A Study on Secure Authentication System using Integrated User Authentication Service

Jae-Kyung Park¹, Hyung-Soo Lee², Sung-Jin Kim³ and Jae-Pyo Park⁴*

¹Department of Cyber Security Research Center, KAIST, Daejeon - 34141, Korea
²Department of Computer, Soongsil University, Seoul - 156-743, Korea
³Department of IT Policy and Managements, Soongsil University, Seoul - 156-743, Korea
⁴Department of Information Security, Soongsil University, Seoul - 156-743, Korea; pjerry@ssu.ac.kr

Abstract
Recently, Certificate has been loosed growth 100 times in a four years as Phishing or hacking. The service that uses a certificate in financial services occur practical and secure issues. Therefore, the Korea government abolished the mandatory system used in the certificate service. However, they did not provide a replacing method for a certificate. And it is not to fill the gaps of the certificate with OTP (One Time Password) or secure card. Therefore, this paper is proposed the alternative method with total authentication service, which is lead the more secure electronic commercial. This total authentication service can be used to verify personal identity and transaction services.

Keywords: Authentication Method, Certificate, Electronic Commerce, Internet Banking, Total Authentication

1. Introduction
Recently, the large scale of personal information leakages occurs frequently and this result in high level of anxiety in regards to personal information and electronic commerce. Additionally, bank certificates that leaked through phishing or hacking grew 100 times over in 4 years¹. Also, it is time adapt new and practical techniques and systems that are intuitive certification services that reduce anxiety levels. In 2014, Electronic Financial Transaction Act and Digital Signature Act were amended, substantiation of accidents in regards to hacking vest in financial companies and forcible e-commerce articles using Certificate were deleted². However, there has no other form to replace Certificate; it is time urgent issue to come up with alternative means. Standard OTP (One Time Password) and Smart OTP, enhanced methods widely applied, also turned out to be insufficient from security safety perspectives³. OTP roles merely as a back-up device, key passwords need to be input during actual electronic finance business and this remains as the biggest issue.

As hacking technique gets intellectualized, damages from electronic finance business and electronic commerce are expected to grow significantly; illegal transaction cases and amounts are also expected to rise. In order to remedy these cases, dual channel certification such as ARS or SMS certifications are applied; still there are cases with hacking using fake phones⁴.

The use of QR code, primarily used as marketing tool, is getting broader to verify document authenticity and certification means. However, QR code itself has a high possibility of forged, and authenticity cannot legally guaranteed; people point out its careful use. Fraud cases that forged and falsified QR codes occurred but impossible for ordinary people to verify. With the simple program being available, anyone can forge and falsify easily⁵.

In this paper, a total authentication that replaces certificate and exceeds the security level of current security system is suggested. As Figure 2 indicates, preemptive and open type standards of total authentication offer in consideration of vitalizations of non-face-to-face services. Future non-face-to-face service security gets

*Author for correspondence
2. Related Research

2.1 Certificate and Active-X

The certificate is one of the cyber transaction certificates of one's seal impression that is issued by public certification institute to verify identity during e-commerce, prevent document forge, falsification and transaction factual denial. Hacking instances by extorting certificates are increasing; 15,376 cases in 2014. According to the paper that was written to Kim, Tae-Hwan, cases of the certificate discard occurred 15 times in 2011, 8 times in 2012, and rapidly increased to 5,871 times in 2013, and already occurred 15,376 cases until August. Nong-up bank had the most incidents with 3,946 cases, KB (3,365 cases) and Shinhan (2,089 cases) followed after Nong-up. These three financial firms had the most leakages of Certificates with 1,540 cases, 1,423 cases and 739 cases, respectively in last year7.

Active-X is the technique that MS Windows users can directly connect to the internet using existing application programs. For instance, PCs that are installed with financial trade and security programs when one does e-banking, Active-X is the tool to spread this type of programs. The majority of local Internet sites are built up with IE's Active-X and other web browsers including Firefox does not allow normal Internet services; hacking through Active-X occurred frequently. Due to these reasons, Korean government discarded Active-X in March 2015. Another controversy of Active-X is that it exposed its weakness in the security field. So to speak, when one Internet site requires Active-X based programs to play videos, one needs to download this Active-X based programs. Upon its download, PC will automatically install and will be misused by hacking without deletion. Key damage cases were 7.7 DDOS incident that caused uproar the country in 2009. At that time, Active-X was pointed out with misuse since the Blue House and other agencies were attacked simultaneously by making them zombie PCs7. There had been many pieces of research to block hacking through Active-X, and it is essential to introduce essential solutions over malignant code8,9. Since the mobile environment is facing rapid growth, a system that considers both cable and mobile environments should be developed10.

2.2 FinTech

FinTech is a mixed word using financial and technique. FinTech is the new form of financial technique that stands on the basis of IT including mobile payment and wire transfer, personal asset management, cloud funding, etc. Criteria to categorize FinTech business models and business ranges are largely into four parts: Banking and Data Analytics, Payment, Capital Market Tech, and Finance Management. The introduction of FinTech destroyed existing financial order and generates creative and innovative business models. Existing barriers such as types of currency and payment systems fell apart, and much more simple techniques are introduced one after another. Recently, not only simple payment or wire transfer services but also algorithm techniques to accurately grasp with big-data analysis appear to personal asset management services8.

2.3 Smart OTP(One Time Password)

OTP, certification means based on ownership, is the most powerful security tool since it only generates one-time password to users who have OTP token. However, one needs to purchase OTP token, register directly at banks, always need to carry along to use it. This results inconveniences to people who use OTP.

Smart OTP is to generate one-time password using software methods to overcome OTP certification problems and increase user efficiencies. This Smart OTP is categorized as intelligence based certificate since its password gets generated through software11.

3. Total Authentication Services

This paper suggests total authentication services which resolve problems with certificate discards. This service will be the foundation for standardization and establishment of safe certification systems. Above all things, non-face-to-face certificate systems will be the main certificate system in future, creative and efficient system prepared with safety, openness and standardization.

3.1 System Concept

Figure 1 shows the concept of total authentication; and this universal system targets to provide identity confirmation, connection authorization, transaction authorization and others.
Total authentication is defined as 3rd certification organization certifies one with on-line and off-line personal identity certification and transactions. Previously, these certifications were directly done by a person oneself; hacking was easy as the recognition was difficult. Additionally, current 2-channel certifications also are open-ended issues since there are roundabout methods such as usage of duplicated devices. To resolve, a much more perfect form of the certification which strengthens pros of certificate and reduces roundabout methods will propose.

3.2 System Structure

Figure 2 presents system diagram of total authentication. The user who uses terminal for certifying personal identity or transactions receive goes through certification device to receive needed authenticator that can submit to transaction agencies for safe transactions. The proposed concept from this research is to allow the user to be certified in real-time by external agencies during transactions, unlike existing certificate methods. User needs to input manually user’s random value for transactions; this part can always automate with some additional technologies. Wearable devices and others can make this possible; if smartphones add with automatic awareness functions, automation is not that impossible. In order word, when smartphones and user's distinctly owned devices recognized correlations during certification process; duplicate or hacking will be impossible.

Since most of the smart devices support Bluetooth and NFC (Near Field Communication), generating authenticators that cannot duplicate on the basis of certification with devices. Recent interests in FinTech allowed many interests I NFC certification. This type of methods in transaction devices-person oneself owns and generates random numbers that cannot duplicate-has not introduced prior, more thorough review from certification device utilization perspectives are required. Previously indicated, future devices claim to be smart devices, functions to generate random numbers will not be that difficult. Next chapter will design suggested system from protocol level.

4. Design

This chapter will propose the detailed design of the suggested system. First, subject and object function lists are presented and subject authentication flow will suggest in that order. Table 1 indicates user's device and user possessed authentication device function lists; Table 2 indicates functions of transaction servers, neutral servers, and authentication servers.
The neutral server directly link to transaction server and authentication server; the possibility of hacking is introduced to fully eliminated while transact transparently.

Figure 3 presents authentication flow of user possessed devices and authentication devices. In this time, user’s terminal sends encoded information to authentication device first and then decode information to certify user.

Subject authentication flow from Figure 3 check authenticator to confirm data and a random number.

---

**Table 1.** Subject function list

<table>
<thead>
<tr>
<th>Authentication Device</th>
<th>User’s Terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Key and Decoding</td>
<td>Load authentication program</td>
</tr>
<tr>
<td>Saving Algorithm</td>
<td>Receive coded information</td>
</tr>
<tr>
<td>Receive coded information</td>
<td>Send coded information</td>
</tr>
<tr>
<td>Decode information</td>
<td>Receive random number</td>
</tr>
<tr>
<td>Transaction confirmation information</td>
<td>Generate authenticator</td>
</tr>
<tr>
<td>Send random number</td>
<td>Send authenticator</td>
</tr>
</tbody>
</table>

**Table 2.** Object function list

<table>
<thead>
<tr>
<th>Transaction Server</th>
<th>Neutral Server</th>
<th>Authenticator Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate and send transaction confirmation information</td>
<td>Receive transaction confirmation information</td>
<td>Send public key</td>
</tr>
<tr>
<td>Receive Authenticator</td>
<td>Generate Hash Value</td>
<td>Receive random number</td>
</tr>
<tr>
<td>Send coded information</td>
<td>Request and receive public key</td>
<td>Receive authenticator</td>
</tr>
<tr>
<td>Receive authenticator</td>
<td>Generate random number</td>
<td>Generate authenticator</td>
</tr>
<tr>
<td>Send authenticator</td>
<td>Send random number</td>
<td>Send certification result</td>
</tr>
<tr>
<td>Receive certification result</td>
<td>Encode public key</td>
<td></td>
</tr>
<tr>
<td>Notify certification result</td>
<td>Send coded information</td>
<td>Managing public key</td>
</tr>
</tbody>
</table>

---

**Figure 3.** Subject authentication flow.
• Data and Random number acknowledgement: Public-key(Data+Rand)⇒Private-key(Public-key (Data+Rand)).
• User check can be done biometrics such as voice or face recognitions to strengthen security level.
• Prior to the transaction, user sends public key that one will use during a transaction to the authentication server for future usages.

Through above mentioned procedure, user’s authenticator gets sent to the transaction server. Transaction server generates a random number for transactions at Neutral server; this gets sent to the user to check whether the user has a personal key or not. Then, based on authenticator that generated by user’s authenticated device allow transactions to perform.

Total authentication service that proposed in this research allow existing public key to use during authentication process; pros and benefits of the certificate will remain as is. Additionally, security issues such as hacking or duplicating can resolve by utilize user possessed authentication devices. By making authentication server being real-time, methods to maintain the role of certificate agency’s roles. If one uses this proposed service, its benefit is to pursue open type authentication service without any service limit.

As Figure 4, the user uses user terminal to do financial transaction services; transaction confirmation information will receive from a certificate server. The received certificate information encode with user's public key; the personal key can decode this information to allow user certificate. After then, proposed in Figure 5, the user uses certificate device to generate authenticator and send this information to certificate server in receiving approval by executing transactions. By using public key methods rather than existing certificate methods, high-security proportion gets maintained while users experience easy approval for transactions. Therefore,

![Figure 4. Object authentication flow.](image-url)

services free from essential hacking or duplicate can be provided.

5. Conclusion

Total authentication suggested in this research resolves existing certificate problems and presents additional certification devices for security and convenience. Future certificate device market is expected to grow. With the discard of certificate systems, business operators and agencies that provide transaction services need to prepare separate certification methods. If certificate device that can simply own by the user being distributed to perform total authentication, it is no doubt that certification during non-face-to-face services will also provide similar level with face-to-face services. One thing, much simple way for initial set-up procedure of saving public key to certification server needs to study further. This total authentication service can also use to verify personal identity other than transaction services. If total authentication be used during identity card forge, this service can also be used as e-identity card systems-this will be the most significant benefit of total authentication.

6. Acknowledgement

This work was supported by the ICT R&D program of MSIP/IITP [R0112-14-1061, the analysis technology of a vulnerability on an open-source software and the development of platform].

7. References