International Journal of Advanced Smart Convergence Vol.8 No.1 44-57 (2019)
http://dx.doi.org/10.7236/IJASC.2019.8.1.44

IJASC 19-1-6

Evolution of PKI Internet Banking in Korea

Seungchul Park

School of Computer Science and Engineering, Korea University of Technology and Education, Cheonan, Chungnam, Korea
scpark@koreatech.ac.kr

Abstract

Most banks in Korea have provided Internet banking services based on PKI(Public Key Infrastructure) certificates since the early 2000s when Internet banking began in Korea. To support PKI Internet banking, the Korean government backed the electronic signature law and supported the rapid spread of PKI-based Internet banking by regulating the application of PKI certificates to be compulsory in Internet banking until 2015. PKI Internet Banking in Korea has been developed as a pioneer in this field through many challenges and responses until its present success. Korea's PKI banking, which started with soft-token-based closed banking, has responded to various types of cyber attack attempts and promoted the transition to open banking by accepting various criticisms due to lack of compatibility with international standards. In order to improve the convenience and security of PKI Internet banking, various attempts have been made, such as biometric-integrated smartphone-based PKI authentication. In this paper, we primarily aim to share the experience and lessons of PKI banking by analyzing the evolution process of PKI Internet banking in Korea. It also has the purpose of presenting the challenges of Korea's PKI Internet banking and sharing its development vision.

Keywords: *PKI, Internet banking, Authentication, Cyber attacks, SSL/TLS*

1. Introduction

PKI Internet banking is a system in which users connect to a banking server using certificates issued through a PKI and receive the banking services. Every user of the PKI banking has his or her own public key certificate issued by a specific certification authority of the PKI and a private key corresponding to the public key. The private key is a secret key that is protected by a password or the like. The PKI banking server authenticates the user and authenticates the transaction by verifying through the certificate that the user has the corresponding private key. PKI authentication generates a digital signature with a private key corresponding to the public key of the certificate of the user in response to a challenge provided by the banking server and delivers the digital signature to the server, and verifying the digital signature via the public key. In PKI banking, a PKI key exchange scheme may be used to encrypt and transmit a cryptographic key(symmetric key) using the server's public key for transaction information encryption. PKI banking supports two factor authentication, which consists of private key possession and private key

Manuscript Received: Jan. 7, 2019 / Revised: Jan. 15, 2019 / Accepted: Jan. 21, 2019
Corresponding Author: scpark@koreatech.ac.kr
Tel: +82-41-560-1492, Fax: +82-41-560-1462
School of Computer Science and Engineering, Korea University of Technology and Education, Cheonan, Chungnam, Korea

protection password knowledge, which provides a strong authentication service compared to existing password based authentication. In addition, when setting up a web session, it provides a strong security service such as defending a Man-In-The-Middle(MITM) attack by mutually authenticating a server and a client(user) based on a server certificate and a client certificate, respectively[1]. However, PKI banking has not been so much activated globally because of the difficulty of establishing a PKI for individual users, the difficulty of certificate management, and the cost.

Unlike the global PKI Internet banking situation, Korea's banks have been providing PKI banking services very successfully since the early 2000s when they began to provide Internet banking services. The Korean government enacted the electronic signature law in 1999 to promote PKI construction and provided the grounds for recognizing the legal effect of electronic signatures. In 2000, the National PKI was established by designating 6 certification authorities certified by the government. The Korean government, which trusted the high security of the PKI compared to the password-based authentication that was the usual authentication system at that time, came to mandate the PKI certificate application to the Internet banking in 2002[2]. A certificate based on the national PKI is called an accredited certificate. In this paper, a certificate is used in the same way as an accredited certificate. Since then, all banks in Korea have started Internet banking based on PKI certificates, and Korea's Internet banking has spread rapidly due to the user's high interest in Internet banking and high trust in PKI banking.

In the early 2000s, when deciding to provide the PKI Internet banking service in the Web environment, the Web service environment was somewhat lacking in terms of security. The Data Encryption Standard(DES), which used a 56-bit cryptographic key, and the RC4 cryptographic algorithm based on a 40-bit cryptographic key were insufficient to guarantee the security of Internet banking. Therefore, Korea's banks have adopted SEED, a 128-bit cryptographic key-based encryption algorithm developed by the Korean government[3]. Because, at that time, SEED was not supported by standard web browsers, it had to be solved by installing a separate web browser extension software. Since the web browser did not provide effective private key storage, protection, and signature generation functions, related functions were also implemented by the method of installing the browser extension software. And PKI Internet banking in Korea adopted a soft-token-based authentication method, mainly for the convenience of users, in which a private key is stored in a file system(hard disk, USB memory) and a private key is encrypted using a cryptographic key generated by a password. As a result, Korea's PKI Internet banking has been launched as a soft- token-based closed banking that is incompatible with the web browser standards and security communication protocol standards. The implementation adopts a plug-in method of installing the extension software in a standard web browser. At that time, Microsoft's Internet Explorer(IE) web browser was dominant in Korea's market, so plug-in software was implemented based on ActiveX, the extension language of IE[2].

Korea's soft-token-based, closed-type PKI Internet banking, implemented with ActiveX plug-in software, has contributed significantly to the rapid deployment of PKI Internet banking, allowing new requirements to be implemented quickly and flexibly regardless of the development of international standards. However, on the one hand, there has been various problems such as security vulnerabilities due to cyber attacks on soft tokens and banking applications, inconvenience due to additional authentication methods adopted during cyber attack countermeasures, user inconvenience due to the installation of plug-in software, and lack of compatibility with other web browsers due to IE-dependent ActiveX plug-in software implementation[4,5]. In addition, it has been criticized that the mandated application of PKI certificate to Internet banking may hinder the development of various security technologies, especially authentication technology. Therefore, the Korean government abolished the regulation of compulsory application of PKI certificates in Internet banking in 2015, while encouraging the transition from closed PKI Internet banking to open PKI Internet banking compatible with standard SSL/TLS based web browsers[6]. Most of banks have begun to offer the open PKI Internet banking services in Korea. And there are efforts to improve the security problem of soft token based PKI banking in a way that does not hinder convenience. One of them is the introduction of smart

authentication that supports the generation of digital signatures in the USIM(Univeral Subscriber Identity Module) of smartphones. Currently, smart authentication is combined with FIDO(Fast Identity Online) biometric authentication in some smartphone models to solve some security and convenience problems that password-based soft tokens have[7].

In this paper, we analyze the evolving process of PKI Internet banking in Korea, which is a successful case of PKI internet banking in the world, and shares the experience and lessons of its security, convenience, and implementation process. This paper is also described for the purpose of presenting and sharing the vision of how to develop in order to improve security and convenience of PKI Internet banking in Korea. Sharing the experience and lessons of Korea's PKI Internet banking will be a good reference not only for the banking service providers who are interested in the PKI Internet banking, but also for other secure membership services of other platforms based on the PKI certification.

2. Related Works

It is not known exactly how much PKI Internet banking is taking up in the Internet banking market all over the world. In 2014, a technical report surveyed 80 banks around the world and announced what authentication techniques they are using[8]. It is reported that nine banks among them use certificate-based authentication, which means that PKI banking accounts for about 10%, but since the number of banks to be surveyed is too small, there is a question. The survey did not include Korea's banks. Although the PKI has been developed and standardized in order to create the basis of digital signatures, it can be seen that the proportion of applying PKI in Internet banking, which has a high necessity of digital signature in the Internet transaction process, is currently very low. However, the high security capability of PKI is recognized globally. The US government's authentication guideline defines soft-token-based PKI authentication as level 3 and hard-token-based PKI as level 4, where level 4 is strongest[9]. And the US government requires online identity verification of federal employees to be based on PKI certification to ensure greater safety[10]. The SSL/TLS implementation guideline also recommends implementing PKI client authentication when strong authentication is required[1]. The Hyperledger Fabric, a newly emerging permission-type Blockchain system, also provides the secure membership services based on the PKI[11].

In the case of Korea, data shows that the situation is completely different. A national information security white paper published in April 2016 reports that 33.88 million PKI certificates have been issued and used in the Republic of Korea[12]. And a survey report shows that more than 97% of certificate issuers use certificates for Internet banking[13]. Given that Korea has a total population of 51 million, we can see how active PKI banking is in Korea. Research on the hidden problems behind the explosion of Korea's PKI Internet banking has been actively conducted. A research report written by a research team at Oxford University in England in 2010 summarized the security and usability issues of PKI Internet banking in Korea[4]. This study is considered to have played a role as a catalyst for the efforts to convert the closed PKI Internet banking of Korea into an open type and to enhance user convenience. And the issues discussed, since then, regarding to Korea's PKI Internet banking were summarized and presented by [5]. Efforts to migrate the existing closed PKI Internet banking to the open banking have been conducted mainly by the Korea Internet & Security Agency(KISA), which is a government-run security research and support organization. The report published by KISA in September 2014 provided a key foundation for the implementation of open PKI Internet banking[6].

There have been various attempts to point out the problems of PKI Internet banking in Korea and research directions for its future development. However, there are few studies to share the experience and lessons of PKI Internet banking by analyzing PKI internet banking's evolving process, problems occurred in the evolving process, the process to cope with it, and future tasks and development vision. The study of this paper is different from the related studies in that it focuses on this part.

3. Soft-token-based Closed PKI Internet Banking

Korea's PKI Internet banking, launched in the early 2000s, was constructed with a soft-token-based closed Internet banking structure mainly for user convenience, technical situation at the time, and flexible implementation.

3.1 Soft-token-based PKI Internet Banking

A soft token is a software module on a computer that performs a series of tasks to store and protect a PKI certificate and corresponding private key, and generate a digital signature based on them. PKI Internet banking in Korea was built on the basis of soft tokens due to the technical situation in the early 2000s, cost problems due to the dissemination of extra hardware modules, and user inconvenience caused by possession of hardware modules. The PKI certificate and the private key are stored in the file system of the PC(hard disk or USB memory) and the private key is protected by the encryption key deduced by the password. The user releases the private key by entering the password through the software module whenever a digital signature is needed. The biggest advantage of introducing a PKI soft token was user-friendliness. This is because the user stores the certificate and private key in the hard disk or USB memory of his/her PC and inputs the password only when needed.

However, soft tokens protected by passwords have exposed vulnerabilities in terms of security. An attacker can replicate the certificate and private key stored in the file system and hack the password to create a digital signature for that user, which is at the heart of PKI security. We will discuss in detail the attacks that have been attempted on the soft token of PKI Internet banking in the next section. PKI Internet banking companies have been working hard to develop and distribute hard tokens in order to solve security weakness of soft token. The hard token uses a separate hardware module that acts as a soft module. The hard token is more secure than the soft token because it protects by storing the certificate and private key on the separate hardware where the replication attack is blocked. Nevertheless, the actual penetration rate is negligible due to inconvenience caused by the possession of a separate hard token and the difficulty of supplying hard tokens.

Figure 1 shows the use of PKI certificates and private key storage media in Korea as of the end of December 2015[13]. It can be seen that the usage rate of HSM(Hardware Security Module) and Smart Card (corresponding to the hard tokens) is only about 7%. Most PKI Internet banking users store the PKI certificates and private key in USB memory or HDD, and some store in both USB and HDD.

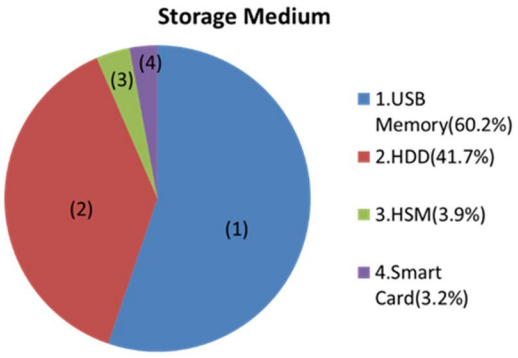

Figure 1. PKI certificate and private key storage medium

3.2 Closed PKI Internet Banking

The characteristics of the Korea's PKI Internet banking system which has been constructed and used from the early 2000s can be summarized as follows.

- Instead of adopting the de-facto international standard encryption algorithms DES and RC4 at

that time, they used their own SEED encryption algorithm. They developed its own SEED algorithm, which supports 128-bit cryptographic keys, with concern for the safety of DES which uses 56-bit cryptographic keys and RC4 which uses 40-bit cryptographic keys. However, SEED could not be supported without an additional extension in the standard web browser of the time.

- At the time, standard web security protocol SSL/TLS lacked confidence in safety and did not support the SEED encryption algorithm. Therefore, instead of using SSL/TLS, secure communication functions were proprietarily developed and used as part of the application program.
- Plug-in software installation method was applied to implement security functions that were not supported in the standard web browser environments. The plug-in software was implemented with ActiveX, the extension language of Microsoft's IE which had dominant market share at the time.

As a result, Korea's PKI Internet banking has become a closed system that is not compatible with standard security communication protocols and standard web browsers. According to the Internet banking guideline published by the Financial Security Agency, the government's Internet banking security support organization, it can be seen that overall procedure of Korea's PKI Internet banking service is the same as in Figure 2[14].

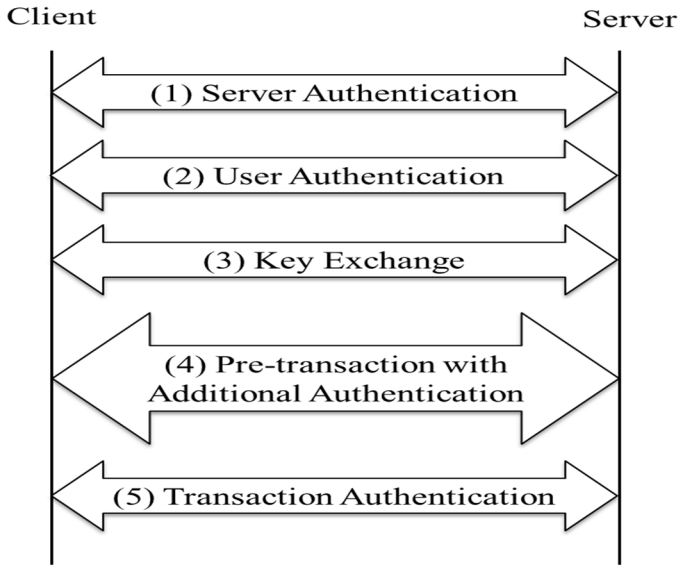

Figure 2. Procedure for implementation of closed PKI Internet banking

An Internet banking client program running on a web browser first performs server authentication. Server authentication is accomplished by verifying the server certificate. Because the closed PKI Internet banking does not use SSL/TLS, server certificate validation occurs in client applications rather than SSL/TLS-based web browsers. The user authentication process of the closed PKI Internet banking is shown in Figure 3. The user(U(i)) receiving the authentication request from the server releases the private key($PK^{-}_{U(i)}$) for generating the signature by inputting the password through the client program, and generates a signature for the challenge of the authentication request message. The signature generation is performed by public key encryption of the signature contents with the user's private key(E($PK^{-}_{U(i)}, challenge$)), and the public key certificate(Cert(U(i), $PK^{+}_{U(i)}$)) and signature (E($PK^{-}_{U(i)}, challenge$)) are sent to the server. After verifying the certificate, the server extracts the public key($PK^{+}_{U(i)}$) of the user and verifies the signature. Signature verification is accomplished by decrypting the signature using the public key(D($PK^{\mp}_{U(i)}$, E($PK^{-}_{U(i)}, challenge$))) and then verifying that the decrypted signature content matches the

challenge it sent. If the signature is successfully verified, the user authentication is terminated successfully.

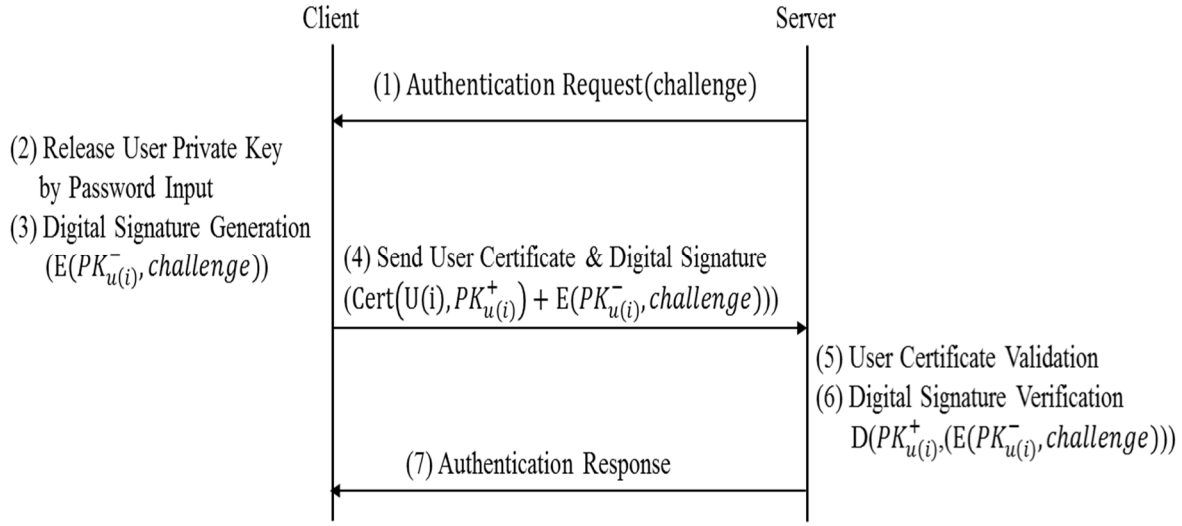

Figure 3. User authentication procedure of closed PKI Internet banking

Figure 4 shows the procedure of key exchange in the closed PKI Internet banking. The client application of a user(U(i)) utilizes the server certificate($Cert(S(j), PK^{+}_{S(j)})$) previously received from the server(S(j)) to exchange a session key which is used for transaction information encryption. The client firstly generates a session key($SK^{U(i)}_{S(j)}$) to be used for transaction information encryption in the session, encrypts the session key with the server public key of the server certificate, and transmits the encrypted session key($E(PK^{+}_{S(j)}, SK^{U(i)}_{S(j)})$) to the server. This type of key exchange scheme is called RSA (Ronald Rivest, Adi Shamir, and Len Adleman) key exchange scheme. The server obtains the session key($SK^{U(i)}_{S(j)}$) by decrypting the encrypted session key using its private key($D(PK^{-}_{S(j)}, E(PK^{+}_{S(j)}, SK^{U(i)}_{S(j)}))$). After that, the client and the server encrypt and exchange the transaction information using the corresponding session key.

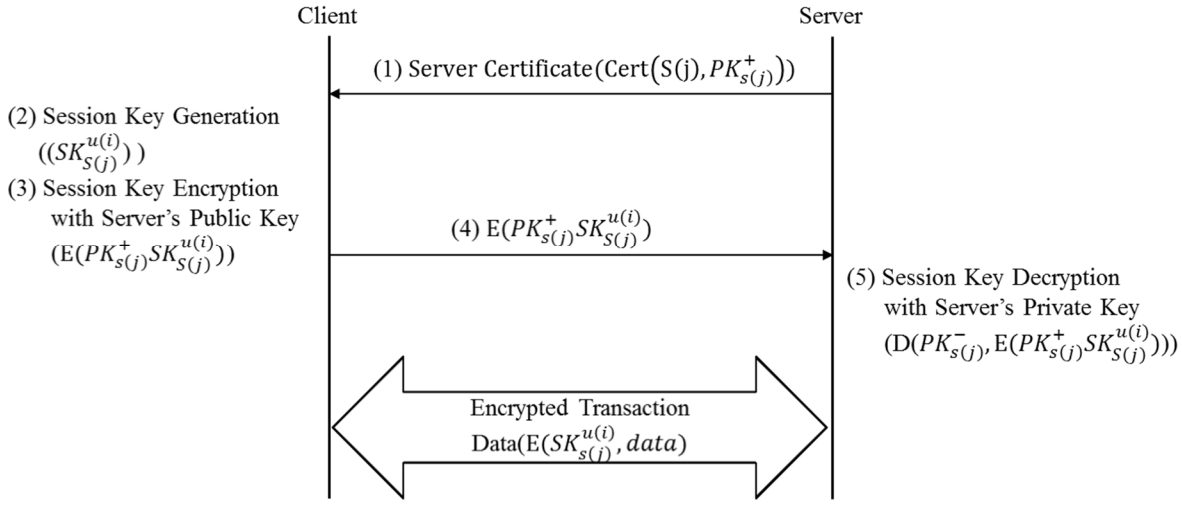

Figure 4. Key exchange procedure of closed PKI Internet banking

4. Cyber Attacks and Countermeasures against Closed PKI Internet Banking

The cyber attacks that have been attempted for the closed PKI Internet banking in Korea are classified

into five types as shown in Table 1. They are offline phishing attack, online phishing attack, keylogger attack, file system hacking attack, and memory hacking attack. Among these, the upper four types are attacks on soft token vulnerabilities, and the last one is attack on application vulnerability.

Table 1. Summary of cyber attacks and countermeasures

vulnerabilities	attack types	countermeasures
- soft token vulnerability	- offline phishing attack	- iTAN deployment
	- keylogger attack	- enhancement of anti-keylogger software - extension of iTAN
	- online phishing attack	- promotion of OTP usage - anti-phishing campaign
	- filesystem hacking attack	- promotion of HSM and OTP usage - enhancement of anti-malware software
- browser application vulnerability	- memory hacking attack	- extension of end-to-end encryption - deployment 2nd channel authentication

4.1 Soft Token Vulnerability Attacks and Countermeasures

Cyber attacks on PKI Internet banking in Korea have been focused on security weaknesses in soft tokens. The first type of attack attempted against the soft token is the offline phishing attack that attacks a user who is vulnerable to security through phone or e-mail in a social engineering way to find out the password of the token. Then the attacker re-issues the PKI certificate online and uses it in fraud financial transactions such as online loaning. This attack utilized a vulnerability in which a PKI certificate is re-issued online with a password input. As a countermeasure against this type of offline phishing attack, iTAN(indexed Transaction Authentication Numbers) called security card was deployed to confirm in addition to the password when re-issuing the online certificate. The security card could then be replaced by an OTP(One Time Password).

The second type is the keylogger attack that seizes the private key protection password and the security card(iTAN) number that the user enters by using the keylogger malicious software. This attack exploited the vulnerability of password-based private key protection of soft tokens and vulnerability of small number of security cards. The attacker reissues a PKI certificate using the acquired victim's password and the security card numbers, and uses the reissued PKI certificate and the security card in fraud financial transactions such as online loaning. Anti-keylogger software has been improved as a countermeasure against this attack. At the time, the number of security cards in 35 or more has been enlarged to more than 1000, making it difficult to take out security card numbers by keyloggers.

The third type of attack against a soft token is the online phishing attack. After luring a vulnerable user to connect to a fake site similar to a bank site, the user is prompted to enter a password, a total security card number, a financial account number, etc. for security reasons. By using this information, the attacker tries to transfer money of the user to his own account so as to cause the monetary damage to the user. This attack exploits the vulnerability of closed PKI banking application software not appropriately distinguishing and warning fraudulent sites based on the PKI server certificates, and the tendency of users to ignore warning messages. As the countermeasures against this type of attack, instead of security cards, the use of OTPs that can not be exposed to counterfeit sites are highly encouraged, and they have strengthened education and campaigns to prevent users from entering the entire credentials.

The fourth type of attack on a soft token is the attack that hijacks the file system and seizes a certificate, a private key, a password recorded in a file, and a security card stored as a photograph. This attack exploited the vulnerability of the PKI certificate and private key of the soft token stored in the file system, and aimed at the careless user who recorded the password in a file, and photographed the security card and stored it in the file system for convenience. The attacker uses the captured information for fraud financial transactions,

such as loan and account transfer, and damaged the user. In response to this attack, the use of anti-malware software such as PC firewall has been promoted, and the storage of certificates and private keys in HSM (Hardware Security Module), which is not possible to attack by malicious software, has been also encouraged. In addition, they encouraged, instead of security card, the use of OTP which can not be totally exposed. As shown in the cyber attacks on the soft tokens mentioned above, the vulnerabilities of the soft token is that, first, replication attacks can be performed on the certificate and private key, and second, the cracking attacks on the private key protection password are possible. One of the complementary countermeasures, the security card has a weak point of being exposed to phishing attacks, so OTP is being preferentially adopted as a countermeasure against soft token. Encouragement for using OTP instead of a security card is being made through incentives such as differentiation of transfer limit. HSM, a hard token, protects against replication attacks, but it does not address the need for password-compliant OTPs. That is, even if HSM is used, OTP must be used at the same time. As a result, PKI Internet banking in Korea based on soft token is supposed to be combined with OTP (or security card) which is another type of hard token.

4.2 Soft Token Vulnerability Attacks and Countermeasures

Most of the cyber attacks against Korea's closed PKI Internet banking were attacks against soft tokens that can cope with the OTP countermeasure, but memory hacking attacks were a completely different type of attack. The memory hacking is an attack that changes the transaction information (account, amount, etc.) in the memory of a client application program operating as a browser application, without the user's perception. Memory hacking attacks are commonly referred to as MITB(Man-In-The-Browser) attacks. This attack was first attempted at the end of 2013, and since it is done after authentication, it can not be defended even by using the OTP. The attacker puts the user in a wait state, changes secretly the amount of the transfer money and the receiving account number to the attacker's account. The user sees the screen as if it is normal because the attacker displays the original data, not manipulated data, so that the user can not notice the change of the transaction content. Even in the transaction signing step, the user can not recognize the manipulation fact because client application program signs the changed contents of the web memory, not the contents displayed on the screen. This attack exploits a vulnerability in which transaction information on the web memory before encryption is exposed to an attacker and a vulnerability in which a transaction signature is made on the web memory. As a countermeasure against this attack, they implemented an extended end-to-end encryption module. As shown in Figure 5, it immediately encrypts the transaction information(account information, money information, etc.) inputted from the keyboard and transmits the encrypted information together with the transaction information processed and signed in the web memory so that they can be compared in the server. If there is a difference in the comparison result, the transaction is recognized abnormal and the transaction is canceled. In addition, when the receiving account is changed in the transaction process, a method of reconfirming through 2-channel authentication is introduced.

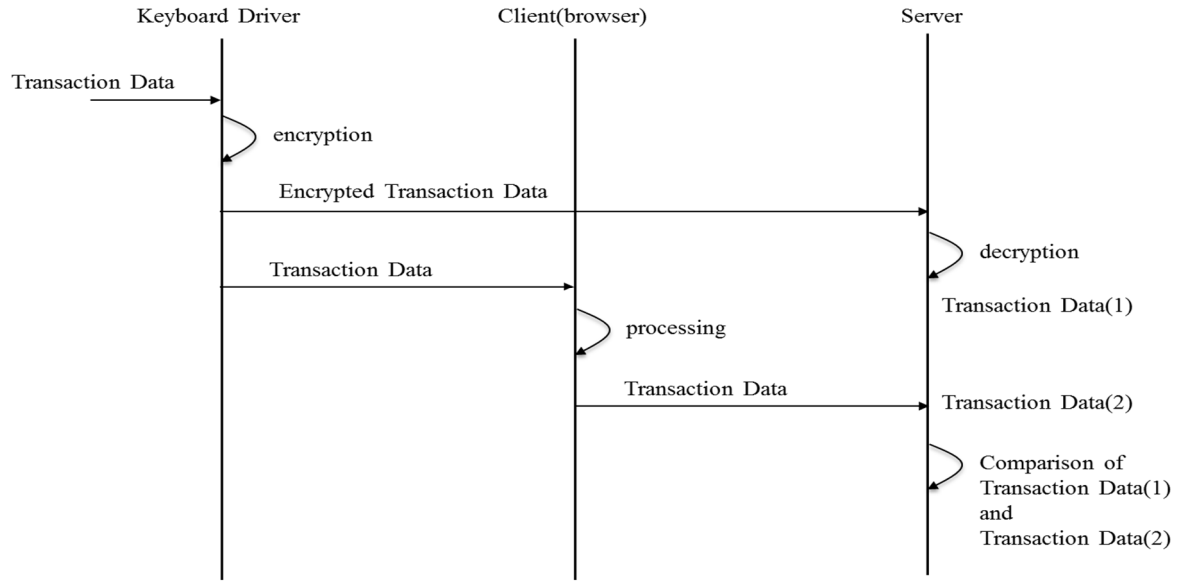

Figure 5. Procedure of extended end-to-end encryption

5. Transition to the Open PKI Internet Banking

5.1 Transition to Open Structure

In the 2010s, criticisms about the inconvenience caused by the lack of compatibility of Korea's closed PKI Internet banking began to grow. The criticisms can be summarized as follows.

- Since PKI Internet banking is implemented as ActiveX plug-in software that is dependent on IE, it is impossible to use Internet banking in Chrome, Safari etc. which are new web browsers.
- Downloading and installing many ActiveX plug-in software is inconvenient and difficult. In particular, malfunctions caused by inconsistencies between the OS version and the plug-in software version increased user inconvenience.
- Downloading and installing Internet banking plug-in software is exploited as a distribution path for malicious software. Most users lacking knowledge of Internet security installed various kinds of malicious software pretending to be Internet banking plug-in software without suspicion on their computers. As a result, many malicious software such as DDoS zombie software was widely spread, which resulted in a lot of cyber attacks in Korea's Internet environment.
- Because it does not support SSL/TLS, which is a standard web security protocol, advanced security features of SSL/TLS included in standard web browser can not be utilized. The advanced security features of SSL/TLS include encryption functions such as AES, key exchange algorithms such as DHE(Diffie-Hellan Ephemeral), ECDHE(Elliptic Curve DHE), and server authentication by EV(Extended Verification) certificate.

In response to this criticism, the Korean government began to make efforts to induce the transition from closed PKI Internet banking to open banking in earnest in late 2014. In addition, the Korea's government has made it possible to develop and apply various authentication technologies by abolishing the PKI certificate obligation in Internet banking in 2015. From the end of 2016, most of Korean banks have started offering open PKI Internet banking services.

5.2 Structure of Open PKI Internet Banking

To solve the criticisms of the existing closed PKI Internet banking, a new open PKI Internet banking was developed in Korea in the following way[6].

- Standard SSL/TLS protocol is used, server authentication is performed using SSL/TLS EV

certificate, and user authentication uses SSL/TLS client authentication.

- In order to eliminate the need for plug-in software installation, it is implemented using the standard web browser security API(Application Programming Interface). If additional browser functionality needs to be extended, it is implemented in a standard language such as HTML5 to ensure web browser compatibility.
- It utilizes the experience of existing closed PKI Internet banking to minimize security threats. In addition to SSL/TLS, additional application-level end-to-end encryption is implemented to protect against application-level memory hacking attacks(MITB attacks).

As a result, the open PKI Internet banking solution was developed as shown in Figure 6. SSL/TLS basically provides a secure channel for the exchange of HTTP messages exchanged between a web browser and a web server.

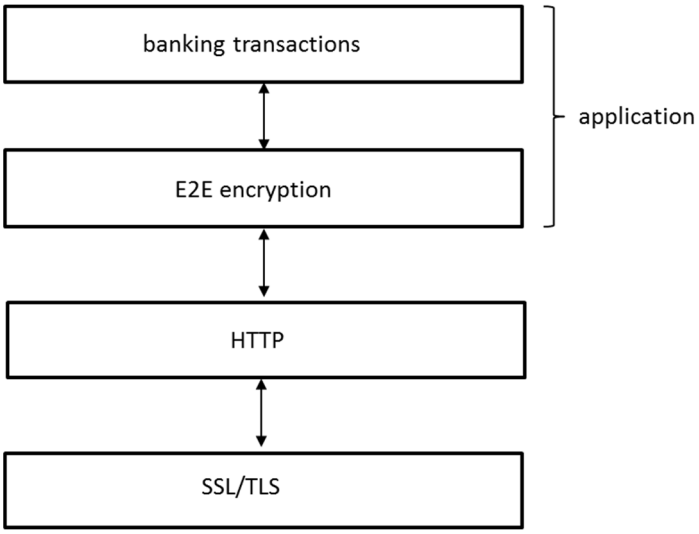

Figure 6. Structure of open PKI Internet banking

However, open PKI Internet banking additionally implements end-to-end(E2E) cryptographic functions at the application level in order to maximize the defense of memory hacking attacks(MITB attacks) which may occur between applications and SSL/TLS. Consequently, the open PKI Internet banking application will use a dual security channel. Figure 7 shows how to utilize SSL/TLS in open PKI Internet banking.

While the existing closed PKI Internet banking provides server authentication by its own application, open PKI banking uses a standard web browser to perform server authentication using the function of SSL/TLS server authentication based on EV certificate, which makes it easier to distinguish the banking server from the phishing site through the standard web browser's user interface. That is, a server authenticated with a normal EV certificate is displayed in a green color in the address bar of the web browser. User authentication of open PKI Internet banking is performed by utilizing client authentication function of SSL/TLS, and authentication is performed by validating the user's PKI certificate and signature. The PKI certificate and the private key are stored in a web-accessible web repository, and the private key protection uses the same password method as the closed PKI Internet banking. While closed PKI Internet banking uses RSA method for cryptographic key exchange, open PKI Internet banking can select one from various methods such as RSA, DHE and ECDHE supported by SSL/TLS.

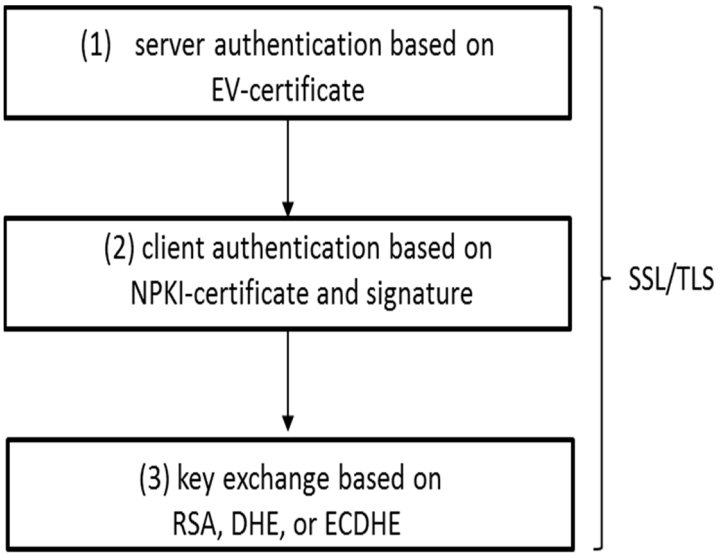

Figure 7. Utilization of SSL/TLS in the open PKI Internet banking

6. Future Challenges of Korea's PKI Internet Banking

As Korea's PKI Internet banking is implemented as an open banking system, problems caused by the lack of compatibility with standard web browsers and user inconvenience due to installation of plug-in software are expected to be solved. However, the necessity of password management for soft token protection and the inconvenience of using additional authentication tools such as OTP to supplement security of soft token are important problems which needs to be solved not late. Currently, FIDO(Fast Identity Online) authentication[15], which is actively being introduced in payment gateway services, is considered to overcome the inconvenience of using password by generating digital signature based on biometric authentication and to guarantee safety above PKI authentication level. FIDO Internet banking is also expected to be implemented in Korea due to the abolishment of the obligation of PKI certificates in Internet banking. Especially, since the establishment of two Internet banks in Korea, K-Bank and Kakao Bank, since 2017, competition for convenient and safe Internet banking is expected to be heated up. Defending against memory hacking attacks, which occur because a digital signature is generated on a web browser, is another challenge for soft-token-based PKI Internet banking. Since the emergence of attack technology that can avoid the end-to-end encryption function at the application level due to the evolution of cyber attack technology is a matter of time, it is necessary to provide a more fundamental solution which can be readily accepted by users from the viewpoint of convenience. Existing hard tokens provide digital signature generation, but users can not verify the content to be signed in hard token. In addition, users have to inconvenience the need to hold hardware separately. Actually, hard tokens have a small usage rate.

We name the PKI security token, that can accommodate all of these requirements, as the smart hard token in this paper. Considering advanced authentication technologies such as FIDO authentication, the requirements for the smart hard token can be summarized as follows.

- It should be implemented on a trust platform where replication of certificates and private keys is not possible.
- It should be able to support more convenient and secure biometrics authentication methods that can replace passwords for private key protection.
- It is necessary to support sufficient security so that additional authentication means such as OTP, which is a problem for user's convenience, should be unnecessary.
- A user interface should be provided to allow the user to check transaction details in the signature generation process for transaction authentication and conveniently enter transaction information

if necessary.

- Users' inconvenience due to additional hardware possession should be minimized.
- The cost burden of the user and the banking service provider should be acceptable.

Since late 2014, mobile phone service providers(KT, SKT, LCU+) in Korea have jointly provided digital signing service using USIM embedded in smartphone in the name of Smart Authentication Service for a fee. The USIM authentication service provides a fingerprint authentication interface in some smartphone models as well as a password to protect the private key. And since most of the users of Internet banking use the smartphone they own, it can solve the user inconvenience due to the possession of additional hardware which is a disadvantage of the hard token. However, the existing USIM smart authentication service is provided by mobile phone service providers as an alternative to the hard token service, apart from the security system of the Internet banking system. Therefore, users of USIM smart authentication still have to use additional authentication methods of Internet banking such as OTP. Also, existing USIM smart authentication has limitation that it does not include confirmation service of transaction contents in the smartphone. Considering that 42.4% of users who are reluctant to switch to a secure storage medium are found to be incurring expenses[13], it can be seen that paid services are also a problem in accepting USIM smart authentication.

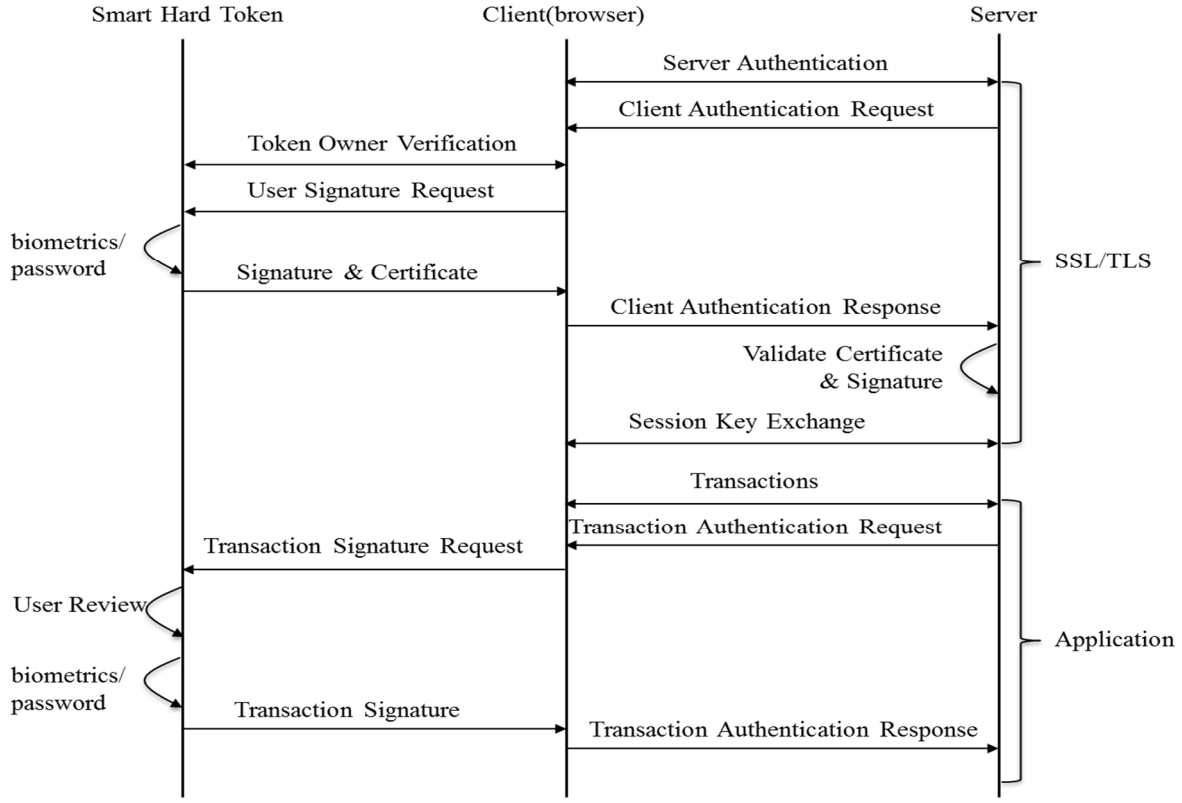

Figure 8. Operation procedure of Smart-token-based Internet banking

Like USIM smart authentication, the smart hard token of this paper should be implemented based on smart phones already carried by most Internet banking users. The storage for certificate and private key and digital signature generation can be implemented through trusted platforms such as USIM, embedded Secure Element(eSE), micro Secure Digital Card(microSD), and so on. Communication with the PC Internet banking application program can be realized not only by the 3G/4G communication network but also by WiFi, and the usage cost should not be additionally incurred in addition to the transmission cost of the exchanged data. It is also necessary to block the memory hacking attack by allowing the user to confirm the transaction information through the smart hard token and perform signature generation. It is necessary for the Internet banking service provider to intervene in the issuance and management process of the smart hard

tokens so as to avoid unnecessary additional authentication means such as OTP in consideration of the high security of the smart hard tokens. For example, a smart hard token user is allowed not to possess an OTP, which will improve user convenience.

The expected operation procedure of smart-token-based Internet banking is shown in Figure 8. The process of identifying a token owner between a client application on a web browser and a smart hard token should be supported(token owner verification). The smart hard token must support biometrics or password for private key protection. In the signature generation step, the user confirms the contents of the transaction through the smart hard token(user review), and generates a signature through biometric authentication or password input. In the course of Internet banking transaction through application program, additional authentication through OTP is unnecessary. In the future, it is expected that open PKI Internet banking based on the smart hard tokens will have sufficient competitiveness in terms of convenience as well as security in comparison with other FinTech-based Internet banking services such as FIDO banking.

7. Conclusion

From the very beginning of the Internet banking service, Korea has built Internet banking on the basis of PKI, and made a world-class success story of PKI application. This paper analyzed the evolution process of PKI internet banking in Korea so as to share its experience and lessons. Korea's PKI Internet banking has used soft tokens mainly, and the soft tokens have become a major target in many cyber attacks attempted against internet banking in Korea. This paper analyzed what types of cyber attacks have been attempted and what countermeasures have been introduced in response. This analysis will be a good reference for deciding what type of security tokens to adopt in PKI application services. We also analyzed the background of Korea's PKI Internet banking which was constructed not compatible with the standard web browser and SSL/TLS, and the criticisms raised about it, and introduced the process of transition to the open PKI Internet banking from the closed Internet banking. As a result, Korea's PKI Internet banking has evolved a lot, but there are still challenges. User inconvenience caused by using additional security measures such as OTP is a challenge to be solved. Another key challenge is the introduction of a solution that can more reliably defend against memory hacking attacks(MITB attack). This paper proposes the introduction of smart hard tokens, which are quite different from the existing USIM hard tokens, to solve the remaining challenges of PKI Internet banking in Korea. A smart hard token is implemented on the trusted platform of a smartphone where replication attacks against certificate and private key are not possible. And the smart hard token provides not only the signature generation function but also the signature content checking function by the user to protect the memory hacking attack. Smart hard tokens are also integrated with user-friendly security interfaces such as biometrics. It is expected that the experience and lessons of Korea's PKI Internet banking analyzed in this paper and its future development vision will contribute to the activation of security services based on PKI, including not only future Internet banking but also other secure membership services of the permissioned Blockchain systems, for example.

Acknowledgement

This paper was supported by the 2019 professors' teaching and research promotion program of Korea University of Technology and Education.

References

[1] National Institute of Standards and Technology, *Guidelines for the selection, configuration, and use of Transport Layer Security(TLS) implementations*, NIST Special Publication 800-52 Revision 1, 2014.

[2] J. H. Lee, "Usability and problems of accredited certificate in smart environments," *Internet & Security Focus*, pp. 23-53, March 2013.

[3] TTA Standard, *128-bit Symmetric Block Cypher(SEED)*, TTA.KO-12.004, 1999
[4] H. S. Kim, J. H. Huh, and R. Anderson, *On the security of Internet banking in South Korea*, Oxford Univ. Computing Laboratory, Technical Report CS-RR-10-01, 2010.
[5] S. W. Chai, K. S. Min, and J. H. Lee, "A study of issues about accredited certification methods in Korea," *International Journal of Security and Its Applications*, Vol. 9, No. 3, pp. 77-84, 2015.
DOI: http://dx.doi.org/10.14257/ijsia.2015.9.3.08
[6] Ministry of Science, ICT and Future Planning and Korea Internet & Security Agency, *Technology guideline for improving Internet usability environment*, MSIFP and KISA Special Publication, Sept. 2014.
[7] Korea Internet & Security Agency, *Implementation Guideline for Safe Usage of Accredited Certificate Using Bio Information in Smartphone*, KCAC.TG.IMP V1.00, May 216.
[8] S. Kiljan, K. Simoens, D. D. Cock, M. V. Eekelen, and H. Vranken, *Technical report : security of online banking systems*, Technical Report of Open Universiteit, Feb. 2014.
[9] National Institute of Standards and Technology, *Electronic authentication guideline*, NIST Special Publication 800-63-2, 2013.
[10] National Institute of Standards and Technology, *Personal Identity of Verification(PIV) of Federal Employees and Contractors*, FIPS PUB 201-2, 2013.
[11] Hyperledger Fabric, *https://hyperledger-fabric.readthedocs.io/en/release-1.1/identity/identity.html*
[12] National Information Agency, and et. al, *2016 National Information Security White Paper*, White Paper, April 2016.
[13] Korea Internet & Security Agency, *Research on the Actual Condition of Electronic Signature System Usage*, KISA-WP-2015-0032, Dec. 2015.
[14] Financial Security Agency, *A Management Guide for Financial Part Encryption Technologies*, FSA Special Publication, Jan. 2010.
[15] FIDO Alliance, *Specifications Overview*, *https://fidoalliance.org*.