



## Electronic Signatures Law of the People's Republic of China

Promulgated on 28 August 2004 as Presidential Decree No.18  
and effective as of 1 April 2005

### Chapter I General Provisions

**Article 1** This law is enacted to regulate acts concerning electronic signatures, establish the legal validity and effect of electronic signatures, and safeguard the lawful rights and interests of relevant parties.

**Article 2** All references to an "electronic signature" in this law are to electronic data that is contained in or attached to a data message and used to identify the signatory and indicate its endorsement of the contents of such data message.

All references to a "data message" in this law are to information that is generated, transmitted, received or stored by electronic, optical, magnetic, or similar means.

**Article 3** The parties to contracts, bills and other documents used in civil activities may agree to use or not to use electronic signatures and data messages.

If the parties agree to use electronic signature or data message documents, they may not deny the legal validity of such documents solely on the basis that the documents take the form of data messages or use electronic signatures.

The preceding paragraph shall not apply to documents pertaining to:

- (1) personal relationships, such as marriage, adoption or succession;
- (2) the transfer of rights and interests in real property, such as land or housing;
- (3) the suspension of the supply of public utilities, such as water, heat, gas or electricity; and
- (4) other conditions specified in laws and regulations for which electronic documents are inappropriate.

## Chapter II Data Messages

- Article 4** Data messages with content that can be displayed in tangible form and be retrieved, read and used at any time shall be deemed to comply with the requirements of laws and regulations for items in written form.
- Article 5** A data message shall be deemed to satisfy the requirement of laws and regulations for an original document if:
- (1) its contents can effectively be displayed and may be retrieved, consulted and used at any time; and
  - (2) it can reliably maintain the integrity of its contents without modification from the time of its finalization. However, the addition of an endorsement on a data message, or changes in the format of a data message arising during data exchange, storage or display, shall not affect the integrity of such message.
- Article 6** A data message shall be deemed to satisfy the requirements of laws and regulations for document preservation if:
- (1) its contents can effectively be displayed and may be retrieved, consulted and used at any time;
  - (2) its format remains the same at the time of its creation, transmission or receipt, or its format is different but the data message can accurately display its original content when created, transmitted or received; and
  - (3) its sender, recipient, and the time of transmission and receipt can be identified.
- Article 7** The use of a data message as evidence may not be refused solely on the grounds of its creation, transmission, receipt or storage in electronic, optical, magnetic or other similar form.
- Article 8** When examining the authenticity of a data message as evidence, the following factors shall be considered:
- (1) the reliability of the method of its creation, storage or transmission;
  - (2) the reliability of the method of maintaining the integrity of its contents;
  - (3) the reliability of the method of identifying its sender; and
  - (4) other related factors.
- Article 9** A data message shall be deemed transmitted by its sender if:
- (1) the sender authorized its transmission;
  - (2) it was transmitted automatically by the sender's information system; and

- (3) the recipient has verified the data message using a method approved by the sender, which results in a corresponding confirmation.

Where the parties have agreed otherwise regarding the matters specified in the preceding paragraph, such agreement shall prevail.

**Article 10** If laws or administrative regulations stipulate, or the parties agree, that the receipt of a data message requires confirmation, then its receipt must be confirmed. Once the sender receives confirmation of receipt from the recipient, the data message shall be deemed received.

**Article 11** The time at which a data message enters an information system not under the sender's control shall be deemed to be the time at which the data message is sent.

If the recipient designates a specific system for the receipt of data messages, the time at which a data message enters that specific system shall be deemed the time at which the data message is received. If the recipient has not designated a specific system, the time at which a data message first enters any of the recipient's systems shall be deemed to be the time at which the data message is received.

If the parties have agreed otherwise regarding the time data messages are sent or received, such agreement shall prevail.

**Article 12** The principal place of business of the sender shall be deemed the place from where a data message is sent, and the principal place of business of the recipient shall be deemed the place where the data message is received. In the absence of a principal place of business, the sender's or the recipient's usual place of residence shall be deemed the place where the data message is sent or received.

If the parties have agreed otherwise regarding the place from which a data message is sent, or at which it is received, such agreement shall prevail.

### **Chapter III Electronic Signatures and Certification**

**Article 13** An electronic signature shall be deemed a reliable electronic signature if:

- (1) at the time the electronic signature creation data is used for an electronic signature, it is proprietary to the electronic signatory;
- (2) at the time of signing, the electronic signature creation data is controlled solely by the electronic signatory;
- (3) any change to the electronic signature after signing is noticeable; and
- (4) any change to the content and form of the data message after signing is noticeable.

The parties may use such electronic signatures that comply with the conditions for reliability as agreed by them.

- Article 14** A reliable electronic signature shall have the same legal validity and effect as a handwritten signature or an affixed seal.
- Article 15** An electronic signatory shall duly safeguard its electronic signature creation data. If an electronic signatory learns that the secrecy of its electronic signature creation data has or may have already been compromised, it shall promptly notify the relevant parties and cease using such electronic signature creation data.
- Article 16** If an electronic signature requires certification by a third party, such certification service shall be provided by a lawfully established electronic certification service provider.
- Article 17** An electronic certification service provider must:
- (1) have professional technicians and management personnel suitable for the provision of electronic certification services;
  - (2) have funds and business premises suitable for the provision of electronic certification services;
  - (3) possess technology and equipment that complies with national security standards;
  - (4) have documentary evidence from the state secrecy administrative department consenting to the use of encryption; and
  - (5) meet other conditions specified in laws or administrative regulations.
- Article 18** To engage in the provision of electronic certification services, an application and the relevant materials complying with the conditions specified in Article 17 hereof shall be submitted to the State Council department in charge of the information industry. After the State Council department in charge of the information industry has received the application, has examined the application in accordance with the law, and has solicited the opinions of the State Council department in charge of commerce and other relevant departments, it shall render a decision on whether or not to grant permission within 45 days of receiving the application. If permission is granted, an electronic certification permit will be issued. If permission is denied, the applicant will be notified in writing and informed of the reason.
- The applicant shall carry out enterprise registration procedures with the administration for industry and commerce in accordance with the law on the strength of the electronic certification permit.
- An electronic certification service provider that has obtained certification qualifications shall post such information as its name and permit number on the Internet in accordance with the regulations of the State Council department in charge of the information industry.

**Article 19** An electronic certification service provider shall formulate and publish electronic certification rules that comply with relevant national regulations, and submit the same for the record to the State Council department in charge of the information industry.

Electronic certification rules shall include scope of liability, operating standards, measures for the preservation of information security, etc.

**Article 20** When applying to an electronic certification service provider for an electronic signature certificate, an electronic signatory shall provide true, complete and accurate information.

After receiving an application for an electronic signature certificate, an electronic certification service provider shall check the applicant's identity and examine the relevant materials.

**Article 21** Electronic signature certificates issued by an electronic certification service provider shall be accurate and free from errors, and shall record:

- (1) the name of the electronic certification service provider;
- (2) the name of the certificate holder;
- (3) the serial number of the certificate;
- (4) the term of validity of the certificate;
- (5) the certificate holder's electronic signature verification data;
- (6) the electronic signature of the electronic certification service provider; and
- (7) other particulars specified by the State Council department in charge of the information industry.

**Article 22** Electronic certification service providers shall ensure that the contents of electronic signature certificates are complete and accurate during their valid term, and shall ensure that parties relying on electronic signatures can verify or comprehend all of the recorded contents of electronic signature certificates and other relevant matters.

**Article 23** If an electronic certification service provider intends to suspend or terminate its provision of electronic certification services, within 90 days before the suspension or termination of services it shall notify the relevant parties of the taking over of its business by another provider and other relevant matters.

If an electronic certification service provider intends to suspend or terminate its provision of electronic certification services, within 60 days before the suspension or termination of services it shall submit a report to the State Council department in charge of the information industry, and shall consult with other electronic certification service providers on the taking over of its business by another provider and make appropriate arrangements.

If the electronic certification service provider is unable to reach agreement with another electronic certification service provider on matters relating to the taking over of its business, it shall apply to the State Council department in charge of the information industry to arrange for another electronic certification service provider to take over its business.

If an electronic certification service provider has its electronic certification permit revoked in accordance with the law, matters relating to the taking over of its business shall be handled in accordance with the regulations of the State Council department in charge of the information industry.

**Article 24** For at least 5 years after an electronic signature certificate expires, the electronic certification service provider shall appropriately preserve information relating to the certificate.

**Article 25** The State Council department in charge of the information industry shall formulate specific administrative measures for the electronic certification service industry in accordance with this law, and shall regulate electronic certification service providers in accordance with the law.

**Article 26** After their approval by the State Council department in charge of the information industry in accordance with the relevant agreement or the principle of reciprocity, electronic signature certificates issued by electronic certification service providers outside the PRC shall have the same legal validity and effect as electronic signature certificates issued by electronic certification service providers established in accordance with this law.

#### **Chapter IV Legal Liability**

**Article 27** If an electronic signatory is aware that the security of its electronic signature creation data has been compromised or may have been compromised but does not timely inform the relevant parties and fails to cease using such electronic signature creation data, or does not provide true, complete and accurate information to the electronic certification service provider, or if it commits another error and thereby causes those who rely on electronic signatures and/or the electronic certification service provider to incur a loss, it shall bear liability for damages.

**Article 28** If an electronic signatory or a person who relies on a electronic signature incurs a loss as a result of relying on the electronic signature certification service provided by an electronic certification service provider while engaging in civil activities, and if the electronic certification service provider fails to provide evidence that the provider was not at fault, then the electronic certification service provider shall bear liability for damages.

**Article 29** If electronic certification services are offered without a permit, the State Council department in charge of the information industry shall order the violation to cease. If there is illegal income, such illegal income shall be confiscated. If the illegal income totals RMB 300,000 or more, a fine equivalent to 3 times the illegal income amount shall be imposed. If there was no illegal income or if such illegal income was less than RMB 300,000, a fine of not less than RMB 100,000 and not more than RMB 300,000 shall be imposed.

- Article 30** If an electronic certification service provider suspends or terminates the provision of its electronic certification services but fails to submit a report to the State Council department in charge of the information industry within 60 days prior to such suspension or termination, the State Council department in charge of the information industry shall fine the person directly in charge not less than RMB 10,000 and not more than RMB 50,000.
- Article 31** If an electronic certification service provider fails to abide by the certification rules, fails to appropriately preserve information relating to certificates, or commits another violation of the law, the State Council department in charge of the information industry shall order the provider to rectify the matter within a specified period of time; if rectification is not done within that period, then the provider's electronic certification permit shall be revoked and the person directly in charge and the other persons directly responsible shall be prohibited from engaging in the provision of electronic certification services for 10 years. Those that have their electronic certification permits revoked should give a public announcement and notify the administration for industry and commerce.
- Article 32** Where a third party's electronic signature is forged, used fraudulently or misappropriated so as to constitute a crime, criminal liability shall be pursued in accordance with the law; if the third party was made to incur a loss, civil liability shall be borne in accordance with the law.
- Article 33** If a member of the working personnel of a department responsible under this law for the regulation of the electronic certification service industry fails to perform his administrative licensing or regulatory responsibilities lawfully, he shall be subjected to administrative punishment in accordance with the law; if a criminal offense was committed, criminal liability shall be pursued in accordance with the law.

## Chapter V Supplementary Provisions

- Article 34** The meanings of the following terms used in this law are as follows:
- "Electronic signatory" means a person who holds electronic signature creation data and implements an electronic signature in his own capacity or in the name of any person he represents.
- "Party that relies on electronic signatures" means a person who engages in the relevant activity based on his reliance on an electronic signature certificate or electronic signature.
- "Electronic signature certificate" means the data message or other electronic record that can authenticate the connection between an electronic signatory and electronic signature creation data.
- "Electronic signature creation data" means data such as symbols and numbers. used in the electronic signature process that can reliably connect an electronic signature to an electronic signatory.

"Electronic signature verification data" means the data used to verify an electronic signature, including codes, passwords, algorithms and public keys.

**Article 35** The State Council or departments specified by the State Council may formulate specific measures for the use of electronic signatures and data messages in political activities and other social activities based on this law.

**Article 36** This law shall come into effect as of 1 April 2005.

\* \* \*

TransAsia is a leading law firm, licensed in the People's Republic of China and providing clients with a full service package ranging from market entry strategies to litigation. Our legal team is comprised of approximately 40 lawyers and professionals, the majority of whom are admitted to practice in the PRC, with others qualified in the United States, Australia and Hong Kong. Our professionals have an intimate knowledge of Chinese law and culture and provide international clients with a thorough understanding of how to do business in China.

Please visit our [publications website](#) for a complete set of translations and commentaries of all the relevant laws in the fields of IT, media, employment, and real estate.

---

**Beijing**

Suite 2218 China World Tower 1  
1 Jianguomenwai Avenue  
Beijing 100004, China  
Tel: (86 10) 6505-8188  
Fax: (86 10) 6505-8189

**Shanghai**

Suite 619-620 Shanghai Center  
1376 Nanjing Road West  
Shanghai 200040, China  
Tel: (86 21) 6279-8212  
Fax: (86 21) 6279-8112

<http://www.TransAsiaLawyers.com>

*This translation is for informational purposes only and does not constitute legal advice. Use of this translation does not create an attorney-client relationship between TransAsia Lawyers and the reader. Readers should contact appropriate legal counsel for advice on any particular issue. Entire content copyright is owned by TransAsia Lawyers. Reproduction and distribution of this translation in whole or in part without the written permission of TransAsia Lawyers is expressly prohibited.*