



中华人民共和国密码行业标准

GM/T 0053—2016

密码设备管理 远程监控与合规性检验接口数据规范

Cryptographic equipment management—
Data interface specification of remote monitoring and compliance testing

2016-12-23 发布

2016-12-23 实施

国家密码管理局 发布



目 次

前言	I
引言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 密码设备管理应用体系	2
5.1 体系结构	2
5.2 对密码设备的基本要求	3
5.3 对管理代理的基本要求	3
5.4 对安全通信的基本要求	3
6 密码设备远程监控与合规性检验的接口数据	4
6.1 密码设备远程监控	4
6.1.1 远程监控消息格式	4
6.1.2 请求监控信息的消息格式	4
6.1.3 返回监控信息的消息格式	4
6.2 设备合规性检验	6
6.2.1 设备合规性检验概述	6
6.2.2 设备合规性检验消息格式	6
6.2.3 算法有效性校验	6
6.2.4 设备自检	17

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

GM/T 0053《密码设备管理 远程监控与合规性检验接口数据规范》是密码设备管理类规范之一。该类规范由一个基础规范和系列管理应用规范组成,目前包括:

- 基础规范:GM/T 0050《密码设备管理 设备管理技术规范》
- 管理应用规范:GM/T 0051《密码设备管理 对称密钥管理规范》
- 管理应用规范:GM/T 0052《密码设备管理 VPN 设备监察管理规范》
- 管理应用规范:GM/T 0053《密码设备管理 远程监控与合规性检验接口数据规范》

本标准凡涉及密码算法相关内容,按国家有关法规实施。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位:上海信息安全工程技术研究中心、上海信昊信息科技有限公司、卫士通信息产业股份有限公司、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、李高健、田立、黄志荣、廖烨、邹钊、潘淑媛、药乐、吕明忠、王贺刚、王善义、张元臣、周志洪、李俊山、潘利民。

引 言

本标准依据 GM/T 0050《密码设备管理 设备管理技术规范》中密码设备管理平台架构,提出针对密码设备远程监控、设备合规性检验等管理应用的接口数据规范,定义了管理应用与密码设备间的消息传递格式。本标准采用的安全通道,依据 GM/T 0050 中的管理应用接口建立,相关内容请参考GM/T 0050。

密码设备管理 远程监控与合规性检验接口数据规范

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接口数据,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 0050—2016 密码设备管理 设备管理技术规范

3 术语和定义

GM/T 0050—2016 界定的以及下列术语和定义适用于本文件。

3.1

密码设备 cryptography device

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 0050—2016,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 0050—2016,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 0050—2016,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 0050—2016,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 0050—2016,定义 3.6。

3.6

密码设备管理平台 cryptography device management platform

为管理应用提供与被管对象建立远程安全通道的管理系统。

[GM/T 0050—2016,定义 3.9]

3.7

密钥失步 key desynchronization

进行加密通信的双方由于通信报文不完整、密钥不一致造成通信报文无法正确加解密的情况为密钥失步。一般需要密码设备从密钥管理中心获取密钥或互相通信的双方重新协商密钥。

3.8

隧道连通性 tunnel connectivity

密码设备与需要互连的其他设备之间的通信和连接。

4 缩略语

下列缩略语适用于本文件。

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 0050—2016 的 5.3,结构图如图 1 所示(图中实线表示物理连接,虚线表示逻辑连接)。管理体系按照功能划分为三层,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 0050—2016 的 5.4、5.5 和 5.6。

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。

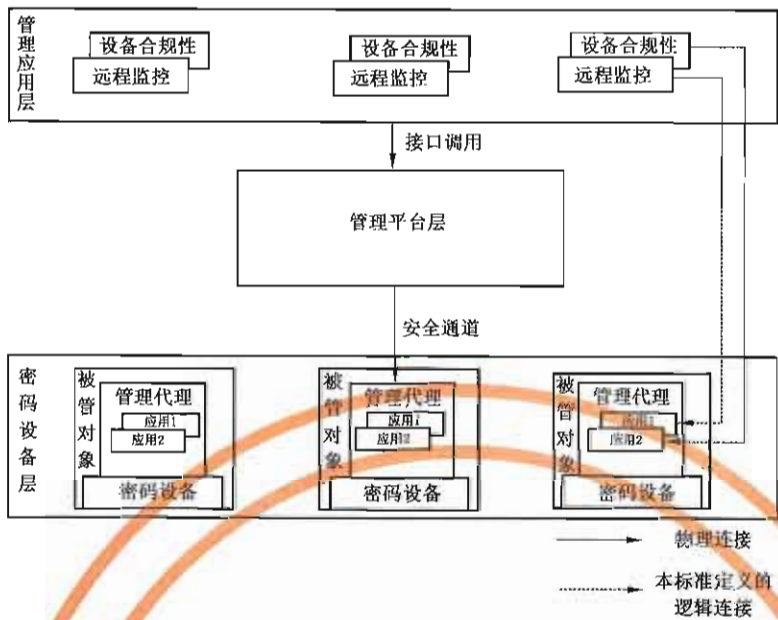


图 1 密码设备管理应用体系结构图

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,其应用接口遵循本标准。

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 0050—2016 的 5.6。

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



图 2 管理代理示意图

5.4 对安全通道的基本要求

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 0050—2016 的 6.2 定义,安全通道的使用说明遵循 GM/T 0050—

2016 的 6.3、6.4。

6 密码设备远程监控与合规性检验的接口数据

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,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 0050—2016 的 9.4.1 中 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,具体消息格式如图 3 所示(参见 GM/T 0050—2016 的 6.2):

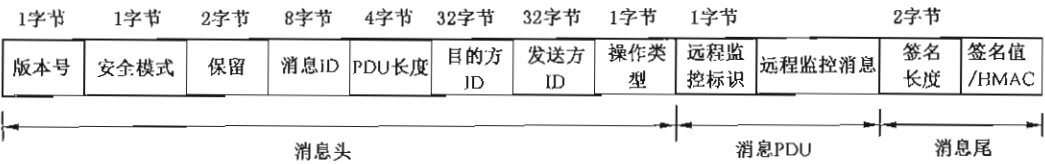


图 3 设备远程监控消息格式定义

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 0050--2016 的 7.2。

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表 2 所示,参见 GM/T 0050—2016 中 7.3 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 取得口 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 0050—2016 中 8.6 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

设备合规性检验包括密码设备的算法有效性校验和设备自检。

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,并按照密码算法(算法标识遵循 GM/T 0006—2012)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 0050—2016 中 9.4.1 的 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,具体消息格式如图 4 所示(参见 GM/T 0050—2016 的 6.2):



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

6.2.3.1.1 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: SM2	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;
- 方案编号是依据算法类别、工作模式、密码技术和标准数据组合等内容确定的数据格式;
- 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 12 定义。

6.2.3.1.2 对称算法

a) 对称算法加密明文,标准数据组合为明文,对应返回值为密文和密钥,定义格式如表 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和密钥,对应返回值为密文,定义格式如表 5 所示。

表 5 对称算法加密,明文和密钥

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和密钥,对应返回值为明文,定义格式如表 6 所示。

表 6 对称算法解密,密文和密钥

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
			0x00000102	ECB					
			0x00010102	CBC					
			0x00020102	CFB					
			0x00030102	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。

6.2.3.1.3 非对称算法

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

表 7 非对称算法加密,公钥和明文

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	SM2					

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和数字信封,对应返回值为明文,定义格式如表 8 所示。

表 8 非对称算法解密,私钥和数字信封

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	SM2					

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和明文,对应返回值为数字签名,定义格式如表 9 所示。

表 9 非对称算法签名,私钥和明文

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	SM2					

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和签名值,对应返回值为明文,定义格式如表 10 所示。

表 10 非对称算法验签,公钥和签名值

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	SM2					

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、临时公钥和发起方 ID,对应返回值为公钥、临时公钥和响应 ID,定义格式如表 11 所示。

表 11 密钥交换,公钥、临时公钥和发起方 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	SM2

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。

6.2.3.1.4 杂凑算法

对应返回值为杂凑值,定义格式如表 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

6.2.3.2.1 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 6.2.3.1.1 规定;
- 方案长度指示后面方案内容的字节数;
- 方案内容由表 14~表 22 定义。

6.2.3.2.2 校验成功

6.2.3.2.2.1 返回消息

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。

6.2.3.2.2.2 对称算法

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

表 14 返回值为密文和密钥的对称算法

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和密钥，返回值为密文的消息格式定义如表 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和密钥，返回值为明文的消息格式定义如表 16 所示。

表 16 返回值为明文对称算法

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。

6.2.3.2.2.3 非对称算法

- a) 非对称算法加密明文，标准数据组合为公钥和明文，返回值为数字信封的消息格式定义如表 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	请求设备ID	数据方向	校验结果	方案编号	方案长度	算法标识	数字信封长度	数字信封
0x94		0x01	0x00					
				0x01000000	RSA			
				0x01010000	SM2			

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和数字信封，返回值为明文的消息格式定义如表 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	请求设备ID	数据方向	校验结果	方案编号	方案长度	算法标识	明文长度	明文
0x94		0x01	0x00					
				0x01000101	RSA			
				0x01010101	SM2			

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) 非对称算法签名明文，标准数据组合为私钥和明文，返回值为签名值的消息格式定义如表 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	请求设备ID	数据方向	校验结果	方案编号	方案长度	算法标识	签名值长度	签名值
0x94		0x01	0x00					

0x01000200	RSA
0x01010200	SM2

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和签名值，返回值为验签明文的格式定义如表 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	请求设备ID	数据方向	校验结果	方案编号	方案长度	算法标识	明文长度	明文
0x94		0x01	0x00					

0x01000300	RSA
0x01010300	SM2

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、临时公钥和发起方 ID,返回值为公钥、临时公钥和响应方 ID 的消息格式定义,如表 21 所示。

表 21 返回值为公钥、临时公钥和响应方 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	请求设备ID	数据方向	校验结果	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	相应方ID
0x94		0x01	0x00								

0x01000400	RSA
0x01010400	SM2

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。

6.2.3.2.2.4 杂凑算法

杂凑算法的消息格式定义,如表 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。

6.2.3.2.3 校验失败

算法有效性验证失败,返回失败结果,并列出生失败原因,如表 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)
								<div><div>错误信息的原因</div><div>0x01000000+0x00000001 未知错误</div><div>0x01000000+0x00000003 与设备通信失败</div><div>0x01000000+0x00000008 不存在的密钥调用</div><div>0x01000000+0x00000009 不支持的算法调用</div><div>0x01000000+0x0000000A 不支持的算法模式调用</div><div>0x01000000+0x0000000B 公钥运算失败</div><div>0x01000000+0x0000000C 私钥运算失败</div><div>0x01000000+0x0000000D 签名运算失败</div><div>0x01000000+0x0000000E 验证签名运算失败</div><div>0x01000000+0x0000000F 对称算法运算失败</div><div>0x01000000+0x00000014 密钥类型错误</div><div>0x01000000+0x00000015 密钥错误</div></div>

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;
- 方案编号见 6.2.3.1.1;
- 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。

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。
-

中华人民共和国密码
行业标准
密码设备管理
远程监控与合规性检验接口数据规范
GM/T 0053- 2016

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址 www.spc.net.cn

总编室:(010)68533533 发行中心:(010)51780238

读者服务部:(010)68523946

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

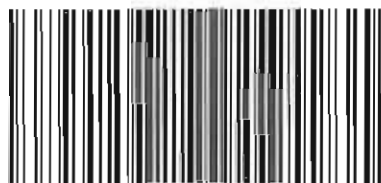
*

开本 880×1230 1/16 印张 1.5 字数 42 千字
2017年5月第一版 2017年5月第一次印刷

*

书号: 155066·2-31470 定价 27.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68510107



GM/T 0053-2016



中华人民共和国密码行业标准

GM/T 0046—2016

金融数据密码机检测规范

Test specification for financial cryptographic server

2016-12-23 发布

2016-12-23 实施



国家密码管理局 发布

中华人民共和国密码
行业标准
金融数据密码机检测规范
GM/T 0046—2016

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址 www.spc.net.cn

总编室:(010)68533533 发行中心:(010)51780238

读者服务部:(010)68523946

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 1.5 字数 40 千字
2017年5月第一版 2017年5月第一次印刷

*

书号: 155066·2-31452 定价 30.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68510107

目 次

前言	Ⅲ
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	3
5 检测环境要求	4
6 检测内容及检测方法	4
6.1 检测项目	4
6.2 外观和结构的检查	5
6.3 功能检测	5
6.3.1 初始化检测	5
6.3.2 密码运算检测	5
6.3.3 密钥管理检测	6
6.3.4 随机数检测	7
6.3.5 访问控制检测	7
6.3.6 设备管理检测	7
6.3.7 日志审计检测	7
6.3.8 设备自检检测	8
6.3.9 数据报文接口检测	8
6.4 性能检测	8
6.4.1 性能指标计算方法	8
6.4.2 PIN 加密性能测试	9
6.4.3 PIN 转加密性能测试	9
6.4.4 MAC 计算性能测试	9
6.4.5 ARQC 验证性能测试	9
6.4.6 对称密码算法的加解密性能测试	9
6.4.7 非对称密码算法的加解密性能测试	9
6.4.8 数据杂凑算法性能测试	10
6.4.9 随机数发生器性能测试	10
6.4.10 非对称密钥生成性能测试	10
6.4.11 非对称算法签名、验签性能测试	10
6.5 其他检测	10
6.5.1 设备安全性测试	10
6.5.2 环境适应性检测	10
6.5.3 可靠性检测	10
7 送检技术文档要求	10

8 合格判定条件·····	11
附录 A (规范性附录) 测试项目列表·····	12
参考文献·····	18

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：无锡江南信息安全工程技术中心、国家密码管理局商用密码检测中心、卫士通信产业股份有限公司、兴唐通信科技股份有限公司、山东得安信息技术有限公司。

本标准主要起草人：张所成、齐传兵、李大为、邓开勇、罗鹏、李国友、刘常、肖秋林、丁余泉、刘先祥、李元正、王妮娜、孔凡玉。



金融数据密码机检测规范

1 范围

本标准规定了金融数据密码机的检测要求和检测方法。

本标准适用于金融数据密码机的检测,以及该类密码设备的研制。

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。

GB/T 32915 信息安全技术 二元序列随机性检测方法

GM/T 0028 密码模块安全要求

GM/T 0039 密码模块安全检测要求

GM/T 0045—2016 金融数据密码机技术规范

GM/T 0050 密码设备管理 设备管理技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

金融数据密码机 financial cryptographic server

用于金融领域,保护金融数据安全,主要实现 PIN 加密、PIN 转加密、MAC 产生和校验、数据加解密、签名验证以及密钥管理等密码服务功能的密码设备。

3.2

对称密码算法 symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。

3.3

非对称密码算法/公钥密码算法 asymmetric cryptographic algorithm/public key cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥(公钥)可以公开,另一个密钥(私钥)必须保密,且由公钥求解私钥是计算不可行的。

3.4

密码杂凑算法 HASH algorithm

又称杂凑算法、密码散列算法或哈希算法。该算法将一个任意长的比特串映射到一个固定长的比特串,且满足下列三个特性:

- 为一个给定的输出找出能映射到该输出的一个输入是计算上困难的;
- 为一个给定的输入找出能映射到同一个输出的另一个输入是计算上困难的;
- 要发现不同的输入映射到同一输出是计算上困难的。

3.5

加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。

3.6

解密 decipherment/decryption

加密过程对应的逆过程。

3.7

电码本工作模式 electronic codebook operation mode

ECB

分组密码算法的一种工作模式,其特征是将明文分组直接作为算法的输入,对应的输出作为密文分组。

3.8

密文分组链接工作模式 cipher block chaining operation mode

CBC

分组密码算法的一种工作模式,其特征是将当前的明文分组与前一密文分组进行异或运算后再进行加密得到当前的密文分组。

3.9

SM2 算法 SM2 algorithm

一种椭圆曲线公钥密码算法,其密钥长度为 256 比特。

3.10

SM3 算法 SM3 algorithm

一种密码杂凑算法,其输出为 256 比特。

3.11

SM4 算法 SM4 algorithm

一种分组密码算法,分组长度为 128 比特,密钥长度为 128 比特。

3.12

物理安全环境 physical secure environment

PSE

具有访问控制机制或其他安全机制的环境,设计上防止密钥部分或全部泄露、或环境中存储的其他秘密数据泄露等任何非授权访问。例如,具有不间断的访问控制、物理安全保护和监控的房间或安全实体。

3.13

物理防护 physical protection

PP

用物理手段保护硬件密码设备及其密钥或敏感信息,例如:采用防撬手段防止密码机被非法开箱。

3.14

主密钥 master key

MK

在密钥加密密钥和传输密钥的层次关系中,最高级的密钥加密密钥称为主密钥。也可称为主文件密钥(master file key)或本地主密钥(local master key)。

3.15

密钥分隔 key separation

KS

保证每个密码操作只采用指定的密钥类型,例如,MAC 密钥只能用于产生消息认证码。

3.16

数据密钥 data key

DK

指保护 PIN 和计算 MAC 的密钥,包括 MAC 密钥(MAK)和 PIN 密钥(PIK),也称为工作密钥。

3.17

校验值 check value

CV

通过不可逆转算法计算的结果值,校验值通常在密钥下采用密码变换一个任意串的结果。在未知密钥的情况下,计算正确的校验值是不可行的,不能通过校验值来测定一个密钥。

3.18

个人识别码 personal identification number

PIN

在金融业务中,授权请求消息中认证持卡人的一种数字身份标识码,PIN 只包含十进制数字。

3.19

密钥装载 key loading

KL

人工或电子手段传送密钥到金融数据密码机中的过程。

3.20

人工密钥分发 manual key distribution

MKD

密钥通常以明文形态(采用物理保护措施),用密码信封等非电子手段分发的一种密钥分发方式。

3.21

人工密钥注入 manual key entry

MKE

用键盘等注入密钥到金融数据密码机。

4 缩略语

下列缩略语适用于本文件:

API	Application Program Interface	应用程序接口简称应用接口
ARQC	Authorization Request Cryptogram	授权请求密文
CBC	Cipher Block Chaining	(分组密码的)密码分组链接(工作方式)
CMAC	Cipher-Based Message Authentication Code	基于加密算法的消息认证码
DK	Data Key	数据密钥
ECB	Electronic Codebook	(分组密码的)电子密本(工作方式)
HASH	HASH Algorithm	散列函数运算,又称杂凑运算
LMK	Local Master Key	本地主密钥
MAC	Message Authentication Code	消息认证码
MAK	MAC Key	计算 MAC 的密钥,属于数据密钥

MK	Master Key	主密钥
PAN	Primary Account Number	主账号
PIK	PIN Key	PIN 加密密钥,属于数据密钥
PIN	Personal Identification Number	个人识别码
TAK	Terminal MAC Key	终端 MAC 计算密钥
TEK	Terminal Encryption Key	终端加密密钥
TMK	Terminal Master Key	终端主密钥
TPK	Terminal PIN Key	终端 PIN 加密密钥
ZAK	Zone MAC Key	区域 MAC 计算密钥
ZEK	Zone Encryption Key	区域加密密钥
ZMK	Zone Master Key	区域主密钥
ZPK	Zone PIN Key	区域 PIN 加密密钥

5 检测环境要求

金融数据密码机检测环境用于测试金融数据密码机的功能、性能。检测环境拓扑可参考图 1。

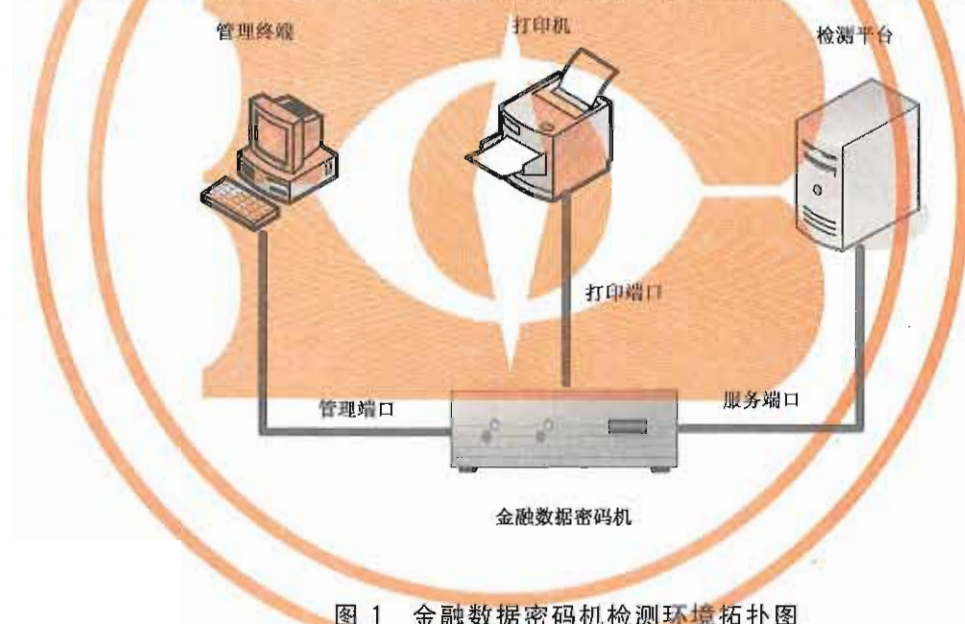


图 1 金融数据密码机检测环境拓扑图

检测环境主要由金融数据密码机、管理终端、打印机、检测平台以及相关通信链路组成。管理终端用于对金融数据密码机进行初始化检测、密钥管理检测、访问控制检测、日志审计检测、设备自检检测；检测平台用于密码运算检测、应用编程接口检测、随机数检测、设备管理检测以及性能检测；打印机用于应用编程接口检测时打印密码信封的功能检测。

6 检测内容及检测方法

6.1 检测项目

检测内容包括外观和结构检查、提交文档的检查、功能检测、性能检测、环境适应性检测和稳定性检测等。具体的检测项目见附录 A。

6.2 外观和结构的检查

根据产品的物理参数,对金融数据密码机的外观、尺寸、内部部件及附件进行检查。

金融数据密码机应具备以下部件或端口:

- a) 要求面板印字清晰,标牌粘贴牢固,整机外壳无明显划痕,附件齐全;
- b) 具备电源指示灯;
- c) 具备状态指示灯;
- d) 具备故障指示灯;
- e) 具备至少 1 个服务端口;
- f) 具备至少 1 个管理端口;
- g) 如果密钥存储采用微电保护存储方式,应具备密钥自毁机制。

金融数据密码机宜具备以下部件或端口:

- a) 宜具备 1 个打印端口;
- b) 如果密钥使用时会以明文方式出现在金融数据密码机内存中,宜具备内存清除机制;
- c) 宜具备机箱外壳接地装置;
- d) 宜具备冗余电源;
- e) 宜具备 IC 卡插座;
- f) 宜具备 USB 端口;
- g) 宜具备人机交互部件。

6.3 功能检测

6.3.1 初始化检测

金融数据密码机应具备初始化功能,实现设备的初始状态到工作状态的转换。

金融数据密码机的初始化操作主要包括系统初始配置、初始化管理员或操作员、初始密钥生成(或恢复)与安装。金融数据密码机只有在初始化操作完成之后才能提供密码服务。经过初始配置的金
融数据密码机,可自动进入工作状态,提供密码服务。

如果没有进行过初始化配置,金融数据密码机启动时应通过指示灯和声音进行报警,提示用户进行初始化,此时金融数据密码机不能提供密码服务。

金融数据密码机初始化应支持:

- a) 未初始化状态指示;
- b) 管理员的生成;
- c) 金融数据密码机服务端口配置,如 IP 地址、掩码的配置及查询;
- d) 金融数据密码机管理端口配置。

6.3.2 密码运算检测

密码运算检测的范围应包括国家密码管理主管部门批准/审批的每个对称密码算法、非对称密码算法和杂凑算法的每个功能函数。

金融数据密码机在进行密码运算功能检测时,需预置测试密钥,测试密钥由检测平台来确定。

密码运算的检测方法是:由检测平台生成测试数据并调用金融数据密码机进行密码运算,然后检测平台调用自身的密码运算模块对运算结果进行验证,如果验证结果正确,则测试通过;否则,测试失败。

金融数据密码机应支持的算法:

- a) SM4 ECB 加密;

- b) SM4 ECB 解密;
- c) SM4 CBC 加密;
- d) SM4 CBC 解密;
- e) SM3 杂凑;
- f) SM2 密钥生成;
- g) SM2 签名;
- h) SM2 验签;
- i) SM2 加密;
- j) SM2 解密;
- k) SM2 密钥协商。

金融数据密码机密码运算检测方法:

- a) SM4 ECB 加密:对给定的密钥和明文经 ECB 模式加密,结果和给定密文完全相同;
- b) SM4 ECB 解密:对给定的密钥和密文经 ECB 模式解密,结果和给定明文完全相同;
- c) SM4 CBC 加密:对给定的 IV、密钥和明文经 CBC 模式加密,结果和给定密文完全相同;
- d) SM4 CBC 解密:对给定的 IV、密钥和密文经 CBC 模式解密,结果和给定明文完全相同;
- e) SM3 杂凑:对给定消息调用 SM3 算法计算杂凑值,结果和给定杂凑值完全相同;
- f) SM2 密钥生成:调用金融数据密码机生成一个 SM2 密钥对,再用其私钥对指定数据签名;然后由检测平台用其公钥验证签名结果是否正确;
- g) SM2 签名:多次调用金融数据密码机 SM2 签名功能对指定数据签名,由检测平台检查:
 - 1) 签名结果是否正确;
 - 2) 签名结果应每次不同。
- h) SM2 验签:检测平台进行 SM2 签名,调用金融数据密码机的 SM2 验签功能,检查:
 - 1) 正确的签名应验证通过;
 - 2) 错误的签名应验证失败。
- i) SM2 加密:多次调用金融数据密码机 SM2 加密功能对指定数据加密,由检测平台检查:
 - 1) 加密结果是否正确;
 - 2) 加密结果应每次不同。
- j) SM2 解密:检测平台进行 SM2 加密,调用金融数据密码机的 SM2 解密功能,检查解密的结果是否正确;
- k) SM2 密钥协商:调用金融数据密码机 SM2 密钥协商功能,同时检测平台调用自身的 SM2 密钥协商接口,检查协商结果是否一致。

6.3.3 密钥管理检测

金融数据密码机应具备完善的密钥管理功能,密钥管理包括密钥的产生、注入、导入/导出、备份/恢复、查询和销毁,金融数据密码机必须保证密钥在生存周期的各个环节的安全性。

金融数据密码机密钥管理功能的检测由金融数据密码机自身的密钥管理工具实现,管理工具应具备以下功能:

- a) 产生主密钥。管理工具按照指定的参数生成主密钥,并以安全的方法存储到安全介质中;
- b) 导入主密钥。管理工具通过外部安全介质导入主密钥,并显示主密钥检查值;
- c) 查询主密钥。管理工具按照指定的查询参数查询主密钥,显示主密钥检查值;
- d) 销毁密钥。管理工具按照指定的密钥销毁参数销毁密钥,如金融数据密码机提供硬件销毁方式,则通过销毁开关销毁密钥。密钥销毁后通过管理工具查询应显示密钥不存在;
- e) 密钥自毁机制。如果密钥存储采用微电保护存储方式,密码机加电与不加电两种情况下打开

机箱,密钥都必须能被自动销毁。

金融数据密码机应具备以下功能:

- a) 通过密钥管理工具注入成员主密钥,并显示其检查值;
- b) 通过密钥管理工具以安全的方法备份内部存储密钥到安全介质;
- c) 通过密钥管理工具以安全的方法将安全介质中备份的密钥恢复到金融数据密码机,恢复到金融数据密码机的密钥可被管理工具查询状态;
- d) 通过备份介质安全的将密钥同步至另一台相同的设备;
- e) 如果密钥使用时会以明文方式出现在金融数据密码机内存中,加电情况下打开机箱,应能自动清除内存中的密钥。

6.3.4 随机数检测

金融数据密码机应具备真随机数生成功能,真随机数发生器需采用国家密码管理主管部门认可的物理噪声源芯片实现且至少采用两个独立的物理噪声源芯片。密钥的产生和初始 PIN 的产生应使用真随机数。

金融数据密码机应具备随机数采集接口,能够根据随机数检测规范生成符合检测要求的检测样本。

金融数据密码机生成的随机数比特流作为测试样本,输入到随机数检测程序中检测随机数的质量。

随机数的产生和使用应符合 GM/T 0045—2016 的要求,随机数质量检验按照 GB/T 32915 的要求进行检测。

随机数检测内容包括:出厂检测、上电检测和使用检测,其中使用检测包括周期检测和单次检测。检测方法为审查源代码,以确认随机数的生成、自检和使用是否符合标准要求。

6.3.5 访问控制检测

金融数据密码机应提供措施防止非授权打开设备,打开金融数据密码机应有物理上的访问控制措施限制。

采用金融数据密码机配用的管理工具或管理界面进行访问控制检测。

不同的管理操作应设置不同的操作权限,登录金融数据密码机的管理工具应具备完善的身份认证机制;金融数据密码机应拒绝任何非授权的访问或操作。

金融数据密码机访问控制应满足以下要求:

- a) 提供物理防护措施防止非授权打开设备;
- b) 管理权限有明确的角色划分,至少具备管理员、审计员、操作员三类角色;
- c) 管理操作授权有严格的身份认证机制;
- d) 金融数据密码机的关键安全操作应由管理员授权后才能进行。关键安全操作包括:密钥注入、密钥备份/恢复、密钥产生、密钥分散、密钥导入/导出、密钥归档、密钥销毁;
- e) 金融数据密码机服务端口应设计有授权访问机制。

6.3.6 设备管理检测

金融数据密码机设备管理功能的实现应符合 GM/T 0050 的要求。

金融数据密码机应能正确响应密码设备管理中心按照 GM/T 0050 下发的管理指令。

6.3.7 日志审计检测

金融数据密码机应提供日志记录、查看和导出功能。采用金融数据密码机配用的日志管理工具或界面进行日志审计检测。

金融数据密码机的日志内容应包括:

- a) 管理员操作行为,包括登录认证、系统配置、密钥管理等操作;
- b) 异常事件,包括自检失败、认证失败、非法访问等异常事件的记录。

金融数据密码机的日志内容宜包括:

- a) 开机启动事件记录,包括开机时间、开机时的系统状态等;
- b) 密码服务程序重启记录,记录由于程序 BUG 或者内存溢出等原因,导致密码服务程序重启的事件,包括重启的时间、系统状态等;
- c) 其他异常事件,如端口连接异常、系统资源不足等。

6.3.8 设备自检检测

金融数据密码机的设备自检功能主要包括密码算法正确性检测、随机数发生器产生的随机数质量检测、存储密钥和数据的完整性检测,以及关键部件的正确性检测等。

金融数据密码机应支持上电/复位自检、手工自检和周期性自检功能。

上电/复位自检在每次加电/复位启动后自动执行。自检成功,金融数据密码机自动进入管理状态或工作状态。自检失败,金融数据密码机应报告检测结果并且停止对外提供密码服务。

手工自检在金融数据密码机启动后通过管理界面执行,自检结束后应报告检测结果。

周期性自检在金融数据密码机运行过程中,按设定的周期自动执行。如果自检失败,金融数据密码机应报告检测结果并且停止对外提供密码服务。

6.3.9 数据报文接口检测

检测平台按照 GM/T 0045—2016 规定的应用编程接口逐条进行测试。只有所有接口测试正确,才认为检测通过。

- a) 正确的调用环境和调用过程,API 函数应该返回正确的结果,并完成相应功能;
- b) 不正确的调用环境和调用过程,API 函数应返回相应的错误代码。

6.4 性能检测

6.4.1 性能指标计算方法

性能检测的目的是测试各项密码运算的速度指标。

性能检测的内容包括:对称密码算法性能、非对称密码算法性能、杂凑算法性能、常用计算方法性能(PIN、MAC)。

下列各项速度性能测试中的测试量由数据报文长度和测试次数决定。可以根据各个测试项的具体耗时情况,依照等比序列来选取测试次数,例如:测试次数 N 可以选择 1 次、10 次、100 次、1 000 次等,分别测试后得到不同测试次数时的性能序列。数据报文长度的选择在各个速度性能测试项中分别定义。

在 6.4.6、6.4.8 和 6.4.9 中包含的各个测试项的速度性能的计算式(1)所示:

$$S = 8LN / (1\ 024 \times 1\ 024T) \quad \dots\dots\dots (1)$$

式中:

S ——各个测试项的速度,单位为兆比特/秒(Mbit/s);

L ——数据报文的长度,单位为字节(byte);

N ——测试次数;

T ——测量所耗费的时间,单位为秒(s)。

在 6.4.2、6.4.3、6.4.4、6.4.5、6.4.7、6.4.10 和 6.4.11 中包含的各个测试项的速度性能的计算如式(2)所示:

$$S = N/T \quad \dots\dots\dots (2)$$

式中:

S ——各个测试项的速度,单位为次(对)/秒(tps);

N ——测试次数;

T ——测量所耗费的时间,单位为秒(s)。

测试次数 N 根据测试项目的不同,设定不同的数值。要求测试次数 N 不能太小,以保证测试结果的精确度;同时 N 也不要太大,以免测试时间过长。

6.4.2 PIN 加密性能测试

将一个 PIN 进行加密操作,重复操作 N 次,测量其完成时间 T 。用于测试的数据由检测机构选取。测试应进行多次,结果取平均值。PIN 加密性能单位统一为 tps(次/秒)。

金融数据密码机应支持:SM4 PIN 加密。

6.4.3 PIN 转加密性能测试

将一个由 LMK 保护的 PIN 块转加密为 ZPK 保护的 PIN 块,重复操作 N 次,测量其完成时间 T 。用于测试的数据由检测机构选取。测试应进行多次,结果取平均值。PIN 转加密性能单位统一为 tps(次/秒)。

金融数据密码机应支持:SM4 PIN 转加密。

6.4.4 MAC 计算性能测试

计算一个随机的 256 字节数据的 MAC 值,重复操作 N 次,测量其完成时间 T 。用于测试的数据由检测机构选取。测试应进行多次,结果取平均值。MAC 计算性能单位统一为 tps(次/秒)。

金融数据密码机应支持:SM4 MAC 计算。

6.4.5 ARQC 验证性能测试

验证一个 ARQC 值,重复操作 N 次,测量其完成时间 T 。用于测试的数据由检测机构选取。测试应进行多次,结果取平均值。ARQC 验证性能单位统一为 tps(次/秒)。

金融数据密码机应支持:SM4 ARQC 验证。

6.4.6 对称密码算法的加解密性能测试

将一个定长数据报文进行加/解密操作,重复操作 N 次,测量其完成时间 T 。用于测试的数据由检测机构选取,测试应进行多次,结果取平均值。对称密码算法的加解密性能单位统一为 Mbps(兆比特/秒)。

金融数据密码机应支持:

- a) SM4 ECB 加密;
- b) SM4 ECB 解密;
- c) SM4 CBC 加密;
- d) SM4 CBC 解密。

6.4.7 非对称密码算法的加解密性能测试

将一个定长数据报文进行加/解密操作,重复操作 N 次,测量其完成时间 T 。用于测试的数据由检测机构选取。测试应进行多次,结果取平均值。支持多种非对称算法,必须测试所支持的所有非对称密码算法及其各种应用模式。非对称密码算法的加解密性能单位统一为 tps(次/秒)。

金融数据密码机应支持:

- a) SM2 加密;
- b) SM2 解密。

6.4.8 数据杂凑算法性能测试

将一个定长数据报文进行摘要运算,重复操作 N 次,测量其完成时间 T 。用于测试的数据由检测机构选取。测试应进行多次,结果取平均值。数据杂凑算法性能单位统一为 Mbit/s(兆比特/秒)。

金融数据密码机应支持:SM3 杂凑算法。

6.4.9 随机数发生器性能测试

让金融数据密码机生成并输出长度为 L 的符合随机特性的随机序列 N 组,测量其完成时间 T 。测试应进行多次,结果取平均值。随机数发生器性能单位统一为 Mbit/s(兆比特/秒)。

6.4.10 非对称密钥生成性能测试

让金融数据密码机生成并输出指定数量的密钥对,测量其完成时间 T 。测试应进行多次,结果取平均值。非对称密钥生成性能单位统一为 tps(对/秒)。

金融数据密码机应支持:SM2 密钥生成。

6.4.11 非对称算法签名、验签性能测试

将一个定长数据报文进行签名/验签操作,重复操作 N 次,测量其完成时间 T 。用于测试的数据由检测机构选取。测试应进行多次,结果取平均值。支持多种非对称算法,必须测试所支持的所有非对称密码算法的签名/验签性能。非对称密码算法的签名/验签性能单位统一为 tps(次/秒)。

金融数据密码机应支持:

- a) SM2 签名;
- b) SM2 验签。

6.5 其他检测

6.5.1 设备安全性测试

金融数据密码机设备安全性测试遵照 GM/T 0039。

6.5.2 环境适应性检测

金融数据密码机设备环境适应性测试应达到 GM/T 0045—2016 中 6.4 的要求。

6.5.3 可靠性检测

金融数据密码机设备可靠性测试应达到 GM/T 0045—2016 中 6.5 的要求。

7 送检技术文档要求

金融数据密码机研制单位按照国家密码管理主管部门检测要求提交相关文档资料,作为金融数据密码机的检测依据。文档资料应包含但不限于以下内容:

- a) 后台服务程序、应用编程接口和客户端管理软件的结构框图、流程图;
- b) 开机自检的工作原理说明;

- c) 自测程序的工作原理说明；
- d) 敏感数据信息的存储和使用说明；
- e) 物理防护措施说明；
- f) 技术工作总结报告；
- g) 安全性设计报告；
- h) 安装使用说明；
- i) 源代码及说明；
- j) 算法自检说明；
- k) 随机数自检原理说明；
- l) 产品清晰彩照。

8 合格判定条件

在本标准 6.2、6.3.1、6.3.2、6.3.3、6.3.4、6.3.5、6.3.8、6.3.9、6.5.1 和第 7 章所规定的检测项目中，如果任意一项必须具备的功能项检测结果不合格，判定为产品不合格。

附 录 A
(规范性附录)
测试项目列表

表 A.1 外观和结构测试项目表

测试项目	测试内容	备注
外观和结构检查	面板印字清晰, 标牌粘贴牢固, 整机外壳无明显划痕, 附件齐全	
	金融数据密码机应具备以下主要部件或端口: a) 具备电源指示灯; b) 具备状态指示灯; c) 具备故障指示灯; d) 具备至少 1 个服务端口; e) 具备至少 1 个管理端口; f) 如果密钥存储采用微电保护存储方式, 应具备密钥自毁机制	
	金融数据密码机宜具备以下部件或端口: a) 宜具备 1 个打印端口; b) 如果密钥使用时会以明文方式出现在金融数据密码机内存中, 宜具备内存清除机制; c) 宜具备机箱外壳接地装置; d) 宜具备冗余电源; e) 宜具备 IC 卡插座; f) 宜具备 USB 端口; g) 宜具备人机交互部件	

表 A.2 初始化检测项目表

测试项目	测试内容	备注
初始化检测	如果没有初始化, 是否提示报警	
	执行初始化后, 是否能进入工作状态	
	管理员生成	
	服务端口配置	
	管理端口配置	

表 A.3 密码运算检测项目表

测试项目	测试内容	备注
密码运算检测	SM4 ECB 加密	
	SM4 ECB 解密	
	SM4 CBC 加密	

表 A.3 (续)

测试项目	测试内容	备注
密码运算检测	SM4 CBC 解密	
	SM3 杂凑	
	SM2 密钥生成	
	SM2 签名	
	SM2 验签	
	SM2 加密	
	SM2 解密	
	SM2 密钥协商	

表 A.4 密钥管理检测项目表

测试项目	测试子项目	备注
密钥管理检测	金融数据密码机密钥管理应具备以下功能： a) 产生主密钥：生成主密钥，并以安全的方法存储到安全介质中。 b) 导入主密钥：从安全介质导入主密钥。 c) 查询主密钥：显示主密钥状态。 d) 销毁密钥：通过管理工具或者硬件开关销毁密钥。 e) 密钥自毁机制：如果密钥存储采用微电保护存储方式，在加电及不加电两种情况下打开机箱，然后检查密钥是否被自动销毁。	
	金融数据密码机密钥管理宜具备以下功能： a) 注入成员主密钥：以安全的方法注入成员主密钥，并显示其检查值。 b) 密钥备份：以安全的方法备份金融数据密码机内部存储密钥到安全介质。 c) 密钥恢复：清除金融数据密码机内的密钥，然后以安全的方法将安全介质中备份的密钥恢复到金融数据密码机，再查询密钥。 d) 密钥同步：通过备份介质安全地将密钥同步至另一台相同的设备。 e) 清除内存密钥：如果密钥使用时会以明文方式出现在金融数据密码机内存中，加电时打开机箱，应能自动清除内存中的密钥。	

表 A.5 随机数检测项目表

测试项目	测试内容	备注
随机数检测	随机数发生器芯片型号、随机源个数	
	随机数质量检测	
	出厂检测	
	上电检测	
	周期检测	
	单次检测	

表 A.6 访问控制检测项目表

测试项目	测试内容	备注
访问控制检测	物理访问控制	
	管理权限角色划分	
	授权身份认证机制	
	关键安全操作必须由管理员授权	
	服务端口授权访问机制	

表 A.7 设备管理检测项目表

测试项目	测试内容	备注
设备管理检测	按照 GM/T 0050 的要求进行检测	

表 A.8 日志审计检测项目表

测试项目	测试内容	备注
日志审计检测	<p>金融数据密码机的日志内容应包括：</p> <p>a) 管理员操作行为,包括登录认证、系统配置、密钥管理等操作；</p> <p>b) 异常事件,包括自检失败、认证失败、非法访问等异常事件的记录。</p> <p>金融数据密码机的日志内容宜包括：</p> <p>a) 开机启动事件记录,包括开机时间、开机时的系统状态等；</p> <p>b) 密码服务程序重启记录,记录由于程序 BUG 或者内存溢出等原因,导致密码服务程序重启的事件,包括重启的时间、系统状态等；</p> <p>c) 其他异常事件,如端口连接异常、系统资源不足等</p>	

表 A.9 设备自检检测项目表

测试项目	测试内容	备注
设备自检检测	上电/复位自检	
	手工自检	
	周期性自检	

表 A.10 数据报文接口(API)检测项目表

测试项目	测试内容	备注
数据 报文 接口 检测	X0 产生密钥	
	A6 导入密钥	
	A8 导出密钥	
	GG 合成 ZMK	
	X2 LMK 加密密钥	
	AG TAK 从 LMK 到 TMK	
	MG TAK 从 LMK 到 ZMK	
	MI TAK 从 ZMK 到 LMK	
	KA 生成密钥校验值	
	BA 加密 PIN	
	NG 解密 PIN	
	BE PIN 验证	
	JE PIN 块从 ZPK 到 LMK	
	JC PIN 块从 TPK 到 LMK	
	JG PIN 块从 LMK 到 ZPK	
	MA 产生终端 MAC	
	MC 验证终端 MAC	
	ME 验证并转换终端 MAC	
	CW 产生 CVV	
	CY 验证卡校验码 CVV	
	PE 打印密码信封	
	V2 分散密钥加密	
	EI 产生 RSA 密钥对	
	UA 分解 RSA 私钥分量	
	UK 公钥运算	
	VA 外部私钥运算	
	GM 产生消息摘要	
	EW RSA 签名	
	VC 安全报文计算	
	EY RSA 验签	
	VM ARQC/ARPC 产生或验证	
	VI 脚本加解密	
	VK 计算脚本 MAC	

表 A.10 (续)

测试项目	测试内容	备注
数据报文接口检测	VS IC卡发行数据转加密保护	
	WO PIN转加密	
	UO 产生SM2密钥对	
	UQ SM2签名	
	US SM2验签	
	UU SM2公钥加密	
	UW SM2私钥解密	
	UY 转加密SM2私钥	
	B8 数据加解密	

表 A.11 性能检测项目表

测试项目	测试内容	备注
性能测试	PIN加密:调用BA命令,用SM4密码算法加密PIN	
	PIN转加密:调用JE命令,用SM4密码算法将PIN块从ZPK加密转到LMK加密	
	MAC计算:调用MA命令,用SM4密码算法对256字节的数据进行MAC计算	
	ARQC验证:调用VM命令,用SM4密码算法验证256字节数据的ARQC	
	SM4 ECB加密:调用B8命令,用SM4密码算法加密4096字节的数据	
	SM4 ECB解密:调用B8命令,用SM4密码算法解密4096字节的数据	
	SM4 CBC加密:调用B8命令,用SM4密码算法加密4096字节的数据	
	SM4 CBC解密:调用B8命令,用SM4密码算法解密4096字节的数据	
	SM2加密:调用UU命令,用SM2公钥加密256字节的数据	
	SM2解密:调用UW命令,用SM2私钥解密UU命令的加密结果	
	SM3杂凑:调用GM命令,用SM3杂凑算法计算4096字节数据的杂凑值	
	随机数产生性能:调用XO命令,产生随机数	
	SM2密钥生成:调用UO命令,产生SM2密钥对	
	SM2签名:调用UQ命令,对32字节数据进行签名	
	SM2验签:调用US命令,对32字节数据进行验签	

表 A.12 设备安全性测试项目表

测试项目	测试内容	备注
设备安全性测试	设备安全性测试遵照 GM/T 0039	

表 A.13 环境适应性检测项目表

测试项目	测试内容	备注
环境适应性检测	设备环境适应性测试应达到 GM/T 0045—2016 中 6.4 的要求	

表 A.14 可靠性检测项目表

测试项目	测试内容	备注
可靠性检测	设备可靠性测试应达到 GM/T 0045—2016 中 6.5 的要求	

参 考 文 献

- [1] GB/T 4943—1995 信息技术 设备(包括电气事务设备)的安全
- [2] GB/T 9813—2000 微型计算机通用规范
- [3] GB/T 17903.3—1999 信息技术 安全技术 密钥管理 第1部分:框架
- [4] GB/T 17903.3—1999 信息技术 安全技术 密钥管理 第2部分:使用对称技术的机制
- [5] GB/T 17903.3—1999 信息技术 安全技术 密钥管理 第3部分:使用非对称技术的机制
- [6] GB/T 17964—2000 信息技术 安全技术 加密算法 第1部分:概述
- [7] GB/T 17964—2000 信息技术 安全技术 加密算法 第2部分:非对称加密
- [8] GB/T 17964—2000 信息技术 安全技术 加密算法 第3部分:对称加密
- [9] GB/T 17964—2008 信息技术 安全技术 分组密码算法的工作模式
- [10] GB/T 18336—2001 信息技术 安全技术 信息技术安全性评估准则
- [11] GB/T 18238.1—2000 信息技术 安全技术 散列函数 第1部分:概述
- [12] GB/T 18238.2—2002 信息技术 安全技术 散列函数 第2部分:采用 n 位块密码的散列函数
- [13] GB/T 18238.3—2002 信息技术 安全技术 散列函数 第3部分:专用散列函数
- [14] GB/T 32905—2016 信息安全技术 SM3 密码杂凑算法
- [15] GB/T 32907—2016 信息安全技术 SM4 分组密码算法
- [16] GB/T 32918.1—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第1部分:总则
- [17] GB/T 32918.4—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第4部分:公钥加密算法
- [18] GM/Z 0001 密码术语



GM/T 0046-2016

版权专有 侵权必究

*

书号:155066·2-31452

定价: 30.00 元