

ICS 35.040
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 38625-2020

**Information security technology - Security test requirements for
cryptographic modules**

信息安全技术 密码模块安全检测要求

(English Translation)

Issued on: April 28, 2020

Implemented on: November 1, 2020

**Issued by: State Administration for Market Regulation, China National
Standardization Administration**

Table of Contents

Preface
1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviations
5 Overview
6 Safety testing requirements
6.1 General requirements
6.2 Cryptographic module specifications
6.3 Password module interface
6.4 Roles, services and identification
6.5 Software/Firmware Security
6.6 Operating environment
6.7 Physical Security
6.8 Non-intrusive security
6.9 Management of sensitive security parameters
6.10 Self-test
6.11 Life Cycle Guarantee
6.12 Mitigation of other attacks
6.13 Documentation requirements
6.14 Password module security policy
6.15 Approved safety features
6.16 Approved methods for generating and establishing sensitive security parameters
6.17 Approved authentication mechanism
6.18 Non-invasive attacks and common mitigation methods
Appendix A (Normative Appendix) Security Level Correspondence Table

1 Scope

According to GB/T 37092-2018, this standard specifies the testing requirements for cryptographic modules and the corresponding material requirements for inspection.

This standard applies to the testing of cryptographic modules submitted for inspection by

testing organizations, and can also be used to guide the self-testing of cryptographic module developers.

2 Normative references

The following documents are indispensable for the application of this document. For dated reference documents, only the dated version applies to this document.

For undated references, the latest version (including all amendments) applies to this document.

GB/T 25069-2010 Information Security Technical Terms

GB/T 37092-2018 Information Security Technology Cryptographic Module Security Requirements

3 Terms and definitions

The terms and definitions defined in GB/T 37092-2018 and GB/T 25069-2010 apply to this document.

4 Abbreviations

The following abbreviations apply to this document.

5 Overview

Chapter 6 describes in detail the requirements for the materials provided to the testing organization by the submitting manufacturer and the program requirements used by the testing organization.

Chapter 6 has 18 articles, including 6.1 general requirements and 11 security domains corresponding to GB/T 37092-2018 and Appendix A to Appendix F.

This standard uses the "[xx.yy]" method to identify and serially number all evaluation units in the standard, where xx means the chapter 6 The corresponding bar, yy is the numerical index of the evaluation unit. Each evaluation unit includes safety requirements, requirements for materials submitted for inspection, and requirements for inspection procedures.

Among them, the content of the safety requirements directly refers to each of the corresponding safety requirements clauses in GB/T 37092-2018. For the completeness of the sentence, the Some of the safety requirements clauses cited are supplemented, and the supplementary sentences are written in italics; the requirements for materials submitted for inspection describe the The document type or detailed material requirements provided so that the inspector can verify (document or material) compliance with the given safety

requirements;

The testing procedure requirements indicate the procedures that the testing personnel should perform when testing whether the cryptographic module meets the given security requirements.

In this standard, "safety requirements [xx.yy]", "required materials for inspection [xx.yy]" and "test procedure requirements [xx.yy]" respectively represent the corresponding evaluation Unit [xx.yy] safety requirements, material requirements and testing procedures requirements.

The security level of the cryptographic module corresponding to each evaluation unit in this standard is shown in Appendix A.

6.1.1 Test purpose

The general requirements test includes 4 evaluation units to test whether the cryptographic module submitted for inspection matches the security specified in GB/T 37092-2018 Domain, and whether the inspection manufacturer has provided all relevant materials for the cryptographic module.

6.1.2 Evaluation unit [01.01]

Safety requirements.

The security requirements that a cryptographic module that meets this standard should meet. Material requirements for inspection. This article does not provide separate materials. Testing procedure requirements. This article is not tested separately.

6.1.3 Evaluation unit [01.02]

Safety requirements.

The cryptographic module shall be tested according to the requirements of each domain.

Note: If the cryptographic module submitted for inspection is not subject to some of the security requirements specified in GB/T 37092-2018, the testing organization will exclude the corresponding security requirements from testing. Material requirements for inspection. This article does not provide separate materials. Testing procedure requirements.

The testing agency can test the security of the cryptographic module in one or more of the following ways.

- a) The inspector uses the equipment of the inspection agency to perform the test.
- b) The inspector uses the equipment of the supplier to perform the test.
- c) Inspectors supervise the submitting manufacturer to use the equipment of the submitting

organization for testing. In this case, the testing agency needs to.

- 1) Explain the reason why you cannot conduct the test;
- 2) Develop the required test plan and test tasks;
- 3) Directly observe the execution of the test.

If any one of the tests is unsuccessful, then this one fails.

6.1.4 Evaluation unit [01.03]

Safety requirements. Cryptographic modules should be rated independently in each domain. Material requirements for inspection. This article does not provide separate materials. Testing procedure requirements. This article is not tested separately.

6.1.5 Evaluation unit [01.04]

The cryptographic module to be confirmed or evaluated shall provide all relevant documents, including user and installation manuals, design instructions, life cycle documents, etc. Material requirements for inspection. This article does not provide separate materials. Testing procedure requirements. This article is not tested separately.

6.2.1 General requirements for cryptographic module specifications

Safety requirements.

6.2.1.1 Test purpose

General requirements for cryptographic module specifications The test includes 2 evaluation units to test whether the cryptographic module submitted for inspection meets GB/T 37092-2018 The general requirements of the specified cryptographic module specifications, and whether the cryptographic module specification documents are written in accordance with the requirements specified in GB/T 37092-2018.

6.2.1.2 Evaluation unit [02.01]

The cryptographic module should be a collection of hardware, software, firmware, or a combination of them. This collection uses at least one approved cryptographic algorithm, security The full function or process implements a cryptographic service and is contained within the defined cryptographic boundary. Material requirements for inspection. This article does not provide separate materials. Testing procedure requirements.

- a) This article is not tested separately.
- b) Appendix C of GB/T 37092-2018 lists the approved safety functions.