ICS 35.040
L 80
备案号:58558—2017

GM

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

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、邹铷、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]