



/2026

DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES

Authors:



Nguyen Thi Huyen Anh
Senior Associate



Vo Thi Anh Nhi
Paralegal

✉ info@cdlaf.vn

☎ +84 909 668 216

🌐 cdlaf.vn

|



/cdlaflawfirm

DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



Effective from 01 September 2026 and providing detailed regulations for **the Law on Cybersecurity, Decree No. 341/2026/ND-CP** comprehensively regulates business activities involving civil cryptographic products and services, identifies 12 categories of exempted devices, and tightens the three-point matching principle for customs clearance. To assist enterprises in systematizing the new requirements, the following in-depth Q&A has been prepared with reference to each provision, appendix, and form of the Decree. We hope that, through these concise **Q&As**, enterprises can readily grasp the key requirements applicable to the business and import/export of civil cryptographic products under the new regulations.

Q&A CONTENT:

Question 1: How is legal consistency between the Law on Cybersecurity and Decree No. 341/2026/ND-CP reflected in national administration of civil cryptography?

Answer:

Decree No. 341/2026/ND-CP is issued directly pursuant to the Law on Cybersecurity No. 116/2025/QH15. The Decree provides detailed regulations and establishes implementation measures for the Law on Cybersecurity in respect of civil cryptographic activities.

This combination creates a consistent legal framework from border control (import/export) through domestic circulation, distribution, and actual use, ensuring information security in the non-state sector while supporting secure digital economic development.

Question 2: How are state management powers over civil cryptography allocated among the Government Cipher Committee, Ministry of Public Security, Ministry of National Defence, and Ministry of Finance under Decree No. 341?

Answer:

The state management system is subject to a strict inter-agency allocation of responsibilities:

/2026

    /cdlafirm

DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



- Government Cipher Committee: Assists the Minister of National Defence in exercising state management over civil cryptography; directly assesses dossiers and issues, amends, supplements, temporarily suspends, and revokes business licenses and civil cryptographic import/export licenses.
- Ministry of Public Security: Manages cybersecurity in respect of dual-use products incorporating both civil cryptographic and cybersecurity functions, and issues licenses after obtaining written consensus from the Government Cipher Committee.
- Ministry of Finance (General Department of Customs): Coordinates physical control at border gates, carries out customs clearance based on import/export licenses, and immediately suspends customs clearance upon receipt of a decision by the Government Cipher Committee to revoke a license.
- Ministries, ministerial-level agencies, and provincial-level People's Committees: Coordinate state management within their respective functions and powers.

Question 3: What are the legal definitions of “Civil Cryptographic Products” and “Civil Cryptographic Services”? What is the substantive distinction between civil cryptography and cryptography protecting state secrets?

Answer:

Civil Cryptographic Products: Hardware, software, documents, technical equipment, and cryptographic operations designed and manufactured to protect information.

Civil Cryptographic Services: Services comprising information protection using civil cryptographic products; assessment of civil cryptographic products; and security and cybersecurity consultancy using civil cryptographic products.

Substantive distinction: Civil cryptography may only be used to protect information outside the scope of state secrets. Information classified as state secrets must use specialized national cryptographic standards and systems under the strict management of the Ministry of National Defence and the Government Cipher Committee in accordance with laws on protection of state secrets.

DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



Question 4: Analyze the effectiveness and transitional provisions under Article 18 applicable to licenses issued before 01 July 2026.

Answer:

Effectiveness: The Decree officially takes effect from 01 September 2026.

Transitional provisions (Article 18): Business licenses for civil cryptographic products and services and import/export licenses for civil cryptographic products issued before 01 July 2026 remain valid until the expiry date stated in the respective license.

Applications for issuance, amendment, or supplementation of licenses received by the Government Cipher Committee before 01 July 2026 but not yet resolved shall continue to be processed under the former procedures until before 01 July 2026. Applications arising from that date onward must comply with the conditions and procedures under the new Decree.

Question 5: What are the legal requirements for digital signatures when submitting a licensing application online through the National Public Service Portal?

Answer:

To ensure the legal validity of electronic dossiers, an online application must be digitally signed by the enterprise's legal representative (or a duly authorized person) using a valid public digital signature.

Accompanying documents submitted as electronic copies must either bear a certified digital signature or be scanned from originals bearing a digital signature confirming the integrity of the enterprise's documents.

Question 6: What are the detailed minimum technical personnel requirements for an enterprise conducting civil cryptographic business? Which fields of study are considered valid?

/2026



DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



Answer:

Under Article 5.1(a), an enterprise must have at least 02 technical personnel meeting the mandatory standards: holding a bachelor's degree or higher, with the qualification being in one of the following specialized fields: electronics and telecommunications, information technology, mathematics, or information security.

Note: Foreign qualifications must undergo recognition procedures in accordance with regulations of the Ministry of Education and Training to ensure their legal validity in the licensing application dossier.

Question 7: What are the standards applicable to managerial and executive personnel of a civil cryptographic enterprise? What is the legal solution where the manager has graduated in a non-technical field?

Answer:

Article 5.1(a): The enterprise must have 01 managerial/executive officer with a bachelor's degree or higher in electronics and telecommunications, information technology, mathematics, or information security.

Non-specialized degree: An additional information security and cybersecurity training certificate is required.

Question 8: How is the “appropriate facilities” requirement under Article 5 concretized to ensure operational safety and prevent loss of test data?

Answer:

The enterprise must demonstrate that it has equipment and facilities appropriate to the registered scope, target users, and field of provision of civil cryptographic products and services. To ensure operational safety, the facilities should include: office premises, laboratories or production/testing areas with independent access-control security systems; computers and servers used for programming, packaging, or configuring cryptographic products that are securely network-isolated (with internal networks separated from the public Internet or protected by dedicated firewalls); and secure physical

/2026



DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



storage systems for original technical documents and cryptographic key-generation and key-loading devices.

Câu 9: What structure and mandatory contents must be included in the “Technical Plan” (Form No. 03, Appendix III) submitted with a licensing application?

Answer:

The Technical Plan is the core document demonstrating the enterprise’s actual capabilities and must contain the contents specified in Form No. 03:

Licensed product: General introduction to the product; functions and cryptographic technical characteristics.

Cryptographic technical characteristics: Clearly state the cryptographic algorithms and key parameters used in the product (symmetric, asymmetric, etc.); and assessment or certification results issued by competent authorities, if any.

Deployment model: Description of the system model and the principles for using the product to secure and authenticate information.

Cryptographic parameter configuration: Documentation describing the setup and configuration of algorithms and management of cryptographic keys in the product.

Product warranty and maintenance plan: Specific procedures, scope, and locations for warranty and maintenance.

Question 10: Question 10: What SLA commitments must be stated in the Technical Plan?

Answer:

In the Technical Plan dossier (Form No. 03), the enterprise must provide detailed service-level commitments (SLA):

/2026



DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



For customers: Commitments on technical incident response times; availability of information-security services; 24/7 technical support procedures; and compensation provisions where service disruption results from the enterprise's system failures.

For regulatory authorities: A commitment to ensure service quality complies with applicable national technical regulations and readiness to coordinate in handling widespread information-security incidents.

Question 11: What stringent technical standards must the warranty and maintenance plan for civil cryptographic products under Form No. 03 satisfy?

Answer:

Under Part II of Form No. 03, the warranty and maintenance plan must clearly specify:

Maintenance procedures: A detailed process for applying software security patches without compromising integrity or causing leakage of users' cryptographic keys.

Maintenance scope: Clear limits on technical intervention. Technical personnel are prohibited from unauthorized access to or storage of customers' private keys or encrypted data during hardware maintenance.

Warranty and maintenance address: A fixed, secure physical location clearly registered with the Government Cipher Committee.

Question: Why must CCPS undergo inspection, conformity certification, and conformity declaration before commercial circulation?

Answer:

Mandatory requirement: Civil cryptographic products must undergo conformity inspection and certification before being placed on the market to

/2026



DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



ensure that cryptographic quality meets applicable standards.

Regulatory mechanism: The Government Cipher Committee is responsible for managing the quality of civil cryptographic products and services by designating and supervising conformity assessment and certification organizations.

This mechanism protects end users from products containing dangerous cryptographic vulnerabilities or embedded spyware/malicious code and safeguards national cybersecurity.

Question 13: How are the procedure and timeline for assessment and issuance of a new Business License streamlined and monitored?

Answer:

The administrative process is designed to be expeditious and transparent.

- Day 1: Receipt of dossier. The Government Cipher Committee checks validity within 01 working day. If the dossier is incomplete, it issues a written request for supplementation.
- Days 2–4 (03 working days): The enterprise is responsible for amending, supplementing, and completing the dossier for resubmission.
- Day 5: The Government Cipher Committee issues a written refusal within 01 working day if the enterprise fails to complete the dossier within the prescribed period or the dossier remains unsatisfactory.

In-depth assessment (12 working days): From the date of receipt of a complete and valid dossier, the Government Cipher Committee conducts substantive assessment and issues the Business License for civil cryptographic products and services (Form No. 04). Any refusal must be notified in writing with reasons stated.

Question 14: What are the substantive legal and documentary differences between “Amendment of a License” and “Supplementation of a License” for civil cryptographic business?

/2026



DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



Answer:

License amendment: Applies to administrative/legal changes that do not alter the technical nature of the business, including a change of enterprise name or legal representative. The dossier is simpler and does not require submission of a new Technical Plan.

License supplementation: Applies where the enterprise expands its physical or technological operations, including a change of head-office address or addition of new civil cryptographic products/services. The dossier must include a detailed Technical Plan for the supplementary scope for reassessment.

Question 15: What are the procedure, dossier, and processing time for an application to “Amend the Business License” for civil cryptographic business?

Answer:

The procedure is implemented under Article 6:

Dossier: The enterprise submits 01 dossier comprising: an application for amendment of the License under Form No. 02, Appendix III; a copy of the issued Business License; and documents evidencing the legal change (enterprise name or representative).

Procedure and timeline:

The Government Cipher Committee examines the dossier within 01 working day.

If unsatisfactory, a supplementation notice is issued and the enterprise has 02 working days to complete the dossier.

If the deadline is missed, a written refusal is issued within the following 01 working day.

Assessment and issuance of the amended License within 05 working days from receipt of a complete and valid dossier.

/2026



DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



The enterprise must return the hard copy of the old License within 02 working days from the date the new License is issued.

Question 16: What are the procedure, dossier, and processing time for an application to “Supplement the Business License” for civil cryptographic business?

Answer: The procedure is implemented under Article 7:

Dossier: Application for supplementation of the Business License (Form No. 02) and the Technical Plan for the supplementary products/services under Form No. 03.

Procedure and timeline:

- Validity check within 01 working day.
- The enterprise has 02 working days to supplement the dossier where deficiencies are identified.
- A written refusal is issued within 01 working day if the enterprise fails to complete the supplementation within the prescribed period.
- The Government Cipher Committee conducts an in-depth assessment of the new Technical Plan and issues the supplementary License within 09 working days from receipt of a complete and valid dossier.

Question 17: What three circumstances may result in the temporary suspension of a civil cryptographic business for up to 06 months?

Answer:

Under Article 8.1, an enterprise may be subject to temporary suspension of its civil cryptographic business activities for a period not exceeding 06 months in the following cases:

- Providing civil cryptographic products or deploying civil cryptographic services inconsistently with the contents of the issued Business License.

/2026

    /cdlaflawfirm

DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



- Failing to satisfy any mandatory requirement concerning specialized personnel (at least 02 qualified technical personnel and 01 qualified manager), facilities, or the Technical Plan standards prescribed in Article 5.1.
- Other violations prescribed by law (such as violations of cybersecurity or public order requirements).

Question 18: What circumstances mandatorily result in “Revocation of the Business License” under Article 8? What are the legal consequences for ongoing service contracts?

Answer:

Revocation cases (Article 8.2): Falsification of the licensing dossier; alteration or erasure of License contents; a License issued by an incompetent authority or through an improper procedure; failure to commence services within 01 year from licensing without a legitimate reason; expiry of the License; failure to remedy the grounds for suspension upon expiry of the 06-month suspension period; or cessation of business, dissolution, or bankruptcy of the enterprise.

Legal consequences: The enterprise loses its legal capacity to provide civil cryptographic products/services to the market;

All ongoing information-security service contracts with customers must be terminated; the enterprise is responsible for compensating customers for contractual losses and must hand over, destroy, or transfer customers' cryptographic keys in accordance with applicable security requirements.

Question 19: How is the condition of “failure to commence service provision within 01 year from licensing” monitored and enforced by the competent authority?

Answer:

Monitoring: The Government Cipher Committee monitors enterprise activities through periodic reports submitted before 31 December each year (Form No. 07), as well as post-licensing supervision and periodic or ad hoc inspections at the enterprise's premises.

/2026



DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



Enforcement: If, after 01 year from issuance of the civil cryptographic Business License, inspection and reporting establish that the enterprise has generated no sales, provided no products, or had no actual service customers and cannot provide a written legitimate force majeure justification, the Government Cipher Committee will issue a decision revoking the Business License.

Question 20: What are the necessary and sufficient conditions for an enterprise to obtain an import/export license for CCPs?

Answer:

Under Article 10.1, the enterprise must satisfy all 03 mandatory conditions below:

- Hold a valid Business License for the corresponding civil cryptographic products and services.
- Imported civil cryptographic products must undergo conformity certification and conformity declaration in accordance with Vietnamese technical standards.
- The recipient and intended use of the CCPs must not prejudice national defence, national security, public order, or social safety.

Question 21: What is the validity period of a civil cryptographic import/export license? Why is it significantly shorter than the Business License?

Answer:

Validity period: Up to 03 years.

Rationale: The Business License is valid for 10 years to provide stability for the enterprise's business rights. By contrast, the import/export license is valid for only 03 years to enable strict control over the cross-border movement of technological equipment. This allows the competent authorities to continuously reassess the technical safety of imported products and prevent obsolete equipment containing security vulnerabilities or outdated encryption algorithms from entering the Vietnamese market and creating risks to national information security.

Question 22: What core technical information must be included in the application dossier for an import/export license for CCPs (Form No. 05)?

/2026



DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



Answer:

The dossier is submitted in 01 set and includes an application for an import/export license under Form No. 05, Appendix III, which must contain the following core information:

- Name of the civil cryptographic product for which the license is requested.
- Manufacturer information, country of manufacture, and model/part number of the product.
- Detailed cryptographic technical characteristics and the technical standards and regulations applicable to the product.
- The number of the enterprise's valid principal Business License for civil cryptographic products and services.
- Detailed list of the products proposed for export/import (form attached to the application).

Question 23: What are the procedures and timelines for receiving, reviewing, and assessing an import/export license application?

Answer:

The procedure is prescribed in Article 10.3:

- Validity check (01 working day): The Government Cipher Committee reviews the dossier and requests supplementation if invalid. The enterprise has 01 working day to complete it; otherwise, a written refusal is issued the next working day.
- Assessment and licensing (06 working days): The Government Cipher Committee assesses the complete, valid dossier and issues the import/export license (Form No. 06). Refusals must be notified in writing with reasons.

Question: In what circumstances will an enterprise's import/export license for civil cryptographic products be revoked under Article 11?

Answer:

The enterprise's import/export license shall be revoked immediately upon the occurrence of any of the following circumstances:

- Falsification of the licensing dossier or unauthorized alteration/erasure resulting in inaccurate contents of the import/export license.
- The license was issued by an incompetent authority or contrary to the prescribed dossier or procedures.

/2026



DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



- The enterprise has its Enterprise Registration Certificate/Investment Registration Certificate revoked, is dissolved, bankrupt, or ceases operations.
- The imported civil cryptographic product has reached the end of its circulation period as notified by the manufacturer, or a competent authority identifies a serious defect causing information-security risks that cannot be remedied.
- The enterprise has been licensed but does not conduct export/import activities throughout the validity period of the license (except where it has notified a temporary suspension of business).
- The enterprise fails to maintain all applicable import/export conditions throughout its operations.
- The enterprise's principal Business License for civil cryptographic products and services is revoked.

Question 25: What is the inter-agency coordination mechanism between the Government Cipher Committee and the Customs Authority upon revocation of a civil cryptographic import/export license?

Answer:

A strict coordination mechanism is established to immediately prevent customs clearance of non-compliant goods:

Under Article 11.2, immediately after a decision is issued to revoke an import/export license for civil cryptographic products, the Government Cipher Committee must promptly send the decision to the Customs Authority.

The Customs Authority shall rely on the revocation decision to immediately suspend customs procedures and customs clearance for the civil cryptographic products identified in the revocation decision.

The Ministry of Finance shall closely coordinate with the Government Cipher Committee in performing this state-management function over import and export activities.

Question 26: Analyze the “dual application” principle when consulting the list of CCPs subject to import/export licensing (Appendix II).

/2026



DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



Answer:

Under Article 9.3(a), the list in Appendix II applies only to products satisfying all three criteria simultaneously (dual application):

- Matching HS code (classification code for imported/exported goods).
- Matching commercial goods description.
- Matching detailed cryptographic technical description of the listed product.

Note: Where there is a discrepancy in determining the HS code between the list attached to this Decree and the current Vietnam List of Imports and Exports, the commodity code shall be determined in accordance with customs law.

Question 27: What categories of data are covered by the enterprise's obligations under Article 12 to establish, retain, and protect the confidentiality of customer information systems?

Answer:

Under Article 12.1(c), the enterprise is responsible for establishing, retaining, and strictly protecting customer information, including:

- Name of the organization/individual, address, telephone number, email, and legal representative of the customer.
- Type of business/activity and quantity of civil cryptographic products/services provided.
- Purpose of use, installation address, or deployment scope of the products/services.
- Records and detailed documentation concerning the technical solution, cryptographic technology, and cryptographic key system applied to the customer.

Question 28: Under what circumstances must an enterprise proactively refuse to supply civil cryptographic products/services to a customer?

Answer:

Under Article 12.1(d), an enterprise has a mandatory legal obligation to proactively refuse to provide products or terminate civil cryptographic services when it discovers that the customer falls into any of the following circumstances:

/2026



DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



- The customer violates laws governing the use of civil cryptography (e.g., using cryptography to conceal criminal conduct or activities intended to undermine national security).
- The customer violates cybersecurity laws.
- The customer breaches written commitments agreed between the parties regarding the scope and purpose of use of CCPs/services.

Question 29: What are the specific deadlines and contents of the enterprise's annual periodic reporting obligation (Form No. 07, Appendix III)?

Answer:

Annual reporting obligations of the enterprise:

Reporting deadline: Before 31 December each year.

Receiving authority: Government Cipher Committee.

Mandatory contents (Form No. 07): Report on actual business activities involving civil cryptographic products/services; detailed report on actual quantities exported/imported; and a consolidated record of customer information, customer lists, and purposes of use during the year.

Question 30: What compliance obligations apply to organizations and individuals (customers) using CCPs/services under Decree No. 341?

Answer:

Under Article 12.2, users have the following obligations:

Strictly comply with commitments made with the supplier concerning management and use of cryptographic keys and procedures for transfer, repair, maintenance, and destruction of civil cryptographic products.

/2026



DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



Provide all information relating to cryptographic keys to competent state authorities upon a lawful request.

Actively cooperate with and facilitate state authorities in implementing measures to prevent information theft, decryption, or unlawful use of cryptographic products.

Question 31: What is the mandatory declaration procedure for organizations and individuals using civil cryptographic products not supplied by a domestically licensed enterprise (Form No. 08)?

Answer:

Under Article 12.2(d), this requirement is intended to control information security in respect of unregulated or self-imported cryptographic products:

Requirement: An organization or individual using cryptographic products not supplied by an enterprise licensed to conduct business in Vietnam must prepare a Declaration Form under Form No. 08, Appendix III, and submit it to the Government Cipher Committee.

Declaration information: Product name, origin, model/part number, country of manufacture, applicable standards and technical regulations, purpose, timing, scope, and actual scale of use.

The following must also be enclosed: product technical documentation, system usage diagram, and an origin explanation for self-developed open-source cryptographic products.

Question 32: Which special categories of entities in Vietnam are exempt from the obligation to declare the use of foreign cryptographic products under Form No. 08?

Answer:

/2026



DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



Under Article 12.2(d), the following special entities are exempt from the declaration obligation when using foreign civil cryptographic products:

- Foreign diplomatic missions in Vietnam.
- Foreign consular offices in Vietnam.
- Representatives of intergovernmental international organizations in Vietnam.

Question 33: What on-site inspection activities may competent state management authorities conduct in respect of enterprises conducting civil cryptographic business?

Answer:

Under Article 16, periodic or ad hoc inspections by competent state authorities (the Head of the Government Cipher Committee or the relevant specialized regulatory authority) comprise three principal areas:

- Verification of the legality of documents in the enterprise's legal dossier and comparison of the business activities stated in the Business License with the enterprise's actual activities.
- Inspection of compliance with operational conditions, reporting obligations, and customer data confidentiality requirements under this Decree and relevant legislative documents.
- Physical inspection of civil cryptographic products being marketed, cryptographic services being provided, and activities related to the enterprise.

Question 34: What core product groups are included in the list of conditional civil cryptographic products for business (Appendix I)?

Answer:

Part I of Appendix I specifies 07 groups of civil cryptographic products subject to mandatory regulatory control:

- Products for generating, managing, or storing cryptographic keys.
- Products for securing stored data.
- Products for securing data exchanged over networks.

/2026



DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



- Products for securing IP traffic.
- Products for securing analog and digital voice communications.
- Products for securing radio communications.
- Products for securing fax and telegraph communications.

Question 35: What technical exclusion criteria apply to operating systems, Internet browsers, and general-purpose software incorporating cryptography so that they are not treated as licensed civil cryptographic products?

Answer:

Under Item I, Explanation, Clause 1 of Appendix I, these products are excluded where they simultaneously satisfy the following criteria:

- Cryptography is built into the operating system, Internet browser, or software, but cryptography is not the principal function of the product.
- The product is widely used and designed for consumers to install and use themselves without requiring any specialized technical support from the supplier.

Question 36: Why are ordinary mobile phones excluded from the requirement to obtain a civil cryptographic business license? What technical criterion distinguishes them?

Answer:

Under Item I, Explanation, Clause 3 of Appendix I, ordinary mobile phones are excluded where they satisfy the following technical criteria:

- The mobile phone does not have an independent dedicated end-to-end encryption capability for securing transmitted voice/message data.
- Cryptography is integrated only at the level of standard public telecommunications network transmission, and users cannot modify the algorithm.

Question 37: What is the technical basis for excluding smart cards and software/multimedia copyright protection devices (DRM)?

DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



Answer:

These products are excluded based on their specific intended use:

Smart cards: Specifically manufactured with limited cryptographic functionality solely to protect personal information or facilitate ordinary access (such as parking cards or ATM cards for standard financial transactions), and not used to encrypt other network communication data flows.

Digital Rights Management (DRM) devices: Designed to use cryptographic functions solely to prevent unauthorized copying of software or control access rights to publicly readable/writable data and copyrighted audio, image, and video content.

Question 38: What is the technical basis for excluding self-encrypting drives (SED) and integrated circuits using TPM technology?

Answer:

The exclusion grounds are specifically provided in Appendix I:

- Self-Encrypting Drive (SED): Cryptography is hard-wired into the drive controller solely to protect physically stored data if the device is lost or stolen, automatically encrypting the data without allowing users to customize algorithms or independently configure key management.
- Trusted Platform Module (TPM): Cryptography is used solely to authenticate hardware integrity and protect system passwords during boot-up, and does not perform dedicated network data encryption functions.

Question 39: Are products that only incorporate cryptography for cybersecurity monitoring, identity authentication, or remote access subject to civil cryptographic licensing?

Answer:

No. Under Item I, Explanation of Part I of Appendix I, the following product lines are completely excluded from conditional civil cryptographic business regulation:

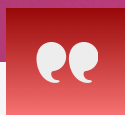
/2026



DECREE NO. 341/2026/ND-CP: Q&A ON CIVIL CRYPTOGRAPHIC PRODUCTS AND SERVICES



- Products whose functions are limited to identity authentication and which have no data-encryption functionality.
- Products using cryptographic techniques for remote access or system-device administration.
- Products using cryptographic techniques for monitoring, preventing, or detecting cyberattacks (dedicated cybersecurity functions).



CDLAF supports enterprises with procedures for obtaining business and import/export licenses for civil cryptographic products. For legal advice and support, please contact:

- ***CDLAF Law Firm***
- Hotline/Zalo: **+84 909 668 216**
- Email: **info@cdlaf.vn**



OUR ECOSYSTEM



OFFICE LEASING



CORPORATE COMPLIANCE

-
-  **Head Office:** R7.01, Transimex Building, 172 Hai Ba Trung Str., Tan Dinh Ward, Ho Chi Minh City, Vietnam.
 -  **Branch Office:** 330 Nguyen Van Troi Str., Phu Loi Ward, Ho Chi Minh City, Vietnam.
 -  **Transaction Office:** 101/20 Street 11, Thu Duc Ward, Ho Chi Minh City, Vietnam.
-

 info@cdlaf.vn

 +84 909 668 216

 cdlaf.vn

|



[/cdlaflawfirm](https://www.instagram.com/cdlaflawfirm)