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

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。

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 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　cryptography device management API

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　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　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。

3.13

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。

3.14

密钥格式配置文件　general key config profile

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。

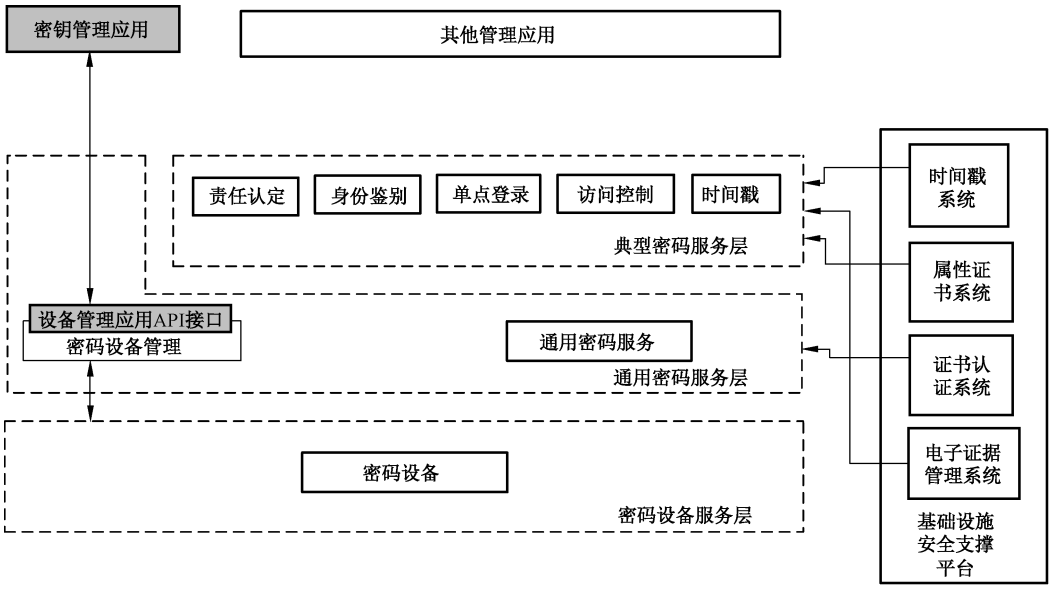

图 1 密钥管理应用与密码基础设施的关系

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。

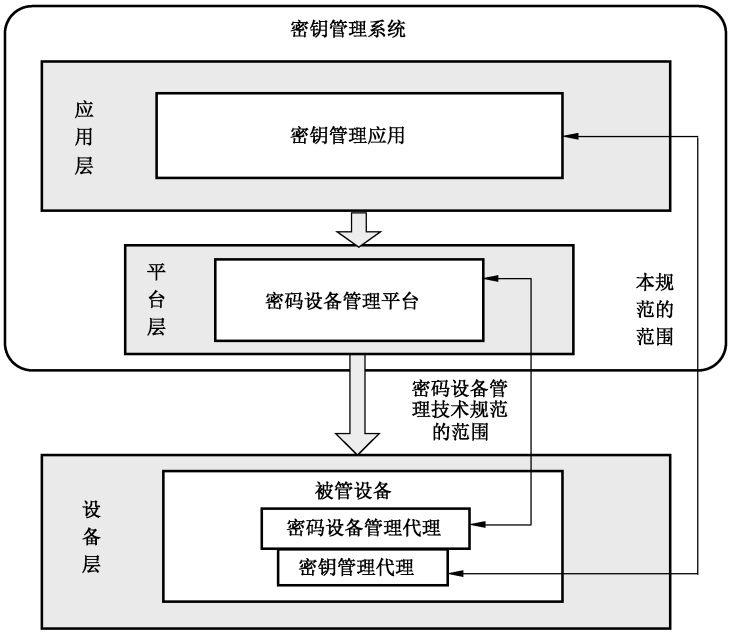

图 2　密钥管理应用与密码设备管理平台的关系

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。

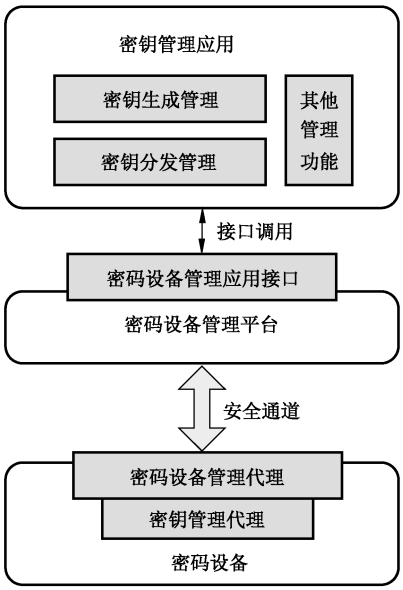

图 3　密钥管理总体技术框架

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。

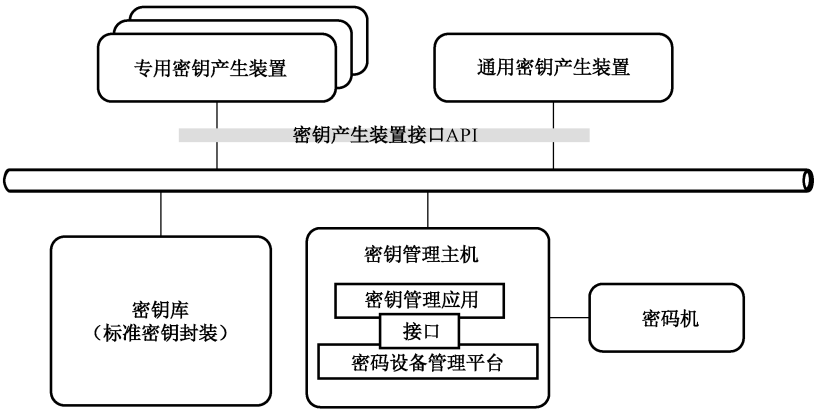

图 4　密钥管理系统组成框架

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。

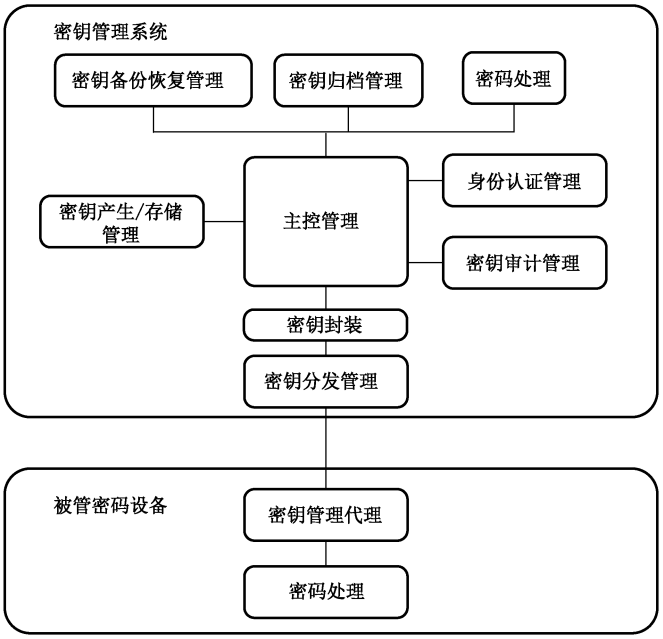

图 5 密钥管理系统功能结构

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具体操作。

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；

——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 主控管理模块

应满足以下功能要求：
——制定密钥生成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 密钥生成模块

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钥管理系统；
——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，所生成密钥为密钥管理系统的原子密钥。

密钥生成装置接口参见 7.3。

通用密钥生成装置，需由密钥管理端的主控管理模块按照密钥格式配置文件（参见附录 B）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 GM/T 0050—2016 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钥管理系统中转换为用本地存储密钥加密，7.2.2 标准格式对原子密钥密文进行封装，最后存储于密钥管理中心的密钥库中。

密钥分发时，密钥管理中心与被管设备在安全通道中以本标准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生成接口、分发保护密钥协商接口参见 7.2 和 7.3。

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 7.2.2。

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他策略。

——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。

——支持本标准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、智能密码钥匙等载体离线分发；

——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 7.2.2；
- 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。

本标准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 7.2.4。

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，在用库记录应包含产生时间、有效期等标志，历史库记录应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；
——配置国家密码管理主管部门批准的对称算法、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；
——接收与审查司法取证部门的恢复密钥申请，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钥管理系统提出业务密钥恢复请求。通过密钥管理系统审查后，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，通过密钥管理系统书面审查后，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。司法恢复专职人员应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，在密钥管理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：
——对密钥生成、密钥存储、密钥分发、主控管理模块、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 0050—2016 的要求。

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。

设备管理代理中应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 7.2。

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

本标准密钥管理系统建立在 GM/T 0050—2016 的设备管理平台之上，密钥管理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 0050—2016　5.8“注册流程”。

7 对称密钥管理应用指令及管理接口

7.1 基本要求

指令中加密算法采用国家密码管理主管部门规定的算法，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。

7.2 应用指令

7.2.1 指令产生和处理

密钥管理指令是设备管理指令的载荷数据，密钥管理指令应符合设备管理指令的要求。

密钥管理指令由密钥管理应用产生，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 6 所示（参见 GM/T 0050—2016）。

图 6　密钥管理指令在设备管理安全通道消息中的位置和格式

本标准定义密钥管理应用的标识为：0xC0。

密钥管理指令处理流程如图 7 所示。

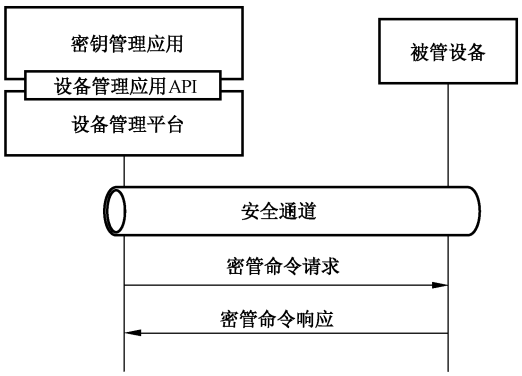

图 7　密钥管理指令流程

——密钥管理应用根据管理应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 0050—2016 中 9.4.1 的 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；

——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。

7.2.2　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，参见图 8
2	密钥类型	KeyType	SGD_UINT32	4	所产生的密钥种类，密钥标识 OID 遵循 GM/T 0006
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	由密钥生成装置生成的密钥。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	对原子密钥进行正确性校验的算法，采用 SM3。算法 OID 遵循 GM/T 0006
6	校验值长度	AtomKeyChkVLen	SGD_UINT8	32	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

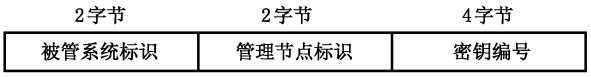

图 8　密钥唯一标识结构

7.2.3　指令结构

7.2.3.1　PDU 格式

密钥管理指令 PDU 格式如图 9 所示。

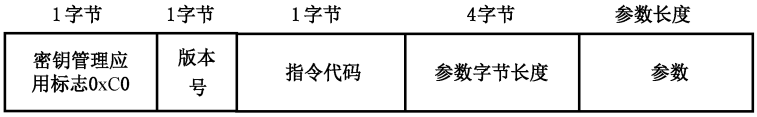

图 9　密钥管理指令 PDU

——应用标志

密钥管理指令的标志：0xC0。指设备管理指令载荷为密钥管理指令。

——版本号

指密管协议的版本号。

——指令代码

密钥管理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 7.2.3.2。

——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。

7.2.3.2　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
其他		可扩展命令，如密钥查询等

7.2.4 分发保护密钥协商指令

密钥在分发前，由密钥遵循管理中心与被管设备协商的分发保护密钥加密保护（见图 10），再通过安全通道分发。

——保护密钥协商请求指令 PDU

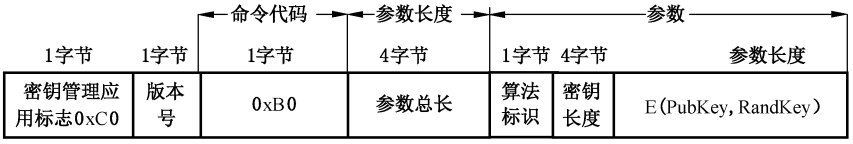

图 10 分发保护密钥协商请求

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 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。

——保护密钥协商响应 PDU（见图 11）

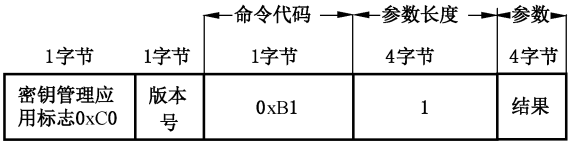

图 11 分发保护密钥协商响应

结果：为 0 则分发成功，否则为错误码。

7.2.5 密钥分发

用于密钥管理中心向被管设备分发密钥。

——密钥分发请求 PDU（见图 12）

密钥管理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 7.2.2，其中的 AtomKeySet 用密钥管理中心与被管设备之间共享的分发保护密钥加密保护。

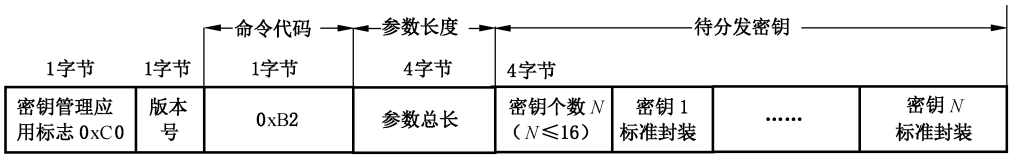

图 12 密钥分发请求

——密钥分发响应 PDU（见图 13）

图 13 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A)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。

7.2.6 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PDU(见图14)

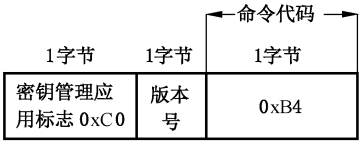

图14 密钥销毁请求

——密钥销毁响应PDU(见图15)

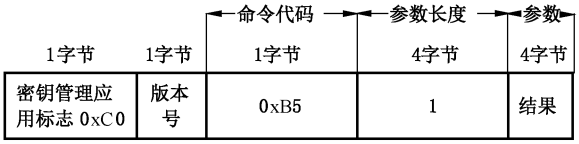

图15 密钥销毁响应

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。

7.2.7 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PDU(见图16)

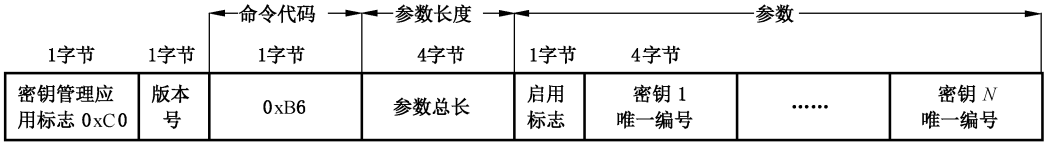

图16 密钥启用请求

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PDU(见图17)

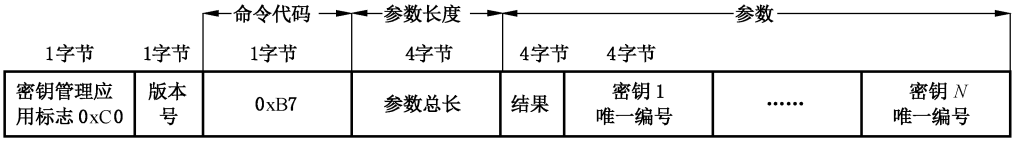

图 17　密钥启用响应

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。

7.2.8　密钥申请

用于被管设备向密钥管理中心申请更新密钥。

——密钥申请指令请求 PDU(见图 18)

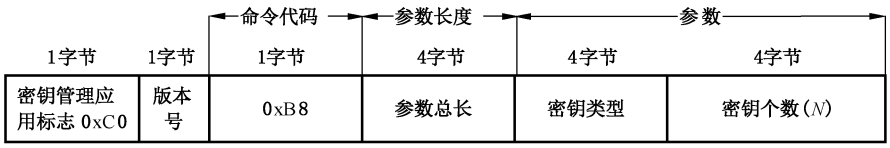

图 18　密钥申请请求

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，$N \leqslant 16$。

——密钥申请指令响应 PDU(见图 19)

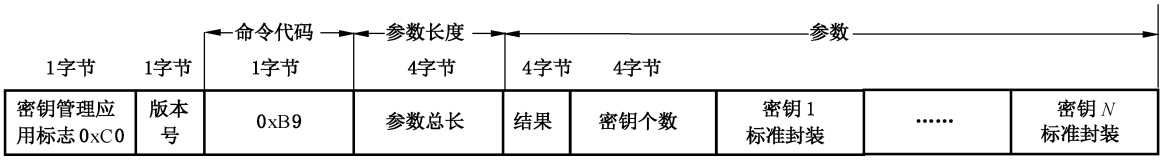

图 19　密钥申请响应

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 7.2.2，其中的 AtomKeySet 用密钥管理中心与被管设备之间共享的分发保护密钥加密保护。

7.3　管理接口

本标准定义密钥生成装置、被管设备密钥管理代理、密钥管理应用的标准接口，被管对象与管理代理之间的接口由其他标准规定。

7.3.1 密钥生成装置接口

原型：
```
int SMF_GenAtomKey(
    SGD_CHAR SourceID[32],
    SGD_CHAR DestID[32],
    SGD_UINT32 ParaDataLen,
    SGD_CHAR *ParaData,
    SGD_UINT32 SessionKeyLen,
    SGD_UINT32 SessionAlg,
    SGD_UINT32 SignAlg,
    SGD_UINT32 DataSignLen,
    SGD_CHAR *DataSign,
    SGD_UINT32 *AtomKeyLen,
    SGD_CHAR *AtomKey,
    SGD_UINT32 *CipheredSKeyLen,
    SGD_CHAR *CipheredSkey,
    SGD_CHAR *AtomKeySign
);
```

描述：用于密钥生成装置产生被管设备所需原子密钥，与密钥管理中心协商会话密钥，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(密钥生成装置)的设备唯一标识
ParaDataLen [in]	密钥生成参数长度
ParaData [in]	密钥生成参数
SessionKeyLen[in]	密钥生成的会话密钥长度
SessionAlg[in]	密钥生成的会话密钥加密算法标识，参见 GM/T 0006
SignAlg[in]	签名算法标识，参见 GM/T 0006
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]	用密钥生成会话密钥加密的原子密钥
CipheredSKeyLen[out]	加密的密钥生成会话密钥长度
CipheredSkey[out]	用发送方(密管密码机)公钥加密的密钥生成会话密钥
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) 密钥管理中心根据被管密码设备的需求形成密钥生成参数，并用本地密码机私钥对以下请求数据进行签名：SourceID//DestID//ParaData。SignAlg 参数指定的签名算法应与证书算法相同；
2) 密钥管理中心调用本接口向指定密钥装置请求密钥；
3) 密钥生成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。证书格式符合 GM/T 0015 要求；
4) 请求验证和比对通过后，密钥生成装置根据专用参数生成所需原子密钥；

5） 密钥生成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） 密钥生成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） 密钥管理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） 密钥管理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。

7.3.2 密钥管理指令发送接口

指用于发送密钥管理指令的设备管理应用 API 接口。

应调用 GM/T 0050—2016 9.4.1 中的 SMF_SecTunnelSendData 函数，密钥管理指令赋值在 sendData 字段。

7.3.3 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。密钥管理代理的实现与密码设备直接相关，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。

附 录 A
（规范性附录）
错误码定义

表 A.1 错误码定义表

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	签名错误
# 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
……	KDR_BASE + 0x0000000D 至 KDR_BASE +0x00FFFFFF	预留

附 录 B
（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，调用密钥生成装置，为被管密码设备产生原子密钥。

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 B.1。每项属性项以[]符号标识，密钥生成参数和原子密钥采用网络字节序。

表 B.1 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:密钥生成参数
[密钥生成参数表]	适配于专用密钥生成装置的参数表(多项)
[密钥模板表]	待通用密钥生成装置填充随机数的原子密钥码流表(多项)

对于专用密钥生成装置，“密钥生成参数表”为待产生原子密钥的密钥生成参数，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 //专用密钥生成装置密钥生成参数
[密钥生成参数表]
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。

专用密钥生成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。

对于通用密钥生成装置，“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 //通用密钥生成装置原子密钥结构

[密钥模板表]
KeyStart1:KeyLen1:AtomKeyClass1
……
KeyStart$N$:KeyLen$N$:AtomKeyClass$N$

AtomKeyClass 为原子密钥模板码流。原子密钥模板应由被管设备厂商提供。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。

密钥管理中心调用接口，发给通用密钥生成装置的 ParaData 码流格式如图 B.1 所示。

图 B.1　通用密钥生成装置 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。通用密钥生成装置只填充随机数密钥，原子密钥模板中其他项应当在输入时已填充完毕。