



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—
Specification of symmetric key 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	III
引言	IV
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 对称密钥管理安全要求	2
5.1 系统安全要求	2
5.2 功能安全要求	3
6 对称密钥管理系统	4
6.1 在密码基础设施技术框架中的位置	4
6.2 管理范围	5
6.3 系统技术框架	5
6.4 系统功能结构	7
6.5 功能描述	7
6.6 系统设计的要求	8
7 对称密钥管理应用指令及管理接口	12
7.1 基本要求	12
7.2 应用指令	12
7.3 管理接口	17
附录 A (规范性附录) 错误码定义	20
附录 B (规范性附录) 密钥格式配置文件	21

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 `symmetrickeymanagesystem`
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 `cryptographydevice`

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-managedequipment`

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 `applicationkey`

密码应用系统中与具体应用相关的密钥。

3.5

被管系统 `be-managedsystem`

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。

3.6

安全通道 `securitytunnel`

密钥管理中心与被管设备间通过数据交互安全协议所建立的逻辑通道，为密钥管理应用提供管理报文的机密性和完整性保护。

3.7

密码设备管理平台 `cryptographydevicemanagementplatform`

为密钥管理应用提供与被管对象建立远程安全通道的管理系统。符合 GM/T 0050,为密钥管理系统提供平台支撑。

3.8

密码设备管理应用程序接口 `cryptographydevicemanagementAPI`

由 GM/T 0050 定义，为上层应用提供安全通道及密码设备管理接口服务。

3.9

分发保护密钥 `distributionprotectingkey`

安全通道中保护一次密钥分发数据的临时性密钥。

3.10

分发保护密钥协商 `distributionprotectingkeyagreement`

密钥管理中心与被管设备通过安全通道协商分发保护密钥的过程。

3.11

原子密钥 `atom key`

被管密码设备自定义的私有格式封装的密钥。

3.12

专用密钥生成装置 `customizedkeygenerator`

为特定密码应用系统、特定型号被管设备产生私有格式封装的原子密钥的硬件装置。

3.13

通用密钥生成装置 `generalkeygenerator`

为不同被管设备产生标准格式封装的原子密钥的硬件装置。

3.14

密钥格式配置文件 `generalkeyconfigprofile`

专用密钥生成装置和通用密钥生成装置产生原子密钥的配置文件。

4 缩略语

下列缩略语适用于本文件。

API: 应用程序接口 (Application Programming Interface)
CA: 数字证书认证中心 (Certification Authority)

5 对称密钥管理安全要求

5.1 系统安全要求

- 密码设备应经过国家密码管理主管部门认证；
- 操作人员应经过身份鉴别，按照所授权限访问密钥管理系统；
- 密钥管理操作应根据密钥管理策略执行；
- 密钥分发协议应保证所分发密钥的机密性和完整性；

- 密钥的封装和导入应与分发方式无关；
- 密钥管理操作应进行安全审计；
- 密钥管理系统应保证密钥存储及备份安全。

5.2 功能安全要求

5.2.1 密钥生成

密钥和密钥分量应使用经过国家密码管理主管部门检测的物理噪声源产生，符合 GM/T 0050 的要求。

5.2.2 密钥存储和备份

密钥存储应确保机密性和完整性，防止未经授权密钥的泄露和替换。
针对不同的密钥形态，具体存储要求如下：

— 明文密钥

需长期存储的明文密钥，应当存储于安全密码设备的物理安全模块中，当物理安全模块失效时，其中存储的明文密钥立即失效。

— 密钥分量

密钥分量在生命周期内应隔离存储于不同介质中，由不同的管理人员分别持有。

— 密文密钥

可以存储在密码设备内，也可以存储于密码设备外。若存储于密码设备外，应确保经过授权才能访问。

密钥备份也应确保机密性和完整性，具体要求与密钥存储一致。

5.2.3 密钥分发和加载

密钥分发和加载，可以通过人工加载、移动存储介质直接加载、专用密钥传递设备加载、网络分发的方式。

具体分发要求如下：

— 明文密钥

当明文密钥在两个安全密码设备之间传递时，应该采用分量传递、口令保护或其他方式，防止密钥泄露、篡改和替换。

— 密钥分量

密钥分量分发过程不应泄露密钥分量的任何部分给未授权人。

— 密文密钥

密文密钥可以通过网络分发和加载。密文密钥的分发应防止密钥篡改和密钥替换。

5.2.4 密钥使用

- 密钥应指定属性或控制向量，防止密钥被非授权使用；
- 密钥只能用于指定应用；

- 密钥只能用于指定用途或功能；
- 当已知密钥被泄露时，应停止使用；
- 当怀疑密钥被泄露时，可以主动停止使用。

5.2.5 密钥更新

密钥管理系统应针对被管系统和被管设备设置密钥更新策略。

当密钥超过使用期限、已泄露、怀疑密钥不安全时，应根据相应的更新策略进行更换。如果泄露

或被怀疑的密钥是密钥加密密钥或根密钥，所有被该密钥加密的密钥或子密钥都应被更换。

因密钥更换带来的应用数据解密并再加密过程，不由密钥管理中心负责。

具体要求如下：

- 严格按照密钥更新策略进行更新；
- 新密钥不可逆向推导出旧密钥；
- 不能增加其他密钥的泄露风险。

5.2.6 密钥归档

当密钥超过使用期限，或不再使用时，根据密钥管理策略可以被归档。

密钥可以采用下述形式归档：

- 以至少两个分离的密钥分量形式分别存储于密码设备；
- 使用密钥加密密钥加密归档密钥；
- 已归档的密钥只能用于证明在归档前进行的交易的合法性；
- 已归档的密钥不应返回到操作使用中；
- 归档密钥不能影响在用的密钥的安全。

5.2.7 密钥销毁

根据密钥管理策略，可以对密钥进行销毁，要求从各种已用的介质中销毁待销毁密钥。销毁结果要求不可逆，不可从销毁结果中恢复原密钥。

5.2.8 密钥恢复

恢复的密钥不能以明文方式输出密码设备。 可以支持用户密钥恢复和司法密钥恢复。

6 对称密钥管理系统

6.1 在密码基础设施技术框架中的位置

密钥管理应用在密码基础设施体系结构中的位置如图 1 所示。

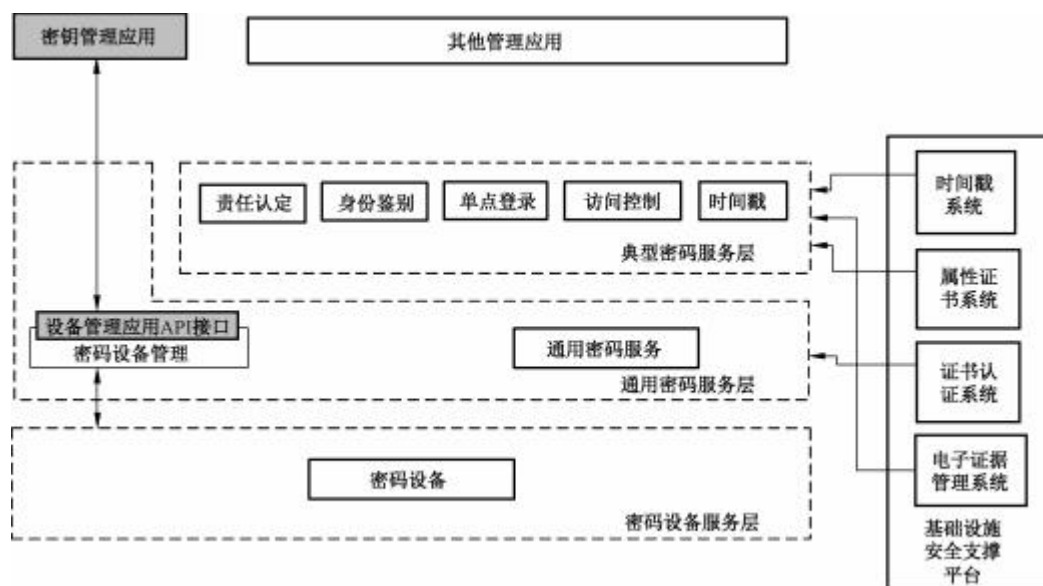


图 1 密钥管理应用与密码基础设施的关系

密钥管理应用与被管设备间的密钥管理协议，通过 GM/T 0050 定义的安全通道承载。密钥管理系统调用 GM/T 0050—2016 中 9.2.1 的初始化设备管理环境 API 接口，获取与被管设备的安全通道句柄，调用 GM/T 0050—2016 中 9.4 的安全通道数据发送接口，将密钥管理指令封装在安全通道消息 PDU 中发送至被管密码设备。

本标准规定的技术范围与 GM/T 0050—2016 技术范围的关系如图 2 所示，其中，密钥管理系统中的应用层和设备层中的密钥管理代理属于本标准的范围。

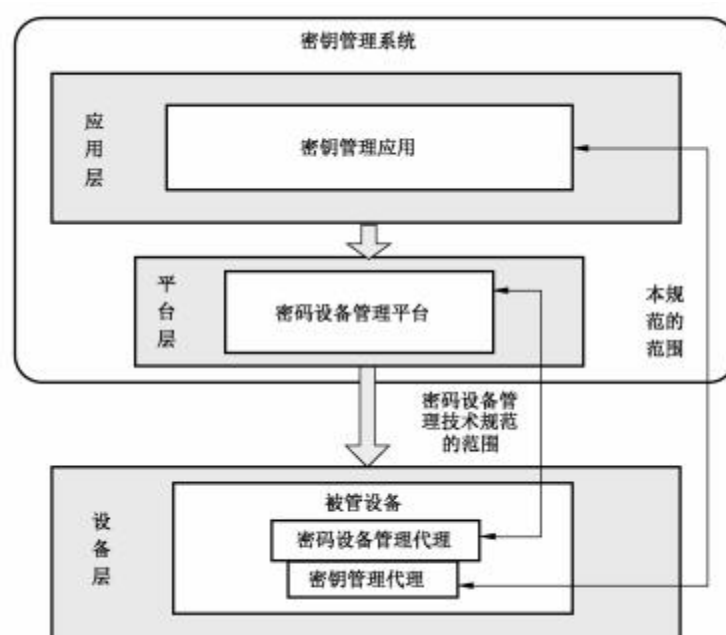


图 2 密钥管理应用与密码设备管理平台的关系

6.2 管理范围

本标准提出统一的商用密钥管理平台技术要求，对支持本标准的商用密码应用系统和各型号的商用密码设备实现密钥统一产生和统一分发。

本标准仅管理被管系统的业务密钥，由被管系统临时产生的对称密钥（如应用的会话密钥）不在本标准管理范围之内。

6.3 系统技术框架

6.3.1 总体技术框架

本标准的密钥管理总体技术框架如图 3 所示。

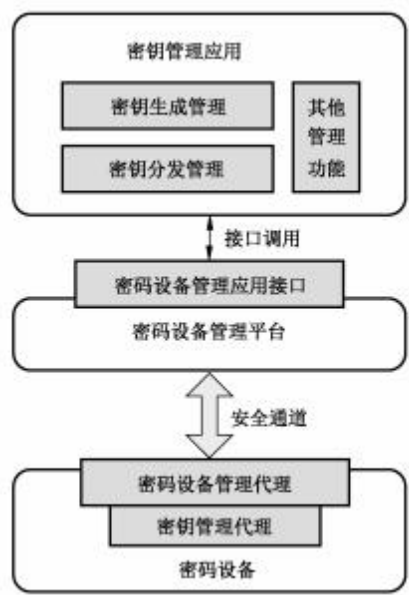


图 3 密钥管理总体技术框架

密钥管理技术分为生成、分发和其他管理功能几个部分。通过设备管理平台提供的应用 API 接口在设备管理平台与被管设备代理间建立的安全通道，实现密钥分发。

密钥生成管理中，密钥由专用密钥生成装置或通用密钥生成装置产生，用密钥管理中心与密钥生成装置间协商产生的会话密钥加密，安全传输至密钥管理中心。

密钥分发管理中，密钥管理应用调用密码设备平台 API 与被管设备建立安全通道，根据分发策略，以密钥管理专用指令分发标准封装密钥。被管密码设备的设备管理代理从安全通道中分离密管指令，由密钥管理功能模块拆封、解析、接收密钥。

密码设备管理平台以密码设备管理 API 的方式向密钥管理等上层应用提供设备信息、安全通道、安全分发等功能。设备管理平台相关技术标准参见 GM/T 0050—2016。

6.3.2 系统技术框架

密钥管理系统组成框架如图 4 所示。

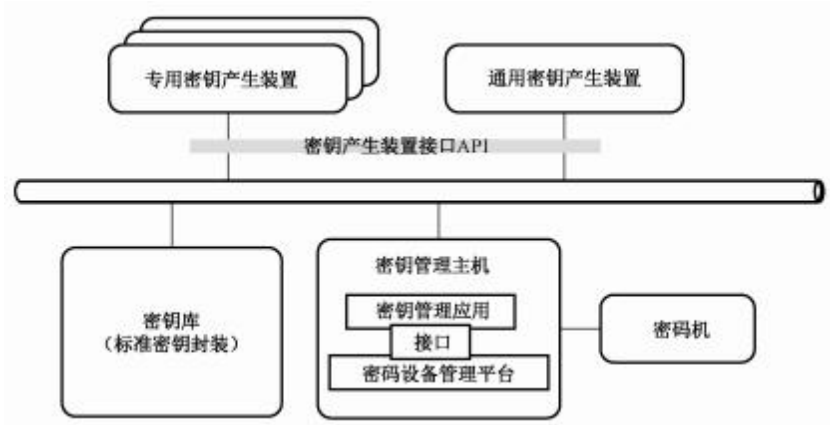


图 4 密钥管理系统组成框架

密钥管理系统由密钥管理中心和被管密码设备组成。密钥管理中心统一产生和分发各系统、各型号被管设备的业务密钥，实现业务密钥的产生、分发、备份、查询、更新、归档和销毁。被管设备接收和执行标准密钥管理命令。密钥管理系统根据具体情况采用多级管理中心的方式。

6.4 系统功能结构

密钥管理系统主要由主控管理、密钥生成/存储管理、密钥分发管理、备份/恢复/归档管理、身份认证、审计管理、密管代理、密码处理等模块组成。

密钥管理系统功能结构如图 5 所示。

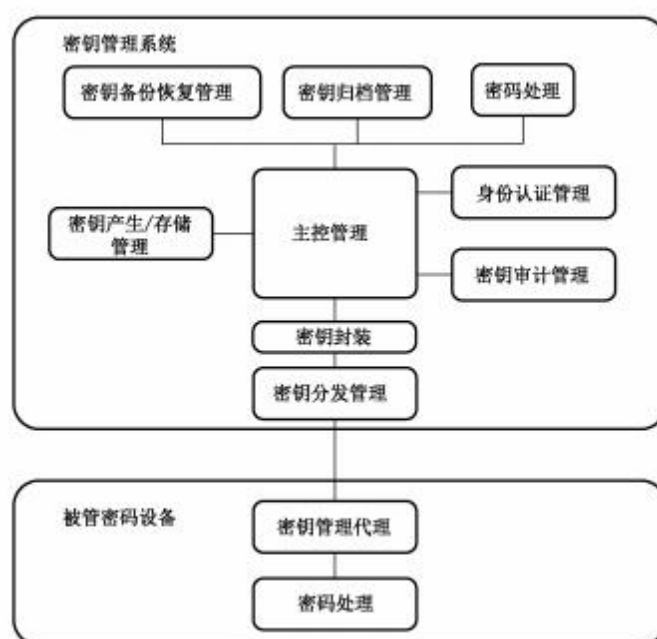


图 5 密钥管理系统功能结构

6.5 功能描述

6.5.1 主要功能

密钥管理系统主要功能是管理业务密钥，同时应具备身份认证、审计管理功能，以确保管理系统的安全。

6.5.2 主控管理

管理、调度其他模块的关键模块，完成策略配置、密钥分发、密钥查询等主要密管功能。

密钥生成策略的配置包括是否使用专用密钥生成装置、密钥生成的数量及长度要求等，由密钥管理系统根据密钥管理应用需求制定。

密钥分发策略的配置包括一系列组合条件，参见 6.5.4。

其他策略的配置包括密钥查询方式、通用密钥生成装置封装格式的导入等操作。

当策略条件满足时，将触发相应的密钥管理操作。

6.5.3 密钥生成 / 存储

本标准以通用密钥生成装置和专用密钥生成装置分别产生通用格式密钥和专用格式密钥。

通用密钥生成装置生成随机密钥，主控管理模块根据被管设备密钥格式配置文件的要求将所产生的随机密钥封装为原子密钥。

专用密钥生成装置生成有变换要求或格式复杂的专用原子密钥。基于随机数复杂变换的密钥，只能通过专用密钥生成装置生成。

密钥生成由密钥生成策略触发，所生成原子密钥经本地主密钥加密保护和格式化封装后，存储于系统密钥库中。密钥管理系统产生的原子密钥均为被管系统的业务密钥，被管系统所需一次性密钥不由密钥管理系统产生。

6.5.4 密钥分发

应根据密钥分发策略进行在线分发或离线分发。在线密钥分发过程应遵循本标准制定的密钥分发协议。离线分发支持多种分发介质，包括专用密钥加载装置、通用移动密钥加载装置等，应遵循介质的安全分发协议。

密钥封装及导入处理与分发方式无关。

6.5.5 密钥管理代理和密码处理

密钥管理代理内嵌于被管设备中，用于接收、解析并导入所分发密钥的模块。

被管设备的密钥管理代理由设备厂商定制，应支持本标准规定的密钥分发协议，支持在线接收或离线介质接收。

被管设备的密码处理单元执行密钥管理相关的操作。

6.5.6 密钥备份 / 恢复 / 归档

为增强系统的容灾性，密钥管理系统应对各种形态的密钥数据进行备份，可以采用异机备份、异地备份等。

密钥管理系统应提供用户密钥恢复和为司法取证服务的司法密钥恢复。用户密钥恢复由被管设备所属单位提出申请，司法密钥恢复由司法取证部门提出申请，依据密钥管理系统的管理要求通过审批后执行。

对于过期的加密密钥，根据使用策略，由密钥管理系统进行归档保存，且应保证归档密钥的机密性和完整性。

6.5.7 身份鉴别

密钥管理系统的管理人员、操作人员、维护人员应通过身份鉴别才能进行相应的授权操作。

身份鉴别可以根据系统的安全强度要求，使用口令、生物特征（如指纹）、数字证书等技术措施或其组合。

6.5.8 系统审计

密钥管理系统应对各密钥管理操作及其内容进行审计，应确保审计信息不可被修改和删除，并在要求的期限内备份。

6.6 系统设计要求

6.6.1 总体原则

- 密钥管理系统遵循标准化、模块化、松耦合设计原则；
- 应保障系统模块之间连接的安全性，包括完整性、机密性、防重放、不可否认性；

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：

<https://d.book118.com/818134033003006112>