ICS 35.040
L 80
备案号：58555—2017

GM

中华人民共和国密码行业标准

GM/T 0050—2016

密码设备管理
设备管理技术规范

Cryptography device management—
Specification of device management technology

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。

《密码设备管理》由一系列标准组成，其中 GM/T 0050《密码设备管理　设备管理技术规范》是此类标准的核心基础；其余标准由不同的管理应用标准组成，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　对称密钥管理技术规范；

——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　远程监控和合规性检验接口数据规范。

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。

本标准的附录 A、附录 B 是规范性附录。

本标准起草单位：兴唐通信科技有限公司、无锡江南信息安全工程技术中心、成都卫士通信息产业股份有限公司、山东得安信息技术有限公司、上海格尔软件股份有限公司、北京海泰方圆科技有限公司、长春吉大正元信息技术股份有限公司、北京数字证书认证中心有限公司、上海市数字证书认证中心有限公司、万达信息股份有限公司。

本标准主要起草人：王妮娜、李玉峰、林岳嵩、王海霞、徐强、李元正、高志权、谭武征、柳增寿、李伟平、李述胜、韩玮、周栋。

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

密码设备管理向上层管理应用提供设备管理应用接口，为实现远程密钥管理、设备维护、设备监控、设备合规性检查等上层管理应用提供设备管理功能，将上层管理应用的管理请求转换为标准的消息调用，通过安全协议建立应用层安全通道，实现管理应用与密码设备间的消息传递。

本标准规定了密码设备管理的应用接口、管理流程、管理协议、管理信息结构，明确了密码设备实现管理代理的具体要求，实现设备管理应用与具体密码设备的无关性，达到依据本标准设计开发的密码设备可以由依据本标准开发的管理系统进行统一管理、统一配置的目的。有关密码设备管理系统的建设要求和运行管理要求请参考CA管理系统相关标准，本标准不再另行定义。本标准为密码设备和上层管理应用的研制和开发提供指导和依据。

本标准制定一套密码设备管理应用接口，确定密码设备实现管理代理的具体要求，实现设备管理应用与具体密码设备的无关性，达到依据本标准设计、开发的密码设备，可以进行统一管理、统一配置的目的。

本标准第5、第6、第7、第8、第9章针对密码设备管理系统开发商使用。

本标准第5、第6、第7、第8章针对密码设备厂商使用。

本标准第5、第9章针对管理应用厂商使用。

本标准的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
设备管理技术规范

1 范围

本标准规定了密码设备管理的体系结构、管理流程、安全通道协议、管理信息结构、应用接口和标准管理消息格式。

为应用技术体系框架内的密码设备和上层管理应用的研制和开发提供指导和依据。

本标准适用于密码设备管理系统、密码设备管理应用、密码机等密码设备的研制和开发，也可用于指导密码设备管理系统、密码设备的检测。

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 密码应用标识规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0018 密码设备应用接口规范

3 术语和定义

下列术语及定义适用于本文件。

3.1

密码设备 cryptography device

为密钥等秘密信息提供安全存储，并基于这些秘密信息提供密码安全服务的设备。本标准中，专指可以接受设备管理操作的密码设备，主要包括网络密码机、应用密码机/卡；但不包括智能密码终端、密码芯片等部件级设备。

3.2

设备证书 device certificate

可以标识密码设备身份的数字信息，包含密码设备的基本信息、设备公钥信息及其他补充信息等。设备证书可以由专门的 CA 系统签发，也可以由设备管理平台签发。

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数据交互安全协议建立起来的应用层安全连接，目的是为设备管理应用与密码设备之间的应用层信息交互提供机密性和完整性保护。

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，包含签名密钥对和加密密钥对。