GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GM/T 0132-2023

Implementation guide for information system cryptography application

信息系统密码应用实施指南

Issued on: December 04, 2023 **Implemented on: June 01, 2024**

Issued by: State Cryptography Administration

Table of Contents

Implementation guide for information system cryptography application

1 Scope

This document provides process guidance and recommendations for the information system cryptography application. It describes the implementation process and main activities in the planning, construction, operation and termination stages.

This document is intended to guide the implementation of information system cryptography application.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 20984, *Information security technology - Risk assessment method for information security*

GB/T 39786, *Information security technology - Baseline for information system cryptography application*

GM/T 0115, *Testing and evaluation requirements for information system cryptography application*

GM/T 0116, *Testing and evaluation process guide for information system cryptography application*

GM/Z 4001, *Cryptography terminology*

3 Terms and definitions

For the purposes of this document, the terms and definitions defined in GB/T 39786 and GM/Z 4001 apply.

4 Overview of implementation of information system

cryptography application

4.1 Roles and responsibilities

The various roles and responsibilities involved in the information system cryptography application are as follows.

a) Cryptography management department

Responsible for managing cryptography work in accordance with the law.

b) Information system responsible unit

Usually including project construction units and information system operation and use units, responsible for designing cryptography application solutions in accordance with the management specifications and technical standards of information system cryptography applications. Use cryptography algorithms, cryptography technologies, cryptography products and cryptography services that comply with national regulations and meet the basic requirements of information system corresponding level cryptography applications to carry out information system cryptography application construction or rectification work. Formulate and implement various supporting security management systems for cryptography applications. Regularly conduct self-inspections on the security status of information system cryptography applications, the implementation of supporting security management systems and measures for cryptography applications. Conduct commercial cryptography application security assessments (referred to as "security assessments") by themselves or entrust commercial cryptography application security assessment institutions, including cryptography application solution security assessments (referred to as "solution security assessments") and information system security assessments (referred to as "system security assessments"). Conduct emergency response to cryptography application security incidents.

c) Cryptography application integration service unit

Responsible for assisting the information system responsible unit to complete the planning, construction, operation and termination stages of information system cryptography application (including but not limited to cryptography application consultation, cryptography application demand analysis, cryptography application solution design, cryptography application integrated construction or rectification services) according to the entrustment of the information system responsible unit and in accordance with the management specifications and technical standards of information system cryptography application.

d) Commercial cryptography application security assessment agency

structure, major software and hardware components, major cryptography products, etc. that may bring high-risk problems), the security requirement level of the information system cryptography application changes, and major cryptography-related security incidents lead to major adjustments, and the cryptography application solution needs to be modified, it shall enter the planning stage from the operation stage, to restart the implementation process of the information system cryptography application.

For information systems that have not developed a cryptography application solution, regardless of whether the information system has started construction and is online, the construction or transformation process of its cryptography application is deemed to start from the planning stage.

The main processes, activities, inputs and outputs of each stage in the basic process of implementing information system cryptography applications shall be in accordance with the provisions of Annex A.

5 Planning of cryptography application in information systems

5.1 Workflow of the planning phase

The goal of the information system cryptography application planning stage is to analyze and clarify the information system's cryptography application requirements and design a clear cryptography application solution based on the basic information system situation, network topology, software and hardware composition, business information, and security requirements, in accordance with the requirements of GB/T 39786. The workflow of the information system cryptography application planning stage is shown in Figure 2.

Understand the overall information of the information system, including basic conditions, network topology, carried business conditions, and software and hardware composition.

b) Identify the management of information systems

Understand the management of information systems, including management organizations, managers, management responsibilities, management systems, and security strategies.

c) Identify the information assets of the information system

Investigate the information assets processed by the information system. Identify important information resources and important data that need to be protected according to national and industry standards for data classification and grading.

d) Determine the security requirements for the application of information system cryptography

Determine the level of security requirements for the information system cryptography application based on the information system's network security protection level.

If the information system has not completed the network security level protection classification, the security requirement level for information system cryptography application shall be determined based on the proposed classification.

e) Comprehensive description of information system

Organize and analyze the collected information to form a description of the current status of the information system from the following aspects:

1) Basic information of the information system;

2) Information system network topology;

3) Business conditions carried by the information system;

4) Information system hardware and software composition;

5) Information system management conditions;

6) Important information assets that need to be protected, including but not limited to important information resources and important data;

7) Security requirement level for information system cryptography application.

Activity output: Information system overview section of the cryptography application solution.

5.2.2 Analysis of security risks in cryptography applications

Activity objectives:

Based on the current status of information systems, analyze the cryptography application security risks in information systems.

Participating roles: information system responsible unit, cryptography application integration service unit.

Activity input: general description document of the information system, classification report of network security protection level, and analysis document of information system assets, threats and vulnerabilities.

Activity description:

According to the corresponding level indicator requirements of GB/T 39786, analyze the current status of the information system to see if it meets the indicator requirements one by one. For those that do not meet the indicator requirements, analyze the security risks they face according to GB/T 20984.

Activity output: security risk analysis of the cryptography application solution.

5.2.3 Determination of basic requirements for cryptography applications

Activity objectives:

Based on the security risk analysis of information system cryptography application, the basic requirements for information system cryptography application are proposed.

Participating roles: information system responsible unit, cryptography application integration service unit.

Activity input: security risk analysis part of the cryptography application solution.

Activity description:

According to the corresponding level indicator requirements in GB/T 39786, basic technical requirements are proposed from four technical levels: physical and environmental security, network and communication security, equipment and computing security, and application and data security. Determine the indicator items that do not involve the corresponding cryptography application requirements at each level. Propose basic requirements for cryptography application management from four aspects: management system, personnel management, construction and operation, and emergency response. Among them, at the network and communication security level, special attention should be paid to the ownership of the responsible party of the

communication channels connecting different information systems, and the cryptography application requirements of the corresponding communication channels should be clarified. At the application and data security level, it is necessary to focus on clarifying the authenticity protection requirements of different login methods of information system users. Clarify the integrity or security protection requirements of each type of important data. Clarify the non-repudiation protection requirements in the business activities of the information system.

Activity output: basic requirements for cryptography application of the cryptography application solution.

5.2.4 Determination of special requirements for cryptography applications

Activity objectives:

Based on the industry characteristics of information systems, special protection requirements for critical information infrastructure and important data, special requirements for information system cryptography application are proposed.

Participating roles: information system responsible unit, cryptography application integration service unit.

Activity input: security risk analysis of cryptography application solutions, and requirements of the industry and critical information infrastructure.

Activity description:

This activity mainly includes the following sub-activities.

a) Special compliance requirements

In response to the actual security risks faced by information systems, special compliance requirements are proposed in accordance with the laws, regulations and requirements related to the industry, critical information infrastructure and important data, the cryptography application requirements proposed by the competent authorities, and the cryptography application requirements proposed in the critical information infrastructure standards that are not included in GB/T 39786 or are higher than GB/T 39786.

b) Special requirements for protecting important information assets

In view of the actual security risks faced by important information assets in information systems, the necessity of implementing special measures for cryptography application is judged. Special requirements for the protection of important information assets are proposed.

Activity output: special requirements for the cryptography application of the

cryptography application solution.

5.2.5 Documentation of requirements analysis results

Activity objectives:

Summarize the basic requirements and special requirements of cryptography applications to form the cryptography application requirements analysis part of the cryptography application solution.

Participating roles: information system responsible unit, cryptography application integration service unit.

Activity input: security risk analysis of cryptography application solution, basic requirements part of cryptography application, and special requirements for cryptography application.

Activity description:

Based on the security risk analysis, basic requirements for cryptography applications, and special requirements for cryptography applications, determine the cryptography application requirements for the information system and form a cryptography application requirements analysis. The cryptography application requirements analysis includes the following:

a) Security risk analysis;

b) Description of basic requirements for cryptography applications;

c) Description of special requirements for cryptography applications.

Activity output: analysis of cryptography application requirements of the cryptography application solution.

5.3 Design of cryptography application solutions

5.3.1 Overall strategy design

Activity objectives:

Determine the overall design goals and design principles for information system cryptography applications so as to carry out the specific design of information system cryptography applications.

Participating roles: information system responsible unit, cryptography application integration service unit.

Activity input: overall security policy document of the information system responsible unit, project establishment, construction and management documents of the information system, system overview part and cryptography application requirements analysis part of the cryptography application solution.

Activity description:

Based on the overall security strategy of the information system responsible unit, combined with the actual situation of information system construction planning and cryptography application needs, the design goals and principles of information system cryptography application should be clarified.

Activity output: design objectives and principles of cryptography application solutions.

5.3.2 Design of cryptography application technology solutions

Activity objectives:

Based on the analysis of cryptography application needs, cryptography application technical measures that need to be implemented in information systems are proposed to guide the specific construction of information system cryptography application.

Participating roles: information system responsible unit, cryptography application integration service unit.

Activity input: the cryptography application requirements analysis of the cryptography application solution.

Activity description:

Design a technical framework for cryptography application based on the analysis of cryptography application requirements. Analyze cryptography protection objects at the levels of physical and environmental security, network and communication security, equipment and computing security, and application and data security. Design and propose cryptography application technical measures to be adopted. Among them, at the level of network and communication security, it is necessary to focus on designing cryptography application technical measures for communication channels across insecure networks. At the level of application and data security, it is necessary to focus on different information systems and design cryptography security mechanisms for their key business links, important business data, business objects, etc. according to their specific security needs. Select login authentication mechanisms for users. Select the national and industry standards for cryptography that need to be followed for the implementation of these mechanisms.

Design the information system key management system. Focus on the types of keys at the application and data levels and the technical implementation and protection methods

of various keys throughout their life cycle. Clarify the technical measures for information system key management.

Determine the sharing of cryptography technology resources within the information system and the supply capacity of cryptography products and services in the market. Make a list of cryptography products and services required.

Determine the need for application system modification when information systems adopt cryptography functions.

Activity output: the cryptography application technical solution of the cryptography application solution.

5.3.3 Design of cryptography application security management solution

Activity objectives:

Based on the analysis of cryptography application needs and combined with the original management model and management strategy, a unified cryptography application supporting security management system is formed.

Participating roles: information system responsible unit, cryptography application integration service unit.

Activity input: cryptography application requirements analysis and cryptography application technical solution of the cryptography application solution.

Activity description:

Based on the analysis of information system cryptography application needs and combined with cryptography application technical solutions, a supporting security management system for cryptography applications should be determined.

Activity output: the cryptography application security management solution of the cryptography application solution.

5.3.4 Compliance self-inspection

Activity objectives:

Conduct self-inspection against the corresponding level requirements of GB/T 39786 and the relevant requirements of the industry and key information infrastructure. Ensure that the cryptography application technology solution and cryptography application security management solution meet the requirements.

Participating roles: information system responsible unit, cryptography application integration service unit.

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

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