Challenges and Risks for a Secure Communication between a Smartcard and a Service Provider through Cellular Network

Kerem Ok, Vedat Coskun, Rahmi Cem Cevikbas

***Abstract*—Smart cards used in mobile phone, namely Subscriber Identity Module (SIM) cards, became a place where various value added services are proposed. SIM cards, in addition to authenticating users to the cellular network, contain a secure storage area, which provides necessary security conditions and performs data encryption and decryption. Mobile Network Operators (MNOs) and service providers such as banks use this area to provide value added services to the users. Security required value added services such as mobile financial services, e-government services, digital signature services can also be offered via SIM cards which require end-to-end secure data exchange between the service provider and the SIM card. In this paper, we analyze the current situation deeply, list several publications those are somewhat related to the subject, and put forward the risks and challenges with the problem.**

***Index Terms*—Smart card, SIM card, Mobile Network Operator, Service Provider, end-to-end security**

I. Introduction

Smart cards, being invented in the 1970s, initially used for cabled telephone payments in the 1980s. Microprocessor smart cards were introduced in those years as well, after which microchips were integrated into debit cards in the 1990s. Smart card based electronic purse systems which store values on a card and do not need network connectivity, i.e. offline systems, began to be used in Europe from the mid 1990s. One major improvement in smart card technology occurred in the 1990s; smart card based SIMs were introduced and used in GSM based mobile phone environments in Europe. The use of smart cards increased with the ubiquity of mobile phones. After the invention of smart card based SIM cards, SIM card technology is still developing.

The main motivation on the innovation of mobile phones and SIM cards was to make telephony –voice– calls on the go. In a short time, Short Messaging Service (SMS) is offered to users as a value-added service. MNO and the user of the phone were the only actors in the mobile communication during those times; when only voice and text messaging services had been used. A user needed to get a SIM card associated with her mobile phone number and place it to her mobile phone in order to use the proposed services.

In the upcoming years mobile phones are evolved to smart phones and started to fulfill additional needs of the users such as navigation, Internet access, digital camera etc. At the same time, SIM cards also needed to store more data and perform faster calculations. In this manner, SIM card capacities and capabilities are increased from 8K to 512K, which can store more data, perform faster calculations, and provide security functions as well. Smart phones together with SIM cards have been consequently used for digital signature, mobile financial services, e-government services, physical access control, loyalty and so on. Additional companies, called as Service Providers provided those new services, but not the MNOs. The name service provider is a general term and may change according the offered service such as bank, mobile phone manufacturer, transportation authority, and so on. The mobile communication ecosystem is flourished after new value-added services are offered to users and new technical requirements arose.

Security requirements for financial applications are vital. No financial service can be provided unless required security requirements are met, which required appropriate security protocols. Financial Service Providers also demanded that the intervention and role of the MNOs shall be minimal, so that, they need not trust the MNOs at all, but their protocols. End-to-end security is demanded between SIM card and the service provider for this purpose. The communication should be secure enough so that no one can actively or passively affect the communication, even MNO. A secure end-to-end communication protocol can satisfy this security requirement in which both the service provider and the SIM card share a secret key for encryption and decryption of the data. Moreover, data should be encrypted with a strong encryption algorithm so that third parties cannot break the communication.

The aim of this paper is to illustrate the current situation on end-to-end security between SIM card and the service provider on security required services, and discuss the risks and challenges associated with the current condition.

The remainder of this paper is organized as follows. In section 2, details on the smart cards and SIM cards are given which are essential to the current study. Section 3 presents the

Kerem Ok / Vedat Coşkun
Işık University
Turkey

Rahmi Cem Cevikbas
Turkcell Technology
Turkey

Over the Air (OTA) technology, which enables end-to-end communication between service provider and SIM card via MNO. In Section 4, secure communication between SIM Card and service provider for private key equipped SIM cards and also security requirements for such applications are given. Section 5 includes the related studies in the literature. Finally, we conclude with implications of the findings in Section 6.

II. Smart Cards

Cards with a direct physical contact interface are called as contact smart cards whereas cards with a remote contactless interface are called as contactless smart cards. A contact card is to be inserted into to card reader, so that it receives power from the reader and exchange data with it using physical contacts. Contactless smart cards, on the other hand, will be waived from a very short distance so that electromagnetic wave from the reader will be used as the energy source, and wireless communication will be used for data exchange at the same time.

The contents of smart cards are retrieved with a smart card reader, which generally connects to the backend server system to store and manage the data. Smart cards in nowadays provide promising solutions for secure data storage, efficient data processing and transfer and yet yields multi application environment [1]. These cards have their own operating system, which is very much similar to regular computers.

Smart cards are divided into two groups in terms of their capability: memory based and microprocessor based smart cards.

A. Memory vs. Microprocessor Based Smart Cards

Memory based smart cards do not have a processing facility whereas they can store any kind of data. The processing is performed by external reader device. The smart card reader reads the data inside the card and performs processing. An example to memory - based smart cards is prepaid telephone cards [1].

On the other hand, microprocessor based smart cards can achieve data processing with the embedded microprocessor. The card also contains memory and card's microprocessor conducts the data management.

Microprocessor based smart cards are a minimal form of a computer with input, storage processing, and output components, without any internal power. It is true that input and output peripherals of the card are not highly useful as well. These cards have also an operating system and they can store and process data and perform complex calculations unlike memory based smart cards. Their storage capabilities vary but are high than memory based smart cards [1].

B. Smart Card Operating Systems (SCOSs)

Developments on memory, integrated circuit chips and smart card operating systems empowered implementing multiple applications on the same smart cards. SCOSs now enable dynamic multi application card platforms.

Smart cards that have secure microcontroller can store large amount of data and can perform on-card functions such as encryption, decryption with their embedded integrated circuits. These cards also can interact directly with a smart card reader and have their own operating system, which allows smart card programming. These smart cards can interact intelligently with a smart card reader.

For the time being, each smart card has its own SCOS, which is embedded in card's ROM (Read Only Memory). SCOSs are divided into two categories. The first one is general purpose SCOS which has a generic command set; and the second one is dedicated SCOS which has commands designed for specific applications and can contain only the related application(s); e.g. a payment smart card which is designed to support only payment transactions [2]. Some of the basic functions of SCOS are managing the data stored in memory, controlling the access to information and functions, and managing interchanges between a smart card and a smart card reader.

Currently, the most notable OSs that has bigger market exposure is MULTOS (Multi-application Operating System) [3] and Java Card OS [4]. MULTOS is one of the ideal SCOSs with enhanced security features. Its aim is to provide a standard, secure operating system for any silicon chip and execute any smart card application such as payment, ticketing, identification, etc. Also various applications can run on the same smart card independently and securely [5].

Another important SCOS is the Java Card. Java Card OS enables applications written in Java Card programming language, which is similar to Java programming language to run on smart cards. The technology is standardized by Sun Microsystems and the Java Card Forum. Java Card provides a secure, interoperable and multi application platform for smart cards. It uses the advantages of the Java programming language such as object-oriented programming, reuse of existing development environments, and interoperability [5].

C. SIM Cards

A SIM card is a smart card that contains unique set of information that is required for mobile communication by its owner. The most important data on the SIM card are serial number named ICCID (Integrated Circuit Card Identifier), IMSI (International mobile subscriber identity), and an authentication key (Ki) to identify and authenticate itself to the mobile network [6]. Please note that all of the three numbers mentioned are unique for each SIM card globally. ICCID identifies each SIM uniquely throughout the world. IMSI of each SIM is also unique worldwide, and is used to identify the SIM card as well as the GSM network that it belongs.

ICCID contains following fragments (See Figure 1):

- **Major Industry Identifier:** 2-digit code for defining the industry. 89 is for "Telecommunications administrations and private operating agencies"
- **Country Code:** 1 to 3 digit code defined for countries
- **Issuer Identifier:** 1 to 4 digit code for card issuer

- **Subscriber's Account ID:** The digits may vary, however all subscribers under same issuer have same number of digits.
- **Checksum Digit:** 1 digit checksum calculated with Luhn algorithm [7].

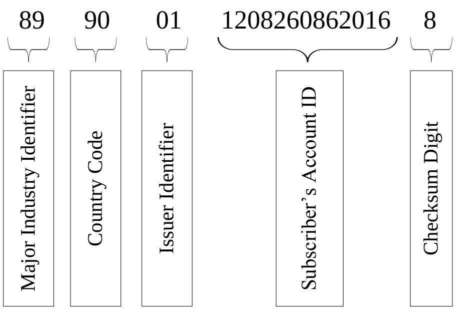

Figure 1. Sample ICCID Number

IMSI contains following fragments (See Figure 2):

- **Mobile Country Code:** 3 digit country code
- **Mobile Network Code:** 2 or 3 digit carrier code
- **Identification number.** Id number of the subscriber in generally 10 digits

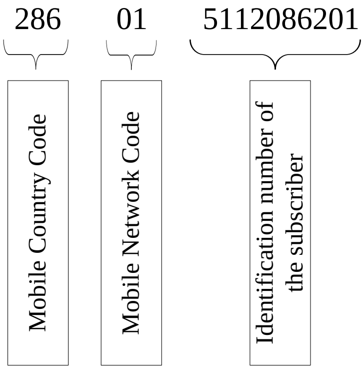

Figure 2. Sample IMSI Number

European Telecommunications Standards Institute (ETSI) introduced "3GPP TS 03.48 Security mechanisms for SIM application toolkit" standard [8] that supports the standard security services such as integrity, confidentiality, peers authentication, and no replay attacks in GSM networks. "3GPP TS 11.14 Specification of the SIM Application Toolkit (SAT) for the SIM - Mobile Equipment (SIM-ME) interface" standard also defines the interface between the SIM and the Mobile Equipment (ME), and mandatory ME procedures, specifically for "SIM Application Toolkit" [9].

III. OTA

OTA is the technology for exchanging applications and application related information through wireless communications media [1]. It enables to manage SEs (i.e., SIM cards, USIM cards) or without being connected physically to the card. By OTA technology, the SEs can be easily accessed, manipulated, and modified in a rapid and cost effective way; new services or applications can be introduced.

Based on the ecosystem that has been agreed upon, the OTA service can be provided by an MNO or another trusted entity. They have the ability to remotely configure a single mobile device, an entire fleet of mobile devices, or any IT defined set of mobile devices such as Operating System (OS) updates, remotely lock a device to protect the application and the data when it is for example lost or stolen; remotely troubleshoot the device.

Figure 3 illustrates the basic architecture of OTA technology. OTA is based on a client-server based architecture consisting of a backend system as the server, and a SIM card within the mobile phone as the client.

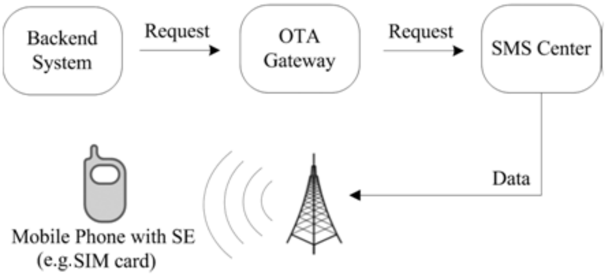

Figure 3. Basic OTA architecture

The backend system -such as a customer care operator or content provider- sends requests to the OTA gateway which transforms these requests into short messages These requests can be actions such as activate, deactivate, load or modify.

OTA Gateway receives these requests through a Gateway API. OTA Gateway has a card database, which consists for each card; the SIM vendor, the card's identification number, the IMSI and the MSISDN [10]. OTA Gateway has a set of libraries, which enables to transform the incoming request depending on the recipient card. After transformation of requests into short messages, OTA gateway sends these formatted messages to SMSC (SMS Center). During this sending process, OTA Gateway is also responsible for the integrity and security of the messages.

OTA technology has several advantages for stakeholders in the ecosystem. In terms of MNOs or authorized third parties, OTA technology provides increased cost effectiveness, remote management, and hence increases the value of the investment. By making use of these advantages, diverse value-added services can be offered to users by OTA. Furthermore it allows authorized third parties to keep control of the information downloaded on smart cards. They own the content, thus they own the customer.

From users' point of view, they are able to select the services they want on their own personalized phone. Applications (i.e., recharging prepaid subscriptions, changing subscription parameter set) can be performed with OTA while they are mobile, instead of getting their phone to the customer service. This increased service quality provides convenience for the user and enables control over her subscription parameters.

Today SIM is the major component of the GSM ecosystem and paving the way to value added services such as sophisticated menus, speed dialing, secure transactions, ability to send SMSs to query a database, and so on. With the development of SIM cards, USIM (Universal SIM) cards became valuable smart cards to enable enhanced services such as NFC technology and OTA management [11] .

IV. Communication of SIM Card with a Service Provider

STK applications enable SIM cards to be used for diverse value added services. Some of these services include mobile financial services, e-government services, physical access control, and loyalty. Most of these services require security services such as integrity and secrecy of the data. Thus cryptographic functions and keys stored in the SIM card perform these operations.

The SIM cards manufactured according to the Global Platform Card Specification have the symmetric encryption and decryption keys embedded into the card and the desired security measures can be satisfied. Cards include Security Domains (SD) which allows OTA management of applications securely. The applications installed to the SDs also use the reserved security keys in order to perform end-to-end secure communication.

There are several card management approaches defined in the Global Platform card specification. In this paper, we define one of them that can be used for a service provider to securely communicate with a SIM card. The processes performed between service provider, MNO and SIM card for secure communication are as follows (See Figure 4):

- MNO distributes the SIM card to the user
- Service provider wishes to offer a secure service via SIM card, and agrees with the MNO to use a specified SD of that MNO's SIM cards
- MNO notifies SIM card manufacturer about the agreement with the corresponding service provider
- SIM card manufacturer shares the key of the corresponding SD with the service provider with the key ceremony
- Service provider communicates with the applet in that slot securely by encrypting the data using the symmetric key (K_n). Since MNO doesn't have any knowledge about the slot key, it cannot alter or understand the communication.

Currently all SIM cards yields following security measures, which are also necessary for authenticating the SIM card to the mobile network:

- Identification of the SIM on the mobile network by IMSI number
- Authentication of the SIM on the mobile network by Authentication key (Ki)

However, additional security services are only supported by some SIM cards, which are necessary for value added services. These security services are:

- Secrecy of the transmitted data
- Integrity of the transmitted data
- Non-repudiation of the sender

In order for a SIM card to use value added services, these security services need to be satisfied. Because of this, SIM cards must have symmetric slot keys, which are installed in card manufacturing process.

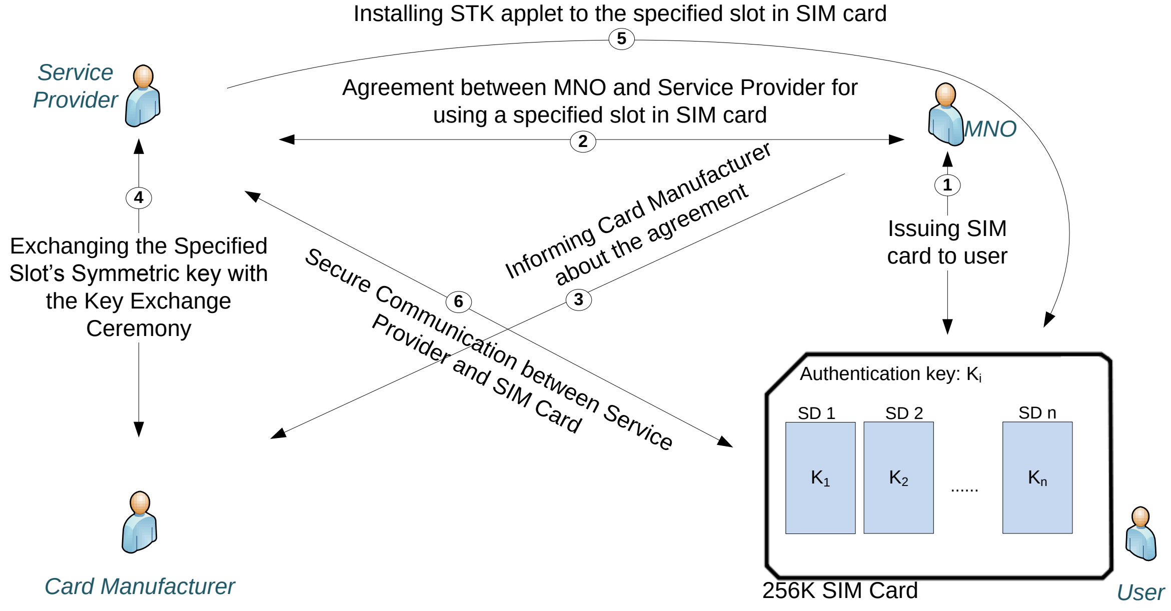
Installing STK applet to the specified slot in SIM card
5
Service Provider
Agreement between MNO and Service Provider for using a specified slot in SIM card
2
MNO
1
Issuing SIM card to user
4
Exchanging the Specified Slot's Symmetric key with the Key Exchange Ceremony
Informing Card Manufacturer about the agreement
3
6
Secure Communication between Service Provider and SIM Card
Authentication key: K_i
SD 1
SD 2
SD n
K_1
K_2
......
K_n
256K SIM Card
User
Card Manufacturer

Figure 4. Secure Communication between Service Provider and SIM Card in 256K SIM Cards

V. Related Studies on Secure Communication with SIM Cards

In this study, we focused on the current situation of secure communication between the service provider and the SIM card on the mobile phone, when a value added secure service is to be provided via SIM applications. In the literature there are some studies on smart cards, SIM cards and their security [12, 13, 14]. However, there isn't much studies on the end-to-end communication between SIM card and service providers.

Another study on the security on value added SIM applications are performed in [15]. In the study, authors analyses the security hole of traditional application model based on SMS. Also they design a security model for private key equipped SIM cards on mobile commerce. The model includes the authentication process, intercommunicative process between SIM card and the security access server, the internal process of the security access server.

In [16], authors proposed SSL (Secure Sockets Layer) protocol to assure end-to-end authenticated session key exchange for SIM smartcards. The goals are to prevent a plain text message being exchanged between the SIM and the OTA platform in the terminal and to provide data integrity and confidentiality and to reduce the cryptographic load for the SIM card.

VI. Conclusion

Smart cards and smart phones, hand in hand, created big opportunities after common acceptance throughout the world. The initially provided services such as voice communication, text messaging, and data access through the Internet. As the people tend to use their mobile for any possible purpose and at all times, companies tend to provide vast variety of services in order to gain more money, or vice versa. Financial companies, especially the banks, become not different. They searched for solutions to expand their financial services through SIM cards, with even more –and even amazing– functionalities such as mobile wallet through additional technologies such as NFC. One handicap through this path was enabling secure communication between the Bank and the user, or bank server and the SIM card in the mobile phone in technical terms. The banks of course could not endure to intervention of MNO who manages all communication between those two, and obviously could interfere easily since MNO easily can intercept and data that it handles. Hence, a method that provides secure communication between the bank server and the SIM card is required.

In this paper, we have initially put forward the case and its details. A potential solution had to skip over many barriers such as limited computational and storage capacity of the smart card, secure communication over an unsecure channel, personal preferences of the users such as ease of use, timeliness etc. We have exposed the risks and challenges deeply in this study. We also browsed the public solutions those are related to our case.

Acknowledgment

This work is funded by TUBİTAK (The Scientific And Technological Research Council Of Turkey) and Turkcell Technology under project number 5130053.

References

[1] V. Coskun, K. Ok, and B. Ozdenizci, "Near Field Communication (NFC): From Theory to Practice", John Wiley & Sons, 2011.

[2] Cardwerk, http://www.cardwerk.com/smartcards/ (accessed 23 June 2014).

[3] Multos, http://www.multos.com/ (accessed 23 June 2014).

[4] Java Card technology, http://www.oracle.com/technetwork/java/javacard/ (accessed 23 June 2014).

[5] D. Sauveron, "Multiapplication smart card: Towards an open smart card?", Information Security Technical Report, 14 (2), pp. 70-78, 2009.

[6] L. Perkov, A. Klisura, and N. Pavkovic. "Recent advances in GSM insecurities." MIPRO, 2011 Proceedings of the 34th International Convention, 2011, pp. 1502-1506.

[7] ISO/IEC 7812-1:2006. Identification Cards - Idnetification of issuers - Part 1: Numbering system, 3rd edn., ISO, Geneva (2006)

[8] 3GPP TS 03.48, Digital cellular telecommunications system (Phase 2+); Security mechanisms for the SIM Application Toolkit; Stage 2 (2001)

[9] 3GPP TS 11.14, Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit (SAT) for the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (2003)

[10] Gemalto - OTA Technology, https://www.gemalto.com/techno/ota/ (accessed 23 June 2014).

[11] V. Coskun, B. Ozdenizci, and K. Ok. "A Survey on Near Field Communication (NFC) Technology." Wireless personal communications, 71 (3), pp. 2259-2294, 2013.

[12] Messerges, Thomas S., Ezzat A. Dabbish, and Robert H. Sloan. "Examining smart-card security under the threat of power analysis attacks." Computers, IEEE Transactions on 51, no. 5 (2002): 541-552.

[13] Markantonakis, Konstantinos. Smart cards, tokens, security and applications. Springer, 2007.

[14] Vedder, Klaus. "GSM: Security, services, and the SIM." In State of the art in Applied Cryptography, pp. 224-240. Springer Berlin Heidelberg, 1998.

[15] H. Rongyu, Z. Guolei, C. Chaowen, X. Hui, Q. Xi, and Q. Zheng. "A PK-SIM card based end-to-end security framework for SMS." Computer Standards & Interfaces, 31 (4), pp. 629-641, 2009.

[16] Y. Li, M. Chen, and J. Nie. "Mobile commerce security model construction based on sms." In Wireless Communications, 2011 7th International Conference on Networking and Mobile Computing (WiCOM), pp. 1-3, 2011.