Song, Yeongkwan

Research Report

Lessons from the Dispute over Korea's Digital Certification Regulation and Policy Suggestions for Electronic Commerce

KDI Focus, No. 51

Provided in Cooperation with:
Korea Development Institute (KDI), Sejong

Suggested Citation: Song, Yeongkwan (2016) : Lessons from the Dispute over Korea's Digital Certification Regulation and Policy Suggestions for Electronic Commerce, KDI Focus, No. 51, Korea Development Institute (KDI), Sejong, https://doi.org/10.22740/kdi.focus.e.2015.51

This Version is available at:
https://hdl.handle.net/10419/200853

KDI FOCUS
March 12, 2015 (No. 51, eng.)

For Inqury: KDI Communications Unit
Address: 263, Namsejong-ro, Sejong-si 30149, Korea
Tel: 82-44-550-4030 **Fax:** 82-44-550-0652

Authors | Yeongkwan Song, Fellow at KDI(82-44-550-4172)

KDI FOCUS | Analysis on critical pending issues of the Korean economy to enhance public understanding of the economy and provide useful policy alternatives

Korea's Leading Think Tank

www.kdi.re.kr

Lessons from the Dispute over Korea's Digital Certification Regulation and Policy Suggestions for Electronic Commerce

Yeongkwan Song, Fellow at KDI

"For e-commerce to serve as a platform for innovation, all forthcoming regulations on e-commerce must adhere to the principles of technological neutrality and private sector-driven leadership and should include additional policy goals of enhancing consumer benefit and protection. It is important to consistently develop and implement policies that reflect the different roles of government and the private sector, and resolve the fragmentation within government ministries."

Ⅰ. Issue

Government regulations mandating consumer authentication via digital certification for electronic financial transactions attracted massive social attention during the 1st Ministerial Meeting on Regulatory Reform and Public-Private Joint Regulatory Reform Conference held on March 20th, 2014; digital certification is now widely used in domestic

* This is the translated version of KDI FOCUS released on March 12, 2015.
** Note that this paper is written based on the main points from Song (2014, 2015), hence there may be some overlap.

Dispute over digital certification has been ongoing for the past ten years with respect to its mandatory use as a means to verify personal identity in online banking and electronic commerce.

online banking, electronic commerce payment, government procurement, electronic bidding systems, online stock trading, electronic trade and customs clearance, etc. However, since the mandate was put into place a decade ago as a means to verify personal identity in online banking and electronic commerce (hereinafter e-commerce), dispute over digital certification has been ongoing.

Shedding light on the consequential effects of the government policies that mandate the use of digital certification in electronic financial activities, essentially forcing the use of a specific technology for certification, this study aims to evaluate whether the regulation has achieved its intended policy goals and, based on the evaluation results, suggest a desirable future direction for e-commerce regulations. To that end, it first closely outlines the background of the regulations, identifying the initial policy goals and examining the trajectory which has changed in line with the progress in e-commerce. Additionally, an evaluation was conducted on how well the regulation has fulfilled it policy goals, focusing on the ongoing disputes. The study finally concludes with suggestions for the future direction of e-commerce regulations.

Ⅱ. Summary of Digital Certification Regulations

1. Background

Digital certification was adopted "to ensure the safety and reliability of electronic messages and to promote their use" in response to the expansion of electronic transactions.

E-commerce enables fast, convenient and low-cost transactions, but due to the impersonal nature, security and credibility issues have increasingly been called to attention. The most conventional solution is the use of digital signatures and certification. As stipulated in Article 1 of the Digital Signature Act, digital certification was adopted "to ensure the safety and reliability of electronic messages and to promote their use" in response to the expansion of electronic transactions. Specifically, in order to verify the identity of the user and prevent forgeries and denial i.e. non-repudiation, the government recognized and granted legal status to digital signatures embedded in certificates issued by the licensed certification authority.

With the rise of e-commerce, heated discussions regarding the legal status of the digital signature have continued since the 1980s. The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Signatures (MLES) in 2001 in an effort to establish a harmonized legal framework among different countries with different laws. The MLES builds on three fundamental principles of non-

1) According to the UNCITRAL Model Law on Electronic Commerce, "the principle of non-discrimination ensures that a document would not be denied legal effect, validity or enforceability solely on the grounds that it is in electronic form ..... The functional equivalence principle lays out criteria under which electronic communications may be considered equivalent to paper-based communications."

discrimination, technological neutrality and functional equivalence,[1] which underlay the UNCITRAL Model Law on Electronic Commerce. Technological neutrality was adopted to avoid favoritism of any one technology by governments in order to establish an innovation-driven environment by preventing e-commerce from being overly dependent on a specific technology and allow the introduction of new, advanced technologies without additional legislative procedures. In Korea's initial provision, the Digital Signature Act (July 1999), Article 3 and 8 recognized that the 'electronic signature key' was the sole qualified technology for electronic signatures. This was later amended and the principle of technological neutrality was adopted in the April 2002 revision.

The principle of technological neutrality was adopted in the revised Digital Signature Act which went into effect in April 2002.

2. Development

Korea's adoption of digital certification is rooted in the Digital Signature Act, in response to the expansion of e-commerce. It is a government-authorized digital signature and is akin to electronic seal certification for identity verification in electronic transactions. Following the adoption, the government initiated a policy mandating the use of digital certification in online banking and stock transactions in September 2002 and March 2003, respectively. The policy was first applied to online credit card purchases of 300,000 won or more in April 2004 and then to 100,000 won or more later in the same year, in October. However, in November 2005, the government revised the regulation, leaving the decision of whether to demand digital certification for credit card transactions up to the credit card companies while mandating its use for bank transfers of 300,000 won or more.

Although the government first implemented the mandate in 2002, the use of digital certification in electronic financial activities was only legislated in 2007, through the Electronic Financial Transactions Act. Stipulated in the Act, paragraph 3 Article 21 (Duty to Secure Safety), the Financial Services Commission (FSC) may determine the standards for and authorization methods of authorized certification, referred to in subparagraph 8 Article 2 (definitions) of the Digital Signature Act, to secure the safety and reliability of electronic financial transactions. Specifically, the FSC was granted the authority to select a technology for digital certification in electronic financial transactions. Article 7 legislated the mandatory use of digital certification in electronic financial transactions (Guidelines for the Use of Public Certificates) of the amended Regulation on the Supervision of Electronic Financial Activities (December 28th, 2006), stipulating that all electronic financial transactions shall be made via public certification under the Digital Signatures Act with the exclusion of those for which public certificates are unavailable either technically or systematically. The Article also specifies that cases of exemption shall be determined by the Governor of the Financial Supervisory Service (FSS). The second amendment made on the same day, the Detailed Regulations on Supervision of Electronic Finance paragraph 4 of Article 31 (Exceptions in the Use of Accredited Certifications or Similar in Electronic

Although the government implemented the mandatory use of digital certification in 2002, it was only legislated in 2007.

It was after the 1st Ministerial Meeting on Regulatory Reform and Public-Private Joint Regulatory Reform Conference held by the President on March 20th, 2014 that the government became active in the establishment of improvement measures.

The latest revision of the Electronic Financial Transactions Act does not recognize the FSC's authority over the choice of authentication method e.g. digital certification.

Financial Transactions), exempted credit card payments and on-line money transfers of under 300,000 won in e- commerce.

The mandatory policy triggered a backlash, prompting the Office of the Corporate Ombudsman under the Prime Minister's Office to formulate and release safety guidelines for the authentication of electronic financial transactions in May 2010. Based on the guidelines, the Regulation on the Supervision of Electronic Financial Activities was amended to alleviate the mandatory use of digital certification and went into effect on June 30th, 2010. In order to provide a legal basis for the termination of mandatory use in response to the challenges in the mobile communication environment, the amendment states that financial transactions for which digital certifications are not available are exempt from the regulation. The most noticeable change brought by the amendment is found in Article 7 (Authorization Method, etc.), which allows the use of not only existing digital certification but also other certifying methods that are recognized as digital certification and stipulates the establishment of the Committee for the Evaluation of Authentication Methods as a FSS-affiliated organization.

To repeal the digital certification regulation and adopt diverse certification methods, bills for a partial amendment of the Electronic Financial Transaction Act and full revision of the Digital Signature Act were submitted to the National Assembly in May 2013. Thereupon, in March 2014, problems within the digital certification regulation were addressed at the Ministerial Meeting on Regulatory Reform and Public-Private Joint Regulatory Reform Conference. In April of the same year, the Ministry of Science, ICT and Future Planning (MSIP) announced the initiation of its regulatory reform efforts with the release of a reform plan for 2014, containing measures to develop technology that does not require ActiveX for digital certification. Consequently, the FSC amended Article 4 of the Detailed Regulations on the Supervision of Electronic Finance to lift the requirement on digital certification use for online payments via credit/debit cards and online bank transfers of less than 300,000 won, starting from May 20th. Specifically, the scope of mandatory use was reduced to online bank transfers of 300,000 won or more. In July, the government presented the "Plan to Simplify Online Payment for E-commerce" which allows the use of alternative methods for online payments of 300,000 won or more and storage of credit card information by payment gateway firms. On September 23rd, the FSS released additional measures for easier online payment, planning to develop ActiveX-free digital certification and adopt a simpler payment service. Accordingly, Article 21 of the Electronic Financial Transactions Act (October 16th, 2015), states that the FSC shall not force the use of a specific technology or service and shall make efforts to encourage fair competition for security and authentication technologies.

Ⅲ. Disputes over Digital Certificate Regulation and Evaluation

As stipulated in Article 1 of the Digital Signature Act, digital certification was introduced "to ensure the safety and reliability of electronic messages and to promote their use." The government's intent in mandating the use of digital certification in electronic financial transactions was to enhance the safety and reliability of e-commerce. However, there has been increasing criticism. The following reviews and evaluates the relevant disputes.

1. Digital Certification Safer than Other Authentication Methods?

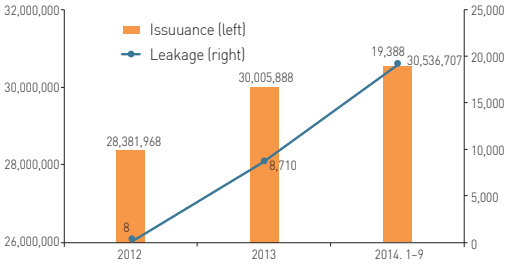
Digital certification is a seal-like certificate electronically issued to e-commerce users so service providers can verify the authenticity of the client, confirming user identity, checking against forgeries and alteration of transaction information resulting from hacking and non-repudiation. Accordingly, digital certification helps verify customer identity more accurately, compared to merely using username and password. Even if the transaction information is hacked, any alteration can be identified by verifying the electronic signature. Moreover, cases where a user denies his/her transaction with malicious intent to misuse the non-face-to-face characteristics of e-commerce can also be debunked.

However, despite its use as a means to verify identity, there are security concerns regarding digital certification. In Korea, it is heavily dependent on ActiveX which is deemed to have high security risks and lack cross-browser compatibility. The technology is essentially a method that enables Windows applications with rich user interfaces to run on a web browser, IE in this case. However, due to security concerns, its developer, Microsoft, advises users to avoid this technology when possible. Although digital certification itself is not based on ActiveX, most financial institutions in Korea provide digital certification service using various ActiveX-based services such as firewall and virtual keyboard.

Additionally, as digital certification must be saved in a specific folder i.e. NPKI, according to standard specifications, it is highly vulnerable to cyber-attacks including hacking when it is saved on hard drives; private keys and digital certification saved on hard drives or USB devices cannot be protected. Specifically, in the public key encryption structure, on which digital certification is based, private key is not protected, as such it is vulnerable when the storage device itself is hacked. In particular, once ActiveX is installed on users' hard drives, it can run via any temporary website and used to obtain access to users' system resources without being stopped by security applications.

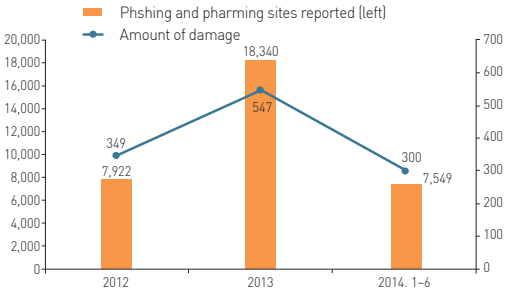
The financial supervisory authority has so far insisted on the use of digital certification, arguing that there are no alternatives available and while other authentication methods can ensure the security fundamentals of confidentiality, integrity and authentication, they cannot fend against non-repudiation. However, there are growing doubts over the capability of digital certification with regards to non-repudiation when it can be so easily

[Figure 1] Digital Certificate Issuance and Leakage



Note: Uses data gathered until Sep. 2014.
Source: Jeon, Byeong-hun assemblyman's office (2014).

[Figure 2] Phishing and Pharming Attacks



Note: Uses data gathered until Jun. 2014.
Source: FSS (2014).

Digital certification may be a safe authentication method for financial institutions and electronic financial service providers, but it does not guarantee consumers' security as it is exposed to the risks of loss or hacking.

lost, stolen or hacked. Much like a seal, digital certification can best serve as a means of personal identification, but the responsibility of storing them safely is entirely up to the user. In other words, digital certification serves as a powerful security tool for service providers such as financial institutions and e-commerce businesses, but it provides consumers with little protection against risks.

Indeed, the number of reported digital certification leaks has skyrocketed. Although the Korea Internet & Security Agency refuses to disclose the relevant data, those that have been submitted to the National Assembly's audit and inspection of state affairs in 2014 show that a total of 19,388 digital certifications were leaked from computers and smartphones due to malware, smishing, etc. between January and September. The numbers indicate an astronomical increase, leaping from 8 in 2012 to 8,710 in 2013. Reports of phishing and pharming attacks also exhibited an alarming escalation, surging from 7,922 in 2012 to 18,340 in 2013, and 7,549 in January-June 2014 (5,814 cases in first half of 2013). The amount of damage is estimated to have totaled 34.9 billion won, 54.7 billion won and 30.0 billion won during the respective periods (20.7 billion won in first half of 2014). As evidenced, the mandatory use of digital certification has left customers with no choice but to use ActiveX-based services, implying that unless customers pay particular attention to online security, they may easily become exposed to the risk of leaks and loss, exacerbating the weakening of digital certification-based security.

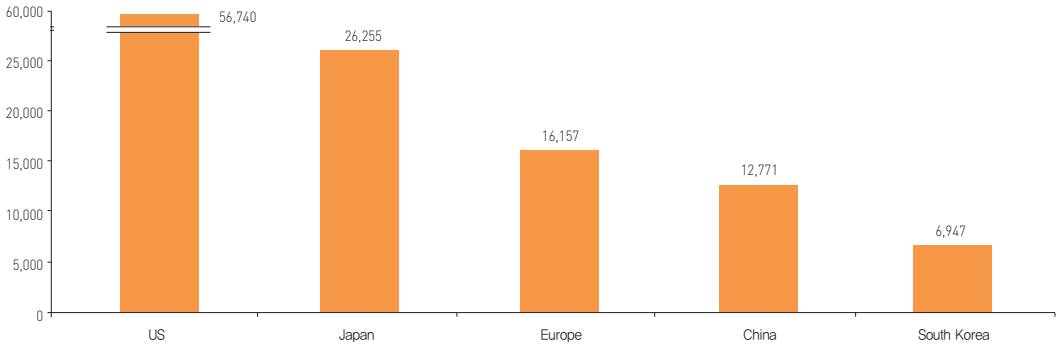
Between January and September 2014, a total of 19,388 digital certificates were reportedly leaked, and consumer damages caused by phishing and pharming sites are growing rapidly.

2. Is the Digital Certification Regulation Hindering the Development of the E-commerce Environment?

Critics have argued that the government regulation on the mandatory use of digital certification generates negative impact on the progress and advent of new technologies as the government is essentially monopolizing the development of digital certification technology.[2] Moreover, it has also been claimed that the regulation may undermine

2) Song, Yeongkwan, "Past, Present and Future of Public Key Certificate Policy in Korea's Electronic Commerce," Policy Study, 2014-07, Korea Development Institute, 2014 (in Korean).

[Figure 3] International Comparison of Encryption Technology Patent



Note: Encryption-related patent classifiaction codes are as follows: H04K1 (Secret communication (ciphering or deciphering apparatus)), H04L9 (Arrangements for secret or secure communication), H04W12 (Security arrangements, e.g. access security or fraud detection: Authentication, e.g. verifying user identity or authorization; Protecting privacy or anonymity)
Source: WIPO-PatentScope (http://patentscope.wipo.int/search/ja/search.just, access date: Feb. 24, 2015).

the incentive structure of private companies to invest in information security, which will eventually obstruct the development of relevant industries. Expressly, Article 9 of the Electronic Financial Transactions Act does not hold financial institutions and electronic financial business operators accountable for any incidents of digital certification leaks resulting from phishing and hacking. As such, the regulation serves to reduce investment in the information security of e-commerce providers.

Indeed, statistics show that there is a lack of interest in IT and security investment in Korea. According to the Survey on Information Security by the Ministry of Science, ICT and Future Planning (MISP), only 2.7% of surveyed firms invested 5% of their IT budget in information security, which is far below that of the US (40%) and UK (50%), highlighting the striking lack of information security investment in Korean firms. The budget for information security in 18 domestic banks totaled a mere 250 billion won, much lower than the Bank of America's 400 billion won.[3] Additionally, the ratio of budget execution in the financial sector has remained below 62% since 2010 which indicates profoundly low investment. This naturally leads to a significant shortage of security patents compared to major countries. According to national data on the number of patented encryption technologies, Korea marked just half of China (12,771) at 6,947, with the US leading at 56,740, followed by Japan (26.255) and Europe (16,157). Such a lack of investment and patents could become a serious obstacle to the competitiveness of Korea's information security industry.

The regulation on digital certification serves to reduce investment in the information security of e-commerce providers. Indeed, according to relevant data, Korean companies have invested little in IT security and the number of encryption patents is very small.

In addition, large online retailers such as Amazon and Alibaba have respective market caps of about 178 trillion won and 215 trillion won, a vast comparison to Hyundai Motors' 42 trillion won and LG Electronics' 10 trillion won. It is therefore easy to imagine what would happen to the Korean economy if a new e-commerce company emerges holding

3) Lee No Keun Assemblyman's Office (2014), Charlotte Business Journal (2015).

a market cap as large as that of Samsung Electronics (224 trillion); most major new IT companies in recent years have larger market caps than that of major Korean companies.

Ⅳ. Future Direction of E-commerce Regulations

Heightened efficiency in all industries is necessary to enhance the potential growth of the nation's economy. As technological progress advances rapidly in the e-commerce industry, it will serve as a platform for innovation, bringing new vigor to the economy. The digital certification regulation, however, has forced the industry to rely heavily on inferior technology i.e. ActiveX, and dragged down the development of digital certification technology itself. Moreover, the mandatory use of digital certification has weakened the private sector's incentive to drive more investment into developing methods for client authentication and information security, consequently hindering the development of new technologies and rise of innovative companies and industries. Consumers have also voiced their grievances over the fact that the regulation affords security to only the providers and not the consumers.

The government should develop and implement comprehensive, organic measures by resoling fragmentation issues within different ministries.

Accordingly, the government should focus on developing and executing well-balanced, comprehensive policies, taking into account the differences in the role of the private sector and government, and the trade-off between standardization and innovation and between information security and convenience. E-commerce encompasses a wide range of areas, involving several government ministries. There are doubts, however, over how well the respective authorities will be able to formulate and execute their policies in a comprehensive, organic and rigid manner. For instance, in September 2005, the then Ministry of Information and Communication (abolished in 2008) announced comprehensive measures to strengthen the security of electronic financial transactions, which allowed credit card companies to decide on whether to demand digital certification for online credit card purchases, based on the possibility that merchants may suffer from decreased sales. However, in the second revision of the Detailed Regulations on the Supervision of Electronic Finance on December 28th 2006, Article 31 paragraph 4, only online credit card purchases of less than 300,000 won were granted exemption from digital certification. In a further revision on May 20th 2014, Article 4 was amended to add debit card purchases to the exemption. Also, in 2008, the Korea Communications Commission (KCC) mandated that telecommunications service providers authenticate servers for the purpose of protecting consumers from online scams such as phishing. This, however, was not extended to financial institutions, who are most in need of such a mandate.

To overcome the inconsistencies between policy formulation and execution like the aforementioned examples, it is important to resolve fragmentation issues within different government ministries and develop and implement cross-government policies.

Furthermore, the competence and specialty of policy makers should be enhanced so that policies fully reflect the distinctive features of the e-commerce industry. To that end, this paper suggests the following two policy directions.

1. Technological Neutrality and Private Sector-driven Leadership

Through the regulation on digital certification, the government has, essentially, forcibly established a specific technology to become the standard for electronic financial transactions. However, every regulation and policy comes at a price to benefit and cost. Specifically, the government's technology standardization might be justifiable in the event of market failure caused by a network effect. But, standardization, as shown in Acemoglu *et al*. (2012), can easily fall into the spectrum of being in conflict with innovation. In areas undergoing fast technological progress, in particular, a hasty approach of standardization could cripple the incentive to increase investment in new technologies necessary for innovation, and deter the commercialization of rapidly advancing technologies which could hamper the vast dissemination of technological achievements. Moreover, due to rent-seeking activities by interest groups associated with existing standardized technologies, there could be resistance to any changes in existing technologies, thwarting the rise of new ones. Considering the negative consequences on innovation brought on by standardization, the cost of government intervention in technology standardization could be much higher than expected. And, as seen in the case of the Wireless Internet Platform for Interoperability (WIPI) standard, government-led standardization that overlook international standards could cause trade disputes in the global market.[4)]

The mandated use of digital certification in electronic financial transactions has resulted in the standardization of authentication methods. And, although this may have its merits, in an industry like e-commerce which undergoes rapid technological progress, a hasty approach of standardization could cripple investment in and innovation of new technologies.

Showcasing the rapid technological progress of the e-commerce industry is the US peer-to-peer lending company, Lending Club, a rising star in the FinTech business, whose innovation swiftly turned it into a large enterprise with a market cap equivalent to that of LG Electronics. In order to foster more innovative firms in the Korean economy, it is important that the future direction of e-commerce regulations incorporate the essence of the US-Korea Joint Statement on Electronic Commerce, which was announced in November 1998 before Korea established its own laws and regulation systems on e-commerce. In the agreement, the Korean government recognizes that "electronic commerce will become an engine for economic growth in the twenty-first century and enhance standard of living." The general principles in the agreement states: 1) the private sector will play a leading role in the development of electronic commerce; 2) government

Forthcoming regulations on e-commerce should fully respect the principles of technological neutrality and private sector-driven leadership in accordance to the US-Korea Joint Statement on Electronic Commerce.

4) The WIPI standard was aggressively promoted by the then Ministry of Information and Communication (MIC) in 2002 with the purpose of institutionalizing a single national standard for wireless internet access. At that time, Qualcomm's Binary Runtime Environment for Wireless (BREW) and Sun Microsystem's Java were competing for a share of the wireless software market, making it doubtful that the WIPI would survive the competition. Upon the release of the MIC's plan to impose the WIPI as the mandatory standard, the US Trade Representatives (USTR) expressed strong opposition, starting in the second half of 2002, arguing that it is in violation of global trade laws and international telecommunications standards. The Ministry suspended it thereafter.

Korea suffers from a significantly higher number of personal information leaks per 100,000 persons than the US.

regulations will be minimal, transparent, non-discriminatory, and predictable to the private sector; and 3) regulations will be globalized.

However, although technological neutrality and private sector-driven leadership had already been endorsed in the original provision of the Framework Act on Electronic Documents and Transactions and the Digital Signature Act in 1999, they were negated by the mandatory use of digital certification, which also violates the fundamental principle of the Civil Act i.e. the freedom of contract. Accordingly, the regulation should be gradually abolished and the coverage of digital certification adjusted. Recent positive actions include the implementation of the revised Electronic Financial Transactions Act in October 2015 and the FSC's release of supportive measures for IT-finance convergence which incorporates the principle of technological neutrality.

2. Additional Policy Goals to Enhance Consumer Benefit and Protection

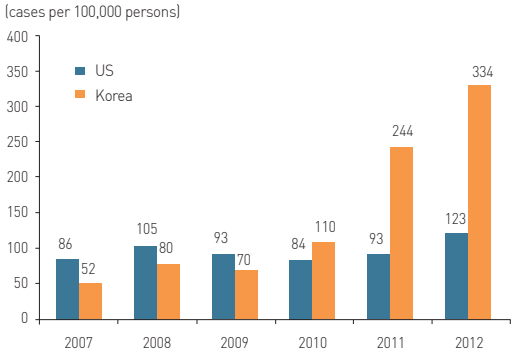
All forthcoming regulations on e-commerce should have additional policy goals on consumer benefit and protection.

The regulation on digital certification may be a safe authentication method for financial institutions and electronic financial service provider but it does not provide the same safety for consumers who are susceptible to hacking and phishing scams. Before the mandated use of server authentication—safe tool for consumers—in 2012, it was almost impossible for consumers to be sure of the authenticity of the website that was demanding personal information. According to OECD data, as of 2012, the number of security servers per 100,000 persons marked a mere 21 for Korea, a significant contrast to the US' 166, followed by Germany's 113 and Japan's 83; there are some domestic banks that do not even use security servers.

Korea has suffered from a relatively high level of online consumer damage. Along with a rapidly growing number of digital certification leaks, there was a recorded 334 cases (per 100,000 persons) of leaked personal information reported in 2012, much higher than the US' 123 cases. Meanwhile, it is important to note that Korea has witnessed a sharp increase since 2010, while that of the US has remained steady. Also, in terms of the number of cybercrimes (per 100,000 persons) reported in 2013, Korea recorded 311 cases, far exceeding the US' 88 cases.

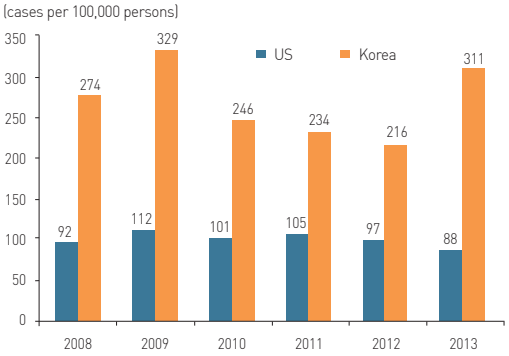
To establish e-commerce as a platform for innovation, the market must provide ample opportunities for businesses, which can only be made possible by the active participation of consumers who are the driving force of demand. In this regard, an environment must be created in which online consumers can enjoy the convenience of using diverse e-commerce services while feeling protected from cyberattacks and wrongful disputes. Moreover, forthcoming regulations on e-commerce should focus on creating an e-commerce environment which can be easily accessed by the general public and explicitly adhere to the policy goals of enhancing consumer benefit and protection. At the same

[Figure 4] Reported Cases of Personal Information Leakage : Korea vs. US



Source: Internet Ststistics Information System (http://isis.kisa.or.kr, access date: Feb. 21, 2015); FTC (2013).

[Figure 5] Reported Cases of Cyber Crimes : Korea vs. US



Note: INcludes other cyber crimes including e-commerce related.
Source: Cyber Bureau of National Police Agency (http://cyberbureau.police.go.kr, access date: feb. 23, 2015); FBI (2014).

time, companies must bear the responsibility of information security rather than the government strengthening regulations on cyber security. This will encourage companies to expand their investment in information security and consumer protection, and technological and industrial development in information security can be achieved. Meanwhile, relevant insurances should be reinforced so that companies operating on a weak capital base can fulfill the responsibility. Finally, although Korea's financial authority has set forth measures to hand more responsibility to companies and promote the system for information security insurance, fundamentally, e-commerce regulations should include additional policy goals to enhance consumer benefit and protection.■

References

- Acemoglu, D., Gino Gancia, and Fabrizio Zilibotti, "Competing Engines of Growth: Innovation and Standardization," *Journal of Economic Theory*, Vol. 147, No. 2, 2012, pp.570~601.
- Charlotte Business Journal, "Moynihan: BofA's Cyber Security Given Unlimited Budget 'To Keep Us Safe'," 2015. Accessed by http://www.bizjournals.com/charlotte/blog/bank_notes/2015/01/moynihan-bofas-cyber-security-given-unlimited.html?page=all
- Federal Bureau of Investigation (FBI), *2013 Internet Crime Report*, 2014.
- Federal Trade Commission (FTC), *Consumer Sentinel Network Data Book*, 2013.
- Financial Supervisory Service, "Women in their 30s Most Susceptible to Phishing Scams, Men in their 40s to Loan fraud," press release, Nov. 11, 2014 (*in Korean*).
- Jeon, Byeong-hun Assemblyman's Office, "Digital certification Used by 30,500,000 Population Faces a 2.5-fold Increase in Leakage in One Year," National Assembly audit data 37, Oct. 23, 2014 (*in Korean*).
- Lee, No Keun Assemblyman's Office, "IT Security Status in Financial Sectors," Feb. 2014 (*in Korean*).
- Ministry of Science, ICT and Future Planning, "Transforming Cyber Security into an Income Earner," press release, Feb. 4, 2015 (*in Korean*).
- Song, Yeongkwan, "Past, Present and Future of Public Key Certificate Policy in Korea's Electronic Commerce," Policy Study, 2014-07, Korea Development Institute, 2014 (*in Korean*).
- Song, Yeongkwan, "Technology Standardization, Government Intervention, and Public Electronic Certificate in Korea," *KDI Journal of Economic Policy*, 2015 special edition, 2015 (*in Korean*).

<Website>

- Cyber Bureau of National Police Agency (http://cyberbureau.police.go.kr, access date: Feb. 23, 2015).
- Internet Statistics Information System (http://isis.kisa.or.kr, access date: Feb. 21, 2015).
- WIPO-PatentScope (http://patentscope.wipo.int/search/ja/search.jsf, access date: Feb. 24, 2015).