GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

Record No.: 61709-2018

GM/T 0054-2018

General Requirements for Information System Cryptography Application

信息系统密码应用基本要求

Issued on: February 08, 2018 **Implemented on: February 08, 2018**

Issued by: State Cryptography Administration

Table of Contents

General Requirements for Information System Cryptography Application

1 Scope

This Standard specifies the general requirements for information system commercial cryptography application.

This Standard is applicable to guide, regulate and assess the information system commercial cryptography application.

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 document.

GM/T 0005 Randomness Test Specification

GM/T 0028 Security Requirements for Cryptographic Modules

GM/T 0036 Technical Guidance of Cryptographic Application for Access Control Systems Based on Contactless Smart Card

GM/Z 4001-2013 Cryptography Terminology

3 Terms and Definitions

For the purposes of this document, the terms and definitions given in GM/Z 4001-2013 and the following apply. For the benefit of use, some terms and definitions given in GM/Z 4001-2013 are listed repeatedly as follows.

3.1 One-time-password; OTP; dynamic password

The one-time password dynamically generated based on time, event, etc.

3.2 Access control

3.12 Message authentication code; MAC

The output of the message authentication algorithm; also known as the message authentication code.

3.13 Authenticity

The property ensuring that the identity of the subject or resource is the claimed one. The authenticity is applicable to the entities such as users, processes, systems, and information.

3.14 Non-repudiation

The nature that proves an action that has occurred can't be denied.

4 Abbreviation

The following abbreviation is applicable to this document.

MAC (Message Authentication Code)

5 General Requirements

5.1 Cryptographic algorithm

The cryptographic algorithm used in the information system shall conform to the provisions of laws and regulations, as well as the relevant requirements of national and industry standards related to cryptography.

5.2 Cryptographic technology

The cryptographic technology used in the information system shall follow the national and industry standards related to cryptography.

5.3 Cryptographic products

The cryptographic products and cryptographic modules used in the information system shall be approved by the state cryptography administration department.

5.4 Cryptographic service

The cryptographic service used in the information system shall be licensed by the state cryptography administration department.

a) Authentication of personnel entering the important physical areas;

b) Authentication of the two parties of communication;

c) Authentication when network device is accessed;

d) Authentication for platform using the trusted computing technology;

e) Authentication of user who login the operating system and database system;

f) Authentication of user who applies the system.

6.4 Non-repudiation

The non-repudiation of entity behavior that is achieved by using the digital signature, and the like cryptographic technology; it is against all behaviors that can't be denied in the information system, such as sending, receiving, approving, creating, modifying, deleting, adding, configuring, etc.

7 Cryptographic Technology Application Requirements

7.1 Physical and environmental security

7.1.1 General

The general rules for cryptography application of the physical and environmental security are as follows:

a) Use the cryptographic technology to implement the physical access control against the important sites, monitoring equipment, etc.;

b) Use the cryptographic technology to implement the integrity protection against the physical and environmental sensitive information data such as physical access control records, monitoring information, etc.;

c) Electronic access control systems achieved by using the cryptographic technology shall follow GM/T 0036.

7.1.2 Class-I information system with classified protection

The requirements for the Class-I information system are as follows:

a) The authenticity function of the cryptographic technology may be used to protect the authentication information of the physical access control; ensuring the identify authenticity of the personnel entering the important area;

integrity of the entry and exit records of the electronic access control system;

c) The integrity function of the cryptographic technology shall be used to ensure the integrity of the video surveillance audio record;

d) The Level-III and above cryptographic modules satisfying GM/T 0028 and the hardware cryptographic products approved by the state cryptography administration department shall be used to achieve the cryptographic operation and key management.

7.2 Network and communication security

7.2.1 General

The general rules for network and communication security cryptography application are as follows:

a) Use cryptographic technology to conduct the security authentication against the device connected to the internal network;

b) Use cryptographic technology to conduct authentication against the identities of the two parties of the communication;

c) Use cryptographic technology to ensure the data integrity during the communication process.

d) Use cryptographic technology to ensure the confidentiality of the sensitive information data fields and the entire message during the communication process;

e) Use cryptographic technology to ensure the integrity of the network boundary access control information and the system resource access control information;

f) Use cryptographic technology to establish a secure information transmission channel; then conduct centralized management against the security devices or security components in the network.

7.2.2 Class-I information system with classified protection

The requirements of Class-I information system are as follows:

a) Authentication may be conducted based on cryptographic technology before communication; use the confidentiality and authenticity functions of the cryptographic technology to achieve anti-interception, anti-counterfeiting and anti-reuse; so that ensure the confidentiality of the authentication information and identity authenticity of the network device entity during the transmission;

c) Cryptographic technology shall be used to ensure the data integrity during the communication process;

d) Cryptographic technology shall be used to ensure the confidentiality of the sensitive information data fields or entire message during the communication process;

e) Cryptographic technology shall be used to establish a secure information transmission channel; then conduct centralized management against the security devices or security components in the network;

f) The Level-III and above cryptographic modules satisfying GM/T 0028 and the hardware cryptographic products approved by the state cryptography administration department should be used to achieve the cryptographic operation and key management.

7.2.5 Class-IV information system with classified protection

The requirements for Class-IV information system are as follows:

a) Authentication shall be conducted based on cryptographic technology before communication; use the confidentiality and authenticity functions of the cryptographic technology to achieve anti-interception, anti-counterfeiting and anti-reuse; so that ensure the confidentiality of the authentication information and identity authenticity of the network device entity during the transmission;

b) Cryptographic technology shall be used to conduct authentication against the device connected to the internal network; so that ensure the authenticity of the device connected to the network;

c) The integrity of cryptographic technology shall be used to ensure the integrity of network boundary and system resources access control information;

d) Cryptographic technology shall be used to ensure the data integrity during the communication process;

e) Cryptographic technology shall be used to ensure the confidentiality of the sensitive information data fields or entire message during the communication process;

f) Cryptographic technology shall be used to establish a secure information transmission channel; then conduct centralized management against the security devices or security components in the network;

g) The Level-III and above cryptographic modules satisfying GM/T 0028 and the hardware cryptographic products approved by the state cryptography

a) Cryptographic technology should be used to conduct identification and authentication against the logged in user; the identification is unique; the authentication information has complexity requirements and is periodically replaced; use the authenticity of the cryptographic technology to achieve the anti-counterfeiting of the authentication information;

b) In the remote management, the confidentiality of the cryptographic technology should be used to achieve the anti-eavesdropping of the authentication information;

c) The integrity of cryptographic technology should be used to ensure the integrity of the system resource access control information;

d) The integrity of cryptographic technology should be used to ensure the integrity of the sensitive tags of the important information resource;

e) The integrity of cryptographic technology should be used to protect the integrity of the log records;

f) The Level-II and above cryptographic modules satisfying GM/T 0028 and the hardware cryptographic products approved by the state cryptography administration department should be used to achieve the cryptographic operation and key management.

7.3.4 Class-III information system with classified protection

The requirements for Class-III information system are as follows:

a) Cryptographic technology shall be used to conduct identification and authentication against the logged in user; the identification is unique; the authentication information has complexity requirements and is periodically replaced;

b) In the remote management, the confidentiality of the cryptographic technology shall be used to achieve the anti-eavesdropping of the authentication information;

c) The integrity of cryptographic technology shall be used to ensure the integrity of the system resource access control information;

d) The integrity of cryptographic technology shall be used to ensure the integrity of the sensitive tags of the important information resource;

e) Trusted computing technology shall be used to establish a trust chain from the system to the application; so that achieve the integrity protection of the important procedures and files during the system operation process;

f) The integrity of cryptographic technology shall be used to protect the integrity of

resource access control information;

c) Use the integrity of cryptographic technology to ensure the integrity of sensitive tags of important information resource;

d) Use the cryptographic technology to ensure the important data confidentiality and integrity during the transmission process;

e) Use the cryptographic technology to ensure the important data confidentiality and integrity during the storage process;

f) Use cryptographic technology to conduct security control against the loading and unloading of important procedure;

g) Use cryptographic technology to achieve non-repudiation of entity behavior;

h) Use the integrity of cryptographic technology to protect the integrity of the log records.

7.4.2 Class-I information system with classified protection

The requirements for Class-I information system are as follows:

a) Cryptographic technology may be used to conduct identification and authentication against the logged in user; achieving the anti-interception, anti-counterfeiting and anti-reuse of the authentication information; ensuring the identity authenticity of the user of application system;

b) The integrity of cryptographic technology may be used to ensure the integrity of business application system access control policy, database table access control information, and sensitive tag of important information resource, etc.;

c) Cryptographic technology may be used to ensure the confidentiality of important data during the transmission process, including but not limited to authentication information, important business data and important user information, etc.;

d) Cryptographic technology may be used to ensure the confidentiality of important data during the storage process, including but not limited to authentication information, important business data and important user information, etc.;

e) Cryptographic technology may be used to ensure the integrity of important data during the transmission process, including but not limited to authentication data, important business data, important audit data, important configuration data, important video data and important user information, etc.;

f) Cryptographic technology may be used to ensure the integrity of the important data during the storage process, including but not limited to authentication data,

administration department should be used to achieve the cryptographic operation and key management.

7.4.4 Class-III information system with classified protection

The requirements for Class-III information system are as follows:

a) Cryptographic technology shall be used to conduct identification and authentication against the logged in user; achieving the anti-interception, anti-counterfeiting and anti-reuse of the authentication information; ensuring the identity authenticity of the user of application system;

b) The integrity of cryptographic technology shall be used to ensure the integrity of business application system access control policy, database table access control information, and sensitive tag of important information resource, etc.;

c) Cryptographic technology shall be used to ensure the confidentiality of important data during the transmission process, including but not limited to authentication information, important business data and important user information, etc.;

d) Cryptographic technology shall be used to ensure the confidentiality of important data during the storage process, including but not limited to authentication information, important business data and important user information, etc.;

e) Cryptographic technology shall be used to ensure the integrity of important data during the transmission process, including but not limited to authentication data, important business data, important audit data, important configuration data, important video data and important user information, etc.;

f) Cryptographic technology shall be used to ensure the integrity of the important data during the storage process, including but not limited to authentication data, important business data, important audit data, important configuration data, important video data, important user information, important executable programs, etc.;

g) The integrity of cryptographic technology shall be used to achieve the protection against the integrity of log records;

h) Cryptographic technology shall be used to conduct security control against the loading and unloading of important application program;

i) The Level-III and above cryptographic modules satisfying GM/T 0028 and the hardware cryptographic products approved by the state cryptography administration department should be used to achieve the cryptographic operation and key management.

and key management.

8 Key Management

8.1 General

Key management of information system shall include the whole process of management and strategy formulation for key generation, storage, distribution, input, output, use, backup, recovery, archiving and destruction, etc.

8.2 Class-I information system with classified protection

Key management of Class-I information system shall include at least three processes, such as key generation, storage and use; and satisfy:

a) Key generation

The generated keys can't be duplicated and their confidentiality shall be guaranteed.

b) Key storage

Take necessary security protection measures to prevent unauthorized access to the key.

c) Key use

Take necessary security protection measures to prevent illegal use of the key.

8.3 Class-II information system with classified protection

Key management of Class-II information system shall include the processes such as key generation, storage, distribution, input, output, use, backup and recovery, etc.; and satisfy:

a) Key generation

The random number used for generating the key shall meet the requirements of GM/T 0005; key shall be generated in the cryptographic module conforming to the GM/T 0028.

b) Key storage

Key shall be stored in an encryption mode; and take necessary security protection measures to prevent the illegal access to the key.

The key distribution shall take security measures such as authentication, data integrity, data confidentiality; it shall be able to resist attacks such as interception, counterfeiting, tampering, replay, etc.; ensure the security of the key.

d) Key input and output

Security measures shall be taken to prevent illegal access or tampering of keys during the input and output period; and ensure the correctness of the key.

e) Key use

The key use shall be confirmed, and the key shall be used corrected as per the use. For the public key cryptosystem, the public key shall be verified before use; there shall be security measures to prevent the disclosure and replacement of the key. When key is disclosed, stop using it; start corresponding emergency treatment and response measures. The key shall be replaced according to the key replacement cycle; effective security measures shall be taken to ensure the security of key replacement.

f) Key backup and recovery

A clear key backup strategy shall be developed; take secure and reliable key backup and recovery mechanism to conduct key backup and recovery. The key backup and recovery shall be recorded; and generate the audit information; the audition information includes the subject/time of backup and recovery, etc.

g) Key archiving

Effective security measures shall be taken to ensure the security and correctness of the archive key. The archive key can only be sued to decrypt the history information encrypted by such key, or verify the history information signed by such key. The key archiving shall be recorded, and generate audit information. The audit information includes archive key, archive time, etc.; the archive key shall be conducted data backup; and take effective security protection measures.

h) Key destruction

There shall be measures to destroy the key in an emergency.

8.5 Class-IV information system with classified protection

Key management of Class-IV information system shall include the whole process of management and strategy formulation such as key generation, storage, distribution, input, output, use, backup, recovery, archiving, destruction, etc.; and satisfy:

a) Key generation

audition information includes the subject/time of backup and recovery, etc.

g) Key archiving

Effective security measures shall be taken to ensure the security and correctness of the archive key. The archive key can only be sued to decrypt the history information encrypted by such key, or verify the history information signed by such key. The key archiving shall be recorded, and generate audit information. The audit information includes archive key, archive time, etc.; the archive key shall be conducted data backup; and take effective security protection measures.

h) Key destruction

There shall be measures to destroy the key in an emergency.

9 Security Management

9.1 System

9.1.1 Class-I information system with classified protection

The requirements for Class-I information system are as follows:

a) Cryptographic security management system and operation rules, security operation rules may be formulated. The cryptographic security management system shall include, cryptography management related contents such as cryptography construction, operation and maintenance, personnel, device, key, etc.;

b) The rationality and applicability of the cryptography security management system may be regularly demonstrated and verified; the security management system that has shortcomings and places needed to be improved shall be modified.

9.1.2 Class-II information system with classified protection

The requirements for Class-II information system are as follows:

a) Cryptographic security management system and operation rules, security operation rules should be formulated. The cryptographic security management system shall include, cryptography management related contents such as cryptography construction, operation and maintenance, personnel, device, key, etc.;

b) The rationality and applicability of the cryptography security management system should be regularly demonstrated and verified; the security management system that has shortcomings and places needed to be improved shall be modified.

9.2.2 Class-II information system with classified protection

The requirements for Class-II information system are as follows:

a) Relevant cryptography laws and regulations shall be learned;

b) Cryptographic products shall be used correctly;

c) The corresponding post responsibility system shall be established to clarify the responsibility and authorities of the relevant personnel in the security system;

d) The personnel training system shall be established to provide specialized training for the personnel involving the cryptography operation and management, as well as the key management;

e) The personnel confidentiality system and transfer system for key positions shall be established; sign confidentiality contracts and assume the obligations of confidentiality.

9.2.3 Class-III information system with classified protection

The requirements for Class-III information system are as follows:

a) Relevant cryptography laws and regulations shall be learned;

b) Cryptographic products shall be used correctly;

c) The crucial positions such as key management, security audit, key operation, etc. shall be established according to the cryptography management policy, data security and confidentiality policy, combined with the actual situation of the organization. Establish corresponding post responsibility system; clarify the responsibility and authority of relevant personnel in the security system; establish multi-person co-management system for the crucial positions; the personnel involving key management, security audit, cryptography operation shall be mutually controlled and mutually supervised; the management of relevant device and system, and the use accounts shall not be shared by many people;

d) The personnel assessment system shall be established; post personnel assessment shall be carried out regularly; a reward and punishment system shall be established and improved;

e) The personnel training system shall be established to provide specialized training for the personnel involving the cryptography operation and management, as well as the key management;

f) The personnel confidentiality system and transfer system for key positions shall be established; sign confidentiality contracts and assume the obligations of

9.3.1.2 Class-II information system with classified protection

In the planning stage of the information system, the responsible organization should formulate the cryptography application plan according to the relevant cryptography standard.

9.3.1.3 Class-III information system with classified protection

In the planning stage of the information system, the responsible organization shall formulate the cryptography application plan according to the relevant cryptography standard; organize experts to review; the review opinions serve as the important material for project planning.

The plan after passing the expert examination shall serve as an important basis for construction, acceptance and evaluation.

9.3.1.4 Class-IV information system with classified protection

In the planning stage of the information system, the responsible organization shall formulate the cryptography application plan according to the relevant cryptography standard; organize experts to review; the review opinions serve as the important material for project planning.

The plan after passing the expert examination shall serve as an important basis for construction, acceptance and evaluation.

9.3.2 Construction

9.3.2.1 Class-I information system with classified protection

The cryptography implementation plan may be formulated according to the relevant national standard.

9.3.2.2 Class-II information system with classified protection

The cryptography implementation plan should be formulated according to the relevant national standard.

9.3.2.3 Class-III information system with classified protection

The requirements for Class-III information system are as follows:

a) The implementation plan shall be formulated according to relevant national standard; the plan contents shall include but not limited to information system overviews, security requirements analysis, cryptosystem design plan, cryptographic product list (including product qualification, function and performance list; product manufacturer, etc.), cryptosystem security

9.3.3.4 Class-IV information system with classified protection

The requirements for Class-IV information system are as follows:

a) The security assessment shall be carried out by the cryptography assessment agency before the information is put into operation; only when assessment is passed, can it be put into formal operation;

b) The responsible organization shall entrust the cryptography assessment agency to carry out cryptography application security assessment every year after the information system is put into operation; carry out rectification according to the assessment opinions; if major security hazards are found, the system shall be stopped operating; formulate the rectification plan; when the rectification is finished and assessment is passed, can it be put into operation.

9.4 Emergency

9.4.1 Class-I information system with classified protection

The cryptography security event is handled by the user autonomously according to the security strategy provided by the cryptography product.

9.4.2 Class-II information system with classified protection

Formulate emergency plan; prepare for emergency resource. When the incident occurs, timely dispose according to emergency plan, and combined with actual situation.

9.4.3 Class-III information system with classified protection

The requirements for Class-III information system are as follows:

a) Formulate emergency plan; prepare for emergency resource. When the incident occurs, timely dispose according to emergency plan, and combined with actual situation;

b) After the incident occurs, timely report to the higher authorities of the information system;

c) After the incident is disposed, timely report to the cryptography authority at the same level for the occurrence and disposal of the incident.

9.4.4 Class-IV information system with classified protection

The requirements for Class-IV information system are as follows:

a) Formulate emergency plan; prepare for emergency resource. When the incident

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

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