Journal of Korean Law | Vol. 20, 577-614, August 2021

Analyzing and Evaluating the 2020 General Amendments to the Korean Digital Signature Act*

*Jaeso Ahn***

Abstract

The purpose of this paper is to present the requirements that the Korean Digital Signature Act (hereinafter "Digital Signature Act") must fulfill and to verify the legitimacy of the 2020 General Amendment to the Digital Signature Act. With the enforcement of the amended Digital Signature Act on December 10, 2020, the "certified digital signature system" was abolished. Consequently, various digital signatures are now recognized as equally effective without the need for national authorization, and different certificates that verify the effectiveness of digital signatures are currently competing in the market. However, domestic research regarding the status quo is limited.

Digital signatures guarantee safety and convenience of electronic documents by confirming the identity of the parties and effectiveness of an electronic contract. In modern society, where digital signatures are widely used to help building a trust system, changes in related laws are bound to have a major impact on the overall economy. Therefore, it is necessary to trace why the general amendment of the Digital Signature Act in 2020 was necessary and to evaluate whether the amended law is sufficiently suitable for creating a desirable digital environment. For an adequate evaluation of both the old and amended laws and to provide appropriate recommendations, this research was organized in the following order.

First, by clarifying the significance of digital signatures and by analyzing the documents on "Reasons for Revisions" of the Korean Digital Signature Act and the Digital Signature Model Act of the United Nations Commission on International Trade Law (UNICITRAL), this research derived four criteria for evaluating the appropriateness of the Digital Signature Act: stability and reliability of electronic documents; contribution to the expansion of use of electronic documents; contribution to informatization; and contribution to the improvement of public convenience. Then, based on these four criteria, this research argued why it was necessary to generally amend the old Digital Signature Act (hereinafter "the old law"). The state-led certified digital signature system guaranteed a stable legal environment for electronic contracts

* Professor Sang-Jo Jong instructed this article. I greatly appreciate Professor Jong for providing invaluable ideas to develop this article and giving advice on the writing process in general. Without his guidance, I would not have been able to complete this paper.

** J.D. Candidate, Class of 2024, Seoul National University School of Law.

in the short term; however, in the process, there has been an increase in risk and inconvenience caused to users and the potential development of various authentication technologies has been hampered.

Finally, this research summarizes the main contents of the amended Digital Signature Act (hereinafter "the amended law") and evaluates it based on the abovementioned four criteria. Consequently, the research reveals that the amended law positively contributes to informatization and increases public convenience by promoting a desirable competition among certificate operators. However, for the newly implemented "Recognition System for Compliance with Operating Standards" to be effective, the distribution of responsibility among related government departments must be fair and clearer than what the amended law and practice currently provides.

I. Introduction

The purpose of this paper is to present the requirements that must be fulfilled by the Korean Digital Signature Act (hereinafter the "Digital Signature Act") and to evaluate the legitimacy and appropriateness of the 2020 General Amendment based on these requirements. With the enforcement of the amended Digital Signature Act on December 10, 2020, the "certified digital signature system"[1] was abolished and various digital signatures were recognized as equally effective, even in the absence of national authorization. The Ministry of Science and Information and Communication Technology, the government department that initiated the amendment, presented the following reasons for the initiation of this amendment: creating non-discriminatory competitive conditions for various digital signature certification methods, enhancing trust in digital signatures, and establishing a certificate recognition system in

1) A 'certificate' for a digital signature is a document that certifies that a digital signature was created by the person and has not been tampered with. Korean media outlets state that the amended Digital Signature Law abolished the 'certified digital signature system'. However, it is most accurate to say that the 'certified digital signature system' has been abolished. This paper will also refer to the system under the old Digital Signature Act, in which the state officially designates a specific certificate among digital signature certificates, as the 'certified digital signature system'.

consideration of international standards.[2] In other words, the amendment focuses on balancing the two values of safety and convenience. The new system proposed by the amendment involves protecting electronic documents from forgery, falsification, and hacking so that the public can engage in electronic transactions without compromising on convenience.

The "certified digital signature system" was first introduced in Korea in 1999. In the early days of e-commerce, business operators had to rely on digital contract offers that had uncertain legal effects. Since Internet transactions were an unfamiliar territory, it was rare for operators to reserve their own hacking detection technology. Private hacking detection security technology that ensures the authenticity of digital signatures was also insufficient. Public institutions encountered the same problem. This broad demand for verifying the sincerity of a digital signature led to the enforcement of the Digital Signature Act in 1999. In accordance with this law, a system was designed in which a "licensed certification authority" attaches a certificate to a specific digital signature to ensure its effectiveness and authenticity. The authorized certificates utilize the public key infrastructure (PKI) system, which is a standard encryption technology that has proven its stability for over 20 years since 1999. Ever since, authorized certificates have been widely used in private and public transactions; in 2017, 94.7% of online identity authentication service users used the "authorized certificate."[3] Along with its widespread use, the certified digital signature system provided a stable foundation for various digital transactions, including online securities transactions, e-commerce, Internet banking, and government procurement.

However, as online legal practices matured in the 2010s, legislative proposals emerged in the National Assembly to abolish the "certified digital signature system." In 2013, Jae-Chun Choi, a member of Congress, proposed an amendment on the Digital Signature Act, which amended the concept and effect of digital signatures on one hand and eliminated all articles on licensed certification authority, authorized certificates, and certified digital signatures (the core articles that were included in the

2) Reasons for Enactment and Amendment of the Digital Signature Act.

3) World Research Inc, 17Nyumdo Daegugmin Jeonjaseomyeong Iyongsiltae Josa [Public Survey on the use of electronic signatures in 2017] 26 (2017) (In Korean).

"certified digital signature system") on the other hand. He believed that the certified digital signature system was overly dependent on the state, even at the time.[4] Although this proposal was discarded at the end of the official term of the 19th National Assembly, his claim that domestic e-commerce relied heavily on government-authorized certificates gained widespread support and, thus, influenced subsequent legislations. On May 20, 2014, an article in "Rules of Operations on Regulation on Supervision of Electronic Financial Activities," which required an authorized certificate for certain electronic transactions (e.g., shopping on the Internet for over 300,000 won or more) was eliminated. On March 18, 2015, major articles were amended in "Regulation on Supervision of Electronic Financial Activities," which specifies user(individuals who participate in electronic financial activities) obligation to use authorized certificates.

As obligatory usage clauses gradually diminished, a member of the 20th National Assembly, Yong-Jin Koh, proposed an amendment of the Digital Signature Act, which shared its core contents with the 2013 proposal of Choi. Instead of abolishing the entire certification system, the proposal included a permit system that allows only those companies that have security requirements at the level of a licensed certification authority to conduct the business of issuing certificates. Since then, a total of seven different amendments to the Digital Signature Act have been proposed. After a long-term review and discussion, a hackathon by the Presidential Committee on the Fourth Industrial Revolution under the direct control of the government, and final discussions between stakeholders and government department officials, a new system was proposed.[5] The Science, ICT, Broadcasting, and Communications Committee of the

4) Ministry of Economy and Finance(of Republic of Korea), 2016 Gyeongjebaljeongyeongheom Modyulhwasa-eob: Jeonjasanggeolae Hwalseonghwa-leul Wihan Jeongbujeongchaeg [2016 Economic Development Experience Modularization Project: Government Policy for E-commerce Promotion] 28 (2016) (In Korean).

5) Young-Kyu Woo, Gaeinjeongbo Gwanlyeon Beobjeog Gaenyeom Chegye Jeongbi Hab-ui, Jeonja Seomyeongbeob Gaejeongeul Tong-han Dayanghan Jeonja Seomyeong Hwalseonghwa Bang-an Non-ui: 4-cha San-eob Hyeog-myeong-wi Je-2-cha Gyu-je, Je-do Hyeogsin Haekeoton Gaechoe [Agreement upon a overhaul on the legal conceptual system related to personal information, Discussion on Activating the use of various Digital Signatures through the revision of the Digital Signature Act: The 4th Industrial Revolution Committee holds 2nd Regulatory and Institutional Innovation Hackathon] 3 (2018) (In Korean).

National Assembly billed the final draft of the amendment on the Digital Signature Act. The amendment passed the plenary session on May 20, 2020 and came into effect on December 10, 2020. As such, the certified digital signature system was carefully and gradually abolished.

However, such a gradual amendment process does not necessarily imply that the current system does not require examination. In fact, the status requires careful evaluation and guidance. First, unpredictable variables tend to appear after the implementation of an amendment. Both Korean and Global technological environment is constantly changing and practices that go against the goals of the amendment may tend to be the ones that become fixed. As digital signatures are directly related to security technology and since the former licensor of licensed certification authorities was a government department, there is a high risk that technology and administrative variables will have major effects after the enforcement of the amendment. Second, changes in digital signature-related systems affect the overall national economy. Digital signatures form the basis of electronic contracts. If the trustworthiness of digital signatures is not guaranteed, online transactions will reduce, thereby resulting in a vast reduction in the radius of citizen's legal activities. There is also a possibility that citizens may become anxious of the fact that their once-used digital signature is no longer recognized by the state. Since approximately 39.66 million authorized individual certificates and 18 million authorized institutional certificates were issued and in use before the amendment,[6] it is necessary to avoid a large-scale confusion due to a systematic change. In other words, it is necessary to assess whether the amended Digital Signature Act is making a soft landing in the domestic e-commerce environment. If any flaws are detected, these flaws must be corrected before legal norms lead to the establishment of wrong practices. In the process, it is also necessary to review whether or not a general amendment was justifiable.

Unfortunately, domestic studies on the legitimacy of the amendment, the status of the system under the amended law, or the direction of

6) Jae-Ju Lim, Jeonja Seomyeongbeob Jeonbugaejeong-an Geomto Bogoseo [Review Report on the General Amendment of the Digital Signature Act] 30 (2018) (In Korean). As of 2018, 39 million individuals and 1,800 private companies and public institutions have issued and are using authorized certificates.

improvement are lacking. Numerous researchers, including In-Soon Kim (2021)[7] and Yong-Hoon Jung (2021),[8] present individual private certificates as an alternative to authorized certificates from a technological viewpoint (i.e., technology related to security and convenience). However, these studies do not directly compare the effectiveness of private and authorized certificates; furthermore, they do not analyze whether or not the ultimate goal of the Digital Signature Act can be sufficiently achieved with the development of a private certificate. Former research conducted by Ki-Chang Kim (2017)[9] and Eung-Jun Jeon (2017)[10] suggested an amendment to the Digital Signature Act based on comparative studies. However, the authors have not yet provided their opinions on the recent amendment. Hyun-Cheol Kim (2021)[11, 12] indicates the problems associated with the amended law and argues that it must be improved by adopting certain articles of European Union's (EU) eIDAS, but his blueprint goes against the direction of the recent amendment in that it greatly strengthens the state's regulations. Above all, there is no study that clearly states what a domestic law on digital signature must pursue. Thus, a comparison between the old and amended laws must be based on the goal of the laws.

Ultimately, it is appropriate to answer the following questions. "On what standard must a domestic digital signature legislation be evaluated?" "According to this standard, was the recent general amendment on the

---

7) In-Soon Kim, *Gongininjeungseo Sidae Gago Mingan Jeonjainjeung Sidae Dorae [Era of Authorized Certificates goes and Era of Private Certificates comes]*, 42 KISO J. 36-38 (2021) (In Korean).

8) Yong-Hoon Jung, *Beullokchein Giban Saeroun Sinwonhwagin Chegye [Blockchain-based New Identification System]*, 22(2) J. KOREA ACAD.-INDUS. cOOPERATION SOC'Y, 452-458 (2021) (In Korean).

9) Ki-Chang Kim, *Jeonja Seomyeong beobje Gaeseon Banghyang [Reform Proposals for the Korean Electronic Signature Act]*, 79 J. COMP. PRIV. L. 1883-1930 (2017) (In Korean).

10) Eung-Jun Jeon, *Saeroun Jeonjageumyunghwangyeongeseo Gongininjeungchegyeui Gaeseonbanghyange Gwanhan Yeongu [A study on the Improvement of Accredited certification system in new electronic financial environment]*, 21(3) J. KOREA INFO. L. 285-310 (2017) (In Korean).

11) Hyun-Cheol Kim, Bidaemyeon Sidae-e Jeonjaseomyeong Dedo-ui Jaengjeomgwa Gaeseon Banghyang [Issues and Improvement Directions of the Electronic Signature Legal System in the Non Face-To-Face Era], 81 KOREA L. REV. 1-20 (2021) (In Korean).

12) Hyun-Cheol Kim, *Gaejeong Jeonjaseomyeongbeob-ui Jaengjeomgwa Gukjejeok Heureum [Issues and International Trends of Revised Electronic Signature Act]*, 18(1) J. LEGIS. STUD. 81-109 (2021) (In Korean).

Digital Signature Act legitimate?" "If so, does the current system under the amended law meet the criteria for a desirable digital signature law?" This research attempts to answer these questions. Specifically, Chapter II explains the significance of digital signatures and introduces four criteria for evaluating the digital signature method. Chapter III justifies the general amendment of the old law based on the above criteria, and Chapter IV evaluates the appropriateness of the amended law. Furthermore, the research mentions the effort required on the part of different entities to ensure that the amended Digital Signature Act fully satisfies the above criteria. By doing so, the research aims to provide clues on how the Digital Signature Act must establish a safe and convenient electronic transaction environment and create a fair certificate market even in the current transition period.

II. The Significance of Digital Signatures and the Objectives of the Digital Signature Act

There are four criteria for evaluating the Korean legal system in terms of digital signatures: 1) Whether it secures the safety and trust of electronic documents; 2) whether it activates the use of electronic documents; 3) whether it promotes informatization; and 4) whether it enhances the convenience of people's lives. The above four criteria are derived from both the Korean Digital Signature Act and the Digital Signature Model Act of the United Nations Commission on International Trade Law(herein after UNCITRAL).

1. The Significance of Digital Signatures

First, by clarifying the function and nature of a digital signature, the necessity of a separate law governing digital signatures becomes evident. A signature is a symbol of or a statement made by a party to indicate their identity and clarify their responsibilities. A valid signature assures that the document has been written by the signee and that its contents have not been altered. Take an example of a contract: the Korean Civil Procedure Act recognizes strong evidence for disposal documents (written contracts, etc.)

with signatures and seals.[13] The parties may prepare and sign a written contract in advance to fulfill their burden of proof in a legal dispute. In cases where various special laws stipulate a signature or a sealing as a requirement for validity, only signed or sealed documents are valid. Thus, signing and sealing are symbols of stability and trust in our society—which comprises numerous legal acts—by confirming the contents and parties of a legal act as authentic and, occasionally, making it effective.

The strictness of the requirements for a valid signature or seal are dependent on legislative policy decisions that comprehensively consider the characteristics of legal acts, the circumstances of the times, and the technological environment. If the requirements are relaxed, legal activities are concluded easily, but transaction safety may be impaired. Conversely, if strict requirements are presented, transaction safety is secured while high hurdles hinder the establishment of a contract. In occasional face-to-face relationships, signature and seal requirements are relaxed. This is because, compared to digital transactions, "identity authentication," which confirms whether the person indicated by the signature/seal is the actual signer, is simpler. It is reasonable to believe that the parties and the contents are confirmed just by confirming each other and signing or sealing the contract with one's own handwriting or seal. The social utility is increased by easing the requirements for signing and sealing, promoting convenience in legal acts, and ensuring transaction safety through general principles of the law, like "apparent representation" in Korean civil law.[14]

However, stricter standards are required to grant trust to digital signatures and seals (hereinafter referred to as digital signatures). Because of the non-specificity of data, parties cannot adopt the same methods that are used to guarantee the authenticity of physical documents. Additional

---

13) Article 358 of the Civil Procedure Act "Private documents are presumed to be genuine when they are signed, sealed, or unattended by the principal or his/her agent."

14) *See* Korean Civil Act Article 125, 126 and 127. In signature theft cases(where a third party trusted a contract with a stolen signature), the Korean court applies the jurisprudence of "unauthorized representation." (1) If a person is not responsible of the theft, he is free from contractual obligations. (2) If the victim is responsible for creating the appearance, the third party is protected only under a condition that his trust is a legitimate and just one. (3) The thief who recklessly stole the other person's signature is subject to responsibilities regarding 'unauthorized agents(including Article 135 paragraph 1).'

security technology is required to authenticate the fact that (1) the sender attached his or her digital signature and (2) that the document with the digital signature has not been tampered with from transmission to reception. For digital identity authentication to guarantee the same effect as conventional signing and sealing, a digital signature must have an attached certificate that technologically proves the authenticity.[15] The better the security technology of the certification authority, the stronger the reliability of the digital signature.

To summarize, a digital signature is a type of signature that establishes the parties to a legal act and determines the establishment of a contract when it is required by law. For digital signatures to guarantee the effectiveness of a transaction at the same level as face-to-face signatures and seals, it must be backed up with security technology. A digital signature has the same effect as a face-to-face signature when transmitted with a certificate that guarantees its authenticity. The Digital Signature Act strengthens the role of digital signatures by pre-determining the general effect of the digital signature, certification authority, certification procedure, and the effectiveness of the certificate with certain technology levels.

2. The Objectives of the Digital Signature Act

Obviously, a digital signature should function as a "signature." The ultimate goal of the Digital Signature Act is to create an environment where digital signatures are as commonly used and are regarded as equal as face-to-face signatures and seals. For this, first, the ramifications of its usage must be the same. In other words, digital signatures must also guarantee and confirm authenticity. Second, electronic documents with digital signatures must be more frequently as compared to physical documents. Third, the online world in which digital signatures are used must be sufficiently mature. Fourth, the signing process must be at least as simple as a face-to-face signature. By doing so, digital signatures could come to be widely used in electronic legal activities.

Further, international norms pertaining to digital signatures share the

15) the operator that certifies the digital signature through security technology is called a 'certification authority'.

abovementioned four goals but are expressed differently. Model Law on digital signatures, the most representative international document related to digital signatures, adopted by the UNCITRAL, states that its ultimate goal is to create an Internet environment where digital signatures and paper-based signatures are equally used.[16] To achieve this goal, the Model Law states that the effectiveness of digital signatures and face-to-face signatures must be at the same functional level, that the e-commerce activities in each country must become active[17], and that the development of identity authentication technology must be encouraged.[18]

The Korean National Assembly also expressed the same goal in its initiative of the Digital Signature Act in 1999. "Regarding the expansion on the use of electronic documents, the goal of this Act is 1) to secure the safety and reliability of electronic documents and 2) to promote the use of digital signatures and 3) to promote informatization of the national society by stipulating matters related to the legal effect of digital signatures and the management of government-authorized certification agencies and 4) to improve the convenience of people's lives."[19, 20] As this quoted sentence that states that the "purpose" still remains the same as that in Article 1 (purpose) of the current Digital Signature Act, it is reasonable to assume that the quoted goal still remains the goal of the current Digital Signature Act.

---

16) United Nations Commission on International Trade Law (2001). UNCITRAL model law on digital signatures. New York: United Nations, p. 9: "objectives include enabling or facilitating the use of digital signatures and providing equal treatment to users of paper-based documentation and users of computer-based information"

17) Tae-Yeop Kim, Yuengukjesanggeoraebeobwiwonhoe (UNCITRAL) Je-4-Silmujageopban Sinwongwanli mit Silloeseobiseu (IdM and Trust services) Choangyujeong-ui Gugnaebeobgwa-ui Bigyo - Choangyujeong Nae Uimuwa Chaeg-im Johang-eul Jungsim-euro [Comparison between the Draft Provisions on IdM and Trust Services of the UNCITRAL Working Group IV and the Korean Domestic Law—Focusing on the Obligation and Liability Clauses—], 146 Int'l Trade L. 289 (2020) (In Korean).

18) *See supra* note 16, at viii : "where such digital signatures are functionally equivalent to handwritten signatures" "Mindful of the great utility of new technologies used for personal identification in electronic commerce and commonly referred to as digital signatures."

19) Although the requirement that an electronic signature should be as simple as a face-to-face signature is not the same as the improvement of public convenience, the research classified the two by the same number because of their close relationship and for convenience.

20) Jeonjaseomyeongbeoban [Digital Signature Act], Provision (S. Kor.) (1998).

As such, the Korean Digital Signature Act, from 1999 (when it was enacted) to 2021(after the most recent amendment) states the above four goals in Article 1. The Digital Signature Model Act, a representative evidence of international norms, also expresses a similar goal. The above four goals are in line with the essence of digital signatures, "pursuing the equal use of digital signatures with face-to-face signatures." Therefore, from this point on, the research evaluates the Korean digital signature system based on the following four criteria: 1) safety and trust, 2) activation of electronic document use, 3) informatization, and 4) improvement in public convenience.

III. Drawbacks of the Old Digital Signature Act

1. Contents of the Old Digital Signature Act

The digital signature system under the old law can be summarized as (1) a state-led government-authorized certificates (2) and a superior status of the government-authorized digital signature. First, the certified digital signature system is a system in which the state actively intervenes in the authentication process of digital signatures and grants a "state-authorized" status to specific digital signatures. Under the old law, the Ministry of the Interior and Safety designates licensed certification authorities that are responsible for obtaining a digital signature verification key from the Korea Internet and Security Agency (KISA). Then, the authorities used a "creating key" that matches with the "verifying key" to authorize other signatures (the old Digital Signature Act Article 8). In addition, prior to the commencement of certification business, the authorities were required to prepare certification business rules that follow a certain technology type of certification business, methods and procedures, conditions of use, fees, and other matters necessary for certification business, and then reported it to the Minister of the Interior and Safety (as per Article 6 of the old Digital Signature Act). These authorities had to report to the Minister of the Interior and Safety before any actions regarding changes in its business activities, such as transfer of certification business and merger with other companies. Any violation of such duty could lead to a suspension of the

certification business.

Next, the old law gave superior effect only to "certified digital signatures,"[21] which were attached with an authorized certificate that obtained its status through the above process (Article 3 of the old Digital Signature Act). Other than certified digital signatures, irrespective of how excellent the security technology of the certificate attached to it was, the authenticity of these digital signature was not equally granted by the Digital Signature Act. Consequently, the effectiveness of these signatures had to be determined according to the general principles of the Civil Procedure Act, and according to a systematic interpretation of the Digital Signature Act by the Supreme Court of Korea, these signatures were not recognized to be as effective as certified digital signatures.[22]

Several special laws stipulated that only a certified digital signature must be used for certain types of transactions that require strong transaction safety, and there were numerous cases where business operators required that customers mandatorily use a certified digital signature. Consequently, authorized certificates had been firmly established as the most widely used digital signature certificates in electronic contracts, such as Internet banking, public and civil affairs, e-commerce, Internet securities businesses, and Internet insurance credit card businesses. In this manner, the stability of domestic electronic transactions was strongly guaranteed in the early 2000s, which marked the beginning stages of electronic transactions. Security was solid, and apart from cases in which the user of an authorized certificate leaked its password, until 2018, there was not a single case in which an official certificate issued to an individual was tracked through the security system (PKI) and hacked.

---

21) Digital signature approved by an attached authorized certificate, issued by a licensed certification authority. Note that non—'certified digital signatures' may also attach a certificate, but an unauthorized one.

22) Kyung-Won Chang, Jeonjaseomyeongui Gongbeobjeok Munje [Public Law Problems of Digital Signatures] 29 Admin. L. J. 158 (2011) (In Korean).

2. The Necessity of an Amendment

1) Safety and trust: loss of safety, comparative advantage, and transfer of responsibility

Despite its wide use and approved safety, the authorized certification system for digital signatures has indicated many side effects that justify the recent general amendments. This portion of the research analyses and criticizes the disadvantages of the old law and the system it prescribed based on the four criteria suggested above in chapter II.

In terms of safety and reliability, it is difficult to deny a short-term stability of the old certification system. The PKI technology adopted by public digital signatures is an essential information protection mechanism in e-commerce and has great potential for development.[23] The stability of authorized certificates has been maintained by updating the associated security technology several times, such as strengthening the algorithms involved in 2012. Although there were approximately 120,000 leak cases of authorized certificates 2010 to 2020, only 6 successful hacking incidents caused the leaks. [24] Cases where such hackings led to personal financial damage were rare due to double protection features, like the one time password (OTP).

However, such safety and stability must not be overestimated. First, a non-authorized certificate can provide equal or even better security service. For example, biometric authentication is a technology that authenticates a person by extracting and converting an individual's specific biometric information—such as fingerprints, iris, sweat gland structure, and blood vessels—which are different for each individual. The multi-biometric recognition technology that combines numerous layers of biometric information has a high security performance, thereby making forgery and falsification virtually impossible. An additional advantage of this technology is that the possibility of theft due to negligence or third-party

23) Young-Sub Cho, Dae-Gi Lee, Hyun-Sook Jin & Gyo-Il Jung, *PKI Gisulhyeonhwang Mit Jeonmang [PKI Technology Status and Prospect]*, 29(3) Mag. IEEE. 91-99 (2002) (In Korean).

24) This shows that the frequency of hacking incidents can overestimated when only focusing on media outlets that emphasizes large number (120,000) of total certificate leaks.

fraud is rather low. Irrespective of how sophisticated the intrinsic security system of the authorized certificate is, there are many cases in which the removable disk that stores the certificate is lost or leaked. On the other hand, multi-biometric authentication is incomparably convenient for users' follow-up management. As such, numerous security technologies with both great stability and convenience are being developed. For example, photoplethysmogram (PPG) certification, Electroencephalography (EGG) certification etc. The argument that "the certified digital signature system that rejects other certificates is justified because the authorized certificate is safe" draws from a logic that overlooks modern security technologies that have numerous attractive alternatives. Rather, the old law prevents the emergence of certificates that provide greater security to Internet users, thereby damaging the long-term safety and trust of electronic documents. Furthermore, considering that 90% of authorized certificate leaks occur in smartphones and that smartphone financial transactions are becoming increasingly popular, a policy that relies on authorized certificates may cause a security crisis.

Second, even if the authorized certificate guarantees the safety and trustworthiness of electronic documents, the old Digital Signature Act unjustly shifts legal responsibility to the consumer. Therefore, it was difficult to regard the transaction security provided by authorized certificates as a true safe and trustworthy digital environment for users. Moreover, under the old law, the authenticity of a document was strongly guaranteed only by the fact that an authorized certificate was used, and it was consumers who were held responsible for transactions even if the document contained a counterfeit signature (in cases of signature theft). Even a transaction that disposes of property with a stolen authorized certificate was treated as a transaction that deserves protection, and the original owner of the authorized certificate was considered responsible for the transaction. 2013DA86489[25] and 2017DA257395[26] are leading cases in this regard.

In 2014, the Supreme Court ruled that even a victim of fraud whose resident registration number, phone number, credit card number, deposit

25) Supreme Court [S. Ct.], 2013Da86489, Jan. 29, 2014 (S. Kor.).

26) Supreme Court [S. Ct.], 2017Da257395, Mar. 29, 2018 (S. Kor.).

account number and password, and security card number and password were all stolen through voice phishing must be held responsible for the fraudster's loan transactions. This was after the scammer took a loan in the victim's name and withdrew the loan to his account. When the lender requested return of the loan to the victim, the Supreme Court ruled against the victim who plead that he had no legal obligations under a frauded contract.

In a similar case in 2017, the Supreme Court once again ruled in favor of the lenders. The key arguments were Article 3, Paragraph 2 of the Old Digital Signature Act, which stipulated the presumed power of authorized certificates, and Article 18-2 of the Old Digital Signature Act, which stipulated the identity verification function of authorized certificates. Because the fraudster used the authorized certificate, it was ruled that the trust of the lender deserves protection, regardless of other circumstances.[27)]

> "Combining the above regulations[28)] and the legislative purpose of securing the safety and reliability of electronic documents and electronic transactions, it can be seen that in transactions using electronic documents, regardless of it being written or sent against one's will, shall be seen as 'sent by the party or the representative of the party' according to the Digital Signature Act Article 7 Paragraph 2."

As such, the court found that a transaction using an authorized certificate is valid without considering the following aspects: (1) the circumstances in which the other party received the authorized certificate, (2) the unusualness of the transaction, (3) or the illegality or incompleteness of the procedure for reissuing the authorized certificate. Of course, criticisms regarding the court's decision were prevalent even before the amendment of the Digital Signature Act. The main criticisms focused on the

---

27) Ki-Chang Kim, Jeonjageumyunggeoraebeobsang 'Iyongja-ui Jungdaehan Gwasil'—Daebeobwon2013Da86489 Pangyeor-ui Munjejeom—['Gross Negligence' under the Electronic Financial Transaction Act of Korea—A critical look at the Supreme Court case 2013Da86489—], 18(3) J. Korea Info. L. (2014) (In Korean).

28) Digital Signature Act Article 3 Paragraph 2, and Article 18-2.

aspect that the above precedent itself represented a misreading of the Loan Business Act and the Electronic Documents Act, as victims of authorized certificate theft could also be protected even without an amendment of the Digital Signature Act.[29)]

However, the old Digital Signature Act played a major role in casting strong responsibilities on users of authorized certificates. Moreover, it is naive to expect that a pre-established e-commerce practice, which presupposes the absoluteness of authorized certificates, can be easily overturned without any amendments. Kim Ki-Chang (2018) also argued that the self-propagation of this legal principle must be blocked with a general amendment of the old law.[30)] Ultimately, the official certificate that was introduced to ensure the stability of Internet transactions became the basis for unjustly transferring transaction responsibilities to users and, thus, a general amendment was required to undo this practice.

In short, although the certified digital signature system could provide stability and trust to digital signatures with excellent security in the short run, (1) such a need is not as great in the modern era as it was in the past, as private security technology has developed to a large extent and (2) it hinders the growth of various security technologies while (3) illegitimately transferring responsibility to users. Consequently, the old law had a potential of harming the stability and trust of the electronic transaction environment in Korea in the long term. Therefore, the standards of electronic document safety and trust are more in keeping with a theoretical basis for an amendment rather than the maintenance of the old law.

2) Activation of electronic document use: a new barrier

The certified digital signature system under the old law functioned as a barrier to the use of electronic documents and electronic transactions in modern Korean society. For a certified digital signature to activate the use of electronic documents, there must be ruling incidents where (1) a citizen will not engage in electronic transactions without an authorized certificate,

---

29) Ki-Chang Kim, *Jeonjamunseobeob Je-7-Jowa Pyohyeondaeri [Article 7 of Korean Electronic Transactions Act and the rule of apparent authority—the problems with Supreme Court Judgment 2017Da257395—]*, 22() J. Korea Info. L. (2018) (In Korean).

30) *Id.* at 130.

or (2) only currently engages in electronic transactions due to the existence of an authorized certificate. In the early days of e-commerce, a certified digital signature fulfilled the above function by guaranteeing transaction safety.

However, from the 2010s onward (before the revision of the old law), incidents that were in contrast to the abovementioned incidents took place. First, complaints were raised that authorized certificates acted as a barrier to smartphone financial transactions and that citizens could not conduct electronic transactions because of authorized certificates. This was because the authorized certificate technology was based on "Active X," which could only properly function with Microsoft Explorer and not on most smartphone devices. Other concerns focused on the inconvenience of foreigner's online shopping on Korean websites due to authorized certificate rules.[31] In the "1st Regulatory Reform Ministerial and Public-Private Joint Regulatory Reform Inspection Meeting" hosted by the Blue House on April 20, 2014[32], the president at the time, Park Geun-Hye, suggested that both Koreans and foreigners must freely conduct electronic transactions without experiencing the inconvenience of authorized certificates. In the "New Government Regulation Reform Promotion Direction" of September 7, 2015, the incumbent President Moon Jae-In announced that the government will create a free Internet environment through the abolition of authorized certificates.[33] Thereafter, in a survey of 3,500 adults in 2018, 41.4% favored the abolition and 17.7% were against the abolition of the certified digital signature system; moreover, over 50% of the respondents chose biometric authentication as their preferred method of

31) The so-called 'Cheon Song-i Coat Incident' has led to the rise of the theory of abolition of public certificates in 2014. The false information that Chinese consumers cannot purchase coats that appear in famous Korean dramas due to domestic shopping malls requiring official certificates has spread through newspaper articles in 2014. Afterwards, various problems related to public certificates and ActiveX were additionally pointed out, leading to the abolition of public certificates.

32) Chung-Sik Jung, Jeonjajeongburon [The Theory of Electronic Government] (1st ed., 2018) (In Korean).

33) Office of Government Policy Coordination, *Daehanminguk Jeongchaek Beuriping. Gyujehyeoksin Toronhoe [Korea Policy Briefing. Regulatory Innovation Forum]*, Korea Policy Briefing (Jul. 27, 2021, 08:30 AM), https://www.korea.kr/news/pressReleaseView.do?newsId=156249614 (In Korean).

authentication.[34)]

As such, in modern society, where digital contracts and e-commerce are already prevalent, the certified digital signature system—which requires the installation of a specific program—may hinder convenience. Thus, it can be said that the existence of an authorized certificate hinders, and does not encourage, e-commerce. Thus, repealing the old law was justified on the grounds that it would promote and smoothen the use of electronic documents.

3) Informatization: reliance on authorized certificates and suppression of innovation

Third, it is self-evident that the certified digital signature system goes against the promotion of informatization. In the past, when the Digital Signature Act was first enacted, "informatization" was automatically achieved by ensuring safety of electronic transactions. In the introductory stages of e-commerce, electronic transactions were unconventional and unfamiliar. If government agencies and legal systems guaranteed the stability of electronic transactions, the number of transactions would increase and, consequently, a lower level of informatization would be achieved. However, in modern society where electronic transactions are already typical, informatization does not expand simply by keeping transactions safe. Informatization is achieved by making non-face-to-face legal transactions more convenient and efficient—that is, by encouraging innovation in information and communication technologies (ICTs). The Digital Signature Act and related systems must also contribute to national informatization via the development and innovation of various certificates.

However, the certified digital signature system causes dependence on authorized certificates and prevents informatization (technological development). Until the old law was repealed, many institutions, mainly public ones, became excessively dependent on authorized certificates. As authorized certificates were used online as identity cards, there have been

34) Incruit Brand Communication Team, *Pyeji Apdun Gongininjeungseo…. Huimang Injeungsudan 2wie Hongchaeinjeung, 1wineun? [Authorized certificate about to be revoked…. Iris authentication second most desired, which is the first?]*, Incruit (Jul. 27, 2021, 08:33 AM), https://info.incruit.com/pr/report_view_mobile.asp?newsno=4090039 (In Korean).

frequent cases of enterprises demanding authorized certificates in other areas where the use of authorized certificates was not compulsory by law.[35] This is because, as mentioned above, the counterparty (business operator) who has verified the authorized certificate benefits from high protection by the court. Consequently, non-authorized certificates were unable to compete fairly with authorized certificates in the certificate market.

Even if the practice of requiring authorized certificates disappears, the competition between certified and non-certified institutions is impossible in a system that ascribes superiority to a certain subject. Irrespective of how superior the security is, the legal effect of a non-authorized signature is weaker than an authorized one due to the systematic interpretation of law. After all, under the old law, the priority of a business operator that produces certificates was not to develop excellent certification technology but to become a licensed authority that produces authorized certificates by meeting the requirements announced by the Ministry of Public Administration and Security and KISA. Even after becoming a certified institution, these institutions had no choice but to prioritize government requirements and the changes therein. Maintaining the status of an authorized certification body was more crucial than technological innovation. In short, the old law ascribed superiority to authorized certificates, which eliminated competition between public and non-authorized certificates. Consequently, security technology and certificate innovation diminished.

4) Improvement in public convenience: causing extreme inconvenience

The issuance and use of authorized certificates is difficult and complicated. The issuance process is done in 10 steps, takes an average of 9 minutes and 40 seconds, and has a short validity period of 1 year. When the validity period expires, users must manually (because it cannot be automatically done) renew the certificate; each time the certificate is used, a password of at least 10 characters, including special characters, must be entered. The procedure for recovering or resetting lost passwords is also rather complicated. Because it is impossible to register an authorized

35) *Supra* note 10, at 304.

certificate on the cloud, users must make various transactions only on one device (e.g., PC) where the certificate is stored or possess a removable disk (e.g., USB) that stores the certificate. Moving or copying certificates to other devices is also complicated. In addition, the authorized certificate uses ActiveX, which works only in a specific computer operating system and web browser. Thus, ActiveX and several other security programs must be installed together. It is common for errors to occur at this installation stage, and ActiveX itself is vulnerable to security problems. It is difficult to list all the inconveniences associated with authorized certificates.

To add on, authorized certificates are not uniformly used in all electronic legal transactions. As mentioned in the introduction, the mandatory use of authorized certificates in various special laws has been abolished. Authorized certificates are mainly used in certain financial transactions and legal acts of the government, including year-end tax settlement. Therefore, while the use of authorized certificates for transactions before the revision of the old law was less frequent than that in the past, a few essential legal transactions (year-end settlement, etc.) required these certificates, so the inconvenience experienced by users increased. Forgetting a complicated password or forgetting the storage location, discarding the existing authorized certificate, and having the certificate reissued by following the 10-step procedure is a typical example. However, despite the complaints that the authorized certificate is too complicated, the abovementioned problems mentioned were not addressed until December 2020, which shows how much an oligopolistic and non-competitive market lacks innovation. In short, all procedures for issuing, installing, using, renewing, reissuing, copying, and transferring an authorized certificate are too complicated compared to other certificates. Although this problem has been discussed by the public and by legislators for over 10 years, there has been no improvement. Thus, as the authorized certificate gradually lost its status as a standard, there was more inconvenience caused.

5) Summary

The certified digital signature system under the old law 1) did not guarantee the safety and trustworthiness of electronic documents in the long term as it shifted the legal responsibility to users to ensure safety and

2) hindered innovation in the certificate market. Further, the inconvenience of signing up and using an authorized certificate has limited the 3) utility of the certificate for citizens and 4) discouraged the use of electronic documents. Therefore, a general amendment to the Digital Signature Act was legitimate and justified. The rationale of a general amendment stated by the National Assembly of the Republic of Korea fully reflects this problem.[36] The evaluation of the old system under the old law in Chapter 3 is summarized in the following table.

Table 1. Drawbacks of authorized certificates under the old Digital Signature Act

Standards	Certified Digital Signature System Under the Old Law
Safety and trustworthiness of electronic documents	Short-term positive, long-term negative Disadvantages of shifting responsibility to consumers and hindering the development of other good certificates.
Enabling the use of electronic documents	Disadvantage: Authorized certificates and ActiveX function as new barriers to electronic contracts
Promotion of informatization	Disadvantage: The informatization of the certificate market is hindered by dependence on authorized certificates and the elimination of innovation incentives
Promoting the convenience of people's lives	Disadvantage: Inconvenient procedures have not been improved, and the benefits of authorized certificates are reducing due to their reduced usage

36) Jeonjaseomyeongbeop [Digital Signature Act], Act No. 5792, Feb. 5, 1999. amended by Act No. 14839, Dec. 10, 2020. Reasons of general amendment: "Authorized certificates were widely used in the early days of the introduction of the digital signature system in Korea and contributed to national informatization such as activation of e-commerce. However, at this point, there are problems such as causing a monopoly of the market, hindering the development of digital signature technology and service innovation, and limiting the people's right to choose various and convenient electronic signature means. To solve this problem, the certified digital signature system is abolished to create conditions where various private digital signature means can compete without discrimination based on technology and services. the electronic signature system will be reorganized from the state-oriented to the private sector to enhance the competitiveness of related industries and expand the people's options."

IV. Major Contents and the Evaluation of the Amended Digital Signature Act

1. Major Contents of the Amended Digital Signature Act

This chapter comprehensively evaluates whether the amended Digital Signature Act has been enacted in a manner that sufficiently achieves the provisions of the general amendment, whether the problems of the old law have been completely corrected, and whether the domestic digital signature environment has been sufficiently improving since the enforcement of the amended law. First, the major amendments to the Digital Signature Act can be summarized as (1) the abolition of the certified digital signature system, (2) the abolition of superior status ascribed to specific certificates, and (3) the introduction of a system for acknowledging compliance with operating standards.

1) Abolition of the certified digital signature system

The amended law deleted all articles of the old law regarding certified digital signatures, authorized certificates, authorized certification work, and licensed certification authorities. Consequently, the Ministry of Science and Technology has not designated a licensed certification authority since the enactment of an amendment. Licensed certification authorities are non-existing terms, along with the ban of authorized certificates. Institutes that issued authorized certificates in the past now issue "joint certificates," and authorized certificates that have already been issued are referred to as joint certificates since the enforcement of the amendment. Of course, the performance and security mechanisms of the two are identical. However, the latter does not enjoy any legal superiority and status of an approved product anymore.

Even under the certified digital signature system of the old law, the use and development of private certificates was not technically prohibited. However, as the practice of relying on authorized certificates was gradually developed, and because Article 3 of the old Digital Signature Act and various special laws provided benefits only to authorized certificates (superior status and mandatory use regulations, etc.), the use of private

certificates inevitably reduced. However, as the certified digital signature system has now been abolished, private digital signature certification institutions have become the main providers of certificates under the amended law. Simultaneously, 22 "digital signature-related" laws were revised[37], most of which were special laws that contained regulations on the use of authorized certificates. Since joint certificates are not a nationally authorized certificates, there is no basis for allowing only the use of joint certificates even for major transactions that guarantee stability.

Table 2. Major contents and an evaluation of the amended Digital Signature Act and the abolishment of the certified digital signature system

	The Old Law	The Amended Law
Basis	Certified digital signature system: Articles regarding "Certified Digital Signature" and "Authorized Certificate" forms the core	Abolishment of the certified digital signature system: Articles regarding national authorization deleted
Host Institution	The Ministry of Science and ICT; KISA	None. Host deleted due to market privatization
Licensed certification authorities	Korea Information Certificate Authority (KICA), Koscom Corporation, Korea Financial Telecommunications and Clearings Institute (KFTC), Korea Electronic Certification (Crosscert), Korea Trade Network (KTNET), National Information Society Agency (NIA)	None. Authorities on the left issue "joint certificates"

37) *Supra* note 12, at 86.

The Ministry of Science and ICT, which previously stipulated security requirements for authorized certificates and the KISA, which distributed digital signature authentication keys to licensed certification authorities, no longer oversee the entire certification system. As described later, the Ministry of Science and ICT only provides non-binding criteria for evaluating the performance of various certificates. KISA evaluates certificates according to these standards, but this evaluation is not a mandatory procedure for the certificate to be distributed in the market.

2) Status of authorized certificates: from superior to equal

The amendment not only eliminated processes regarding national authorization and changed the name of the authorized certificate but also reduced the superior status of the joint certificate (former authorized certificate) by deleting Article 3 of the old law. Instead, the following provision was added. "All digital signatures are not denied because they are electronic, and all forms of digital signatures can be presumed to be signatures and seals according to laws and regulations or agreements between the parties." Now, a joint certificate does not have superior proof power over other certificates just because it is or was "authorized" under the old law. It only enjoys the effect corresponding to its technology and security level.

Of course, this does not imply that all digital signatures have identical effects under the amended law. It simply implies that no certificate is presumed to have a higher validity (a superior status) by law. Thus, all digital signatures can be recognized as valid by the will of the parties, regardless of their security level or algorithmic form, and if a separate agreement does not exist, the effects are decided in light of the overall situation such as types of transactions or technology level.[38] Judgment on what is a valid certificate is also pronounced according to the contract between the parties; if it is not, the technology of the certificate or the concept of transaction are considered. This is an expansion of the general principles of the Korean Civil Law in interpreting a contract.

38) *Supra* note 12, at 96.

Table 3. Major contents and the evaluation of the amended Digital Signature Act and the abolishment of the superior status of certified digital signatures

The Old Law	The Amended Law
Article 3 (Effect of Digital Signature) (1) It shall be deemed that such requirements are satisfied if there is a certified digital signature affixed (2) Where a certified digital signature is affixed, it shall be presumed that there has been no change in the contents of such a message since it has been digitally signed. (3) A digital signature other than a certified digital signature shall have such an effect of a signature, signature and seal, or name and seal, as is agreed between the parties concerned.	Article 3 (Effect of Digital Signature) (1) An electronic signature shall not be denied its effect as a signature, affixed seal, or signed seal just because it is in an electronic form. *Contents regarding former paragraph 2 deleted* (2) If an electronic signature is selected as the form of signature, affixing, or signature in accordance with the provisions of laws and regulations or an agreement between the parties, the electronic signature has the effect of signature or affixed seal.

3) Recognition system for compliance with operating standards

However, if the national authorization system disappears and market is not sufficiently mature to make its own evaluation, the parties will be inevitably confused regarding which certificates to use to establish the legal effect of a contract.[39] It is also unreasonable to leave the market to evaluate the technology and reliability of each certification institute, because the general public only indirectly understands the utility of security technology. In addition, it takes trials and errors for a market evaluation to be valid. Individuals cannot be left out until the market matures. Accordingly, the amended Act established a system for "recognizing" compliance with the operating standards. Among only the certification institutions that voluntarily apply for an evaluation, a recognition can be issued to institutions that meet the requirements announced by the Ministry of Science and ICT.

Under the amendment, the Ministry of Science and ICT will determine

39) Additionally, there hasn't been any evaluation on technology level of non-authorized or newly introduced certification institutions. This is because, under the old law, the effectiveness of certification institution other than authorized certificates could not be properly evaluated.

the operating standards and evaluation standards of digital signature certification institutions by Presidential Decree (Article 10 (5) of the Digital Signature Act) and select an "evaluation institution" to perform the evaluation task. (Article 10, Paragraph 1 of the same Act). Then, the "recognition institution" is selected, which issues a note of recognition to a certification institution that has passed the evaluation of the evaluation institution (Article 9, Paragraph 1 of the same Act). On the date of the revision of the Digital Signature Act, the Ministry of Science and ICT announced the operation standards for digital signature authentication, but this cannot be regarded as a practical examination standard because it is more like a mere abstract requirement.[40] It is expected that the actual evaluation and recognition will depend on the standards and instructions of the Ministry of Science and ICT, which have yet not been announced. The KISA announced that detailed standards will be announced in the second half of 2021.[41] Currently, the KISA has been selected as a "recognition institution," and Korea Information and Communication Technology Association (TTA), Financial Security Agency, and Deloitte (Anjin Accounting Corporation) have been selected as "evaluation institutions." No certification institute has been issued a note of recognition by the "recognition institute" yet.

The recognition system for compliance with operating standards functions in the following manner: (1) A certification business operator can freely apply for evaluation to an evaluation agency. (2) The evaluation institution shall evaluate whether the certification business operator complies with the operating standards and the performance of the authentication technology according to the standards of the preceding Presidential Decree. (3) Evaluation agencies submit their evaluation results

40) Jeonjaseomyeonginjeungeobmu Unyeonggijun [Operational Standards for Digital Signature Recognition], Dec. 10, 2020. Article 4(Use of Appropriate Technologies) Recognized business operator provides a digital signature certification service using technology that meets the requirements of each of the following 1. Possible to identify the signer of the electronic document, etc. For further information, *see* subparagraphs of Article 4.

41) Yun-Hee Kim, *Jeongbu, Gongininjeungseo Daeche Saeobja Pyeonggaje Anchage Juryeok. [Korean Government focues on Establishing a Recognition system that replaces Authorized Certificates]*, ZD Net Korea (Jul. 27, 2021, 08:38 AM), https://zdnet.co.kr/view/?no=20210425183939 (In Korean).

to the recognition agency (KISA). (4) The KISA decides whether to recognize the certification business and (5) issues a note of recognition. This is summarized in the following diagram.

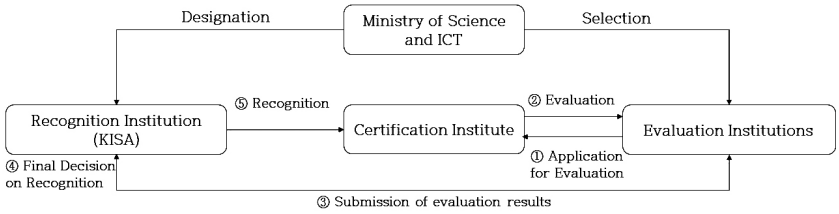

Diagram 1. Major contents of the Amended Digital Signature Act 3: Recognition System for Compliance with Operating Standards[42]

4) Summary

The amended Act abolished the certified digital signature system by collectively deleting regulations related to licensed certification authorities and certified digital signatures. A system for recognizing compliance with standards has been established to provide a means for certification institutes to selectively display their security technology to consumers.

Table 4. Comparison between the old and amended Digital Signature Act

	Under the Old Law	Under the Amended Law
Certified Digital Signature System	Licensed Certification Authority, Authorized Certificates	Elimination of the certified digital signature system
Status of Certificates	Superior status of authorized certificates	Elimination of superior status of any certain certificates
Role of the Government	Selection of "licensed certification authority" and the "Issuer" of authorized certificates	Recognition and evaluation upon request by individual institutions

42) KISA, *Jeonjaseomyeonginjeungsaeopja Injeong · Pyeongga jedo [Digital Signature Certification Business Recognition and Evaluation System]*, KISA (Jul. 27, 2021, 08:42 AM), https://www.kisa.or.kr/business/infor/inforcon_1.jsp (In Korean).

2. Evaluation and Suggestions

The legal system related to digital signatures should contribute to the stability and use of electronic documents, promotion of informatization, and improvement of public convenience. However, the old law did not achieve the above goals, which lead to its general amendments. Now it is necessary to evaluate the amendments under the same standards. It is difficult to accurately measure and evaluate the amendment's impact on the certificate market and the national economy, as less than a year has passed since its enforcement. However, this research analyzes the positive effects and side effects that have already occurred or are expected to occur in the current stage and suggest improvement directions on its own point of view.

1) Safety and trust: improvement of the recognition system and establishment of a reasonable responsibilities sharing structure

The amended law contributes to securing the safety and trustworthiness of an electronic document in two ways. First, by opening the certificate market, customers are provided with certificates with superior security as compared to authorized certificates. Before the revision of the Digital Signature Act, the stability of authorized certificates was under doubt. In a hacking incident in July 2020, five licensed certification authorities—including the Korea Financial Telecommunications and Clearings Institute, Koscom, and Korea Electronic Certification Authority—were hacked and 46,604 authorized certificates were leaked. After receiving the report from the KISA, Vice Chairman Kim Sang-Hee of the National Assembly suggested that the "Advanced Hacking methods against the Authorized certificates," was the presumed cause. As various hacking methods are being tailored specifically to the public authentication system, the certified digital signature system may become more vulnerable. In this case, new authentication technologies with higher stability, such as multi-biometric recognition technology or globally verified certificates, have greater utility. With the opening of the certification market, consumers can utilize both fully verified overseas certificates and innovative certificates without relying on former authorized certificates. This change is expected to secure

the safety and trustworthiness of electronic documents in the long term. Second, customers are less likely to take on unreasonably heavy responsibilities, and victims of certificate theft are less likely to hold responsibilities on contracts based on stolen certificates. This is because Article 3, which states superior authenticity of a certified digital signature, has been deleted, thereby making judgments such as 2013DA86489 or 2017DA257395 impossible.

Of course, the amended law and its system requires certain major improvements. First, the system for recognizing compliance with operating standards must be improved and redesigned. Now that the certified digital signature system has been abolished and the market has not had sufficient time to evaluate the performance of the certificate, transaction safety may be seriously compromised in the short term if this system loses effectiveness. The current recognition system does not clarify itself with regard to the following aspects: (1) the criteria under which the Ministry of Science and ICT selects an evaluation institution, (2) how it materializes the evaluation and operation standards, (3) the reasons for separating the "recognition institution" from the "evaluation institution," (4) identifying who is ultimately responsible for the recognition process, (5) and how to reasonably resolve conflicts of interest regarding the responsibility between two departments.

In particular, the distinction between the "recognition institution" and the "evaluation institution" requires a legitimate explanation. Academia criticizes the spread of responsibility because it creates confusion on who is responsible for recognition failure and only increases the cost of maintaining the system.[43] This is a valid criticism, and for the government to give minimum credibility to recognition work by managing the evaluation and recognition institutions, at least the core responsibility must be centralized. If the evaluation institution is to subsidize the heavy work of the recognition institution, the "recognition institution" must be given the authority to refuse to issue a certificate despite the approval of the evaluation institute. In this case, the recognition institute, KISA, will be the ultimately responsible. Considering that the KISA has played a pivotal role

43) *Supra* note 11, at 13.

in the authorized certificate system, and current evaluation institutions have a relatively brief work experience (and because the continuity of its working period is not guaranteed,), it appears reasonable to put KISA as the final manager in control. Furthermore, KISA has stated that it will design its responsibility standards with reference to international standards. In addition, this research suggests that the KISA adopt the principle of technology neutrality,[44] which is considered an international norm in the field of digital signatures, as one of its evaluation standards.

Next, a reasonable legal responsibility sharing structure must be created. In a transition period after an amendment, various private certificates may present extremely simple passwords, which may increase password leak cases. In this case, a reasonable responsibility sharing system must fairly distribute damages. The most reasonable responsibility sharing structure is achieved by a company's voluntary business policies. If an e-commerce dispute arises in a legal system where the difference in validity between certificates is not stipulated, the court will follow the general principles of the Civil Procedure Act. In this case, the special agreement between the parties is primarily decisive. In numerous cases, companies sign a special agreement to compensate for the loss caused by their simple authentication procedures. Simultaneously, these firms take advantage of market share through their convenient services. In the United States, where the government abandoned the state-led authorization system (a parallel counterpart of the Korean certified digital signature system) in 1995 and actively promoted private certificates, major financial companies, such as Citigroup and Wells Fargo Bank, and card companies, such as Visa and Mastercard, specified the "so-called zero liability policy" in their terms and conditions. The zero liability policy implies a sales strategy to lure customers by requesting a simple certificate from their own company or other companies that indicates that customers will deal with various security incidents at their own costs. The case of the United States suggests that both the convenience and stability of consumers can be guaranteed in

44) Kyoung-Jun Choi, "*UNCITRAL Sinwongwanli Mit Sinloeseobiseu-ui Gugjejeog Seungin-e Gwanhan Gyujeongan"-e Daehan Gochal [A Study of UNCITRAL Draft Provisions on the Cross-border Recognition of IdM and Trust Services]*, 2(1) Korean F. Int'l Trade & Bus. L. 79 (2019) (In Korean).

an autonomous market competition. Similarly in Korea, Toss introduced a "full liability system for customer damage" in June 2020, and Kakao Pay introduced a compensation system for hacking damage in August 2020. In view of the above changes, with the enforcement of the amended law, financial companies may enter a double competition by developing their own certificates to lower the payment barrier on one hand and by bearing the potential damage caused by them on the other hand. The state must promote such competition by guaranteeing fair trade.

Some scholars argue that the Korean digital signature system must distinguish between eligible digital signatures and ineligible digital signatures by referring to the EU eIDAS regulation, which gives only qualified digital signatures the same legal effect as handwritten signatures (EU eIDAS[45] Article 25 (2)) However, this classification system is most likely to become another version of the old Korean system, which differentiated between public and non-public certificates. By imposing such an excessive entry barrier, innovation may be hindered once again. The moment the government distinguishes between eligible and ineligible signatures, the primary goals of private entities become qualification not innovation. Therefore, it is necessary to provide the certification institutes an equal opportunity to receive recognition only up to the level that they choose and unify the responsibilities of the recognition process.

Further, the validity of certificates must be determined in accordance with the general principles of the Civil Act and special agreements among market entities and not by discriminating between the effect of digital signatures by a separate standard. In this case, it is highly likely that both stability and convenience will be guaranteed to consumers. Thus, it is a desirable role of the state under the current Digital Signature Act to not regulate certification institutes and certificates, but to have a clear recognition process and intervene in the market only to catalyze fair competition in times of market failures.

45) The Electronic Identification and Trust Services Regulation.

2) Activation of electronic document use: expectations regarding gradual activation

It is hasty to make final evaluations on whether the amended law has promoted the use of electronic documents. Therefore, in this section, the research provides mere deductions on the impact that the amendment may cause. The amendment can promote the use of electronic documents in transactions where authorized certificates were difficult to be used in the past, such as smartphone financial transactions and insurance. However, it cannot be expected that transactions will increase immediately even in such areas; thus, the short-term effect would be negligible. Most citizens still use unexpired joint certificates because they are familiar to them. An example is year-end tax settlement. In the settlement of January 2021, when the use of private certificates was permitted for the first time, the use rate of joint certificates reached 88%. Of the 81.07 million certificates used, 71.06 million were joint certificates, followed by 5.86 million Kakao certificates, and 2.4 million PASS certificates. However, considering that over 50% of the citizens who used private certificates, like Kakao Certificates, are distributed to be aged in their 20s–40s, the use of private certificates is expected to increase in the future. Many experts predict that the conversion to private certificates will increase from 2022 onward, when the previously issued joint certificates expire. As such, the amended Digital Signature Act can positively contribute to revitalizing the use of electronic documents in all areas of electronic contracts both in the short and long terms. However, rather than drawing hasty conclusions, a cautious observation is required.

3) Informatization: maturation of the certificate market

Certification institutions are releasing various private certificates and securing significant market share. As of December 2020, 22 million PASS certificates (jointly developed by the three telecommunication companies; SK, KT, and LG), 20 million Kakao certificates, and 2 million Naver certificates were issued. TOSS, which first entered financial services in 2015 through "quick money transfer," issued 23 million certificates. On the other hand, BankSign, an authentication service jointly developed and introduced by 16 domestic conventional banks, has only 300,000 users and is in danger of being eliminated from the market. Such a market landscape

reveals the potential for innovation in the private certificate market. This is because the market share is determined by the utility provided to consumers, not by any former recognition. Although BankSign is a safe certificate that can be used by all 16 banks participating in the development, it is being ignored in the market due to various inconveniences. BankSign is slower than other certificates, cannot be duplicated and used on multiple devices, and has poor compatibility with banking applications. This exemplifies the research result that when customers select a payment service in an electronic transaction, convenience of service is considered the most important factor in various stages, such as payment information input, service entry, identity verification, and payment completion.[46] The fact that Kakao certificates, which have lower approval from the financial market than traditional banks, are well received in the market is also due to the convenience of being linked to Kakao platforms such as KakaoTalk and Kakao Bank.

Further, technological advancement and diversity in this market are also evident. For example, the Kakao Certificate combines blockchain technology with public key infrastructure.[47] NHN Payco Certificate improved its security by storing certificate usage history on a cloud blockchain. KB certificate combined biometrics and patterns. When the above competition continues, the "activation of the use of various digital signature methods," specified in Article 6 of the amended Digital Signature Act, may be sufficiently achieved. Several studies express disappointment that Article 6 of the Amended Act has not been sufficiently materialized.[48] The Article is insufficient to act as a guideline for government intervention. However, considering that the market competition has matured, as described above, within six months after the amendment, the state

46) Na-Rae Kim & Jae-Young Yun, *Moba-il Ganpyeon Gyeolje Seobiseu-ui Ganpyeonseong-gwa Bo-anseong-i Seonhodo-e Michi-neun Yeonghyang-e Daehan Yeongu [The Effect of Easiness and Security on Preference of Mobile Easy Payment Service]*, 15(1) J. HCI Soc'y. Korea. 34 (2020) (In Korean).

47) Ji-Young Lee, *Gongininjeungseo Binjari nuga? Beullokchein Giban Injeung Seobiseu Itdan Yego [Who Fills the Vacant Seat of Authorized Certificates? A Series of Notices of Blockchain-based Authentication Services]* (Jul. 27, 2021, 08:55 AM), https://www.mk.co.kr/news/economy/view/2020/05/536989/ (In Korean).

48) *Supra* note 12, at 108.

intervention at this stage has little benefit compared to the side effects. The certificate market autonomy policy has been rather successful thus far.

4) Improvement in public convenience: solving transitional and versatility problems

Lastly, the amended law is contributing to the improvement of convenience and utility by minimizing confusion in the transitional period and promoting convenient certificate development. The amended law did not discard all previously issued authorized certificates at once. Rather, it retained them by converting them into joint certificates. In electronic contracts, an individual can compare the inconvenience of an authorized certificate with the inconvenience of certificate conversion and use a certificate that meets their needs and interests. In this manner, the inconvenience of the transition period is reduced by half.

Of course, there are often situations in which a user must issue a new certificate each time because private institutions release different certificates and the certificates requested by institutions may differ. It is unlikely that a universal certificate will appear. However, the inconvenience caused by an individual having to use multiple certificates is less than the inconvenience caused by former authorized certificates. First, since the amendment is still in the early stages of enforcement, a partnership agreement between markets and private certificate services has not been sufficiently concluded. The above inconvenience will decrease as private certification institutions enter into various alliance agreements for the purpose of sales and as they expand the versatility of their products. Even if the versatility of the certificate is not improved, the inconvenience is offset if the method of issuing and using each certificate is sufficiently convenient. A platform operator or individual bank may not accept a competitor's certificate, and a financial institution may force the use of its own certificate if it operates a certification business in parallel. However, they must streamline the certification process to facilitate the use of their services.

5) Summary

With the enforcement of the amended law, competition in the digital signature certificate market has expanded. Various authentication and security technologies are being developed (3)), and the public is freed from

Table 5. Evaluation of and suggestions for improvements in the amended Digital Signature Act

Evaluation Standard	Evaluation	Suggestions
Safety and Trust	- Beneficial for long-term safety - Just distribution on responsibilities required - Responsible party unclear regarding the recognition system - Insufficient evaluation criteria of the recognition system	- Maintain market-orientation - Legal responsibility distribution based on general principles of Civil Law - Unification of responsibility to KISA - Adopt technology neutrality
Electronic Documents	- Currently difficult to accurately evaluate activation	- Maintain the current system - Further examination required
Informatization	- Ideal competition witnessed in the certificate market - Declarative articles are sufficient	- Minimal intervention in cases of market failure Revision of Article 6 unnecessary
Public Convenience	- Minimized transitional confusion through joint certificates - Versatility inconvenience offset by convenience of individual certificates	- Maintain the current system

various inconveniences caused by authorized certificates (4)). However, the current recognition system vaguely determines the responsibilities between the evaluation institution and the recognition institution, while not disclosing any specific evaluation guidelines. Consequently, it is impossible to even predict which certification business will be issued a note of recognition. If confusion becomes severe, the standard of a certificate that the public can trust will disappear and the stability and trust of electronic documents may be greatly damaged (1)) in the short-term. Therefore, beginning with the unification of responsibilities of the recognition system to the KISA, practical evaluation standards must be established as soon as

possible. The government must provide sufficient notice so that the recognition institution and the general public can recognize it. The immediate problem of lacking compatibility of certificates (2)) needs to be discussed again after practice matures. The above evaluations and suggestions on the digital signature and certificate market under the amended Digital Signature Act are summarized in the table below.

V. Conclusion

This paper derived the criteria for judging the appropriateness of the Korean Digital Signature Act from domestic and foreign legal documents and then evaluated both the old and amended Digital Signature Acts based on this standard. The Korean Digital Signature Act must be evaluated based on whether it guarantees the safety and trust of electronic documents, on whether it expands the use of electronic documents, on whether it contributes to national informatization, and on whether it contributes to the improvement of public convenience. By satisfying the above four criteria, digital signatures can perform similar functions to written signatures.

The certified digital signature system under the old Digital Signature Act was a system in which the government designates licensed certification authorities. The KISA granted digital signature verification keys to the authorities and the system guaranteed superior status only to certificates issued by the authorized certification institutions. However, in the process of guaranteeing the superior status, responsibility was unjustly shifted to users and certificates were differentiated based only on whether they were publicly recognized regardless of the level of security technology. It was an inadequate system to guarantee the safety of electronic documents in the long term. Licensed certification authorities, which had no incentive to innovate, long neglected the inconvenient issuance process of their certificates and associated technical problems (ActiveX, etc.). A general amendment was reasonable because the old law functioned as a key element of a system that failed to meet all four criteria.

Accordingly, on December 10, 2020, the fully amended Digital Signature Act came into force. The market-led certification system under the

amended law effectively improved the problems of the old law and buffered its disadvantages relatively well. Furthermore, it has the potential to achieve the original goal of the Digital Signature Act—for example, stability of electronic documents, expansion of the use of electronic documents, informatization, and public convenience.

However, this optimism presupposes the following aspects: First, if the evaluation and recognition institutions are to be operated separately, at least the responsibility between the two should be clearly defined and unified; moreover, a clear evaluation standard must be established. Second, a sound competitive order must be established so that deregulation does not lead to unfair trade or abuse of market power. Currently, multiple certification institutes are launching different certificates and, thus, entering the market competition. In addition, the fruits of competition (stability and convenience) are being shared with consumers owing to the emergence of companies that introduce policies that resemble the zero-liability system of the US. It appears that the purpose of the Digital Signature Act can be sufficiently achieved just by monitoring the certificate market and preventing market failure.

With the spread of COVID-19, the demand for electronic legal activities is now greater than ever. Electronic legal practices are no longer 'to be introduced' but 'to be more naturally permeated into our daily life.' As the goal of the Digital Signature Act is to ensure that digital signatures can be treated equally to written signatures, the purpose of laws related to the online environment is to resolve the legal gap between virtual and physical environments. This is because the private autonomy, basic rights, and legal stability of members of modern society can be extended to digital areas only when the gap is resolved. The abolition of authorized certificates and autonomy of the certificate market is a significant beginning. This does not imply that state intervention must be minimized in all electronic transactions. As the state establishes a registration system to make certain transactions trustworthy, certain electronic legal transactions may require specific certificates. However, in a free-market economy society, state intervention is an exception and individual freedom is the principle; thus, the distribution of responsibilities in accordance with freedom must be done fairly. The research concludes with the provision that a fair distribution of responsibilities must follow, as freedom in the selection of

digital signatures and certificates has been established as a governing principle in the amendment.