World Academy of Science, Engineering and Technology
International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:10, No:9, 2016

Secure Cryptographic Operations on SIM Card for Mobile Financial Services

Kerem Ok, Serafettin Senturk, Serdar Aktas, Cem Cevikbas

***Abstract*—**Mobile technology is very popular nowadays and it provides a digital world where users can experience many value-added services. Service Providers are also eager to offer diverse value-added services to users such as digital identity, mobile financial services and so on. In this context, the security of data storage in smartphones and the security of communication between the smartphone and service provider are critical for the success of these services. In order to provide the required security functions, the SIM card is one acceptable alternative. Since SIM cards include a Secure Element, they are able to store sensitive data, create cryptographically secure keys, encrypt and decrypt data. In this paper, we design and implement a SIM and a smartphone framework that uses a SIM card for secure key generation, key storage, data encryption, data decryption and digital signing for mobile financial services. Our frameworks show that the SIM card can be used as a controlled Secure Element to provide required security functions for popular e-services such as mobile financial services.

***Keywords*—**SIM Card, mobile financial services, cryptography, secure data storage.

I. Introduction

THE Internet has played an important role in changing the interaction between people and the businesses they do. As a result, electronic commerce has emerged, allowing businesses to more efficiently interact with their customers and other corporations inside and outside their sectors. One industry that is using this new communication channel to reach its customers is the banking industry.

Electronic banking focuses on new trends such as anytime and anywhere response for customers' demands. However, new trends increase the security and privacy of information and communication. And also the security of transactions and authentication of users is of vital important. Security of the transactions is the primary concern of Internet-based industries together with privacy. A lack of security and privacy may result in serious damages. Encryption may help make transactions to be more secure, but there is also a need to guarantee that data are not tampered with at either end of the transaction.

Kerem Ok is with Information Technologies Department, Isik University, Istanbul, Turkey (e-mail: kerem.ok@isikun.edu.tr).

Serafettin Senturk and Serdar Aktas are with Kuveyt Türk Participation Bank, Inc., Istanbul, Turkey (e-mail: serafettin.senturk@kuveytturk.com.tr, serdar.aktas@kuveytturk.com.tr).

Cem Cevikbas is with Turkcell Technology, Istanbul, Turkey (e-mail: cem.cevikbas@turkcell.com.tr).

This paper includes partial results of the Celtic+ project (#C2013/2-3) in which institutions from Turkey, South Korea, and Netherlands are participated.

Together with security considerations, the banking industry uses new communication media to offer value added services to users. This type of new system between consumers and banks are called as electronic banking. In [1], the authors define electronic banking as "the use of a computer to retrieve and process banking data (statements, transaction details, etc.) and to initiate transactions (payments, transfers, requests for services, etc.) directly with a bank or other financial services provider remotely via a telecommunications network" [1].

In this work, we present an architecture that aims to secure electronic banking system those are used via smartphones. The architecture contains a SIM (Subscriber Identity Module) Card and smartphone frameworks, smartphone applications and server applications. In the architecture, SIM cards are used to provide security functions such as secure key generation, key storage, data encryption, data decryption and digital signing for mobile financial services. The developed frameworks prove that SIM card can provide the required security functions for mobile financial services.

The remainder of this paper is organized as follows. In Section II, background information of SIM card and smartphone security are given. In Section III, the proposed architecture is given with all the details. Section IV includes the discussion of the architecture in mobile finance services and the conclusion.

II. Literature Review

In general, the communication between a customer's smartphone and electronic banking system is carried out on the session layer protocol over an untrusted channel. Thus the communication needs to be secured with a strong encryption in the communication, secure storage of keys and codes at both end points. Software based, hardware based, or hybrid solutions can be applied at both sides. Software-based solutions include public and private keys and uses software for performing encryption such as Secure Electronic Transaction used by MasterCard [2] and Pretty Good Privacy [3]. Hardware-based solutions such as smart cards, use hardware based encryption techniques. Software-based solutions are easy to develop and cheap, but hardware-based solutions are generally more secure and fast.

For mobile financial services, the security of the data can be provided from different sources such as mobile OS (Operating System) and SIM card. Android as an open source OS currently has 84.1% market share on worldwide smartphone sales in the first quarter of 2016, according to Gartner's report [4]. Android's popularity encouraged developers to provide more applications but also attracted hackers to try to find new

ways to alter the OS and applications. As identified in [5], Android faces with many security threats such as privilege escalation attacks, privacy leakage, malicious apps, and Denial of Service attacks.

Android has many different versions on the market, because different manufacturers provide different customized Android versions. Thus, implementing security critical scenarios on Android is more challenging task than other OSs [6].

In order to store encryption keys, Android uses a system named Keystore which protects keys from unauthorized use [7]. Android applies extraction prevention and authorization to secure the generated keys. In [8], the authors described different key storage solutions for Android and proposed some improvements to Keystore system. On the other hand, a SIM card is a type of smart card that is used with a smartphone for MNO's (Mobile Network Operator) serviced such as cellular communication [9]. Each SIM card contains some unique values such as ICCID (Integrated Circuit Card Identifier), IMSI (International Mobile Subscriber Identity), Authentication Key to identify and authenticate itself to the MNO on the mobile network, and a cryptographically protected area called SE, to store critical data safely [9], [10]. The SIM card can provide trust in any service deployed by MNO using cryptographic keys, certificates, security policies, and so on. Its underlying SE platform can also store any data securely [11]. All the data in SE are protected and only can be accessed by authorization. SIM cards are also able to perform secure cryptographic operations such as public and private key pair generation, asymmetric encryption such as RSA, symmetric encryption such as DES and 3-DES, signing and hash operations. On the other hand, the data capacity of SIM cards is small, so that only important data should be stored in. As a result, using SIM card for cryptographic is a one good alternative, especially for the applications where secure considerations are high, such as mobile banking.

III. Proposed Architecture

As given in the previous section, storing any data in SE is seen as secure. On the other hand, the smartphone OSs may be subject to security threats. If a threat on the encryption key occurs, the communication between the smartphone and the other party can be under threat. For these reasons, storing encryption keys in a secure environment is important for a secure communication between the smartphone and other parties. The SIM card is a good alternative since it includes a cryptographically protected SE.

In the current situation, SIM cards can be used to secure the PIN entry of users from mobile applications. However, when this mechanism is used, the user has to wait more than 10 seconds for the PIN entry screen to appear, since the mobile application communicates with the SIM card via OTA (Over the Air). Consider the case given in Fig. 1. A user opens a mobile application that requests to be authenticated. In order for a mobile application to request the authentication from the SIM card, the mobile application firstly needs to send an authentication request to the MNO's OTA server. Secondly, the OTA server communicates with the SIM card via OTA technology, and requests PIN from SIM card. Thirdly, SIM card sends the encrypted PIN to the OTA server. Finally, the OTA server compares the received encrypted PIN with the encrypted PIN in its database. Then it sends the authentication result (success or fail) to the mobile application. This process takes an average of 10 seconds, which is considered a long time.

As already described in the introduction section, the aim of the paper is to design and implement software frameworks on both the smartphone and SIM card that provide the required security functions of the SIM card to popular e-services, such as mobile commerce and financial transactions. Then, the mobile finance products will be able to integrate the frameworks into their products and use SIM card's capabilities for security services directly from the smartphone such as secure key generation, key storage, data encryption, data decryption, and digital signing. The desired case is given in Fig. 2, in which the mobile application directly communicates with the SIM card and requests authentication which eliminates the time for OTA access.

With the designed and implemented frameworks, the desired case will be obtained. So, the duration of the communication with the SIM card will be shortened and a more enhanced experience will be provided to users. Also, direct access to the SIM card through mobile applications will also increase the potential value of SIM cards and pave the way for new secure value added services.

A. The Architecture

The proposed frameworks are given in Fig. 3. As it can be seen from the figure, the framework includes a SIM card with an installed SIM card framework, a smartphone framework, a smartphone application for the service provider, and a server of the service provider with the required server architecture.

1) **Server side architecture:** The server is responsible for encrypted communication with the smartphone application of the service provider. A key pair is generated and a private key is installed on a server as a non-exportable certificate which is used to decrypt a password that is stored in server-side configuration file. A password is generated and encrypted with the public key and stored in a configuration file. Whenever the password is needed to access services, it is retrieved from the configuration file and decrypted to access services.
2) **Service Provider application:** The smartphone application is the application of the service provider, such as a financial institution. It both communicates with the service provider's server and with the smartphone framework. It requests security services such as key generation, encryption, and decryption from SIM card framework via a smartphone framework.

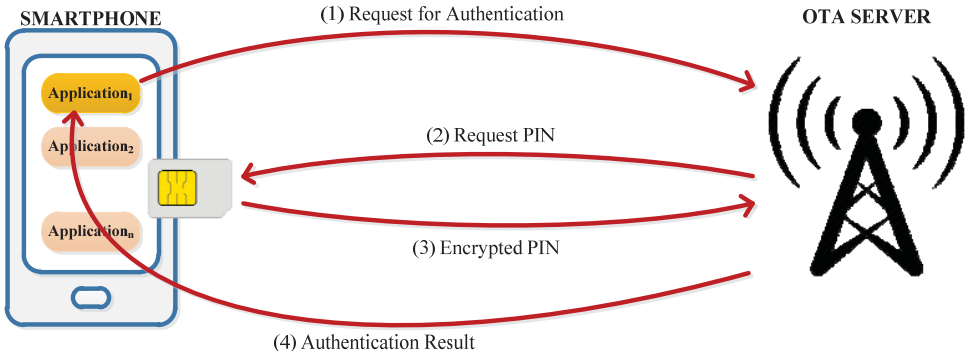

Fig. 1 PIN authentication via OTA server

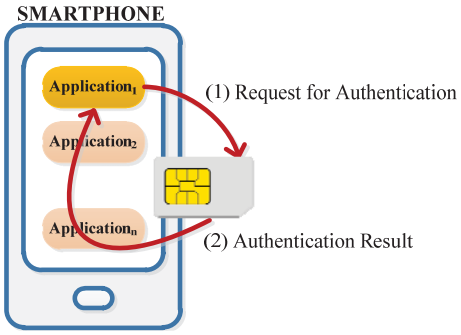

Fig. 2 PIN authentication using designed architecture

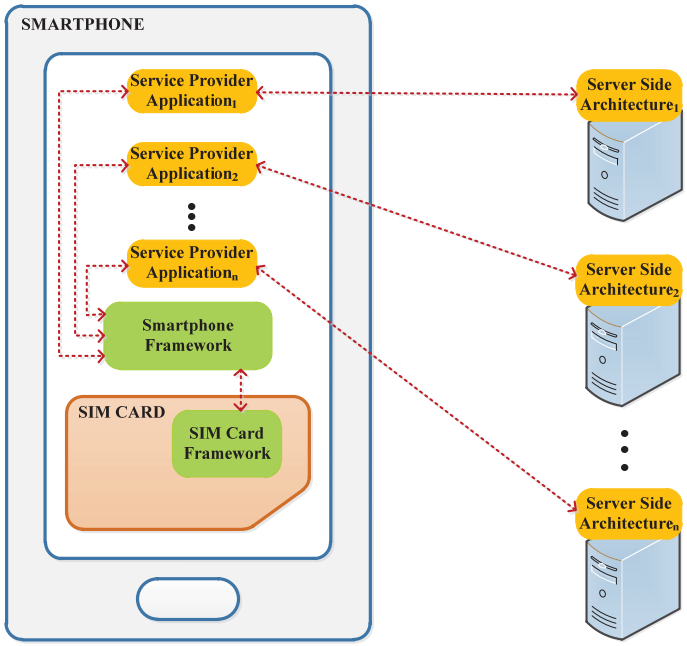

Fig. 3 Proposed Architecture

3) **Smartphone framework:** A smartphone framework is the connecter between smartphone application and the SIM card framework. It receives the requests from the smartphone application, translates these requests into an APDU messages and sends those messages to the SIM card framework. When the SIM card framework responds to the requests, the smartphone framework forwards these response messages to the smartphone application. With the use of the smartphone framework, smartphone applications do not need to handle complex communication with APDU messages with the SIM card framework. Instead, the smartphone framework handles the messaging, and the smartphone applications communicate with the smartphone framework for

standard calls.

4) **SIM card framework:** The SIM card framework is responsible for various operations on the SIM card including key generation, key encryption, symmetric encryption and decryption, asymmetric encryption and decryption. A SIM card framework is installed to the SIM card by MNO via OTA. Only the smartphone framework can communicate with the SIM card framework based on pre-defined Application Protocol Data Unit (APDU) messages.

B. Security of the Architecture

One of the most important topics in the proposed architecture is security of key storage and security of the communication between the smartphone application and the server.

In the presented framework, we chose a SIM card as the secure hardware for performing key related operations. The SIM card is a Secure Element (SE) in which all the data in its secure area is cryptographically protected. The SIM card framework offers following security mechanisms:

Master Key: A master key is generated on SIM card framework when it is installed to the SIM card. This key is cryptographically secure and cannot be extracted from the framework. Master key is used to encrypt any key that is created in SIM card framework.

Key generation: SIM card framework is used for secure key generation. Service Provider application on Smartphone requests whenever a new key pair is required and SIM card performs the requested key generation.

Key encryption: When a new key is generated by the SIM card framework, framework encrypts the private key with the master key and then sends it to the service provider application on the smartphone. So, service provider application can store this key in any environment without any drawbacks, since the key is encrypted with the master key and the master key is never extracted from the SIM card framework.

Data encryption: When a service provider application requests encryption or decryption from the SIM card framework, it also sends the encrypted key to the SIM card; thus, that SIM card decrypts the incoming key with its master key and obtains the encryption/decryption key. Finally, it uses this key for encryption/decryption.

Smartphone framework: Only the mobile framework on the smartphone can communicate with the SIM card framework. In order for any smartphone application to communicate with a SIM card, it needs to be registered by MNO, since MNO imposes related security mechanisms for communication with the SIM card. In the proposed architecture, the smartphone framework is registered by MNO and only it can communicate with the SIM card framework. Service provider applications can communicate with the smartphone framework in order to request security services from the SIM card.

IV. Discussion and Conclusion

Online financial fraud is a phenomenon today that causes customers to lose their confidence in financial services. As the number of fraud incidences increases, customers become more wary of the services they are receiving on their mobile phones.

A number of security vulnerabilities identified on SSL protocol, which is widely used in the financial services industry for secure communication justifies costumers' wariness. The industry is in need of new technological approaches to meet the security levels required for online banking transactions.

The advancement in SIM card technology allows cryptographic operations to be done on SIM cards without relying on SSL protocols.

A SIM card provides symmetric and asymmetric key generation, encryption, decryption and secure data storage services. These services are exploited to provide secure banking transactions.

In the presented architecture, a customer installs a mobile banking application on their mobile phone. Upon successful authentication, a symmetric key is generated between the SIM card and the bank mutually, and public-private key pairs are generated securely on the SIM card. Both the symmetric key and private key are encrypted with the SIM card's master key and sent to the mobile application. The public key of the customer is encrypted with the bank's public key which is already in the mobile banking application and the encrypted public key is transferred to the bank's server. The encrypted public key is decrypted with the bank's private key and together with the symmetric key; they are stored in the bank's environment. When a customer wants to make a transaction, the transaction request is generated and encrypted with the symmetric key and signed with the customer's private key. The request is transferred to the bank and verified on the bank's server and decrypted with the symmetric key. This process eliminates the fraud caused by the vulnerabilities in SSL protocol and man-in-the middle attacks, as all cryptographic operations are done inside the SIM card securely. The proposed architecture uses the SIM card's capabilities and all keys, other than public keys, are stored in the SIM card encrypted.

References

[1] Electronic Banking System. http://www.electrobank.com/ebaeb.htm, Last Access: Aug. 15, 2016.
[2] Master Card, www.mastercard.com, Last Access: Aug. 15, 2016.
[3] The International PGP Home Page, http://www.pgpi.org, Last Access: Aug. 15, 2016.
[4] Gartner Says Worldwide Smartphone Sales Grew 3.9 Percent in First Quarter of 2016. Online at: http://www.gartner.com/newsroom/id/3323017, Last Access: Aug. 15, 2016.
[5] Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., & Rajarajan, M., "Android security: a survey of issues, malware penetration, and defenses," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 998-1022, 2015.
[6] Teufl, P., Andreas, F., Daniel, H., Alexander M., Alexander, O., Thomas Z., "Android encryption systems," in *Proc. 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, Denmark, pp. 1-8, 2014.

[7] Android Keystore System, https://developer.android.com/training/articles/keystore.html, Last Access: Aug. 15, 2016.
[8] Cooijmans, T., de Ruiter, J., Poll, E, "Analysis of secure key storage solutions on Android," in *Proc. 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, USA, pp. 11-20, 2014.
[9] Ok, K., Coskun, V., Yarman, S.B., Cevikbas, C., Ozdenizci, B., "SIMSec: A Key Exchange Protocol between SIM Card and Service Provider," *Wireless Personal Communications*, vol. 89, no. 4, pp. 1371-1390, 2016.
[10] Perkov, L., Ana, K., and Nikola, P., "Recent advances in GSM insecurities," in Proc. MIPRO *34th International Convention*, Croatia, 2011, pp. 1502-1506.
[11] Ahmad, Z., Francis, L., Ahmed, T., Lobodzinski, C., Audsin, D. Jiang, P., "Enhancing the Security of Mobile Applications by using TEE and (U) SIM," in Proc. *2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC)*, Italy, pp. 575-582, 2013.