Chinastandards.org

ICS 35.040
CCS L 80

GM

GM/T 0116-2021

Testing and evaluation process guide for information system cryptography application

信息系统密码应用测评过程指南

(English Translation)

Issued on: October 18, 2021 **Implemented on: May 1, 2022**

Issued by: State Administration of Cryptography

Preview: page 1 of 5 shown, 28 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0116-2021

Chinastandards.org

Table of Contents

Scope 1
Normative References 2
Terms and Definitions 3
Testing and evaluation agency 4
Agency under testing and evaluation 5
Commercial cryptography application security evaluation staff 6
Basic Principles 7
Risk Identification of Testing and Evaluation 8
Avoidance of Testing and Evaluation Risks 9
Testing and evaluation preparation activities 10
Scheme preparation activities 11
Analysis and report preparation activities 12
Workflow of Testing and Evaluation Preparation Activities 13
Project startup 14
Information collection and analysis 15
Determination of testing and evaluation objects 16
Determination of testing and evaluation indicators 17
Determination of testing and evaluation content 18
Preparation of cryptography evaluation scheme 19

1 Scope

This document specifies the testing and evaluation process of information system cryptography application and standardizes the testing and evaluation activities and work tasks.

This document is suitable for commercial cryptography application security evaluation institutions and information system responsible organizations to carry out cryptography application security evaluation work.

2 Normative References

The contents of the following documents constitute indispensable clauses of this document through the normative references in the text. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references

Preview: page 2 of 5 shown, 28 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0116-2021

without a specified date, the latest version (including all the modifications) is applicable to this document.

GB/T 25069-2010 Information Security Technology - Glossary GM/T 0115 Testing and Evaluation Requirements for Information System Cryptography Application GM/Z 4001 Cryptology Terminology

3 Terms and Definitions

The terms and definitions defined in GB/T 25069-2010 and GM/Z 4001, and the following are applicable to this document.

3.1 Testing and evaluation agency

The subject that conducts cryptography application security evaluation (referred to as "cryptography evaluation") on information systems.

NOTE: specifically, it can be a commercial cryptography application security evaluation institution or information system responsible organization.

3.2 Agency under testing and evaluation

Information system responsible organization.

3.3 Commercial cryptography application security evaluation staff

Personnel engaged in testing and evaluation activities in the testing and evaluation agency.

NOTE: referred to as "cryptography evaluation staff".

4.1 Basic Principles

When conducting cryptography application security evaluation on an information system, the testing and evaluation agency shall follow the following principles.

a) Principle of objectivity and impartiality During the testing and evaluation implementation process, the testing and evaluation agency shall ensure that the testing and evaluation activities are carried out in accordance with the cryptography evaluation scheme jointly agreed upon by the agency under testing and evaluation and based on clearly defined testing and evaluation modes and explanations, in compliance with the requirements of the national cryptography management department and with minimal subjective judgment.

b) Principle of reusability the testing and evaluation work may reuse existing testing and evaluation results, including commercial cryptography testing and certification results and the testing and evaluation results of cryptography application security evaluation, etc. All reuse results shall be based on the premise that the existing testing and evaluation results are still applicable to the current information system under test and can objectively reflect

Preview: page 3 of 5 shown, 28 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0116-2021

the current security status of the system.

c) Principle of repeatability and reproducibility in accordance with the same requirements, using the same testing and evaluation method, and in the same environment, different cryptography evaluation staffs shall obtain the same results by repeatedly executing each testing and evaluation implementation process. The difference between repeatability and reproducibility is that the former focuses on the consistency of the testing and evaluation results by the same cryptography evaluation staff, while the latter focuses on the consistency of the testing and evaluation results by different cryptography evaluation staffs.

d) Principle of result perfection Based on a correct understanding of the content of each requirement of GM/T 0115, the results generated by testing and evaluation shall objectively reflect the current status of cryptography application in an information system. The testing and evaluation process and results shall be based on correct testing and evaluation methods to ensure that they satisfy the requirements.

4.2 Risk Identification of Testing and Evaluation

The execution of the testing and evaluation work may bring certain risks to the information system under test. The testing and evaluation agency shall identify risks in a timely manner before the start of testing and evaluation and during the testing and evaluation process. During the testing and evaluation process, the risks mainly include the following aspects.

a) Verification test may affect the normal operation of the information system under test During on-site testing and evaluation, certain verification tests need to be carried out on the equipment and systems. Some test content requires checking the information on the computer, which may have an unexpected impact on the operation of the information system under test.

b) Tool test may affect the normal operation of the information system under test During on-site testing and evaluation, based on actual demands, some testing and evaluation tools may be used for the test. When the testing and evaluation tools are used, redundant data writing may be generated, and meanwhile, it may have a certain impact on the load of the system, which in turn may cause certain impact or even damage to the server and network communication in the information system under test.

c) Possible leakage of sensitive information of the information system under test During the testing and evaluation process, sensitive information of the information system under test may be leaked, such as: encryption mechanisms, operational processes, security mechanisms and related document information, etc.

d) Other possible risks During the testing and evaluation process, risks may also arise that affect the availability, confidentiality and integrity of the information system under test.

Preview: page 4 of 5 shown, 28 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0116-2021

4.3 Avoidance of Testing and Evaluation Risks

During the testing and evaluation process, the following measures may be taken to avoid risks.

a) Sign a commissioned testing and evaluation agreement Before the testing and evaluation work official starts, the testing and evaluation agency and the agency under testing and evaluation need to clarify the goals, scope, personnel composition, planning arrangements, implementation steps and requirements, and the responsibilities and obligations of both parties through the mode of commission agreement, so that both parties of the testing and evaluation can

4.4.2 Testing and evaluation preparation activities

The testing and evaluation preparation activities are the premise and foundation for carrying out the testing and evaluation work. The main tasks are to grasp the details of the information system under test, prepare testing and evaluation tools, and prepare for the preparation of cryptography evaluation scheme.

4.4.3 Scheme preparation activities

Scheme preparation activities are the key activities in carrying out the testing and evaluation work. The main tasks are to determine the testing and evaluation objects, testing and evaluation indicators, testing and evaluation inspection points, and testing and evaluation content, etc. that are suitable for the information system under test, and form a cryptography evaluation scheme to provide a basis for the implementation of on-site testing and evaluation.

4.4.4 On-site testing and evaluation activities on-site testing and evaluation activities are the core activities of testing and evaluation work.

The main tasks are to implement all testing and evaluation items step by step in accordance with the cryptography evaluation scheme, so as to understand the real status of cryptography application of the information system under test, obtain sufficient evidence and find out the existing security issues of cryptography application.

4.4.5 Analysis and report preparation activities

The analysis and report preparation activities are activities that provide the results of testing and evaluation work. The main tasks are to find out the gaps between the security protection status of cryptography application of the information system under test and the protection requirements of the corresponding level through methods of unit testing and evaluation, overall testing and evaluation, quantitative evaluation and risk analysis in accordance with the cryptography evaluation scheme and the relevant requirements of

Preview: page 5 of 5 shown, 28 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0116-2021