

Cryptography Law of the PRC

Dan Young Business Consultancy — www.danyoungcpa.com
Unofficial English translation prepared for reference only. The official Chinese text prevails.

Contents

Table of Contents	1
Chapter I — General Provisions	1
Chapter II — Core Cryptography and Common Cryptography	2
Chapter III — Commercial Cryptography	3
Chapter IV — Legal Liability	4
Chapter V — Supplementary Provisions	5

Adopted at the 14th Session of the Standing Committee of the Thirteenth National People's Congress on October 26, 2019
Effective: January 1, 2020

Table of Contents

- Chapter I — General Provisions
- Chapter II — Core Cryptography and Common Cryptography
- Chapter III — Commercial Cryptography
- Chapter IV — Legal Liability
- Chapter V — Supplementary Provisions

Chapter I — General Provisions

Article 1 — This Law is enacted for the purposes of regulating the application and administration of cryptography, promoting the development of the cryptography industry, safeguarding network and information security, protecting the lawful rights and interests of citizens, legal persons and other organizations, and maintaining national security and the public interest.

Article 2 — The term "cryptography" as used in this Law refers to technologies, products and services that use specific transformation methods to encrypt, protect or security-authenticate information and the like.

Article 3 — Cryptography work shall adhere to the holistic approach to national security, comply with the leadership of the Communist Party of China, and follow the principles of unified planning, openness and transparency, proper management, and the combination of development and security.

Article 4 — The State shall adhere to the principle that both the development and the regulation of cryptography shall receive equal emphasis, and shall integrate cryptography work into the national economic and social development plan, so as to ensure the alignment of the cryptography industry with the informatization process.

Article 5 — The national cryptography administrative department shall be in charge of the national cryptography work. The local cryptography administrative departments at or above the county level shall be in charge of the cryptography work within their respective administrative regions. State organs and entities involved in cryptography work shall be responsible for the cryptography work of their own organs, entities, and systems.

Article 6 — The State shall implement classified administration of cryptography. Cryptography shall be classified as core cryptography, common cryptography, and commercial cryptography.

Article 7 — Core cryptography and common cryptography shall be used to protect state secret information. The maximum level of state secrets that may be protected by core cryptography is top secret; the maximum level of state secrets that may be protected by common cryptography is secret. Core cryptography and common cryptography are state secrets, and the cryptographic administrative departments shall, in accordance with the provisions of this Law and relevant laws, regulations and state provisions, exercise strict and unified administration over core cryptography and common cryptography.

Article 8 — Commercial cryptography shall be used to protect information that is not a state secret. Citizens, legal persons and other organizations may use commercial cryptography to protect network and information security in accordance with the law.

Article 9 — The State shall encourage and support research in cryptography science and technology, and shall protect intellectual property rights in cryptography in accordance with the law.

Article 10 — The State shall strengthen the cultivation of cryptography professionals and teams, and shall commend and reward organizations and individuals that have made outstanding contributions in cryptography work.

Article 11 — The people's governments at or above the county level shall include cryptography work in their budget at the corresponding level.

Article 12 — No organization or individual may steal other persons' encrypted information, or illegally intrude into other persons' cryptography protection systems, or use cryptography to engage in activities endangering national security, the public interest, or the lawful rights and interests of others. No organization or individual may use cryptography to engage in illegal and criminal activities such as endangering national security, undermining social order, or infringing upon the lawful rights and interests of others.

Chapter II — Core Cryptography and Common Cryptography

Article 13 — The State shall strengthen the scientific planning, development, and utilization of core cryptography and common cryptography, strengthen system building, and improve administrative measures to enhance the security level of core cryptography and common cryptography.

Article 14 — Where state secrets need to be transmitted by means such as wired or wireless communications, or stored or processed in information systems, core cryptography or common cryptography shall be used for encryption protection and security authentication in accordance with laws, administrative regulations and state provisions.

Article 15 — Entities engaged in the research, production, services, testing, equipment, use, and destruction of core cryptography and common cryptography (hereinafter referred to as cryptography work institutions) shall, in accordance with laws, administrative regulations, state provisions, and the requirements of core cryptography and common cryptography standards, establish sound security management rules, adopt strict confidentiality measures and accountability systems, and ensure the security of core cryptography and common cryptography.

Article 16 — The cryptographic administrative departments shall guide and supervise the security management work of cryptography work institutions in accordance with the law, and shall, by means such as

spot checks and on-site inspections, conduct inspections of the security management of core cryptography and common cryptography.

Article 17 — The cryptographic administrative departments shall, in accordance with the needs of their work, establish cooperation mechanisms with public security, state security and other relevant departments, and in conjunction with those departments, carry out the work of handling illegal cryptography activities and investigating cryptography-related criminal offenses, so as to safeguard the security of core cryptography and common cryptography.

Article 18 — The State shall strengthen the work exchange and collaborative support between cryptography work institutions and the armed forces regarding core cryptography and common cryptography.

Article 19 — Where cryptography work institutions need to engage in activities involving the import and export of core cryptography or common cryptography for the purpose of performing their functions, they shall obtain approval from the State Council's cryptography administrative department in conjunction with the foreign trade department.

Article 20 — The cryptographic administrative departments and cryptography work institutions shall establish sound strict systems for supervision and security review, and shall cooperate with the performance of such work, so as to strengthen the security management of their personnel.

Article 21 — The specific measures for the security management of core cryptography and common cryptography shall be formulated by the State Council's cryptography administrative department in conjunction with the relevant departments and submitted to the State Council for approval before implementation.

Chapter III — Commercial Cryptography

Article 22 — The State shall encourage and promote the application of commercial cryptography and the innovation of commercial cryptography science and technology, and shall promote the transformation and application of commercial cryptography science and technology achievements. The State shall improve the standardization system and testing and certification system of commercial cryptography, and formulate and improve national and industry standards for commercial cryptography series products.

Article 23 — The State shall promote the participation of enterprises, public institutions, social organizations, and educational and research institutes in international standardization activities for commercial cryptography.

Article 24 — The State shall encourage and support enterprises, public institutions, social organizations, and individuals to carry out cryptography science and technology research, exchanges, and cooperation in accordance with the law. No organization or individual may impair national security or the public interest, or infringe upon the lawful rights and interests of other organizations or individuals, when engaging in cryptography science and technology exchanges and cooperation.

Article 25 — The State shall promote the development and utilization of commercial cryptography testing and certification technologies, and shall, in accordance with the relevant state provisions, establish a commercial cryptography testing and certification system. Commercial cryptography testing and certification institutions shall obtain relevant qualifications in accordance with the law and shall be responsible for the testing and certification results within the scope of their approved qualifications.

Article 26 — Where network products and services are involved, and where commercial cryptography is used in critical information infrastructure, the commercial cryptography application security assessment shall be conducted. Where commercial cryptography is used in critical information infrastructure, the security review of such commercial cryptography shall be conducted. The entities operating critical information infrastructure shall procure network products and services that involve the use of commercial cryptography

and may affect national security, and shall undergo a national security review in accordance with the law.

Article 27 — Where laws, administrative regulations and relevant state provisions require the use of commercial cryptography for protection, commercial cryptographic products shall be used and commercial cryptographic services shall be provided. The commercial cryptography used shall be included in the list of commercial cryptography testing and certification products.

Article 28 — The State Council's commerce department and the national cryptography administrative department shall implement import licensing for commercial cryptography involving state security or the public interest, and where there are international treaty obligations, shall implement export control in accordance with the law. Where commercial cryptography does not involve state security or the public interest, the import of commercial cryptography shall not be subject to the import license system or be prohibited on the grounds of being state secrets or cryptography. Where commercial cryptography does not involve state security or the public interest, and where there are no international treaty obligations, the export of commercial cryptography shall not be subject to any restriction.

Article 29 — The national cryptography administrative department shall be responsible for the establishment of commercial cryptography technology standards, as well as the establishment, planning, and guidance of the commercial cryptography testing and certification system and the commercial cryptography application security assessment system.

Article 30 — Commercial cryptographic product manufacturers and commercial cryptographic service providers shall ensure the quality, safety, and stable operation of their products and services, and shall not engage in unfair competition or other acts that disrupt market order.

Article 31 — The cryptographic administrative departments and relevant departments and their staff members shall not require commercial cryptographic product manufacturers and commercial cryptographic service providers to provide source code or other proprietary cryptographic information. The cryptographic administrative departments and relevant departments and their staff members shall keep confidential the trade secrets and personal privacy of commercial cryptographic product manufacturers and commercial cryptographic service providers that they learn of in the performance of their duties.

Chapter IV — Legal Liability

Article 32 — Whoever, in violation of the provisions of Article 12 of this Law, steals other persons' encrypted information, illegally intrudes into other persons' cryptography protection systems, or uses cryptography to engage in activities endangering national security, the public interest, or the lawful rights and interests of others shall be pursued for legal liability by the relevant departments in accordance with the Law of the PRC on Cybersecurity and other relevant laws and administrative regulations.

Article 33 — Whoever, in violation of the provisions of Article 14 of this Law, fails to use core cryptography or common cryptography for encryption protection or security authentication in accordance with the requirements shall be ordered by the cryptography administrative department to make corrections or to cease the use of such cryptography, and a warning shall be issued. The directly responsible supervisors and other directly responsible persons shall be punished in accordance with the law.

Article 34 — Where a commercial cryptographic product manufacturer or commercial cryptographic service provider, in violation of the provisions of Article 26 of this Law, fails to conduct a security assessment or security review in accordance with the requirements, the cryptography administrative department shall order it to make corrections and give it a warning. Where the circumstances are serious, the cryptography administrative department may, in conjunction with the relevant departments, impose a fine. The directly responsible supervisors and other directly responsible persons shall be subject to sanctions in accordance with the law.

Article 35 — Where a commercial cryptographic product manufacturer or commercial cryptographic service provider, in violation of the provisions of Article 27 of this Law, fails to use commercial cryptographic products or provide commercial cryptographic services as required, the cryptography administrative department shall order it to make corrections and give it a warning. Where the circumstances are serious, the cryptography administrative department may, in conjunction with the relevant departments, impose a fine. The directly responsible supervisors and other directly responsible persons shall be subject to sanctions.

Article 36 — Whoever, in violation of the provisions of Article 28 of this Law, engages in the import or export of commercial cryptography shall be punished by the State Council's commerce department or the customs authorities in accordance with the law.

Article 37 — Where a commercial cryptographic product manufacturer or commercial cryptographic service provider, in violation of the provisions of Article 30 or Article 31 of this Law, engages in unfair competition or disrupts market order, or fails to keep trade secrets and personal privacy confidential, the relevant departments shall pursue its liability in accordance with the Law of the PRC on the Protection of Consumer Rights and Interests, the Anti-Unfair Competition Law of the PRC, and other relevant laws.

Article 38 — Where any staff member of a cryptography administrative department or other relevant department, in violation of the provisions of this Law, abuses their powers, neglects their duties, or engages in malpractice for personal gain, sanctions shall be imposed in accordance with the law.

Article 39 — Where a violation of the provisions of this Law constitutes a crime, criminal liability shall be pursued in accordance with the law. Where personal injury, property damage, or other harm is caused to another person, civil liability shall be borne in accordance with the law.

Chapter V — Supplementary Provisions

Article 40 — The specific meanings of the following terms in this Law:

- (1) "Cryptography product" refers to a product that uses cryptographic technology to provide encryption protection, security authentication and other functions for information;
- (2) "Cryptography service" refers to a service activity that provides encryption protection, security authentication and other functions for information based on cryptographic technology;
- (3) "Cryptography protection system" refers to a system that is composed of cryptographic products, services and related IT equipment and facilities and that provides encryption protection, security authentication and other functions for information.

Article 41 — The Chinese People's Liberation Army and the Chinese People's Armed Police Force shall separately formulate measures for the administration of cryptography work in accordance with this Law and the relevant regulations of the Central Military Commission.

Article 42 — The national cryptography administrative department shall, in accordance with the provisions of this Law, formulate administrative provisions for commercial cryptography.

Article 43 — Where the use of cryptography to engage in activities related to government affairs is involved, the cryptography administrative department shall provide relevant technical support and services.

Article 44 — This Law shall take effect on January 1, 2020.

Disclaimer: This English translation is provided for informational purposes only. While every effort has been made to ensure accuracy, this is not an official translation. The original Chinese text as published by the National People's Congress of the People's Republic of China shall prevail in all legal matters. Neither Dan Young Business Consultancy nor any of its affiliates shall be held liable for any loss or damage arising from reliance on this translation. For official legal advice, please consult qualified legal professionals.