



Llinks Corporate and M&A Bulletin
November 2019

上海
上海市银城中路 68 号
时代金融中心 16 楼和 19 楼
邮编: 200120
电话: +86 21 3135 8666
传真: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编: 100005
电话: +86 10 8519 2266
传真: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话: +852 2592 1978
传真: +852 2868 0883

伦敦
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

SHANGHAI
16F/19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

HONG KONG
27F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

master@llinkslaw.com

The Encryption Law: Gist and Compliance

By David Pan | Nigel Zhu | Shana Sha

The Encryption Law of the People's Republic of China (hereinafter referred to as "the Encryption Law") was approved and passed by the Standing Committee of the National People's Congress on October 26, 2019. It will take effect on January 1, 2020. As the law with the highest legal authority and the widest application scope in field of encryption, the Encryption Law is finally enacted after nearly three years of legislative process and seeking public comments for twice. The law will provide guidance for regulating and promoting the development of the encryption industry, and lay down foundation for corporate compliance. In this article, the authors will briefly interpret the Encryption Law based on the current legal framework for encryption and other applicable laws such as the Cybersecurity Law, and offer suggestions in corporate compliance.

I. Definition and Function of Encryption

The Encryption Law defines "encryption" as "technologies, products, or services applying specific transformations to information to effect encryption protection and security authentication". This definition

如果您需要本出版物的中文本,
请与下列人员联系:

郭建良: +86 21 3135 8756
Publication@llinkslaw.com

For more Llinks publications,
please contact:

Roy Guo: +86 21 3135 8756
Publication@llinkslaw.com

Llinks Law Offices
www.llinkslaw.com

The Encryption Law: Gist and Compliance

embodies three characteristics of encryption: first, encryption must transform plaintext to ciphertext by means of specific transformations; second, encryption is used to effect encryption, protection and security authentication for information; and third, encryption can be a technology, product or service.

The password we often come across in our life is not the encryption defined in the Encryption Law. In our daily life, the “password” used to protect bank accounts, mobile application accounts and so on, is a kind of plaintext and there is no transformation process from plaintext to ciphertext; meanwhile, such passwords do not fit the legal definition of encryption being a technology, product, or service. The encryption in the Encryption Law is a “complex and massive information processing system”.¹ It is a process of encrypting identifiable digital and biological information (i.e. plaintext) into unidentifiable symbol sequences so as to provide encryption protection, or a means of authenticating whether the above information has been tampered with, whether the information source is reliable, and whether the subject and behavior are authentic. Taking the commercial encryption as an example, the commercial encryption technology is the core, which can realize encryption, decryption and authentication of commercial encryption (including cryptographic programming and cryptographic algorithm chip, cryptographic card, etc.).

Although the definition of encryption in the Encryption Law differs from people’s general understanding, the Encryption Law is closely related to people’s life. Before the enactment of the Encryption Law, the application of encryption has reached all walks of life. In security authentication, USB Key, which is commonly used in E-government and E-commerce, is a relatively secure authentication method. USB Key isolates the encryption operation from the complex environment of the user terminal through the operation of data encryption and decryption in the use of built-in CPU or secure crypto-chip.² Each USB key corresponds to a hardware PIN code to execute a two-factor authentication mechanism for users, and only users with both the USB key and PIN code can pass the authentication. In encryption protection, the common application of encryption is the HTTPS encrypted transport used in financial transactions or enterprise intranets, where HTTPS utilizes SSL (Secure Sockets Layer) as a sublayer of the HTTP application layer and SSL encrypts network connections at the transport layer. For example, Alipay processes the plaintext and uses HTTPS transmission, so as to protect data security and prevent data breach and network attacks.

II. Legislative Background and Purpose of the Encryption Law

A. Legislative Background

Before the enactment of the Encryption Law, the main legislation in China is the Regulation for Administration of Commercial Encryption in 1999. From 2000 to 2010, the State Cryptography Administration issued or revised a number of legislations on research, production, use, sales and other aspects of commercial encryption. In recent years, the rapid development of cloud computing, Internet of Things, big data and other information technologies has stimulated the vigorous development of

The Encryption Law: Gist and Compliance

emerging industries as they integrate into traditional industries. The emerging fields supported by Internet technology need to adopt encryption technologies and products to improve security. Although the National Information Security Standardization Committee took the initiative to formulate the Basic Requirements for Encryption Application in Information Systems (GM/T 0054-2018) and other relevant national standards and industrial standards, the status quo of legislation clearly cannot provide sufficient legal support for the fast development of the encryption industry. In addition, issues existing under the current encryption legal framework such as the sole law enforcement agency, the strict administrative licensing system and the conflict with new regulations such as the Cybersecurity Law have become increasingly prominent. In this context, it is necessary to adopt a unified legislation in the field of encryption, and China urgently needs a national, systematic encryption regulation. The objective of the Encryption Law is therefore introduced and promulgated.

B. Legislative Purpose

1. Protect network and information security

The Cybersecurity Law emphasizes “protecting cybersecurity”, while encryption is the foundation of such protection, and it plays a pivotal role in national security, economic development and social stability. Cryptographic algorithm and cryptographic modules are the basis of information security. If China cannot establish an independent and controllable encryption industry, the domestic information security will be plagued with uncontrollable risks. For example, the State Cryptography Administration issued a security alert on SHA-1 cryptography algorithm in 2017, prompting enterprises to fully support and apply SM3 and other domestic cryptography algorithms³. This shows the practical significance of building up encryption industry for information security.

The Encryption Law is an important tool to improve the legal system for national security under the legal framework of national cybersecurity. It conforms to the policies on localization requirements of information security products. As a necessary means for encryption technologies, products and services to play important roles in cyberspace, it promotes the construction of a security system with encryption technologies at the core and cross-integration of multiple technologies.⁴

The Encryption Law: Gist and Compliance

2. Regulate encryption applications and promote encryption development

The Encryption Law specifies obligations of encryption authorities, articulates the scope of obligations of encryption-related entities, provides financial support, and manages encryption by category. In terms of encryption science and technology studies, the Encryption Law stresses efforts to encourage and support innovations in encryption science and technology, protect intellectual property rights and strengthen the development of encryption talents. Meanwhile, it requires strengthening the encryption security education and enhancing the public awareness of encryption security. The purpose of the Encryption Law is to provide comprehensive support for the development of encryption.

Compared with the current laws on commercial encryption, the Encryption Law also endeavors to reduce the burden of enterprises. It makes room for independent development of commercial encryption enterprises in order to effectively manage and support encryption. At present, the application of blockchain technology is proliferating in finance, education, labor employment and health care. Encryption is an important supporting technology of blockchain. The enactment of the Encryption Law reflects the integration of encryption and blockchain technology, provides core support and guarantee for blockchain, and will also affect the industrial reform and economic transformation in China.

III. Key Analysis: Hierarchical Administration of Encryption

The Encryption Law administers encryption by category. The Encryption Law classifies encryption into core encryption, ordinary encryption, and commercial encryption. The three types of encryption correspond to different types of information: core encryption and ordinary encryption are used to protect state secrets; and commercial encryption is used to protect information that does not fall into the category of state secrets. State secrets are classified into three levels: top secret, confidential and secret. Core encryption can be used to protect all three types of state secrets, but ordinary encryption can only be used to protect state secrets categorized as confidential and secret.

A. Core Encryption and Ordinary Encryption

Core encryption and ordinary encryption per se are state secrets, which shall be strictly and uniformly managed. In terms of the administration of core encryption and ordinary encryption, the draft of Encryption Law (hereinafter referred to as the “Draft”) once specifically classified the administration

The Encryption Law: Gist and Compliance

scope, including scientific research, production, testing, installation, use and destruction of encryption. Although the Encryption Law deletes the above provisions, it should be interpreted as a generality of legislative language, while the law still regulates the full life cycle of core encryption and ordinary encryption.

The government agencies of core encryption and ordinary encryption⁵ shall establish and improve their security management systems, take strict security measures and guarantee the confidentiality accountability. The confidentiality accountability requirement is also a new addition to the Draft. It requires encryption agencies to assume their responsibilities so as to ensure the “consistency between power and responsibility” and effectively protect encryption security. Therefore, the agencies of core encryption and ordinary encryption must keep a close eye on encryption security management.

In addition to encryption agencies, the encryption administration has the authority to guide, supervise and inspect the operation of core encryption and ordinary encryption. It should establish cooperative mechanisms with other related departments in respect of security monitoring and early warning, security risk assessment, information disclosure, consultation on major matters, and emergency response, and eliminate major problems and potential risks that affect encryption security in a timely manner. This is not only the cooperative supervision of encryption, but also the overall safeguard for encryption security.

B. Commercial Encryption

The Regulations for Management of Commercial Encryption and its ancillary regulations stipulate strict approval requirements for the R&D, production, import and use of commercial encryption products, but such approval requirements have failed to keep pace with the development of information networks and applications. In practice, prior to the Encryption Law, the State Cryptography Administration had already abolished most administrative approval requirements in relation to commercial encryption. In order to further develop the commercial encryption market, the Encryption Law intends to reform the commercial encryption management system, the most prominent of which is the “double voluntariness” principle of commercial encryption. First, the Encryption Law clearly stipulates that foreign-invested enterprises which engage in commercial encryption activities enjoy equal rights with domestic enterprises. As a result, foreign-invested enterprises may voluntarily carry out commercial encryption cooperation, while the Encryption Law prohibits administrative agencies from forcing mandatory transfer of commercial encryption technology. Second, other than commercial encryption products which involve national security,

The Encryption Law: Gist and Compliance

national economy, social welfare, and public interests, inspection and certification for enterprises in possession of commercial encryption is carried out on a voluntary basis, thus removing the pre-license and special control management for R&D, production, import, export, and use of commercial encryption products. In addition, the Encryption Law specifically stipulates that commercial encryption used in mass consumer products is not subject to import licensing and export control.

In terms of the confidentiality of commercial encryption, the Encryption Law also provides “dual protection.” First of all, the Encryption Law requires encryption inspection and certification institutions to abide by the confidentiality obligations of the state secrets and business secrets; secondly, administrative agencies may not force commercial encryption practitioners and commercial encryption inspection and certification institutions to disclose the source code and other encryption-related information. Administrative agencies shall also bear the obligation of confidentiality for business secrets and personal privacy collected in the process of performing their duties.

IV. Compliance Suggestions

Below the authors summarize the compliance obligations of enterprises in relation to the use, production and sale of encryption. Above all, all enterprises should fully and correctly understand the encryption management legal system.

Legal Framework for Encryption Legislation		
Laws (the NPC, the National People's Congress)	Special Law Encryption Law	Other Relevant Laws State Security Law, Guarding State Secrets Law, Cybersecurity Law, Anti-terrorism Law, Electronic Signature Law, Technology Import and Export Management Regulations, etc.
Administrative Regulations (the State Council)	Regulations of Management of Commercial Encryption;	
Departmental Rules (State Cryptography Administration)	Regulations for Production Management of Commercial Encryption Products; Regulations for R&D Management of Commercial Encryption; Measures for Encryption Management of Electronic Certification Services; Measures for Management of Commercial Encryption in Information	

The Encryption Law: Gist and Compliance

	Security Level Protection;
National Standards, Industry Standards	GM/T 0054-2018: Information System Encryption Application Basic Requirements; GM/T 0044-2016: SM9 Identification Encryption Algorithm; GM/T 0045-2016: Specification of Finance Data Encryption Tools; GB/T 22239-2008: Information Security Technology – Information System Level Protection Basic Requirements, etc.

A. Users of Encryption

1. Using core encryption and ordinary encryption

As described in the Section III of this article, core encryption and ordinary encryption shall be used to protect state secrets. Core encryption and ordinary encryption per se are state secrets. The encryption users shall take measures to keep confidential the state secrets collected in the process of using encryption. Enterprises shall implement the confidentiality accountability system pursuant to regulations related to core encryption and ordinary encryption. Enterprises shall promptly eliminate major irregularities or potential risks that may cause state secrets breach. In the occurrence of the aforementioned incidents, enterprises shall respond immediately and report to the secrecy bureau and the cryptography administration.

2. Using commercial encryption

Although the Encryption Law has loosened restrictions on commercial encryption, enterprises still are still subject to certain mandatory obligations in the process of using commercial encryption.

First, in terms of the inspection and authentication of commercial encryption, the Encryption Law encourages commercial encryption practitioners to voluntarily conduct commercial encryption inspection and certification. Where encryption products involve national security, national economy, social welfare and public interest, the encryption products must pass the compliance certification conducted by the commercial encryption certification authority.

Second, with respect to the security assessment of commercial encryption, if the enterprise uses commercial encryption to protect the critical information infrastructure (CII), it should conduct a

The Encryption Law: Gist and Compliance

security assessment of the encryption application by itself or by a commercial encryption inspection institution. The security assessment requirements set forth in the Encryption Law are consistent with those of the CII security inspection and certification and cybersecurity multi-level protection system provided in the Cybersecurity Law. Additionally, if the purchase of commercial encryption products and services may affect national security, such purchase will be subject to national security review.

Third, with regard to import licenses and export controls for commercial encryption, if the commercial encryption imported by enterprises involve national security and public interests, and is featured with encryption protection functions, it shall obtain import licenses from the competent department of commerce of the State Council and the State Cryptography Administration; if the commercial encryption exported by enterprises involve national security, public interest or China's international obligations, it will be subject to regulations of export control. Enterprises should watch out for the list of commercial encryption import license and export control (except for commercial encryption used by mass consumer products).

3. Other obligations under relevant regulations

For compliance purpose, commercial encryption users shall also pay attention to other obligations provided in legislations related to the Encryption Law.

The provisions of the Encryption Law for commercial encryption involving national security, national economy, social welfare and public interests are consistent with those of the Cybersecurity Law on critical network equipment and dedicated cybersecurity products. In accordance with the mandatory requirements of relevant national standards, aforesaid products can only be sold or provided after being inspected or certified by qualified institutions, and the security certification and security inspection results are mutually recognized.⁶ It is worth noting that the Office of the CPC Central Committee for Cybersecurity and Informatization and other departments have been promoting the formulation of the National Standard Requirements for Critical Network Equipment and Dedicated Cybersecurity Products. Two draft versions have been issued to seek public comments and the final version is expected to be promulgated soon.

The requirements on protection of CII with commercial encryption are consistent with those set forth in the Cybersecurity Multi-level Protection Regulations (Draft for Comment).⁷ Meanwhile, in terms of security review, the Encryption Law stipulates that CII operators' purchase of

The Encryption Law: Gist and Compliance

network products and services involving commercial encryption that may affect national security shall conduct national security review. This echoed relevant regulatory requirements stated in the Cybersecurity Law⁸, the Measures for the Security Review of Network Products and Services⁹, and the Critical Information Infrastructure Security Protection Regulations (Draft for Comment)¹⁰.

B. Manufacturers and Sellers of Encryption Products

Enterprises which engage in the production of core encryption and ordinary encryption shall establish a sound security management system, adopt strict security measures and a confidentiality accountability system to ensure the security of core encryption and ordinary encryption.

The production and sale of commercial encryption shall not harm national security, public interests or the legitimate rights and interests of others, and shall comply with applicable laws, administrative regulations, mandatory national standards for commercial encryption, and technical requirements set forth in publicly-available standards of the industry. Any commercial encryption distribution company should note that if the encryption products sold fall into the critical network equipment and dedicated cybersecurity products catalog (that is, the encryption products involve national security, national economy, social welfare and public interests), such products must be inspected and certified by accredited institutions. Only after passing the inspection and certification may the products be sold or provided, otherwise the distribution company may face administrative penalties such as warnings and fines.

V. Conclusion

The Encryption Law is significant for the development of the encryption industry in China and other industries that need encryption for information protection. On the one hand, the Encryption Law protects and limits core encryption and ordinary encryption as state secrets. On the other hand, it loosens control on commercial encryption, which is conducive to the R&D and use of encryption technologies and products in the commercial field. Moreover, jointly with the Guarding State Secrets Law, the Electronic Signature Law, the Cybersecurity Law, the E-commerce Law, etc., the Encryption Law will provide systematic guidance for information protection in all sectors.

The Encryption Law: Gist and Compliance

Contact Details

If you would like to know more information about the subjects covered in this publication, please feel free to contact the following people or your usual Llinks contact.

Author	
David Pan Tel: +86 21 3135 8701 david.pan@llinkslaw.com	
Shanghai	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	Bernie Liu Tel: +86 21 3135 8678 bernie.liu@llinkslaw.com
Selena She Tel: +86 21 3135 8770 selena.she@llinkslaw.com	Nicholas Lou Tel: +86 21 3135 8783 nicholas.lou@llinkslaw.com
Dali Qian Tel: +86 21 3135 8676 dali.qian@llinkslaw.com	Kenneth Kong Tel: +86 21 3135 8777 kenneth.kong@llinkslaw.com
David Wu Tel: +86 21 6043 3711 david.wu@llinkslaw.com	David Pan Tel: +86 21 3135 8701 david.pan@llinkslaw.com
Elyn Jiang Tel: +86 21 6043 3710 elyn.jiang@llinkslaw.com	
Beijing	
David Yu Tel: +86 10 8519 2266 david.yu@llinkslaw.com	Bernie Liu Tel: +86 10 8519 2266 bernie.liu@llinkslaw.com
Yuhua Yang Tel: +86 10 8519 1606 yuhua.yang@llinkslaw.com	
Hong Kong(in Association with Dennis Fong & Co., Solicitors)	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	Sandra Lu Tel: +86 21 3135 8776 sandra.lu@llinkslaw.com
London	
Yuhua Yang Tel: +44 (0)20 3283 4337 yuhua.yang@llinkslaw.com	

The Encryption Law: Gist and Compliance

¹ Shanghai Bureau of Justice: What? The login password is not “the encryption?” What do you know about the Encryption Law? : <https://mp.weixin.qq.com/s/cTWhLLkIRuFWLOVSfKdzhQ>, The last visit was on November 5, 2019.

² Li Ming, Shi Guozhen, Lou Jiapeng, *USB Key Authentication Scheme Based on Encryption Service Platform, Computer applications and software*, 2018(9), p.288.

³ *Risk Tips on Using SHA-1 Cryptographic Algorithm*: http://www.sca.gov.cn/sca/xwdt/2017-04/03/content_1002918.shtml. The last visit was on November 3, 2019.

⁴ *The principal of the State Cryptography Administration answered questions about the Encryption Law of the People's Republic of China*: http://www.oscca.gov.cn/sca/xwdt/2019-10/27/content_1057218.shtml. The last visit was on November 2, 2019.

⁵ Agencies of core encryption and ordinary encryption refer to those engaged in the scientific research, production, services, testing, installation, use and destruction of core encryption and ordinary encryption.

⁶ Article 23 of the *Cybersecurity Law*.

⁷ Article 4 of the *Cybersecurity Level Protection Regulations (Draft for Comment)*.

⁸ Article 35 of the *Cybersecurity Law*.

⁹ Article 9 and 10 of the *Measures for the Security Review of Network Products and Services*.

¹⁰ Article 30 and 31 of the *Critical Information Infrastructure Security Protection Regulations (Draft for Comment)*.