ICS 35.040
L 80
备案号:58556—2017

GM

中华人民共和国密码行业标准

GM/T 0051—2016

密码设备管理
对称密钥管理技术规范

Cryptography device management—
Specifications of symmetric key management technology

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
密码设备管理
对称密钥管理技术规范
GM/T 0051—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.org.cn
服务热线:400-168-0010
2017年5月第一版
*
书号:155066·2-31472

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

GM/T 0051《密码设备管理　对称密钥管理技术规范》是密码设备管理类标准之一。该类标准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：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、山东得安计算机技术有限公司、上海格尔软件股份有限公司、北京海泰方圆科技有限公司。

本标准主要起草人：王妮娜、李玉峰、徐强、李元正、孔玉凡、谭武征、柳增寿。

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，提出针对上层对称密钥管理应用的技术标准，为符合GM/T 0050的商用密码设备提供统一分发对称密钥的密钥管理系统技术要求。本标准采用的密钥管理安全通道，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
对称密钥管理技术规范

1 范围

本标准规定了对称密钥管理应用的密钥及系统相关安全技术要求，包括对称密钥管理安全要求、系统体系结构及功能要求、密钥管理安全协议及接口设计要求、管理中心建设、运行及管理要求等。

本标准适用于对称密钥管理系统的研制、建设、运行及管理。

本标准采用《密码设备管理　设备管理技术规范》中的安全通道技术，应使用《密码设备管理　设备管理技术规范》中第6章和第9章的接口。

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　信息安全要求　二元序列随机性检测方法

GM/T 0006　密码应用标识规范

GM/T 0015　基于SM2密码算法的数字证书格式规范

GM/T 0050—2016　密码设备管理　设备管理技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

对称密钥管理系统　symmetric key manage system

为密码应用系统产生和分发对称密钥的管理系统。

3.2

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。

3.3

被管设备　be-managed equipment

接受、解析和处理密钥管理系统指令的密码设备。

3.4

业务密钥　application key

密码应用系统中与具体应用相关的密钥。

3.5

被管系统　be-managed system

接受密钥管理系统管理的密码应用系统，根据密钥管理策略，接收本系统相关的业务密钥。