A SIM CARD BASED KEY MANAGEMENT SYSTEM

[1]BUSRA OZDENIZCI KOSE, [2]SEMI ENIS MORKOYUN, [3]MOHAMMED ALSADI, [4]HACI ALI MANTAR, [5]VEDAT COSKUN

[1]Gebze Technical University, [2]Turkcell Technology, [3]Istanbul University, [4]Tubitak Bilgem, [5]Beykent University
E-mail: [1]busraozdenizci@gtu.edu.tr, [2]semi.morkoyun@turkcell.com.tr, [3]mehmet.alsadi@gmail.com, [4]ali.mantar@tubitak.gov.tr, [5]vedatcoskun@beykent.edu.tr

Abstract - Smartcard and mobile technologies are continuously evolving and leading to introduction of new value added mobile applications and services which offer attractive business opportunities. The aim of this paper is to present an efficient SIM based key management system (SIM-GAYS) including an innovative OTP generator to enhance cryptographic and security requirements of diverse mobile applications provided by service providers. By getting the advantages of SIM card technology and GSM capabilities of MNOs, the proposed framework fulfills the need for a centralized secure key management on SIM card that can be used by all sensitive service applications installed on the SIM card as well as on the Smartphone. This model will enable engagement of more service providers on SIM cards to provide new value added services easily, achieve compatibility faster and enrich the mobile ecosystem.

Keywords - Mobile, Smartcard, SIM Card, Key Management System.

I. INTRODUCTION

Mobile phones were firstly introduced to provide voice communication and then short messaging services (SMS). Later, Internet access via Wi-Fi or cellular data, camera capabilities, touch screen enhancements and other I/O operations came on the scene with the advancements on information storage and processing capacities of the mobile phones and GSM technologies. The Internet access and increasing data communication speed capability facilitated promising and innovative services -such as instant messaging, location based services, social media applications, electronic commerce, mobile signature, bank and payment transactions, public and citizenship operations, and even high performance gaming- on mobile phones. These developments lead mobile phones to evolve into Smartphones [1, 2].

The mobile ecosystem expanded and get rich with the developments on Smartphones. The initial status of the mobile ecosystem included only MNOs and mobile phone users as actors. Today, new technical requirements and specifications enriched the ecosystem with new players and actors such as Smartcard manufacturers and issuers, Smartphone manufacturers, mobile application developers, service providers, mobile phone users and Mobile Network Operators (MNOs). It is obvious that the role of MNOs is indisputable within the mobile ecosystem from the beginning to present. Smartphones need to have a SIM (Subscriber Identity Module) card which is obtained from a MNO in order to connect to the cellular network and Internet.

A SIM card -namely Smartcard of Smartphone- has its own operating system (such as JavaCard) and uses the energy of the Smartphone -on which it is embedded- to operate [3, 4]. Some programs and data are installed on SIM card by the card manufacturer and MNO before card is given to the user. After personalization of the card, it is made available to the user; however, the control on the card still belongs to MNO.

Without MNO approval, Smartphone user is not allowed to install a mobile application or to save data on the SIM card. When the capacity of the SIM card is enough and the permission of MNO is obtained, additional value-added mobile applications can be installed by the user on SIM card.

Depending on the service provided, data exchange is inevitable between the service application on Smartphone and the server of service provider. At the same time, exchange of the user's sensitive data (e.g., financial data, social media data, location data, identity data, and address data) should be safeguarded and protected against unwarranted disclosure; since such data is always threatened by malicious people.

The encryption keys and related algorithms -that are required to be used by third party organizations for performing payment operations or processing personal data– must be kept securely on mobile applications installed by the service providers on the Smartphone or SIM card. Furthermore, One-Time Password (OTP) service is required for more sensitive operations, which is produced by either the same mobile application or by the server of service provider and then delivered to the user via SMS.

Almost all services need a secure communication design for carrying sensitive data to minimize the security risks between the Smartphone user and service provider. In this sense, they may differ in terms of their security specifications; key management models, OTP services and encryption methods.

Technically, it is possible to install mobile applications on the SIM card or on the Smartphone. In terms of operating performance, memory, and storage capacity; it is difficult to install all service applications on SIM cards due to varying security requirements of mobile applications [5]. However, as a positive aspect, the enhanced capabilities of the

SIM cards provide much safer operating environment than Smartphone due to the robust security infrastructure -created by the card manufacturers during the design and applied the security procedures by MNO- which makes SIM card technology indispensable.

It is clear that service providers need to increase the efficiency of their applications and enhance compatibility of their security mechanisms via SIM cards owned by MNOs. Recently, there is a definite need for a centralized secure key management and OTP service on SIM card, which can be used by all sensitive service applications on the SIM card as well as on the Smartphone.

The aim of this paper is to present an efficient and centralized SIM based key management system, called SIM-GAYS to enhance cryptographic operations of diverse applications provided by various service providers. The proposed model will facilitate secure key management of services and provide the OTP generation capability on SIM cards. This model will enable engagement of more service providers on SIM cards to provide new value added services easily, achieve compatibility faster and enrich the mobile ecosystem.

This paper mainly describes the preliminary studies on the requirement for a SIM based key management framework, and introduces the conceptual model of the proposed framework. The rest of this paper is organized as follows: Section II highlights a brief information about SIM cards and concerns for key management. Section III discusses the proposed model with conceptual diagrams. Finally, the study is concluded and further work is explained in Section IV.

II. SIM CARDS AND KEY MANAGEMENT

Almost all of the mobile services running on the SIM card contain sensitive information and transactions. Each transaction performed on SIM card -such as mobile signature, personal data, ticketing and payment transactions- requires secure data storage, secure data processing, and secure data communication between the SIM card and the service provider [5, 6]. To enable secure communication, appropriate security algorithms, public and private key production, key exchange, and key management are important considerations.

SIM cards are improved from a few K capacity to 512K to contain more data, perform faster calculations, and provide advanced security functions. Depending on their key hosting capability, SIM cards are categorized into two groups; keyed SIM card and un-keyed SIM cards [5, 6]. Keys of the keyed SIM cards are registered by the card manufacturer on the SIM card during the production phase; which later will be used for encryption operations. Keyed SIM cards also have high data storage and computing capabilities. In case of un-keyed SIM cards, there is no key to use the services that require high security.

64K cards as un-keyed SIM cards, do not have embedded key pair for enabling secure service by the service provider application and hence do not have a key applet (i.e., the application that can generate and store keys on SIM card). On the other hand, 128K cards as keyed SIM cards are associated with key pair and segment. Also, 256K and 512K cards as keyed SIM cards have progressed with a high acceleration in the number of segments, key security and other issues; they have richer infrastructure and higher flexibility [5, 6].

According to the recent developments, data storage, data processing and data communication of the services to be provided on the SIM cards have some concerns as described hereunder:

- Since 64K cards have no key to be used by the service provider, a symmetric encryption key between the service provider and the SIM card needs to be generated via OTA as presented in our previous studies [5, 6].
- As SIM cards provide ideal environment for secure data and key storage, it is efficient to use stored keys on SIM cards for secure data encryption. However, currently it is not available for actors other than MNOs to perform data encryption via SIM card. The reason is that there is no centralized framework to manage the appropriate keys on the SIM card and to meet external requests.
- Depending on the SIM card type and capabilities, different keys must be stored on the card itself. Since 512K SIM cards are more flexible due to their high capacity, apparently more keys can be used and managed on them. On the other hand, as Smartcard capacities increase, the complexity of key management issue increases too.

It is clear that Smartcard processing and storage capacities increases as the mobile ecosystem advances. On the other hand, the complexity of managing security keys on the smartcards will increase as well. Therefore, there is an urgent need to develop an effective framework for secure key management on SIM cards.

III. A KEY MANAGEMENT SYSTEM ON SIM CARDS

In this paper, we introduce an innovative secure key management framework running on the SIM cards, called SIM-GAYS, which allows storage and usage of all keys (i.e., keys in MNO control, keys produced on the card, or even keys which will be produced later) on the SIM card. The proposed framework enable the keys on the SIM card to be safely used for authentication and authorization procedures and solve the aforementioned concerns.

A conceptual diagram of our proposed system is given in Fig. 1. The framework including an OTP

generator enables to perform key management and OTP operations on the SIM card itself in an efficient, scalable, secure and generic way.

As shown in Fig.1, key management system on SIM card communicates with Smartphone applications, SIM applets and Key applets in order to fulfill encryption, decryption and other tasks of Smartphone and SIM card applications. As mentioned, currently the number and type of keys used on the SIM cards vary according to the security requirements of mobile applications. The proposed framework aims to work with all currently existing and prospective Smartcard types, communicates with each key applet in the requested format and fulfills different communication requirements of each key applet.

When a SIM Applet -such as a credit card application- or a Smartphone application -such as a mobile ticketing application- needs to encrypt or decrypt a data –such as PIN or credit card number- or wishes to access a service provided by a key applet, it will access the SIM-GAYS module embedded on SIM card.

Consider a virtual mobile banking case. A mobile banking application on a Smartphone will store the credit card number in the application itself, but in an encrypted format provided by SIM-GAYS; instead of storing it in the memory. When credit card information is needed, the application asks SIM-GAYS to decrypt the data in order to obtain the sensitive data. After usage, the mobile application will destroy the sensitive data and continue to store the encrypted state of that data.

Another important module of SIM-GAYS is OTP generator that serve for all service providers to facilitate the OTP operation of users and service providers.

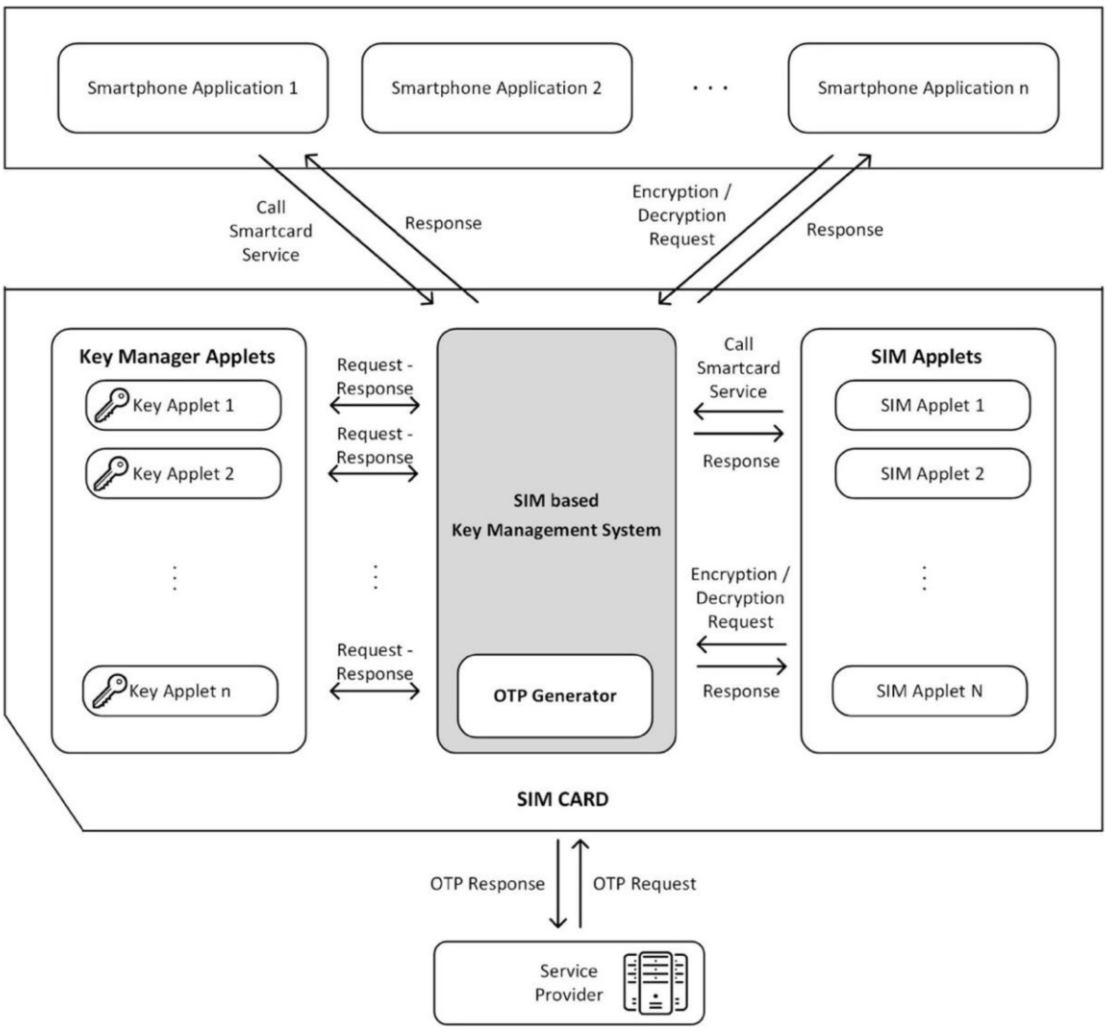


Fig. 1. SIM based Key Management System (SIM-GAYS)

Currently, OTP implementations are generally performed in two models: user enters the OTP code that comes from Service Provide server via SMS to the website; or an OTP code is generated by a mobile application and then the user enters the data on the website. In order to eliminate the differences and costs on service providers, and also to standardize the OTP operations for all applications, the SIM-GAYS provides its own OTP process; the user only needs to do is to approve usage of OTP generator on her Smartcard.

The preliminary conceptual design of the proposed OTP generator is given in Fig. 2. The flow of proposed OTP process under SIM-GAYS is described as follows:

(1) The user wants to enter a service provider's web page and inputs login details.
(2) When the service provider obtains user's request, this request is forwarded to the MNO of the user.
(3) MNO sends this request to the SIM card running on the Smartphone of the user by using GSM capabilities.
(4) SIM card sends a request to the user to confirm OTP generation.
(5) If the user provides approval, OTP generation process initiates by using the algorithm which will be detailed in further research.
(6) The generated OTP is forwarded to MNO.
(7) MNO forwards the generated OTP to Service provider.
(8) Service provider validates and confirms the entry of the user.
(9) Finally, service provider sends success notification to the user.

The proposed SIM-GAYS targets to communicate with applications that have different security requirements and specifications on the Smartphone as well as on the SIM card. The SIM-GAYS software and OTP algorithm on the SIM card to be developed needs to comply with the international GSM standards: GSM 11.14-SIM Application Toolkit (SAT) for the Subscriber Identity Module (SIM-ME) [7] and GSM 3.48-SIM Toolkit Security [8].

IV. CONCLUSION

This paper presents the preliminary research on a centralized SIM card based key management system, namely SIM-GAYS, which ensures multiple key management and storage in a secure zone of SIM cards. With the help of the framework model, the keys can be properly and safely managed according to the authentication, authorization and encryption requirements of applications installed on SIM card or on the Smartphone itself. Moreover, OTP generator component of SIM-GAYS on the SIM card allows more efficient transactions for all mobile applications by eliminating the complexities on service provider side. The further work will include security details of the SIM-GAYS, OTP algorithm design and other developmental issues.

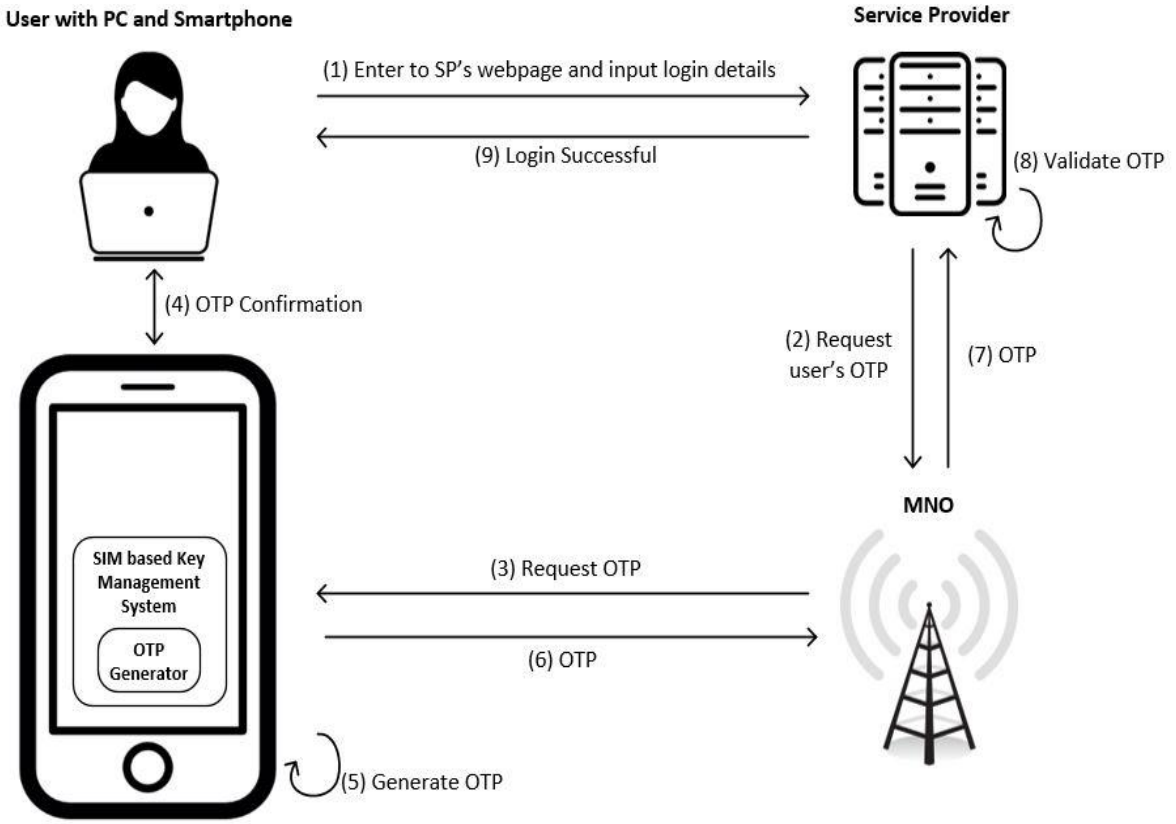


Fig. 2. OTP Generator Model

ACKNOWLEDGMENTS

This work is funded by TurkcellTechnology A.S. and TUBITAK (The Scientific and Technological Research Council of Turkey) under 1505 Program, Project no 5180027.

REFERENCES

[1] D. Theo, and S. Hultén. "A brief history of mobile communication in Europe." Telematics and Informatics 24.3, 164-179, 2007.

[2] K. Sameer and C Zahn. "Mobile communications: evolution and impact on business operations." Technovation 23.6, 515-520, 2003.
[3] J. Borst, B. Preneel, V. Rijmen. “Cryptography on smart cards”. Computer Networks, 36(4), 423–435, 2001.
[4] Smart Card Alliance. Smart card standards and specifications. http://www.smartcardalliance.org/smart-cards-intro-standards/. Accessed 25 May 2019.
[5] K. Ok, V. Coskun, S. B., Yarman, C. Cevikbas, B. Ozdenizci. “SIMSec: A key exchange protocol between SIM card and service provider.” Wireless Personal Communications, 89(4), 1371-1390, 2016.
[6] K. Ok, V. Coskun, C. Cevikbas, B. Ozdenizci. “Design of a key exchange protocol between SIM card and service provider.” 23rd IEEE Telecommunications Forum (TELFOR), pp.281–284, 2015.
[7] 3GPP, GSM 11.14-SIM Application Toolkit (SAT) for the Subscriber Identity Module (SIM-ME). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=423. Accessed 25 May 2019.
[8] 3GPP GSM 3.48-SIM Toolkit Security. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=149. Accessed 25 May 2019.

★★★