International Journal of Security and Its Applications
Vol.9, No.9 (2015), pp.9-20
http://dx.doi.org/10.14257/ijsia.2015.9.9.02

A Study on Service Architecture for Secure Authentication System

Sung Jin Kim[1], Myung Chul Ma[2], Hyeon-Kyung Lee[3] and Jong-Bae Kim[4*]

[1,2]*Dept. of IT Ploicy and Mgnt., Graduate School of Soongsil Univ., Sangdo-dong, Dongjak-gu, Seoul 156-743, Korea*
[3,4*]*Graduate School of Software, Soongsil University, Sangdo-dong, Dongjak-gu, Seoul, Korea*
[1]*sujnkim@itnomads.com,* [2]*mcma@posod.co.kr,* [3,4*]*{hklee,kjb123}@ssu.ac.kr*

Abstract

This study designed a safe combined certification system by approaching the matter of certification upon recent expansion of the cyber world and the market size of mobile shopping through a newer plan. Recently, mobile field has drawn much attention and it is used for most means of living for users like purchase of commodity, payment, and user certification. The mobile economy also grows by this trend, but hacking accidents or financial crimes are also in full swing. It is expected that the service for mobile in the future will increase more than ever, but in security aspects we still use problematic certification and security system. Data control service in the future is expected to do a lot with the service, which basically stores all services in phones as well as service providers through cloud service. Data control service will lead to the expansion of IoT (Internet of Things) service, as it substitutes existing off-line backup and safely provide user data regardless of location or kinds of devices. That is, users can use data from the devices connected to the Internet without copying or moving to devices users want to use. To use this data safely, establishing a certification system of users will be an ever more important factor. Therefore, this treatise is going to suggest the plan that we can conduct the certification in a safer way among several threats. In particular, mobile hacking is a very serious and important issue, as it could directly lead to monetary loss. When certification is insufficient, the possibility of a third party reaping benefits through hacking is greater. This treatise is going to suggest a model that service providers can provide safe certification service by performing verification of transaction and data through electronic certification. Building of a combined and safe certification system upon recent FinTech boom is a very important factor and this study is going to suggest various structures in aspects of security and convenience.

Keyword: *Certificate, ISP, Authentication, Mobile, Payment*

1. Introduction

Recently, the mobile field has drawn much attention and is used for most means of living for users, like purchasing commodities, payment, and user certification. Mobile economy also grows by this trend, but hacking accidents or financial crimes are also in full swing. It is expected that the service for mobile in the future will increase more than ever, but in security aspects we still use problematic certification and security system. Mobile service market, as in Figure 1, has been expected to reach estimates of 750 billion won in 2015 in data control service business, e-notarization business and e-Banking business.

[4*] Corresponding author. Tel. : +82-10-9027-3148.
Email address: kjb123@ssu.ac.kr (Jong-Bae Kim).

ISSN: 1738-9976 IJSIA

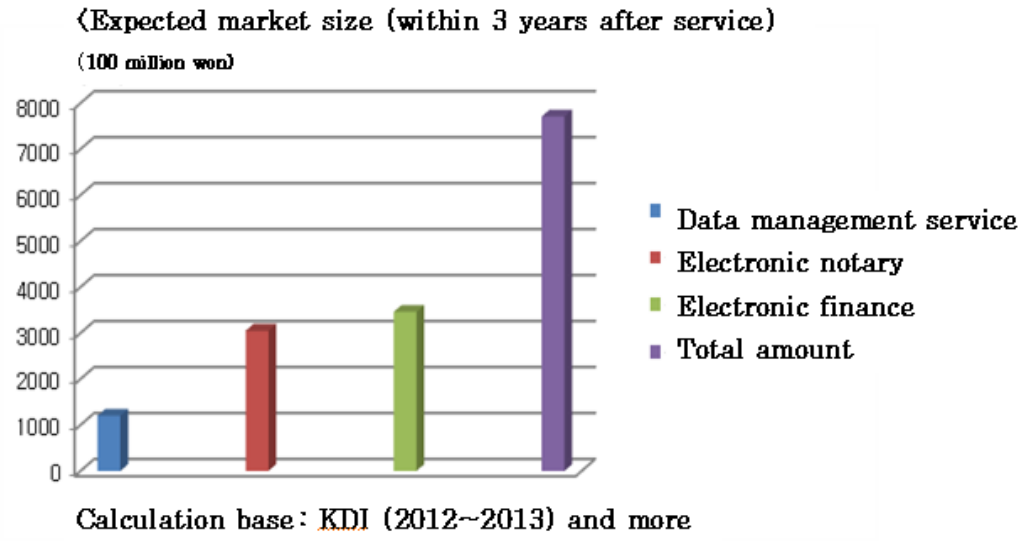

Figure 1. Predict Market Sizing of Mobile Service

Data control service in the future is expected to do a lot with the service which basically stores all services, based on cloud service, in phones as well as service providers. Data control service will lead to the expansion of IoT (Internet of Things) service, as it substitutes existing off-line backup and safely provides user data regardless of location or kinds of devices. That is, users can use data from the devices connected to the Internet without copying or moving to devices users want to use. To use this data safely, establishing a certification system of users will be an ever more important factor. Therefore, e-notarization for electronic data will be also revitalized. As in Figure 2, the size of the Internet shopping market is expected to be over 5 trillion won, according to the survey of KOLSA (Korea On-line Shopping Association) in 2015, and this is an about 12% increase compared with 2014, and with the uptrend of mobile sectors more noticeable [1].

With the emergence of companies in which this mobile gravity occupies over 70% of entire Internet shopping, the mobile market is expected to increase further. However, the measure for mobile security being used now is still not current or up to date, which appears as the biggest threat to mobile security and the mobile economy ecosystem [2].

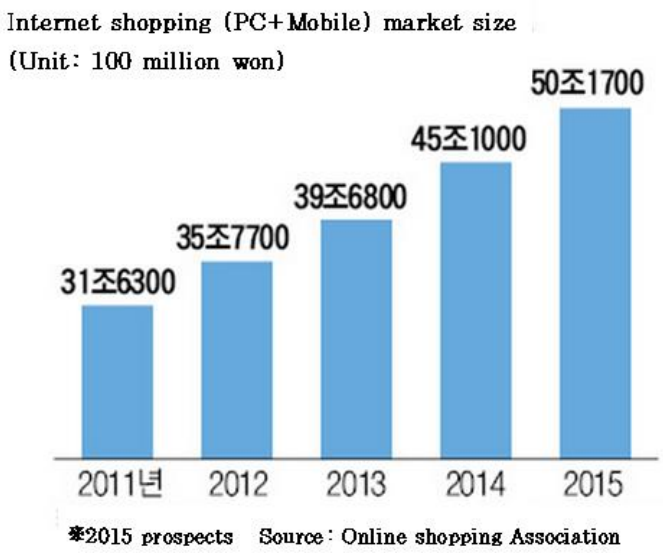

Figure 2. Market Sizing of Internet Shopping

Therefore, this study is going to suggest a plan that we can conduct in a safer way against several threats to mobile, especially for the certification sector. Mobile hacking is a very serious and important issue, as it could directly lead to monetary loss. In particular, when certification is insufficient, the possibility of a third party reaping benefits through hacking is greater. This study is going to suggest a model that service providers can use to provide safe certification service by performing verification of transaction and data through electronic certification.

2. Related Works

2.1 Certificate Verification and Active-X

Certificate verification is a kind of certificate of seal impression for cyber trade, where electronic information is issued by licensed certificate authorities in order to check identity in e-commerce, and prevent forgery and alteration of document and denying of transactions fact. Hacking incidents that snatch certificate verification is being increased now after decades since the introduction of certificate verification, reaching 15,386 cases in 2014. According to 'destruction status due to leakage of certificate verification in each bank' submitted by Financial Supervisory Service to Assemblyman Kim Taewhan (Gumi Eul) in Saenuri Party on the 16th, the cases destroyed by leakage of certificate verification rapidly increased to 5871 cases in 2013 from 15 cases in 2011, and 8 cases in 2012, and also this year 15,376 cases occurred until the end of August. Nonghyup had the biggest with 3946 cases, followed by Kookmin Bank (3365 cases) and Shinhan Bank (2089 cases). Nonghyup (1540 cases), Kookmin (1423 cases) and Shinhan (739 cases) also had the biggest certificate verification leakage cases last year [7].

Active-X is a technology developed by MS so that Windows users can use the document written by existing application program as it is with internet access. For instance, internet banking is available only on PC on which financial transaction and security program are installed, and Active-X is a means to distribute this program. In many cases, normal internet service is difficult with other web browsers like Firefox, as majority of domestic internet sites are based on Active-X of IE, and the government abolished this Active-X in March 2015 because many targets of hacking occurred due to Active-X. Another criticism of Active-X is that it made a loophole in security. For example, when receiving an Active-X based program needed for playing a video file in a site, this file could be used for hacking after it is automatically installed on PC without deletion [12]. A representing damage case is the 7.7 DDOS case which made a noise in the entire country in 2009. At that time Active-X was pointed out as it was misused in making zombie PCs which simultaneously attacked Blue House and others [8].

2.2 Smart OTP (One Time Password)

OTP, a certification method based on ownership, has a very strong safety feature as it creates a password through its only OTP token. However, purchasing OTP tokens, registering it to the bank in person, and always carrying it for use can cause inconvenience for users in using OTP.

Smart OTP means creation of one time password in software without OTP tokens to overcome this problem and raise user efficiency, and it is classified as knowledge-based certification as one time password is created based on confidential information, which is basically shared between user and computer [15].

2.3 KakaoPay

This is a service where we can simply make payments using only a password entry when purchasing goods when shopping on the Internet. This is done after registering your

credit card information on application (App application program). Using the mobile payment solution of LG CNS, Kakao started its service in September of 2014. To use KakaoPay, we should execute KakaoTalk and register credit card information in the menu of 'More view->Setup->KakaoPay' along with authentication and setup password. We can register up to 20 credit cards. We can use the service immediately after registering BC Card (Woori/IBK/Standard Chartered/Daegu/Busan/Kyongnam) and BC affiliated card (Suhyup/Gwangju/Jeonbuk/Jeju/MG/e-Postbank/Shinhyup/Hyundai Securities/KDB/Savings Bank/China Bank) [13]. Though Hyundai Card, Lotte Card is going to start the service after building the system; it is a little inconvenient that Shinhan/KB Kookmin/HanaSK/Samsung/NH Nonghyup/City Card do not participate in KakaoPay this time, and this service requires certificate verification when paying more than 300,000 won. Kakao and LG CNS are going to build a system that do not need certificate verification when making payments of more than 300,000 won with update to a new version until the end of 2014 [11].

2.4 FinTech

A new type of financial technology based on information technology (IT), such as mobile payment, remittance, personal assets management, cloud funding, as a compound of financial, meaning finance, and technique. The standard classifying FinTech business model and business area is largely being arranged to 4 areas of Banking & Data Analytics, Payment, Capital Market Tech, and Finance Management. The appearance of FinTech destroys existing financial order and pours up business models based on creation and innovation. Because the technologies, which held more simple and security issues, breaking existing barriers like kinds of currency, and payment system, are appearing one after another. And recently, the appearance of an algorithm which correctly grasps not only simple payment or remittance service but also clients' personal information/credit rating/financial accident through big data analysis is expanding its area up to personal assets management service [9].

3. Service Architecture for Secure Authentication System

This study is going to suggest a combined certification service in order to solve certification issues upon current abolition of certificate verification. This study judges that this service will become the foundation for standardized and safe certification systems in the future. More than anything, as it is expected that future certification systems will be focused on non-facing service, it should be a creative and efficient system with safety, openness, and standard form.

3.1 System Concept

As a concept of combined certification suggested by this study, this study suggests as in Figure 3, and aims at providing general use combined certification service like identification, assess certification, and transaction certification.

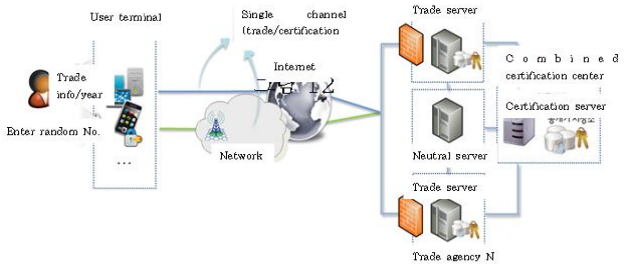

Figure 3. Total Authentication System Diagram

Combined certification means a type in which individuals receive certification through online or offline, or a 3rd certification provider acts for certification for transaction. Problems have occurred in the past, which had to confirm the person himself in case of hacking, as the person himself in person performed certification. Also in the case of existing 2 channel certification, the current situation is that problems still exist with indirect methods like using reproduced instrument. In order to solve this, this study is going to suggest a more perfect type of certification by making use of existing certificate verification and removing indirect method.

3.2 System Configuration

Figure 4 shows the system flow of combined certification suggested by this study. Users who will have identification or transactions through the Internet can do as such safely by submitting certification for transaction to the trade institution through a certification device. The concept suggested by this study is different in that users receive certification in real time through outside institutions at the point of transaction, unlike existing public certification types. Though users just enter arbitrary value for transaction, this part is technically available for automation without limit. That is, it is available when using Smart Watch or wearable devices which will be introduced in the future, and automation is possible when adding auto recognition function on current Smart Phone. That is, when using the device, owned by both Smart Phone and user, for certification with mutual recognition, reproduction or hacking is impossible.

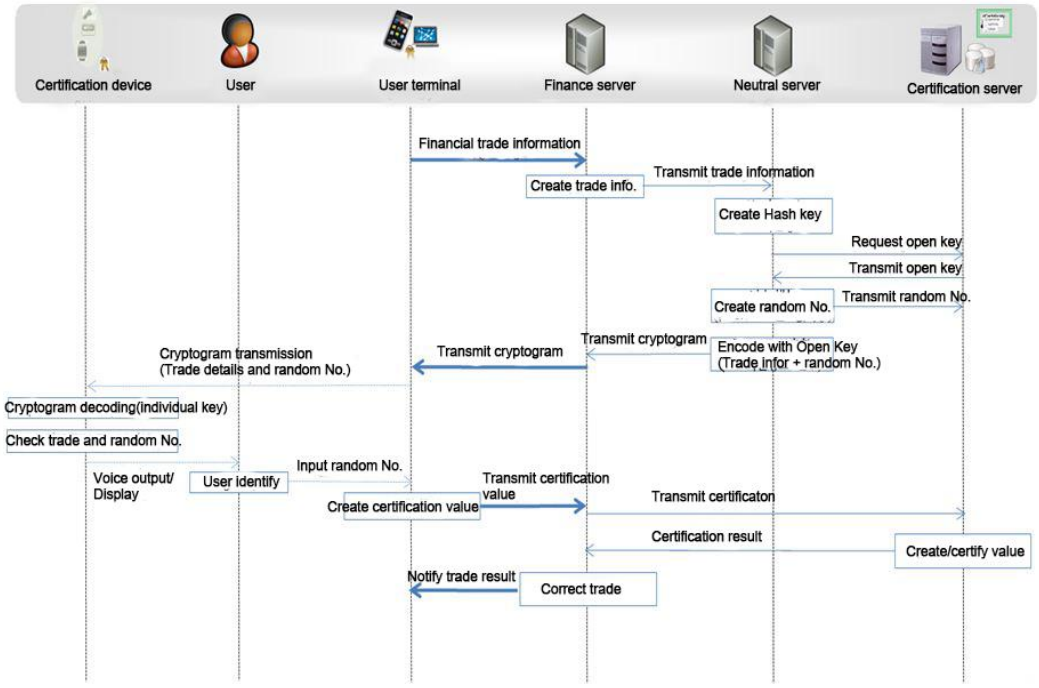

Figure 4. System Flow

As most of the latest smart devices support Bluetooth or NFC (Near Field Communication), we can create certification values impossible for reproduction based on certification with such devices. Recently, certification for NFC draws attention with interest in Fin Tech [10]. However, the type that individuals use to get random numbers through a medium unavailable for reproduction for transaction devices has never been introduced, so it is necessary to review more in aspect of using certification device. However, as mentioned earlier, the function of producing random numbers would not be so difficult as most of future devices uphold Smart.

3.3 System Profile

This study is going to suggest in-depth design for the system suggested by this study. First, this study is going to define the function for each subject and object and suggest a certification flow for each object. Table 1 specifies the function of the user's terminal and certification device, and table 2 shows the function of transaction server, neutral server, and certification server.

Table 1. Subject Function List

Certification device	User terminal
Individual key and decoding	Load certification program
Save algorithm	Cryptogram receipt
Cryptogram receipt	Cryptogram decryption
Cryptogram decoding	Random No. receipt
Transaction ID	Certification value creation
Random No. delivery	Certification value transmission

Table 2. Object Function List

Transaction server	Neutral server	Certification server
Transmit after creation transaction ID	Transaction ID receipt	Open key transmission
Cryptogram receipt	Create hash value	Random No. receipt
Cryptogram transmission	Request/receipt open key	Certification value receipt
Certification value receipt	Random No. creation	Certification value creation
Certification value transmission	Random No. transmission	Certification result transmission
Certification result receipt	Open key encoding	
Transaction result notice	Cryptogram transmission	Open key control

Neutral server is introduced to perfectly exclude availability of hacking and to make transparent transactions, where transaction server and certification server are directly connected. It is delivered to transaction servers after receiving certification value through above course. Transaction servers create random numbers for transaction from a neutral server and delivers this again to the user and checks possession of individual key. After this, it performs transactions based on certification values created at user's certification device.

3.4 System Design

This study is going to suggest an in-depth design for the system described in this study. First, this study is going to define the function for each subject and object and suggest a certification flow for each object. Table 1 specifies the function of the user's terminal and certification device, and table 2 shows the function of transaction server, neutral server, and certification server.

3.4.1 System Design: First, the authentication device performs functions such as existing OTP, but the biggest difference from existing OTP is that the user enters the random number after checking the random number received and recreating it for transaction. This time the method of user's input is not to use a simple keypad, but to enter thorough biometrics unavailable for hacking such as voice input. Like this, the most important factor of combined certification system is the one in types where certification information for transaction comes down via server and user certifies this via external terminal; the biggest character is that it is safe from hacking in system or terminal.

Table. 3. Detail Interaction Function List

Certification device	User	User terminal	Financial transaction server	Neutral server	Certification server
Individual key and decryption	Creation of certification information	Certification program load	Transaction ID cryptogram	Transaction ID information Hash creation	Public key receipt
Algorithm save	Random number receipt	Cryptogram receipt	Cryptogram receipt	Public key request	Public key transmission
Cryptogram receipt	Random No. check	Cryptogram delivery	Cryptogram delivery	Public key receipt	Random No. receipt
Cryptogram decryption	Random No. input	Random number receipt	Random number receipt	Random No. creation	Certification value receipt
Transaction ID information	Transaction check	Certification value creation	Certification value receipt	Open key encryption	Certification value creation
Random number delivery	Final check	Certification value transmission	Certification value transmission	Cryptogram transmission	Certification

Neutral server is introduced to perfectly exclude availability of hacking and to make transparent transaction, where transaction servers and certification servers are directly connected. It is delivered to a transaction server after receiving certification value through the above course. Transaction server creates random numbers for transaction from neutral server and deliver this again to the user and check possession of individual key. After this, it performs transactions based on certification value created at user's certification device.

3.4.2 System Expansion Design

In case of operating payments via this combined certification system, the plan is to prevent the damage at the source by hacking on the terminal such as malignant codes, as it receives the random number value through external authentication devices. Therefore,

also in case of using other external terminals other than simply trading via terminal, we can use a combined certification service suggested by this study.

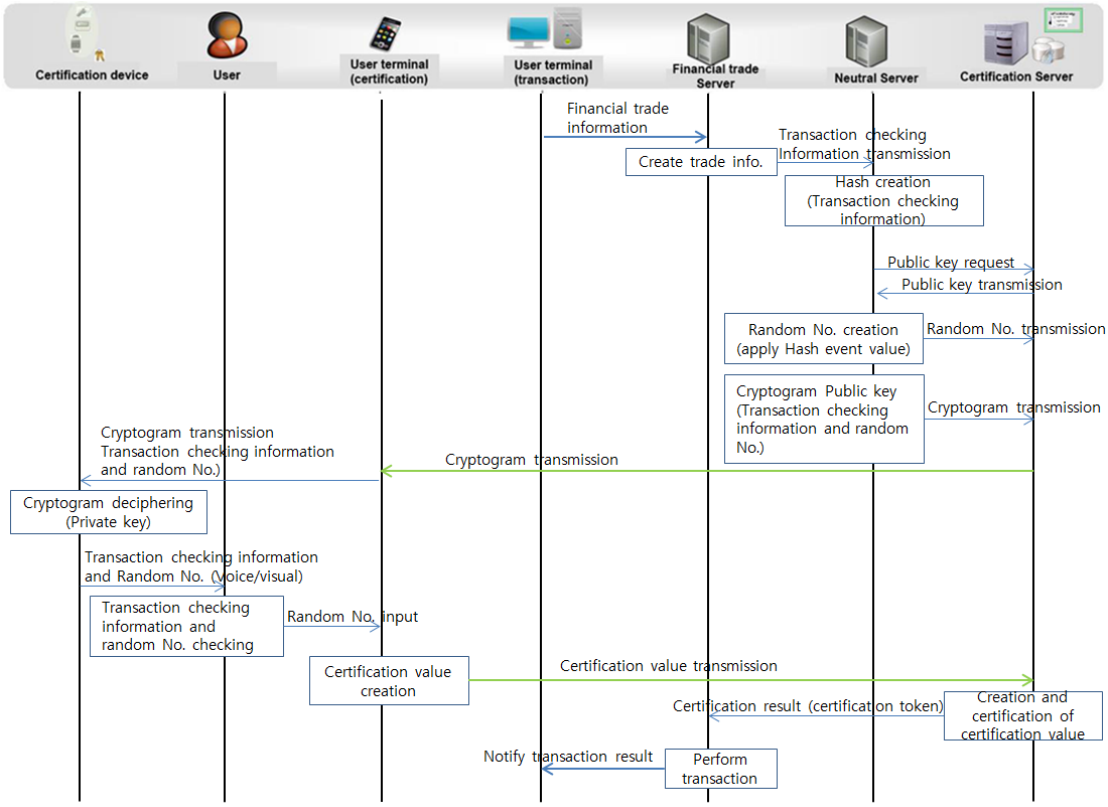

Figure 5. Transaction Using Authentication Device

As in Figure 5, in the case of operating the service from user terminal, we can get the same security effect when passing the request for certification after passing through transaction server, neutral server, and certification server via existing external certification device. Currently, we can compare ISP service with the service which uses types like this. In case of using ISP service, if you choose cellular phones as authentication, it will be operating in the type of inputting authentication numbers via apps installed on cellular phones and performing additional certification via password; however, the disadvantage is if a malignant code is installed on user's cellular phone, the activities after this could be manipulated. Therefore, when using a combined certification service which uses the authentication device suggested by this study, a perfect security service can be performed.

3.4.3 Certification Detailed Design: This paragraph suggests a detailed content for major certification parts suggested by this study. This time, authentication device has a premise of having saved the content inside as follows.

- Available for data transmission through the terminal and communication such as mobile
- Save user' s private key
- Random No. check function
- Random No. input function
- Specific character string input-output function

Certification devices basically can perform the above functions and perform roles of checking or acting for certification according to acts of users, or checking or creating specific texts. The benefit of having a separate authentication device like this is because we can perfectly respond to security if we check certification value through separate medium unavailable for this hacking and make required data for certification as hacking is available for existing terminals using malignant code.

- Transaction checking information: HASH = prf (financial transaction information)
- User public key: Upub_k
- User private key: Upri_k
- Cryptogram transmission: prf (Upub_k, transaction checking information + Ni)
- Deciphering: prf (Upri_k, cryptogram transmission)
- Certification value: HASH = prf (Ni)
- Certification token: prf (Upub_k, certification value + Ni)

Through above certification protocols, we can perform safe payment service via transaction checking and certification procedures between certification server, user, and certification device. But, in the case of Figure 6, the structure is designed in a way in which one must have a certification device, being realized into combined type two channels, and it is shown in Figure 6 that the design was more effective and more convenient for users, as recently the feeling of denial is overflowing against this external device.

In addition, when operating comparative evaluation for the convenience and security of this suggestion, it has shown that it scored an absolutely higher grade than other plans. As in Figure 7, it received a higher evaluation in total score than certification plans that used virtual machine or USIM.

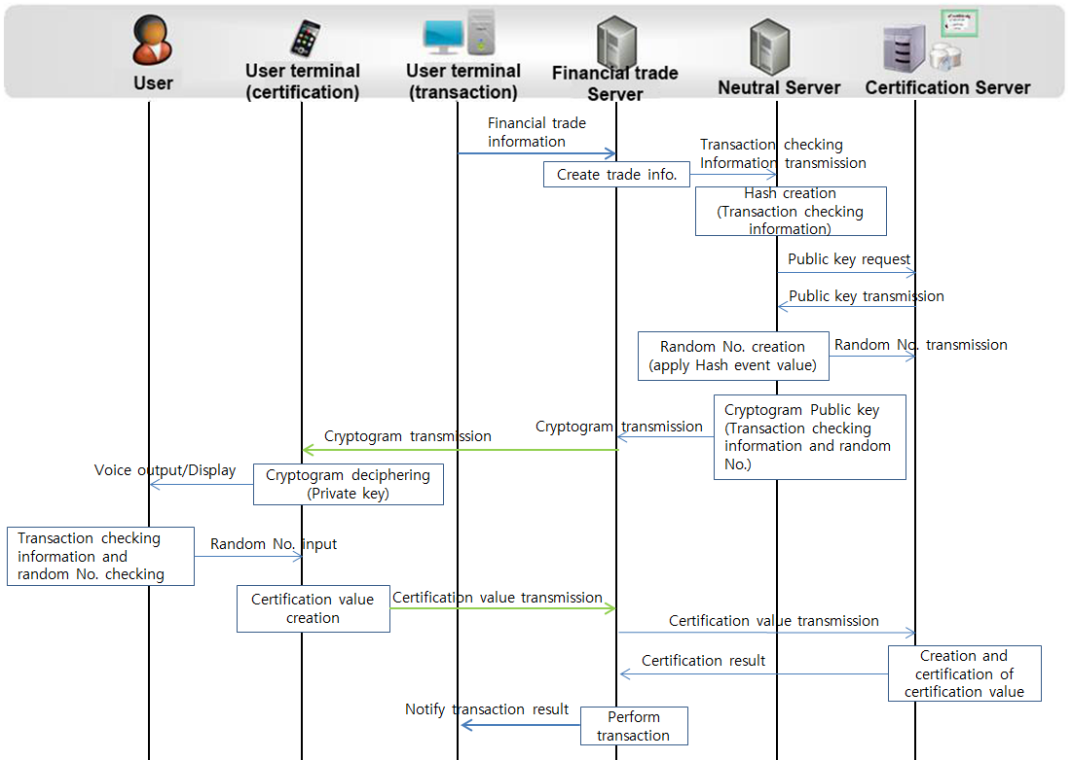

Figure 6. User Terminal Certification Model not using Certification Device

Review method	Details	Weighted value	Certification device		VM		USIM	
			Evaluation	Score	Evaluation	Score	Evaluation	Score
Possession convenience	Portableness/possession availability of certification medium	High(3)	Insufficient	3	Excellent	3	Excellent	3
Response to off-line attack	Available for phishing, pharming	High(3)	Excellent	3	Excellent	3	Excellent	3
Response to on-line attack	Available for MITM	High(3)	Excellent	3	Excellent	3	Excellent	3
Response to transaction manipulation	Available for MITB, memory manipulation attack	High(3)	Excellent	3	Normal	2	Insufficient	1
Evaluation		36	36		33		30	
		100	100		91.7		83.3	

Figure 7. Comparison of Security with Other certification Medium

However, in the aspect of convenience, as in Figure 8, the convenience score was measured lower than other methods due to the problem that we would need to carry a certification device. Like this, it can be very effective if users select the plan to put more weighted value on the aspect of security or convenience.

Review method	Details	Weighted value	Certification device		VM		USIM	
			Evaluation	Score	Evaluation	Score	Evaluation	Score
Response to existing hacking attack	Available for traditional hacking skill	High(3)	Insufficient	1	Excellent	3	Excellent	3
Use convenience	Intuitiveness of use and input	Normal(2)	Normal	2	Excellent	3	Excellent	3
Management convenience	Response availability to stealing/exposure	Normal(2)	Excellent	3	Normal	2	Normal	3
Issuance convenience	Convenience of issuing/registry/replacement	Low(2)	Insufficient	1	Insufficient	1	Excellent	3
Education convenience	Probability of accidents upon insufficient education	Low(1)	Excellent	3	Excellent	3	Excellent	3
Evaluation		30	18		24		28	
		100	**60.0**		**80.0**		**93.3**	

Figure 8. Convenience Comparison with Other Certification Medium

4. Conclusions

Combined certification suggested by this study solved problems of certificate verification types as well as security and convenience by suggesting additional certification devices. It is expected that future certification devices will expand further. With the abolition of certificate verification systems, employers or institutions who provide transaction services should prepare a separate certification type. It is judged that if we perform combined certification service by providing certification devices that user can conveniently own, non-facing services can also perform as much as facing services. However, we should prepare a plan that can make a more convenient initial registry procedure to save open keys in certification server.

References

[1] http://www.hankyung.com/news/app/newsview.php?aid=2015010549971&intype=1
[2] http://www.mt.co.kr/view/mtview.php?type=1&no=2015040214203877091&outlink=1
[3] http://news1.kr/articles/?1906344
[4] http://opennet.or.kr/e-finance-e-signature-reform.pdf
[5] http://biz.chosun.com/site/data/html_dir/2015/04/20/2015042003040.html
[6] http://www.datanet.co.kr/news/articleView.html?idxno=81727
[7] http://www.dt.co.kr/contents.html?article_no=2015041402100351800001
[8] http://www.hidomin.com/news/articleView.html?idxno=249918
[9] http://www.hidomin.com/news/articleView.html?idxno=249918
[10] http://view.asiae.co.kr/news/view.htm?idxno=2015032509531946839
[11] http://terms.naver.com/entry.nhn?docId=2118001&cid=42107&categoryId=42107
[12] http://www.ittoday.co.kr/news/articleView.html?idxno=59377
[13] http://terms.naver.com/entry.nhn?docId=2166759&cid=42107&categoryId=42107
[14] J.-K. Park and S.-Y. Choi, "Studying Security Weaknesses of Android System", International Journal of Security and Its Applications, vol. 9, no. 3, **(2015).**
[15] J.-K. Park, "A Realtime Malware Detection Technique Using Multiple Filter", Journal of The Korea Society of Computer and Information, vol. 19, no. 7, **(2014)**.
[16] H.-N. Kim, "Realtime hybrid analysis based on multiple profile for prevention of malware", Hongik Univ., **(2014).**
[17] S. Yoo, J. Yu, H. Jang and J. Ryou, "A Study on OTP Generation Method based on Software", Journal of the HCI Society of Korea, HCI 2011, vol. 1, **(2011).**

Authors

Sung Jin Kim, Currently, in a doctoral course in Soongsil University IT Policy Department, graduated from the Security department of Information Science graduate school in Soongsil University and lives in Seoul, Korea. He is the representative director of ITNOMADS Co., Ltd. and has worked as an expert in IT field for 27 years. Fields of interest: Network security, database security, next generation network security as IoT information security field.

Myung Chul Ma, Currently, in a doctoral course of IT Policy Department in Soongsil University, graduated from information communication department of industrial graduate school in Soongsil University and lives in Seoul. He is the representative director of POSOD Co., Ltd. and has worked as an IT expert in IT industry development for about 30 years. Fields of interest: CCTV-based Image information system and IoT equipment development.

Hyeon-Kyung Lee, she received her bachelor's degree of Computer Information in Baewha Women's University, Seoul(2015). She is studying her master's degree of software engineering in Graduated Soongsil University, Seoul. Her current research interests include software engineering and open source software.

Jong-Bae Kim, he received his bachelor's degree of Business Administration in University of Seoul, Seoul (1995) and master's degree (2002) and doctor's degree of Computer Science in Soongsil University, Seoul (2006). Now he is a professor in the Graduate School of Software, Soongsil University, Seoul, Korea. His research interests focus on Software Engineering, and Open Source Software.