GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

CCS L 80

GM/T 0115-2021

Testing and Evaluation Requirements for Information System Cryptography Application

信息系统密码应用测评要求

Issued on: October 19, 2021 **Implemented on: May 1, 2022**

Issued by: State Cryptography Administration

Table of Contents

Testing and Evaluation Requirements for Information System Cryptography Application

1 Scope

This document specifies the testing and evaluation requirements for different levels of cryptography application in information systems. From the perspectives of cryptographic algorithm compliance, cryptographic technology compliance, cryptographic product compliance, cryptographic service compliance and key management security, etc., it proposes the general testing and evaluation requirements for cryptography application from Level 1 to Level 5. From four technological levels: physical and environmental security of information systems, network and communication security, equipment and computing security, application and data security, etc., it proposes the testing and evaluation requirements for cryptography application technology from Level 1 to Level 4. From four management perspectives: management system, personnel management, construction and operation, and emergency response, it proposes the testing and evaluation requirements for cryptography application management from Level 1 to Level 4. In addition, the requirements for the testing and evaluation links, such as: overall testing and evaluation, risk analysis and evaluation, and testing and evaluation conclusions, etc., are provided.

This document is applicable to guide and standardize the security evaluation of commercial cryptography application in the planning, construction and operation of information system cryptography application.

NOTE: for Level 5 cryptography application testing and evaluation requirements, only general testing and evaluation requirements are described in this document.

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

GB/T 39786-2021 Information Security Technology - Baseline for Information System Cryptography Application

GM/Z 4001 Cryptology Terminology

3 Terms and Definitions

The terms and definitions defined in GB/T 39786-2021 and GM/Z 4001, and the following are

applicable to this document.

3.1 commercial cryptography application security evaluation staff

Personnel engaged in security evaluation of commercial cryptography application in a commercial cryptography application security evaluation institution.

NOTE: referred to as “cryptography evaluation staff”.

3.2 examine

The process, in which, the cryptography evaluation staff observes, inspects and analyzes the testing and evaluation object, which helps the cryptography evaluation staff understand, clarify or obtain evidence.

4 Overview

In accordance with GB/T 39786-2021, the testing and evaluation requirements for information system cryptography application are divided into general testing and evaluation requirements, testing and evaluation requirements for cryptography application technology, and testing and evaluation requirements for cryptography application management. Chapter 5 is used to guide the implementation of Chapter 6. The testing and evaluation will not be separately implemented, nor will it be separately reflected in the unit testing and evaluation results and overall testing and evaluation results of the security evaluation report on cryptography application. Appendix A is a reference for the implementation of testing and evaluation of 5.5. Appendix B and Appendix C respectively provide the testing and evaluation technology for typical cryptographic product application and the testing and evaluation technology for typical cryptographic function, as a reference for the cryptography evaluation staff when implementing the testing and evaluation of the specifically used cryptographic products or applied cryptographic functions in information system.

The testing and evaluation unit in this document corresponds to a relatively independent and complete set of testing and evaluation content, consisting of testing and evaluation indicators, testing and evaluation objects, testing and evaluation implementation and result determination.

a) Testing and evaluation indicators: derived from the requirements at all levels in GB/T 39786-2021. The security level corresponding to the indicator is indicated after each indicator.

b) Testing and evaluation objects: objects affected by different testing and evaluation methods in the information system cryptography application testing and evaluation process, including related physical security facilities, communication channels, cryptographic products, general equipment, applications, personnel and institutional documents, etc.

c) Testing and evaluation implementation: for a certain testing and evaluation indicator,

the key points for the testing and evaluation of information system cryptography application are specified.

d) Result determination: in accordance with the evidence obtained through testing and evaluation implementation, determine whether the cryptography application of an information system satisfies the method and principle requested by a certain testing and evaluation indicator.

If the testing and evaluation unit involves two or more testing and evaluation objects, then, each testing and evaluation object needs to be respectively subjected to the testing and evaluation implementation and result determination. The result of the testing and evaluation unit is summarized from the results of testing and evaluation implementation of all testing and evaluation objects involved in the unit.

When carrying out actual testing and evaluation, the cryptography evaluation staff shall determine whether to include the "can", "should" and "shall" clauses of different security protection levels in GB/T 39786-2021 in the testing and evaluation scope through the following methods.

a) For the "can" clauses, it is up to the responsible party of the information system to decide whether to include them in the testing and evaluation scope of standard compliance. If it is included in the testing and evaluation scope, then, the cryptography evaluation staff shall carry out the testing and evaluation, and result determination in accordance with the corresponding requirements of the testing and evaluation indicators in Chapter 6; otherwise, the testing and evaluation indicator will be "inapplicable".

b) For the "should" clauses, the cryptography evaluation staff shall decide whether to include them in the testing and evaluation scope of standard compliance in accordance with the cryptography application scheme and scheme evaluation opinions of the information system. If the information system fails to pass the cryptography application scheme being evaluated or the cryptography application scheme is not clearly stated, then, the "should" clauses will be included in the testing and evaluation scope of standard compliance by default.

    1) If they are included in the testing and evaluation scope of standard compliance, then, the cryptography evaluation staff shall carry out testing and evaluation, and result determination in accordance with the corresponding requirements of the testing and evaluation indicators in Chapter 6.

    2) If they are not included in the testing and evaluation scope of standard compliance, the cryptography evaluation staff shall further verify whether the applicable conditions of the risk control measures described in the cryptography application scheme are satisfied in the actual information system, and whether the implementation of the information system is consistent with the described risk control measures in accordance with the cryptography application scheme

technology, such as: dynamic password mechanisms, message authentication code (MAC) mechanisms based on symmetric cryptographic algorithms or cryptographic hash algorithms, and digital signature mechanisms based on public key cryptographic algorithms, for the authentication of the identity of persons entering important areas; verify whether the authenticity implementation mechanism of the identity of the persons entering is correct and effective.

d) Result determination

For an individual testing and evaluation object, if the above contents of testing and evaluation implementation are all YES, then, the testing and evaluation object complies with the testing and evaluation indicator requirements of this unit; if 3) of c) is NO, then, it does not comply with the testing and evaluation indicator requirements of this unit; otherwise, it partially complies with the testing and evaluation indicator requirements of this unit. For this testing and evaluation unit, summarize the determination results of all the testing and evaluation objects involved in the unit. If the determination results are all conforming, then, the testing and evaluation result of this unit is conforming; if the determination results are all non-conforming, then, the testing and evaluation result of this unit is non-conforming; otherwise, the testing and evaluation result of this unit is partially conforming.

6.1.2 Storage integrity of electronic access control record data

See the specific testing and evaluation units below.

a) Testing and evaluation indicators

Adopt cryptographic technology to ensure the storage integrity of the entry and exit record data of the electronic access control system (Level 1 to Level 4).

b) Testing and evaluation objects

Important areas, for example, computer rooms where the information system is located, and their electronic access control systems.

c) Testing and evaluation implementation

1) Check whether the cryptographic algorithms and cryptographic technology comply with 5.1 and 5.2;

2) Check whether the cryptographic products, cryptographic services and key management comply with 5.3, 5.4 and 5.5;

3) Verify whether cryptographic technology, such as: message authentication code (MAC) mechanisms based on symmetric cryptographic algorithms or cryptographic hash algorithms, and digital signature mechanisms based on public key cryptographic algorithms, are adopted for the storage integrity

protection of the entry and exit record data of the electronic access control systems; verify whether the integrity protection mechanism is correct and effective.

d) Result determination

For an individual testing and evaluation object, if the above contents of testing and evaluation implementation are all YES, then, the testing and evaluation object complies with the testing and evaluation indicator requirements of this unit; if 3) of c) is NO, then, it does not comply with the testing and evaluation indicator requirements of this unit; otherwise, it partially complies with the testing and evaluation indicator requirements of this unit. For this testing and evaluation unit, summarize the determination results of all the testing and evaluation objects involved in the unit. If the determination results are all conforming, then, the testing and evaluation result of this unit is conforming; if the determination results are all non-conforming, then, the testing and evaluation result of this unit is non-conforming; otherwise, the testing and evaluation result of this unit is partially conforming.

6.1.3 Storage integrity of video surveillance record data

See the specific testing and evaluation units below.

a) Testing and evaluation indicators

Adopt cryptographic technology to ensure the storage integrity of video surveillance audio and video record data (Level 3 to Level 4).

b) Testing and evaluation objects

Important areas, for example, computer rooms where the information system is located, and their video surveillance systems.

c) Testing and evaluation implementation

1) Check whether the cryptographic algorithms and cryptographic technology comply with 5.1 and 5.2;

2) Check whether the cryptographic products, cryptographic services and key management comply with 5.3, 5.4 and 5.5;

3) Verify whether cryptographic technology, such as: message authentication code (MAC) mechanisms based on symmetric cryptographic algorithms or cryptographic hash algorithms, and digital signature mechanisms based on public key cryptographic algorithms, are adopted for the storage integrity protection of the video surveillance audio and video record data; verify whether the integrity protection mechanism is correct and effective.

d) Result determination

communication entities; verify whether the communication entity identity authenticity implementation mechanism is correct and effective.

d) Result determination

For an individual testing and evaluation object, if the above contents of testing and evaluation implementation are all YES, then, the testing and evaluation object complies with the testing and evaluation indicator requirements of this unit; if 3) of c) is NO, then, it does not comply with the testing and evaluation indicator requirements of this unit; otherwise, it partially complies with the testing and evaluation indicator requirements of this unit. For this testing and evaluation unit, summarize the determination results of all the testing and evaluation objects involved in the unit. If the determination results are all conforming, then, the testing and evaluation result of this unit is conforming; if the determination results are all non-conforming, then, the testing and evaluation result of this unit is non-conforming; otherwise, the testing and evaluation result of this unit is partially conforming.

6.2.2 Communication data integrity

See the specific testing and evaluation units below.

a) Testing and evaluation indicators

Adopt cryptographic technology to ensure the integrity of data during the communication process (Level 1 to Level 4).

b) Testing and evaluation objects

Network communication channels established outside the boundaries of information system and network, as well as equipment or components and cryptographic products that provide communication protection functions.

c) Testing and evaluation implementation

1) Check whether the cryptographic algorithms and cryptographic technology comply with 5.1 and 5.2;

2) Check whether the cryptographic products, cryptographic services and key management comply with 5.3, 5.4 and 5.5;

3) Verify whether cryptographic technology, such as: message authentication code (MAC) mechanisms based on symmetric cryptographic algorithms or cryptographic hash algorithms, and digital signature mechanisms based on public key cryptographic algorithms, are adopted for the integrity protection of data during the communication process; verify whether the communication data protection mechanism is correct and effective.

d) Result determination

For an individual testing and evaluation object, if the above contents of testing and evaluation implementation are all YES, then, the testing and evaluation object complies with the testing and evaluation indicator requirements of this unit; if 3) of c) is NO, then, it does not comply with the testing and evaluation indicator requirements of this unit; otherwise, it partially complies with the testing and evaluation indicator requirements of this unit. For this testing and evaluation unit, summarize the determination results of all the testing and evaluation objects involved in the unit. If the determination results are all conforming, then, the testing and evaluation result of this unit is conforming; if the determination results are all non-conforming, then, the testing and evaluation result of this unit is non-conforming; otherwise, the testing and evaluation result of this unit is partially conforming.

6.2.3 Confidentiality of important data during communication

See the specific testing and evaluation units below.

a) Testing and evaluation indicators

Adopt cryptographic technology to ensure the confidentiality of important data during the communication process (Level 1 to Level 4).

b) Testing and evaluation objects

Network communication channels established outside the boundaries of information system and network, as well as equipment or components and cryptographic products that provide communication protection functions.

c) Testing and evaluation implementation

1) Check whether the cryptographic algorithms and cryptographic technology comply with 5.1 and 5.2;

2) Check whether the cryptographic products, cryptographic services and key management comply with 5.3, 5.4 and 5.5;

3) Verify whether the encryption and decryption functions of cryptographic technology are adopted for the confidentiality protection of sensitive information or communication messages during the communication process; verify whether the confidentiality protection mechanism for sensitive information or communication messages is correct and effective.

d) Result determination

For an individual testing and evaluation object, if the above contents of testing and evaluation implementation are all YES, then, the testing and evaluation object complies with the testing and evaluation indicator requirements of this unit; if 3) of c) is NO, then, it does not comply with the testing and evaluation indicator requirements

determination results of all the testing and evaluation objects involved in the unit. If the determination results are all conforming, then, the testing and evaluation result of this unit is conforming; if the determination results are all non-conforming, then, the testing and evaluation result of this unit is non-conforming; otherwise, the testing and evaluation result of this unit is partially conforming.

6.2.5 Secure access authentication

See the specific testing and evaluation units below.

a) Testing and evaluation indicators

Adopt cryptographic technology to authenticate the access of equipment connected to the internal network from the outside, so as to ensure the authenticity of the identity of the access equipment (Level 3 to Level 4).

b) Testing and evaluation objects

Internal network of the information system, as well as equipment or components and cryptographic products that provide equipment network access authentication functions.

c) Testing and evaluation implementation

1) Check whether the cryptographic algorithms and cryptographic technology comply with 5.1 and 5.2;

2) Check whether the cryptographic products, cryptographic services and key management comply with 5.3, 5.4 and 5.5;

3) Verify whether cryptographic technology, such as: message authentication code (MAC) mechanisms based on symmetric cryptographic algorithms or cryptographic hash algorithms, and digital signature mechanisms based on public key cryptographic algorithms, are adopted for the access authentication of equipment connected to the internal network from the outside; verify whether the secure access authentication mechanism is correct and effective.

d) Result determination

For an individual testing and evaluation object, if the above contents of testing and evaluation implementation are all YES, then, the testing and evaluation object complies with the testing and evaluation indicator requirements of this unit; if 3) of c) is NO, then, it does not comply with the testing and evaluation indicator requirements of this unit; otherwise, it partially complies with the testing and evaluation indicator requirements of this unit. For this testing and evaluation unit, summarize the determination results of all the testing and evaluation objects involved in the unit. If the determination results are all conforming, then, the testing and evaluation result of

this unit is conforming; if the determination results are all non-conforming, then, the testing and evaluation result of this unit is non-conforming; otherwise, the testing and evaluation result of this unit is partially conforming.

6.3 Equipment and Computing Security

6.3.1 Identity authentication

See the specific testing and evaluation units below.

a) Testing and evaluation indicators

Adopt cryptographic technology to authenticate the identity of users logging in to the equipment, so as to ensure the authenticity of the user's identity (Level 1 to Level 4).

b) Testing and evaluation objects

General equipment, network and security equipment, cryptographic equipment, various virtual equipment, and cryptographic products that provide identity authentication functions.

c) Testing and evaluation implementation

1) Check whether the cryptographic algorithms and cryptographic technology comply with 5.1 and 5.2;

2) Check whether the cryptographic products, cryptographic services and key management comply with 5.3, 5.4 and 5.5;

3) Verify whether cryptographic technology, such as: dynamic password mechanisms, message authentication code (MAC) mechanisms based on symmetric cryptographic algorithms or cryptographic hash algorithms, and digital signature mechanisms based on public key cryptographic algorithms, are adopted for the identity authentication of users logging in to the equipment, for example, equipment operators; verify whether the identity authentication implementation mechanism of users logging in to the equipment is correct and effective.

d) Result determination

For an individual testing and evaluation object, if the above contents of testing and evaluation implementation are all YES, then, the testing and evaluation object complies with the testing and evaluation indicator requirements of this unit; if 3) of c) is NO, then, it does not comply with the testing and evaluation indicator requirements of this unit; otherwise, it partially complies with the testing and evaluation indicator requirements of this unit. For this testing and evaluation unit, summarize the determination results of all the testing and evaluation objects involved in the unit. If the determination results are all conforming, then, the testing and evaluation result of

6.3.3 System resource access control information integrity

See the specific testing and evaluation units below.

a) Testing and evaluation indicators

Adopt cryptographic technology to ensure the integrity of system resource access control information (Level 1 to Level 4).

b) Testing and evaluation objects

General equipment, network and security equipment, cryptographic equipment, various virtual equipment, as well as cryptographic products that provide integrity protection functions.

c) Testing and evaluation implementation

1) Check whether the cryptographic algorithms and cryptographic technology comply with 5.1 and 5.2;

2) Check whether the cryptographic products, cryptographic services and key management comply with 5.3, 5.4 and 5.5;

3) Verify whether cryptographic technology, such as: message authentication code (MAC) mechanisms based on symmetric cryptographic algorithms or cryptographic hash algorithms, and digital signature mechanisms based on public key cryptographic algorithms, are adopted for the integrity protection of system resource access control information on the equipment; verify whether the integrity protection mechanism for the system resource access control information is correct and effective.

d) Result determination

For an individual testing and evaluation object, if the above contents of testing and evaluation implementation are all YES, then, the testing and evaluation object complies with the testing and evaluation indicator requirements of this unit; if 3) of c) is NO, then, it does not comply with the testing and evaluation indicator requirements of this unit; otherwise, it partially complies with the testing and evaluation indicator requirements of this unit. For this testing and evaluation unit, summarize the determination results of all the testing and evaluation objects involved in the unit. If the determination results are all conforming, then, the testing and evaluation result of this unit is conforming; if the determination results are all non-conforming, then, the testing and evaluation result of this unit is non-conforming; otherwise, the testing and evaluation result of this unit is partially conforming.

6.3.4 Important information resource security tag integrity

See the specific testing and evaluation units below.

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

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