

CERTIFICATE OF TRANSLATION ACCURACY

I am a professional translator, reviewer, and project manager specializing in translating Korean, Japanese and Chinese to English and vice versa.

I served as Chief Examiner of the certified court interpreter test for the State of California and as a contract translator and interpreter for various federal agencies through the U.S. Department of State for more than a decade. I served as an instructor at the University of California at Berkeley, and the Middlebury Institute of International Studies at Monterey (MIIS) Graduate Program in Translation.

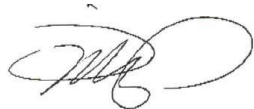
I have more than 35 years of experience translating thousands of technical, legal, and business documents from Korean to English submitted to, among others, Korean judicial authorities, U.S. federal courts, the U.S. International Trade Commission (ITC), the U.S. Patent and Trademark Office (USPTO), and the USPTO Patent Trial and Appeal Board (PTAB).

I certify that this is a true, correct, and complete translation of the corresponding source text to the best of my knowledge and ability.

**Design of Safe AKA Module for Adapted Mobile Payment System
on Openness Smartphone Environment**

I certify under penalty of perjury that the foregoing is true and correct.

Executed this 15th day of October 2025 in Contra Costa County of the State of California.

By: 

Alex N. Jo
Member, ATA

A Design of Safe AKA Module for Adapted Mobile Payment System on Openness Smartphone Environment

Eun-Hee Jeong[†], Byung-kwan Lee^{††}

ABSTRACT

The USIM-based AKA authentication process is essential to a mobile payment system on smart phone environment. In this paper a payment protocol and an AKA module are designed for mobile payment system which is suitable for openness smart phone environment. The payment protocol designs the cross authentication among components of the mobile payment system to improve the reliability of the components. The AKA module of mobile payment system based on 3GPP-AKA protocol prevents the exposure of IMSI by creating the SSK (Shared safe Key) through advance registration and solves the SQN (SeQuence Number) synchronization problem by using timestamp. Also, by using the SSK instead of authentication vector between SN and authentication center, the existing bandwidth $(688 \times N) \times R$ bit between them is reduced to $320 \times R$ bit or $368 \times R$ bit. It creates CK and IK which are message encryption keys by using OT-SSK (One-Time SSK) between MS and SN. In addition, creating the new OT-SSK whenever MS is connected to SN, it prevents the data replay attack.

A Design of Safe AKA Module for Adapted Mobile Payment System on Openness SMART Phone Environment

Eun-Hee Jeong[†], Byung-kwan Lee^{††}

ABSTRACT

The USIM-based AKA authentication process is essential to a mobile payment system on smart phone environment. In this paper a payment protocol and an AKA module are designed for mobile payment system which is suitable for openness smart phone environment. The payment protocol designs the cross authentication among components of the mobile payment system to improve the reliability of the components. The AKA module of mobile payment system based on 3GPP-AKA protocol prevents the exposure of IMSI by creating the SSK(Shared Secure Key) through advance registration and solves the SQN(SeQuence Number) synchronization problem by using timestamp. Also, by using the SSK instead of authentication vector between SN and authentication center, the existing bandwidth $(688 \times N) \times R$ bit between them is reduced to $320 \times R$ bit or $368 \times R$ bit. It creates CK and IK which are message encryption key by using OT-SSK(One-Time SSK) between MS and SN. In addition, creating the new OT-SSK whenever MS is connected to SN, it prevents the data replay attack.

Key words- USIM, Mobile Payment System, Mobile Payment Protocol, Mobile Payment Protocol

Corresponding Author: Eun-Hee Jeong, Address: (Room 308, Humanities and Social Sciences Building, Gangwon National University Samcheok Campus) 1 Jungang-ro, Gyodong, Samcheok-si, Gangwon-do (245-711), Tel: 033) 570-6646, FAX: 033) 574-6640, E-mail: jcongch@kangwon.ac.kr

Received: October 5, 2010, Revised: November 1, 2010

Completion date: November 26, 2010

[†] Full Member, Associate Professor, Department of Regional Economics, Kangwon National University Samcheok Campus

^{††} Full Member, Professor, Department of Computer Science, Kwandong University

(E-mail: bklee@kwandong.ac.kr)

1. Introduction

Convergence is one of the hot topics in recent years across industries. Convergence is a phenomenon in which various devices and underlying technologies such as computers, home appliances, and telecommunications are organically converged with each other through digital technology. This convergence is meaningful to us because the financial industry itself is becoming digitalized and developing into an information industry [1].

In addition, the advancement of mobile networks and the rapid development of terminals have led to the emergence of smartphones that meet the diverse needs of users, and from the third generation of mobile terminals, USIM cards, called Universal Subscriber Identity Modules (USIM), are used to provide network authentication and additional functions. In other words, smartphones can provide various additional services such as communication, finance, transportation, and other mobile services that users want anytime and anywhere through various interfaces, and this has brought tremendous opportunities to our business and life [2].

However, mobile services operating in a wireless network environment are susceptible to various security threats such as illegal tampering, eavesdropping, and identity disguise, and since the smartphone environment is an open environment unlike the closed service environment of traditional mobile communications, users can acquire various contents to their devices through various routes, and illegal contents can cause damage to business methods and economic losses, and even damage caused by mobile viruses due to the installation of virus-infected contents.

Currently, the 3rd Generation Partnership Project (3GPP) has established the 3GPP-Authentication Key Agreement (3GPP-AKA) standard to provide user authentication, encryption, and message integrity in mobile environments, but the 3GPP-AKA protocol has been criticized for problems such as synchronization issues with SQN (SeQuence number) and attacks using false base stations, privacy issues due to plaintext transmission of IMSI (International Mobile Subscriber Identity), a permanent identifier of the device, and authentication data overhead due to the use of multiple authentication vectors [3, 4, 5].

This paper aims to safe these problems of 3GPP-AKA and design a safe AKA module for mobile payment systems that can respond to the openness of the smartphone environment and various network

interfaces and interworking infrastructures to provide safe and efficient services through network authentication and service authentication for users or devices.

This paper is organized as follows. In Section 2, we review related research results, Section 3 describes the mobile payment system proposed in this paper, and Section 4 presents the results of the reliability evaluation and efficiency evaluation of the AKA module of the mobile payment system. Finally, this paper is concluded in Chapter 5.

2. Related Research

2.1 Mobile Payment System

Mobile payment is defined as a payment service that uses the mobile communication network to pay for services and goods purchased online and offline. In other words, mobile payment is a new type of payment that can replace existing payment methods such as cash or credit card, and it means that the payment process such as user identification, transaction information transmission, and transaction authentication is carried out through part or all of the mobile communication network.

The mobile payment system is structured as shown in Figure 2, and the protocol of the mobile payment system consists of a payment transaction protocol and a session key generation protocol [6, 7].

The payment transaction protocol in Figure 1 generates a session key for safety between the mobile phone and the issuing bank, but there is no reliable verification procedure for the issuing bank, and the issuing bank plays the role of managing the USIM card, but the USIM management is limited due to the lack of a USIM management system. Therefore, this paper proposes a more safe mobile payment system that uses the IMSI of the USIM card instead of the Payment ID to manage the USIM card, verify the issuing bank, and verify the user, store, and settlement center by having a trusted certificate authority.

2.2 USIM Authentication

The USIM has a small CPU and memory to run the cryptographic algorithms and processes used to authenticate a single word, thus performing the Authentication and Key Agreement (AKA) process, and

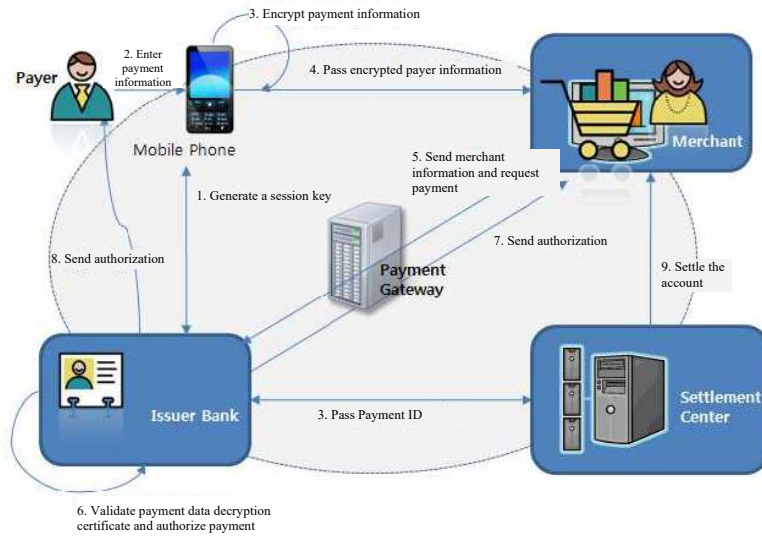


Figure 1. Mobile payment systems and payment transaction protocols

accordingly, the encryption key generated during this process is used to provide encryption and authentication services for terminal user data [8, 9].

Figure 2 illustrates 3GPP-AKA, the USIM authentication process in the wireless Internet environment. When the USIM/MS identifies itself by sending IMSI (International Mobile Subscriber Identity) or TMSI (Temporary Mobile Subscriber Identity) information to the SN

(Serving Network), the SN transmits an authentication data request message and the IMSI/TMSI received from the terminal to the AuC (Authentication Center) of the HN (Home Network), which is the authentication center. The HN generates an authentication vector AV (A-uthentication Vector) for the received IMSI and transmits it to the SN in response to the authentication data request.

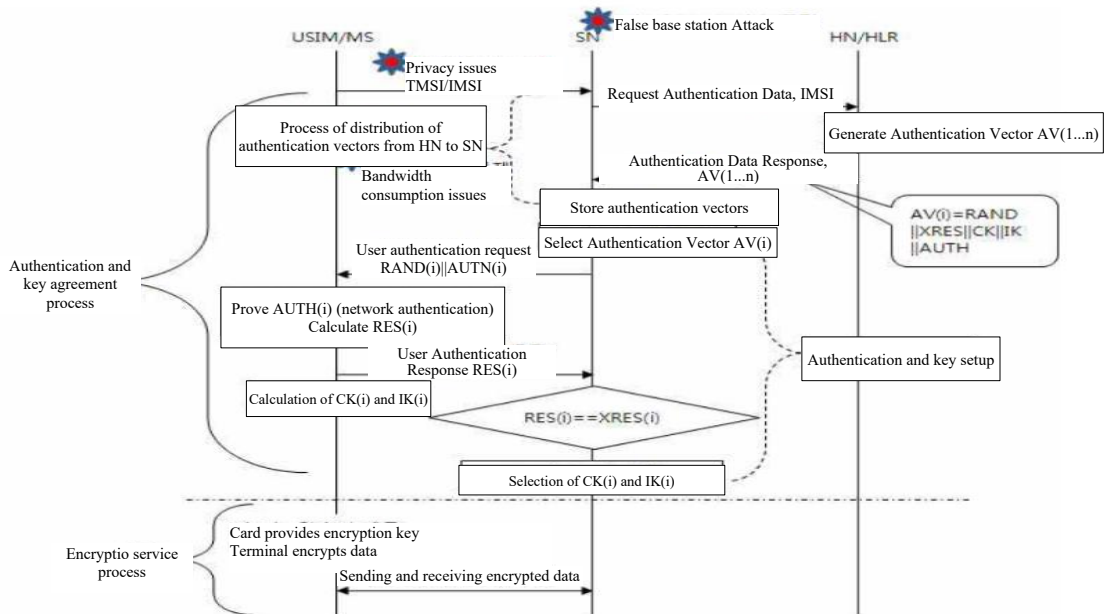


Figure 2. 3GPP-AKA Mutual Authentication Flow [10]

The SN selects one of the AVs, generates a random number to extract the authentication token (AUTN) in the AV, and attempts to authenticate the user on the device. The device authenticates this data using the network authentication algorithm of the USIM and transmits a user authentication response to the SN, while generating encrypted session keys CK and IK. The SN authenticates the device and the user by comparing the received RES with the XRES it has stored, and then generates a session key to be used for encrypting the user's data, completing the authentication and key agreement process [10,11,12].

However, the mutual authentication of 3GPP-AKA is facing problems such as SQN synchronization problem, which is the phenomenon of authentication failure due to SQN non-synchronization, false base station attack, which intervenes in the communication between the terminal and SN and redirects the user to another SN that the user does not intend, bandwidth consumption problem between SN and HN, and privacy due to IMSI plaintext transmission.

3. Mobile Payment System Design

This chapter describes the overall flow of the mobile payment system and designs the authentication modules for each leg of the mobile payment system. A mobile payment system consists of a trusted certificate authority, issuing bank, payment center, merchant, and user, and the roles of each member are as follows.

- Issuer Bank: The bank that issued the credit card. The issuer bank is responsible for managing the USIM card, but the USIM management is limited due to the lack of a USIM management system, so a trusted certificate authority is appointed to manage the USIM card separately.
- Settlement Center Settlement Center: responsible for managing payment requests and responses for the actual mobile payment system and for forwarding the results of transactions to the issuing bank to update user account information.
- Certificate Authority: A trusted certificate authority. It manages USIM cards, registers issuing banks, merchants, and settlement centers to perform mutual authentication.
- Merchant: refers to online and offline stores that use the mobile payment system.
- User: A user of the mobile payment system who is the owner of a mobile phone equipped with a USIM card.

Figure 3 illustrates the overall flow between the components of a mobile payment system.

3.1 Mobile Payment Protocol Design

The mobile payment protocol designed in this paper is designed to request mobile payment at the same time as the user authentication request by encrypting and transmitting the information of the mobile's USIM card to the store.

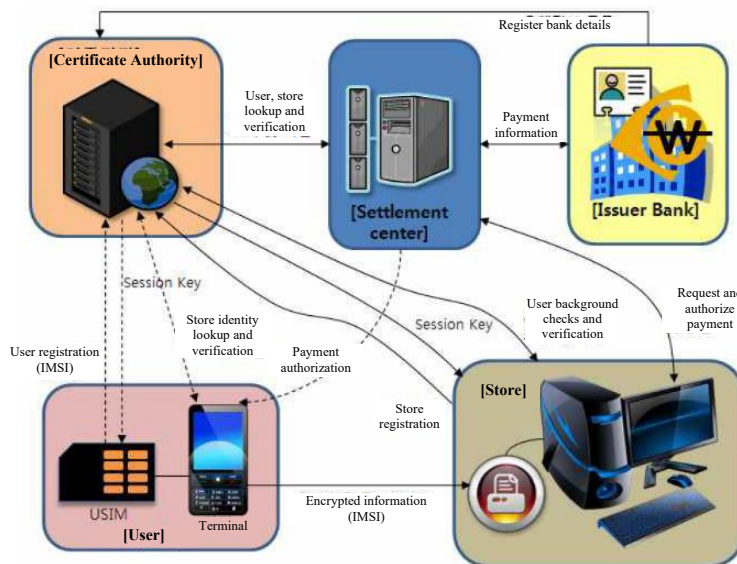


Figure 3. Mobile payment system flowchart

At this time, the user, store, certificate authority, payment center, and issuing bank have each generated a shared secret key while registering their information with the certificate authority in advance, so the information to be transmitted is encrypted with the shared secret key and transmitted.

Figure 4 illustrates the overall process of the mobile payment protocol, which consists of a registration phase where each member registers with the certifier, an authentication phase where mutual authentication is performed in the actual transaction, and a payment authorization and payment information organization phase according to the payment request.

3.1.1 Registration phase

Users, merchants, issuing banks, and payment centers that comprise the mobile payment system register their respective master keys with the certificate authority, and users, merchants, issuing banks, and payment centers generate shared secret keys with the certificate authority.

The shared secret key is generated by the EC-DH algorithm, and the shared secret key is used for mutual authentication. Among the components of the mobile payment system, the process of generating a shared secret key between the certificate authority and the store is as follows.

- (1) The merchant registers the merchant's information when

- registering with the certificate authority.
- (2) The certificate authority delivers to the merchant the initial point P , E_p , and the certificate authority's public key A_{SKP} , which are necessary for generating the shared secret key.
- (3) The merchant generates a shared secret key $M_{(SK)}(A_{SK}P)$ with the certificate authority's public key and passes it to the certificate authority as M_{SKP} , the merchant's public key.
- (4) The certificate authority generates a shared secret key $A_{(SK)}(M_{(SK)}P)$ with the merchant's public key and validates it with the shared secret key delivered by the merchant.
- (5) The merchant checks the validity of the shared secret key received from the certificate authority against the shared secret key generated by the merchant.
- (6) If the validation is TRUE, the shared secret is used as the shared secret of the merchant and the certificate authority.

3.1.2 Authentication Steps

In a mobile payment system, it refers to the steps of mutual authentication between the user and the store, mutual authentication between the store and the payment center, and mutual authentication between the payment center and the issuing bank.

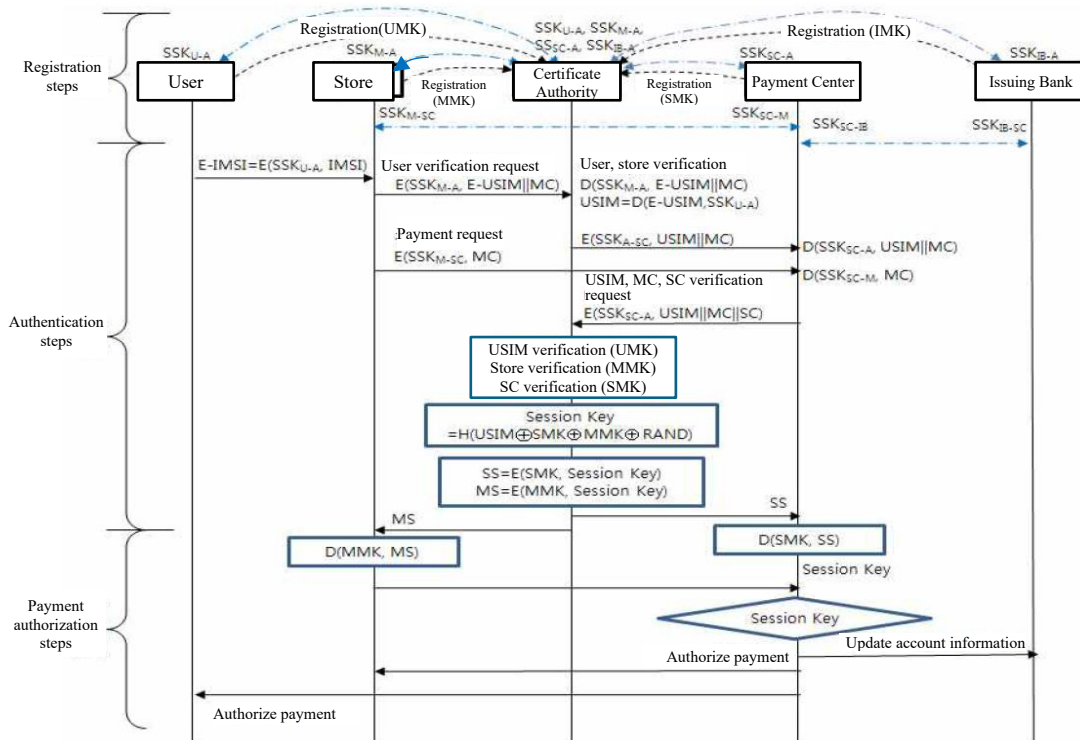


Figure 4. Mobile payment protocol flowchart

In the authentication stage, each user encrypts their information with the shared secret created in the registration stage and transmits it to the destination to protect their information. In particular, a one-time session key is created at this stage and used in the payment authorization stage to prevent personal information and account exposure due to session key exposure.

- (1) When a user makes a mobile payment to a store, the user delivers the IMSI, the unique value of the USIM card, encrypted with $SSK_{(U-A)}$, the shared secret key between the user and the authentication server, to the store. At this time, the store concatenates the store's unique code, MC, to the encrypted USIM information ($E-USIM$) and encrypts it with SSK_{M-A} to request user identity authentication from the authenticator and transmits it to the payment center to request payment. Similar to user authentication, the store encrypts the store's code, MC, with SSK_{M-SC} , a shared secret key between the store and the payment center, and transmits it to the payment center.

$$E-USIM = E(SSK_{U-A}, USIM) // \text{Encrypt USIM with shared secret key } SSK_{U-K}$$

$$E(SSK_{M-A}, E-USIM || MC) // \text{Concatenate } E-USIM \text{ and MC to encrypt with } SSK_{M-A}$$

$$E(SSK_{M-SC}, MC) // \text{Encrypt MC with } SSK_{M-SC}$$

- (2) The certificate authority decrypts the ciphertext delivered with each shared secret key to verify the user's identity and the store's identity, and transmits the user's USIM and the store's MC to the payment center encrypted with the shared secret key SSK_{A-SC} between the payment centers.

$$D(SSK_{(U-A)}, E(SSK_{(U-A)}, E-USIM)) = USIM // \text{decrypt passphrase to } SSK_{(U-A)}$$

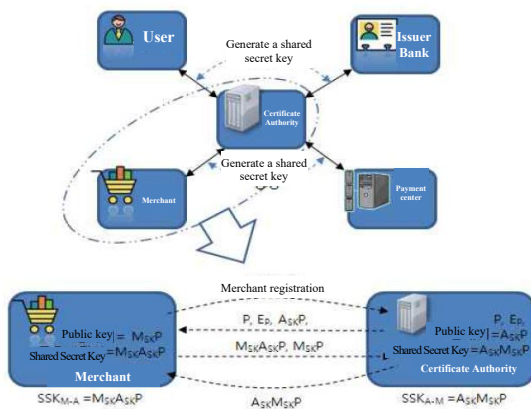


Figure 5. Generate shared secret key (merchant and certificate authority)

$$D(SSK_{M-A}, E(SSK_{M-A}, E(SSK_{U-A}, USIM) || MC))$$

$$= E-USIM || MC$$

→ EXTRACT MC

$$E(SSK_{A-SC}, USIM || MC) // \text{CONCATENATE USIM AND MC AND ENCRYPT WITH } SSK_{A-SC}$$

- (3) The payment center encrypts the payment request message transmitted from the store and the identity verification of the user and store received from the certifier with SSK_{A-SC} and requests the certificate authority.

$$D(SSK_{A-SC}, E(SSK_{A-SC}, USIM || MC)) = USIM || MC$$

// Decrypt the ciphertext with SSK_{A-SC}

$$E(SSK_{A-SC}, USIM || MC || SC) // \text{Concatenate USIM, MC, and SC to encrypt with } SSK_{A-SC}$$

- (4) The certificate authority decrypts the message transmitted from the payment center with SSK_{A-SC} , verifies the identity of the USIM, store, and payment center, and finds the respective master key stored in the database.
- (5) The certificate authority generates a session key by XORing and then hashing the USIM, each master key, and a random value required for mobile payment authorization.

$$Session\ Key = H(USIM \oplus SMK \oplus MMK \oplus RAND)$$

At this point, the session key is encrypted using each master key and delivered to the store and payment center.

$$SS = E(SMK, Session\ Key), MS = E(MMK, Session\ Key)$$

3.1.3 Payment request authorization steps

- (1) The store decrypts with its master key (MMK) and transmits the session key to the payment center.
- (2) The payment center decrypts the session key with its own master key (SMK) and compares it with the session key received from the store, and if they match, the payment authorization message is transmitted to the store and the user, respectively, and the mobile payment process ends.

At this time, if the authentication server does not transmit the session key to the store within 3 minutes, or the user does not transmit the session key to the store, the transaction is treated as canceled.

- (3) The payment center encrypts and transmits the user's information to the issuing bank.
- (4) The issuing bank updates the user's information.

3.2 Design of a safe Authentication Key Agreement (AKA) Module for Adapted Mobile Payment on Openness Smartphone Environment

Since mobile payment protocols are not limited to fixed locations due to the nature of mobile phones, the existing 3GPP-AKA mutual authentication protocol was applied to authenticate users using USIM cards. However, we propose a robust user authentication module that improves the SQN (Sequence Number) synchronization problem, false base station attack, bandwidth consumption problem between SN (Serving Network) and certificate authority, and privacy problem due to IMSI plaintext transmission in the existing 3GPP-AKA mutual authentication.

The proposed user authentication module assumes that the MS knows the identity of the SN to which it belongs, that the MS knows the identity of the Certificate Authority (HD) to which it is registered, that the SN and the HD are trusted organizations, and that the communication channel between the SN and the HD is secure.

Figure 6 shows the user authentication process using USIM, and each step is described as follows.

- (1) In the existing AKA, we need to solve the privacy problem and the synchronization problem of SQN by transmitting the IMSI

plaintext of the terminal.

Therefore, the $IMSI$, T_{MS} (timestamp), and SN_{ID} located near the terminal are concatenated to generate the authentication value of the MS using the function $f_K^1()$. Also, $E-IMSI_{MS}$, MAC_{MS} , HN_{ID} , and T_{MS} , which are values encrypted with SSG_{MS-HN} , a shared secret key between HN and MS , are transmitted to the SN located near the MS.

$$MAC_{MS} = f_{SSK_{MS-HN}}^1(IMSI_{MS} || T_{MS} || SN_{ID})$$

$$E-IMSI_{MS} = E(SSK_{MS-HN}, IMSI_{MS})$$

- (2) The SN forwards the received $E-IMSI_{MS}$, MAC_{MS} , T_{MS} to the corresponding certificate authority (HN).

- (3) The Certificate Authority (HN) decrypts the $E-IMSI_{MS}$ with the shared secret key SSK_{MS-HN} between the MS and HN to restore the IMSI value of the MS, and then checks whether the IMSI of the MS is in the database of the Certificate Authority (HN). In addition, the message integrity is checked by computing $XMAC_{MS}$ using $IMSI_{MS}$ restored by the certificate authority (HN) and the received T_{MS} comparing it with the received MAC_{MS} .

$$E-IMSI_{MS} = D(SSK_{MS-HN}, E-IMSI_{MS}) = IMSI_{MS}$$

$$XMAC_{MS} = f_K^1(IMSI_{MS} || T_{MS} || SN_{ID})$$

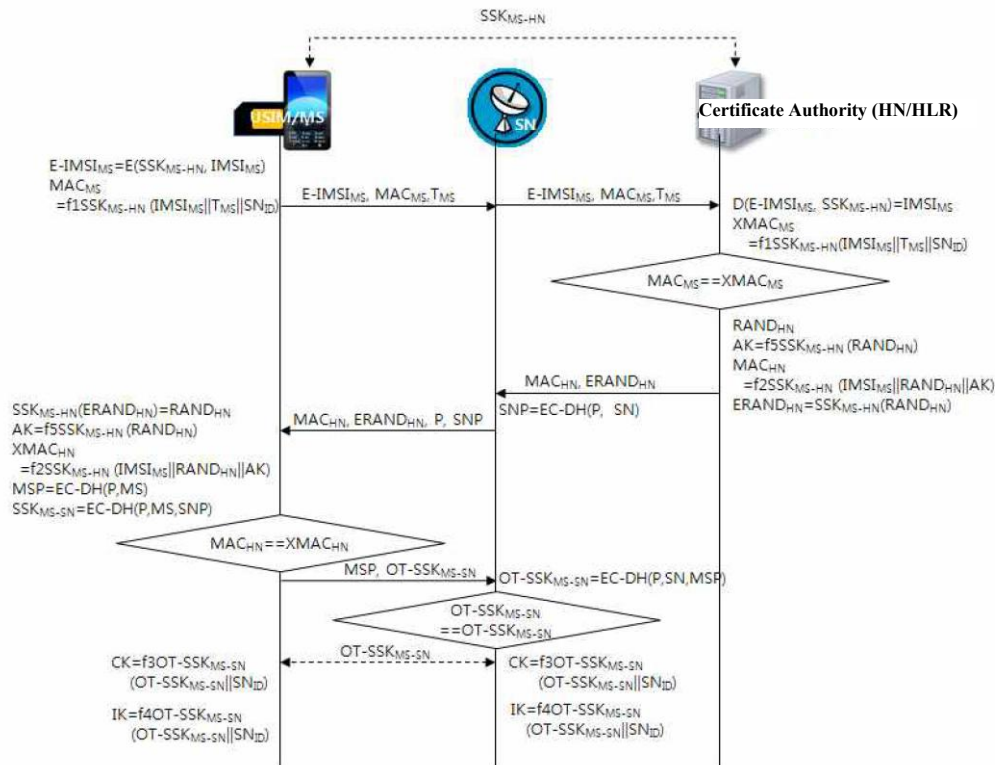


Figure 6. Safe AKA Procedure

- (4) After verifying the identity of the MS, the Certificate Authority (HN) generates MAC_{HN} , and E_RAND_{HN} to verify the identity of the Certificate Authority (HN) and delivers them to the SN. At this time, the Certificate Authority (HN) uses a randomly selected random value, $RAND_{HN}$, and transmits the value of the XOR operation with the $IMSI_{MS}$ of the MS to the SN.

$$AK = f_{SSK_{MS-SN}}^5(RAND_{HN})$$

$$MAC_{HN} = f_{SSK_{MS-SN}}^2(IMSI_{MS} \parallel RAND_{HN} \parallel AK)$$

$$ERAND_{HN} = IMSI_{MS} \oplus RAND_{HN}$$

- (5) The SN forwards the MAC_{HN} , and $ERAND_{HN}$ received from the Certificate Authority(HN) to the MS. At this time, the SN transmits to the MS the initial point for generating a one-time SSK, $OT-SSK_{MS-SN}$, and the SN's public key, P , and SNP so that the MS can verify the SN's identity.

$$SNP = EC-DH(P, SN)$$

- (6) The MS decrypts the received $ERAND_{HN}$ using the shared secret key SSK_{MS-HN} to extract the random value $RAND_{HN}$ of the certificate authority (HN). Using this value, $XMAC_{HN}$ is calculated and compared with the MAC_{HN} received to verify the identity of the certificate authority (HN). At this time, the MS generates $OT-SSK_{MS-SN}$ with its own secret key to the public key received from the SN. Then, it transmits its public key, MSP , and a one-time shared secret key, $OT-SSK_{MS-SN}$ to the SN.

$$E(SSK_{MS-HN}, ERAND_{HN}) = RAND_{HN}$$

$$XMAC_{HN} = f_{SSK_{MS-SN}}^2(IMSI_{MS} \parallel RAND_{HN})$$

$$OT-SSK_{MS-SN} = EC-DH(P, MS, SNP)$$

- (7) Since the mutual authentication of the MS and the HN is completed, mutual authentication between the MS and the SN is performed for safe information transmission. The SN generates a one-time shared secret key, $OT-SSK_{MS-SN}$, using the MS public key, MSP , received from the MS, and mutually authenticates the identity of the MS by checking whether it matches the $OT-SSK_{MS-SN}$ received from the MS.

$$OT-SSK_{ms-sn} = EC-DH(P, SN, MSP)$$

- (8) Finally, generate CK and IK for safe information transmission, and in this paper, $OT-SSK_{MS-SN}$ using EC-DH's algorithm is utilized to generate CK and IK.

$$CK = f_{OT-SSK_{MS-SN}}^3(OT-SSK_{MS-SN} \parallel SN_{ID})$$

$$IK = f_{OT-SSK_{MS-SN}}^4(OT-SSK_{MS-SN} \parallel SN_{ID})$$

4. Analysis

In this paper, we designed a safe Authentication Key Agreement (AKA) module for mobile payment system suitable for openness smartphone environment. The AKA module designed in this paper uses the existing 3GPP-AKA authentication method, but we analyzed the problems that may occur in the existing 3GPP-AKA and improved the problems.

4.1 Safety Analysis

4.1.1 Mutual Authentication

(1) Mutual authentication of MS and Certificate Authority

The AKA module proposed in this paper uses SSK_{MS-HN} , a shared secret key based on the EC-DH algorithm, between the MS and the certificate authority (HN) for mutual authentication. The shared secret key, SSK_{MS-HN} , is generated using the initial point and secret key registered in the USIM card and the certificate authority when the USIM card is first registered, and MAC_{MS} and $XMAC_{MS}$ are generated for mutual authentication.

(2) Mutual authentication of MS and SN

The AKA module proposed in this paper uses $OT-SSK_{MS-SN}$ based on EC-DH as a one-time shared secret key, which is set differently depending on the initialization point, for mutual authentication between MS and SN. This one-time shared secret key, $OT-SSK_{MS-SN}$, is used for mutual authentication between MS and SN.

(3) Store and Payment Center Authentication

Stores and payment centers in the mobile payment protocol proposed in this paper also generate a one-time shared secret key and generate a new session key using their respective master keys for mutual authentication.

4.1.2 Enhancing Privacy Protection

The AKA module proposed in this paper solves the privacy problem of IMSI plaintext transmission by encrypting IMSI with SSK_{MS-SN} and transmitting it to the certificate authority.

In the mobile payment protocol proposed in this paper, the store unique code (MC) and payment center unique code (SC) are encrypted using OT_SSK and delivered to the certificate authority, so the information of the store and payment center is also protected.

4.1.3 Retransmission Attack

The AKA module proposed in this paper is safe against attackers' retransmission attacks because it uses a timestamp every time the MS and the certificate authority request mutual authentication and uses the OT-SSK method to generate a new authentication key.

4.1.4 Full Omnidirectional Safety Satisfaction

Since the mobile payment protocol and the AKA module proposed in this paper use SSK and OT-SSK based on EC_DH, even if the initial point P and the public key are disclosed, the SSK and OT-SSK cannot be derived because they do not know each other's secret key, and they satisfy full omnidirectional safety.

4.2 Efficiency Analysis

Table 1 compares the performance of the existing 3GPP-AKA and the AKA module proposed in this paper [13].

4.2.1 Bandwidth Reduction

As can be seen from the amount of authentication data memory in Table 1, the AKA module proposed in this paper does not use authentication vectors, so no authentication vectors are generated and transmitted between the SN and the certificate authority as in the existing 3GPP-AKA. Therefore, the bandwidth between the SN and the certificate authority is reduced from $(688 \times N) \times R$ bits to

$320 \times R$ bits and $368 \times R$ bits, respectively.

4.2.2 Reduced SN storage data

Since the AKA module proposed in this paper does not use the authentication vector AV, the SN does not need to store the authentication vector AV transmitted from the HN separately, so the storage data of the SN is reduced from $(688 \times N) \times R$ bits to $320 \times R$ bits, respectively.

5. Conclusion

With the rapid development of communication and the widespread use of the Internet, many people are frequently accessing remote servers in a distributed computing environment, but data transmission over insecure channels without an authenticated protection system is exposed to many problems such as replay attacks, offline password attacks, and impersonation attacks. In this paper, we design a safe Authentication Key Agreement (AKA) module for mobile payment system suitable for openness smartphone environment that can solve these problems.

The AKA module proposed in this paper prevents IMSI exposure by generating a shared secret key between the MS and the HN for user authentication and encrypting and transmitting the IMSI value of the USIM, and prevents data replay attack by generating a new OT-SSK for each connection by generating message encryption keys, CK and IK, using a one-time shared secret key, OT-SSK, between the MS and SN.

Table 1. Performance Comparison of Proposed Methods

Comparison Items		3GPP-AKA	Proposed Technique
Sequence Problem		Yes	No
Authentication data memory capacity	MS	560bit	496 bit
	SN	$(688 \times N) \times R$ bit	$320 \times R$ bit
	HN	$(688 \times N) \times R$ bit	$368 \times R$ bit
Authentication parameters that should be stored	MS	RAND, CK, IK, SQN, AK, AMF, MAC	MAC, AK, XMAC, CK, IK, SSK, T
	SQN	RAND, CK, IK, SQN, AK, AMF, MAC, XRES	CK, IK, SSK
	HN	RAND, CK, IK, SQN, AK, AMF, MAC, XRES	RAND, MAC, XMAC, AK, SSK
Storage space per Authentication Data	RAND: 128 bits, XRES: 128 bits, CK: 128 bits, IK: 128 bits, SQN: 48bit, AK: 48bit, AMF: 16bit, MAC: 64bit, SSK: 64bit N: Number of authentication vectors, R: Number of MSs		

In addition, the AKA module proposed in this paper does not use authentication vectors and SQN, which reduces the bandwidth of SN and HN, and solves the SQN synchronization problem by checking the currently connected MS using shared secret key SSK instead of SQN.

The user authentication of the mobile payment protocol proposed in this paper eliminates the possibility of USIM exposure by encrypting and transmitting the USIM from the store to the certifier with each shared secret key, and generates a new session key using the USIM, a random value, the user's master key, the store's master key, and the payment center's master key every time the identity of the user, store, and payment center is verified, so that malicious users cannot attempt to make mobile payments due to the exposure of the previous session key. In addition, a new session key is generated each time the identity is verified to prevent data retransmission attacks, and the two-step authentication process is designed to make transactions more secure.

References

- [1] Yong Hee Lee, "Third-generation mobile communications and the development direction of mobile financial services," *Finance*, Vol. 637, No. 20-29, April 2007.
- [2] Ki Young Kim, Dong Ho Kang, "Smartphone security technology in openness mobile environment," *Review of the Korea Institute of Information Security and Cryptology*, Vol. 19, No. 5, pp. 21-28, Oct. 2009.
- [3] W. Juang and J. Wu, "Efficient 3GPP authentication and key agreement with robust user privacy protect," *Proceedings of the 2007 IEEE on Wireless Communications and Networking Conference*, pp. 2720-2725, 2007.
- [4] M. Zhang, Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *IEEE Transactions on Wireless Communications*, Vol. 4, No. 2, pp. 734-742, 2005.
- [5] C. Huang, J. Li, "Authentication and key agreement protocol for UMTS with low bandwidth consumption," *Proceedings of the 19th International Conference on Advanced Information Networking and Application 2005*. pp. 392-397, 2005.
- [6] Li Xi, Hu Han-Ping, "A secure mobile payment system," *Computer Technology and Application*, ISSN1934-7332, Vol. 1, No. 1, June 2007.
- [7] Soon Hwa Sung, "Authentication and key agreement using delegation authority for safe mobile payment protocols," *Journal of The Korea Institute of Information Security and Cryptology (JKIISC), Information and Communications*, Vol. 37, No. 2, pp. 135-141, 2010.
- [8] GPP TS 33.102: "3G Security: Security Architecture," V3.10.0. Dec. 2001.
- [9] Shin Hyo Kim, Byung Ho Jung, "Trends in smartcard-based mobile terminal security technology," *Electronic Communications Trends and Analysis*, Vol. 17, No. 3, pp. 15-22, Aug. 2002.
- [10] Choon Soo Kim, "Design and implementation of USIM security module for wireless network interworking," *Journal of the Korea Institute of Information Security and Cryptology (JKIISC)*, Vol. 17, No. 2, pp. 41-49, 2007.
- [11] Yoo Jin Song, Jae Yong Lee, "USIM authentication vulnerability and security mechanism in wireless internet environment," *Review of Korean Society for Internet Information*, Vol. 9, No. 3, pp. 32-37, 2008
- [12] Dong Kyu Won, Eun Sung Jo, Hyung Kyu Yang, Seung Joo Kim, Dong Ho Won "A study on the standardization trend of SIM/ USIM," *Review of the Korea Institute of Information Security and Cryptology*, Vol. 15, No. 3, pp. 48-60, 2005
- [13] Doo Hwan Kim, Soo Hwan Jung "An improved AKA protocol for efficient authentication data management in 3GPP networks," *Journal of The Korea Institute of Information Security and Cryptology (JKIISC)*, Vol. 19, No. 2, pp. 93-103, 2009.



Eun-Hee Jeong

B.S., Statistics, Gangneung National University,
Feb. 1991
M.S., Department of Computer Science and
Engineering (CSE), Kwandong
University, Feb. 1998
Ph.D., Department of Computer Science and
Engineering (CSE), Kwandong
University, Feb. 2003

Currently since Sept. 2003: Associate Professor, Department of
Regional Economics, Kangwon
National University, Samcheok
Campus

Research Interests: Network Security, E-commerce, Web
Programming, Multimedia, Multimedia



Byung-kwan Lee

Graduated from Pusan National University,
Department of Mechanical
Design, Feb. 1975
M.S., Department of Computer Science and
Engineering (CSE), Chung-Ang
University, Feb. 1986
Ph.D., Department of Computer Science and
Engineering (CSE), Chung-Ang
University, Feb. 1990

Currently since Mar. 1998: Professor, Department of
Computer Science, Kwandong
University

Research Interests: Network Security, Computer Networks,
E-commerce