

Electronic Signature Law of the People's Republic of China

(Chairman Order of the People's Republic of China, No. 18)

“Electronic Signature Law of the People's Republic of China”, adopted at the 11th Meeting of the Standing Committee of the 10th National People's Congress of the People's Republic of China on August 28, 2004, is hereby promulgated and shall go into effect as of April, 1st, 2005.

Hu Jin Tao

President of the People's Republic of China

August 28, 2004

Electronic Signature Law of the People's Republic of China

(Adopted at the 11th Meeting of the Standing Committee of the 10th National People's Congress on August 28th, 2004)

Content

- Chapter I General Provisions
- Chapter II Data Message
- Chapter III Electronic Signature and Authentication
- Chapter IV Legal Responsibility
- Chapter V Supplementary Provisions

Chapter I General Provisions

Article 1 This law is enacted in order to establish the legal effect of electronic signature and protect lawful interests of parties involved by standardizing the behavior of electronic signers.

Article 2 The so called electronic signature in the law means the content data, in the form of electronic message, contained in and attached to a data message, to identify the signer and indicate that the signer accepts the content data.

The so called data message in the law means message created, sent, received or stored in the forms of electronic, optical, magnetic and similar methods.

Article 3 The parties may or may not use electronic signature and data message in their contracts or any other documents of papers, bills and so on in their civil activities according to their agreement. The parties that have agreed to utilize documents of electronic signature and data message shall not deny the legal effect of the papers for the adoption of electronic signature and data message.

The above provisions are not applicable for the following papers:

1. Papers relating to personal relations of marriage, adoption and heirdom and so on;
2. Papers relating to estate transfers of lands and houses;
3. Papers relating to suspension of public utility services of water, heat, gas and electrical power and so on;
4. Any other cases not applicable for electronic message stipulated by laws and administrative regulations.

Chapter II Data Message

Article 4 Any data message that is able to tangibly manifest the carried content and be available for query at any time shall be regarded as the written form satisfactory to laws and regulations.

Article 5 Any data message that satisfies the following requirements shall be regarded as the original form satisfactory to laws and regulations:

1. Messages able to manifest their content and be available for query at any time;
2. Messages that may reliably guarantee content intact and unchanged ever since they were created. However, any form of changes of endorsement, data exchange, data storage

and data display shall not influence their integrity.

Article 6 Any message that satisfies the following requirements shall be regarded as satisfying document storage laws and regulations.

1. Messages able to manifest their content and be available for query at any time;
2. Messages that are the same as they are created, sent and received in format or, if not the same in format, can actually manifest the content originally created, sent and received;
3. Messages that can identify the data message senders and receivers and the time of message sending and receiving.

Article 7 As evidence, data messages shall not be rejected in excuse of their being created, sent, received or stored by means of electronic, optical and magnetic methods.

Article 8 The following factors shall be taken into account when examining the facility of a data message as evidence:

1. Reliability of method to create, store or transmit the data message;
2. Reliability of method to retain content integrity of the data message;
3. Reliability of method to identify the data message sender;
4. Other factors related.

Article 9 The data message shall be regarded as the message sent by the sender in the case that one of the following events happens:

1. It is sent with an authorization of the sender;
2. It is sent automatically from the information system of the sender;
3. It is found to be identical when the receiver validates it in accordance with the validation method agreeable to the sender.

Parties shall observe their own agreement in case they have separate agreement on the items regulated above.

Article 10 The data messages that require confirmation of due reception according to laws and regulations or agreements by the parties shall be confirmed for due reception. The data message shall be regarded as being dully received when the sender receives the receipt from the receiver.

Article 11 It shall be regarded as the sending time when a data message goes into a message system out of the sender's control.

In the case that a receiver has designated a specific system to receive the data message, it shall be regarded as the data message receiving time when the data message enters the designated system. In case a receiver has not designated a specific system to receive the data message, it shall be regarded as the data message receiving time when it initially enters any system of the receiver.

The parties shall observe their agreement in case they have separate agreement on data message sending/receiving time.

Article 12 The principal offices of senders shall be regarded as the data message sending locations. The principal offices of receivers shall be regarded as the data message receiving locations. For those who have not any principal offices, their regular residence shall be regarded as their sending or receiving locations.

The parties shall observe their agreement in case they have separate agreement on data message sending/receiving locations.

Chapter III Electronic Signature and Authentication

Article 13 The electronic signatures shall be regarded as reliable electronic signatures when they simultaneously satisfy all the following requirements:

1. Electronic signature manufacturing data is exclusive to the electronic signer when it is used for electronic signature.
2. Electronic signature manufacturing data is under the control only of the electronic signer.
3. After signed, any modification made to the signature can be detected, found and discovered.
4. After signed, any modification made to the content/modality of the data message can be detected, found and discovered.

Parties may use any other reliable electronic signatures agreeable to themselves.

Article 14 Electronic signatures shall have the same legal effect as hand writing signatures or seals.

Article 15 Electronic signers shall carefully manage their electronic signature manufacturing data. In the case that it is disclosed, or is possibly disclosed, they shall inform the related parties and cancel the utilization of the disclosed electronic signature manufacturing data.

Article 16 In the case that the electronic signatures are required to be authenticated by a third party the authentication service shall be provided by legally established electronic authentication service providers.

Article 17 To provide electronic authentication service, the following requirements shall be satisfied:

1. Possessing technical and management personnel corresponding to the provision of electronic authentication service;
2. Possessing funds and operation sites corresponding to the provision of electronic authentication service;
3. Possessing the technology and equipment complying with government safety standards;
4. Possessing the certificates issued by the state password administration agencies to allow the use of passwords;
5. Other conditions required by laws and regulations.

Article 18 All those who want to provide electronic authentication service shall submit their applications, along with the related materials required in Article 17 of the law to the responsible department of the Ministry of Information Industry for approval. The responsible department of the Ministry of Information Industry, after receiving the applications, shall review them according to law. After consultation with the related departments of the State Council, the responsible department of the Ministry of Information Industry shall determine if the applicants' applications are or are not to be approved within 45 days after receiving the applications. For those who have been awarded approval the ministry shall issue licenses of electronic authentication. For those who fail to be awarded approval written notice shall be provided to explain reasons for their failure.

Applicants shall register according to law at the Department of Administration of Industry and Commerce with the license of electronic authentication.

Electronic authentication service providers who have obtained licenses shall publish their names and license numbers on the Internet according to the requirement of the responsible department of the Ministry of Information Industry.

Article 19 Electronic authentication service providers shall prepare and publish their business rules regarding electronic authentication business according to the related state provisions on the electronic authentication industry, and submit them for filing to the responsible department of the Ministry of Information Industry.

The rules of electronic authentication business shall include the measures of responsibility scope, operation standard and information safety guarantee.

Article 20 Applicants for electronic signing shall provide genuine, integral and accurate information when they apply for electronic signature authentication certificates with electronic authentication service providers.

Electronic authentication service providers shall verify the identification of applicants and review relevant materials after receiving their electronic signature authentication certificates application.

Article 21 Electronic signature authentication certificates issued by electronic authentication service providers shall be accurate and include the following items:

1. Name of electronic authentication service provider;
2. Name of authentication certificate holder;
3. Serial number of authentication certificate;
4. Valid period of authentication certificate;
5. Electronic signature authentication data of authentication certificate holder;
6. Electronic signature of electronic authentication service provider;
7. Other provisions regulated by the responsible department of the Ministry of Information Industry.

Article 22 Electronic authentication service providers shall make sure that the content of the electronic signature authentication certificate is entire and accurate, and guarantee that the electronic signature relies may prove or learn the content and related items carried by the electronic signature authentication certificates within the valid period of time.

Article 23 In the case that electronic authentication service providers plan to temporally suspend or terminate their electronic authentication service they shall inform related parties of the business succession and other related matters 90 days before the suspension or termination of the business.

In the case that electronic authentication service providers plan to temporally suspend or terminate their electronic authentication service, they shall inform the responsible department of the Ministry of Information Industry 60 days before their suspension and termination of the business and negotiate with other electronic authentication service providers on succession of

the business so as to work out an appropriate arrangement.

In the case that electronic authentication service providers fail to reach agreement with other electronic authentication service providers for the succession of the business, they shall request the responsible department of the Ministry of Information Industry to arrange successors to undertake their business.

In the case that the electronic authentication license of an electronic authentication service provider is revoked, the succession of their business shall be handled in accordance with the provisions regulated by the responsible department of the Ministry of Information Industry.

Article 24 Electronic authentication service providers shall properly store the authentication related information. The least reservation period of the information shall be longer than 5 years after the electronic authentication certificate is expired.

Article 25 The responsible department of the Ministry of Information Industry shall be responsible for the establishment of a detailed management method for electronic authentication business according to this law and the execution of supervision and administration over electronic authentication service providers according to law.

Article 26 After being approved by the responsible department of the Ministry of Information Industry according to the related agreement and principle of equity, the electronic signature authentication certificates issued at places by electronic authentication service providers outside the borders of the People's Republic of China shall have the same legal effect as the electronic authentication certificates issued by the electronic authentication service providers established according to this law.

Chapter IV Legal responsibility

Article 27 Electronic signers shall bear compensation responsibility in case they fail to timely inform the related parties of their known disclosure or possible disclosure of electronic signature manufacturing data and terminate the use of their electronic signature manufacturing data, or they fail to provide the electronic authentication service providers with genuine, integral and accurate information, or have any other mistakes, which result in losses for the electronic signature relies and electronic authentication service providers.

Article 28 Not being able to prove themselves to be unblamable, the electronic authentication service provider shall bear compensation responsibility for the losses of electronic signers or

electronic signature relies that conduct their civil activities on the basis of the electronic authentication service provided by the electronic authentication service provider.

Article 29 The responsible department of the Ministry of Information Industry shall order those who provide electronic authentication service without approval to stop their illegal behavior. For those who have illegal income, the illegal income shall be seized. For those who have illegal income more than 300 thousand yuan, a fine of not less than one time but not more than three times the illegal income shall be imposed. For those who do not have illegal income or have illegal income less than 300 thousand yuan, a fine of not less than 100 thousand yuan but not more than 300 thousand yuan shall be imposed.

Article 30 The responsible department of the Ministry of Information Industry shall impose a fine of not less than 10 thousand yuan but not more than 50 thousand yuan on the directly responsible person of the electronic authentication service provider in case he or she fails to report to the responsible department of the Ministry of Information Industry 60 days before their suspension or termination of their electronic authentication service.

Article 31 For those who fail to observe authentication business rules, fail to properly reserve the information relating to authentication or have any other illegal activities, the responsible department of the Ministry of Information Industry shall order them make corrections within a given period time. For those who fail to make corrections, their electronic authentication licenses shall be revoked and the persons in charge and other directly responsible people shall not be allowed to be engaged in electronic authentication business for 10 years. For those whose electronic authentication licenses are revoked, the revocation shall be bulletined and the department of administration of industry and commerce shall be informed.

Article 32 For those who forge, falsify or commit fraudulent use of other's electronic signatures and are convicted as criminals, their criminal responsibilities shall be investigated according to law. For those who cause loss for others, they shall bear civil responsibilities.

Article 33 As for the staffs working in the responsible department and responsible for the supervision and management of electronic authentication service industry according to this law, those who fail to execute administrative license and undertake supervision and management responsibilities accordingly, administrative punishment shall be imposed. For those who are convicted as criminals, criminal responsibility shall be investigated according to law.

Chapter V Supplementary Provisions

Article 34 The glossaries used in this law shall have the following meanings:

1. Electronic signer means the person who holds electronic signature manufacturing data and performs electronic signature in his own name or on behalf of others.
2. Electronic signature relies mean those who conduct related activities based upon their belief on the electronic signature authentication certificates or electronic signatures.
3. Electronic signature authentication certificates mean the data message or any other electronic records that may prove that the electronic signer and the electronic signature manufacturing data are relevant.
4. Electronic signature manufacturing data means the data of characters and codes used in the process of electronic signing, which reliably link the electronic signatures with electronic signers.
5. Electronic signature authentication data means the data used in the authentication of electronic signing, including the codes, passwords, algorithm and public keys.

Article 35 The State Council or the departments designated by the State Council may establish detailed methods on utilization of electronic signature and data message for their governmental affairs and other social activities.

Article 36 This law shall be enacted on April 1st, 2005.