ARTICLE:

A note to China's new law on electronic signatures

By **Chris Cao**

The history of China's legal structure for electronic signatures started in 1999. It was that year electronic signatures were statutorily recognized by contract law in the People's Republic of China (PRC) as legitimate, namely a type of data message for contracts. The Electronic Signature Law was enacted in 2004,[1] although electronic records had been used as documentation in transactions for several years. The PRC government revised its Electronic Signature Law in 2015,[2] a move made to facilitate the country's booming technology sector.

When comparing the old and new versions of the law, we note that not too many changes have been made. The new law imposes an additional requirement for licensed electronic verification service providers, making it clear that it should be an enterprise legal person. Holding such a license is no longer a prerequisite before incorporating a company with the administration for industry and commerce.[3]

Article 13 of the new Electronic Signature Law provides for an electronic signature as follows:

> 1. Electronic signature creation data exclusively belongs to the electronic signatory;
>
> 2. When a signature is entered, the creation of its data is controlled only by the signatory(ies);
>
> 3. After the signature is entered, any alteration made to the electronic signature can be detected; and
>
> 4. After the signature is entered, any alteration made to the contents and form of a data message can be detected.[4]

Legislation and judicial practice regarding electronic signatures is a cross-disciplinary issue that spans the legal and technology sectors.[5] A typical electronic signature is in the form of an electronic certificate based on a public key infrastructure (PKI), provided by electronic certification service providers. Such providers are licensed by the administrative authorities. Electronic certificates provided or verified by licensed authorities are widely accepted as legitimately reliable in both the business and legal worlds. The licensing rules are subscribed under the PRC's Administrative Measures for Electronic Certification Services. Each licensed electronic certification service provider should hold an 'Electronic Certification Services License', issued by the Ministry of Industry and Information Technology (MIIT). An extra process to enhance the reliability of electronic certification is to obtain a timestamp from a reliable time source, with the best being the official one: the National Time Service Center under Chinese Academy of Sciences. The timestamp, however, is not a prerequisite in order to render electronic signatures reliable.[6]

There are also other forms of electronic signature that contain the features outlined in article 13, and can therefore be employed in legal documents. Acceptable types of electronic signatures include, among other things, fingerprints, voice, and retinal images. Passwords and personal identification numbers qualify as well. These types of electronic signature are quite common in normal business practices as a way to confirm a transaction. Many judicial decisions reached before and after enactment of the Electronic Signature Law of 2005 supported the

[1] For a translation of the law into English, see Minyan Wang and Minju Wang, 'Electronic Signatures Law of China, translation and introduction', 2 *Digital Evidence and Electronic Signature Law Review*, (2005) 79 – 85.
[2] Electronic Signature Law, document number: Order No. 24 of the President of the People's Republic of China, promulgated on and effective since 4 April 2015.
[3] A pre-incorporation entity has to be licensed in advance if its business scope covers certain specially regulated industries, otherwise it cannot be successfully incorporated as a company in the PRC. Running an electronic verification service was previously among such regulated industries under the old law. Under the new law, this industry is still a license-required one, but holding such license is no longer a prerequisite for company incorporation.
[4] Article 13, Electronic Signature Law.
[5] In some cases, the technical reliability of an electronic signature might be in question. The burden of proof is on the party who argues the electronic signature is technically authentic and reliable. See (2015) 深福法民二初字第1164号.
[6] In some causes of action, a time stamp is critical. For example, in an intellectual property dispute, a time stamp is essential for identifying the true creator of a piece of intellectual work. See (2012) 民申字第1513号.

use of passwords and PINs as electronic signatures, and shared the opinion that passwords can function as electronic signatures providing they are unique, secretly kept, and privately owned.[7]

The Electronic Signature Law not only touches on rules regarding electronic signatures but also data messages.[8] A data message is categorized as a written form contract, a legal contract form, if contractual parties use it as the documentation of a contract. To be qualified as a contract or agreement, data messages must be authentic, duly preserved, and affixed with a reliable electronic signature. The authenticity of a data message therefore relies to a large extent on the reliability of the electronic signature. Article 3 of this law states as follows: 'the parties concerned may agree to use or not to use an electronic signature or data message in such documents as contracts and other documents, receipts and vouchers in civil activities,' except for the following situations: documents related to marriage, adoption and succession; documents related to the transfer of the rights and interests residing in real estate such as land and housing; documents related to the termination of public utility services as water, heat, gas and power; and other circumstances where electronic documentation is not applicable, as provided for by relevant laws and administrative regulations.[9]

The new Electronic Signature Law outlines a framework for electronic messages and signatures. It does not touch on how to create a reliable electronic message or electronic signature. Some legal commentators believe this is not included because of the principle of technology neutrality, and opine that the criteria of reliability should be left to the judiciary to decide.[10]

Chris Cao is an associate at Eiger in Shanghai. He is an experienced PRC attorney with a focus on corporate, contract, commercial, and employment law. His responsibilities at Eiger include, among others, compliance and legal research. Chris completed his legal studies in China, and then the U.S.

chris.cao@eigerlaw.com

[7] Judicial decisions numbered (2008) 浙民二终字第154号 and (2014) 深中法商终字第249号 are typical decisions with opinions; See also the following translations into English: Yang Chunning v Han Ying (2005) hai min chu zi NO.4670, Beijing Hai Dian District People's Court, commentary by Jihong Chen, 5 *Digital Evidence and Electronic Signature Law Review* (2008) 103 – 105; Xinchuan Online (Beijing) Information Technology Co. Ltd. v Zigong Branch of China Network Communication Group (2008) Min Shen Zi No. 926, translation and commentary by Dr Jiong He, 10 *Digital Evidence and Electronic Signature Law Review* (2013) 158 – 161; also the following case notes: Rong-Shu-Xia Computer Ltd. v China Society Publisher, by Minyan Wang, 4 *Digital Evidence and Electronic Signature Law Review* (2007) 95; Beijing Han-Hua-Kai-Jie Technology development Ltd. v Chen Hong, by Minyan Wang, 4 *Digital Evidence and Electronic Signature Law Review* (2007) 96; Zhang Hua v Shanghai Danwei Information Consultation Co. Ltd, Shanghai People's Court of Jing'an District, by Dr Minyan Wang, 6 *Digital Evidence and Electronic Signature Law Review* (2009) 275 – 276.

[8] Data messaging is also a cross-disciplinary issue, as explained in Stephen Mason, ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012). See (2009) 深中法民一初字第942号.

[9] Article 3, Electronic Signature Law.

[10] See 于海防，我国电子签名框架性效力规则的不足与完善[J]，法学.2016（1）and 黄瑞鹏，电子签名与认证法律问题研究[D]，中国海洋大学 2006.