GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
File No.: 58558-2017

GM/T 0053-2016

Cryptography device management – Data interface specification of remote monitoring and compliance testing

密码设备管理 - 远程监控与合规性检验接口数据规范

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

Issued by: State Cryptography Administration

Table of Contents

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

GM/T 0053 Cryptography device management - Remote monitoring and compliance verification interface data specification is one of the cryptography device management standards. This type of standard consists of a basic specification and a series of management application specifications and currently includes:

- Basic specifications: GM/T 0050 Cryptography device management - Device management technical specifications;

- Management application specification: GM/T 0051 Cryptography device management - Specifications of symmetric key management technology;

- Management application specification: GM/T 0052 Cryptography device management - VPN device monitoring management specification;

- Management application specification: GM/T 0053 Cryptography device management - Remote monitoring and compliance verification interface data specification.

Any contents of this standard related to the contents of cryptographic algorithms are implemented in accordance with relevant national laws and regulations.

This Standard was proposed by and shall be under the jurisdiction of Cryptography Industry Standardization Technical Committee.

Main drafting organizations of this Standard: Shanghai Information Security Engineering Technology Research Center, Shanghai Xinhao Information Technology Co., Ltd., Weishitong Information Industry Co., Ltd., Shanghai Jiaotong University School of Information Security, Shanghai Pengyue Jinghong Information Technology Development Co., Ltd., Shanghai Tianrongxin Network Security Technology Co., Ltd., Shanghai Huatang Network Co., Ltd.

Main drafters of this Standard: Wang Hao, Yuan Feng, Li Gaojian, Tian Li, Huang Zhirong, Liao Ye, Zou Ru, Pan Shuyuan, Yao Le, Lu Mingzhong, Wang Hegang, Wang Shanyi, Zhang Yuanchen, Zhou Zhihong, Li Junshan, Pan Limin.

Cryptography device management – Data interface specification of remote monitoring and compliance testing

1 Scope

This standard specifies interface data of such management applications as remote monitoring and compliance testing of the cryptography device, defines the message transmission format between management applications and cryptography devices.

This standard applies to the development and application of management agents in cryptography devices, it can also guide the detection of such cryptography device-managed agents.

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 standard.

GM/T 0006-2012 Cryptography application identity specification

GM/T 0050 Cryptography device management - Device management technical specifications

3 Terms and definitions

The terms and definitions of GM/T 0050-2016 and the following terms and definitions apply to this document.

3.1

Cryptography device

Cryptography devices that can accept device management operations, such as network cryptography machines, application cryptography machines/cards, excluding component-level devices such as smart cryptography terminals and cryptography chips.

3.6

Cryptography device management platform

A management system that establishes remote security tunnels with the be-managed objects for management applications.

[GM/T 0050-2016, Definition 3.9]

3.7

Key desynchronization

It refers to the case of failing to make correct encryption and decryption for the communication message due to communication message incompleteness and key inconsistency between the both parties for the encrypted communication. Generally, it requires the cryptography device to obtain the key from the key management center or the both parties of mutual communication re-negotiate the key.

3.8

Tunnel connectivity

Communication and connection between cryptography devices and other devices that need to be interconnected.

4 Abbreviations

The following abbreviations apply to this document.

PDU: Package Data Unit

VID: Device be-managed attribute identifier (Value ID)

5 Cryptography device management application system

5.1 Architecture

For the cryptography device management architecture, please refer to clause 5.3 of GM/T 0050-2016, and the structure diagram is shown in Figure 1 (The solid line refers to the physical connection and the dotted line refers to the logical connection). The management system is divided into three layers in accordance with functions: management application layer, management

G	32-byte	H	1-byte
I	1-byte	J	2-byte
K	Version number	L	Security mode
M	Reserved	N	Message ID
O	PDU length	P	Destination ID
Q	Sender ID	R	Operation type
S	Device compliance identifier	T	Device compliance testing message
U	Signature length	V	Signature value/HMAC
W	Message header	X	Message PDU
Y	Message tail		

Figure 4 -- Device compliance testing message format definition

Where:

- The operation type sends a message for the security tunnel, the identifier is 0xA3.
- The management application identifier of the device compliance testing is 0xC4.
- This clause regulates the device compliance testing message PDU behind the management application identifier 0xC4.
- The 0x93 command is used to send data between the management application layer and the management agent, and the 0x94 command is used to receive data.
- Management application layer to send standard data (such as symmetric algorithm ID, algorithm length, plaintext, key, ciphertext) to the management agent, management agent receives 0x93 data packets, parses the standard data in accordance with the defined message format, calculates the corresponding returned value in accordance with the relevant algorithm, seals it using the message format as defined by the application layer and sends it to the application layer. The application layer verifies the returned data with the standard data.

6.2.3 Algorithm validation verification

6.2.3.1 Sending data

6.2.3.1.1 Message format

The format of the sending data message defines the message format of the cryptography device algorithm validity verification instruction, as shown in Table 3.

Table 7 -- Asymmetric algorithm encryption, public key and plaintext

1-byte	32-byte	1-byte	4-byte	4-byte	4-byte	4-byte		4-byte	
Packet type 0x93	Request device ID	Data direction 0x00	Scheme number	Scheme length	Algorithm identifier	Public key length	Public key value	Ciphertext length	Ciphertext

0x01000000	RSA
0x01010000	SM2

Where:

- Type 0x93 is the identifier of the sent data;
- The request device ID is the device uniqueness identifier obtained from the device management platform layer when requesting the device to register;
- The data direction 0x00 indicates that the management application layer sends data to the management agent;
- The scheme number identifies two asymmetric algorithms for encryption;
- The scheme length indicates the number of bytes of the following scheme content. The scheme content includes the algorithm identifier, public key length, public key value, plaintext length, and plaintext content;
- The cryptographic algorithm identifier follows GM/T 0006-2012;
- The public key length indicates the number of bytes of public key values;
- The public key is the standard data of the public key;
- The plaintext length indicates the number of bytes in the plaintext content;
- The plaintext is standard data in plaintext.

b) Asymmetric algorithm decryption, the standard data combination is the private key and digital envelope. The corresponding returned value is plaintext. The defined format is shown in Table 8.

Table 10 -- Asymmetric algorithm check, public key and signature value

1-byte	32-byte	1-byte	4-byte	4-byte	4-byte	4-byte		4-byte	
Packet type 0x93	Request device ID	Data direction 0x00	Scheme number	Scheme length	Algorithm identifier	Public key length	Public key value	Signature value length	Signature value

0x01000300	RSA
0x01010300	SM2

Where:

- Type 0x93 is the identifier of the sent data;
- The request device ID is the device uniqueness identifier obtained from the device management platform layer when requesting the device to register;
- The data direction 0x00 indicates that the management application layer sends data to the management agent.
- Scheme number identifies two asymmetric algorithms for signature verification;
- The scheme length indicates the number of bytes of the following scheme contents. The scheme contents include such contents as the algorithm identifier, the public key length, the public key value, the signature value length, and the signature value;
- The cryptographic algorithm identifier follows GM/T 0006-2012;
- The public key length indicates the number of bytes of public key values;
- The public key value is the standard data of the public key;
- The signature value length indicates the number of bytes of the signature value content;
- The signature value content is the standard data of the signature value.

e) Key exchange. The standard data combination is public key, temporary public key, and initiator ID. The corresponding returned values are public key, temporary public key, and response ID. The definition format is shown in Table 11.

Table 14 -- Symmetric algorithm of returned value in ciphertext and key

1-byte	32-byte	1-byte	1-byte	4-byte	4-byte	4-byte	4-byte		4-byte	
Packet type 0x94	Request device ID	Data direction 0x01	Verification succeeded 0x00	Scheme number	Scheme length	Algorithm identifier	Key length	Key value	Ciphertext length	Ciphertext value

0x00000000	ECB
0x00010000	CBC
0x00020000	CFB
0x00030000	OFB

Where:

- Type 0x94 is the identifier of the returned data;
- The request device ID is the device uniqueness identifier obtained from the device management platform layer when requesting the device to register;
- The data direction 0x01 indicates that the management agent sends data to the management application layer;
- Verification result 0x00 means that the verification is succeeded;
- The scheme number identifies the four working modes of symmetric algorithm encryption;
- The scheme length indicates the number of bytes of the following scheme contents. The scheme contents include the algorithm identifier, key length, key value, ciphertext length, and ciphertext contents.
- The cryptographic algorithm identifier follows GM/T 0006-2012;
- The key length indicates the number of bytes of the key value;
- The key value is the key used to encrypt the plaintext;
- Ciphertext length indicates the number of bytes of ciphertext contents;
- The ciphertext content is the result of encrypted plaintext.

b) The symmetric algorithm encrypts the plaintext, the standard data is combined into the plaintext and the key, and the message format returning the ciphertext is defined in Table 15.

Table 18 -- Asymmetric algorithm with returned value in plaintext

1-byte	32-byte	1-byte	1-byte	4-byte	4-byte	4-byte	4-byte	
Packet type 0x94	Request device ID	Data direction 0x01	Verification result 0x00	Scheme number	Scheme length	Algorithm identifier	Plaintext length	Plaintext value

0x01000101	RSA
0x01010101	SM2

Where:

- Type 0x94 is the identifier of the returned data;
- The request device ID is the device uniqueness identifier obtained from the device management platform layer when requesting the device to register;
- The data direction 0x01 indicates that the management agent sends data to the management application layer;
- The verification result 0x00 indicates that the verification is successful;
- Scheme number identifies two asymmetric algorithms to decrypt the digital envelope;
- The length of the scheme indicates the number of bytes of the following scheme contents. The scheme contents include the algorithm identifier, the length of the plaintext, and the contents of the plaintext;
- The cryptographic algorithm identifier follows GM/T 0006-2012;
- The plaintext length indicates the number of bytes of the plaintext content;
- Plaintext content is the result of the digital envelope decrypted with a private key.

c) The asymmetric algorithm signature plaintext, the standard data combination is the private key and the plaintext, the message format definition with the return value in the signature value is shown in Table 19.

Table 20 -- Asymmetric algorithm with return value in plaintext

1-byte	32-byte	1-byte	1-byte	4-byte	4-byte	4-byte	4-byte	
Packet type 0x94	Request device ID	Data direction 0x01	Verification result 0x00	Scheme number	Scheme length	Algorithm identifier	Plaintext length	Plaintext

0x01000300	RSA
0x01010300	SM2

Where:

- Type 0x94 is the identifier of the returned data;
- The request device ID is the device uniqueness identifier obtained from the device management platform layer when requesting the device to register;
- The data direction 0x01 indicates that the management agent sends data to the management application layer;
- The verification result 0x00 indicates that the verification is successful;
- Scheme number identifies two asymmetric algorithm signatures;
- The length of the scheme indicates the number of bytes of the following scheme contents. The scheme contents include the algorithm identifier, the length of the plaintext, and the contents of the plaintext.
- The cryptographic algorithm identifier follows GM/T 0006-2012;
- The plaintext length indicates the number of bytes of the plaintext content;
- The content of the plaintext is the contents of the signature decrypted with public key.

e) Key exchange. The standard data combination is public key, temporary public key and initiator ID. The return values are public key, temporary public key, and message format definition of responder ID, as shown in Table 21.

6.2.4 Device self-test

The cryptography device self-test means that the management application layer issues a status query instruction to the cryptography device-managed agent, allowing the device to check the correctness of the cryptographic algorithm, the integrity of the key, and whether the main function is normal.

The device self-test message format is shown in Table 24.

Table 24 -- Device self-test message

1-byte	32-byte	1-byte	4-byte	4-byte
Type 0x93	Request device ID	Data direction 0x00	Scheme number	Scheme content

1-byte	1-byte	1-byte	1-byte
Cryptography algorithm correctness	Random number	Key completeness	Cryptography service function correctness
(0x00: inspection;	(0x00: inspection;	(0x00: inspection;	(0x00: inspection;
0x01: not inspected)	0x01: not inspected)	0x01: not inspected)	0x01: not inspected)

Where:

- Type 0x93 is the identifier of the sent data;
- The request device ID is the device uniqueness identifier obtained from the device management platform layer when requesting the device to register;
- 0x00 of the data direction identifier indicates that the management application layer sends data to the management agent;
- The scheme number 0x03000000 identifies the device self-test message.

The format of the message returned by the successful device self-test operation is shown in Table 25.

Table 25 -- Return operation success result message

1-byte	32-byte	1-byte	1-byte	4-byte	4-byte
Type 0x94	Request device ID	Data direction 0x01	Self-test result 0x00	0x03000000	Scheme content

1-byte	1-byte	1-byte	1-byte
Cryptography algorithm correctness	Random number	Key completeness	Cryptography service function

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

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