International Journal of Security and Its Applications
Vol. 9, No. 3 (2015), pp. 77-84
http://dx.doi.org/10.14257/ijsia.2015.9.3.08

A study of issues about Accredited Certification methods in Korea

Seung-Woan Chai*, Kyoung-Sik Min** and Jeong-Hyun Lee***

Korea Internet & Security Agency (,**,***)*
chaisw@kisa.or.kr, kyoungsik@kisa.or.kr, hyunlee@kisa.or.kr (Corresponding author)

Abstract

In line with the e-Government strategy, Korea has implemented a global standard electronic signature and certification system since the Electronic Signature Act was enacted by Act No. 5792 in 1999. Over a decade Korea has been using the electronic signature and certification system in daily life. In the cyberspace where the contracting parties cannot meet face to face, electronic signatures and authentication are inevitable. On the other hand, with the explosive use of smart devices, some critics argue that the current certified electronic signature is regarded as uncomfortable system in electronic commerce. They also point out that such certified electronic signature system is not commonly used in foreign countries. Yet, so far, the accredited certificate is still the most reliable method even though the usage of accredited certificates presumably decreases in the areas that do not require security significantly. Thus, it must be unwise to discard the accredited electronic signature on account of an "unnecessary obstacle". Therefore, legal and technical issues regarding the accredited certificate need to be discussed. Additionally, methods to promote certified electronic signature and to improve certification system should be explored.

1. Background for Debate on the Accredited Certification System

The Korean Financial Services Commission revised the detailed regulations on Supervision of Electronic Finance in May 2014 and abolished the mandatory use of the accredited certificate in e-commerce. As issues related to the accredited certificate were pointed out in the regulatory reform meeting held jointly by the public and private sectors and presided over by the President, the mandatory usage system of the accredited certificate in e-commerce has finally become history.

Ahead of that, the presidential candidate promised in the electoral commitment to permit various types of accredited certificate services that meet global standards as a part of creating a sound and sustainable ICT ecosystem. As a result, requests for usage bases of various types of certification tools that are used internationally other than the current accredited certificate are occurring under the current government.

The situation was initiated as some civic groups requested the disuse of the mandatory accredited certificate as well as the permission of using various types of certification tools such as the OTP (one time password). It was pointed out that there are issues in the ActiveX-type service realization which enables the usage of the accredited certificate as well as safety issues of the accredited certificate now that smart phones are being used nationwide and e-commerce or electronic money transfers have become a part of everyday life. These discussions are being expanded to the extent of abolishment of the accredited certificate system and diversification of certification tools.

The focal point of the discussion is about the 'mandatory usage of the accredited certificate'. Conflicts collide between the government which claims that the mandatory usage of the

ISSN: 1738-9976 IJSIA

accredited certificate is essential for identification in cyber space and to secure safety and credibility of electronic documents, and social requests which claim that e-commerce services are restricted due to the excessive usage of ActiveX and mandatory usage of the accredited certificate, making it more inconvenient for the consumers. It has now become an urgent matter to prepare measures to improve the current accredited certificate system as claims are being raised that not only by PC users but also smart phone users who are experiencing inconvenience and that the usage of the accredited certificate is only mandatory in Korea, which does not go in line with international standards as well as with the 'creative economy' set up as a national agenda of the current government because it has become a hurdle in boosting the industry.

This document aims to examine accredited certificate issues that are currently being raised in Korea and also briefly discuss about improvement measures.

2. Concept and Current Status of the Accredited Certification System

Since electronic transactions using electronic documents are performed via non-contact and non-face-to-face, it is difficult to check the identification of the counterpart and the genuineness of the transaction intent, as well as there are risks of misuse of e-documents by committing fraud. Not only is it easy to fake or falsify e-documents in the distribution process and difficult to prove the fact of having drawn up the document, but it is also difficult to maintain secrecy of the transferred contents. To solve such issues inherent in e-document and e-transactions, a new type of signature means is required that can be applied in e-documents and can secure identification and integrity of the writer of the electronic message.

In this context, the 'digital signature' using encryption technology was developed, which is an electronic replacement of the manual signature. In other words, it is information created by the computer instead of using the pen and provides the same functions and even more than a manual signature.

Digital signature is a technology developed to prevent the disguising of identification, counterfeiting of transactions and denial of transaction, which serves the same role as signatures (seal) used on paper documents and is information included or attached to the concerned e-document with the purpose to secure the identification of the writer of the e-document and to prevent changes of the e-document. With Korea securing legal proving power of the digital signature through the Digital Signature Act of 1999, the Digital Signature Act provides the base to vitalize the usage of e-documents and accelerate information distribution of the nation, secures safety and credibility of the e-document and also defines the basic matters on digital signature to vitalize its usage.

‘Accredited digital signature’ is a digital signature that distinguishes the user who has done the digital signature and publicly guarantees that the e-document with a digital signature has not been forged or falsified by providing accredited certification to the digital signature.

‘Accredited certificate’ is an electronic type of certificate issued by a certification authority to identify the owner of the digital signature. If the traditional way was to meet face-to-face in the same place for identification, the accredited certificate enables people to identify each other through credible information without having to see each other face-to-face via cyber space. Moreover, since the accredited certificate is directly related to the protection of the property rights of the public, strict identification of the applicant is required by meeting face-to-face when issuing a certificate.

Accredited certificates that are required for digital signatures are issued by accredited certification authorities appointed by the Korean government.

As of end of December 2013, the number of issued accredited certificates totals 30 million,

which accounts for 116% of the economically active population (25.87 million) within Korea. According to the UNCITRAL Model Law on Electronic signatures of 2001 proposed by the United Nations Commission on International Trade, countries are operating Electronic signature laws respectively. In Korea, although it is a limited use certificate, the range of its application covers various fields such as banking/securities/card/insurance/civil service etc. meaning a single certificate can be used in internet banking, internet shopping, online insurance and online civil service, which is a completely different service from the 'one certificate one field' service of other countries.

3. Major Issues

3.1. Accredited Certificate and the Issue of ActiveX

ActiveX is a technology developed to extensively support functions that are not provided by Internet Explorer (IE), the web browser of MS, and was widely used by most internet operators when setting up a service web site due to the high market share(more than 99%) of IE.

The biggest advantage of ActiveX is that its functions can be expanded infinitely. Once ActiveX is installed, just by executing it on the PC enables easy interlocking of web sites and functions, making the process of controlling the functions of the user PC from the web site very simple, therefore service developers have voluntarily used it extensively.

Its weakness on the other hand is that it can only be run in IE and as for Google's Chrome, Apple's Safari and Mozilla's Firefox, ActiveX cannot be used at all in smart phones and tablet PCs if it's not a windows-based PC. There are also compatibility and security issues such as cases of implanting malicious codes or leakage of private information by misusing the characteristics of ActiveX that are directly installed in the user's PC.

However, since operators that provide internet banking services such as Korean banks set up systems based on IE, internet banking utilizing accredited certificate must install ActiveX and this has raised complaints by users of other web browsers who cannot install ActiveX. Also because ActiveX has weak security and needs to be continuously used due to its mandatory usage, some media and civic groups claimed that only the abolition of accredited certificate can lead to the disuse of ActiveX, considering that accredited certificate and ActiveX are the same.

The Financial Services Commission and Financial Supervisory Service made it mandatory to use the accredited certificate in all electronic financial transactions according to the rules, which secured safety and credibility of electronic transactions but also caused complaints by users of other web browsers and devices by providing internet banking and electronic financial transaction services based on IE users, linking it with the issue of ActiveX.

With the smart phone boom in Korea since 2009, the use of wireless internet using the smart phone increased but in the case of e-commerce in Korea, e-commerce services were limited due to the excessive use of ActiveX and mandatory use of the accredited certificate, resulting in increased requests of users related to e-commerce and financial services.

3.2. Leakage of Accredited Certificate

Currently in Korea, accredited certificates can be stored in the hard disk of the user's PC, which also makes it highly possible for the accredited certificate to be leaked in case the PC is hacked. Since the leakage cases by the accredited certificate from 2012, security weakness issues of the accredited certificates are on the increase. Accredited certificate has to be stored in the mobile devices such as smart phones or tablet PCs to do electronic transactions by

using the accredited certificate and requires special care of the user because the risk of leakage of the accredited certificate exists equally in the mobile environment since it is the same principle as storing the certificate on a PC's hard disk.

Until 2011, there were no cases of certificate leakage in Korea. But in 2013, the number of certificate leakage cases dramatically increased from eight cases in the previous year to 7,633 cases. Among those cases, 777 cases were leaked from PCs whereas 6,856 cases were leaked from smart phones.

The Bank of Korea explained that the sudden increase in the number of leakages is primarily due to advanced techniques of hackers extorting accredited certificates such as pharming and smishing, and especially the rapid increase of certificate leakage of smart phones is considered to be due to smishing.

3.3. Debate about the Disuse of the Accredited Certificate

Currently as the industry circle acknowledges that identification through the accredited certificate is the most reliable means among various types of identification in Korea, accredited certificates are being used in various fields for user identification such as joining membership or expense settlement after having provided service. However the mandatory usage of the accredited certificate for mere identification or formal actions is leading to the aversion of using non-accredited digital signatures, and comments are being raised that such will hinder the development of the security industry. In other countries, there is no separate installment of a security SW and various types of certification tools are being used by mainly using coded communication loaded in the web browser and OTP devices, and therefore it is becoming more convincing that the mandatory usage of a single accredited certificate which is the target of hacking, is unnecessary.

The Korean Financial Services Commission revised the Detailed regulations on Supervision of Electronic Finance in May 2014 and abolished the mandatory use of the accredited certificate from the previous regulation of having to use the accredited certificate in e-commerce such as internet shopping worth more than 300,000 KRW to not having to use the accredited certificate in e-commerce such as card payment of credit card or debit card. Currently an environment is being fostered where electronic transactions can take place through other certification methods and not necessarily through the accredited certificate.

4. Improvement Measures of the Accredited Certificate

4.1. Support with Safe Usage Policy of the Accredited Certificate

Foreign countries are experiencing direct financial damages due to malicious codes, whereas in Korea there are no direct financial damages yet but administrative issues such as leakage of the accredited certificate are being exposed. In this regard, it is necessary to promote utilization of the security USB instead of the USB and using a USB rather than a hard disk is better when storing on the PC. It is also necessary to upgrade the security level by utilizing the USIM of the mobile phone or smart phone as a security token and at the same time to enhance the usage convenience of the accredited certificate. It is necessary to set up a policy to expand the usage of security tokens by solving usage inconvenience and by minimizing cost burden through the usage of USIM and providing certification services through smart phones.

Also, security issues can arise in an environment where the accredited certificate is stored in the smart phone due to the increase in mobile banking, however leakage of the accredited certificates or abnormal usage of electronic transactions can be blocked by strengthening security through the USIM, storing the accredited certificate in the IC card or utilizing the

near field communication (NFC) function of smart phones.

But it is most import to provide policy support so that users use safe storage methods for the certificate and companies providing electronic transaction services voluntarily come up with new technologies.

One of the policies that can be suggested is to define the grades of electronic transactions by the size or amount of the transaction and differentiate the classification criteria of the liability for damages of the certificate according to the respective grades. It is also required to extend the expiration date of the accredited certificate with storage of medium to high security levels from the previous one year and to limit the usage range by level.

4.2. Create a Convenient Usage Environment for Accredited Certificate

One of the major reasons the discussions on abolishing the accredited certificate was brought up is because it is not user friendly. Accredited certificates in Korea have to be renewed every year and have to be registered in all institutions where electronic transactions are used such as banks. In the mobile environment, accredited certificates have to be loaded in the smart phones through a series of steps which are not convenient at all.

The complicated process of installing through ActiveX maximizes complaints of the users. Users claim that it is an issue when inconvenience is raised because of having to pay through the accredited certificate whereas payment systems of other countries allow easy purchasing of goods after going through some simple steps.

Therefore, if the use of the accredited certificate is going to be continued, it should be improved as soon as possible in a way that users feel comfortable because there is a high possibility that new certification methods which will compete with the current accredited certificate will be developed in the direction of improving usage restrictions and inconvenience of the PC or smart phone environment.

The Ministry of Science, ICT and Future Planning has a plan to develop and proliferate a technology for the accredited certificate that does not use ActiveX, however financial institutions are using ActiveX when installing other security programs currently in use such as the computer virus vaccine, key logger prevention programs etc. Therefore, although an environment is set up where the accredited certificate can be used regardless of ActiveX, financial institutions can still use the accredited certificate through ActiveX for the time being.

It is expected that the number of accredited certificate users will decrease rapidly due to the rapid increase in mobile commerce and emergence of simple payment means in the mobile environment.

In this regard, the government and related institutions are currently making efforts to improve the mandatory usage of the accredited certificate in domestic online shopping malls and the ActiveX installment practices. As for improvement of online payment, payment convenience can be provided to mobile users and overseas consumers can also buy goods within Korea.

4.3. Exploring Various Means of Accredited Certification

As for certification methods in the electronic environment other than the accredited certificate, various certification methods are being raised including biometric identification such as fingerprints and voice, combination of SSL, and OTP and transaction linked OTP creator. Such certification methods are mainly used in foreign countries and were suggested as an alternative to accredited certification. SSL could be suggested as an alternative to the accredited certificate, however it is not able to provide functions such as integrity and signature that is provided by the accredited certificate and cannot provide non-repudiation

functions for transaction details. Other existing methods are continuously being developed as an alternative to the accredited certificate.

In the meantime, expansion of the digital signature OTP generator (hardware) can be considered as an alternative to the accredited certification and SSL, and also another alternative is to research biometric technologies utilizing biometric information of the person and accept it as a tool for accredited certification. Biometric technology that checks identification by partially using bio information of the body does not require memorizing the type of knowledge (what you know) nor having to carry it (what you have) but only to prove biometric information of oneself (who you are).

As fingerprint recognition functions are being loaded in various smart phones, development of accredited certification measures utilizing biometric information is being accelerated.

5. Closing

The number of smart phone subscribers in Korea as of July 2014 was 39.04 million. The number of accredited certificate issuance as of the end of December 2013 was 30 million cases and the economically active population in Korea is 25.87 million people. A larger number than the current economically active population is using smart phones and accredited certificates.

Accredited certificates are spread widely enough for most of the economically active population to use it, however there are also many issues related to the accredited certificate due to a lack of understanding as digital signature is a technological area.

Accredited certificates are deeply rooted in our daily lives, but complaints about its inconvenience are always pointed out due to emphasis on security. With payment rapidly becoming electronic and cyber fraud becoming more sophisticated than ever before, new certification tools are being developed and introduced in tele banking, mobile banking, e-commerce using smart phones. Since the user will experience inconvenience such as having to remember or carry the proper certification tool when doing various transactions, it is becoming more important to introduce a new certification means that can consolidate the tools. However up to now, since more people think the accredited certificate is the safest, it is expected that usage of the accredited certificate will only be reduced in fields where security is not greatly required. A program called ActiveX was greatly used even though the security level is weak in electronic transactions utilizing the accredited certificate because most of the Korean public used a certain internet web browser. As there are claims that Electronic signature through the accredited certificate is incapable of being used in other web browsers, there is an urgent need for improvement measures. There were discussions about loading the accredited certificate in the smart phone and about electronic payment due to the explosive increase in smart phone usage, which led to the end of the mandatory usage regulation of the accredited certificate in the financial sector in 2010. Also, the Korean Financial Services Commission revised the Regulations in May 2014 and abolished the mandatory use of the accredited certificate from the previous regulation of having to use the accredited certificate in e-commerce such as internet shopping worth more than 300,000 KRW to not having to use the accredited certificate in e-commerce such as card payment of credit card or debit card. The government allowed the continued usage of accredited certificates for online money transfers worth more than 300,000 KRW, but plans to abolish this as well when an alternative certification method is introduced and integrated. Simple payment methods of global payment gateways (PG) such as “Alipay” of China and “Paypal” of the US are expected to be introduced in Korea when payment through accredited certificate disappears.

Accredited certificates have maintained a monopolistic position for the past decade as a

tool for identification in cyber space, but its share is reducing dramatically due to the penetration of smart phones and cyber-crime.

However, since the accredited certificate has much value as an identification tool in the internet environment, interest, research and improvement efforts of related parties are required to create a simple and convenient environment. Electronic transaction companies have to develop services of which people can use the accredited certificate safely and conveniently and also try to explore and introduce other certification tools rather than abusing the accredited certificate. Also the government should come up with policy and execution measures such as creating a safe usage policy of the accredited certificate as well as a convenient usage environment and exploring other means of certification.

References

[1] E.-K. Kim, "Legislative direction for digital signature and certification system," Legislation Division of the National Assembly Secretariat, pending legislation, no. 2001-4, **(2001)**.
[2] D.-H. Bae, "Digital signature and internet law", Saechang Publishing Company, **(2000)**.
[3] J.-H. Lee, "Legal research on digital signature and certification system," Ph.D. thesis of Kyung Hee University, **(2012)**.
[4] J.-H. Lee, "Usage and issues of accredited certificates in a smart environment," INTERNET & SECURITY FOCUS, Korea Internet Security Agency, vol. 3, **(2013)**.
[5] W.-Y. Chung, "Electronic Commerce Act (third version)", Bubyoung Company, **(2009)**.
[6] "Report on operation status and development plan of the accredited digital signature certification system", Korea Information Security Agency, **(2003)**.
[7] "Report on fact-finding survey of digital signature usage of the public in 2009," Fiduciary institution: Mbrain Inc., Korea Information Security Agency, **(2009)**.
[8] "Research on current status of overseas digital signature and certification," Fiduciary institution: Korea Legislation Research Institute, Korea Internet and Security Agency, **(2013)**.
[9] "Digital payment and consumer protection," material from the 18th symposium of the Korea Consumer Law Association. Korea Consumer Law Association, **(2014)**.
[10] Bank of Korea (2014) Report on payment and settlement system in, **(2013)** April 8.
[11] "Issuance of accredited certificates by year", Korea Internet and Security Agency, **(2014)**.
[12] Y.-J. Choi, "Usage status of the accredited certificate in smart phones and technology trend", Payment and information technology, Korea Financial Telecommunications and Clearings Institute, no. 56, **(2014)**.
[13] "UNCITRAL (United Nations Commission on International Trade)", http://www.uncitral.org/.

Received: Month xx, 20xx