Electronic Transactions Act
and Digital Signature Act:
Background, Major Provisions and Implication

OECD Forum on Electronic Commerce, 12~13 October 1999, Paris

October 1999

Ministry of Information and Communication
Republic of Korea
1. **Background**

The explosive growth of the Internet brought the emergence of e-commerce at a rapid pace as the new mode of commerce transcends the restrictions of time and space. According to an OECD report, the combined worth of business-to-business and business-to-consumer transactions conducted over the Internet is projected to increase from 26 billion dollars in 1997 to 330 billion dollars in 2002.

Although domestic e-commerce markets are in an initial step, they are rapidly expanding. For example, the National Computerization Agency of Korea forecasted that the size of the e-commerce market would increase from 60 million dollars in 1998 to 3,150 million dollars in 2002. Meanwhile, WEFA, an economic agency based in the United States, prospected that the size of the e-commerce market in Korea will expand from 354 million dollars in 1998 to 2,168 million dollars in 1999, and to 9,613 million dollars in 2003.

E-commerce is fundamentally different from the conventional commercial transactions based on face-to-face interaction and document exchange. As e-commerce spreads rapidly, nations began to review the methodology, practices and rules applicable in conventional transactions and are focusing on readjusting their legal settings to create an environment more conducive to e-commerce.

The Government of Korea, having recognized the importance of e-commerce, enacted in December 1998 the Electronic Transactions Act and the Digital Signature Act with a view to promoting e-commerce nationwide and lending digital transactions legal predictability and security, which became effective from July this year.

The purpose of the Electronic Transactions Act is, by giving electronic documents an equal level of legal validity as paper documents and by regulating basic matters related to achieving reliability, protecting consumer rights and implementing policies to promote e-commerce, with a view to creating a legally predictable environment in which the private citizens can make secure transactions in the Information Age.

The Digital Signature Act regulates matters related to digital signature and certification considered as the essential tool to confirm the identity of the other party and guarantee the integrity and authenticity of the digitally signed documents. The Digital Signature Act was enacted to achieve security and reliability of electronic documents and thereby facilitate e-commerce.

Both Acts were enacted to promote e-commerce but are different in terms of basic objectives. While the Electronic Transactions Act provides for general and policy measures to promote e-commerce, the Digital Signature Act focuses on achieving security and reliability of digital documents with clear provisions regarding digital signature technologies and the designation and management of the accredited certification authorities.

2. **Major provisions**
(1) The Electronic Transactions Act

The Electronic Transactions Act is divided into six chapters of General Provisions, Electronic Messages, Security for E-commerce, Promotion of E-commerce, Consumer Protection and Supplementary Provisions. The major provisions are as follows.

First, except for cases for which other laws provide specifically, electronic documents have the same level of legal effect as written paper documents and the digital signatures are equally valid with signatures written down on paper documents.

Second, only a minimum level of legal restrictions have been laid out as for the time and place of dispatch and receipt of electronic messages, messages deemed sent by the author, individuality of electronic messages received and acknowledgement of receipt, taking into account that the specifics are subject to change according to the terms of individual contracts between the parties.

Third, the parties to electronic transactions must obtain the expressive consent of the other party before collecting personal information on him or her in matters related to e-commerce and shall not use the collected information for purposes other than conducting electronic transactions.

Fourth, in order to protect users’ basic consumer rights, the Electronic Transactions Act includes provisions that require the service provider to make available information users need to make informed decisions and guidelines for damage payment.

Fifth, building infrastructures necessary for the promotion of e-commerce should be led by private initiatives in principle. In order to support the private initiatives, the Electronic Transactions Act stipulates that the government organizes the Policy Committee on E-commerce and draws and implements measures to promote e-commerce.

In addition, it provides that the government establishes the Korea Institute for E-commerce with a mandate to carry out research activities on e-commerce and study policy measures on dispute settlement with a view to developing redress mechanism and helping fair trade practices take firm root.

(2) The Digital Signature Act

The Digital Signature Act is divided into six chapters of General Provisions, Accredited Certification Authorities, Certificate, Achievement of Security and Reliability of Certification Practice, Supplementary Provisions and Penal Provisions. The major provisions are as follows.

First, the first chapter defines that “digital signature” means information created by a private key using an asymmetric cryptography technology and recognizes the legal validity of digital documents and signatures.
Second, with a view to laying out the legal settings for the secure use of digital signatures the second chapter provides for the introduction of the accredited certification authorities system and offers provisions necessary to deliver appropriate and consistent accreditation services.

Third, the provisions of the third chapter stipulate the information that a certificate must contain and details of the procedures for the issuance, suspension and revocation of a certificate in order to achieve reliability.

Fourth, in order to achieve the secure use of digital documents and signatures and settle potential disputes, Chapter 4 provides for the obligations and responsibilities of the certification authorities including the maintenance of a secure and reliable certification system and the secure management of the private key and certificate-related records.

Chapter 4 also recognizes the importance of protecting the private key for the enforcement of the accreditation system in a safe and effective manner, and prohibits the fraudulent use of other person’s private key and being issued with a certificate in the name of other person. Chapter 6 provides for penalties for actions in violation of these rules.

Fifth, taking into account the fact that the increased demand for certification services and advances in information technology makes it increasingly easier to collect, process, store and distribute private information, the Digital Signature Act includes provisions to limit the collection of private information to the extent necessary to carry out the certification practice. It also prohibits using or disclosing collected personal information for any purpose other than certification practice, and prescribes that in case anyone violates these rules, he or she is punished.

Sixth, with a view to creating a secure digital environment and for effective management of certification authorities, the Digital Signature Act designates the Korea Information Security Agency to supervise the certification system.

Seventh, the Digital Signature Act includes provisions on mutual recognition with foreign certification authorities with a view to promoting domestic e-commerce through global harmonization.

3. Implication

The greatest significance of the Electronic Transactions Act and the Digital Signature Act is that they provide a stable legal platform for the electronic merchants and buyers so that they can use digital media in commerce with confidence.

The Electronic Transactions Act is divided largely into three parts: electronic documents and their security, promotion of electronic transactions and consumer protection. The first part is to complement the areas that had remained largely ambiguous from the perspectives of both the consumer and the service provider.
The second part on the promotion of electronic transactions covers the supporting role of the government in such fields as standardization, technology development, assisting relevant organizations and dispute settlement.

Finally, the provisions on consumer protection are intended to facilitate e-commerce by promoting user confidence. Provisions to this end require that consumers be given information equal to that held by the service providers and that redress mechanism be established.

The Digital Signature Act expressly recognizes the legal effect of digital documents and signatures certified by the accredited certification authorities designated by the government, and thereby provide a legal platform for current and future legal actions carried out over the electronic media and communications network.

In the case that an existing law requires certain documents bear a seal and a signature to prove their authenticity, electronic signatures are regarded as a legitimate substitute for a seal or a signature.

In particular, even in the case of legal actions carried out over an open network such as the Internet, digital signatures can be inferred to as the legitimate means, which confirms the identity of, and the decisions made by the parties involved.

As a result of the implementation of the Electronic Transactions Act and the Digital Signature Act, related businesses are expected to develop. More specifically, the accredited certification authorities will be designated following the adoption of the Digital Signature Act. It is likely that the Korea Financial Telecommunications & Clearing Institute and the Korea Securities Computer will be selected as the certification authorities in finance and securities service, respectively.

In addition, the Korea Information Certificate Authority, Inc., a consortium of 22 private companies, was recently founded and is planning to start providing certification services by the end of 1999 as an accredited certification authority.

However, since non-accredited organizations can carry out certification practice under the Digital Signature Act, in prospect, a number of small and medium sized non-accredited certification authorities will co-exist as the demand for certification services increases in the future.