Democratic People's Republic of Korea

Electronic Certification Law

Adopted by Decree No. 2038 of the Standing Committee of the Supreme People's Assembly on December 14, 2011

Revised and supplemented by Decree No. 1492 of the Standing Committee of the Supreme People's Assembly on December 5, 2023

Chapter 1: Basics of the Electronic Certification Law

Article 1 (Mission of the Electronic Certification Law)

The Electronic Certification Law of the Democratic People's Republic of Korea aims to establish strict systems and order in electronic certification operations to ensure the safety of data communication networks and electronic transactions, thereby contributing to the informatization of the people's economy.

Article 2 (Definitions)

The definitions of terms in this law are as follows:

1. **Electronic certification** refers to the electronic verification of the identity of subscribers to data communication networks or electronic transaction systems, and the accuracy of electronic transactions.
2. **Electronic transaction** refers to transactions conducted by exchanging electronic data.
3. **Electronic data** refers to data that can be created, processed, transmitted, or stored using information processing devices such as computers.
4. **Subscriber** refers to institutions, enterprises, organizations, and citizens who subscribe to data communication networks or electronic transaction systems.
5. **Electronic signature** refers to electronic information attached to electronic data that verifies the signer of the electronic data and the signer's approval of the content of the electronic data.
6. **Electronic certification key** refers to information or devices used to verify identity or create electronic signatures.
7. **Electronic certificate** refers to electronic information that certifies the identity or qualifications of subscribers.

8. **Electronic certification institution** refers to institutions that provide electronic certification services.

Article 3 (Principles of Establishing Electronic Certification Systems)

Establishing proper electronic certification systems is a crucial condition for ensuring the safety of data communication networks and electronic transactions. The state shall establish and manage the national electronic certification system in a unified and rational manner.

Article 4 (Strengthening the Material and Technical Foundation of Electronic Certification Operations)

The state shall increase investment in electronic certification operations in line with the demands of current development and actively adopt advanced scientific and technological achievements to strengthen the material and technical foundation of electronic certification operations.

Article 5 (Guidance on Electronic Certification Operations)

Unified guidance on electronic certification operations shall be provided by the central electronic certification guidance institution. The central electronic certification guidance institution shall strengthen control and guidance over electronic certification operations, standardize and regulate electronic certification operations, and further complete the sector structure and functions of the electronic certification system.

Article 6 (Supervision and Control of Electronic Certification Operations)

Supervision and control over electronic certification operations shall be carried out by the central electronic certification guidance institution and relevant supervision and control institutions. The central electronic certification guidance institution and relevant supervision and control institutions shall strictly supervise and control the state of electronic certification operations.

Article 7 (Exchange and Cooperation)

The state shall develop exchanges and cooperation with other countries and international organizations in the field of electronic certification.

Article 8 (Application of the Law)

This law applies to institutions, enterprises, organizations, and citizens who manage, operate, or use data communication networks or electronic transaction systems. It also applies to international organizations, institutions, enterprises, and citizens of other

countries who use our country's data communication networks or electronic transaction systems.

Chapter 2: Subjects and Methods of Electronic Certification

Article 9 (Subjects of Electronic Certification)

The subjects of electronic certification in data communication networks or electronic transaction systems are as follows:

1. Identity and qualifications of subscribers
2. The physical existence of computers and other terminal devices
3. The signer of electronic data and the accuracy of the data content
4. Other subjects determined by the central electronic certification guidance institution

Article 10 (Classification of Electronic Certification Grades)

Electronic certification grades are divided into 1st, 2nd, 3rd, and 4th grades according to the importance of the subjects of electronic certification. The criteria for dividing electronic certification grades are separately determined.

Article 11 (Institutions for Establishing Electronic Certification Grades)

Electronic certification grades are determined by institutions, enterprises, and organizations that operate data communication networks or electronic transaction systems. However, grades for subjects of electronic certification that require nationwide uniformity are determined by the central electronic certification guidance institution. The central electronic certification guidance institution and relevant institutions, enterprises, and organizations shall properly determine electronic certification grades and scientifically conduct electronic certification operations.

Article 12 (Issuance of Electronic Certification Keys and Electronic Certificates)

Institutions, enterprises, organizations, and citizens who wish to subscribe to data communication networks or electronic transaction systems shall register their identity, qualifications, and unique identification information of computers and other terminal devices with the electronic certification institution and receive electronic certification keys and electronic certificates. The procedures for issuing electronic certification keys and electronic certificates are separately determined.

Article 13 (Management of Electronic Certification Keys)

Subscribers shall safely manage and use electronic certification keys according to established order and shall not transfer the usage rights to others. If electronic certification keys are lost, misused, or there is a possibility of misuse, subscribers shall immediately stop using them and notify the relevant electronic certification institution. Institutions, enterprises, organizations, and citizens shall not misuse the electronic certification keys issued to other subscribers.

Article 14 (Suspension, Recovery, and Disposal of Electronic Certificates)

Subscribers may request the suspension, recovery, and disposal of electronic certificates issued by the electronic certification institution as needed. If the content recorded in the electronic certificate changes due to reasons such as retirement or transfer, subscribers shall promptly notify the electronic certification institution.

Article 15 (Methods of Certifying Subscriber Identity and Computer Existence)

The certification of subscriber identity and the existence of computers and other terminal devices shall be conducted using electronic certificates to prove the ownership of electronic certification keys. In this case, the confidentiality of electronic certification keys shall not be disclosed.

Article 16 (Methods of Certifying Electronic Data)

Subscribers who create or approve electronic data shall sign the electronic data with electronic certification keys and then send or store it. Subscribers who receive electronic data shall verify the electronic signature of the relevant electronic data using electronic certificates to confirm the signer and the signer's approval of the data content. If certification of the creation, approval, sending, receiving, and storage time of electronic data is required, subscribers shall request certification from the electronic certification institution.

Article 17 (Effectiveness of Electronic Copies)

Electronic data input by electronically copying paper documents can be used as proof of electronic transactions if the copier, copy date, and identity with the original can be confirmed by electronic signature.

Article 18 (Effectiveness of Electronic Signatures)

Electronic signatures have the same effectiveness as stamping or signing paper documents if the following conditions are met:

1. The electronic certification key used for the electronic signature must be the unique possession of the signer at the time of signing and must be used only by the signer.

2. After signing the electronic data, it must be possible to confirm whether the electronic signature and electronic data have been changed.

Article 19 (Legal Effectiveness of Electronic Data)

Electronic data has legal effectiveness if the following conditions are met:

1. The content of the electronic data must be accessible and searchable as needed.
2. The accuracy of the preservation of the electronic data content must be confirmed.
3. The creator, sender, receiver, time, and place of the electronic data must be confirmed.

Article 20 (Senders and Receivers of Electronic Data)

The person who approves the sending of electronic data, the person who manages the information system that automatically sends electronic data, and the person confirmed as the sender by prior agreement between the parties to the transaction shall be the sender. The person designated to receive electronic data from the sender shall be the receiver. The intermediary of the transmission of electronic data shall not be the sender or receiver.

Article 21 (Sending and Receiving Time of Electronic Data)

The sending time of electronic data is the time when the electronic data leaves the information system controlled by the sender. The receiving time of electronic data is the time when the electronic data becomes accessible at the address designated by the receiver. However, if the receiver has not designated an address, the receiving time is the time when the receiver accesses and becomes aware of the content of the electronic data. If the parties to the transaction have separately agreed on the sending and receiving time of electronic data, the agreement shall be followed.

Article 22 (Sending and Receiving Locations of Electronic Data)

The basic location of the sender shall be the sending point of the electronic data, and the basic location of the receiver shall be the receiving point of the electronic data. If the parties to the transaction have separately agreed on the sending and receiving points of electronic data, the agreement shall be followed.

Article 23 (Recognition of Reliability of Electronic Data and Electronic Signatures from Other Countries)

The recognition of the reliability of electronic data and electronic signatures from other countries shall be based on recognized international standards and treaties to which our

country is a party, and shall be conducted by the central electronic certification guidance institution.

Article 24 (Approval and Standardization of Electronic Certification Means)

Institutions, enterprises, organizations, and citizens who develop or update programs and devices related to electronic certification shall obtain approval from the central electronic certification guidance institution before selling, distributing, or using them. When establishing standards related to electronic certification, the agreement of the central electronic certification guidance institution shall be obtained.

Article 25 (Registration of Data Communication Networks and Electronic Transaction Systems)

Institutions, enterprises, and organizations must establish security measures, including electronic authentication, before operating data communication networks or electronic transaction systems and register with the Central Electronic Authentication Guidance Agency. Changes to registered content must also be re-registered with the agency.

Article 26 (Fees for Electronic Authentication Services)

Subscribers who receive electronic authentication keys and certificates must pay the prescribed fees. The fee-setting business is handled by the state pricing agency.

Chapter 3: Electronic Authentication Agencies

Article 27 (Application for Electronic Authentication Services)

Institutions, enterprises, and organizations wishing to provide electronic authentication services must have the necessary facilities, equipment, and material and technical conditions and submit an application for electronic authentication services to the Central Electronic Authentication Guidance Agency.

Article 28 (Review of Applications for Electronic Authentication Services)

The Central Electronic Authentication Guidance Agency, upon receiving an application for electronic authentication services, must review whether the conditions for providing such services are sufficiently met and approve or reject the application. If approved, an electronic authentication service permit specifying the content and scope of the service will be issued.

Article 29 (Qualifications of Electronic Authentication Agencies)

Institutions, enterprises, and organizations that have received approval for electronic authentication services hold the qualifications of electronic authentication agencies and can issue electronic authentication keys and certificates, as well as verify their validity.

Article 30 (Preparation and Registration of Electronic Authentication Service Rules)
Before providing services, electronic authentication agencies must prepare electronic authentication service rules and register them with the Central Electronic Authentication Guidance Agency. Any changes to these rules must also be re-registered.

Article 31 (Ensuring the Safety of Electronic Authentication Services)
Electronic authentication agencies must inform subscribers of service-related matters and provide safe and normal electronic authentication services. In case of accidents during the service process, they must immediately notify the Central Electronic Authentication Guidance Agency and take appropriate measures. If the safety of data communication networks or electronic transaction systems is compromised, the agency must take measures such as invalidating the relevant electronic certificates.

Article 32 (Suspension of Electronic Authentication Services)
Electronic authentication agencies wishing to suspend services must obtain approval from the Central Electronic Authentication Guidance Agency. Subscribers must be notified of the suspension 30 days in advance.

Article 33 (Delegation of Electronic Authentication Services)
With approval from the Central Electronic Authentication Guidance Agency, electronic authentication agencies can delegate part of their services to other institutions, enterprises, or organizations. The delegated entities must provide services within the scope of the delegation.

Article 34 (Storage and Management of Electronic Authentication Service Records)
Electronic authentication agencies must securely store and manage service records and subscriber information for a specified period. These records and information must not be altered, deleted, or leaked. Access to these records and information requires approval from the Central Electronic Authentication Guidance Agency.

Chapter 4: Legal Responsibilities

Article 35 (Compensation for Damages)
If damages occur during the electronic authentication service process due to the fault of the electronic authentication agency or the subscriber, the responsible party must compensate for the damages.

Article 36 (Fines)
Fines are imposed for the following actions related to electronic authentication subjects of grade 2 or lower:

1. Allowing unauthorized persons to use electronic authentication keys or failing to re-register changes with the electronic authentication agency within the specified period: 100,000 to 500,000 won for institutions, enterprises, and organizations; 5,000 to 10,000 won for citizens.
2. Mismanagement of electronic authentication keys resulting in theft: 100,000 to 200,000 won for institutions, enterprises, and organizations; 5,000 to 10,000 won for citizens.
3. Using electronic authentication keys issued under another subscriber's identity: 200,000 to 1,000,000 won for institutions, enterprises, and organizations; 10,000 to 50,000 won for citizens.

Article 37 (Suspension Penalties)
Operations are suspended in the following cases:

1. Selling, distributing, or using electronic authentication-related programs or devices without approval.
2. Establishing or operating data communication networks or electronic transaction systems without registering or obtaining approval for electronic authentication-related standards.

Article 38 (Warnings and Severe Warnings)
Warnings are issued for the following actions:

1. Failing to properly establish electronic authentication grades for each subject.
2. Not using electronic authentication means that match the established grades. Severe warnings are issued if the actions are particularly serious.

Article 39 (Unpaid Labor and Labor Education Penalties)
The following actions result in penalties of up to three months of unpaid labor or labor education:

1. Submitting false information to obtain electronic certificates.
2. Engaging in actions specified in Article 36 related to electronic authentication subjects of grade 3 or higher.
3. Selling, distributing, or using electronic authentication-related programs or devices without approval, or arbitrarily modifying approved programs or devices.
4. Issuing electronic certificates or altering, deleting, leaking, or destroying service records and subscriber information in violation of established procedures.

5. Operating data communication networks or electronic transaction systems without registering with the Central Electronic Authentication Guidance Agency. Severe cases result in penalties of more than three months of unpaid labor or labor education.

Article 40 (Dismissal, Removal, and Disqualification Penalties)
Severe violations of electronic authentication order resulting in serious consequences lead to dismissal, removal, or disqualification of the responsible party.

Article 41 (Criminal Responsibility)
Actions violating this law that constitute crimes are subject to criminal responsibility under the relevant provisions of the criminal law.

Chapter 5: Supplementary Provisions

Article 42 (Effective Date)
The amended Electronic Authentication Law, adopted by Decree No. 1492 of the Standing Committee of the Supreme People's Assembly on December 5, 2023, shall take effect on December 20, 2023.