ADVANCES IN CYBER-PHYSICAL SYSTEMS

Vol. 7, No. 1, 2022

A SECURE DESIGN ON MIFARE CLASSIC CARDS FOR ENSURING CONTACTLESS PAYMENT AND CONTROL SERVICES

Busra Ozdenizci Kose[1], Hakan Uluoz[2] and Vedat Coskun[3]

[1]Gebze Technical University, Kocaeli, Turkey
[2]Konfides Information Technologies, Istanbul, Turkey
[3]Beykent University, Istanbul, Turkey
Authors' e-mail*: [1] busraozdenizci@gtu.edu.tr,*
[2] hakan.uluoz@konfides.com, [3] vedatcoskun@beykent.edu.tr

https://doi.org/10.23939/acps2022.__.___

Submitted on 25.03.2022

***Abstract*: Today, various contactless smart cards are used to protect our personal information and to perform secure and fast transactions. Many contactless smart card applications are becoming commonplace, from corporate access control cards to electronic passports and financial payment. There is a wide variety of smart cards on the market that differ in size, chasis, memory, computing power, and even the security features they provide. Although MIFARE Classic cards, which are used in many areas due to their price performance, meet certain security and functional needs, the weaknesses of these cards have made the applications and systems they are used in question. The aim of this study is to introduce a new design on MIFARE Classic contactless cards that will eliminate the basic shortcomings with minimum impact, and to perform high-security payment transactions using these cards, which do not support high-security payment transactions in their basic design. By using flexible data organization and storage scheme, their sector structure can be used for different purposes. The proposed new design includes derivation of critical card data by using card-specific information which ensures that the keys that provide access to the sectors of card are different on all cards; protection of card information through a certificate mechanism; usage of a new data structure with mirroring and redundancy methods to ensure data integrity and provide a server-side authentication mechanism for online transactions. It is possible that the proposed new design will pave the way for the secure use of MIFARE Classic cards in new generation payment and control systems.**

***Index Terms*: MIFARE Classic, smart cards, secure design, payment services, control services**

INTRODUCTION

In recent years, smart cards have been used frequently in a wide variety of applications requiring strong security, replacing barcodes, magnetic stripe cards and paper tickets. Contactless smart cards serve many applications covered by contact smart cards by eliminating the need for contact between the card and the reader, enabling faster and more convenient operation.

A contactless smart card includes an embedded smart card secure microcontroller or equivalent intelligence, internal memory and a small antenna and communicates with a reader through a contactless radio frequency (RF) interface [1-3]. It communicates with a card reader wirelessly through an induction technology based on ISO/IEC 14443 standard [1]. Consisting of a small piece of memory that can be accessed wirelessly, contactless smart cards also have some computing capabilities, unlike RFID tags. These cards only need close proximity to an antenna to realize a transaction.

A number of large-scale applications that need to protect personal information and/or deliver fast, secure transactions are provided by contactless smart cards. Transit fare payment cards, government and corporate identification cards, documents such as electronic passports and visas, and financial payment cards are some significant examples of these applications [3, 4].

There is a huge variety of smart cards on the market which differ in size, memory, computing power and even in the security features they provide. Today, the MIFARE product family is reported to be the most widely used contactless smart card technology in the market [5]. All MIFARE cards operate at a 13.56 MHz frequency and are made by NXP Semiconductors – part of Phillips Electronics. MIFARE is a product family that is introduced by NXP Semiconductors in 1995 [5-7]. As it has been highlighted in [5, 8], more than 500 million smart card chips and 5 million reader modules have been sold since the MIFARE card was introduced. The best part of MIFARE cards is that it allows multiple application uses. With a read/write distance of at most 10 cm (4 inches), they can be used in various applications worldwide. There are several distinct types of MIFARE smart cards available: DESFire, Ultralight, Plus, Classic, and SmartMX [5-7].

MIFARE Classic cards have been used in many areas since they were initially introduced in 1994; they are still widely used and preferred in new systems due to the price performance they offer [5-7]. They are facilitated in areas such as automated fare collection system, staff ID cards, access control management, contactless/cashless payment, parking payment, campus/student cards, loyalty cards, tourist cards,

transport ticketing, event ticketing, mobile ticketing, library cards, fuel cards, hotel key cards, taxi cards, product authentication, production control, car rental cards, car fleet management, fuel cards, interactive lottery cards, social welfare cards, waste management [5, 8-10].

A. RESEARCH PROBLEM AND PURPOSE

Although MIFARE Classic cards met certain security and functional needs, the weaknesses of these cards have made running systems questionable over time. The critical weaknesses can be summarized as follows: (1) The fabrication serial number (i.e., Unique Identification Number, UID) of each card was determined 4 octets on previous cards and this value has now been exceeded which is determined as 7 octets on current cards, (2) The keys used to access the data cells of the cards can be captured by examining the reader-card communication with interruption method, (3) Finally, there is no mechanism to ensure information consistency in the data cells of the cards.

In order to eliminate the basic weaknesses, the manufacturer has released new generation MIFARE cards at various levels -such as DesFire, SmartMX- over time. But these cards are partially or completely incompatible with older cards. Both the cost of required implementation and system component changes (software and hardware) and the cost of new cards have limited the use of new generation cards. Today, they are still widely used in systems that do not require extremely tight security.

The aim of this study is to present a new design on MIFARE Classic contactless cards that will overcome the aforementioned basic shortcomings of these old generation cards with minimum impact, and to perform high-security payment transactions using these cards, which do not support high-security payment transactions in their basic designs. Since these cards can respond to various personalization requests with their contactless interface, and have a flexible data organization and storage scheme, the sectors of the card can be used for different purposes.

The rest of this paper is organized as follows: Section II highlights a brief information about MIFARE Classic smart cards and explains the challenges. Section III presents the proposed secure design for MIFARE Classic smart cards. Finally, the study is concluded in Section IV.

MIFARE CLASSIC CARDS

MIFARE Classic card is the pioneer in contactless smart ticket ICs operating in the 13.56 MHZ frequency range with read/write capability and ISO 14443 Type A 1-3 compliance [5]. Like other contactless smart cards, they use an internal antenna and chip those react once a card is within the magnetic field range of a reader. These cards are generally an excellent option for access control systems, event ticketing, public transport payment systems. Its design and implementation details are kept secret by its manufacturer.

The MIFARE Classic smart card is essentially an EEPROM memory chip which is divided into sectors with secure communication architecture [6, 7]. The memory supports basic operations such as read, write, increment, and decrement. Each sector on the memory is divided into blocks of 16 bytes. A logical structure of the memory of a MIFARE Classic 4k card is given in Fig. 1.

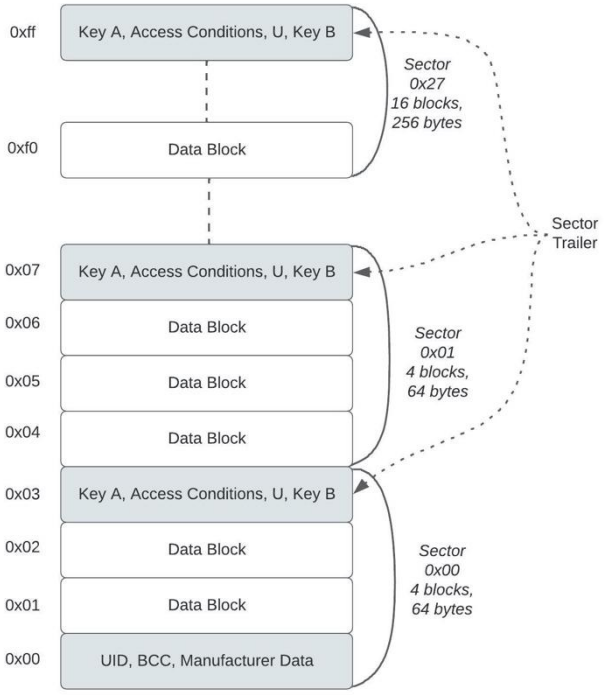


Fig. 1. Logical structure of MIFARE Classic cards with 4k memory [6, 7]

The sector trailer is the last block of each sector and contains two secret keys (i.e., secret keys A and B) and access conditions specific to that sector [6-8]. To operate on a given block, the reader must at first authenticate for the sector that contains that block. The access conditions define the operations that can be performed on the corresponding sector. Whether key A or B must be used depends on the sector's access requirements.

The block 0 of sector 0 includes special data which is read-only. The first 4 bytes contain the unique identifier of the card (UID) followed by 1-byte bit count check (BCC) which is calculated via XOR operation of all UID bytes [6, 7]. The remaining bytes are used to store manufacturer data.

MIFARE Classic EV1 represents the latest evolution of the MIFARE Classic product family [5]. It is available with 1KB or 4KB of memory (i.e., EEPROM) This highest evolution provides increased ESD (i.e., electrostatic discharge) robustness for easy handling of the IC during inlay and card manufacturing, strong radio frequency performance for optimized transactions, and also more flexible antenna designs. In

addition to 4 byte UID feature, this card supports 7 byte UID version with Random ID support [5]. However, as a result of advances in technology, it is no longer recommended to use MIFARE Classic cards for hosting sensitive data or access control [6, 7, 9-11].

One of the common usage patterns of MIFARE Classic cards in the field is to use only the UID information as an identifier without using the card's data fields and internal security mechanisms. However, there is a possibility of repetition of this UID information, especially in old version four-octal cards. In addition, the fact that the clones of the cards are on the market makes it very unsafe to function only on the basis of UID.

Furthermore, in systems where the internal security mechanism of the cards is used, when the keys for accessing the compartments are kept fixed (the same for all cards included in the system), access to all cards in the system can be achieved by examining a card with special devices and obtaining the keys, and even a completely new card can be created.

The other challenging issue is the lack of data integrity in systems where the information in the data cells of the cards is used. This problem arises in two ways: (1) First of all, it is not known whether the data is updated or not, when the data in a field is requested to be updated and no response is received from the card; (2) The more critical one is when the output of an operation on the card involves data cells that are too large to be updated at once. In this case, experiencing the first situation at any time of the transaction will result in a partial update of the card's data. This means that the card will remain in a state with incompatible transaction data and will cause the card to be inoperable without correcting the card's information with the authorized intervention.

PROPOSED DESIGN

As it is illustrated in Figure 2, Generated Access and Application Keys, and Certificate components are the main security dimensions of the proposed design on MIFARE smart card. The context diagram of the proposed design includes following components: MIFARE Classic smart card, Payment Control Device Payment Control Device and Authorization Management Server.

MIFARE Classic smart card is the media for payment and control applications. It includes two main security components: (a) generated access and application keys are the card-specific access and application keys derived from the card UID; and (b) certificate is the encrypted/signed data extract that validates the data on the card.

Payment Control Device evaluates the offline/online card information and authorizes the transaction. Authorization Management Server evaluates online/offline transactions, and disables problem cards when necessary.

As it has been highlighted in Figure 1, in order for the system to work securely, following essential functionalities will be provided by the proposed design on MIFARE Classic smart cards: (a) Derivation of critical card data by using card-specific information which ensure that the keys that provide access to the sectors of a card are different on all cards; (b) Protection of card information through a certificate which is generated by encrypting the information on the card; (c) Usage of a new data structure with mirroring and redundancy methods for ensuring the integrity of the sensitive card data and providing server-side approval mechanism for online transactions.

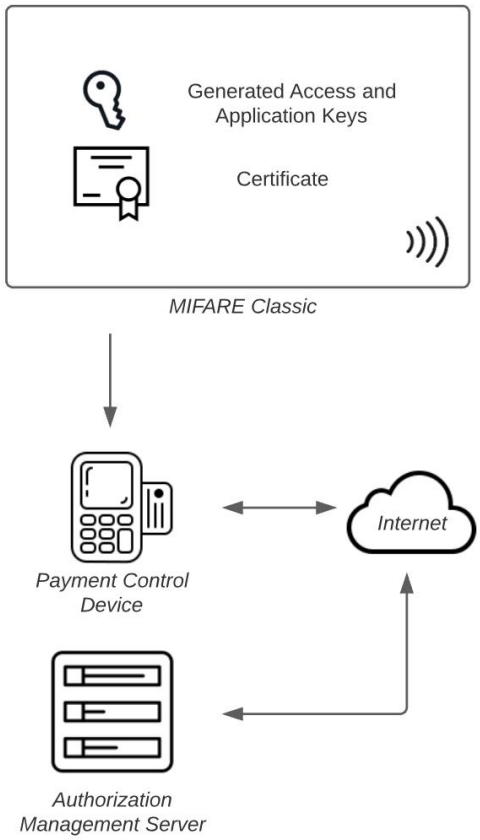


Fig. 2. Context diagram of the proposed model

A. DESIGN CONSIDERATIONS

Usage of different unique identifying information: Since UID information is not reliable enough on its own, this information will not be used directly, a unique identifying information (such as card number) written on the card will be used. However, since the UID is still the card's fabrication identifier, this information will continue to be used in transactions on the card. While it is not a problem for the system to have the same UID of two cards, it is recommended to choose cards with UIDs that are as long (i.e., seven octets) as possible. While the cards are personalized before they are used by a customer, the data relation between UID - Card will be recorded in the system management database. The UID will be used in derivation of card access and privacy keys, which will be detailed in the following sections.

Usage of different card access keys and certificate: Since the access keys of the cards are breakable, the same keys will not be used for all cards. The main keys of the system can be set on the basis of sectors of MIFARE cards, or can be set as same for each sector that provides semantic integrity (e.g., wallet sectors, parameter sectors). The keys of the cards will consist of the derivation of the sectoral information to be generated with the UID information through the one-way function (i.e., padlock function). In this way, the key set of all cards included in the system will be different, as long as their UIDs do not conflict. As a result, even if a card is examined and its keys are revealed, the data obtained will only be valid for that card, it will not be possible to produce or process a different card.

Since the encryption of critical data on the card will affect the read-only operations and third-party software, the critical data on the card will not be encrypted, but the encrypted format of these data as a certificate will also be kept in the relevant data block.

The keys required for the creation of these certificates will also be derived from the UID as a system master key and function code information. Although hardware keys of a card can be learned by intervening, certification keys cannot be obtained in this way. Even though it is possible to copy the card exactly, it is not possible to change the contents of the card.

Techniques for data integrity: For data integrity, mirroring and redundancy techniques are proposed on the sensitive data of the smart card. Accordingly, two pieces of functional blocks (for example wallets) will be kept structurally identical to each other, and cyclic type data to be used for record/history will be as one more record than necessary. There will be one system block in the system that can be updated at once. This block will carry a pointer to the current wallet and last registration information. If there is enough space on this block, wallet-specific information -such as Card Transaction Counter (CTC), balance- can be stored in this block for wallet integration and validity check purposes. The main idea is to make changes on wallets and records that are not valid when processing on a card. It will end up as updating the system block with current pointers.

A card's CTC information must constantly increase in its life cycle; which means that it will increase after each transaction attempt. The management software will check the card's information such as balance, Card Transaction Counter (CTC) constantly. Therefore, when a copied card is active in the system, if both cards are used together, the relevant card will be automatically blacklisted and their transactions will be prevented.

In line with all design issues, Figure 3 presents the basic process flow of payment transaction via MIFARE Classic smart cards. The new process stages that will be added to the existing payment process with other smart cards are indicated in gray.

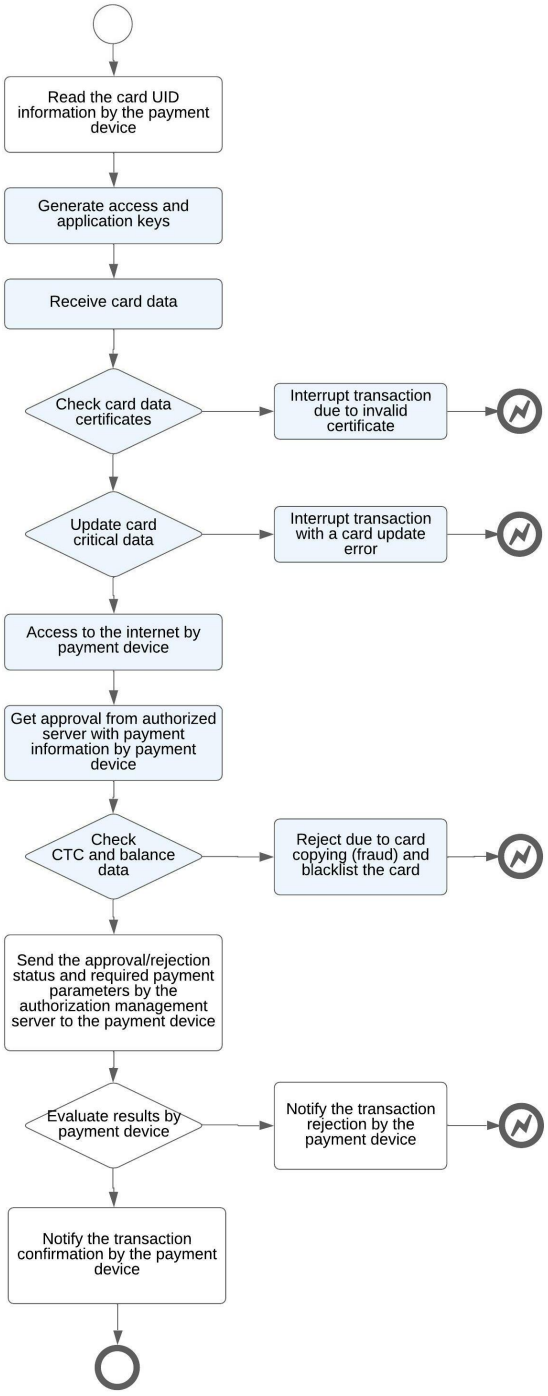


Fig. 3. Lifecycle of a transaction

B. GENERATION OF KEYS AND CERTIFICATE

The derivation of the critical card data is intended to ensure that the keys that provide access to the sectors of the cards are different across all cards. Since the only accessible data of the card is the UID, the sector keys of the cards can be derived with a logic dependent on the UID. For generation, symmetric or asymmetric encryption algorithms can be used considering the possibilities of the reader or the system to which the reader is connected. Many readers also have security

card -Secure Access Module (SAM)- access. In such a case, a SAM card can also be used for derivation/encryption. MIFARE Classic cards use 6 octets keys for accessing sectors.

As an example, suppose the system's master key is named as MK (112-bit TDES key), sector keys can be derived as follows:

Sector N Key A Derivation Data = TA
TA = { <N(1)><UID(m7)><Pad> }$_{8\ octets}$

Sector N Key B Derivation Data = TB
TB = { <Pad><UID(m7)><N(1) > }$_{8\ octets}$

N represents the sector number in Binary-Coded Decimal (BCD) format (0x12 12th Sector). Card UID information is taken as maximum 7 octets (last 7 octets, if more than 7 octets). If the card UID information is less than 7 octets, the information is completed in PKCS7 form to be completed to 8 octets. PKCS7 is the specific standard used for generation and verification of digital signatures and certificates managed by a PKI (Public Key Infrastructure).

Sector N Key A = [$TDES_{MK}(TA)$ XOR $TDES^{-1}{}_{MK}(TA)$] $_{last\ 6\ octets}$

Sector N Key B = [$TDES_{MK}(TB)$ XOR $TDES^{-1}{}_{MK}(TB)$] $_{last\ 6\ octets}$

In the case where the sector keys of each card in the system are generated in this way, for a malicious person who gets critical card data, the only way is to find another card with the same UID. Likewise, there is no way for the malicious person to generate access information for another UID with the information he has. Although this is possible, obtaining a card with the same UID or finding a programmable clone card would be relatively difficult and costly.

Different algorithms (DES, AES, RSA) can be selected considering the capabilities and processing speed of the reader and the connected system. For minimum transaction cost, the same keys can be assigned to sectors that provide semantic integrity in each transaction. For example, if the 3rd, 4th and 5th sectors are used in a transaction, sector 3 can be written to all, thus reducing the key generation time cost by 1/3.

The key(s) to be used for the certification of the data in the card can be generated in a similar way. For example, in the derivation data, a function code (F > 0x40) can be used instead of the sector number:

Certificate 1 Key Derivation Data = TX
TX = { <F(1)><UID(m7)><Pad> }$_{8\ octets}$

Certificate 1 Key Derivation Data = TY
TY = { <Pad><UID(m7)><F(1) > }$_{8\ octets}$

Certificate 1 Key = [$TDES_{MK}(TX)$ || $TDES^{-1}{}_{MK}(TY)$]$_{16\ octets}$
(|| concatenation operator)

Although encryption or certification of data other than the keys of the card cannot prevent the exact copying of the card, it will cause the copied cards to be detected and removed from the system very easily.

While designing the architecture and operation of the card, it is important for the process to be done as quickly and without errors as possible. In recent studies, it is suggested that the ideal contactless operation time should ideally be under 600 milliseconds. The longer the transaction takes, the higher the chance that the card will exit the contactless magnetic field and the transaction will be interrupted.

C. SAMPLE CARD DESIGN

A sample card design on MIFARE Classic Cards that can perform payment transactions is given in Table 1. Also, an example for the sector-based data design can be seen in Table 2.

Table 1

An Example of General Sector Structure

Sector	Description
3	System Sector
4-5	Wallet Sectors (Critical Data, Original and Mirror Data)
6	Parameter Sector (Non-critical data)
7-11	Last 15 transaction history (Critical Data)

The purpose of this sector in the system design is to point to the primary wallet sector and to store critical data. When performing a contactless transaction, there is no option to write or undo all the data at the same time. For this reason, during an operation, the wallet pointed by the system sector is considered as valid (if CTC is compliant) and the changes are made entirely in the other mirror wallet sector. When all changes are completed, the system sector is updated to display the new wallet. The system sector critical block is designed to be updated in just one command. Therefore, this unit works as a mechanism to confirm or undo the transaction.

This method prevents data that can be written to the card from being interrupted. The data is either completely written to the card or none at all. Likewise, when the command is confirmed, the modified wallet becomes valid.

In case of an interruption of transaction, since the last confirmation command is not executed, the old wallet sector will still appear as a valid wallet. The only point that cannot be resolved in this design is that it is not possible to receive a response to the confirmation command from the card. Even in this case, it is known that the transaction is either completely written down or

neglected. In such cases, the card is requested to be read again for transaction confirmation. When the card is read again, it can be understood that the transaction was made by comparing the data with the wallet data; otherwise, the transaction is restarted. Ensuring that quick completion of the process is the only way to avoid such situation.

Table 2

An Example for Sectors Design

	Length	**Description**
System Sector	1 octet	Active Wallet Pointer
	4 octets	CTC
	1 octet	Recent History Record Marker
	4 octets	Balance (Optional)
	2 octets	Status Flags (active, blacklisted etc.)
	36 octets	Reserved
Wallet Sector (x2 pcs.)	4 octets	CTC
	6 octets	Group Number
	6 octets	Transaction Number
	4 octets	Amount
	4 octets	Terminal Number (where the transaction is made)
	2 octets	Process Type
	14 octets	Transaction Date
	4 octets	Balance (optional)
	4 octets	Certificate
Parameter Sector	16 octets	Card Number
	4 octets	Expiry Date (YYAA)
	28 octets	User Name/Surname
Transaction History Sectors (x4 pcs. / 16 records in total)	16 octets	Compressed Transaction Data (CTC, amount, date etc.)

Each time the card is read into the reader, the reader software checks the certificate block after performing a logical check of the current sector. The certificate block encrypts the first 44 octets of the wallet data. As it has been mentioned, the key used in encryption is derived from the UID, so the certification key of each card is different.

If the certificate of the current wallet is correct, the new wallet sector is created with the updated information and the certificate is added. The CTC information is an incremental value each time the card attempts a transaction, as it has been proposed in our model. When the CTC value reaches the limit, the card can be disabled or reset again and continue to be used according to the system's demand.

If the system is operating online, the server is exited for approval after the card has been processed. Importantly, the card's UID information is never sent to the server. While a card is personalized and processed into the system, the UID - Card Number relationship is also recorded in the database at the beginning. Therefore, the server knows the UID information that the card should have. Even if a malicious person somehow copies the same card with a different UID, it will be impossible to pass the server control.

As for the last transaction, the server compares the last known CTC of the card with the incoming CTC information. If there is an inconsistency, it rejects the transaction and blacklists the card. Therefore, even if a malicious person succeeds in copying a card with its UID, it is not possible to continue with the original card. Likewise, regardless of whether the copied card or the original card is used first, if the other card is attempted to be used, both cards will be blacklisted and disabled. In order to prevent the copied card from being used first and reducing the balance with successive transactions, additional limits can be set for the number and total of daily transactions. The system can also work as offline. In such a case, the same situation will occur when the terminal performing the offline transaction does the daily reconciliation. However, although this model will not be as effective as working as online, security can be increased by keeping daily limits and blacklists in terminals.

CONCLUSION

This study aims at presenting a design that will overcome the basic shortcomings of old generation cards and to perform high-security payment and control transactions using MIFARE Classic contactless cards. By using their flexible data organization and storage scheme, their sector structure can be used for different purposes as it was explained.

The proposed design ensures that MIFARE Classic cards can be used securely in new generation payment systems with minimal administrator intervention. The proposed design offers a method in which payment transactions can be made at a level close to the security level of contactless cards, which use more expensive technologies in online transactions.

The model is fully compatible with existing systems and does not require replacement of cards and/or reader hardware. Organization of card keys and encryption or certification of card data are considered in separate contexts. The designed model can never make it impossible to copy cards, however it can definitely prevent creating new cards.

REFERENCES

[1] ISO/IEC 14443. Identification cards - Contactless integrated circuit(s) cards - Proximity cards (2001). Available at: https://www.iso.org/standard/28729.html

[2] K. Finkenzeller, (2010). RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication. (3rd ed.) DOI:10.1002/9780470665121

[3] K. Finkenzeller, (2003). RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. (2nd ed.) DOI:10.1002/0470868023

[4] B. B. Gupta and S. Narayan, (2020). "A survey on contactless smart cards and payment system: technologies, policies, attacks and countermeasures", Journal *of Global Information Management (JGIM)*, *28*(4), pp. 135-159. DOI: 10.4018/JGIM.2020100108

[5] Mifare Classic Family. Available at: https://www.mifare.net/en/products/chip-card-ics/mifare-classic/ (Accessed: 23 March 2022).

[6] F. D. Garcia, G. D. Koning Gans, R. Muijrers, P. V. Rossum, R. Verdult, R. W. Schreur, and B. Jacobs, "Dismantling MIFARE classic", in *Proc. European symposium on research in computer security*, 2008, pp. 97-114. DOI: 10.1007/978-3-540-88313-5_7

[7] G. D. Koning Gans, J. H. Hoepman, and F.D. Garcia, "A practical attack on the MIFARE Classic", in *Proc. International Conference on Smart Card Research and Advanced Applications*, 2008, pp. 267-282. DOI: 10.1007/978-3-540-85893-5_20

[8] W. H. Tan, "Practical attacks on the Mifare Classic. M.S. thesis", Imperial College London, 2009. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.739.1658&rep=rep1&type=pdf (Accessed: 23 March 2022).

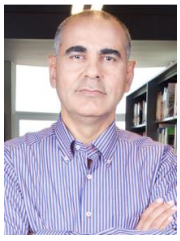
[9] K. Nohl, and H. Plotz, "MIFARE: Little Security, Despite Obscurity". Presented at 24th Congress of the Chaos Computer Club in Berlin, 2007. Available at: https://www.youtube.com/watch?v=QJyxUvMGLr0 (Accessed: 23 March 2022).

[10] F. D. Garcia, P. Van Rossum, R. Verdult, and R. W. Schreur, "Wirelessly pickpocketing a Mifare Classic card", in *Proc. 30th IEEE Symposium on Security and Privacy*, 2009, pp. 3-15. DOI: 10.1109/SP.2009.6

[11] K. E. Mayes and C. Cid, (2010). "The mifare classic story", *Information Security Technical Report*, *15*(1), 8-12. DOI: 10.1016/j.istr.2010.10.009

Dr. Busra Ozdenizci Kose is an Academician, Researcher, and Author. She received her PhD in Informatics at Istanbul University in 2016. She is a co-author of the books entitled ''Near Field Communication: From Theory to Practice'' published by John Wiley & Sons, Inc. in 2012, and ''Professional NFC Application Development for Android'' published by Wrox in 2013. Her research areas include Near Field Communication, Smart Cards, Mobile Communication Technologies and Blockchain Technologies.

Hakan Uluoz, MSc. is a Computer Scientist and Engineer. He is working as a Senior Engineer in R&D department of Konfides Information Technologies, Turkey. He received B.Sc. and M.Sc. degrees in Computer Science at Istanbul Technical University. He focused on various technologies within the payment industry, mainly cryptography, data security and data transmission. He is a believer and supporter of open-source technology.



Dr. Vedat Coskun is a Computer Scientist, Engineer, Academician, Researcher, Author and Consultant. He is the founder and manager of NFCLab@Istanbul (www. NFCLab.org), the world's leading research laboratory for Near Field Communication technology. He teaches contemporary topics in his courses including Blockchain Technologies, Mobile Technologies, Near Field Communication, Front-end – Back-end -Database Programming, Contemporary Software Development Methodologies and Cyber Security. He gave lectures in many universities abroad. He believes in the importance of academy-industry relationship in Information Technology, and in this direction, he undertakes tasks such as project development, research and consultancy for local and international companies.