GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
Record No.: 58555-2017

GM/T 0050-2016

Cryptography Device Management – Specification of Device Management Technology

密码设备管理 设备管理技术规范

Issued on: December 23, 2016 **Implemented on: December 23, 2016**

Issued by: State Cryptography Administration

Table of Contents

Introduction

Cryptographic device management provides application interface of device management to the upper management application; provides device management functions to the upper management applications such as realization of remote key management, device maintenance, device monitoring, device compliance inspection, etc.; convert the management request of the upper management applications into standard message for transferring; establish the security tunnel of application layer through security protocol; realize the message transferring between management application and cryptographic device.

This Standard specifies the application interface, management process, management information structure of the cryptographic device management; confirms the specific requirements for cryptographic device to implement the management agent; realize the irrelevance between device management application and the specific cryptographic device; to achieve the purposes of the cryptographic device designed and developed according to this Standard shall be uniformly managed and configured by the management system developed as per this Standard. The establishment and operation requirements for the cryptographic device management system can refer to the relevant standards of CA management system; this Standard shall not define additionally. This Standard provides guidance and basis for the study and development of cryptographic device and upper management application.

This Standard stipulates a set of cryptographic device management application interfaces, confirms the specific requirements for the cryptographic device to implement the management agent; realizes the irrelevance between device management application and specific cryptographic device; so that achieve the purpose that the cryptographic device designed and developed as per this Standard can be uniformly managed and configured.

The Clause 5, 6, 7, 8, 9 of this Standard shall be used by the developer of the cryptographic device management system.

The Clause 5, 6, 7, 8 of this Standard shall be used by the cryptographic device manufacturer.

The Clause 5, 9 of this Standard shall be used by the management application manufacturer.

The preparation of this Standard has been guided by the overall working group of National Commercial Cryptographic Application System.

Cryptography Device Management – Specification of Device Management Technology

1 Scope

This Standard specifies the system structure, management process, security tunnel protocol, management information structure, application interface and standard management message format of cryptographic device management.

Provide guidance and basis for the study and development of cryptographic device within the technical system framework and the upper management application.

This Standard is applicable to the study and development of cryptographic device management system, cryptographic device management application, cryptographic machine, and the like cryptographic devices; it can also be used for guiding the inspection of cryptographic device management system and cryptographic device.

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 0006 Cryptographic Application Identifier Criterion Specification

GM/T 0009 SM2 Cryptography Algorithm Application Specification

GM/T 0015 Digital Certificate Format based on SM2 Algorithm

GM/T 0018 Interface Specifications of Cryptography Device Application

3 Terms and definitions

The following terms and definitions are applicable to this document.

3.1 Cryptography device

The device that provides secure storage for key and the secret information, provides

cryptographic security service basis on the secret information. In this Standard, it refers specially to the cryptographic device that can accept the device management operations, it mainly includes network cipher machine, application cipher machine/card; however, it excludes intelligent cryptographic end, cryptographic chip, and the like component-level devices.

3.2 Device certificate

The digital information that can identify the cryptography device ID includes the basic information of cryptography device, device public key information, and other supplement information, etc. The device certificate can be issued by special CA system, but also can be issued by device management platform.

3.3 Security tunnels

The application layer security connection established through the data interaction security protocol between device management center and cryptography device-managed agent; it aims to provide confidentiality and integrity protection for application layer information interaction between device management network and cryptography device.

3.4 Device key pair

The asymmetric key pair for device management stored inside the device, it includes signature key pair and encryption key pair.

3.5 Be-managed object

The cryptography device that accepts the management, it becomes the be-managed object through device-managed agent.

3.6 Device-managed agent

The device-managed device is a logic entity that implements the establishment of security tunnels, analysis of device management message; it processes the message command issued by the device management center, the processed results shall be returned to the device management center. Each device-managed agent corresponds to one cryptography device; the device-managed agent can be realized within the cryptography device or realized by the external host computer of the cryptography device. If it is realized externally, the security connection between external device agent and agent cryptography device.

3.7 Security tunnels message

The initialization protocol message that the cryptography device management platform establishes and maintains secure session connection between the managed device

be divided into three layers as per the function, namely: management application layer, management platform layer and cryptography device layer. The management application layer mainly performs specific management application against the cryptography device including remote key management, remote device monitoring, remote device maintenance, effectiveness inspection of remote device, etc. Management platform layer mainly establishes a security tunnel between device management center and cryptography device; so that enable the upper management center to accurately locate the bottom layer of cryptography device, meanwhile, performs secure data interaction with it. The cryptography device layer mainly includes various cryptography devices such as server cryptography device, cryptography card, etc., but not including the intelligent cryptography terminal devices such as intelligent cryptography key, intelligent IC card, etc.

The two-way ID authentication between cryptography device management platform and cryptography device shall be realized through security protocol; establish application layer security tunnel, transfer the command and realize the data confidentiality and integrity protection through the agreed session key. Each management application performs the specific management against the cryptography device through the security tunnel established between cryptography device management platform and cryptography device.

5.4 Management application layer

The management application indicates the application of cryptography device management, key management, device maintenance, device monitoring, etc. that performs state and data management against the cryptography device. The management application obtains the basic information of the managed device in the database through cryptography device management interface provided by device management center; send specific management command of each application to the managed device.

5.5 Device management platform layer

5.5.1 Structure and function of device management platform

The device management platform layer is also known as cryptography device management service layer, it can adopt hierarchical structure as per the actual application requirements such as general center and subcenter of device management.

When adopting the hierarchical structure, the general center of cryptography device management can set several subcenters of cryptography device management. The general management center provides device management function to the upper management application; general center uniformly manages the be-managed object through the subcenters; the subcenter shall not provide service to the management application. Respectively establish security tunnels between general center and

c) Process and forward the messages between the device management center and be-managed objects;

d) Periodically poll the working status of the be-managed objects; after collecting and arranging, submit to the general center of the device management.

The subcenter of device management is equipped with the device management information base of the subcenter; which stores the basic information of the be-managed objects within its jurisdiction; the content is the same as the Table 1.

5.6 Cryptography device layer

The cryptography device layer refers to various specific be-managed objects; it includes the devices such as cipher machine, cipher card, etc. that provide the cryptographic service functions. The be-managed objects perform information interaction through the device managed agent and device management platform.

The be-managed objects are connected through security tunnel. The managed agent shall be realized on the device terminal; provide the ability to accept system management. The basic requirements for be-managed objects are as follows:

a) Algorithm resource requirements

1) Support the device management algorithm of management platform, otherwise the center shall reject the registration of the be-managed object. The management algorithm application uses the nationally recognized cryptographic algorithm such as symmetric algorithm SM4, asymmetric algorithm SM2, summary algorithm SM3;

2) The public and private key pairs can be generated to generate the certificate application; or obtain certificate from the external certification system;

3) It can securely store the be-managed object' s own certificate and private key; the direct subcenter and general center certificate.

b) Requirements for managed agent: it shall realize managed agent, finish the establishment of security tunnel, response the standard management information packet.

1) Internally managed agent: the managed agent is realized within the be-managed object; realize the security tunnel protocol. The cryptography service function used by the security tunnel shall be provided by the be-managed object internally;

2) Externally managed agent: for the be-managed objects that can't support the internally managed agent functions, they can be maintained by using the

5.8.2 Registration for subcenter of device management

The registration process for subcenter of device management is as follows:

a) The subcenter of device management generates the certificate application;

b) The subcenter of device management submits the device information form, certificate application and supported algorithm to the general center of device management; the algorithm ID definition can refer to GM/T 0006;

c) The general center of device management audits the application. If the audit is passed, then record such subcenter information into the device management information base; if the audit isn't passed, then such application shall be rejected (for instance, don't support the algorithm used in the subcenter, etc.);

d) The general center of device management issues dual certificates of the subcenter; the format shall conform to the relevant specification (e.g.: SM2 certificate shall follow GM/T 0015); export the device certificates of general center and subcenter; then submit to the lower device subcenter;

e) The subcenter of device management imports the device certificate of the subcenter and general center.

NOTE: the information transferring for the subcenter registration shall adopt the offline mode.

5.8.3 Registration of be-managed object

The registration procedure of be-managed is as follows:

a) The be-managed device generates the certificate application;

b) The be-managed device submits the device information form, certificate application and supported algorithm to the subcenter of device management; the algorithm identifier definition can refer to GM/T 0006;

c) The subcenter of device management transfers such registration application to the general center through establishing security tunnel with general center;

d) The general center of device management audits the application. If the audit is passed, then record such device information into the device management information base. If the algorithm used by the device is not supported, then such application shall be rejected;

e) The general center of device management issues the device certificate; exports the device certificate and device certificate of general center; sends to the lower device subcenter through the security tunnel;

f) The subcenter of device management sends the general center certificate, subcenter certificate, and device center to the lower be-managed device;

g) The be-managed device imports the device certificate, subcenter device certificate and general center device certificate.

NOTE: The registration of the be-managed device to the management subcenter adopts the offline mode; the registration information is transferred between subcenter and general center through the security tunnel.

6 Security tunnel message

6.1 Security tunnel protocol

The security tunnel protocol is a security protocol used for the management information interaction between device management center and cryptography device management agent; it realizes the establishment of secure connection of the application layers between device management application and cryptography device; provides the confidentiality and integrity protection against the information interaction of application layers. The security tunnel protocol framework is shown in Appendix B.

6.2 Security tunnel message

6.2.1 Definition of format for security tunnel message

The security tunnel message is an initialization protocol message of secure session connection established and maintained by the cryptography device management platform between be-managed device and management center; it is used for ensuring the trusted ID on the two ends of the session; ensuring the confidentiality and integrity of the managed messages that are carried.

This clause defines the format of the security tunnel message, instructs the opportunity for establishing and using the security tunnel.

The signature value in the message format below is the signature of all contents (except the signature value) of the structure shown in Figure 3, which is singed by the message producer. When adopting the SM2 algorithm, the signature format shall follow GM/T 0009; when adopting RSA algorithm, follow the specification of PKCS#1.

The message format is shown in Figure 3.

layer device shall be re-established. The upper management center must send a clear notification to such device; the be-managed device clears the message ID; then the be-managed device launches the establishment of security tunnel.

When the security tunnel adopts the long-connection mode, the bottom-layer device or subcenter shall establish and long-term maintain such connection with the upper-layer center; when the security tunnel adopts the short-connection mode, the bottom-layer device and subcenter shall establish connection and finish the data sending with the upper-layer center, after that disconnect with the upper-layer center; if data is required to be sent again, then restart the connection.

6.4 Use of security tunnel

All messages between management center and be-managed device shall be sent through security tunnel. The subcenter shall be passed between the sender and target party; the sender packs and transmit such message to the subcenter, then the subcenter shall be responsible for transferring to the target party.

7 Device management information

7.1 Definition of device management information

The device management information indicates the standard data format that is queried or configured when cryptography device management system remotely manages the cryptography device.

The management center queries and configures the management information against the cryptography device according to the definition of device management information specified in Clause 8; the be-managed cryptography device requires to support the management attribute defined in this Clause, which is used for the query and configuration of management center.

7.2 Definition of data type

management application

9.1 Overview

The device management platform provides 4 types of interfaces for the management application, which include system initialization interface, device attribute management interface, data sending interface, alarm information management interface. The specific interfaces are as follows:

a) System initialization interface:

1) Initialization device management environment: SMF_Initialize

2) Exit device management environment: SMF_Finalize

b) Device attribute management interface:

1) Get the total number of be-managed device: SMF_GetDeviceCount

2) Get device identifier and information as per device number: SMF_GetDeviceInfo

3) Get device attribute values in batches: SMF_GetMultiDeviceInfo

4) Set device attribute value: SMF_SetDeviceValue

5) Export device certificate: SMF_GetDeviceCert

c) Data sending interface:

1) Send data: SMF_SecTunnelSendData

d) Alarm information management interface:

1) The number of alarm information gotten: SMF_GetTrapCount

2) Get one alarm information: SMF_GetTrapInfo

3) Set alarm information to be processed: SMF_SetTrapInfo

9.2 System initialization interface

9.2.1 Initialization device management environment

Prototype: Int SMF_Initializa (void ** pMangeHandle);

Description: initialization device management, get the security tunnel handle of device management.

a) Establishment of security tunnel:

1) Management agent generates a random number of randomA, after signifying the randomA, use the certificate public key of management center to encrypt it; establish request to send the message to the management center through the security tunnel;

2) Management center decrypts it and obtains the plaintext of randomA, and verifies the signature. After the verification is passed, management center shall store the plaintext of randomA. Meanwhile, generate another random number of randomB, after signifying the randomB, use the certificate public key of management agent to encrypt the randomA and randomB; establish response message and return to management agent through the security tunnel;

3) Management agent decrypts and obtain the plaintext of randomA and randomB; compare whether randomA is consistent with the random number sent by itself; verify the signature of randomB;

4) The two parties perform exclusive-or for randomA and randomB; the obtained results shall be taken as the session key of the security tunnel.

b) Use of security tunnel:

1) The use of security tunnel refers to the communication parties use the established security tunnel to transmit the information securely. The data transmitted by the communication parties shall be encrypted and protected by the agreed session key of the security tunnel; use the agreed HMAC algorithm (SM3) to calculate the whole packet data's MAC values; so that ensure the data confidentiality and integrity during the transmitting process;

2) Within the valid period of security tunnel, the session key shall be stored in the memory of cryptography device on the two ends of the security tunnel. The memory of cryptography device in the device management center shall maintain all session keys of all lower-level cryptography devices; the device management center terminal shall maintain the correspondence between session key and security tunnel.

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

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