ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0086—2020

基于 SM9 标识密码算法的密钥管理系统技术规范

Specification of key management system based on SM9 identity cryptography algorithm

2020-12-28 发布　　2021-07-01 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：上海信息安全工程技术研究中心、北京国脉信安科技有限公司、航天信息股份有限公司、深圳奥联信息安全技术有限公司、三未信安科技发展有限公司。

本文件主要起草人：袁文恭、袁峰、王晓春、郭宝安、蔡先勇、张岳公、封维端、张立圆、王学进、蒋楠、药乐、陈祎。

引　言

本文件依据我国 SM9 标识密码算法的应用需求而制定，给出了基于 SM9 标识密码的标识密钥管理系统（简称标识密钥管理系统）完整的架构包含组成说明、功能要求和技术规范，还给出了用户标识密钥（本文件中特指私钥）的申请、生成、签发、下载、更新、作废、验证以及公开参数查询等实现流程。

基于SM9标识密码算法的密钥管理系统技术规范

1 范围

本文件规定了基于SM9标识密码算法的密钥管理系统架构及其建设要求。该架构可作为基于标识密码应用的普适性基础标准，为其提供密钥生成、管理以及公开参数查询等服务。

本文件适用于指导基于SM9标识密码的标识密钥管理系统设计、建设和管理，也可以用于相关系统的检测。

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 2887—2011 计算机场地通用规范

GB/T 9361—2011 计算机场地安全要求

GB 50174—2017 数据中心设计规范

GB/T 24363 信息安全技术 信息安全应急响应计划规范

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/Z 24364 信息安全技术 信息安全风险管理指南

GM/T 0044(所有部分) SM9标识密码算法

GM/T 0057 基于IBC技术的身份鉴别规范

GM/Z 4001 密码术语

3 术语和定义

GM/T 0044(所有部分)和GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

鉴别 authentication

确认一个实体所声称的身份或属性。

3.2

鉴别凭证 authentication credentials；AC

对用户进行身份鉴别时，被鉴别方提供的有效可信证据。

3.3

双线性对 bilinear pairing

线性空间上的一种函数，其定义为：设V是数域F上的一个线性空间，$f(\alpha,\beta)$是V上一个二元函数，对$\forall\alpha,\beta\in V$，f确定F中唯一的数$f(\alpha,\beta)$与之对应。若对$\forall\alpha,\alpha_1,\alpha_2,\beta,\beta_1,\beta_2\in V,k_1,k_2\in F$，$f(\alpha,\beta)$满足$f(\alpha,k_1\beta_1+k_2\beta_2)=k_1f(\alpha,\beta_1)+k_2f(\alpha,\beta_2)$；和$f(k_1\alpha_1+k_2\alpha_2,\beta)=k_1f(\alpha_1,\beta)+k_2f(\alpha_2,\beta)$，则称$f(\alpha,$

β)为 V 上的一个双线性函数,α,β 为双线性对。

3.4

用户加密密钥　encryption key

由标识密钥管理系统将用户唯一标识利用加密主私钥进行计算产生的密钥,并下发给用户用于加密、解密和密钥协商。

3.5

加密主密钥　encryption master key

标识密钥管理系统的主加密密钥对,包括加密主私钥和加密主公钥,用于进行数字加密、解密和为用户生成用户加密密钥。

3.6

标识符　identifier;ID

唯一标识某一对象的一个数据项序列。

注:在本文件中用标识符 ID 代表身份标识 Identity,当进行密码运算时,见 GM/T 0081 中定义的结构。

3.7

标识　identity

可唯一确定一个实体身份的信息。标识应由实体无法否认的信息组成,如实体的可识别名称、电子邮箱、身份证号、电话号码等。

3.8

基于标识的密码技术　identity-based cryptography;IBC

在指定应用范围内基于用户唯一性身份标识和系统主密钥而生成用户密钥的密码机制。

3.9

密钥生成中心　key generation center;KGC

负责系统参数、主密钥、用户密钥管理、用户注册管理的服务机构。

3.10

标识密钥管理系统　key management system;KMS

支撑 KGC 可信机构的 SM9 标识密钥注册、生成、管理、发布的信息系统。

3.11

主密钥　master key

处于标识密码密钥分层结构最顶层的密钥,包括主私钥和主公钥,主私钥由 KMS 通过随机数发生器产生,主公钥由主私钥结合系统参数产生,其中主公钥公开,主私钥由 KMS 秘密保存。

注:本文件中,签名系统的主密钥与加密系统的主密钥不同。数字签名算法属于签名系统,其主密钥为签名主密钥包括签名主私钥和签名主公钥;密钥交换协议、密钥封装机制和公钥加密算法属于加密系统,其主密钥为加密主密钥包括加密主私钥和加密主公钥。KMS 用主私钥和用户的标识生成用户的私钥。

3.12

私钥生成器　private key generator

用以生成用户签名和加密私钥的设备或系统。

3.13

公开参数服务　public parameter service

用于发布基于标识的密码技术中公开参数、私钥生成策略、用户标识信息和状态等数据的应用服务,通常采用发布服务方式实现该功能。

3.14

用户签名密钥　signature key

由标识密钥管理系统将用户唯一标识利用签名主私钥进行计算产生的密钥,并下发给用户用于数

字签名和验签。

3.15

签名主密钥　signature master key

标识密钥管理系统的主签名密钥对，包括签名主私钥和签名主公钥，用于进行数字签名、验签和为用户生成用户签名密钥。

4　缩略语

下列缩略语适用于本文件。

IBC：基于标识的密码技术（Identity-Based Cryptography）

KMS：标识密钥管理系统（Key Management System）

LA：本地注册代理（Local Agency）

OID：对象标识符（Object Identifier）

PKG：私钥生成系统（Private Key Generator）

PP：参数与策略（Parameter and Policy）

PPS：公开参数服务器（Public Parameter Server）

RA：用户注册服务系统（Registration Agency）

URI：统一资源标识符（Uniform Resource Identifier）

5　基本特征描述

本文件给出的基于标识密码的标识密钥管理系统，由密钥管理系统 KMS 保持系统主密钥，为用户签发私钥，并通过安全方式传递给用户；用户的公钥计算可依据用户标识、公开参数和 SM9 相关算法。本文件支持在线或离线方式为用户签发密钥。

6　标识密钥管理系统架构

标识密钥管理系统组成包括三部分：注册服务部分、密钥生成部分和发布部分，见图 1。

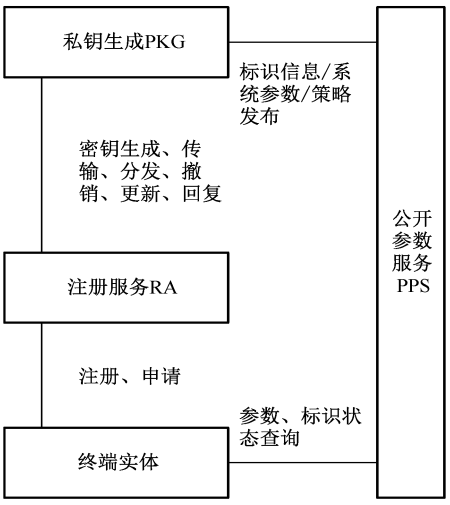

图 1　标识密钥管理系统组成

标识密钥管理系统架构具体内容见图 2，包括以下内容。

a) 私钥生成系统(PKG)，是标识密钥管理系统的核心组成部分，为用户生成私钥，进行相关管理与查询服务。PKG 用系统主密钥和相关参数，生成用户私钥。PKG 接收用户注册服务系统发来的用户私钥生成申请，生成并返回用户私钥。

b) 用户注册服务系统(RA)，用于用户密钥注册申请和本地代理接入服务，承担用户密钥申请注册、申请认证、申请管理、与 PKG 进行业务交流工作，在向 PKG 申请密钥时，为接入认证提供用户 ID 唯一性验证资料服务。用户注册服务系统可以通过本地代理(Local Agent)实现远程注册，本地代理设置于用户注册服务系统外部，用户通过本地的代理接入用户注册服务系统。本地代理作为远程代理的实体，承担为远程用户代理注册并申请密钥的功能。

c) 公开参数服务器(PPS)，是面向用户的信息服务系统，公开参数包括可公开共享的密码参数、用户标识状态目录。PPS 提供公开可访问的地址，进行公开参数和策略的安全查询与分发。

d) 终端实体(User/Client)，是应用系统的终端用户系统，直接或通过注册代理向私钥生成系统申请密钥，实现对自身私钥的存储和使用。

e) 系统安全管理与防护，应依据国家规定，设置必要的安全管理机制和防护机制。

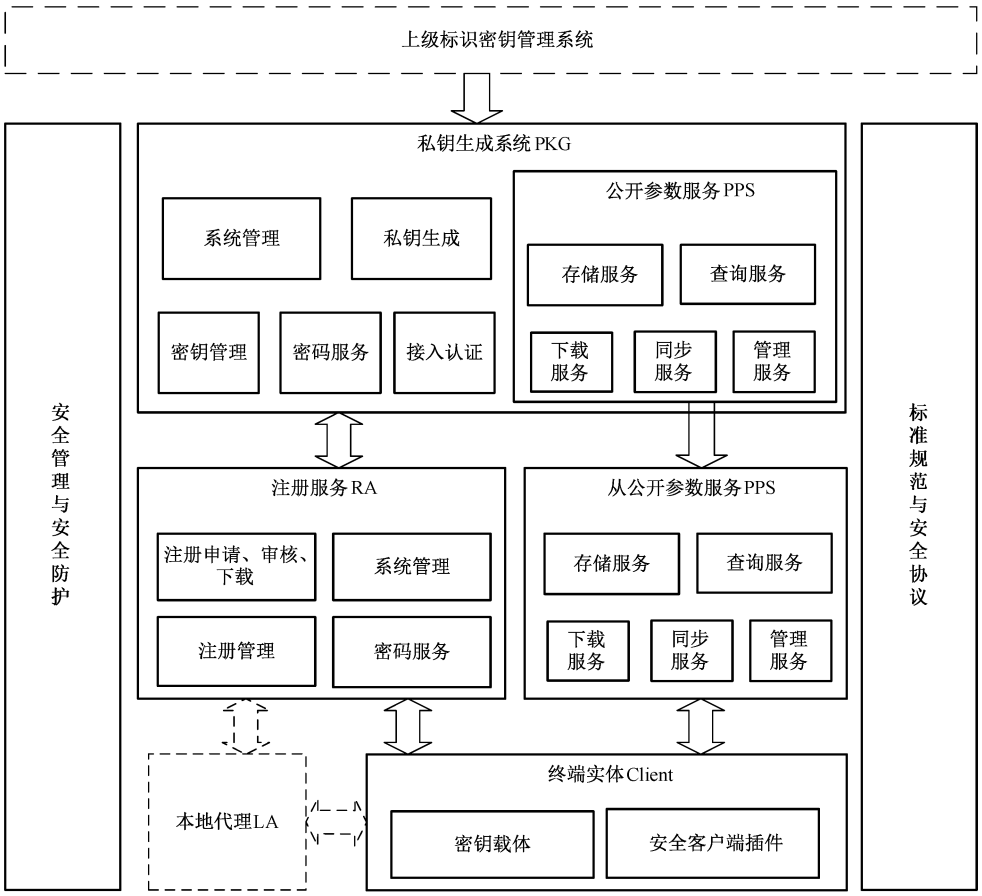

图 2 标识密钥管理系统架构

7 标识密钥管理系统组成与功能

7.1 私钥生成系统

7.1.1 私钥生成系统组成

私钥生成系统模块包括：

a) 私钥生成；
b) 密钥管理；
c) 密码服务；
d) 公开参数服务；
e) 系统管理；
f) 接入认证。

7.1.2 私钥生成系统功能

私钥生成系统功能包括以下内容。

a) 私钥生成，包括私钥生成和发布。依据主私钥和用户标识等数据生成用户私钥，并通过安全协议或安全通道进行传输与下载，密钥产生应在安全密码设备内实现。私钥生成后将产生的标识状态等信息发布到公开参数服务模块中。
b) 密钥管理，包括密钥更新、恢复、主密钥备份，以及用户标识信息存储、查询、注销等功能；
   1) 密钥更新：通过更改用户标识的方式更改密钥；
   2) 密钥恢复：个人密钥恢复可按照个人私钥重新申请方式实现；司法密钥恢复可依据法律或特定文件规定，设置专用接口，专用凭证，并设置安全访问控制技术和载体；
   3) 主密钥备份：系统主密钥实施密钥分割 m/n 安全分散方式、秘密共享机制或其他安全方式进行备份；
   4) 密钥注销：依据用户要求或系统策略实现用户标识注销，撤销后应在公开参数服务中标明已注销的标识状态。
c) 密码服务，包括主密钥生成、存储、用户私钥生成功能，并且为私钥生成模块、公开参数模块、系统管理模块、接入认证模块等提供对称密码、非对称密码以及杂凑密码算法服务。
d) 公开参数服务，包括系统和密码参数管理、系统策略管理、用户标识状态数据管理。及时向从公开参数发布服务 PPS 推送相关数据，或者撤销发布的信息。发布的数据应由 PKG 进行数字签名，保证数据的可认证和完整性。
e) 系统管理，包括系统初始化、管理员管理、安全审计、系统配置与监管等功能；
   1) 系统初始化，包括主密钥生成或导入、服务器私钥生成、相关系统参数配置、服务系统参数配置以及初始管理员生成等。
   2) 管理员管理，包括各类管理员生成、权限管理、访问认证等。
   3) 安全审计，负责各个功能模块的安全审计。具有独立的审计数据库和审计策略。由审计管理员或审计员操作管理。审计数据只可调阅，不可修改。审计日志处理情况需做标记。
   4) 系统配置与监管，包括对各功能模块、设备、系统参数配置、日志查询，以及对各个功能模块运行状态信息的获取。

7.2 注册服务系统

7.2.1 注册服务系统组成

注册服务系统模块包括：

a) 用户密钥注册申请、审核、下载；
b) 注册管理；
c) 系统管理；
d) 密码服务。

7.2.2 注册服务系统功能

注册服务系统功能包括以下内容。

a) 用户密钥注册申请、审核、下载，包括用户密码申请服务、申请信息审核服务、密钥下载服务：
   1) 用户密码申请服务，依据注册表录入用户信息，并确保标识信息的唯一性，存入数据库，包括密钥申请、更新、注销、恢复等请求。可提供单个用户或批量用户的信息录入能力。
   2) 申请信息审核服务，提取用户申请密钥的信息，审核真实身份和申请信息。审核通过后，将密钥生成所需的信息提交 PKG。
   3) 密钥下载服务，接收 PKG 返回的密钥数据包，通过认证后，向密钥数据包写入指定的密钥载体中，分发给用户。
b) 注册管理，对用户及其注册数据进行数据备份和访问控制等安全管理。
c) 系统管理，包括管理员管理、安全审计、系统配置与监管，以及为本地代理操作员签发密钥，实现代理操作员的注册等功能。
d) 密码服务，为注册系统相关功能模块提供对称密码、非对称密码以及杂凑密码算法服务。

7.2.3 注册内容

用户申请注册时，需提交如下用户信息：

a) 标识类型，如 SM9、CLA 等类型等；
b) 标识名称，如手机号；
c) 标识信息；
d) 申请者联系方式(可选)；
e) 密钥载体识别编码；
f) 其他信息(可选)。

注：对语音、图像、视频等特殊类型申请信息，用户应提供所代表对象的证明资料以及语音、图像、视频等特征标识数据。

7.3 公开参数服务系统

7.3.1 公开参数服务系统组成

公开参数服务系统模块包括：

a) 存储服务；
b) 查询服务；
c) 下载服务；
d) 同步服务；
e) 管理服务。

7.3.2 公开参数服务系统功能

公开参数服务系统功能包括：

a) 存储服务，用于存储系统公开参数、标识状态信息、变更历史信息、系统策略信息等，在公开参数服务系统中存储的信息，都应有相应 PKG 系统的签名；
b) 查询服务，包括用户标识状态查询、系统公开参数查询，查询宜支持多种索引法，通过用户状态查询可以获得标识有效性、有效期、对应系统参数、变更信息等信息；通过系统公开参数查询可以获得系统公开参数、参数变更、目前支持的所有其他参数域等信息；
c) 下载服务，支持系统公开参数下载、标识状态信息批量下载；

d) 同步服务，PPS 可采用“推”的方式，将其有关数据同步到从 PPS 中，从 PPS 也可采用“拉”的方式，从主 PPS 中获取信息；

e) 管理服务，提供 URL 配置、系统公开参数配置、系统策略信息配置、发布信息验证功能。

7.4 终端实体

7.4.1 终端实体组成

终端实体包括：

a) 密钥载体；

b) 安全客户端插件。

7.4.2 终端实体功能

终端实体功能包括：

a) 密钥载体，用于安全存储用户私钥，以及进行密码计算，硬件密钥载体中在安全密码芯片中存储私钥并进行相关计算，密钥载体中还存储系统公开参数用于密码计算；

b) 安全客户端插件，包括基于密钥载体的安全中间件接口和安全协议，为客户端密钥管理和各种密码应用提供接口服务。

7.5 本地代理

远程用户可以通过本地代理向注册服务系统提交注册申请，并接受注册服务系统的各种返回信息，以及密钥下载。

8 密钥管理基本要求

8.1 密钥申请登录认证

用户登录标识密钥管理系统申请私钥，应进行登录身份鉴别和私钥申请认证，具体要求包括：

a) 对申请用户的真实性和有效性验证，需提供相应有效材料，有条件的采用现场面对面方式验证；

b) 对硬件密钥载体进行合规性鉴别，应通过国家密码管理部门的认证，并核实载体与用户身份绑定关系；

c) 申请私钥的数据包应做完整性认证。

8.2 密钥生成

8.2.1 系统主密钥对生成

PKG 产生随机数 $k_s \in [1, N-1]$ 作为签名主私钥，计算 G_2 中的元素 $P_{pub-s} = [k_s]P_2$ 作为签名主公钥，则签名主密钥对为 (k_s, P_{pub-s})。PKG 秘密保存 k_s，公开 P_{pub-s}。见 GM/T 0044.2—2016 中 5.3，具体参数见 GM/T 0044.5—2016 中第 3 章。

PKG 产生随机数 $k_e \in [1, N-1]$ 作为加密主私钥，计算 G_1 中的元素 $P_{pub-e} = [k_e]P_1$ 作为加密主公钥，则加密主密钥对为 (k_e, P_{pub-e})。PKG 秘密保存 k_e，公开 P_{pub-e}。见 GM/T 0044.3—2016 中 5.3，具体参数见 GM/T 0044.5—2016 中第 3 章。

8.2.2 用户密钥对生成

用户密钥对的生成包括签名私钥和加密私钥，具体方法见 GM/T 0044.2 和 GM/T 0044.4。

8.3 密钥传输

密钥传输包括：

a) 用户密钥通过安全加密或者安全通道方式传送到用户密钥载体，PKG 对用户密钥进行签名、加密保护，通过注册系统安全下载到用户密钥载体；

b) 用户密钥下载的安全传输协议，参见附录 C。

8.4 密钥存储

密钥存储包括：

a) 本文件支持标识密钥管理系统只存储标识信息（用户标识、名称、相应的主私钥版本号、hid 码版本号、有效期，生成时间），如果有特殊要求需要存储用户私钥，用户私钥依据私钥生成系统存储要求，用对称加密算法加密保护；

b) 对于安全要求高的客户端使安全硬件如智能密码钥匙保存密钥，对于安全要求不高的按照不同密码模块安全要求保存密钥；

c) 作废的私钥目录应安全存储于历史库，以备事后查询，保留年限由系统策略确定。

8.5 密钥更新

用户更新自己的密钥，先申请原密钥作废，再申请新密钥分发。密钥更新可包括改变标识、改变有效期等方式。

8.6 密钥注销

用户密钥注销，由用户到注册点或代理点进行申请。注册点或代理点依据策略，经审核后，进行密钥作废操作，并将相关信息传给 PKG。PKG 将该用户 ID 从在用密钥库撤销，并将其转移到历史库。对该密钥相关的 ID 进行撤消签名，改变该 ID 的状态标志，并送入 PPS 服务器。历史库的数据可依据安全策略，定期转移到磁带、磁盘或其他存储介质安全保留或销毁。

8.7 密钥备份

主私钥备份采用密钥分割、秘密共享机制备份方式或者其他安全方式。备份数据格式应包括私钥版本号、私钥实体、hid 码、有效时间等项。

8.8 密钥恢复

8.8.1 基本要求

系统应分别设置用户密钥恢复与司法密钥恢复。用户密钥恢复只限于对客户本身的密钥进行恢复；司法密钥恢复依据国家安全法规实施。用户密钥恢复应到注册点或代理点申请。司法密钥恢复可到私钥生成系统实施，或经过私钥生成系统认证控制实施。

8.8.2 用户密钥恢复

用户密钥恢复设置单独的管理系统。密钥恢复实施要求：持有效证明材料，到注册服务系统或其代理点申请。经受理者审核后，且只可对有效证明材料一致的用户密钥实施恢复。

8.8.3 司法密钥恢复

司法密钥恢复应依据国家安全法规，严格按照法律程序实施，可设置司法密钥恢复管理平台，配置必需的安全应用软件，建立严格的安全管理程序、工作流程和工作制度，切实保护国家利益，保护公民隐私。

a) 系统结构

司法密钥恢复设置单独的管理系统。该系统涉及认证鉴别，密钥生成，密钥下载，审计管理、参数管理等模块，应保障被执法恢复的数据安全传送和安全下载。

b) 终端部署

司法密钥恢复管理系统设置于私钥生成系统。具体实现方式可采用：

1) 各个地区或部门的应用系统到私钥生成系统实施司法密钥恢复申请，依据系统安全策略，经鉴别验证后，现场进行响应恢复；

2) 应用部门设置访问终端，通过安全通道和访问控制协议实施密钥安全恢复。密钥恢复时，登录私钥生成系统，请求密钥恢复，密钥恢复管理系统验证后，进行响应，依据权限打开相关通道，支持特定执法应用终端实现特定的密钥恢复。

c) 安全审计

密钥恢复应作安全审计。审计管理员依据规定，将密钥恢复审计记录汇总上报。该信息应严格保密控制，不得向外泄露。

8.9 系统主密钥管理

系统主密钥应加密存放在密码机安全存储区，同时采用密钥分散机制安全备份保管。

9 标识密钥管理系统密码使用

9.1 密码算法使用

9.1.1 加密运算

加密运算包括：

a) 非对称加密算法，遵循 GM/T 0044.4—2016；

b) 对称加密算法，遵循 GB/T 32907。

9.1.2 签名/验证运算

遵循 GM/T 0044.2—2016。

9.1.3 密钥交换

遵循 GM/T 0044.3—2016。

9.1.4 密钥封装

遵循 GM/T 0044.4——2016。

9.1.5 密码杂凑算法

遵循 GB/T 32905。

9.2 密码设备

标识密钥管理系统应采用国家密码主管部门批准使用的密码设备，包括：

a) 服务端密码设备：除能提供密钥空间、密钥管理、密码算法（例如：数据加密/解密、数字签名/验证、摘要运算、双线性对运算、密钥生成）等基本功能外，还需设有载体唯一编号、能够配置密码算法参数、支持密钥下载协议等内容；

b) 客户端密码模块：除能提供密钥空间、密码算法（例如：数据加密/解密、数字签名/验证、摘要运算、双线性对运算、密钥生成）等基本功能外，还需设有载体唯一编号、能够配置密码算法参

数、支持密钥下载协议等内容。

10 密钥管理安全操作流程

10.1 系统初始化流程

KMS初始化之前应完成管理人员设置、角色定位、管理制度、通用硬件设备的配置、基础软件安装调试等基础工作。

初始化应在安全条件下完成下列工作。

a) 配置相应密码设备，完成初始化、设备密钥生成以及自检(预先实施)。

b) 安装KMS相关软、硬件系统(预先实施)。

c) 首先，进行PPS系统初始化，配置公开系统参数，等待PKG生成主公钥，并导入PPS用于验证PKG信息，由PKG为PPS生成管理员，当主公钥导入完成后PPS系统初始化完成。

d) 再次，进行PKG初始化，配置系统参数(包括秘密参数和公开参数)，生成系统主密钥(需将主公钥导入到PPS中)，并安全备份；PKG完成自身初始化管理员私钥的签发，生成初始化管理员，向PPS发布自签的PKG标识、主公钥、对应的系统参数和公开参数标识包，PKG初始化完成。由PKG初始化管理员完成PKG其他管理员私钥签发和角色配置，PKG可以正常工作。

e) 最后，进行RA系统初始化，由PKG为RA系统密码设备签发标识私钥，RA系统进行自身初始化配置，生成RA系统初始化管理员，RA系统初始化完成。

f) KMS初始化完成。

g) 如何有LA应继续进行下列工作。

h) 通过RA对LA进行注册，并签发相应LA的标识私钥。

10.2 密钥载体初始化

需预先对用户载体进行初始化，将系统运行所需必要内容安全预制、下载到用户终端载体，内容包括：

系统公开参数：G_1，G_2，P_1，P_2，g_1，g_2，p_{pub1}，p_{pub2}，p，e。

其中，$P_{pub1}=[s]P_1$，$P_{pub2}=[s]P_2$，$g_1=e(p_{pub1},P_2)$，$g_2=e(P_1,P_{pub2})$。P_{pub1}，g_1 用于加密；P_{pub2}，g_2 用于签名，g_1、g_2 为双线性对运算，详细定义见GM/T 0044.1。

10.3 用户密钥生成流程

用户密钥生成流程包括：

a) 用户申请密钥前载体应已经进行了初始化，见10.2；

b) 将密钥载体与申请终端设备连接，进行载体确认，获取载体序列号Sn和载体密钥密文，参见附录C；

c) 用户直接或通过LA向RA系统发出用户私钥申请，如果通过LA向RA申请，需要LA对申请信息附上自身的Sn进行签名，RA对LA的申请信息进行验证；

d) 用户注册时，应如实填写注册登记表。RA的接入认证系统对申请信息进行认证，确认标识的唯一性；

e) 审核用户身份数据真实性、完整性；

f) 若审核通过，RA系统依据用户申请表内容，生成用户申请密钥数据，对有关数据做数字签名和加密，生成申请用户私钥消息，发送给PKG；

g) PKG做双向身份鉴别，验证RA签名，确认标识的唯一性，利用系统参数生成用户私钥，并把用户标识状态信息发布到PPS上；

h) PKG 对用户私钥密文和相关信息组成响应数据包并进行数字签名，回送给 RA；

i) RA 做双向身份鉴别，验证收到的数据，验证通过后，把私钥密文数据直接或通过 LA 下载到用户密钥载体内；

j) 在用户密钥载体内安全解密，验证私钥正确性，如果正确，安全存储用户私钥。

身份鉴别协议应遵循 GM/T 0057。

用户密钥申请总流程如图 3 所示。

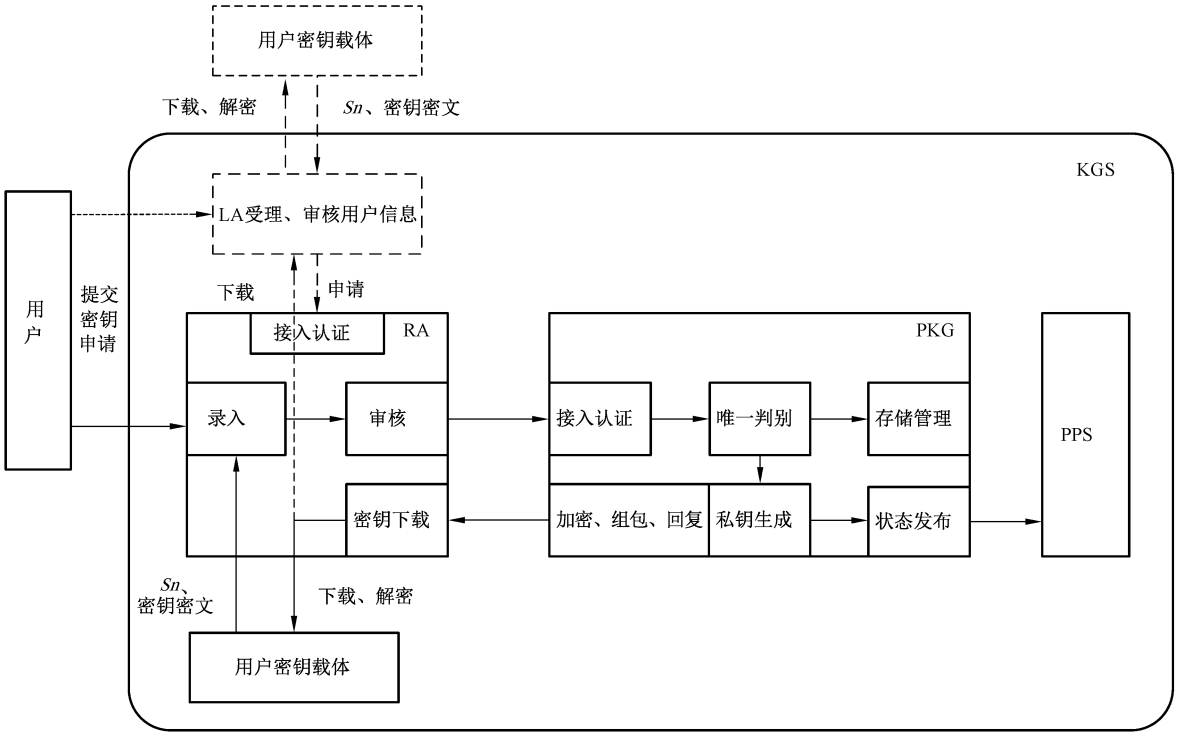

图 3 密钥生成流程图示

10.4 标识状态发布流程

10.4.1 新增用户标识密钥状态发布流程

新增用户标识密钥状态发布流程如下：

a) 用户申请密钥完成后，PKG 系统对该用户的身份标识、相关有效状态、有效期等数据进行签名，发布到 PPS；

b) PPS 对 PKG 的数据进行验证后，由 PPS 增加并标注该标识信息，存放于公开参数服务器的用户标识状态库。

10.4.2 注销用户标识密钥状态发布流程

注销用户标识密钥状态发布流程如下。

a) 由 RA 或 LA 办理标识密钥注销申请。如果欲被注销的标识的密钥可以使用，则用欲被注销的标识私钥对注销信息表签名，并附上申请办理者相关身份信息即可；如果欲被注销的标识的密钥无法使用，申请办理者需提供该标识申请时的证明材料，核实与申请注册时的数据相同即可。

b) RA 将申请注销的标识信息签名发送给 PKG，此过程与 10.3 f)过程相同，PKG 对该标识相关信息进行注销处理，并将相关状态及时间数据进行签名，发布到 PPS。

c) PPS 对 PKG 的数据进行验证后，由 PPS 修改标识信息状态内容，存放于公开参数服务器的用户标识状态库。

10.4.3 冻结用户标识密钥状态流程

冻结用户标识密钥状态流程如下。

a) 由 RA 或 LA 办理标识密钥冻结申请。申请办理者需提供该标识冻结原因证明材料，核实后方能进行。
b) RA 将申请冻结的标识信息签名发送给 PKG，此过程与 10.3 f)过程相同，PKG 对该标识相关信息进行冻结处理，并将相关状态及时间数据进行签名，发布到 PPS。
c) PPS 对 PKG 的数据进行验证后，由 PPS 修改标识信息状态内容，存放于公开参数服务器的用户标识状态库。

10.4.4 恢复用户标识密钥状态流程

恢复用户标识密钥状态流程如下。

a) 由 RA 或 LA 办理标识密钥恢复申请。申请办理者需提供该标识恢复原因证明材料，核实后方能进行。
b) RA 将申请恢复的标识信息签名发送给 PKG，此过程与 10.3 f)过程相同，PKG 对该标识相关信息进行恢复处理，并将相关状态及时间数据进行签名，发布到 PPS。
c) PPS 对 PKG 的数据进行验证后，由 PPS 修改标识信息状态内容，存放于公开参数服务器的用户标识状态库。

10.5 更新用户标识密钥状态流程

更新用户标识密钥状态流程如下。

a) 用户提供规定的变更信息数据，包括原标识、变更标识、变更原因等。
b) 由 RA 或 LA 办理标识密钥更新申请。用原标识私钥对变更信息表签名，并附上申请办理者相关身份信息即可。
c) RA 验证签名数据和申请信息后，RA 将申请变更的标识信息签名发送给 PKG，此过程与 10.3 f)过程相同。PKG 先将原标识及其对应的密钥作废，然后签发新标识对应的密钥，并将更新变化数据送给 PPS 系统，更新目录服务内容。
d) PKG 加密新密钥安全传送 RA，后续过程与 10.3 g)～j)过程相同。

10.6 恢复用户标识密钥状态流程

10.6.1 用户密钥恢复

用户的密钥遭到毁坏，用户可通过 RA 办理密钥恢复，用户密钥恢复流程如下：

a) 用户提出申请密钥时的信息；
b) RA 或者 LA 比对审核注册记录；
c) RA 按照用户密钥生成的流程将密钥恢复数据包送交 PKG；
d) PKG 接收申请数据包，依据系统策略，验证恢复申请；
e) RA 按照用户密钥生成的流程将被恢复的密钥安全下载到用户密钥载体。

10.6.2 司法密钥恢复

司法密钥恢复在 PKG 办理，其操作流程依据 8.8.3 要求实施。

10.7 用户信息状态查询与响应流程

用户信息状态查询与响应流程如下：

a) 用户通过 URL 访问 PPS,提出查询申请;
b) 用户发送查询申请,可以通过注册的名称、注册的标识、注册的唯一编码等,提出需要查询的状态、历史变更信息等;
c) PPS 接收申请数据包,根据请求响应查询,返回被查询标识、状态、有效期、历史变更记录等内容。

10.8 主密钥更新流程

主密钥更新需采用公开参数标识方式标识不同的主密钥。公开参数标识用于区分不同主密钥、其他公开系统参数组成的独立信任域,也可以视为直接区分不同 KMS 的特征标识,主密钥更新流程如下:

a) 主密钥更新由 PKG 实施,主密钥更新将生成新的主密钥,并备份原主公钥及其对应的系统参数;
b) 由原主私密钥签名将更新的主公钥,推送到 PPS 中替换验签中的原主公钥;
c) PKG 将 PKG 标识、原主公钥、对应的系统参数和公开参数标识进行签名,同时将新主公钥对应的系统参数和自己的公开参数标识进行签名,发布到 PPS 中;
d) PPS 将原主公钥和相关参数进行注销操作;
e) PPS 发布新主公钥和相关参数。

11 标识密钥管理系统建设与安全防护

11.1 系统建设

11.1.1 物理环境要求

PKG 中心的建筑和机房建设应按照国家密码管理局相关要求,遵照下列标准实施:

a) GB/T 9361—2011;
b) GB/T 2887—2011;
c) GB 50174—2017。

11.1.2 网络配置

应合理划分系统网络的安全域,在 B/S 结构条件下,至少应划分为三部分:

a) 服务域:应用用户所在的网络,所有用户通过该网络访问 LA 和从 PPS;
b) 管理域:为系统用户提供注册,从公开参数服务,以及提供用户访问界面,该域也是外部用户访问内部功能的前置接入网络系统,RA 部署在该区;
c) 核心域:包括系统的各种核心服务系统、数据系统,PKG、主 PPS 部署在该区。

11.2 安全防护设置

11.2.1 系统安全

应采用合理的系统安全防护机制,包括:

a) 设置综合防护技术,实现统一威胁管理,保护整个系统安全;
b) 设置系统检测与维护机制,保障整个系统的软硬件安全运行;
c) 设置系统可靠性保障机制,保障系统稳定不间断工作。

11.2.2 接入与边界安全

系统应设置安全认证与访问控制机制,保障系统接入和系统边界安全。

a) 访问控制对象包括服务器、代理点 PC 机、密码系统、操作系统、业务系统和数据库系统层面的访问控制，防止受到人为或自然灾害的攻击与破坏。
b) 访问控制技术应设置身份鉴别、授权管理、安全标记、可信路径、安全审计和资源控制等安全保护技术，保障操作系统和数据库系统在内的网络系统安全。
c) 设置边界防护技术，保护网络边界安全，防止受到非法的攻击与破坏，保护系统的安全和网络正常服务。其主要内容包括：设置防火墙、入侵检测、漏洞扫描、恶意代码防治、边界访问过滤控制；设置边界安全访问控制技术，实现安全可靠的访问与响应。

11.2.3 主机安全

系统应设置合理的安全机制保证系统内主机的安全。
a) 应设置访问控制机制；
b) 应设置身份鉴别机制；
c) 应设置主机的安全审计机制；
d) 应设置主机的入侵检测和恶意代码防范机制；
e) 应设置主机或关键元件的备份与资源控制机制；
f) 设置剩余信息保护机制，保护存储空间安全。

11.2.4 密钥数据安全

11.2.4.1 基本要求

KMS 密钥管理的基本要求是：
a) 私钥的生成与使用应在硬件密码设备中实现；
b) 私钥不以明文形态出现在硬件密码设备之外；
c) 主私钥应有安全可靠的备份与恢复机制；
d) 对主私钥的备份、恢复操作应由多个操作员实施。

11.2.4.2 主密钥

主密钥安全应满足如下要求。
a) 系统主密钥应由硬件密码设备生成，主私钥存储于密码设备中。
b) 主密钥应进行安全备份，宜采用密钥分割、秘密共享机制进行备份。依据系统安全策略，选定备份密钥的分管者，分管的密钥应在口令控制下安全存放于有备份的智能密码钥匙中。
c) 主密钥恢复应采用 m/n 机制，选定所需的 m 个分管人员，通过口令认证，在密码设备中恢复。
d) 主密钥更新应依据系统安全策略，参照密钥生成要求实施。若无特殊安全原因，主密钥不宜频繁更新。
e) 主密钥废除与主密钥更新同步进行。
f) 主密钥销毁应由密码主管部门授权机构实施，且其备份密钥同时销毁。

11.2.4.3 代理点密钥

除基本要求外，代理点密钥应满足如下要求：
a) 私钥生成与更新由注册系统管理员实施；
b) 私钥的使用应在硬件密码载体内实施。

11.2.4.4 管理员密钥

除基本要求外，各类管理员密钥应满足如下要求：
a) 管理员私钥的使用应在其硬件载体内实现；

b) 管理员的私钥使用应设置安全可靠的权限管理机制和口令控制；
c) 管理员的账号应和普通用户的账号严格分类管理；
d) 管理员私钥的使用应设置审计机制。

11.2.4.5 用户密钥

除基本要求外，用户密钥应满足如下要求。

a) 用户私钥生成、分发。私钥生成系统依据系统主私钥和用户身份标识统一生成与分发用户私钥。
b) 用户私钥安全传输。私钥生成系统到用户之间通过安全协议，将用户私钥安全加密传输并下载到用户密钥载体。
c) 用户私钥安全存储。用户私钥采取加密方式进行存储。本文件允许不设置用户私钥库，可设置用户密钥记录索引，内含用户名、标识、注册时间、有效期、主私钥版本、hid 码版本等项。
d) 密钥安全恢复。系统支持司法密钥恢复和用户密钥恢复。密钥恢复直接在 PKG 进行，或依据策略和协议通过网络实施。被恢复的密钥应安全注入特定载体。

12 安全管理要求

12.1 安全管理机制

系统应设置合理的安全管理机制，包括：

a) 生成用户私钥的机构应遵守国家相关管理条例和规范，确保系统安全、主私钥安全和用户私钥安全；
b) 系统应采用国家发布的标准密码算法和相应参数；
c) 用户私钥的生成、传送、存储和使用应在安全环境下，通过安全协议实现；
d) 每个客户端载体需配置具有个性特征的安全参数，本文件客户端载体宜采用安全硬件（例如智能密码钥匙）作为私钥载体，含有相关密码算法、用户标识、载体唯一编号、用户密钥、系统基本参数、用户口令字验证码等信息，用户应依据密钥生成机构提示和要求，妥善保护好其私钥和安全载体；
e) KMS 应提供并配置标准的客户端安全插件，包括安全协议、安全参数和安全使用说明；
f) 本文件规定一个用户可拥有多个标识对应于不同应用，但不准许多个用户使用同样的一个标识。

12.2 人员管理

系统应设置如下管理和操作人员：初始化管理员，超级管理员，审计管理员，业务管理员，系统管理员、安全管理员和相应的业务操作员，并规范各类人员职责。

a) 初始化管理员负责系统在初始化过程中创建系统超级管理员、系统主密钥生成等初始操作，初始化完成后不再使用；
b) 超级管理员负责系统策略管理、人员设置管理、人员授权管理；
c) 审计管理员负责系统安全事件、各类管理人员与操作人员的行为审计与监督，参与人员授权管理；
d) 业务管理员负责某个业务子系统的业务管理、操作员设置与授权；
e) 系统管理员负责系统与网络的正常运行、维护与管理；
f) 安全管理员负责整个系统的安全与保密工作；
g) 业务操作员负责执行并完成本职责与权限内的业务操作；
h) 各类人员进行系统登录或操作时，需插入本人密码载体，系统依据身份认证码和预先注册分配

的权限进行身份鉴别和操作权限控制。

12.3 管理制度

系统应制定完善的管理制度，包括：

a) 依据国家相关规范和条例要求建立系统的安全运维管理制度；
b) 依据国家相关要求建立等级保护安全管理机制；
c) 系统应按照 GB/Z 24364 要求，建立管理规范和安全管理制度，定期进行风险分析与评估，明确处理残余风险的原则，实施系统安全技术升级，保障系统和设备高效稳定运行；
d) 系统应按照 GB/T 24363 要求，建立应急处理机制，包括：制定应急响应预案，能及时处理系统故障或重大灾难性事故；依据事件严重程度、紧急程度和事件类别规范其告警、报告、保护、处理、善后、总结等相关流程和处置措施，并应尽快查明起因，消除事故；系统恢复正常运行后，应对应急处理过程进行总结，详细记录事件起因、影响范围、处理过程、明确经验教训，提出改进建议。

12.4 审计管理

系统应建立完善的审计管理机制，包括以下内容。

a) 建立安全审计系统，对系统的操作行为进行安全审计与追踪，实现责任认定功能。依据审计数据存储空间的容量，制定审计数据处理策略。审计管理员可依据策略处理审计数据，但不可修改或删除数据。
b) 功能模块调用审计，系统内各服务功能模块之间发生相互请求调用操作行为时，各模块应做日志记录。
c) 管理员操作审计，系统管理员的有关操作应做日志记录。
d) 业务操作员操作审计，业务操作员的有关操作应做日志记录。
e) 代理点接入审计，代理点的有关操作应做日志记录。
f) 维护员测试操作审计，维护员的有关操作应做日志记录。

12.5 管理平台

依据信息系统安全等级保护要求，系统可设置安全管理平台，通过安全管理平台实现系统安全监控、安全审计、安全防护以及风险评估和等级保护等综合管理。

13 标识密钥管理系统层次结构

13.1 标识密钥管理系统类型

标识密钥管理系统的类型包括独立部署类型和分级类型。

独立部署类型的标识密钥管理系统可以自行产生主密钥和设置应用层主密钥。不同应用系统的用户密钥可由不同或同一主密钥统一管理。

分级类型的标识密钥管理系统依据管理需求，可设置下级标识密钥管理系统，其下级主密钥可由上级标识密钥管理系统产生，利用密钥分发机制导入下级系统；或者采用自行产生后，向上级报备主公钥的方式，如图 4 所示。

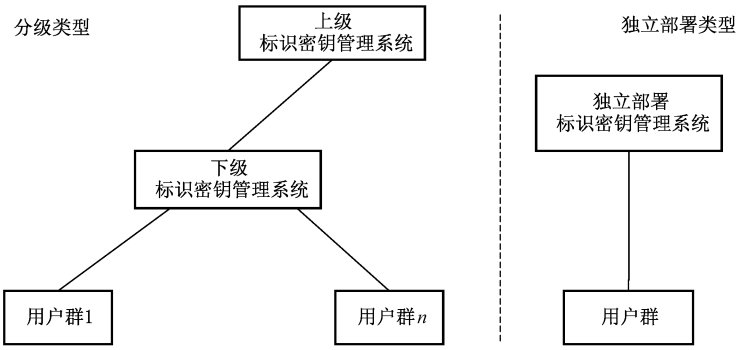

图 4　标识密钥管理系统类型图

13.2　区分 KMS 的标识

在分级类型的标识密钥管理系统中，每一 KMS 应分配唯一标识，这里我们采用 10.8 中公开参数标识的方法。标识数据结构包含当前 KMS 的标识和其上级 KMS 的标识，其定义见 GB/T 33560—2017。

13.3　注册下级 KMS

分级标识密钥管理系统，可以申请注册为当前 KMS 的下级 KMS，实现标识密钥管理系统的分级管理。

下级 KMS 应按照 7.2 的用户注册流程向其上级 KMS 注册并产生用户密钥，用户秘钥用于加密通信或对下级 KMS 的主公钥进行签名。顶级 KMS 的上级 KMS 可视为自己。

13.4　下级 KMS 主密钥生成流程

下级 KMS 的主密钥，可以通过两种方式产生。

a）　报备方式，下级 KMS 根据 8.2.1 产生一对主密钥，并通过下列流程由其上级 KMS 对其主公钥签名：

1）　下级 KMS 发出申请，双方身份认证。

2）　下级 KMS 发送申请数据包：data1 ＝ 申请类型 ‖ 下级 KMS 名称 ‖ 下级 KMS 标识 ‖ 下级 KMS 主公钥密钥（签名主公钥/加密主公钥）‖ 时间。

3）　发送：data2 ＝ $\mathrm{Sign}_{\text{下级KMSPriKey}}$(data1)。

4）　上级 KMS 接收申请数据包并做处理。验证下级 KMS 身份信息和标识，用主签名密钥对下级 KMS 主公钥进行签名，并发布到上级 PPS 中。

5）　响应：响应类型 ‖ 下级 KMS 用户名 ‖ 下级 KMS 标识 ‖ 对下级 KMS 主公钥的签名值 ‖ 签名时间。

6）　下级 KMS 将被上级签名的主公钥信息发布到自己的 PPS 中。

7）　将事件记入审计系统。

b）　分发方式，下级 KMS 通过下列流程向其上级 KMS 申请产生主密钥对并签名。

1）　下级 KMS 发出申请，双方身份认证。

2）　下级 KMS 生成对称加密密钥 r，并用上级主加密公钥加密 $E_{\text{上级KMSenPUBKey}}(r)$。

3）　下级 KMS 发送申请数据包：data1 ＝ 申请类型 ‖ 下级 KMS 用户名 ‖ 下级 KMS 标识 ‖ $E_{\text{上级KMSenPUBKey}}(r)$ ‖ 时间。

4）　上级 KMS 接收申请数据包并做处理。验证下级 KMS 身份信息和标识，采用国家密码管理部门规定的密钥分发算法生成下级 KMS 的主私钥，并用下级 r 加密 data3＝Enc_r（下级 KMS 的主私钥）。

5）　同时计算出下级 KMS 的主公钥，并使用自己的主签名密钥对下级 KMS 主公钥进行

签名。

6) 响应:data3 = 响应类型 ‖ 下级 KMS 用户名 ‖ 下级 KMS 标识 ‖ data3 ‖ 下级 KMS 主公钥签名 ‖ 时间,并由上级 KMS 签名。

7) 下级 KMS 验证 data3 的签名,在密码机中解密获得主私钥,将主公钥发布到自己的 PPS 中。

8) 将事件记入审计系统。

13.5 下级 KMS 主密钥发布

13.5.1 下级 KMS 主密钥生成发布

下级 KMS 主密钥生成发布流程如下:

a) 下级 KMS 产生应向 PPS 发布其公开参数;
下级 KMS 主密钥生成完成后,上级 KMS 对该 KMS 的身份标识、主公钥、状态信息等数据进行签名并提交公开参数服务系统 PPS;
PPS 对提交的数据进行验证,通过后,由 PPS 加注该标识的数据格式信息,存放于公开参数服务器。

13.5.2 下级 KMS 主密钥更新发布

下级 KMS 主密钥更新发布流程如下:

a) 报备方式,按照 13.4 a)方式获得新被签主密钥;

b) 再按照 10.8 b)~10.8 e)的步骤发布信息。

13.5.3 下级 KMS 主密钥作废发布

下级 KMS 主密钥作废发布流程如下:

a) 下级 KMS 向上级 KMS 提出更新申请;

b) 上级 KMS 对该 KMS 的标识及相关作废状态及时间数据进行作废签名并提交公开参数服务系统 PPS;

c) PPS 对上级 KMS 提交的数据进行验证,通过后,由 PPS 加注该作废 KMS 标识的数据格式信息,存放于公开参数服务器的用户 ID 状态库。

13.6 验证 KMS 主密钥

验证 KMS 的主公钥。属不同层级 KMS 下的用户需要相互进行密码运算时,用户本地可能未保存对方 KMS 主公钥信息,或需要验证对方 KMS 主公钥是否可信,则需要向 PPS 查询并验证对方 KMS 的主公钥。

a) 用户向签发自己标识密钥所属 PPS 提出申请。

b) 用户发送查询申请:用户名 ‖ 标识 ‖ 被查询 KMS 标识 ‖ 时间。

c) PPS 接收申请数据包,响应查询:用户名 ‖ 标识 ‖ 被查询 KMS 标识 ‖ 被查询 KMS 的上级 KMS 标识 ‖ 被查询 KMS 主公钥 ‖ 被查询 KMS 主公钥签名 ‖ 时间。

d) 用户接收到 PPS 响应数据包,使用被查询 KMS 的上级 KMS 标识对被查询 KMS 主公钥签名进行签名验证。若想进一步验证被查询 KMS 的上级 KMS 标识及其主公钥,则重复 a)~d)。

e) 验证成功,确认对方 KMS 主公钥。

附 录 A
（规范性）
密码算法的 OID 与算法标识

本附录依据 GB/T 33560 中的有关密码算法 OID，在原基础上宜增补与 SM9 密码算法有关的 OID，具体内容见表 A.1～表 A.4。

表 A.1 算法对象标识符的相关 OID 定义

对象标识符 OID	对象标识符定义	备注
1.2.156.10197.1.302	SM9 标识密码算法	
1.2.156.10197.1.302.1	SM9-1 数字签名算法	
1.2.156.10197.1.302.2	SM9-2 密钥交换协议	
1.2.156.10197.1.302.3	SM9-3 密钥封装机制和公钥加密算法	
1.2.156.10197.1.502	基于 SM9 算法和 SM3 算法的签名	
1.2.156.10197.6.2	PPS 代码	

表 A.2 非对称密码算法的标识

标签	标识符	描述
SGD_SM9	0x00040100	SM9 IBC 密码算法
SGD_SM9_1	0x00040200	SM9 IBC 签名算法
SGD_SM9_2	0x00040400	SM9 IBC 密钥交换协议
SGD_SM9_3	0x00040800	SM9 IBC 加密算法

表 A.3 签名算法的标识

标签	标识符	描述
SGD_SM3_SM9	0x00040201	基于 SM3 算法和 SM9 算法的签名

表 A.4 通用数据对象标识

标签	标识符	描述
SGD_PUBLIC_KEY_SIGN	0x00000118	SM9 签名公钥
SGD_ PUBLIC_KEY_ ENCRYPT	0x00000119	SM9 加密公钥
SGD_ PRIVATE _KEY_SIGN	0x0000011A	SM9 签名私钥
SGD_PRIVATE_KEY_ ENCRYPT	0x0000011B	SM9 加密私钥

附 录 B
（资料性）
标识密钥管理系统网络结构

核心域、管理域和服务域，PKG 的网络结构见图 B.1。系统配置有 SM9、SM3、SM4 密码算法的密码机，并根据需要可设置冗余结构。

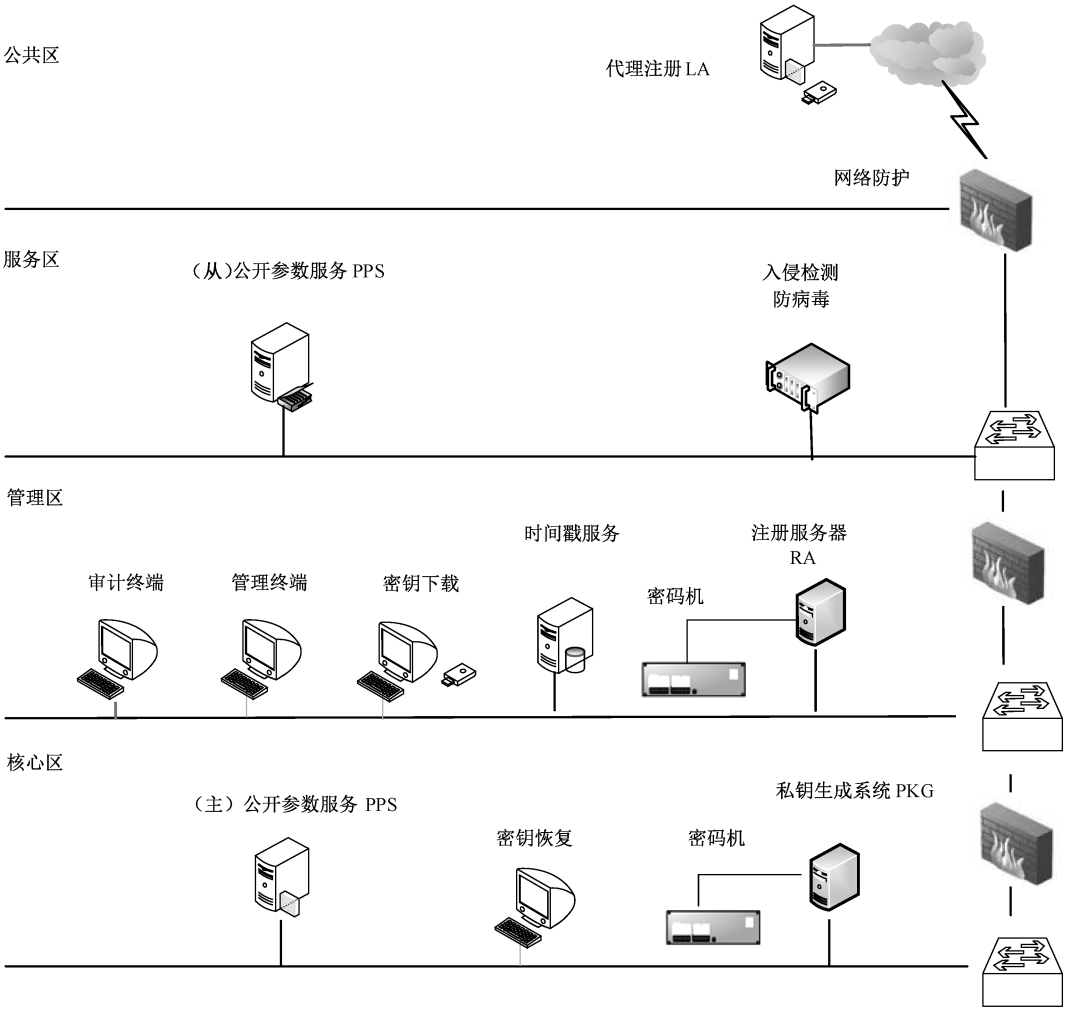

图 B.1 C/S 模式时 PKG 的网络结构图示

附 录 C
（资料性）
用户第一次申请密钥流程

这里给出支持离线方式的用户密钥申请流程。

本部分使用的数学符号的定义见 GM/T 0044。

a） 注册申请

从注册点申请签发密钥，根据提交的资料填写注册表。

b） 注册审核

审核用户申请材料。若未通过审核，则中断操作。若通过，则继续做密钥申请。

c） 注册点生成并发送申请数据

1） 用户载体中生成随机数 $r1$ 作为对称密钥。用 PKG 通信公钥加密生成 $P(r1)$，送给注册点。

2） 注册点提取用户注册表中相关项数据和 $P(r1)$，生成 Data1。

Data1＝[用户注册名、用户标识 ID、终端载体号 EID、$P(r1)$]。

3） 注册点对 Data1 做数字签名 $sign=SIGN$(Data1)，并生成数据包 Data2。

Data2＝[用户注册名 ‖ 用户标识 ID ‖ 终端载体号 EID ‖ $P(r1)$ ‖ $sign$]。

4） 注册点生成随机数 $r2$ 作为对称密钥，用 PKG 公钥加密 $r2$，生成 $P(r2)$。

5） 注册点用对称密钥 $r2$ 对 Data2 加密，生成数据包 Data3。

Data3＝$Er2$(Data2)。

6） 注册点发送申请数据包 Data4 给 PKG。

Data4＝$P(r2)$ ‖ Data3。

d） PKG 验证申请数据包

1） PKG 收到数据包 Data4。用本方私钥 d_{PKG} 解密 $P(r2)$。$Ed_{PKG}[P(r2)]=r2$，得到对称密钥 $r2$。

2） PKG 用 $r2$ 解密数据包 Data3，$DEr2$(Data3)＝Data2＝[用户实名 ‖ 用户标识 ID ‖ 终端载体号 EID ‖ 电话号码 ‖ 电子邮箱 ‖ 通信地址 ‖ $P(r1)$ ‖ $sign$]。

3） PKG 验证 Data2 数字签名 $sign$。

4） PKG 用本方私钥解密 Data2 中的 $P(r1)$。$Ed_{PKG}[P(r1)]=r1$，得到对称密钥 $r1$。

e） PKG 生成并发送用户密钥

1） PKG 生成标识为 ID_A 的用户私钥 d_A。

2） PKG 用 $r1$ 对 d_A 加密，生成 $E(d_A)$，并做 $Hash(d_A)=H$。

3） PKG 生成 Data5，用本方的私钥 d_{PKG} 对 Data5 做数字签名 $sign$。

Data5＝[用户名 ‖ 用户标识 ID_A ‖ $E(d_A$ ‖ $H)$ ‖ 有效期]。

$sign=SIGNd_{PKG}$(Data5)＝(h,S)。

4） PKG 生成随机数 $r3$，作为对称密钥。

PKG 用密钥 $r3$ 对数字签名 $sign$ 和签发时间 t 等数据进行加密，生成 Data6，

Data6＝$Er3$[用户名 ‖ 用户标识 ID_A ‖ $E(d_A$ ‖ $H)$ ‖ 有效期 ‖ $sign$ ‖ t]，

PKG 用注册点的公钥对 $r3$ 加密，生成 $P(r3)$。

5） PKG 发送给注册点：[注册点 ‖ 用户名 ‖ 用户 ID ‖ $P(r3)$ ‖ Data6]。

6） 注册点接收与验证数据。

注册点接收 PKG 发送来的数据：[注册点 ‖ 用户名 ‖ 用户 ID ‖ $P(r3)$ ‖ Data6]。

注册点用本方的私钥做解密 $EdR_A[P(r3)]$。$EdR_A[P(r3)]=r3$，得到对称密钥 $r3$。

注册点用 $r3$ 解密 Data6。$DEr3(\text{Data6})=$[用户名 ‖ 用户标识 ID_A ‖ $E(d_A \| H)$ ‖ 有效期 ‖ $sign$ ‖ t]。

注册点验证数据[用户名 ‖ 用户标识 ID_A ‖ $E(d_A \| H)$ ‖ 有效期]的数字签名。

注册点把加密数据 $E(d_A \| H)$ ‖ 有效期 ‖ t 送入用户载体。

用户载体内用 $r1$ 解密 $E(d_A)$，并存储，

$DEr1[E(d_A)]=d_A$，

用户对 $d_A \| H$ 进行验证。若通过，将私钥及有关数据存入安全区；反之，反馈：申请失败。

参 考 文 献

[1] GB/T 15843.3—2016 信息技术 安全技术 实体鉴别 第3部分:采用数字签名技术的机制

[2] GB/T 16262.1—2006 信息技术 抽象语法记法一(ASN.1) 第1部分:基本记法规范(ISO/IEC 8824-1:2002,IDT)

[3] GB/T 33560—2017 信息安全技术 密码应用标识规范

[4] GM/T 0081 SM9密码算法加密签名消息语法规范

[5] RFC5408 IETF Identity-Based Encryption Architecture and Supporting Data Structures January 2009

[6] RFC5409 IETF Using the Boneh-Franklin and Boneh-Boyen Identity-Based Encryption January 2009

中华人民共和国密码
行业标准
基于SM9标识密码算法的密钥管理系统
技术规范
GM/T 0086—2020
*
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.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 2 字数 55 千字
2021年5月第一版 2021年5月第一次印刷
*
书号:155066·2-35974 定价 36.00 元

GM/T 0086-2020

码上扫一扫 正版服务到