock, observance of schedules and schedules of traffic.

In this case there is a negative, from the point of view of the quality of transportation, built on the money relations "passenger-driver-carrier". Thus, the priority interest of both drivers and carriers is ensured exclusively to the number of paid passengers, which in turn often leads to the neglect of quality indicators of the service of the route network, violations of the high-speed mode, and traffic rules.

The need to improve the quality of services provided by all types of public transport of the city, the need to unload the passenger traffic in areas with high traffic demands a change in the concept of further development of urban transport with an orientation towards European principles and standards.

Therefore, on January 17, 2017, the Verkhovna Rada of Ukraine adopted the Law No. 1812-VIII, which establishes the legal framework for the introduction of an automated payment system for fares in urban passenger transport using an electronic ticket. Therefore, all Ukrainian cities have to introduce this technology in the near future.

This system assumes the following elements:

– self-service terminals for the sale and replenishment of electronic travel documents (with an NFC chip);

– equipment of the vehicle by on-board computer and validators;

– mobile payment control equipment.

Thus, the protection of card data is a pressing issue today [4; 5; 6; 7].

2. NFC TECHNOLOGY

Near Field Communication (NFC) is a short range communication that can connect two devices to transfer and retrieve data and information [[8]]; the technology of wireless data transmission between devices within a radius of 10 cm. The speed of information exchange is about 400 Kbps. It operates at a frequency of 13.56 MHz.

Very clearly the principle of operation of NFC-technology is shown in Figure 1 [8].

Figure 1 NFC using RFID infrastructure [8]

This technology is an extension of the contactless card standard (ISO 14443), which integrates the smart card interface and reader into a single device. The NFC device can communicate with existing smart cards, and with ISO 14443 readers, and with other NFC devices and is thus compatible with the existing infrastructure of contactless cards already used in public transport and payment systems.

The main characteristics of the technology:

- security - beyond 10 centimetres, no one can access the device;
- speed - gadgets with NFC connect almost instantly, with the exception of models with different locations of NFC chips - this takes 5-15 seconds for a connection;
- minimum power consumption - the transmitter does not send and does not catch the signal at a long distance, therefore the battery charge is not consumed.

Gadgets with NFC are connected via Bluetooth without additional approvals - the area of the NFC chip must be brought to the wireless column or headset. And with this feature, it is easy to transfer videos, photos, applications, and a link to a website by tapping devices.

To date, NFC technology has become widespread when paying for public transport. Since this innovation is at the stage of development, it found its main application (in Ukraine) when paying for travel in the metro and from 01.11.18 a test version of the electronic ticket was introduced in Kiev.

3. EXISTING METHODS OF PROTECTION NFC CARDS

As mentioned above, NFC-cards are sufficiently protected, but with the development of this technology, the issue of personal data security is becoming more acute. NFC simplifies and speeds up the payment process, but the risk of fraud and data reading increases, with the help of a special scanner that can debit money from any contactless card by individuals and the fraudster will not need a card number or PIN code to carry out financial transactions. Thus, it becomes necessary to protect personal data.

This technology works on radio waves, the transmission of which is hampered by water and metal. The use of water to protect the cards entails certain difficulties in implementation due to the instability of the substance, therefore, existing technologies use metal in one form or another.

Today there are several protection options:

1) Shielded case for reliable protection of a bank card and a smartphone from fraudsters (Fig. 1) – thanks to its special design, the plastic card will be protected from unauthorized access. It is an ordinary plastic case, but at the base there is a metal layer that allows you to skillfully absorb radio waves and block the possibility of radio communication between the card and the reader. Also, this case helps to keep the card intact and protect it from the possibility of mechanical damage or moisture on the surface. This method of card protection is the most budget and popular.

Figure 2 Shielded plastic case with metal layer

2) Wallet with protection FRID (Fig. 3) – is a more expensive protection option. It is based on special radio-absorbing materials that reliably block all scanner signals when the wallet is closed.

Wallet has options such as:

- blocking from the possibility of access by any foreign devices while the card is in the wallet.
- reliable protection against demagnetization, even in the case of being close to a source that performs strong magnetic or radio emission.
- if it's not a card, but a phone, the wallet can protect it from tracking.

Figure 3 Wallet with protection FRID (design option)

3) Backpack or briefcase, with a compartment or pocket, equipped with blocking signals and preventing wireless infiltration of a laptop, tablet, smartphone, card. Keeps data safe, and

also does not allow to trace a geographical location of the person without the knowledge of the user.

Besides advantages, these devices have several drawbacks, which is why, in our opinion they can not be implemented by the municipality as a means of protecting an electronic ticket.

The main disadvantage of 2 and 3 options is the high cost. The disadvantage of the first option, despite the reasonable price, is that it is not attached to the card itself and can be lost quickly enough. Also, the card in this case is hard to insert into the wallet, because it turns out decently more than a standard card.

Figure 4 Backpack and briefcase with protection FRID (design option)

4. SHIELDING PLATES FOR PROTECTION NFC-CARDS

As shown by the analysis of the risks of implementing smart accounting system in urban passenger transport [9], one of the populations high enough risk is fears about the theft of money from criminals.

To minimize this kind of risk, we suggest using "NFC card with shielding protection". This is a plastic card with a NFC chip, which is protected on both sides by shielding plates attached to it by means of a plastic or metal block (grommet, screw) (Fig. 5-6)

Figure 5 Option design to reduce the cost of technology

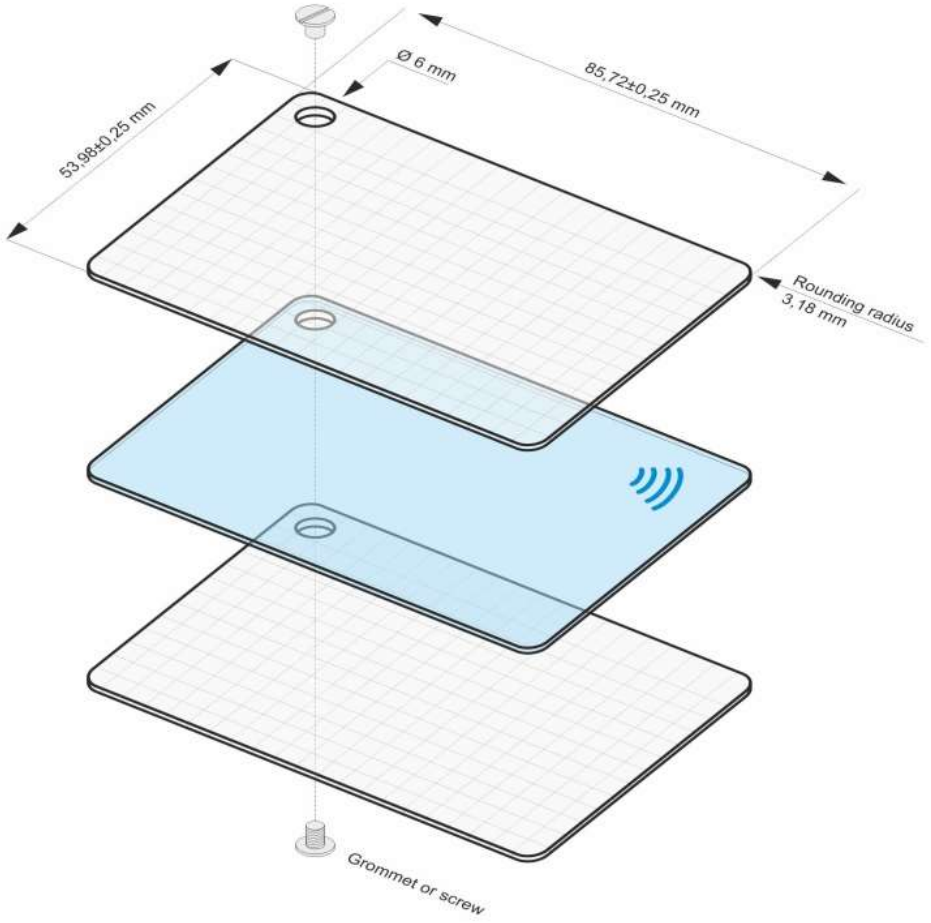

Figure 7 Option design to reduce the cost of technology

Plates are a multi-layer coating, in which the outer layers are made of plastic (with the possible application of graphic and text elements), and the inner one is a foil mesh.

The proposed technology has passed empirical approbation: thea test for effectiveness has been conducted. The simplest way was to use the NFC Tools mobile application (NFC manager, NFC reader etc.). The card with the shielding plates was checked as follows:

- run the NFC scanning application
- open the Reading tab
- attach the card with the plates to the smartphone
- if the application detects a card, this technology does not block NFC / RFID signals. If the application does not detect anything, then the plates work.

This application has confirmed that these plates work and can protect an NFC-tagged card from unauthorized access.

Estimated cost of this technology (including the production of NFC-cards themselves) is shown in Table 1. The calculation was made based on average prices in Odessa, depending on circulation.

Table 1 The calculation of the estimated cost of this technology

Name	Price, $	Circulation, pcs			
		100	**5000**	**10000**	**> 10000**
NFC card	for 1 pc	0,44	0,35	0,34	0,33
	for the total circulation	43,93	1771,43	3435,71	∞
Protective plate	for 1 pc	0,16	0,09	0,08	0,07
	for the total circulation	162,50	375,00	767,86	∞
Grommet1 with installation	for 1 pc	0,03			0,02
	for the total circulation	2,68	133,93	196,43	∞
Screw2 (quick lock), reusable	for 1 pc	0,0307		0,0268	0,025
	for the total circulation	3,07	153,57	267,86	∞
NFC card with shielding protection	for 1 pc1 for 1 pc2	1,06/ 1,0607	0,56/ 0,5607	0,52/ 0.5268	0,49/ 0,495
	for the total circulation1 for the total circulation2	106/ 106.07	2800/ 2803,5	5200/ 5268	from 4900,49/ from 4950,495

5. DISCUSSION

In this part, the answers to our study questions will be discussed.

5.1. Does it make sense in this technology, if on the e-ticket card it is assumed to store small amounts?

As shown by an empirical experiment to test this technology, a smartphone and an application installed on it are enough to interact with NFC-cards. This system protects more against the risks of non-acceptance of an electronic ticket by the public than the protection of financial resources. However, if every day even $ 2 will be stolen from the card, it is enough that in a week the person stops using it.

5.2. Is it possible to reduce the cost of this technology?

Sure. It is even possible to make a profit from the implementation of this system, for example, in an electronic ticket. As mentioned above, the protective plates involve the application of text and graphic images that can be used for promotional purposes, even by municipal services. Figure 1 shows an example of placing advertising text on one of the sides of the card, namely, reference information, where, among ordinary phones, are advertising information.

Emergency telephone numbers and reference information services

911 – emergency;
102 – police;
103 – ambulance;
…
000-00-00 Taxi
000-00-00 Emergency opening of locks
000-00-00 Round-the-clock legal assistance
000-00-00 Pharmacy help

Figure 7 Option design to reduce the cost of technology

5.3. What are the opportunities to use this technology, in addition to an e-ticket?

This technology has a wide range of applications. Particular attention should be paid to reusable screw. This element involves lengthening itself and due to this, you can additionally insert up to 2 cards between the plates (Fig. 8). For example, in addition to this card, you can also add a bank card, which will also be protected from unauthorized access.

Figure 8 Design option for the popularization of technology through usability

6. CONCLUSIONS

The purpose of this study was to study the NFC technology, to study the existing protection technologies and, in identifying shortcomings and the impossibility of using them for e-tickets in urban transport, to offer own technology.

The own technology was proposed, namely the use of shielding plates containing metal with two variants of their attachment to the card: using the grommet and using a screw. The article also examined the advantages and disadvantages of both options.

This protection was tested empirically and its effectiveness was proven using a mobile NFC card reader application.

REFERENCES

[1] T. Sakulyeva. Megapolis public transport system, *International Journal of Civil Engineering and Technology (IJCIET)*, 9(10), 2018, pp. 647–658.

[2] Bashynska, A. Dyskina The overview-analytical document of the international experience of building smart city, *VERSLAS: TEORIJA IR PRAKTIKA / BUSINESS: THEORY AND PRACTICE*, 2018 19: 228-241 https://doi.org/10.3846/btp.2018.23

[3] H. Kotak, P. Mamtora, D. Mehta and G. Vithalani. Automated car parking system with NFC access, *International Journal of Electronics and Communication Engineering & Technology (IJECET)*, 5 (4), 2013, pp. 201-206

[4] M. Amoud, I. Elrhaffari, S. Younoussi, O. Roudiès, Smart buildings: a systematic survey on cyber security *International Journal of Civil Engineering and Technology (IJCIET)*, 9 (10), 2018, pp. 360-368

[5] I. Bashynska, Using SMM by industrial enterprises. *Actual Problems of Economics*, 12 (186), 2018, pp. 360–369

[6] K. Tanashchuk, K. Kovtunenko, Yu. Kovtunenko, Theoretical and Methodical Principles of Capital Structure Management in the Innovation Activity of Telecommunication Operators, *Journal of Automation and Information Sciences* 50 (3), 2018, pp. 71-84. http://10.1615/JAutomatInfScien.v50.i3.60

[7] Prabhakar Naidu R and Prof. Padmavathamma M, An Architectural Approach to Provide Security to The LL and CL in Smart Phone ADHOC Networks (SPAN). *International Journal of Computer Engineering & Technology*, 8(6), 2017, pp. 1–11.

[8] M. Karsen, Y. Kurniawan, C. Cassandra and H. Juwitasary, NFC design for attendance system in the university, *International Journal of Mechanical Engineering and Technology (IJMET)*, 6 (9), 2018, 566-571

[9] I. Bashynska, S. Fillypova, Risk Management. Practical lessons & Case Study: textbook (Kharkiv: Disa plus, 2018), 121 p.