GM

CRYPTOGRAPHIC INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GM/T 0066-2019

Implementation guide to capability construction criteria of production and guarantee for commercial cryptographic products

商用密码产品生产和保障能力建设实施指南

Issued on: July 12, 2019 **Implemented on: July 12, 2019**

Issued by: State Cryptography Administration

Table of Contents

Implementation guide to capability construction criteria of production and guarantee for commercial cryptographic products

1 Scope

This standard specifies the methods, procedures, reports and key points for the implementation of the evaluation of capability criteria of production and guarantee for commercial cryptographic products.

This standard is applicable to the guide for construction of production capacity, quality assurance capability, security assurance capability, service assurance capability of production organizations.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

GM/T 0008-2012 Cryptography test criteria for security IC

GM/T 0028-2014 Security requirements for cryptographic modules

GM/T 0065-2019 Specification for capability construction of production and guarantee for commercial-cryptographic products

GM/Z 4001 Cryptographic terms

3 Terms and definitions

The terms and definitions as defined in GM/Z 4001 and GM/T 0065-2019 as well as the following terms and definitions are applicable to this document.

3.1

Formal examination

Review the formal compliance, completeness and validity of the application materials as submitted by the production organization.

3.2

Substantive examination

On the basis of formal review, review whether the production organization has the qualifications for the main body, whether the application is true, whether the submitted documents and certificates are true, valid, complete, compliant; whether they meet the requirements of national laws and regulations. It includes written reviews and on-site audits, etc.

4 Overview of implementation

4.1 Evaluation content

The evaluation content includes evaluation elements such as basic items, declaration items, evaluation items, etc.

The basic items include the legal person qualification items of the production organization, the main technical personnel items, the product research and development items, the industry management compliance items, etc.

The declaration items include the key personnel information of the production organization, the nature of the organization, data management, etc.

The evaluation items include the production capacity, quality assurance capability, security assurance capability, service assurance capability of the production organization.

4.2 Evaluation method

The production and guarantee capabilities of commercial cryptographic products are evaluated by a combination of the organization’s self-evaluation and expert scoring. Quality assurance, security assurance, service guarantee capabilities shall be the organization's self-verification items, for which the production organization provides proofs of the production and guarantee capability of the commercial cryptographic product. Combined with the basic items and declaration items of the production organization, the expert group will score and judge according to the evaluation elements of the evaluation items.

b) Key positions should be held by senior personnel with rich experience and profound professional skills;

c) The job setting and personnel qualifications of the production organization shall meet the human resources setting; the judging criteria include whether the job setting is complete and reasonable, whether the job qualifications are clear.

5.3.1.1.2 Main technical team

a) It shall verify the number of personnel engaged in cryptographic technology design, implementation, detection or testing and technical support in the production organization; as well as the proportion of personnel with a bachelor degree or above in the technical team, etc.;

b) It shall assess the cryptographic professional technical ability of the person in charge of the core technology; the evaluation criteria shall include at least professional experience, academic qualifications, research results and awards, etc.

5.3.1.1.3 Technology accumulation and advantages

a) The products applied by the production organization shall conform to the main business direction of the production organization;

b) The production organization shall effectively use its own scientific research resources in the product production process, to ensure that the product has a high technical level;

c) The production organization shall have relevant scientific research results and technical reserves. The production organization shall have professional technical research results in the field related to the applied product and the results have been practically applied; the production organization shall have carried out scientific research on similar projects to the applied product and have technical reserves in the past 5 years;

d) The professional technical level of the production organization shall meet the needs of the applied product; it should reach the domestic advanced level.

5.3.1.1.4 Technological innovation

a) The production organization shall have authorized patents, software copyrights, integrated circuit layout registration, etc.;

b) The production organization shall clarify whether the applied product has been identified by experts to fill the gap in domestic or international industry applications;

b) The production organization shall establish product quantity management requirements and ensure the accuracy of quantity management.

5.3.1.2.4 Supply Management

a) The production organization shall assess whether the supplier or the outsourcing organization has the corresponding qualifications and technical capabilities; provide the qualification and ability certification materials of the supplier or the outsourcing organization;

b) The production organization shall have control and supervision measures for the supplier's supply link and outsourcing processing link;

c) The production organization shall set up a full-time responsible for the quality monitoring, measurement and acceptance of suppliers and outsourcing organizations; provide quality criteria for externally processed products, to ensure that the outsourcing process has no impact on product quality;

d) The production organization shall sign a quality assurance agreement with the supplier and conduct regular quality reviews; have clear management regulations on outsourced personnel, processes and outsourcing work.

5.3.1.3 Production conditions

5.3.1.3.1 Production site

a) The production organization shall have the right to use the land and house of the production site; the production facilities and storage sites shall meet the needs;

b) In the case of self-owned production sites, the property rights certificate or lease contract of the production site shall be checked, to confirm that the production organization has a fixed production site and has the infrastructure to meet the basic needs of production (such as water, gas, electricity supply facilities, etc.) and supporting service facilities (such as transportation, communication, information technology, etc.), to ensure the safe and reliable operation of production facilities;

c) If the production organization adopts outsourcing processing, it shall have a corresponding storage place. The storage place shall meet the needs of product storage and ensure that the product is protected from various physical damage;

d) It may evaluate the production sites for outsourcing processing.

5.3.1.3.2 Production equipment

testing system, to ensure the quality of the product;

b) The development system should include system integration design specifications, system integration management specifications, coding specifications, design specifications, development management specifications, change management specifications, etc.;

c) The testing system should include unit testing, integration testing, system testing, acceptance testing, etc.

5.3.2.2.2 R&D process management

a) The production organization shall manage and control the R&D process;

b) The R&D process of the production organization shall be tracked and coordinated by a dedicated person; the entire process shall have a clear stage division and process management;

c) The production organization shall periodically review and audit the project; manage and control changes;

d) The production organization shall have a detailed technical design plan; it shall archive technical documents;

e) The production organization shall control, regularly calibrate and maintain the test equipment used for testing, measurement and product quality determination, to maintain the accurate performance of the test equipment.

5.3.2.2.3 Version management

a) The production organization shall develop a configuration management system;

b) The production organization shall set up configuration management personnel;

c) Production organizations should use configuration management tools and methods.

5.3.2.2.4 Quality problem management

a) The production organization shall have management and control measures for quality problems; perform follow-up management on the resolution of quality problems;

b) The production organization shall establish a quality problem handling system and process; have the ability to track and count quality problems; make requirements for the timeliness of quality problem handling; conduct

who have left the company;

i) The production organization shall provide appropriate encouragement and punishment for correcting and endangering security behaviors.

5.3.3.2 Security management

a) The production organization shall establish and implement security production rules and regulations; understand the national and industry security production regulations and standards; formulate a security production responsibility system and secure operation procedures.

b) The production organization shall divide the physical security area and appoint the corresponding person in charge. The important area shall be equipped with the access control system to record the visits and the records can be checked. The monitored content records shall be kept for at least 30 days. Important assets entering and exiting organizations or important areas shall implement an approval mechanism. Important areas shall have temperature and humidity requirements and be equipped with uninterrupted power supplies. The person in charge of security shall regularly inspect and record the equipment room's firefighting, lightning, leak-proof, dust prevention procedures.

c) The production organization shall have computer software protection measures and network protection measures. Important information assets shall be maintained by dedicated personnel; there shall be remote and mobile office security management systems or provisions. It shall identify the computer asset vulnerabilities and potential threats; establish information security strategies adapted to the organization; guarantee information security in the process of information storage, exchange and destruction. Meanwhile it shall have an emergency disaster preparedness plan.

d) The production organization shall have control over the organization's access mechanism. Important areas shall be identified and focused on protection; access to the organization's intranet through the network shall have access control; employees shall be subject to the access policy control for information access; key data shall be securely transmitted, received and processed; data on storage media shall be deleted or the storage media destroyed in a timely manner; it shall record and store information in detail.

e) The production organization shall have a security management system for mobile storage media. It shall establish a management system and security strategy for the application, use, replacement, maintenance and scrapping of storage media; keep the records of regular inspections of key

5.3.4.2 Emergency response capability

a) The production organization shall establish an emergency response mechanism and make overall planning and coordinate management;

b) The production organization shall have the ability to solve unexpected problems; restore the agreed service requirements as soon as possible through the identification and analysis of the cause of the problem; minimize the impact on the business;

c) The production organization shall promptly report the progress and latest status to the user during the resolution process.

5.3.4.3 Service response mode

a) The production organization shall establish a complete service network; provide product services that meet the needs of the user in combination with the product application;

b) The production organization shall clarify the content of product technical service commitments and operational service plans;

c) The production organization shall establish official acceptance channels in various ways such as call centers, networks, local customer service departments, to ensure that customers can provide feedback and questions;

d) The production organization shall record the user's correspondence and complaints; specify the time limit for handling the problems; report the results of the corresponding handling;

e) The production organization shall establish customer files;

f) The production organization shall conduct customer satisfaction surveys on service quality.

5.3.4.4 Service management system certification

The ISO 20000 certification of the information technology service management system of the production organization shall be verified. For the production organization that has obtained the corresponding certification and is within the validity period, it can score the service guarantee capability item.

first.

If it fails to pass the formal review, the production organization will make corrections and resubmit the application materials after receiving the notice, to perform formal review again.

6.3.2 Pre-evaluation

6.3.2.1 Evaluation start

The evaluation team leader shall be determined, as well as two or more experts shall form the evaluation team. The number of the evaluation team members shall be no less than 3. The members of the evaluation team shall undertake the confidentiality of the evaluation object and evaluation content.

Independent evaluation supervisors shall be set up, to supervise the standardization and fairness of the evaluation work.

The purpose, scope, basis, method of the evaluation shall be determined.

The evaluation item scoring table shall be compiled, including basic items, declaration items, evaluation items. The evaluation items are scores, as shown in Appendix A.

6.3.2.2 Pre-evaluation

The evaluation team conducts pre-evaluation of the application materials, mainly to review the basic items, declaration items and other content and supporting documents.

It must meet all requirements of the basic items; review the authenticity and compliance of the relevant materials. If there is a non-conformity, or there is a situation that does not match the facts, terminate the evaluation process and record the non-conformity in the evaluation result.

The declaration item is not to be used as the basis for judgment and evaluation, but it shall guarantee the authenticity of relevant materials. If the necessary declaration items are missing, or there is a situation that does not conform to the facts, terminate the evaluation process and record the non-conformity in the evaluation result.

6.3.3 On-site audit

6.3.3.1 Audit judgment

The evaluation team shall judge whether on-site audits are required according to the specific conditions of the production organization. If the authenticity of the application materials is lack of supporting evidence, the application

The evaluation results are presented in the form of evaluation reports. The evaluation team shall provide a unified evaluation conclusion.

7 Evaluation report

7.1 Report content

The content of the report shall be complete, truthful, objective; clarify the basic information of the production organization, the basic information of the applied product, the evaluation team members, the evaluation supervisor, the evaluation time, whether the evaluation materials are complete, whether the basic items meet the requirements, whether there will be on-site audit, the descriptions on declaration items and evaluation items, the evaluation conclusions.

7.2 Report form

The evaluation report is in the form of a table, as shown in Appendix B.

7.3 Reporting requirements

7.3.1 Evaluation time

The evaluation report shall specify the time when the evaluation work is started, in the format of "××××year××month××day".

7.3.2 Evaluation location

The evaluation report specifies the location of the evaluation.

7.3.3 Evaluation team and evaluation supervisor

The evaluation report clearly specifies the name of the evaluation team and the evaluation supervisor.

7.3.4 Basic information of production organization

The evaluation report shall specify the name of the production organization, its type, the province (district, city) to which it belongs, wherein the name and type of the production organization shall be filled out in accordance with its business license.

7.3.5 Basic information of application product

for the product type and security level of the application; clarify the time to make the conclusion.

7.4 Report archiving

The evaluation materials shall be archived. The archived materials include product varieties and model application materials, evaluation reports, evaluation records. See Appendix D.

Evaluation records include independent score sheets of evaluation members and records of supervisors, etc.

8 Descriptions of implementation points

8.1 Evaluation organization

8.1.1 Evaluation process

The evaluation work shall be carried out in accordance with the evaluation procedures as specified in Chapter 6, including material review, pre-evaluation, on-site audit, expert evaluation.

It shall be determined whether an on-site audit is required according to the background of the production organization, the type of product to be licensed, the application materials.

8.1.2 Expert scoring

Expert evaluation is carried out by means of scoring. The scoring results include individual score and comprehensive score.

Individual scores include four individual scores: production capability, quality guarantee capability, security guarantee capability, service guarantee capability. The average of the total scores in the scoring results of multiple experts is used as the comprehensive score; the average of the individual scores in the scoring results of multiple experts is used as the individual score.

8.1.3 License requirements for different levels of commercial cryptographic products

The production and guarantee capabilities of commercial cryptographic products shall be compatible with the security level of commercial cryptographic products.

See Table 1 for the requirements for individual scores and comprehensive

Appendix E

(Informative)

Product use requirements in important areas

This Appendix gives product usage requirements in important areas.

Article 31 of the Cybersecurity Law of the People's Republic of China stipulates that the state shall protect important industries and fields such as public communication and information services, energy, transportation, water conservancy, finance, public services, e-government, other important industries and fields, as well as the key information infrastructure which, if damaged or lost or subject to data leakage, may seriously endanger the national security, national economy, people's livelihood, public interest, on the basis of the network security hierarchical protection system.

Article 18 of the Cryptography Law of the People's Republic of China (draft) stipulates that the state conducts classified and grading evaluation of the security of cryptographic applications of critical information infrastructure; follow the requirements of national security review to carry out security reviews on the cryptographic products, cryptography-related service, cryptographic guarantee system which affect or may affect the national security.

The user selects commercial cryptographic products with different security levels according to application scenarios and security protection requirements.

Considering the uncontrollable risks that may exist in the key personnel of the statement item, the nature of the organization, the data management, the recommended system security level protection requirements and the selection of commercial cryptographic products are as shown in Table E.1.

Commercial cryptographic products used in important fields and critical information infrastructure shall refer to Table E.1, to choose products that are no less than three-level protection.

The user shall evaluate whether it has the capability of commercial encryption product service, upgrade and new product R&D based on the registered capital structure and the scale of the registered capital of the production organization.

The user can refer to GM/T 0065-2019 to evaluate the production and guarantee capabilities of the commercial cryptographic product provider; only after the evaluation is qualified can it be purchased and used.

The user selects the product with reference to the declaration item information of the commercial encryption product provider, which mainly includes the key

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------