

ICS 35.040
CCS L 80

GM

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

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

(English Translation)

Issued on: October 18, 2021

Implemented on: May 1, 2022

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative References	2
Terms and Definitions	3
Commercial cryptography application security evaluation staff	4
Overview	5
Compliance of Cryptographic Algorithms	6
Compliance of Cryptographic Technology	7
Compliance of Cryptographic Products	8
Key Management Security	9
Identity authentication	10
Communication data integrity	11
Integrity of network boundary access control information	12
Identity authentication	13
Identity authentication	14
Important data transmission confidentiality	15
Important data storage integrity	16
Security management systems with cryptography application	17
Key management rules	18
Regular cryptography application security evaluation and offensive and defensive	19
Overview	20
Inter-unit Testing and Evaluation	21
Inter-level Testing and Evaluation	22
Risk Analysis and Evaluation	23
Testing and Evaluation Conclusions	24

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.

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.

5.1 Compliance of Cryptographic Algorithms

See the specific testing and evaluation units below.

5.2 Compliance of Cryptographic Technology

See the specific testing and evaluation units below.

5.3 Compliance of Cryptographic Products

See the specific testing and evaluation units below.

5.5 Key Management Security

See the specific testing and evaluation units below.

6 Testing and Evaluation Requirements for Cryptography Application Technology and Cryptography Application Management

6.1.1 Identity authentication

See the specific testing and evaluation units below.

6.2.2 Communication data integrity

See the specific testing and evaluation units below.

6.2.4 Integrity of network boundary access control information

See the specific testing and evaluation units below.

6.3.1 Identity authentication

See the specific testing and evaluation units below.

6.4.1 Identity authentication

See the specific testing and evaluation units below.

6.4.4 Important data transmission confidentiality

See the specific testing and evaluation units below.

6.4.7 Important data storage integrity

See the specific testing and evaluation units below.

6.5.1 Security management systems with cryptography application

See the specific testing and evaluation units below.

6.5.2 Key management rules

See the specific testing and evaluation units below.

6.7.4 Cryptography application security evaluation conducted before putting into operation

See the specific testing and evaluation units below.

a) Testing and evaluation indicators

1) Before putting it into operation, conduct a cryptography application security evaluation (Level 1 to Level 2).

2) Before putting it into operation, conduct a cryptography application security evaluation. The system may be officially operated only after passing the evaluation (Level 3 to Level 4).

c) Testing and evaluation objects Cryptography application security evaluation report, and responsible person of the system.

d) Testing and evaluation implementation

1) For Level 1 to Level 2 system, check whether a cryptography application security evaluation is organized before the information system is put into operation; check whether there is a cryptography application security evaluation report formulated before the system is put into operation.

2) For Level 3 to Level 4 system, check whether a cryptography application security evaluation is organized before the information system is put into operation; check whether there is a cryptography application security evaluation report formulated before the system is put into operation and whether the system has passed the evaluation.

e) Result determination for an individual testing and evaluation object, if the above contents of testing and evaluation implementation of the corresponding level are all YES, then, the testing and evaluation object complies with the testing and evaluation indicator requirements of this unit; otherwise, it does not comply with, or 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.