ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0143—2024

对称密钥管理系统检测规范

Test specification of symmetric key management system

2024-12-27 发布　　2025-07-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：商用密码检测认证中心、三未信安科技股份有限公司、江苏米树科技有限公司、北京安御道合科技有限公司、兴唐通信科技有限公司、中电科网络安全科技股份有限公司、公安部第三研究所、中安网脉（北京）技术股份有限公司。

本文件主要起草人：齐晶晶、冯晓钰、雷银花、邓开勇、高志权、刘文丽、董坤朋、罗川、吕竹青、王新树、梁皓、王亮、呼香艳、黎幸子、杨彬彬、沈芳宇、张琳琳、白婧、徐威、王天顺。

对称密钥管理系统检测规范

1 范围

本文件规定了对称密钥管理系统的检测内容、检测要求、检测方法以及判定规则。

本文件适用于对称密钥管理系统的检测，也用于指导该类产品的研制、生产和测试。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 33560 信息安全技术 密码应用标识规范

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GB/T 38636 信息安全技术 传输层密码协议(TLCP)

GM/T 0005 随机性检测规范

GM/T 0018 密码设备应用接口规范

GM/T 0050 密码设备管理 设备管理技术规范

GM/T 0051—2016 密码设备管理 对称密钥管理技术规范

GM/T 0062 密码产品随机数检测要求

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001 界定的以及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 management system

为密码应用系统产生和分发对称密钥的管理系统。

3.2

主密钥 local main key

对称密钥管理系统顶层密钥，用于加密对称密钥管理系统其他密钥。

3.3

业务密钥 application key

密码应用系统中与具体应用相关的密钥。

3.4

安全通道 security tunnel

对称密钥管理系统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。

3.5

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。

3.6

分发保护密钥　distribution protecting key

安全通道中保护一次密钥分发数据的临时性密钥。

3.7

专用密钥生成装置　customized key generator

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。

3.8

通用密钥生成装置　general key generator

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。

3.9

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。

4　缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Program Interface）

TLCP：传输层密码协议（Transport Layer Cryptography Protocol）

CA：证书认证中心（Certification-Authority）

PDU：分包数据单元（Package-Data-Unit）

5　检测环境

检测环境由待测产品、密钥生成装置和检测平台组成。其中：

待测产品为对称密钥管理系统按照6.2规定的测试程序执行检测；密钥生成装置接口API应符合6.3.2.1接口要求；密钥管理应用接口API应符合6.3.1、6.3.2各项接口要求。

密钥生成装置为待测产品提供格式化封装后的原子密钥。待测产品通过密钥生成装置接口API与密钥生成装置互通，获取密钥生成装置生成的原子密钥。

检测平台部署密钥管理代理，与待测产品通过密钥管理应用接口API互通，完成对待测产品的密钥管理应用接口API的检测。检测平台应符合6.3.1、6.3.2各项接口检测功能要求。

检测环境拓扑图见图1。对称密钥管理系统框架详见GM/T 0051—2016。

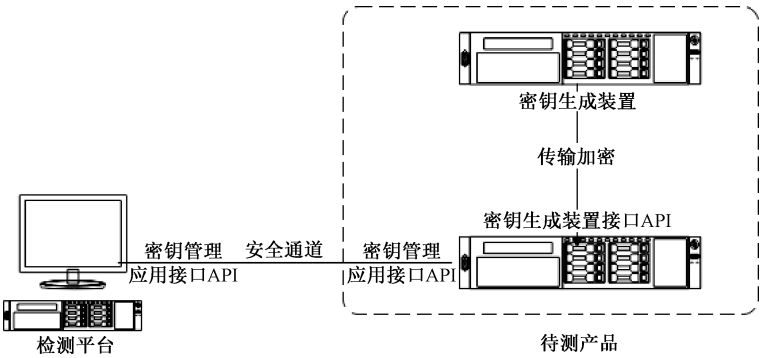

图1　对称密钥管理系统检测环境拓扑图

6 检测内容

6.1 概述

对称密钥管理系统检测项目包括：

a) 功能检测：密钥生成装置检测、初始化检测、密码算法检测、随机数检测、密钥管理检测、管理功能检测、系统审计检测和安全通道检测；
b) 接口检测：应用指令检测和管理接口检测；
c) 性能检测：包含密钥格式封装性能检测、密钥分发性能检测和容量性能检测。

6.2 功能检测

6.2.1 密钥生成装置检测

6.2.1.1 通用密钥生成装置检测

检测要求：

a) 通用密钥生成装置应为经检测认证的硬件密码模块，如密码机、密码卡等；
b) 通用密钥生成装置应具备随机数生成功能；
c) 通用密钥生成装置应通过被管设备密钥格式配置文件生成密钥，密钥格式配置文件应按照GM/T 0051—2016 附录 B 要求实现；
d) 通用密钥生成装置对外 API 具备生成原子密钥接口，接口符合 GM/T 0051—2016 中 7.3.1 要求。

检测方法：

a) 核查通用密钥生成装置具备商用密码认证证书，则测试通过，否则测试不通过；
b) 通过对称密钥管理系统调用通用密钥生成装置接口生成随机数，并返回成功则测试通过，否则测试不通过；
c) 对称密钥管理系统能够导入符合 GM/T 0051—2016 附录 B 要求的被管设备密钥格式配置文件，导入成功，则测试通过，否则测试不通过；
d) 对称密钥管理系统能够执行原子密钥生成操作，并将原子密钥按照密钥封装格式要求将密钥存储至密钥库中，则测试通过，否则测试不通过；通用密钥生成装置对外 API 检测方法详见 6.3.2.1。

6.2.1.2 专用密钥生成装置检测

检测要求：

a) 专用密钥生成装置应为经检测认证的硬件密码模块，如密码机、密码卡等；
b) 专用密钥生成装置应具备随机数生成功能；
c) 专用密钥生成装置应通过被管设备密钥格式配置文件生成密钥，密钥格式配置文件应按照GM/T 0051—2016 附录 B 要求实现；
d) 专用密钥生成装置对外 API 具备生成原子密钥接口，接口符合 GM/T 0051—2016 中 7.3.1 要求。

检测方法：

a) 核查专用密钥生成装置具备商用密码认证证书，则测试通过，否则测试不通过；
b) 通过对称密钥管理系统调用专用密钥生成装置接口生成随机数，并返回成功则测试通过，否则测试不通过；

c) 对称密钥管理系统能够导入符合 GM/T 0051—2016 附录 B 要求的被管设备密钥格式配置文件，导入成功，则测试通过，否则测试不通过；

d) 对称密钥管理系统能够执行原子密钥生成操作，并将原子密钥按照密钥封装格式要求将密钥存储至密钥库中，则测试通过，否则测试不通过。

6.2.2 初始化检测

检测要求：

a) 应创建对称密钥管理系统的管理人员、操作人员、审计人员；

b) 宜由第三方 CA 或密码设备管理平台等签发对称密钥管理系统证书，包括签名证书和加密证书，并导入对称密钥管理系统和被管设备中。

检测方法：

a) 创建所需各类角色，使得不同角色在初始化完成后能够登录对称密钥管理系统，创建成功，则测试通过，否则测试不通过；

b) 支持由对称密钥管理系统发起证书请求申请时，能够导出证书请求，则测试通过，否则测试不通过；

c) 支持由第三方 CA 或密码设备管理平台等签发对称密钥管理系统证书时，对称密钥管理系统能够导入证书，则测试通过，否则测试不通过；

d) 支持导出对称密钥管理系统证书，将对称密钥管理系统证书导入被管设备时，证书能够导入被管设备，则测试通过，否则测试不通过。

6.2.3 密码算法检测

检测要求：

a) 至少支持一种对称密码算法，提供对称算法加密、解密。若采用 SM4 算法时，应按照 GB/T 32907 实现，算法标识应按照 GB/T 33560 实现；

b) 至少支持一种非对称密码算法，提供加解密、签名验签等，若非对称密码算法采用 SM2 算法时，应按照 GB/T 32918(所有部分)、GB/T 35275、GB/T 35276 实现，算法标识应按照 GB/T 33560 实现；

c) 至少支持一种杂凑算法，若杂凑算法采用 SM3 算法时，应按照 GB/T 32905 要求实现，算法标识应按照 GB/T 33560 实现；

d) 密码算法应在经检测认证的硬件密码设备中运行。

检测方法：

a) 通过代码审查方式，核查验证密码算法标识与规范一致，则测试通过，否则测试不通过；

b) 通过各项接口检测，密码功能调用成功则测试通过，否则测试不通过。

6.2.4 随机数检测

检测要求：

a) 应采用经检测认证的物理噪声源提供随机数生成功能，随机数质量检测结果应符合 GM/T 0005；

b) 应支持随机数自检，自检失败，应停止提供安全服务，进入错误状态，输出错误指示。随机数自检应按照 GM/T 0062 中规定的 E 类产品随机数检测要求实现。

检测方法：

a) 随机数质量检测结果判定符合 GM/T 0005 的要求，则测试通过，否则测试不通过；

b) 对称密钥管理系统提供手动随机数自检或策略触发随机数自检，系统反馈自检通过或自检失败，当自检失败时，系统停止提供安全服务，进入错误状态，并反馈随机数自检失败，则测试通

过，否则测试不通过。

6.2.5 密钥管理检测

6.2.5.1 密钥生成

检测要求：

密钥生成由密钥生成策略触发，应生成经格式化封装后的原子密钥。

检测方法：

a) 对称密钥管理系统配置密钥配置文件后，通过调用密钥生成装置 API 接口，生成原子密钥，通过解析密钥封装格式，可成功解析原子密钥，则测试通过，否则测试不通过；

b) 审计员核查系统日志，能成功查找到密钥生成的日志记录，则测试通过，否则测试不通过。

6.2.5.2 密钥存储

检测要求：

a) 应生成对称密钥管理系统密钥并安全存储，应采用密码技术保证密钥的机密性和完整性；明文密钥应存储于密码设备的物理安全模块中，当物理安全模块失效时，明文密钥立即失效；采用密钥分割方式存储保存的密钥，各分量应存储于不同的安全介质中并由不同的管理人员分别持有；

b) 生成原子密钥后，由主密钥加密保护和格式化封装后存储在密钥库中；

c) 原子密钥存储结构采用标准密钥封装格式，封装格式应按照 GM/T 0051—2016 中 7.2.2 格式实现；

d) 密钥库存储管理应按照 GM/T 0051—2016 中 6.6.2.5 密钥库存储管理模块的要求实现。

检测方法：

a) 通过代码审查、存储密钥数据库审查等方式，验证存储密钥均为密文存储，且同步存储相关密钥杂凑值或消息验证码，则测试通过，否则测试不通过；通过原理审查、代码审查等方式，验证存储在密码设备内部的明文密钥在物理安全模块失效时立即失效，则测试通过，否则测试不通过；采用密钥分割方式存储的密钥，验证各分量存储于不同的安全介质中，且不同的安全介质有可区分标识以区分不同的管理人员，则测试通过，否则测试不通过；

b) 对称密钥管理系统调用密钥生成装置接口，向密钥生成装置请求密钥，密钥生成装置生成所需原子密钥，并返回响应数据符合预期，则测试通过，否则测试不通过；

c) 核查对称密钥管理系统能成功解密原子密钥并使用主密钥进行加密保护，对比请求响应及存储结构中的原子密钥，若密文相同则转加密保护测试不通过，若密文不同则采用主密钥进行解密，若解密失败则转加密保护测试通过，否则测试不通过；

d) 核查密钥库中原子密钥，封装结构符合 GM/T 0051—2016 中 7.2.2 的标准密钥封装格式，则测试通过，否则测试不通过；

e) 核查对称密钥管理系统在用密钥库和历史密钥库，在用密钥库记录是否包含产生时间、有效期等标志，历史密钥库记录是否包含作废时间等标志，若缺少记录则测试不通过，否则测试通过；

f) 核查对称密钥管理系统密钥库是否支持查询密钥功能，若不支持则测试不通过，否则测试通过；

g) 核查对称密钥管理系统在用密钥库定期检查功能，若未将超过有效期的或被撤销的密钥转移到历史密钥库则测试不通过，否则测试通过；

h) 核查对称密钥管理系统是否对历史密钥库中超过规定保留期的密钥进行处理，若未将其转移到规定载体则测试不通过，否则测试通过。

6.2.5.3 密钥备份

检测要求：

a) 对称密钥管理系统应提供“密钥备份”功能，如异机备份、异地备份等；
b) 密钥备份应经授权的管理员操作；
c) 备份密钥应是对称密钥管理系统的所有已存储密钥；
d) 应保证备份密钥的机密性与完整性，防止未授权的泄露和替换；
e) 如手动方式备份，则对称密钥管理系统记录管理员操作记录，并用管理员私钥签名；
f) 采用密钥分割方式进行密钥备份时，各分量应存储于不同的安全介质中并由不同的管理人员分别持有。

检测方法（手动方式）：

a) 若采用手动方式备份，管理员按照 6.2.6.1 身份鉴别方法登录对称密钥管理系统；
b) 管理员在管理界面上选择密钥备份，并配置备份策略、备份属性等，则测试通过，否则测试不通过；
c) 管理员在管理界面点击“密钥备份”按钮，能成功备份库中的密钥，则测试通过，否则测试不通过；对称密钥管理系统对采用密钥标准封装格式的密钥进行备份成功，则测试通过，否则测试不通过；
d) 根据备份地址能成功找到备份存储文件，则测试通过，否则测试不通过；
e) 打开密钥备份文件无法获取备份密钥明文信息，则测试通过，否则测试不通过；
f) 审计员核查操作日志中管理员操作，并可验证日志签名有效，则测试通过，否则测试不通过；
g) 对称密钥管理系统提供安全备份、备份恢复操作按钮或指令：执行安全备份操作，依次使用不同安全介质存储对称密钥管理系统的密钥，备份密钥成功，且不同的安全介质有可区分标识以区分不同的管理人员，则测试通过，否则测试不通过；需要执行密钥恢复时，在对称密钥管理系统执行备份恢复操作，依次插入不同安全介质，密钥恢复成功，且不同的安全介质有可区分标识以区分不同的管理人员，则测试通过，否则测试不通过。

检测方法（自动方式）：

a) 若采用自动方式备份，管理员按照 6.2.6.1 身份鉴别方法登录对称密钥管理系统；
b) 管理员在管理界面上能成功配置自动备份策略，且能成功“启用”或“停用”自动备份，则测试通过，否则测试不通过；
c) 管理员在管理界面启用自动备份，在达到自动备份条件后，能成功备份库中的密钥，则测试通过，否则测试不通过；对称密钥管理系统对采用密钥标准封装格式的密钥进行备份，根据备份地址能成功找到备份存储文件，则测试通过，否则测试不通过；
d) 打开密钥备份文件无法获取备份密钥明文信息，则测试通过，否则测试不通过；
e) 审计员核查系统日志，能成功查找到自动备份的日志记录，则测试通过，否则测试不通过。

6.2.5.4 密钥分发

检测要求：

a) 密钥分发应支持多种分发方式，包括在线分发和将业务密钥导出至智能卡、智能密码钥匙等载体离线分发；
b) 密钥分发格式对于离线、在线分发方式应保持一致，密钥封装及导入处理与分发方式无关；
c) 离线分发应按照介质的安全分发协议实现；
d) 密钥分发应按照密钥分发策略管理和密钥更新策略实现；
e) 密钥分发应按照密钥分发的安全性要求实现，包括密钥管理指令的完整性，敏感数据（密钥等）

的机密性和完整性；

f） 密钥分发应支持 GM/T 0051—2016 中定义的标准密钥分发协议，采用安全通道进行分发；

g） 密钥在分发前，应采用有对称密钥管理系统与被管设备协商的分发保护密钥进行转加密；

h） 对称密钥管理系统从数据库中取出被主密钥加密的待分发密钥，调用密码设备将主密钥加密的原子密钥转换为本次分发保护密钥加密，再将标准封装密钥通过安全通道二次保护分发给被管设备；

i） 密钥加密转换只能在密码设备内进行，明文密钥不可导出密码设备。

检测方法（离线分发）：

a） 若采用离线分发，管理员按照 6.2.6.1 身份鉴别方法登录对称密钥管理系统；

b） 管理员在管理界面上选择离线分发，并配置待分发的密钥及分发介质等分发属性，则测试通过，否则测试不通过；

c） 管理员在管理界面点击“密钥分发”按钮，能成功分发选中的密钥到分发介质中，则测试通过，否则测试不通过；

d） 检查分发数据结构，密钥分发符合介质的安全分发协议，则测试通过，否则测试不通过；

e） 检查分发数据结构，密钥格式符合 GM/T 0051—2016 中 7.2.2 的标准密钥封装格式，则测试通过，否则测试不通过；

f） 检查介质中的密钥，能成功找到已离线分发的密钥，则测试通过，否则测试不通过；

g） 审查密钥分发格式对于离线、在线分发方式保持一致，则测试通过，否则测试不通过；

h） 离线分发成功后，审查系统离线分发管理与密钥分发策略管理和密钥更新策略保持一致，则测试通过，否则测试不通过；

i） 审计员核查操作日志中管理员操作，并可验证日志签名有效，则测试通过，否则测试不通过；

j） 审查对称密钥管理系统密钥转加密的过程及代码，原子密钥转加密过程中明文密钥仅在密码设备中使用，则测试通过，否则测试不通过。

检测方法（在线分发）：

a） 若采用在线分发，管理员按照 6.2.6.1 身份鉴别方法登录对称密钥管理系统；

b） 管理员在管理界面上选择在线分发，被管设备与对称密钥管理系统建立安全通道，安全通道符合 GM/T 0050 中安全通道协议相关要求；能成功建立被管设备与对称密钥管理系统的安全通道，则测试通过，否则测试不通过；

c） 使用被管设备发起分发保护密钥协商指令，能成功获取分发保护密钥协商响应，则测试通过，否则测试不通过；

d） 使用被管设备发起密钥申请请求，能成功获取对称密钥管理系统的密钥分发响应，分析密钥申请响应，分发密钥由主密钥保护转为分发保护密钥保护，并能成功按 GM/T 0051—2016 中 7.2.8 格式正确解析密钥，则测试通过，否则测试不通过；

e） 审查密钥分发格式对于离线、在线分发方式保持一致，则测试通过，否则测试不通过；

f） 在线分发成功后，审查系统在线分发管理与密钥分发策略管理和密钥更新策略保持一致，则测试通过，否则测试不通过；

g） 审查对称密钥管理系统密钥转加密的过程及代码，原子密钥转加密过程中明文密钥仅在密码设备中使用，则测试通过，否则测试不通过。

6.2.5.5 密钥使用

检测要求：

a） 密钥应指定属性或控制向量，防止密钥被非授权使用；

b） 密钥只能用于指定应用及设备；

c) 密钥只能用于指定用途或功能；
d) 密钥只能在硬件密码设备中使用；
e) 当已知密钥被泄露时，应停止使用；
f) （可选）当怀疑密钥被泄露时，可以选择主动停止使用。

检测方法：

a) 被管设备按照 6.2.5.4 发起密钥申请请求，检查对称密钥管理系统中密钥申请响应，响应中密钥包含密钥的适配系统标识和适配设备标识（对称密钥管理系统密钥申请响应下发的密钥数据格式符合 GM/T 0051—2016 中 7.2.8，密钥标准封装符合 GM/T 0051—2016 中 7.2.2 要求，检查每个密钥的适配系统标识和适配设备标识等符合预期），则测试通过，否则测试不通过；
b) 使用不同的条件请求同一个密钥，如不同的应用、设备类型、用途或功能，若同一密钥可被用于多个应用、设备类型、或用于多种用途或功能，则测试不通过，否则测试通过；
c) 检查对称密钥管理系统原子密钥封装格式中的适配系统/应用标识、适配设备标识、密钥类型、密钥长度、密钥校验值、密钥校验算法等的正确性，若系统/应用标识、设备标识没有值或与密钥格式配置文件不一致，则测试不通过，否则测试通过；若密钥类型、密钥长度、密钥校验值、密钥校验算法等与 GM/T 0051—2016 中 7.2.2 密钥标准封装要求不一致，则测试不通过，否则测试通过；
d) 通过对称密钥管理系统提供的密钥停用功能停用密钥，密钥状态改变为“停用”，则测试通过，否则测试不通过；
e) 验证密钥处于停用、销毁、归档等状态时，该密钥不能使用，则测试通过，否则测试不通过。

6.2.5.6 密钥停用

检测要求：

a) 对称密钥管理系统密钥停用应经授权的管理员操作；
b) 当已知密钥被泄露时，对称密钥管理系统应支持“原子密钥停用”功能；（可选）当怀疑密钥被泄露时，可以选择主动停止使用；应能通过安全通道将密钥停用命令下发到被管设备；
c) 被停用的原子密钥在被管设备中不能使用；
d) 对称密钥管理系统设置原子密钥状态为“停用”状态；
e) 被停用的原子密钥不可以启用，应更新或者销毁；
f) 对称密钥管理系统应支持主密钥泄露后密钥管理功能停用，禁止执行一切原子密钥管理流程；
g) 密钥管理停用功能应采用两个或两个以上的管理员同时授权执行；
h) 对称密钥管理系统应提供管理员操作日志审计功能，应采用密码技术保障管理员操作记录的完整性、真实性和不可否认性。

检测方法：

a) 管理员按照 6.2.6.1 身份鉴别方法登录对称密钥管理系统；
b) 执行原子密钥停用操作：对称密钥管理系统能够按照附录 A 中 A.2 格式，通过安全通道将“密钥停用”命令发送到被管设备，则测试通过，否则测试不通过；
c) 被管设备正确执行停用命令并给出响应后，核查对称密钥管理系统能够按照 6.2.5.12 发起密钥查询，从被管设备中获取密钥状态，显示密钥状态为“停用”，则密钥停用成功，其他状态则表示密钥停用失败，则测试通过，否则测试不通过；
d) 管理员通过管理界面选择该密钥，执行“密钥启用”验证该密钥不可被继续使用，则测试通过，否则测试不通过；核查对称密钥管理系统能够按照 GM/T 0051—2016 中 7.2.2 格式，将“密钥启用”命令发送到被管设备，被管设备执行密钥启用命令并返回密钥启用响应；通过调用密钥查询指令，从被管设备中获取密钥状态，显示密钥状态为“在用”，则密钥启用成功，则测试不通

过，否则测试通过；其他状态则表示密钥启用失败，测试通过，否则测试不通过；

e) 验证能够对对称密钥管理系统中已停用密钥执行更新或销毁操作，则测试通过，否则测试不通过；尤其是当系统主密钥泄露后，系统发起密钥管理功能停用，禁止执行一切原子密钥管理流程，则测试通过，否则测试不通过；

f) 管理员通过管理界面/指令执行密钥管理功能停用，系统反馈管理员操作执行结果成功，则测试通过，否则测试不通过；

g) 管理员登录对称密钥管理系统管理界面，执行密钥管理功能停用，系统要求多个管理员登录并获得相应权限，则测试通过，否则测试不通过；

h) 核查管理员操作日志审计功能，可查阅本次执行的密钥停用、启用操作日志并可验证日志的完整性，则管理员操作日志审计功能成功；若无法查阅到本次操作日志，或日志完整性验证失败，则管理员操作日志审计功能失败；查阅本次执行的密钥归档操作日志并验证日志的不可否认性，则管理员操作日志审计功能成功。

6.2.5.7 密钥更新

检测要求：

a) 对称密钥管理系统应具有按密钥更新策略自动进行或按需手动进行“密钥更新”的功能，自动更新应计入系统事件日志，手动更新应进入管理员操作日志；

b) 对称密钥管理系统手动密钥更新应经授权的管理员操作；

c) 对称密钥管理系统应支持“密钥更新”功能；

d) 密钥更新操作应采用一条新的密钥替换当前在用密钥，不应使用在用的其他密钥替换的方式更新。更新操作后应更新密钥标识；

e) 对称密钥管理系统应标记被替换密钥状态为停用状态；

f) 对称密钥管理系统应标记新密钥的密钥状态为待启用状态；

g) 对称密钥管理系统记录管理员操作记录，采用密码技术保障管理员操作记录的完整性、真实性和不可否认性。

检测方法：

a) 通过触发密钥更新策略，由对称密钥管理系统执行相关密钥（若更新密钥为主密钥等，范围包括所有被该密钥加密的密钥或子密钥）更新操作，核查密钥更新操作成功，相关密钥更新时间更新；核查系统审计日志，系统事件日志中记录密钥更新策略触发后的自动更新操作，或管理员操作日志中记录密钥更新策略触发后的手动更新操作，以上步骤测试通过，则密钥更新成功，否则密钥更新失败；

b) 若支持手动执行密钥更新操作，管理员按照 6.2.6.1 身份鉴别方法首先登录对称密钥管理系统；

c) 管理员通过管理界面选择需要更新的密钥，执行原子密钥更新，对称密钥管理系统按照密钥管理策略使用一条新的密钥更新需要被替换的密钥，则测试通过，否则测试不通过；

d) 命令执行成功后，管理员在管理界面上查询新密钥的状态，此时密钥状态为“待启用”，核查被替换密钥的状态，此时密钥状态为“停用”，查询结果与要求相同，则密钥更新成功，否则密钥更新失败；

e) 通过操作日志核查管理员操作日志审计功能，可查阅本次执行的密钥更新操作日志并可验证日志的完整性，则管理员操作日志审计功能成功；若无法查阅到本次操作日志，或日志完整性验证失败，则管理员操作日志审计功能失败；查阅本次执行的密钥归档操作日志并验证日志的不可否认性，则管理员操作日志审计功能成功。

6.2.5.8 密钥归档

检测要求：

a) 对称密钥管理系统密钥归档应经授权的管理员操作；
b) 对称密钥管理系统应支持“原子密钥归档”功能；
c) 过期密钥或者停用密钥可以被归档；
d) 归档密钥不应返回到对称密钥管理系统使用；
e) 应采用密码技术确保归档密钥的机密性和完整性；
f) 对称密钥管理系统应提供管理员操作日志审计功能，应采用密码技术保障管理员操作记录的完整性、真实性和不可否认性。

检测方法：

a) 管理员按照 6.2.6.1 身份鉴别方法登录对称密钥管理系统；
b) 管理员通过管理界面选择需要归档的原子密钥，管理员检查可归档密钥的状态为“过期”、“停用”密钥状态标识，否则密钥归档操作失败；
c) 选择一条需要归档的密钥，执行“原子密钥归档”，能生成密钥归档文件，否则密钥归档失败；
d) 管理员在对称密钥管理系统查阅被归档密钥，若未查询到相关密钥则密钥归档成功，否则归档失败；
e) 审查密钥归档技术文件和密钥归档代码，被核查材料中包含采用密码技术保证归档密钥的机密性和完整性的技术文档说明及代码实现；
f) 通过操作日志核查管理员操作日志审计功能，可查阅本次执行的密钥归档操作日志并可验证日志的完整性，则管理员操作日志审计功能成功；若无法查阅到本次操作日志，或日志完整性验证失败，则管理员操作日志审计功能失败；查阅本次执行的密钥归档操作日志并验证日志的不可否认性，则管理员操作日志审计功能成功。

6.2.5.9 密钥销毁

检测要求：

a) 对称密钥管理系统密钥销毁应经授权的管理员操作；
b) 对称密钥管理系统应支持密钥销毁功能；
c) 对称密钥管理系统应能通过安全通道将密钥销毁命令下发到被管设备；
d) 被管设备中被密钥销毁不可逆，被销毁密钥在被管设备中应不存在；
e) 对称密钥管理系统应提供管理员操作日志审计功能，应采用密码技术保障管理员操作记录的完整性、真实性和不可否认性。

检测方法：

a) 管理员按照 6.2.6.1 身份鉴别方法登录对称密钥管理系统；
b) 管理员在管理界面选择需要销毁的密钥，执行密钥销毁，对称密钥管理系统按照 GM/T 0051—2016 中 7.2.6 格式将“密钥销毁”命令发送到被管设备；接收并按照 GM/T 0051—2016 中 7.2.6 格式解析被管设备密钥销毁响应，销毁成功后，管理员在管理界面上查询该被管设备销毁密钥，显示该密钥状态为“销毁”，则测试通过，否则测试不通过；
c) 对称密钥管理系统发起密钥查询操作，查询密钥状态，显示密钥不存在，则密钥销毁测试通过，其他状态则表示密钥销毁测试不通过；
d) 通过操作日志核查管理员操作日志审计功能。查阅本次执行的密钥归档操作日志并验证日志的完整性，则管理员操作日志审计功能成功；若无法查阅到本次操作日志，或日志完整性验证失败，则管理员操作日志审计功能失败；查阅本次执行的密钥归档操作日志并验证日志的不可

否认性，则管理员操作日志审计功能成功。

6.2.5.10 密钥恢复

检测要求：

a) 对称密钥管理系统应支持用户密钥恢复和司法密钥恢复功能；
b) 对称密钥管理系统密钥恢复应经授权的管理员操作；
c) 对称密钥管理系统应支持司法密钥恢复员角色，用于司法密钥恢复；
d) 司法密钥恢复应采用管理员与司法密钥恢复员同时授权执行；
e) 用户密钥恢复应支持恢复用户自己的在用密钥，司法密钥恢复应支持恢复所有的在用密钥、历史密钥和归档密钥；
f) 用户恢复的密钥应能分发到用户的被管设备；司法恢复的密钥仅恢复到载体；
g) 司法密钥恢复员身份认证介质与密钥恢复载体应为同一智能密码钥匙；
h) 司法密钥恢复应在对称密钥管理系统密码设备中执行密钥转保护；
i) 对称密钥管理系统应提供管理员操作日志审计功能，应采用密码技术保障管理员操作记录的完整性、真实性和不可否认性。

检测方法：

a) 管理员按照 6.2.6.1 身份鉴别方法登录对称密钥管理系统；
b) 用户恢复密钥检测：管理员在对称密钥管理系统选择需要恢复的密钥，执行“密钥恢复”操作，能够将用户的在用密钥恢复到一台没有密钥的设备中，密钥恢复成功，则测试通过，否则测试不通过；按照 6.2.5.4 密钥分发和 6.2.5.12 密钥查询，执行密钥分发和密钥查询，被恢复的密钥能正确分发到被管设备并可查询，则测试通过，否则测试不通过；
c) 司法密钥恢复检测：管理员通过管理界面选择执行司法密钥恢复操作，系统要求插入司法恢复员认证介质并执行验证，验证通过获取司法密钥恢复员权限，则测试通过，否则测试不通过，否则司法密钥恢复操作失败；从对称密钥管理系统密钥库中选择需要恢复的密钥，或上传密钥归档文件，执行司法密钥恢复，密钥恢复成功，系统反馈密钥正确写入司法恢复员智能密码钥匙，则测试通过，否则测试不通过，若密钥恢复失败，系统反馈密钥写入司法恢复员智能密码钥匙失败，则测试通过，否则测试不通过；
d) 从归档文件中司法密钥恢复，在对称密钥管理系统查询该密钥显示密钥不存在，则归档密钥的司法密钥恢复通过检测，否则处理过程不合规，不通过检测；
e) 审查司法恢复过程代码，司法密钥恢复过程密钥密文转保护在对称密钥管理系统密码设备内部完成，采用司法恢复员公钥对密钥执行数字信封保护后，写入密钥载体；
f) 通过操作日志核查管理员操作日志审计功能。可查阅本次执行的密钥恢复操作日志并可验证日志的完整性，则管理员操作日志审计功能成功；若无法查阅到本次操作日志，或日志完整性验证失败，则管理员操作日志审计功能失败；查阅本次执行的密钥归档操作日志并验证日志的不可否认性，则管理员操作日志审计功能成功。

6.2.5.11 密钥封装

检测要求：

a) 应能提供原子密钥使用标准封装结构进行存储和分发，密钥封装格式符合 GM/T 0051—2016 中 7.2.2 的标准密钥封装格式；
b) 应能在存储原子密钥时使用主密钥进行转加密，转加密应在密码设备内部处理；
c) 应能在分发原子密钥时使用分发保护密钥进行转加密，转加密应在密码设备内部处理。

检测方法：

a） 核查密钥库中原子密钥，封装结构符合 GM/T 0051—2016 中 7.2.2 的标准密钥封装格式，或通过密钥申请指令等，解析、验证，封装结构正确解封装，则测试通过，否则测试不通过；

b） 审查原子密钥存储转加密接口代码，在密码设备内部完成原子密钥密文的转加密保护，正确解析密钥生成装置输出的原子密钥密文，并用主密钥转加密输出，则测试通过，否则测试不通过；

c） 原子密钥分发转加密接口代码，在密码设备内部完成原子密钥密文的转加密保护，并完成导入主密钥保护的原子密钥并用分发保护密钥转加密输出，正确解封装并转加密输出，则测试通过，否则测试不通过。

6.2.5.12 密钥查询

检测要求：

a） 应能在对称密钥管理系统提出密钥查询申请时对被管设备进行密钥查询操作；

b） 密钥查询管理指令应按照 GM/T 0051—2016 中 7.2.3.1 的密钥管理指令 PDU 实现，指令代码及密钥查询格式按 A.1 实现；

c） 密钥查询指令应采用安全通道进行传递。

检测方法：

a） 管理员按照 6.2.6.1 身份鉴别方法登录对称密钥管理系统；

b） 对称密钥管理系统通过安全通道将密钥查询指令发送到被管设备，被管设备正确解析密钥查询并返回查询结果符合预期，则测试通过，否则测试不通过。

6.2.6 管理功能检测

6.2.6.1 身份鉴别检测

检测要求：

a） 应通过身份鉴别后，管理人员、操作人员、审计人员才能进行相应的授权操作；

b） 应使用密码技术进行身份鉴别。

检测方法：

a） 以正确的方式登录管理人员、操作人员或审计人员的操作界面，系统准入，显示授权管理页面；

b） 以错误的方式登录管理人员、操作人员或审计人员的操作界面，系统拒绝，并给出错误信息反馈；

c） 核查身份鉴别协议，协议采用动态口令机制、消息鉴别码（MAC）机制或数字签名机制等密码技术对人员进行身份鉴别，则测试通过，否则测试不通过。

6.2.6.2 策略配置检测

检测要求：

a） 应提供密钥生成策略配置，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，由对称密钥管理系统根据密钥管理应用需求制定；

b） 应提供密钥分发策略配置，配置包括一系列组合条件，条件应按照 GM/T 0051—2016 中 6.6.2.4 要求实现；

c） 分发策略管理和更新策略应按照 GM/T 0051—2016 中 5.2.5、6.5.2、6.5.4 和 6.6.2.4 要求实现。

检测方法：

a) 核查密钥生成和密钥分发策略配置内容符合要求内容，则测试通过，否则测试不通过；

b) 核查密钥生成策略触发后原子密钥经由密钥生成装置生成，并核查生成的原子密钥是否与配置策略要求的一致；

c) 验证密钥分发策略功能，具备在线分发策略或离线分发策略，分发策略触发后，原子密钥按照在线密钥分发协议或介质安全分发协议分发给被管设备；

d) 通过触发密钥更新策略，由对称密钥管理系统执行相关密钥（若更新密钥为主密钥等，范围包括所有被该密钥加密的密钥或子密钥）更新操作，核查密钥更新操作成功，相关密钥更新时间更新；核查系统审计日志，系统事件日志中记录密钥更新策略触发后的自动更新操作，或管理员操作日志中记录密钥更新策略触发后的手动更新操作，以上步骤测试通过，则密钥更新成功，否则密钥更新失败。

6.2.7 系统审计检测

检测要求：

a) 应通过审计员进入审计管理页面，审计员具有对涉及对称密钥管理系统安全的事件、人员操作的行为进行审计和监督的权限；

b) 应能提供主动运行事件的审计管理界面，能对事件发生的时间、事件的操作者、操作类型及操作结果等信息进行审计，审计应能对记录的签名进行验证，审计过的记录应有明显标记；

c) 应能提供被动运行事件的审计管理界面，能对事件发生的时间、模块类型、模块策略设置、服务状态等信息进行审计，审计应能对记录的签名进行验签，审计过的记录应有明显标记；

d) 审计数据应能导出并不能被篡改，且审计数据的导出采用密码技术保障数据的完整性。

检测方法：

a) 审计员按照 6.2.6.1 身份鉴别方法登录对称密钥管理系统；

b) 在主动运行事件审计界面，对事件发生的时间、事件的操作者、操作类型及操作结果、记录的签名等信息进行审计操作，结果符合检测要求 b)的要求，则测试通过，否则测试不通过；

c) 在被动运行事件审计界面，对事件发生的时间、模块类型、模块策略设置、服务状态、记录的签名等信息进行审计操作，结果符合检测要求 c)的要求，则测试通过，否则测试不通过；

d) 导出审计过的审计记录进行修改，再重新导入系统进行审计，结果符合检测要求 d)的要求，则测试通过，否则测试不通过。审计数据的导出采用密码技术保障其完整性，通过代码审查及审计数据导出格式，验证导出审计数据的完整性成功，则测试通过，否则测试不通过。

6.2.8 安全通道检测

检测要求：

a) 对称密钥管理系统应能与被管设备建立安全通道；安全通道协议按照 GM/T 0050 中安全通道协议相关要求实现；安全通道消息按照 GM/T 0050 中安全通道消息相关要求实现；

b) 当操作员的管理终端与对称密钥管理系统之间进行远程数据通讯时，应采用安全通道进行数据传输，如 TLCP 协议。

检测方法：

a) 被管设备与对称密钥管理系统建立安全通道，能建立成功，且安全通道协议、消息实现正确（根据 GM/T 0050 中安全通道协议的设计，安全通道由被管设备主动发起），则测试通过，否则测试不通过；

b) 管理终端与对称密钥管理系统之间采用传输层密码协议（TLCP）建立安全通道时，验证安全通道建立符合 GB/T 38636 的要求，则测试通过，否则测试不通过。

6.3 接口检测

6.3.1 应用指令检测

6.3.1.1 分发保护密钥协商指令

检测要求：

a) 应能向被管设备协商分发保护密钥；

b) 分发保护协商应在安全通道建立、密钥分发、密钥申请后由对称密钥管理系统主动触发；

c) 分发保护密钥协商指令格式按照 GM/T 0051—2016 中 7.2.1 和 7.2.4 的要求实现。

检测方法：

a) 检测报文数据格式，分发保护密钥协商指令格式符合 GM/T 0051—2016 中 7.2.1 和 7.2.4 的要求，则测试通过，否则测试不通过；

b) 对称密钥管理系统与被管设备建立安全通道后，对称密钥管理系统向被管设备下发分发保护密钥协商指令，能成功完成分发保护密钥协商，则测试通过，否则测试不通过。

6.3.1.2 密钥分发

检测要求：

a) 应能向被管设备分发密钥；

b) 密钥分发指令格式按照 GM/T 0051—2016 中 7.2.1、7.2.5 的要求实现；密钥封装格式按照 GM/T 0051—2016 中 7.2.2 的要求实现。

检测方法：

a) 检测报文数据格式，密钥分发指令格式符合 GM/T 0051—2016 中 7.2.1、7.2.5 的要求，则测试通过，否则测试不通过；检测报文数据格式，密钥封装格式符合 GM/T 0051—2016 中 7.2.2 的要求，则测试通过，否则测试不通过；

b) 对称密钥管理系统与被管设备建立安全通道后，对称密钥管理系统向被管设备下发密钥分发指令，能成功完成密钥分发，则测试通过，否则测试不通过。

6.3.1.3 密钥销毁

检测要求：

a) 对称密钥管理系统应可以对密钥进行销毁，要求从对称密钥管理系统及被管设备中销毁待销毁密钥；

b) 销毁结果要求不可逆，不可从销毁结果中恢复原密钥；

c) 密钥销毁指令格式按照 GM/T 0051—2016 中 7.2.1 和 7.2.6 的要求实现。

检测方法：

a) 检测报文数据格式，指令格式符合 GM/T 0051—2016 中 7.2.1 和 7.2.6 的要求，则测试通过，否则测试不通过；

b) 对称密钥管理系统选择可销毁密钥，通过安全通道将销毁指令发送到被管设备，被管设备成功销毁密钥，并返回响应，响应成功或失败符合预期，则测试通过，否则测试不通过；对使用中的密钥，执行密钥销毁指令后，对称密钥管理系统无法查询被销毁密钥，则测试通过，否则测试不通过；

c) 核查对称密钥管理系统功能中不存在对已销毁密钥实施恢复的方法，则测试通过，否则测试不通过。

6.3.1.4 密钥启用

检测要求：

a) 对称密钥管理系统应能按密钥编号启用被管设备中的密钥；
b) 对称密钥管理系统应能启用被管设备中全部密钥；
c) 密钥启用指令格式按照 GM/T 0051—2016 中 7.2.1 和 7.2.7 的要求实现。

检测方法：

a) 检测报文数据格式，启用被管设备中密钥的请求和响应指令格式符合 GM/T 0051—2016 中 7.2.1 和 7.2.6 的要求，则测试通过，否则测试不通过；
b) 对已分发未启用的密钥，按密钥编号启用被管设备中的密钥，能成功完成密钥启用，被管设备中指定密钥处于可用状态，则测试通过，否则测试不通过；
c) 对已分发未启用的密钥，所有密钥执行启用指令后，能够成功启用被管设备所有密钥并处于可用状态，可以正常使用，则测试通过，否则测试不通过。

6.3.1.5 密钥申请

检测要求：

a) 被管设备应支持按照密钥编号向对称密钥管理系统申请更新当前密码设备中的密钥；
b) 密钥申请指令格式按照 GM/T 0051—2016 中 7.2.8 的要求实现。

检测方法：

a) 检测报文数据格式，被管设备的密钥申请请求和响应指令格式符合 GM/T 0051—2016 中 7.2.8 的要求，则测试通过，否则测试不通过；
b) 被管设备指定不同的密钥类型，向对称密钥管理系统发起密钥申请请求，通过核查对称密钥管理系统密钥库是否新增待分发密钥、系统审计日志、检测报文数据等方式，验证对称密钥管理系统收到密钥申请并成功返回响应，则测试通过，否则测试不通过。

6.3.1.6 密钥查询

检测要求：

a) 对称密钥管理系统应能按照密钥编号查询指定被管设备中的密钥；
b) 对称密钥管理系统应能查询密钥库中的密钥；
c) 向被管设备发送密钥查询指令格式按照 A.1 的要求实现。

检测方法：

a) 检测报文数据格式，对称密钥管理系统向被管设备发起的密钥查询请求和响应指令格式符合 A.1 的要求，则测试通过，否则测试不通过；
b) 对称密钥管理系统选择一条被管设备在用密钥，执行密钥查询，对称密钥管理系统显示查询结果符合预期，则测试通过，否则测试不通过；
c) 指定步骤 b)中选择的密钥，在对称密钥管理系统在用密钥库中执行密钥查询，对称密钥管理系统显示查询结果符合预期，则测试通过，否则测试不通过。

6.3.1.7 密钥停用

检测要求：

a) 对称密钥管理系统应能够按照密钥编号停用指定被管设备中的密钥，应能够停用被管设备中的所有密钥；
b) 向被管设备发送密钥停用指令格式按照 A.2 的要求实现。

检测方法：

a） 检测报文数据格式，对称密钥管理系统向被管设备发起的密钥停用请求和响应指令格式符合A.2的要求，则测试通过，否则测试不通过；

b） 对称密钥管理系统选择一条被管设备在用密钥，执行密钥停用，指令完成后，对称密钥管理系统查询被管设备中该密钥状态为停用，则测试通过，否则测试不通过；对被管设备所有密钥执行密钥停用，指令完成后，对称密钥管理系统查询被管设备中所有密钥状态为停用，则测试通过，否则测试不通过。

6.3.2 管理接口检测

6.3.2.1 密钥生成装置接口

检测要求：

a） 密钥生成装置对外提供API生成原子密钥接口，接口应按照GM/T 0051—2016中7.3.1要求实现；

b） 签名算法标识应按照GB/T 33560要求实现；数字签名及会话密钥密文数据格式应按照GM/T 0018要求实现。

检测方法：

a） 检测报文数据格式，密钥生成装置接口API符合GM/T 0051—2016中7.3.1要求，签名算法标识符合GB/T 33560要求，数字签名及会话密钥密文数据格式符合GM/T 0018要求；

b） 调用密钥生成装置接口生成原子密钥，并返回成功，则测试通过，否则测试不通过。

6.3.2.2 密钥管理指令发送接口

检测要求：

a） 对称密钥管理系统与被管设备密钥管理代理通信应按照GM/T 0051—2016中7.2对称密钥管理应用指令要求实现；

b） 对称密钥管理系统应调用GM/T 0050中安全通道发送数据的要求发送函数，密钥管理指令赋值在数据发送字段中进行密钥管理指令发送。

检测方法：

a） 审查对称密钥管理系统代码，核查是否调用GM/T 0050中安全通道发送数据要求的初始化函数获得设备管理安全通道句柄，核查是否调用数据发送函数发送密钥管理数据，核查是否调用退出函数释放设备管理句柄，符合预期则测试通过，否则测试不通过；

b） 被管设备密钥管理代理与对称密钥管理系统进行密钥管理指令交互，并返回成功，则测试通过，否则测试不通过。

6.4 性能检测

检测要求：

a） 密钥格式封装性能，测试按照GM/T 0051—2016中7.2.2要求的标准密钥封装格式性能；

b） 密钥分发性能，测试对称密钥管理系统向被管设备密钥管理代理分发性能；

c） 容量性能，测试对称密钥管理系统可存储的密钥的最大数量。

检测方法：

a） 创建密钥格式封装性能测试用例，密钥管理代理向对称密钥管理系统发送GM/T 0051—2016中7.2.8密钥申请指令，持续时间不少于10 s，线程数为10，通过密钥申请的方式进行密钥格式封装性能检测，并输出性能指标（单位：次/s）；

b) 创建密钥分发性能测试用例，对称密钥管理系统调用 GM/T 0050 中安全通道的数据发送函数，向被管设备发送 GM/T 0051—2016 中 7.2.5 密钥分发指令，持续时间不少于 10 s，线程数为 10，进行密钥分发性能检测，并输出性能指标（单位：次/s）；

c) 创建容量测试用例，测试对称密钥管理系统存储密钥的最大容量，容量超过一定数量时，对称密钥管理系统无法响应密钥管理代理发送的密钥申请指令，则输出性能指标（单位：条）。

7 送检技术文档要求

研制单位按照商用密码检测认证机构要求提交相关文档资料，作为基于密码设备管理的对称密钥管理系统的检测依据。

8 判定规则

本文件中，除 6.4 以外的各项检测中，其任意一项检测结果为测试不通过，判定为产品不合格。

附 录 A
（规范性）
密钥管理扩展指令

A.1 密钥查询

用于对称密钥管理系统向被管设备查询指定密钥编号的密钥是否存在。密钥查询指令请求 PDU 应与图 A.1 相符。

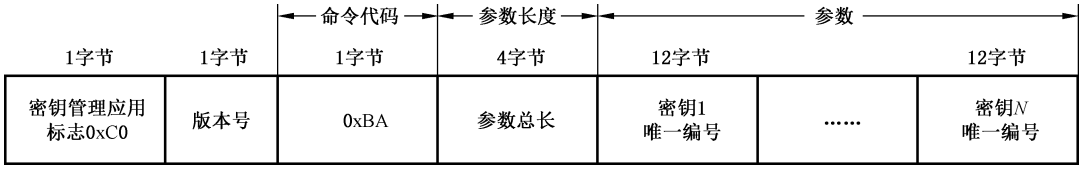

图 A.1 密钥查询请求

密钥查询指令中的密钥唯一编号是指查询密钥的唯一标识。密钥查询指令响应 PDU 应与图 A.2 相符。

图 A.2 密钥查询响应

A.2 密钥停用

用于对称密钥管理系统停用被管设备中的全部密钥或某些密钥。密钥停用指令请求 PDU 应与图 A.3 相符。

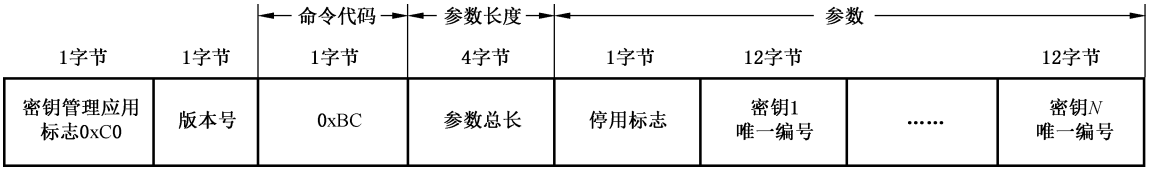

图 A.3 密钥停用请求

密钥停用指令响应 PDU 应与图 A.4 相符。

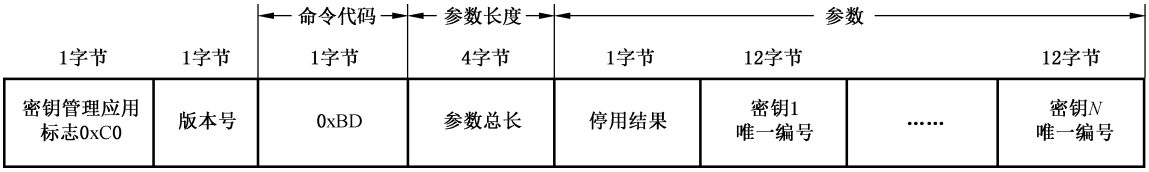

图 A.4 密钥停用响应

中华人民共和国密码
行业标准
对称密钥管理系统检测规范
GM/T 0143—2024
*
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)
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 1.75　字数 36 千字
2025年6月第1版　2025年6月第1次印刷
*
书号:155066·2-39096　定价 49.00 元

GM/T 0143-2024