ICS 35.040
L 80
备案号：

中华人民共和国密码行业标准

GM/T XXXX—XXXX

对称密钥管理系统技术规范

Specifications of

symmetric key management system technology

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

××××-××-××发布　　××××-××-××实施

国家密码管理局 发布

目　次

前　言

本标准依据 GB/T1.1—2009 给出的规则起草。

本规范由密码行业标准化技术委员会提出并归口。

本规范的附录 A 是规范性附录。

本规范规定了对称密钥管理体系及相关管理技术，规定了对称密钥管理系统的体系结构、管理中心的基本功能、管理协议和相应的系统设计安全技术要求，为对称密钥管理系统的研制和开发提供指导和依据。

本规范凡涉及密码算法相关内容，按国家有关法规实施。

本规范起草单位：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、济南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。

本规范主要起草人：刘平、王妮娜、李玉峰、徐强、李元正、谭武征、柳增寿等。

本规范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。

引　言

本规范依据《密码设备管理技术规范》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，为符合《密码设备管理技术规范》的商用密码设备提供统一分发对称密钥的密管系统技术要求。本规范采用的密钥管理安全通道，依据《密码设备管理技术规范》中的管理应用接口建立，相关内容请参考《密码设备管理技术规范》。

对称密钥管理系统技术规范

1 范围

本规范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。

本规范适用于商用对称密钥管理系统的研制、建设、运行及管理。

本规范采用《密码设备管理技术规范》中的安全通道技术，需使用《密码设备管理技术规范》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 AAAAA 密码设备管理技术规范

GM/T 0006 密码应用标识规范

GM/T 0005 随机性检测规范

3 术语

下列术语和定义适用于本规范。

3.1.

对称密钥管理系统 symmetry 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，根据管理策略，接收本系统相关的业务密钥。

3.6.

安全通道 security tunnel

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 cryptography device management platform

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《密码设备管理技术规范》，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 cryptography device management API

由《密码设备管理技术规范》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 distribution protecting key

安全通道中保护一次密钥分发数据的临时性密钥。

3.10.

分发保护密钥协商 distribution protecting key agreement

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

被管设备私有封装格式的密钥。

3.12.

专用密钥产生装置 customized key generator

为特定密码应用系统、特定型号被管设备产生原子密钥的硬件装置。

3.13.

通用密钥产生装置 general key generator

为不同被管设备产生密钥数据为随机数的原子密钥的硬件装置。

3.14.

密钥格式配置文件 general key config profile

专用密钥产生装置和通用密钥产生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部分：

CA：证书认证中心（Certification Authority）

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

5 对称密钥管理安全要求

5.1 系统安全要求

——密码设备应经过密码主管部门认证；

——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；

——密管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 密钥产生

密钥和密钥分量需使用物理噪声源产生，随机性检测需满足国家密码管理局《随机性检测规范》的要求。

5.2.2 密钥存储和备份

密钥存储需要确保机密性，防止未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需隔离存储于不同介质中，由不同的管理人员分别持有。

——已加密密钥

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，需确保经过授权才能访问。

密钥备份也需确保机密性，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，应该采用分量传递或口令保护的方式。

——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；
- 密钥分发和加载过程应使用传输介质与管理口令双因素保护。

——已加密密钥

已加密密钥可以通过网络分发和加载。

- 已加密密钥的分发需防止密钥篡改和密钥替换。

5.2.4 密钥使用

密钥需要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

密钥管理系统需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，应能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转加密，不由密钥管理中心负责。

——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；

——不能增加其它密钥的泄露风险。

5.2.6 密钥归档

当密钥超过使用期限，或不再使用，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，可以对密钥进行删除，要求从各种已用的介质中删除待销毁密钥。删除结果要求不可逆，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：

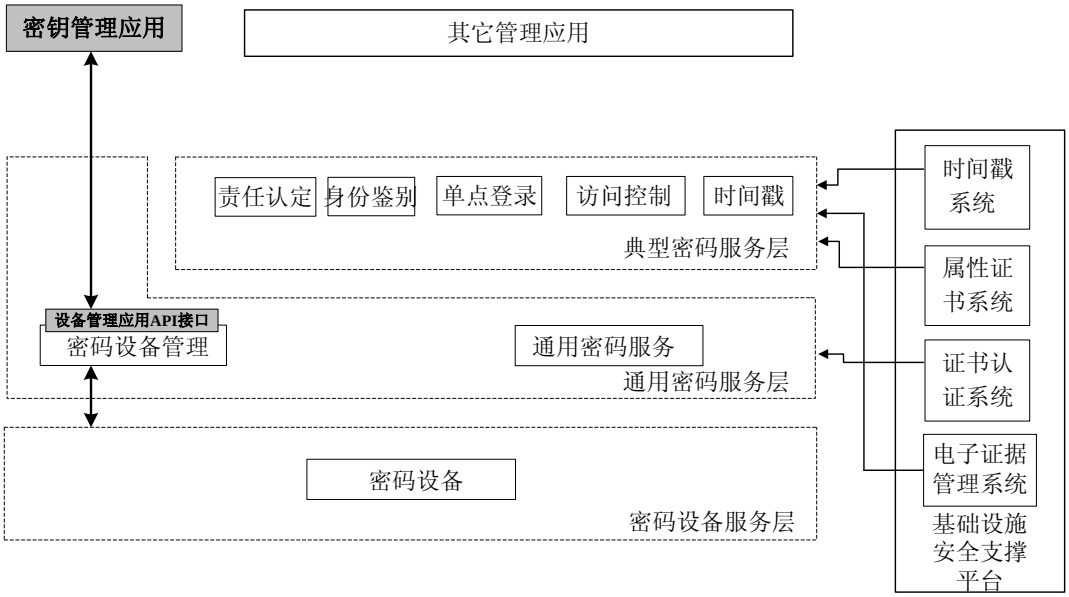

图 1 密钥管理应用技术体系框架

密钥管理应用与被管设备间的密钥管理协议，通过《密码设备管理技术规范》定义的安全通道承载。密钥管理系统调用《密码设备管理技术规范》第 9.1 节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《密码设备管理技术规范》第 9.8 节的安全通道数据发送接口，将密钥管理消息封装在安全通道消息 PDU 中发送至被管密码设备。

本规范规定的技术范围与《密码设备管理技术规范》技术范围的关系如图 1-b 所示：

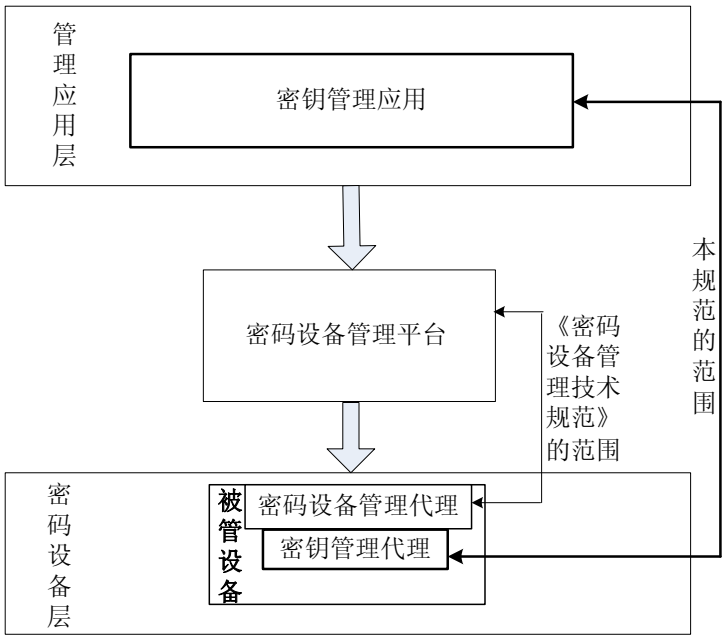

图 2 密钥管理应用与密码设备管理平台的关系

6.2 系统技术框架

密钥管理系统组成框架如图 3 所示：

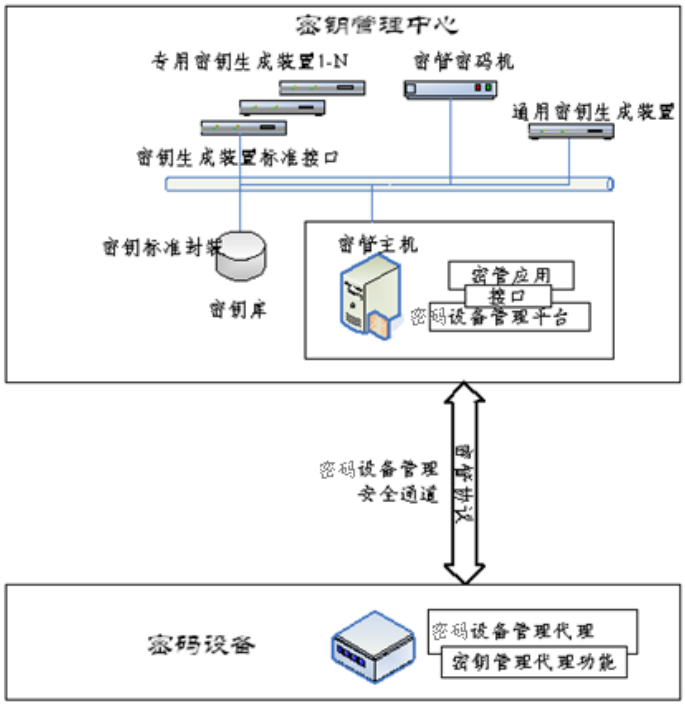

图 3 密钥管理系统组成框架

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。

6.3 管理范围

本规范构建商用密码应用领域统一密钥管理平台应用，对支持本规范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。

本规范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）不在本规范管理范围之内。

6.4 系统功能结构

密钥管理系统主要由核心密管、密钥生成管理、密钥分发管理、备份 / 恢复管理、身份认证、审计管理、密管代理、密钥导入等模块组成。

密钥管理系统功能结构如图 4 所示：

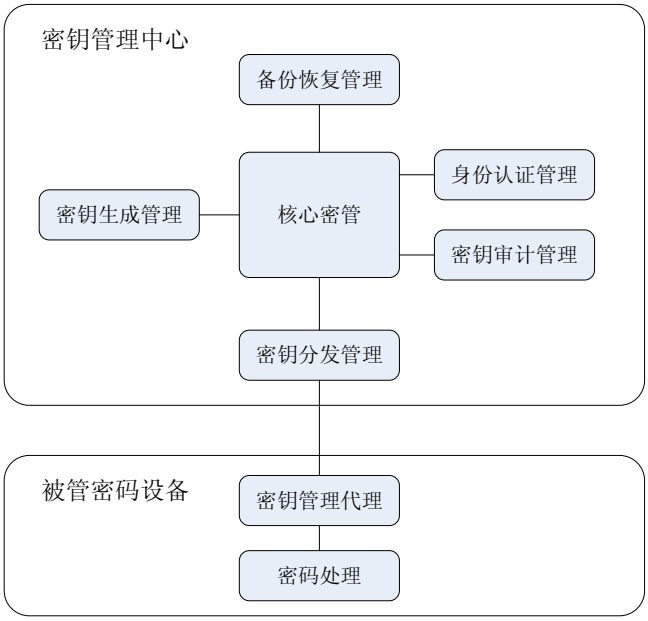

图 4 密钥管理系统功能结构

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，同时需具备身份认证、审计管理功能，以确保管理系统的安全。

6.5.2 核心密管

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

密钥产生策略的配置包括是否使用专用密钥产生装置、密钥产生的数量及长度要求等，由密管系统根据密管应用需求制定。

密钥分发策略的配置包括一系列组合条件，参见下文 6.5.3.4 节。

其它策略的配置包括密钥查询方式、通用密钥产生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

本规范以通用密钥产生装置和专用密钥产生装置分别产生通用格式密钥和专用格式密钥。

通用密钥产生装置生成随机密钥，核心密管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。

专用密钥产生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，只能通过专用密钥产生装置生成。

密钥产生由密钥产生策略触发，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规范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 密管代理

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。

被管设备的密管代理由设备厂商定制，应支持本规范规定的密钥分发协议，支持在线接收或离线介质接收。

6.5.6 密钥备份/恢复/归档

为增强系统的容灾性，密管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。

密管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，依据密管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，由密管系统进行归档保存，且需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

本规范仅提出密钥管理系统及密钥管理功能模块主要功能模型的设计指导。密钥管理系统在实现过程中，应根据具体应用需求进行具体设计。

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；

——需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；

——系统在实现密钥管理功能的同时，必须充分考虑系统本身的安全性。必须具备安全登录、访问控制、加密传输的功能；

——各子系统之间的通信采用基于身份验证机制的安全通信协议；

——明文密钥不得导出硬件密钥设备，加密转换必须在硬件密码设备中完成；

——密码运算必须在硬件密码设备中完成；

——审计文件采用统一的格式传递和存储；

——系统可为多个被管系统提供业务密钥服务。

6.6.2 密钥管理端设计要求

6.6.2.1 核心密管模块

应满足以下功能要求：

——制定密钥产生策略及密钥分发策略；

——协调调度各主要密管模块；

——导入适用于通用密钥生成装置的密钥结构文件。

——查询密钥状态；

——接收业务系统、被管设备的密钥申请；

——封装原子密钥为标准格式并存储于密钥库；

6.6.2.2 密钥产生模块

密钥生成模块应满足以下要求：

——能够为多个被管系统提供业务密钥；

——能够产生高质量随机数、对称密钥；

——密钥生成装置为硬件设备；

——支持以密钥载体方式将外部密钥导入至密管系统；

——必须以加密方式导出密钥生成装置的密钥，明文密钥不可出硬件设备；

——密钥库中存储的密钥必须是已加密的。

不同密码体制的密钥由相应的通用密钥生成装置或专用密钥生成装置生成，所生成密钥为密管系统的原子密钥。

密钥生成装置接口参见 7.2 节。

通用密钥生成装置，需由密钥管理端的核心密管模块按照密钥格式配置文件（参见附录 C）中的原子密钥模板，调用通用密钥生成装置产生要求长度的随机数，填充在原子密钥模板的密钥数据项中。

原子密钥经过密管密码设备与密钥生成装置协商的临时会话密钥加密后导入密管密码机。临时会话密钥的协商采用《密码设备管理技术规范》附录 B 规定的身份验证和密钥协商协议。

被临时密钥加密的原子密钥在密管系统中转换为用本地存储密钥加密， 7.1.1 节标准格式对原子密钥密文进行封装，最后存储于密管中心的密钥库中。

密钥分发时，密管中心与被管设备在安全通道中以本规范定义的专用协议协商分发保护密钥（参见第 7 章），并将密钥库中由本地存储密钥加密的待分发密钥封装转换为由分发保护密钥加密的密钥封装。

密钥加密转换只能在密码设备内进行，要求明文密钥不可导出密码设备。

密钥生成装置的密钥产生接口、分发保护密钥协商接口参见本规范第 7.1 和 7.2 节。

6.6.2.3 密钥封装模块

应满足以下要求：

——能够将密钥生成装置生成的个性化密钥，封装为密钥管理系统标准格式；

——密钥封装的过程不应暴露明文密钥。

密钥封装标准数据结构参见本规范第 7.1 节。

6.6.2.4 密钥分发模块

应满足以下功能要求：

——密钥分发策略管理

管理可组合密钥分发条件的策略簇，包括：

- 分发时间
- 密码产生装置编号
- 密钥类型
- 密钥数量
- 被管设备型号或名称

- 被管设备唯一编号
- 被管设备 IP 地址
- 密管设备所属管理系统
- 密管设备使用单位
- 分发未成功时的处理策略等其它策略。

——满足密钥分发的安全性要求，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

——支持本规范定义的标准密钥分发协议；

——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、密钥枪、USBKEY 等载体离线分发；

——密钥分发格式对于离线、在线分发方式应保持一致；

——支持密钥更新策略，满足密钥的更新需求，包括：

- 根据密钥属性划分的生命周期更新策略。密钥属性包括密钥类型、密钥所属系统、密钥所属设备等，参见 7.1.1 密钥标准封装。
- 根据密钥泄露或威胁等级提高时的特殊情况制定的应急更新策略。

本规范利用设备管理平台的安全通道技术实现密钥安全分发。

设备管理平台与被管设备以设备管理协议建立安全通道，密钥管理应用与被管设备通过安全通道协商本次分发的会话密钥。

密钥管理应用从数据库中取出被主密钥加密的待分发密钥，调用密管密码设备将主密钥加密的原子密钥转换为本次会话密钥加密，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。

分发保护密钥协商过程参见第 7.1.3 节。

6.6.2.5 密钥库存储管理模块

密钥库管理模块负责密钥的存储管理，按照其存储的密钥的状态，密钥库分为在用库和历史库。在用库存放当前使用的密钥，历史库存储过期和撤消密钥。

密钥库存储管理模块应满足以下要求：

——密钥库中的密钥必须加密存放；

——密钥封装为标准封装，在用库记录还需要包含产生时间、有效期等标志，历史库记录还需要包含作废时间等标志；

——支持查询密钥功能；

——能够对在用密钥库中的密钥进行定期检查，将超过有效期的或被撤销的密钥转移到历史密钥库；

——对历史密钥库中的密钥进行处理，将超过规定保留期的密钥转移到规定载体；

6.6.2.6 密码服务模块

应满足以下功能要求：

——密码算法必须在硬件密码设备中运行；

——配置国家密码主管部门批准的标准对称算法、非对称算法、数据摘要算法；

——提供随机数生产、对称密码算法数据加解密运算、非对称密码算法数据加解密运算、数字签名和签名验证运算、密钥协商运算、数据摘要运算、密钥安全导入导出等密码服务。

6.6.2.7 密钥恢复模块

应满足以下功能要求：

——接收与审查用户的恢复密钥申请，依据安全策略进行处理；

——接收与审查司法机关的恢复密钥申请，依据安全策略进行处理；

可选安全策略：

- 用户密钥恢复

由被管系统所属单位向密管系统提出业务密钥恢复请求。通过密管系统审查后，将所需密钥从在用密钥库中取出，以在线或离线密钥分发方式、标准密钥分发流程向被管设备恢复业务密钥。

- 司法密钥恢复

允许进行司法恢复的取证部门，应设置司法恢复专职人员进行司法操作。专职人员需持取证部门的书面申请、介绍信等材料，通过密管系统书面审查后，在密钥管理中心进行注册，根据密钥管理系统身份认证的技术要求为其注册证书、指纹或口令等，作为密钥管理中心的工作角色进行管理。

司法密钥恢复时，应由注册过的司法恢复专职人员与密钥管理中心具备相应权限的操作人员共同操作。司法恢复专职人员需提供其基于证书的密钥载体（如 USBKEY），密钥管理系统根据要求从密钥库中取出指定业务密钥，在密管中心密码设备中解密，同时使用司法恢复专职人员的公钥，为指定业务密钥作数字信封，将数字信封加载至司法恢复专职人员的密钥载体中。整个密钥恢复过程，明文密钥不出密码机，最后以数字信封加密导出至密钥载体，由司法恢复专职人员带回相应单位。

6.6.2.8 审计模块

应满足以下功能要求：

——对密钥产生、密钥存储、密钥分发、核心密管模块、身份认证、密码服务等模块进行事件审计、统计和分析；

——记录用户主动运行事件，包括用户名称、内容、时间、结果等。

——记录模块中间运行事件，包括触发事件名称、内容、时间、结果等。

——记录服务器状态；

——记录系统策略设置；

——审计记录不能进行修改；

——审计记录支持导出备份；

——必须保障审计记录的完整性。

6.6.3 传输通道设计要求

遵循 GM/T AAAAA《密码设备管理技术规范》。

6.6.4 被管设备端的设计要求

内嵌密钥管理代理软件模块，应满足以下功能要求：

——以代理软件的方式驻留于被管密码设备；

——与设备管理结合，根据密钥状态支持密钥申请主动上报；

——支持标准密钥管理协议的接收、解析、处理，将标准封装的密钥解析为密码设备专用原子密钥，执行对应密钥管理操作；

——对于已有密码设备，支持专用密钥管理协议的转换和适配，将标准密钥管理指令转换为原有密钥管理代理可识别的操作指令并执行；

——能够识别在线管理和离线管理两种模式，支持密码设备要求的物理导入接口，如以

太网、通用密钥加载设备等；

在设备管理代理中内嵌密钥管理代理功能。利用设备管理系统建立的安全通道传输密钥管理指令，同时保障密钥管理指令的安全性和密钥数据的安全性。密钥管理指令参见 7.1 节。

设备管理代理接收到密钥管理指令后，将密钥管理指令转交密钥管理代理模块进行处理，解析并执行具体的密钥操作。

6.6.5 系统初始化

本规范密钥管理系统建立在《密码设备管理技术规范》的设备管理平台之上，密管中心及被管设备遵循密码设备管理平台的证书分发流程，具体流程参考 GM/T AAAAA《密码设备管理技术规范》第 5.7 节“注册流程”。

7 指令及接口

指令中加密算法采用国家密码管理部门规定的算法，如 SM4 等对称密钥算法，CBC 模式，初始 IV 为全零。待加密数据必须填充，填充方法为：

第一个字节为 0x80，其后为若干 0x00，填充到分组长度整数倍。

指令采用网络字节序传输。

7.1 指令

密钥管理应用指令作为设备管理平台指令的消息 PDU，填充在设备管理平台指令中发送，如图 5 所示（参见 GM/T AAAAA《密码设备管理技术规范》）：

图 5 密钥管理指令在设备管理安全通道消息中的位置和格式

本规范定义密钥管理应用的应用标识为：0xC0。

密钥管理应用指令处理流程如图 6 所示：

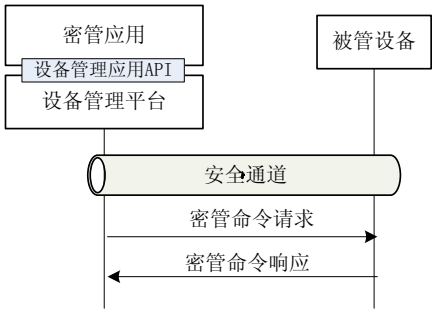

图 6 密管指令流程

——密管应用根据管理需要形成具体的密管指令，其中密钥使用标准封装结构；

——密钥管理应用调用 GM/T AAAAA《密码设备管理技术规范》9.8 节 SMF_SecTunnelSendData 函数，将密钥管理指令赋值在 sendData 字段，自动被填充在设备管理平台指令的消息 PDU 中并通过安全通道发送密管指令；

——设备管理代理解析操作包类型为 0xC0 时，将数据包转交给密钥管理代理解析处理；

7.1.1 密钥标准封装

被管设备原子使用标准封装结构进行存储和分发。密钥封装格式参见表 1：

表1 标准密钥封装格式

序号	参数内容	名称	类型	长度（字节）	说明
1	密钥唯一标识	KeyID	SGD_UINT32	8	密钥在密钥管理系统中的唯一标识，具体构成参见图 6。
2	密钥类型	KeyType	SGD_UINT32	4 字节	所产生的密钥种类，密钥标识 OID 遵循 GM/T 0006《密码应用标识规范》。
3	密钥长度	AtomKeyLen	SGD_UINT32	4	加密后的原子密钥长度。
4	原子密钥	AtomKeySet	SGD_UCHAR	AtomKeyLen	由密钥产生装置生成的密钥。存储时由密管密码机主密钥加密，分发时由分发保护密钥加密。
5	校验算法标识	ChkVAlg	SGD_UINT32	4 字节,采用 SM3	对原子密钥进行正确性校验的算法，算法 OID 遵循 GM/T 0006《密码应用标识规范》。
6	校验值长度	AtomKeyChkVLen	SGD_UINT8	32 字节	原子密钥校验值的长度。
7	校验值	AtomKeyChkV	SGD_UCHAR	AtomKeyChkVLen	解密原子密钥时的校验码。
8	适配系统标识	KeySysID	SGD_UINT32	4	密钥所属应用系统标识。
9	适配设备标识	KeyDeviceID	SGD_UINT32	4	密钥所属应用系统中的密码设备标识。

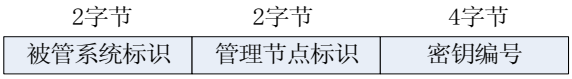

图 7 密钥唯一标识结构

7.1.2 密钥管理应用指令结构

密钥管理应用指令是设备管理指令的载荷数据,密钥管理应用指令需符合设备管理指令的要求。

7.1.2.1 指令结构

密钥管理消息 PDU 格式如图 8 所示：

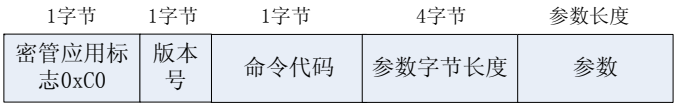

图 8 密钥管理消息 PDU

——应用标志

密钥管理应用指令的标志：0xC0。指设备管理指令载荷为密钥管理应用指令。

——版本号

指密管协议的版本号。

——指令代码

密钥管理应用指令分为上级下发指令、下级上报指令。不同指令以命令代码来区分。参见 7.1.2.2。

——参数总长

命令参数总字节长。

——指令参数

针对不同的密钥管理命令代码，封装具体的参数。

7.1.2.2 指令代码

表2 密钥管理指令代码

命令类型	命令代码	代码含义
上级下发指令及其响应	0xB0	分发保护密钥协商请求
	0xB1	分发保护密钥协商响应
	0xB2	密钥分发请求
	0xB3	密钥分发响应
	0xB4	密钥销毁请求
	0xB5	密钥销毁响应
	0xB6	密钥启用请求
	0xB7	密钥启用响应
下级上报指令及其响应	0xB8	密钥申请请求
	0xB9	密钥申请响应
其它		可扩展命令，如密钥查询等

7.1.3 分发保护密钥协商指令

密钥在分发前，由密管中心与被管设备协商的分发保护密钥预先加密保护。密管指令自身由安全通道二次保护。

密管中心与被管设备间分发保护密钥经安全通道完成。

——请求指令

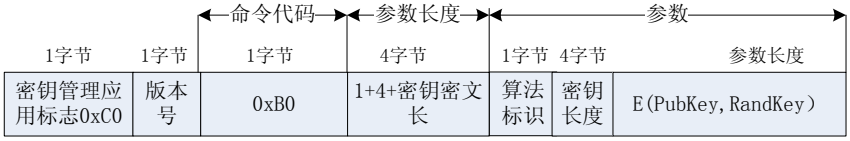

图 9 分发保护密钥协商请求

其中：

算法标识：为分发保护密钥加密待分发密钥的算法。符合 GM/T 0006《密码应用标识规范》中的算法标识要求。

E（PubKey,RandKey）：为被管设备加密公钥加密的分发保护密钥。

——响应 PDU 结构

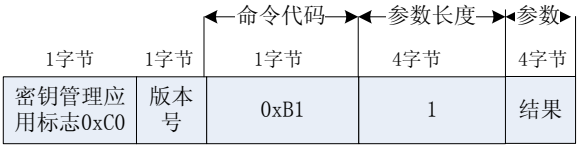

图 10 分发保护密钥协商响应

结果：为 0 则分发成功，否则为错误码。

7.1.4 密钥分发

用于密管中心向被管设备分发密钥。

——密钥分发请求

密管中心每次可以为一个被管设备分发多个密钥。每个密钥分发结构采用标准密钥封装，参见 7.1 节，其中的 AtomKeySet 用密管中心与被管设备之间共享的分发保护密钥加密保护。

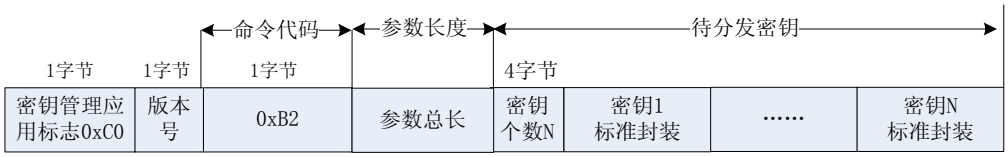

图 11 密钥分发请求

——密钥分发响应

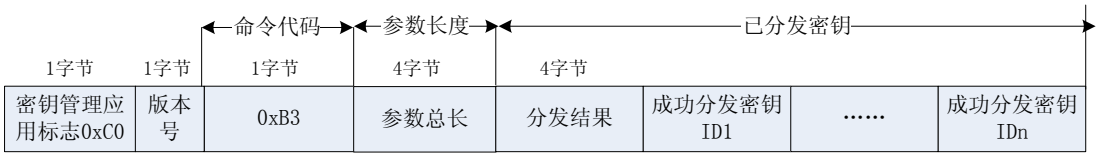

图 12密钥分发响应

其中：

分发结果：结果为 0，则密钥全部分发成功。结果大于零且小于 KMR_BASE（参见附录 B）为成功分发密钥个数，结果大于 KMR_BASE 为全部分发失败的错误码。

成功分发密钥 ID：仅用于结果大于零。表示已成功分发密钥的唯一编号。未列出编号为未成功分发密钥。

7.1.5 密钥销毁

用于销毁被管密码设备中所有密钥。

——密钥销毁请求

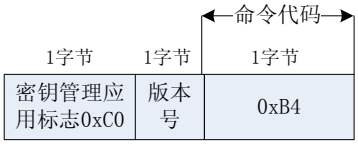

图 13 密钥销毁请求

——密钥销毁响应

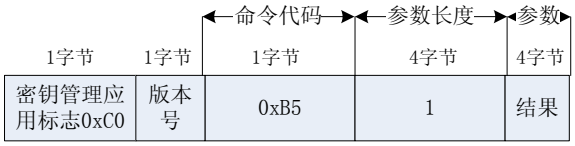

图 14 密钥销毁响应

其中：

结果：结果为 0 则销毁成功。当结果小于零为销毁失败错误码。

7.1.6 密钥启用

用于启用被管设备中的全部密钥或某些密钥。

——密钥启用指令请求

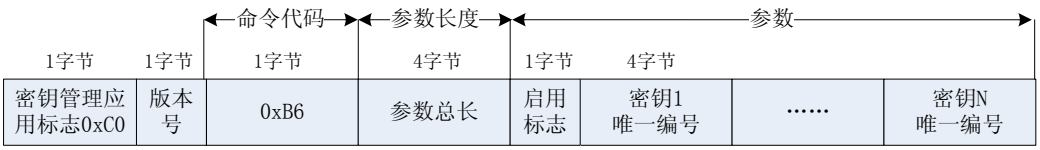

图 15 密钥启用请求

其中：

启用标志：0 代表全部启用，全部启用时指令参数为空。1 代表部分启用，部分启用时指令参数包括密钥唯一编号。

密钥编号：代表需启用密钥的唯一标识。密钥个数为（参数总长-1）/ 4。

——密钥启用指令响应

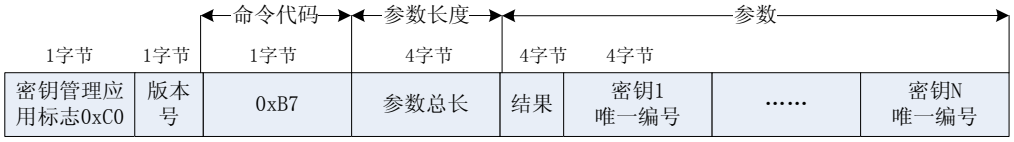

图 16 密钥启用响应

其中：

结果：为 0 则密钥全部启用成功。大于零则表示成功启用个数。

密钥编号：仅用于结果大于零时，表示成功启用密钥的唯一编号。

7.1.7 密钥申请

用于被管设备向密管中心申请更新密钥。

——密钥申请指令请求

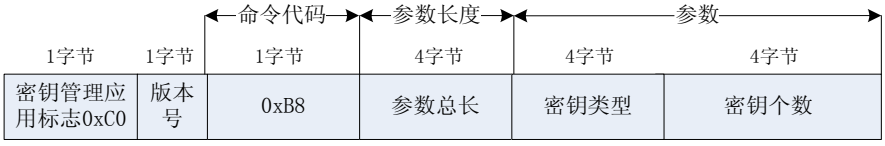

图 17 密钥申请请求

其中：

密钥类型：所请求产生和分发的密钥种类，遵循 GM/T 0006《密码应用标识规范》密钥标识 OID 要求。对称密钥长度最低不小于 128 BITS。

密钥个数：所需密钥的个数。

——密钥申请指令响应

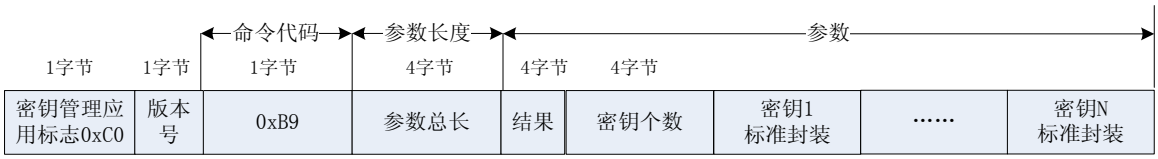

图 18 密钥申请响应

其中：

结果：为 0 则密钥申请成功，非零代表错误码。

密钥 N 标准封装：每个密钥分发结构采用标准密钥封装，参见 7.1 节，其中的 AtomKeySet 用密管中心与被管设备之间共享的分发保护密钥加密保护。

7.2 接口

本规范定义密钥产生装置、被管设备密钥管理代理、密钥管理应用的标准接口。

7.2.1 密钥产生装置接口

原型：

```
int SMF_GenAtomKey(
    SGD_CHAR SourceID[32],
    SGD_CHAR DestID[32],
    SGD_UINT32ParaDataLen,
    SGD_CHAR  *ParaData,
    SGD_UINT32SessionKeyLen,
    SGD_UINT32 SessionAlg,
    SGD_UINT32 SignAlg,
    SGD_UINT32DataSignLen,
    SGD_CHAR  *DataSign,
    SGD_UINT32*AtomKeyLen,
    SGD_CHAR *AtomKey,
    SGD_UINT32*CipheredSKeyLen,
    SGD_CHAR  *CipheredSkey,
    SGD_CHAR *AtomKeySign
);
```

描述：用于密钥产生装置产生被管设备所需原子密钥，与密管中心协商会话密钥，用会话密钥加密原子密钥。

参数：

SourceID[32][in]	发送方（密管密码机）的设备唯一标识
DestID[32][in]	接收方（密钥产生装置）的设备唯一标识
ParaDataLen [in]	密钥产生参数长度
ParaData [in]	密钥产生参数
SessionKeyLen[in]	密钥产生的会话密钥长度
SessionAlg[in]	密钥产生的会话密钥加密算法标识，参见 GM/T 0006《密码应用标识规范》
SessionAlg[in]	签名算法标识，参见 GM/T 0006《密码应用标识规范》
DataSignLen[in]	签名长度
DataSign[in]	对 SourceID//DestID//ParaData 的签名
AtomKeyLen [out]	原子密钥的长度
AtomKey[out]	用密钥产生会话密钥加密的原子密钥
CipheredSKeyLen[out]	加密的密钥产生会话密钥长度
CipheredSkey[out]	用发送方（密管密码机）公钥加密的密钥产生会话密钥
AtomKeySign[out]	对 SourceID//DestID//AtomKey//CipheredSkey 的签名

返回值：

0	成功
非 0	失败，返回错误代码

流程：

1. 密管中心根据被管密码设备的需求形成密钥产生参数，并用本地密码机私钥对以下请求数据进行签名：SourceID//DestID//ParaData。签名算法与证书算法一致。
2. 密管中心调用本接口向指定密钥装置请求密钥；

3. 密钥产生装置用密管密码机公钥证书对请求数据的签名进行验证，并比对所请求 DestID 是否为本地唯一标识；

4. 请求验证和比对通过后，密钥产生装置根据专用参数生成所需原子密钥；

5. 密钥产生装置产生要求长度的会话密钥，用要求的算法对所产生的原子密钥进行加密；

6. 密钥产生装置使用本地密码机私钥对以下响应数据进行签名：SourceID//DestID// AtomKey//CipheredSkey。签名算法与证书算法一致；

7. 密管中心对响应数据签名进行验证并比对 SourceID 是否为本地唯一标识；

8. 密管中心用本地密码机私钥解密会话密钥，并用会话密钥解密原子密钥；

9. 密钥中心用本地密码机主密钥加密原子密钥存储在密钥数据库中。

7.2.2 密钥管理消息发送接口

用于发送密钥管理消息的设备管理应用 API 接口。调用 GM/T AAAAA《密码设备管理技术规范》9.8 节 SMF_SecTunnelSendData 函数，密钥管理消息赋值在 sendData 字段。

7.2.3 被管设备密钥管理接口

指密码设备管理代理与密钥管理代理间接口，用于密钥导入。终端代理的实现与密码设备直接相关，因而这部分由密码设备厂商自定义，至少包括以下四个接口：

——分发保护密钥协商接口

——密钥分发接口

——密钥销毁接口

——密钥启用接口

8 建设要求

8.1 建设原则

密钥管理系统应能为多种密码体系和多种业务系统提供统一密钥服务、统一密钥管理。

8.2 功能要求

密钥管理系统应提供下列服务功能：

——提供密钥产生、密钥分发、密钥查询、密钥更新、密钥恢复、密钥撤销等管理功能；

——支持密钥多级管理；

——为司法机关提供用户密钥恢复服务。

8.3 性能要求

密钥管理系统的性能应满足如下要求：

——密钥的保存期应大于 10 年；

——支持并发服务请求；

——模块的配置信息采用配置文件或数据库方式，支持灵活配置和方便部署；

——支持冗余设计，保证系统的不间断运行。

8.4 初始化要求

密钥管理系统的初始化时需要完成以下准备：

——注册密钥管理系统节点，分发密管服务器证书；

——注册被管系统及被管设备，分发被管设备证书；

——注册密管密码设备及密钥产生装置，分发密管密码设备证书；

——注册密管系统管理员，分发各管理员证书。

8.5 安全要求

8.5.1 物理环境安全

——密钥管理的生成装置应部署在屏蔽环境内，保证系统在安全保密的环境中运行；

——机房和机房重要区域入口设置门禁和监控装置；

——遵守 GB/T 9361-1988：《计算站场地安全要求》；

——遵守 GB/T 2887-1989：《计算站场地技术条件》；

——遵守 GB/T 6650-1986：《计算机机房用活动地板技术条件》；

——遵守 GB/T 50174-1993：《电子计算机机房设计规范》。

8.5.2 系统安全

——应综合采取防火墙、病毒防治、漏洞扫描、入侵监测、主机监控、外联监控、安全审计、数据备份、灾难恢复等安全防护措施，以保障网络、主机系统、应用系统及数据库运行的安全；

——应采取措施保证终端、介质和信息导入的安全。

8.5.3 网络安全

——密钥管理中心/密钥管理分中心之间实现加密传输、数据源认证和接入控制；

——密管系统节点间采取安全通信协议等安全措施。

8.5.4 密码密钥安全

——密钥由通过国家密码管理局鉴定的密码设备生成，确保密钥的随机性；

——密钥在密钥库和密钥介质中应加密存储；

——密钥分发时应以密文形式分发；

——密钥必须有安全可靠的备份恢复机制；

——密码运算必须由硬件密码设备完成。

8.5.5 身份认证

——管理员的身份认证、设备和系统的实体认证基于证书方式实现；

——管理员证书、设备和系统的证书均由国家商用密码管理中心指定的认证系统签发。

8.5.6 安全审计

——系统交互日志

密钥管理基础设施运行过程中，各功能模块之间会发生通信交互，对通信交互的以下属性应进行记录：

- 交互发起方的系统；
- 交互接受方的系统；
- 交互时间；
- 交互内容；
- 交互结果等。

——管理员操作日志

管理员的重要操作行为应当被记录，记录应包括：

- 管理员身份；
- 操作内容；
- 操作时间；
- 操作结果等。

8.5.7 数据备份要求

密钥是密管系统的重要数据，对于所有形态的密钥数据，包括加密密钥、密钥分量等，都应由密管系统进行备份，如进行异机备份、异地备份，以备系统异外时的数据恢复。

不同的应用环境可有不同的备份方案，但应满足以下基本要求：

——备份在不中断系统使用的前提下实施；

——提供人工和自动备份功能；

——提供实时和定期备份功能；

——提供全备份和增量备份功能；

——提供日志记录功能；

——支持数据异地备份功能，支持自动恢复功能。

8.5.8 网络管理

根据密管网络规模，选择性支持对各网络设备和主机进行配置管理、性能管理和故障管理，实现网络和主机资源的监控。

——配置管理要求

- 具备网络拓扑结构自动发现功能；
- 应提供网络设备和主机的配置功能。

——性能管理要求

- 具备对网络设备和主机数据采集功能；
- 提供网络状态监控的图形化界面。

——故障管理要求

- 支持监视策略制定；
- 支持多种网络诊断方式；
- 提供多种故障响应方式。

8.5.9 可靠性

保障网络链路、主机、数据库及电源的冗余配置，提供 7×24 小时服务，

8.5.10 管理分域访问

8.5.10.1 公共区

书面材料审核等功能设置于公共区。

入口之外的区域为公共区。

8.5.10.2 管理区

核心密管、密钥分发、密钥备份/恢复、审计等功能设置于管理区。

所有进入此区的人员需经过身份鉴别才可进入。

8.5.10.3 核心区

密钥产生装置设置于核心区。

所有进入此区人员需要需经过身份鉴别才可以进入，人员进出要有日志记录。

核心区应为屏蔽机房，应加装高强度的钢制防盗门。所有进出屏蔽室的线路都要采取防电磁泄漏措施。屏蔽效果应符合国家密码管理相关政策要求并达到国家相关标准要求。

8.5.11 安全监控和配电消防

密管应设置安全监控室、系统监控室、配电室和消防器材室。

安全监控室是安全管理人员值班的地方，可对整个密管的进出人员实行监控，处理日常的安全事件。只有安全管理人员需经过身份鉴别才可以进入和离开。

系统监控室是网络管理人员工作的地方。需要经过身份鉴别才可以进入和离开。

配电室是放置所有供电设备的房间，只有相应的授权人员需经过身份鉴别才可以进入合离开。

消防器材室是存放消防设备的房间，建议经过身份鉴别才可进入消防器材室。

8.5.12 门禁和物理侵入报警系统

密管应设置门禁和物理侵入报警系统。

门禁系统控制各层门的进出。工作人员都需使用身份识别卡或结合人体特征鉴别才能进出，并且进出每一道门都应有时间记录和相关信息提示。

任何非法的闯入、非正常手段的开门、以及授权人刷卡离开后房内还有非授权的滞留人员，都应触发报警系统。报警系统应明确地指出报警部位。

门禁和物理侵入报警系统应自备有 UPS，并应提供至少 8 小时的供电。

与门禁和物理侵入报警系统配合使用的还应有录像监控系统。对监控区域进行 24 小时不间断的录像。所有的录像资料要根据需要保留一段时间，以备查询。

9 运行管理要求

密钥管理系统应制订业务运行管理规范来指导密钥管理系统日常业务开展。业务运行管理规范通常应包括密钥管理中心管理制度、信息系统安全操作与维护以及客户服务等。

9.1 安全操作与维护管理制度

密钥管理中心管理制度包括密钥管理中心运行场所进出管理制度、系统信息保密制度、工作人员管理制度、机房安全管理制度等，应按国家有关标准执行。

9.1.1 安全操作内容

系统管理的操作与维护规范应包括以下内容：

——对密钥管理系统进行任何操作之前，应充分考虑并预计操作之后的结果，每次操作都必须审计；

——改变系统自身的配置，应制订实施计划和相关文档说明，经上级主管批准后才能进行操作，操作时应至少有两人在场；

——系统出现故障时，应由系统管理人员检查处理，其它人员未经批准不得处理；

——未经批准不得在服务器上安装任何软件和硬件；

——未经批准不得删除服务器上的任何文件。

9.1.2 数据备份

数据备份的操作与维护规范应包括以下内容：

——系统升级后，应立即进行全备份；
——对数据变化量大的服务器，应每天做一次增量备份，每周做一次全备份；
——对数据变化量少的服务器，可每周做一次备份；
——对重要数据应准备两套备份，其中异地存放一套；
——对数据库的备份应单独进行；
——对重要的目录应单独进行备份；
——手工进行的备份，应在介质上标明备份的服务器及路径；
——自动进行的备份，应将备份介质有效区分；
——选择的备份介质应能保证数据的长期可靠，否则应定期更新。

9.1.3 口令管理

口令管理规范应包括以下内容：
——口令长度应为 8 个字节以上，应是字母、数字和特殊字符组成的混合体，口令不得采用有特殊意义的（如姓名、生日、电话号码等）数字和词组；
——应规定口令的使用期限并定期更换；
——口令应妥善保管，防止泄漏；
——通过网络传输的口令必须保护；
——应检查网络设备、主机和应用程序中是否设置有缺省口令的缺省用户名，找出并禁止。

9.1.4 应急处理

密钥管理中心应制订应急处理预案，当出现重大故障或灾难性事故时，应启动预定的应急处理方案进行处理。

应急处理预案应根据事件的严重程度、紧急程度和事件类别，分别规范告警、报告、保护、处置、善后、总结等处理流程和处置措施。

系统恢复正常运行后，应对应急处理过程进行总结，总结中应详细记录事件起因、处理过程、经验教训、改进建议等。

应针对应急事件处理中暴露的问题，不断完善和修改应急处理预案。

9.2 人员管理要求

为防止非授权人员操作密钥管理系统，在每一个操作终端上应设有操作员身份鉴别系统，对系统的所有操作都要对有关操作员进行身份鉴别和权限控制。

密钥管理系统的每个操作人员配置有标明个人身份与相关资料的证书载体，证书载体具有口令保护机制，以保证私钥和应用的安全。

人员管理的主要内容是：增加操作员、注销操作员、设置操作员权限、修改操作员权限。

操作员信息包括：操作员编号、操作员姓名、操作员部门、操作员权限。

系统管理员由系统初始化时产生，主要职责是设置业务管理员并进行管理。其权限为：
——增加业务管理员；
——注销业务管理员；
——设置业务管理员权限；
——修改业务管理员权限。

业务管理员由系统管理员授权，主要职责是设置业务操作员并进行管理。其权限为：
——增加业务操作员；
——注销业务操作员；
——设置业务操作员权限；
——修改业务操作员权限。

业务操作员由业务管理员授权，主要职责是对业务系统进行各种操作。

审计管理员由系统初始化时产生，主要职责是负责对涉及系统安全的事件和各类管理和操作人员的行为进行审计和监督。其权限为：

——证据访问操作；

——日志访问操作。

安全保密管理员由系统管理员授权，主要负责系统的日常安全保密管理工作，包括用户账号管理以及安全保密设备和系统所产生日志的审查分析。

管理员和操作员登录密钥管理系统以及在密钥管理系统中的所有操作都采用基于证书的身份鉴别。当此类人员离职或是被撤职时，应及时注销其证书。

9.3 密钥分量管理要求

密钥管理中心的本地主密钥需要用秘密共享机制分割备份出来，分别交予分管者保管。恢复时，到场的分管者的人数应满足恢复所需的人数。

分管者的选择条件如下：

——分管者应符合可信人员策略规定的条件；

——符合下列条件之一者，不能成为分管者：

- 本密钥管理系统的系统管理员；
- 本密钥管理系统的业务管理员；
- 本密钥管理系统的业务操作员；
- 本密钥管理系统的系统维护人员。

9.4 系统安全管理要求

安全保密管理员的职责主要包括：

——制定安全策略；

——指导安全管理；

——设计和指导安全策略实施；

——对安全管理进行定期的检查和评估；

——对安全策略和执行程序的日常维持；

——定期对相关人员开展安全教育。

安全保密管理员对安全的三个关键领域负有全面的责任，即：

——开发与执行安全策略；

——维护与完善安全策略；

——保持与安全审计的一致性。

安全管理员有责任来定义和委托密钥管理中心的特定个人或部门的安全职责。

9.5 安全审计要求

审计管理员应定期对密钥管理系统进行安全审计，包括：

——人员审计：密钥管理中心的人员必须是可信任的；必须理解安全策略和安全操作程序；

——物理安全审计：物理安全防护措施是否完善；安全物品的管理是否符合安全管理规定；

——操作安全审计：所有的人员的操作记录必须完整保存，并且所有操作必须符合安全管理规定；

——系统安全审计：检查密钥管理系统的操作系统、数据库系统、入侵检测系统、漏洞扫描系统、防病毒系统、防火墙系统、密钥管理系统等的日志记录，以确定系统是否异常。

9.6 文档配备要求

密钥管理中心应配备相关的文档用于指导密钥管理中心的建设、运行、服务、应急和日

常管理。可分为技术实现、物理建设、人事管理、运行管理以及审计与评估五类。

9.6.1 技术实现

技术实现类主要包括密钥管理中心系统设计、密钥管理中心系统安全、密钥管理中心系统安装与配置手册、密钥管理中心系统安全目标、密钥管理中心系统用户手册五类文档，技术实现类文档主要描述内容如下：

——系统设计：描述系统的逻辑结构、网络结构、数据通信设计、密钥管理、业务处理流程以及系统的软硬件配置等；

——系统安全：描述系统通过采用防火墙、入侵检测、漏洞扫描、病毒防治、访问控制、安全配置等措施，保证密钥管理中心的安全性。同时，从数据通讯、密钥管理、证书管理、安全审计、物理安全等各个方面阐述密钥管理中心安全措施的实现；

——系统安装与配置手册：介绍系统的安装与配置；

——系统安全目标：描述系统对国家相关安全标准的满足情况；

——系统用户手册：描述用户对系统使用和操作的技术手册。

9.6.2 物理建设

物理建设类主要包括物理场地安全手册、物理场地安全管理规定两类文档，物理建设类文档主要描述内容如下：

——物理场地安全手册：描述物理场地的安全的要求及实现等；

——物理场地安全管理规定：描述人员进出密钥管理中心各个区域的权限、来访者的接待和管理、门禁系统的使用、监控报警系统的操作使用等管理规定。

9.6.3 人事管理

人事管理类文档主要包括可信人员策略、可信人员职位划分原则与鉴别两类文档，人事管理类文档主要描述内容如下：

——可信人员策略：描述可信人员策略及其如何进行可信人员调查；

——可信人员职位划分原则与鉴别：描述可信人员职位划分原则，可信人员鉴别和背景调查及分析等。

9.6.4 运行管理

运行管理类文档主要包括密钥管理中心管理规范、操作手册、安全应急预案、客户报务规范几类文档，运行管理类文档主要描述内容如下：

——密钥管理中心管理规范：描述密钥管理中心的操作与安全维护管理的规定；

——操作手册：描述认证业务流程；

——安全应急预案：描述密钥管理中心电力系统、消防系统、业务系统、人员变动、安全等方面出现事故时的应急处理流程和措施；

——客户服务规范：制定出的系列客户服务文档，包括客户法律协议、隐私保护政策、客户保障计划等。

9.6.5 审计与评估

审计与评估类文档主要包括密钥管理中心安全与审计规范、安全审核与评估规范两类文档，审计与评估类文档主要描述内容如下：

——密钥管理中心安全与审计规范：规定了密钥管理中心运行系统的审核方法；

——安全审核与评估规范：规定了密钥管理中心运行系统的审核范围和评价标准。

附录 A
（规范性附录）
密钥管理总体技术框架

本规范的密钥管理总体技术框架如图 A-1 所示：

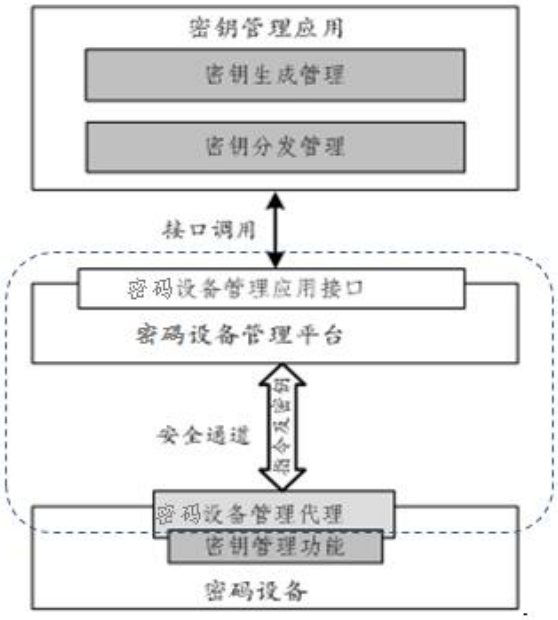

图 A-1 密钥管理总体技术框架

密钥管理系统分为生成和分发两个主要部分，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的密钥产生会话密钥加密，安全传输至密管密码机，由密管密码机将会话密钥加密转换为本地主密钥加密导出。密管应用将加密密钥封装为标准密钥结构后，存储在密钥数据库。

密钥分发管理中，密管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规范参见《密码设备管理规范》。

附录 B
（规范性附录）
错误码定义

宏描述	预定义值	说明
#define KMR_OK	0x0	操作成功
#define KMR_BASE	0x0E000000	错误码基础值
#define KMR_UNKNOW_ERR	KMR_BASE + 0x00000001	未知错误
#define KMR_ID_ERR	KMR_BASE + 0x00000002	ID 不匹配
#define KMR_VERIFY_ERR	KMR_BASE + 0x00000003	验签错误
#define KMR_SIGN_ERR	KMR_BASE + 0x00000004	验签错误
#define KMR_DECRYPT_ERR	KMR_BASE + 0x00000005	解密错误
#define KMR_ENCRYPT_ERR	KMR_BASE + 0x00000006	加密错误
#define KMR_KEYNOTEXIST_ERR	KMR_BASE + 0x00000007	密钥不存在
#define KMR_KEYACCEPT_ERR	KMR_BASE + 0x00000008	密钥接收错误
#define KMR_KEYGEN_ERR	KMR_BASE + 0x00000009	密钥生成错误
#define KMR_KEYDEL_ERR	KMR_BASE + 0x0000000A	密钥销毁错误
#define KMR_KEYACTIVE_ERR	KMR_BASE + 0x0000000B	密钥激活错误
#define KMR_KEYREQUEST_ERR	KMR_BASE + 0x0000000C	密钥请求错误
… …	SDR_BASE + 0x0000000D 至 SDR_BASE + 0x00FFFFFF	预留

附录 C
（规范性附录）
密钥格式配置文件

密钥管理中心按照密钥格式配置文件的要求，调用密钥产生装置，为被管密码设备原子密钥。

密钥格式配置文件采用 txt 文本格式，密钥配置文件包含 5 种基本属性项，参见表 C。每项属性项以[]符号标识，密钥产生参数和原子密钥采用网络字节序。

表C密钥格式配置项

配置项名称	备注
[密钥适配系统名称]	长度小于128字节的变长字符串
[密钥适配设备型号]	长度小于128字节的变长字符串
[配置类型]	0：原子密钥结构，1：密钥产生参数
[密钥产生参数表]	适配于专用密钥产生装置的参数表（多项）
[密钥模板表]	待通用密钥产生装置填充随机数的原子密钥码流表（多项）

对于专用密钥产生装置，“密钥产生参数表”为待产生原子密钥的密钥产生参数，由被管设备厂商定义格式并提供码流表。其密钥格式配置文件示例：

[密钥的应用系统名称]
某局安全报文传输系统
[使用密钥的设备型号]
某某型号网络密码机
[配置类型]
1　　//专用密钥产生装置密钥产生参数
[密钥产生参数表]
ParaData1
……
ParaDataN

密钥管理中心根据该配置文件，调用 N 次专用密码产生装置，使用 N 个 ParaData 参数码流直接调用接口，填写入 ParaData 结构，为该密码机产生 **N** 个原子密钥。

专用密钥产生装置按照被管设备厂商定义格式解析参数并产生原子密钥。

对于通用密钥产生装置，“密钥模板表”结构填充的是待产生原子密钥模板码流，标明其中哪些字节需要用随机密钥填充。其密钥格式配置文件示例：

[密钥的应用系统名称]
某局安全报文传输系统
[使用密钥的设备型号]
某某型号网络密码机型号
[配置类型]
0　　//通用密钥产生装置原子密钥结构

[密钥模板表]

KeyStart1：KeyLen1：AtomKeyClass1

……

KeyStartN：KeyLenN：AtomKeyClassN

AtomKeyClass 为原子密钥模板码流。原子密钥模板需要被管设备厂商提供。密钥管理中心根据以上配置文件，调用 N 次通用密码产生装置，使用 N 个 KeyClass 参数码流，从左数第 KeyStart 个字节开始，填充长度为 KeyLen 的随机数。填充完毕的 KeyClass 即为该设备的原子密钥。

密管中心调用接口，发给通用密钥产生装置的 ParaData 码流格式为：

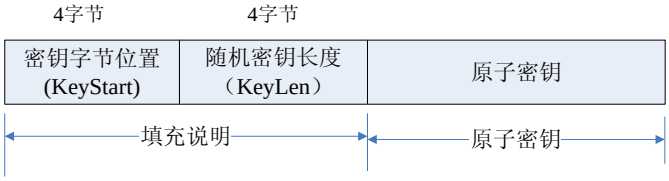

图 C-1 通用密钥产生装置 ParaData 格式

前半部分是随机数填充的说明，后半部分是待填充密钥的原子密钥结构。通用密钥产生装置只填充随机数密钥，原子密钥模板中其它项应当在输入时已填充完毕。