ICS 35.040
L 80
备案号：

中华人民共和国密码行业标准

GM/T XXXX—XXXX

密码设备管理应用的数据接口规范

Data Interface Specification of

Cryptographic Equipment Management Application

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

××××-××-××发布　　××××-××-××实施

国家密码管理局 发布

目　　次

前　言

本标准依据 GB/T 1.1-2009 给出的规则起草。

本标准在 GM/T AAAAA 《密码设备管理技术规范》定义的应用体系框架基础上制定。

请注意本标准的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准由国家密码管理局提出并归口。

本标准起草单位：上海(暨国家)信息安全工程技术研究中心、卫士通信息产业股份有限公司、上海信昊信息科技有限公司、上海交通大学信息安全学院、上海鹏越惊虹信息技术发展有限公司、上海天融信网络安全技术有限公司、上海华堂网络有限公司。

本标准主要起草人：王隽、袁峰、田立、黄志荣、廖烨、潘淑媛、药乐、吕明忠、王贺刚、李高健、王善义、周志洪、李俊山、潘利民。

本标准凡涉及密码算法相关内容，按国家有关法规实施。

引　言

本标准在 GM/T AAAAA《密码设备管理技术规范》定义的应用体系框架基础上，对密码设备管理的远程监控、设备合规性等管理应用的数据接口进行规范，定义了管理应用与密码设备间的消息传递格式。

本标准编制过程中得到了国家商用密码应用体系总体工作组的指导。

密码设备管理应用的数据接口规范

1 范围

本标准规定了对密码设备进行远程监控、设备合规性检验等管理应用的数据接口，定义了管理应用与密码设备间的消息传递格式。

本标准适用于密码设备中的管理代理的研发与应用，也可以指导该类密码设备管理代理的检测。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GM/T 0006-2012 《密码应用标识规范》

GM/T AAAAA 《密码设备管理技术规范》

3 术语和定义

GM/T AAAAA 界定的以及下列术语和定义适用于本标准。

3.1

密码设备 cryptography device

在本标准中，专指可以接受设备管理操作的密码设备，如网络密码机、应用密码机/卡，不包括智能密码终端、密码芯片等部件级设备。

注：改写 GM/T AAAAA，定义 3.1

3.2

设备证书 device certificate

可以标识密码设备身份的数字信息，包括密码设备的基本信息、设备公钥信息及其他补充信息等。

设备证书由设备管理平台签发。

注：改写 GM/T AAAAA，定义 3.2

3.3

安全通道 security tunnels

通过设备管理中心与密码设备管理代理之间的通信协议建立起来的安全连接，目的是为设备管理应用与密码设备之间的信息交互提供机密性和完整性保护。

[GM/T AAAAA，定义 3.3]

3.4

设备密钥 device key pair

存储在设备内部的用于设备管理的非对称密钥对，包括签名密钥对和加密密钥对。

[GM/T AAAAA，定义 3.4]

3.5

设备管理代理 device-managed agent

设备管理代理是介于密码设备管理平台与密码设备之间的逻辑实体，处理设备管理应用层下发的消息命令，并将处理结果返回给设备管理应用层。每个密码设备对应一个设备管理代理，设备管理代理在密码设备内部实现。

注：改写[GM/T AAAAA，定义 3.6]

4 缩略语

下列缩略语适用于本标准。

PDU：包数据单元（Package Data Unit）

VID：设备被管属性标识符（Value ID）

5 密码设备管理应用体系

5.1 体系结构

密码设备管理体系结构请参见 GM/T AAAAA 的 5.2，结构图如图 1 所示。管理体系划分为三层，分别为：管理应用层、管理平台层和密码设备层，其详细定义参见 GM/T AAAAA 的 5.3、5.4 和 5.5。

密码设备管理体系中的管理应用是从管理应用层发起的管理指令，通过设备管理平台层和安全通道到达设备管理代理，由管理代理负责解析，并按指令内容进行操作。

本标准主要涉及密码设备管理平台层和密码设备层的管理应用接口，包括远程监控、设备合规性检验等。

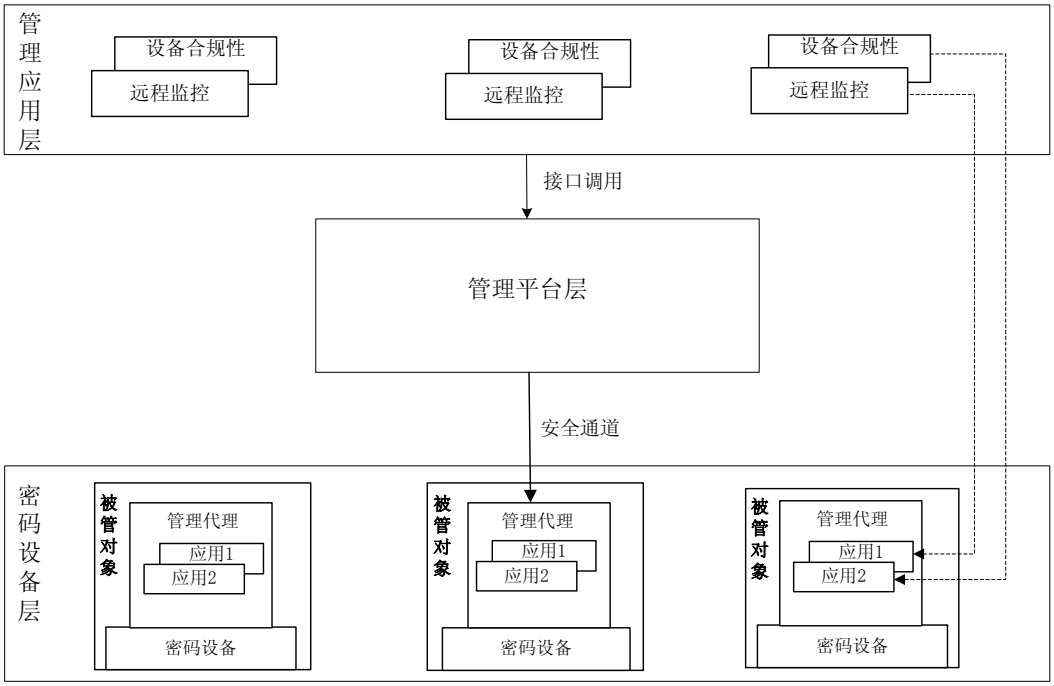

图 1　密码设备管理应用体系结构图

5.2　对密码设备的基本要求

密码设备应配备国家密码主管部门批准的密码算法，包括对称算法、非对称算法和杂凑算法；具有密钥的产生、安装、安全存储、更新、销毁、备份和恢复等密钥管理功能。

设备管理体系中的密码设备内，应安装管理代理，其应用接口遵循本规范。

5.3　对管理代理的基本要求

密码设备管理代理负责接收管理应用层通过设备管理平台和安全通道下发的策略和指令，解析包括安全通道消息、设备管理消息和管理应用消息等指令，调用特定的模块对密码设备进行管理操作，并将操作结果返回。本标准主要涉及管理应用类消息。

对管理代理的基本要求遵循 GM/T AAAAA 的 5.5.1。

管理代理逻辑结构示意图如下图 2 所示。密码设备厂商应根据本标准规定的接口规范实现管理代理。

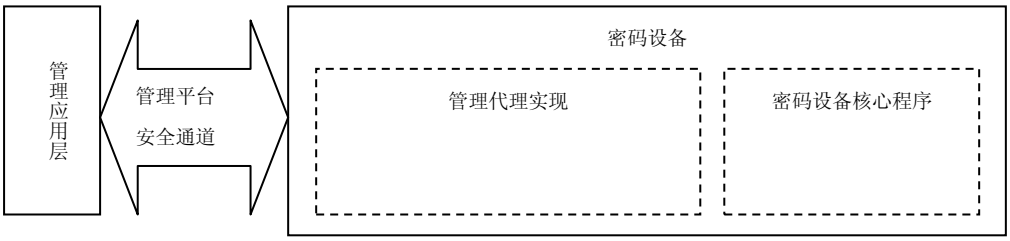

图 2　管理代理示意图

5.4 安全通信

管理代理与设备管理平台间的所有消息，都通过安全通道发送。

安全通道的建立时机，建立安全通道的请求和响应消息格式以及建立安全通道之后，通过安全通道发送的 PDU 消息格式等遵循 GM/T AAAAA 的 6.1 定义，安全通道的使用说明遵循 GM/T AAAAA 的 6.2。

6 设备管理应用的数据接口

6.1 密码设备远程监控

6.1.1 远程监控消息格式

密码设备远程监控是指监控密码设备的状态和密码算法的相关状态，密码设备的状态包括密码服务状态、隧道连通状态等。

设备远程监控应用调用 GM/T AAAAA 的 9.8 节 SMF_SecTunnelSendData 函数，将管理指令填充在设备管理平台指令的消息 PDU 中，管理消息赋值在 sendData 字段，具体消息格式如下图 3 所示（参见 GM/T AAAAA 第 6.2 章节）：

图 3 设备远程监控消息格式定义

其中：

操作类型为安全通道发送消息，标识为 0xA3；

远程监控的管理应用标识为 0xC1。

本章节对 0xC1 后面的远程监控消息 PDU 作出规范。

设备远程监控消息包括监控信息请求消息和监控信息响应消息，分别由表 1、表 2 定义。

6.1.2 请求监控信息的消息格式

管理应用向管理代理请求监控信息的消息格式如下表 1 所示。

表 1 监控信息请求

1字节	32字节	8字节	14字节
类型0XC3	请求设备ID	VID	请求参数（只在获取日志时使用）

其中：

类型 0xC3 是管理应用层向管理代理请求监控信息的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识。

VID 定义见下面表 2；

请求参数只在获取日志时使用，其第 1 个 7 字节是获取日志开始时间，第 2 个 7 字节是获取日志结束时间，时间的具体定义参见 GM/T AAAAA 的第 7.1 章节。

6.1.3 返回监控信息的消息格式

管理代理向管理应用层返回监控信息的消息格式如下表 2 所示，参见 GM/T AAAAA 的第 7.2 章节的树形结构，被管对象的属性分为设备状态监控组和设备日志监管组，组别编号分别为 0x05 和 0x06，设备生产厂商和设备管理应用开发厂商应按照此规则开发。未定义的部分可按照 VID 定义规则自行扩展。

表 2 监控信息响应

1字节	32字节	8字节	N字节
类型0xC4	请求设备ID	VID	返回结果

信息分组	名称	VID	返回结果描述
设备状态监控	密码服务状态	0x05000002 0x00000000	底层硬件是否能提供正常的密码服务（1字节）： 0：正常 1：异常
	密钥更新状态	0x05000003 0x00000000	密钥更新状态（1字节）：1：待更新 2：正在更新 3：已更新 4：更新失败
	隧道连通性	0x05000004 0x00000000	隧道是否连通的状态（1字节）： 0：已连通 1：未连通
	密钥失步监视	0x05000005 0x00000000	密钥是否失步的状态 （1字节）：0：未失步 1：已失步
	IP地址是否变更	0x05000008 0x00000000	判断设备接入的实际IP地址与在管理中心登记的IP是否一致，该监控项由中心端负责处理（1字节）： 0：不一致 1：一致
	随机数发生器的状态	0x05000009 0x00000000	判断密码设备中随机数发生器的状态（1字节）： 0:正常 1：异常
	关键程序校验	0x0500000A 0x00000000	关键程序的有效性（1字节）：0：正常 1：异常（如密码设备中运行的核心程序是否被篡改）
设备日志监管	密码设备日志数目	0x06000001 0x00000000	密码设备的日志数目（4字节）
	密码设备日志表	0x06000002 0x00000000 (注：获取日志采用get_bulk命令进行获取，获取日志前首先要使用get_bulk取得日志的数目)	日志序号（1字节） 日志级别（1字节）： 1：信息 2：警告 3：错误 日志内容（4字节） 日志记录时间（7字节，年月日时分秒）

注：get-bulk 操作的消息格式遵循 GM/T AAAAA 第 8.5 章节的定义。

其中：

类型 0xC4 是管理代理向管理应用层返回监控信息的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识。

6.2 设备合规性检验

6.2.1 设备合规性检验概述

设备合规性检验是对密码设备的算法有效性进行校验。

算法有效性校验是指管理代理接收到管理应用层下发的数据包后，解析出标准数据，并按照有关算法计算得到校验数据，然后将数据封装返回给管理应用层。

设备自检是指管理应用层向密码设备管理代理下发状态查询指令，让设备自己去检查密码算法实现的正确性、密钥的完整性以及主要功能是不是正常。

6.2.2 设备合规性检验消息格式

设备合规性检验调用 GM/T AAAAA 第 9.8 节 SMF_SecTunnelSendData 函数，将管理指令填充在设备管理平台指令的消息 PDU 中，管理消息赋值在 sendData 字段，具体消息格式如下图 4 所示（参见 GM/T AAAAA 第 6.2 章节）：

图 4 设备合规性检验消息格式定义

其中：

操作类型为安全通道发送消息，标识为 0xA3；

设备合规性检验的管理应用标识为 0xC4。

本章节对管理应用标识 0xC4 后面的设备合规性检验消息 PDU 作出规范。

管理应用层与管理代理之间以 0x93 命令发送数据，0x94 命令接收数据。

管理应用层发送标准数据（如对称算法的算法标识、算法长度、明文、密钥、密文）到管理代理，管理代理接收到 0x93 数据包，按照定义的消息格式解析出标准数据，并按照相关算法计算得到相应的返回值，然后按照应用层定义的消息格式封装发送给应用层。应用层将返回的数据与标准数据进行校验。

6.2.3 算法有效性校验

6.2.3.1 发送数据消息格式

发送数据消息格式定义了密码设备算法有效性校验指令的消息格式，如下表 3 所示。

表 3　发送数据消息格式

1字节	32字节	1字节	4字节	4字节	
包类型0x93	请求设备ID	数据方向	方案编号	方案长度	方案内容

1字节算法类别	1字节工作模式	1字节密码技术	1字节标准数据组合
0x00：对称算法	0x00：ECB	0x00：加密	0x00：明文
	0x01：CBC	0x01：解密	0x01：明文+密钥
	0x02：CFB		0x02：密文+密钥
	0x03：OFB		
0x01：非对称算法	算法类型	0x00：加密	0x00：公钥+明文
	0x00：RSA	0x01：解密	0x01：私钥+数字信封
	0x01：ECC	0x02：签名	0x02：私钥+明文
		0x03：验签	0x03：公钥+签名
		0x04：密钥交换	0x04：公钥+临时公钥+发起方ID
0x02：杂凑算法	0x00		0x01：大于等于分组
			0x02：小于分组

其中：

类型 0x93 是发送数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向标识的 0x00 表示管理应用层向管理代理发送数据，0x01 表示管理代理向管理应用层发送数据；

方案长度指示后面方案内容的字节数；

方案内容由下面表 4、表 5、……、表 12 定义。

6.2.3.1.1　对称算法

a)　对称算法加密明文，标准数据组合为明文，对应返回值为密文+密钥，定义格式如下表 4 所示。

表 4　对称算法加密，明文

1字节	32字节	1字节	4字节	4字节	4字节	4字节	
包类型0x93	请求设备ID	数据方向0x00	方案编号	方案长度	算法标识	明文长度	明文内容

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

其中：

类型 0x93 是发送数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x00 表示管理应用层向管理代理发送数据；

方案编号标识对称算法加密的四种工作模式；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、明文长度和明文内容；

密码算法标识遵循 GM/T 0006-2012；

明文长度指示明文内容的字节数；

明文内容为明文的标准数据。

b) 对称算法加密明文，标准数据组合为明文+密钥，对应返回值为密文，定义格式如下表 5 所示。

表 5　对称算法加密，明文+密钥

1字节	32字节	1字节	4字节	4字节	4字节	4字节		4字节	
包类型 0x93	请求设备ID	数据方向0x00	方案编号	方案长度	算法标识	密钥长度	密钥值	明文长度	明文内容

0x00000001	ECB
0x00010001	CBC
0x00020001	CFB
0x00030001	OFB

其中：

类型 0x93 是发送数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x00 表示管理应用层向管理代理发送数据；

方案编号标识对称算法加密的四种工作模式；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、密钥长度、密钥值、明文长度和明文内容；

密码算法标识遵循 GM/T 0006-2012；

密钥长度指示密钥值的字节数；

密钥值为密钥的标准数据；

明文长度指示明文内容的字节数；

明文内容为明文的标准数据。

c) 对称算法解密密文，标准数据组合为密文+密钥，对应返回值为明文，定义格式如下表 6 所示。

表 6　对称算法解密，密文+密钥

1字节	32字节	1字节	4字节	4字节	4字节	4字节		4字节	
包类型0x93	请求设备ID	数据方向0x00	方案编号	方案长度	算法标识	密钥长度	密钥值	密文长度	密文内容

0x00000100	ECB
0x00010100	CBC
0x00020100	CFB
0x00030100	OFB

其中：

类型 0x93 是发送数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x00 表示管理应用层向管理代理发送数据；

方案编号标识对称算法解密的四种工作模式；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、密钥长度、密钥值、密文长度和密文内容；

密码算法标识遵循 GM/T 0006-2012；

密钥长度指示密钥值的字节数；

密钥值为密钥的标准数据；

密文长度指示密文内容的字节数；

密文内容为密文的标准数据。

6.2.3.1.2　非对称算法

a) 非对称算法加密，标准数据组合为公钥+明文，对应返回值为数字信封，定义格式如下表 7 所示。

表 7　非对称算法加密，公钥+明文

1字节	32字节	1字节	4字节	4字节	4字节	4字节		4字节	
包类型 0X93	请求设备 ID	数据方向 0X00	方案编号	方案长度	算法标识	公钥长度	公钥值	明文长度	明文

0x01000000	RSA
0x01010000	ECC

其中：

类型 0x93 是发送数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x00 表示管理应用层向管理代理发送数据；

方案编号标识加密的两种非对称算法；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、公钥长度、公钥值、明

文长度和明文内容；

密码算法标识遵循 GM/T 0006-2012；

公钥长度指示公钥值的字节数；

公钥值为公钥的标准数据；

明文长度指示明文内容的字节数；

明文内容为明文的标准数据。

b) 非对称算法解密，标准数据组合为私钥+数字信封，对应返回值为明文，定义格式如下表 8 所示。

表 8 非对称算法解密，私钥+数字信封

1字节	32字节	1字节	4字节	4字节	4字节	4字节		4字节	
包类型 0X93	请求设备 ID	数据方向 0X00	方案编号	方案长度	算法标识	私钥长度	私钥值	数字信封长度	数字信封

0x01000101	RSA
0x01010101	ECC

其中：

类型 0x93 是发送数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x00 表示管理应用层向管理代理发送数据；

方案编号标识解密的两种非对称算法；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、私钥长度、私钥值、数字信封长度和数字信封内容；

密码算法标识遵循 GM/T 0006-2012；

私钥长度指示私钥值的字节数；

私钥值为私钥的标准数据；

数字信封长度指示数字信封内容的字节数；

数字信封内容为数字信封的标准数据。

c) 非对称算法签名，标准数据组合为私钥+明文，对应返回值为数字签名，定义格式如下表 9 所示。

表 9 非对称算法签名，私钥+明文

1字节	32字节	1字节	4字节	4字节	4字节	4字节		4字节	
包类型 0X93	请求设备 ID	数据方向 0X00	方案编号	方案长度	算法标识	私钥长度	私钥值	明文长度	明文

0x01000200	RSA
0x01010200	ECC

其中：

类型 0x93 是发送数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x00 表示管理应用层向管理代理发送数据；

方案编号标识签名的两种非对称算法；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、私钥长度、私钥值、明文长度和明文内容；

密码算法标识遵循 GM/T 0006-2012；

私钥长度指示私钥值的字节数；

私钥值为私钥的标准数据；

明文长度指示明文内容的字节数；

明文内容为明文的标准数据。

d) 非对称算法验签，标准数据组合为公钥+签名值，对应返回值为明文，定义格式如下表 10 所示。

表 10　非对称算法验签，公钥+签名值

1字节	32字节	1字节	4字节	4字节	4字节	4字节		4字节	
包类型 0X93	请求设备 ID	数据方向 0X00	方案编号	方案长度	算法标识	公钥长度	公钥值	签名值长度	签名值

0x01000300	RSA
0x01010300	ECC

其中：

类型 0x93 是发送数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x00 表示管理应用层向管理代理发送数据；

方案编号标识验签的两种非对称算法；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、公钥长度、公钥值、签名值长度和签名值内容；

密码算法标识遵循 GM/T 0006-2012；

公钥长度指示公钥值的字节数；

公钥值为公钥的标准数据；

签名值长度指示签名值内容的字节数；

签名值内容为签名值的标准数据。

e) 密钥交换，标准数据组合为公钥+临时公钥+发起方 ID，对应返回值为公钥+临时公钥+响应 ID，定义格式如下表 11 所示。

表 11　密钥交换，公钥+临时公钥+发起方 ID

1字节	32字节	1字节	4字节	4字节	4字节	4字节		4字节		4字节
包类型0x93	请求设备ID	数据方向0x00	方案编号	方案长度	算法标识	公钥长度	公钥值	临时公钥长度	临时公钥	发起方ID

0x01000400	RSA
0x01010400	ECC

其中：

类型 0x93 是发送数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x00 表示管理应用层向管理代理发送数据；

方案编号标识两种非对称算法；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、公钥长度、公钥值、临时公钥长度、临时公钥值、发起方 ID；

密码算法标识遵循 GM/T 0006-2012；

公钥长度指示公钥值的字节数；

公钥值为公钥的标准数据；

临时公钥长度指示公钥值的字节数；

临时公钥值为公钥的标准数据；

发起方 ID 是发起设备注册时从设备管理平台层获得的设备唯一性标识；

6.2.3.1.3　杂凑算法

对应返回值为杂凑值，定义格式如下表 12 所示。

表 12　杂凑算法

1字节	32字节	1字节	4字节	4字节	4字节	4字节	
包类型0x93	请求设备ID	数据方向0x00	方案编号	方案长度	算法标识	明文长度	明文

0x02000001	大于等于分组杂凑算法
0x02000002	小于分组杂凑算法

其中：

类型 0x93 是发送数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x00 表示管理应用层向管理代理发送数据；

方案编号标识大于等于分组长度和小于分组长度的杂凑算法；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、明文长度和明文内容；

密码算法标识遵循 GM/T 0006-2012；

明文长度指示明文内容的字节数；

明文内容为明文的标准数据。

6.2.3.2 校验数据消息格式

校验数据消息格式定义了管理代理对管理应用层下发的密码设备算法有效性校验指令进行应答的消息格式，使用 0x94 进行组包，定义如下表 13 所示。

表 13 校验数据消息

1字节	32字节	1字节	1字节	4字节	4字节	
包类型0x94	请求设备ID	数据方向0x01	校验结果	方案编号	方案长度	方案内容

其中：

类型 0x94 是响应数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x01 表示管理代理向管理应用层发送数据；

校验结果中，0x00 表示校验成功，0x01 表示校验失败；

方案编号由算法类别、工作模式、密码技术、标准数据组合等组成，具体定义按 6.3.3.1 规定；

方案长度指示后面方案内容的字节数；

方案内容由下面表 14、表 15、……、表 22 定义。

6.2.3.2.1 校验成功

运算成功，返回校验成功的消息。

本章节根据返回值定义消息格式，返回值含义相同的定义为一种消息格式。

6.2.3.2.1.1 对称算法

a) 对称算法加密明文，标准数据组合为明文，返回值为密文+密钥的消息格式定义如下表 14 所示。

表 14 返回值为密文+密钥的对称算法

1字节	32字节	1字节	1字节	4字节	4字节	4字节	4字节		4字节	
包类型0x94	请求设备ID	数据方向0x01	校验成功0x00	方案编号	方案长度	算法标识	密钥长度	密钥值	密文长度	密文值

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

其中：

类型 0x94 是返回数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x01 表示管理代理向管理应用层发送数据；

校验结果 0x00 表示校验成功；

方案编号标识对称算法加密的四种工作模式；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、密钥长度、密钥值、密文长度和密文内容；

密码算法标识遵循 GM/T 0006-2012；

密钥长度指示密钥值的字节数；

密钥值为用于加密明文的密钥；

密文长度指示密文内容的字节数；

密文内容为加密明文的结果。

b) 对称算法加密明文，标准数据组合为明文+密钥，返回值为密文的消息格式定义如下表 15 所示。

表 15　返回值为密文的对称算法

1字节	32字节	1字节	1字节	4字节	4字节	4字节	4字节	
包类型 0x94	请求设备ID	数据方向 0x01	校验成功0x00	方案编号	方案长度	算法标识	密文长度	密文值

0x00000001	ECB
0x00010001	CBC
0x00020001	CFB
0x00030001	OFB

其中：

类型 0x94 是返回数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x01 表示管理代理向管理应用层发送数据；

校验结果 0x00 表示校验成功；

方案编号标识对称算法加密的四种工作模式；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、密文长度和密文内容；

密码算法标识遵循 GM/T 0006-2012；

密文长度指示密文内容的字节数；

密文内容为加密明文的结果。

c) 对称算法解密密文，标准数据组合为密文+密钥，返回值为明文的消息格式定义如下表 16 所示。

表 16　返回值为明文的对称算法

1字节	32字节	1字节	1字节	4字节	4字节	4字节	4字节	
包类型 0X94	请求设备 ID	数据方向 0X01	校验结果 0X00	方案编号	方案长度	算法 标识	明文 长度	明文值

0x00000100	ECB
0x00010100	CBC
0x00020100	CFB
0x00030100	OFB

其中：

类型 0x94 是返回数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x01 表示管理代理向管理应用层发送数据；

校验结果 0x00 表示校验成功；

方案编号标识对称算法解密的四种工作模式；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、明文长度和明文内容；

密码算法标识遵循 GM/T 0006-2012；

明文长度指示明文内容的字节数；

明文内容为解密密文的结果。

6.2.3.2.1.2 非对称算法

a) 非对称算法加密明文，标准数据组合为公钥+明文，返回值为数字信封的消息格式定义如下表 17 所示。

表 17　返回值为数字信封的非对称算法

1字节	32字节	1字节	1字节	4字节	4字节	4字节	4字节	
包类型 0x94	请求设备ID	数据方向0x01	校验结果0x00	方案编号	方案长度	算法标识	数字信封长度	数字信封

0x01000000	RSA
0x01010000	ECC

其中：

类型 0x94 是返回数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x01 表示管理代理向管理应用层发送数据；

校验结果 0x00 表示校验成功；

方案编号标识产生数字信封的两种非对称算法；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、数字信封长度、数字信封内容；

密码算法标识遵循 GM/T 0006-2012；

数字信封长度指示数字信封的字节数；

数字信封内容为用公钥加密明文的结果。

b) 非对称算法解密密文，标准数据组合为私钥+数字信封，返回值为明文的消息格式定义如下表 18 所示。

表 18　返回值为明文的非对称算法

1字节	32字节	1字节	1字节	4字节	4字节	4字节	4字节	
包类型 0x94	请求设备ID	数据方向0x01	校验结果0x00	方案编号	方案长度	算法标识	明文长度	明文

0x01000101	RSA
0x01010101	ECC

其中：

类型 0x94 是返回数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x01 表示管理代理向管理应用层发送数据；

校验结果 0x00 表示校验成功；

方案编号标识两种非对称算法解密数字信封；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、明文长度和明文内容；

密码算法标识遵循 GM/T 0006-2012；

明文长度指示明文内容的字节数；

明文内容为用私钥解密数字信封的结果。

c) 非对称算法加密明文，标准数据组合为私钥+明文，返回值为签名值的消息格式定义如下表 19 所示。

表 19　返回值为签名值的非对称算法

1字节	32字节	1字节	1字节	4字节	4字节	4字节	4字节	
包类型 0x94	请求设备ID	数据方向0x01	校验结果0x00	方案编号	方案长度	算法标识	签名值长度	签名值

0x01000200	RSA
0x01010200	ECC

其中：

类型 0x94 是返回数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x01 表示管理代理向管理应用层发送数据；

校验结果 0x00 表示校验成功；

方案编号标识两种非对称算法签名；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、签名值长度和签名内容；

密码算法标识遵循 GM/T 0006-2012；

签名值长度指示签名值内容的字节数；

签名值内容为用私钥加密明文后的签名结果。

d) 非对称算法验签，标准数据组合为公钥+签名值，返回值为验签明文的消息格式定义如下表 20 所示。

表 20　返回值为明文的非对称算法

1字节	32字节	1字节	1字节	4字节	4字节	4字节	4字节	
包类型0x94	请求设备ID	数据方向0x01	校验结果0x00	方案编号	方案长度	算法标识	明文长度	明文

0x01000300	RSA
0x01010300	ECC

其中：

类型 0x94 是返回数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x01 表示管理代理向管理应用层发送数据；

校验结果 0x00 表示校验成功；

方案编号标识两种非对称算法验签；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、明文长度和明文内容；

密码算法标识遵循 GM/T 0006-2012；

明文长度指示明文内容的字节数；

明文内容为用公钥解密签名的内容。

e) 密钥交换，标准数据组合为公钥+临时公钥+发起方 ID，返回值为公钥+临时公钥+响应方 ID 的消息格式定义，如下表 21 所示。

表 21　返回值为公钥+临时公钥+响应方 ID

1字节	32字节	1字节	1字节	4字节	4字节	4字节	4字节		4字节		4字节
包类型0x94	请求设备ID	数据方向0x01	校验结果0x00	方案编号	方案长度	算法标识	公钥长度	公钥值	临时公钥长度	临时公钥	响应方ID

0x01000400	RSA
0x01010400	ECC

其中：

类型 0x94 是返回数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x01 表示管理代理向管理应用层发送数据；

校验结果 0x00 表示校验成功；

方案编号标识两种非对称算法；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、公钥长度、公钥值、临时公钥长度、临时公钥值、响应方 ID；

密码算法标识遵循 GM/T 0006-2012；

公钥长度指示公钥值的字节数；

公钥值为公钥的标准数据；

临时公钥长度指示公钥值的字节数；

临时公钥值为公钥的标准数据；

响应方 ID 是响应设备注册时从设备管理平台层获得的设备唯一性标识；

6.2.3.2.1.3 杂凑算法

杂凑算法的消息格式定义，如下表 22 所示。

表 22 返回杂凑值的消息格式

1字节	32字节	1字节	1字节	4字节	4字节	4字节	4字节	
包类型0x94	请求设备ID	数据方向0x01	校验结果0x00	方案编号	方案长度	算法标识	杂凑值长度	杂凑值

0x02000001	大于等于分组杂凑算法
0x02000002	小于分组杂凑算法

其中：

类型 0x94 是返回数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x01 表示管理代理向管理应用层发送数据；

校验结果 0x00 表示校验成功；

方案编号标识大于等于分组长度和小于分组长度的杂凑算法；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、杂凑值长度和杂凑内容；

密码算法标识遵循 GM/T 0006-2012；

杂凑值长度指示杂凑值的字节数；

杂凑值是用杂凑算法的计算结果。

6.2.3.2.2 校验失败

算法有效性验证失败，返回失败结果，并列出失败原因，如下表 23 所示。

表 23　算法有效性验证失败

1字节	32字节	1字节	1字节	4字节	4字节	4字节	4字节	
包类型 0x94	请求设备ID	数据方向 0x01	校验失败 0x01	方案编号	方案长度	算法标识	返回错误信息长度	错误信息(UTF-字符串)

错误信息的原因	
0x01000000 + 0x00000001	未知错误
0x01000000 + 0x00000003	与设备通信失败
0x01000000 + 0x00000008	不存在的密钥调用
0x01000000 + 0x00000009	不支持的算法调用
0x01000000 + 0x0000000A	不支持的算法模式调用
0x01000000 + 0x0000000B	公钥运算失败
0x01000000 + 0x0000000C	私钥运算失败
0x01000000 + 0x0000000D	签名运算失败
0x01000000 + 0x0000000E	验证签名运算失败
0x01000000 + 0x0000000F	对称算法运算失败
0x01000000 + 0x00000014	密钥类型错误
0x01000000 + 0x00000015	密钥错误

其中：

类型 0x94 是返回数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x01 表示管理代理向管理应用层发送数据；

校验结果 0x01 表示校验失败；

方案编号参见本规范 6.2.3.1 定义；

方案长度指示后面方案内容的字节数，方案内容包括算法标识、错误信息长度和错误信息内容；

密码算法标识遵循 GM/T 0006-2012；

错误信息长度指示错误信息的字节数；

错误信息内容见表 26。

6.2.4　设备自检

密码设备自检是指管理应用层向密码设备管理代理下发状态查询指令，让设备自己去检查密码算法实现的正确性、密钥的完整性以及主要功能是不是正常。

设备自检的消息格式如下表 24 所示。

表 24　设备自检消息

1字节	32字节	1字节	4字节	4字节
类型 0x93	请求设备ID	数据方向0x00	方案编号	方案内容

1字节	1字节	1字节	1字节
密码算法正确性 (0x00：检查； 0x01：不检查)	随机数 (0x00：检查； 0x01：不检查)	密钥完整性 (0x00：检查； 0x01：不检查)	密码服务功能正确性 (0x00：:检查； 0x01：不检查)

其中：

类型 0x93 是发送数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向标识的 0x00 表示管理应用层向管理代理发送数据；

方案编号 0x03000000 标识设备自检消息。

设备自检返回运算成功的消息格式如下表 25 所示。

表 25　返回运算成功结果消息

1字节	32字节	1字节	1字节	4字节	4字节
类型 0x94	请求设备ID	数据方向 0x01	自检结果 0x00	0x03000000	方案内容

1字节	1字节	1字节	1字节
密码算法正确性 (0x00：正确； 0x01：错误)	随机数 (0x00：正确； 0x01：错误)	密钥完整性 (0x00：正常； 0x01：异常)	密码服务功能 (0x00：正常； 0x01：异常)

其中：

类型 0x94 是返回数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x01 表示管理代理向管理应用层发送数据；

自检结果 0x00 表示自检成功；

方案编号 0x03000000 标识设备自检消息。

设备自检验证失败，返回失败结果，并列出失败原因，消息格式定义如下表 26 所示

表 26　返回自检验证失败结果消息

1字节	32字节	1字节	1字节	4字节	4字节	
类型 0x94	请求设备ID	数据方向 0x01	自检结果0x01	0x03000000	返回错误信息长度	错误信息(UTF-字符串)

0x01000000 + 0x00000001	未知错误
0x01000000 + 0x00000016	状态值获取不到

其中：

类型 0x94 是返回数据的标识；

请求设备 ID 是请求设备注册时从设备管理平台层获得的设备唯一性标识；

数据方向 0x01 表示管理代理向管理应用层发送数据；

自检结果 0x01 表示自检失败；

方案编号 0x03000000 标识设备自检消息；

错误消息长度指示后面错误消息的字节数。