



# 中华人民共和国国家标准

GB/T 46798—2025

## 网络安全技术 标识密码认证系统 密码及其相关安全技术要求

Cybersecurity technology—Technical requirements for cryptography and  
related security of identity-based cryptographic authentication system

2025-12-02 发布

2026-07-01 实施

国家市场监督管理总局 发布  
国家标准化管理委员会



目 次

前言 ..... III

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 3

5 标识密码认证系统 ..... 3

    5.1 系统组成 ..... 3

    5.2 标识管理 ..... 5

    5.3 标识格式 ..... 5

6 密码算法、密码设备及接口要求 ..... 6

    6.1 密码算法 ..... 6

    6.2 密码设备 ..... 6

    6.3 密码设备服务接口 ..... 6

7 密钥生成服务系统要求 ..... 6

    7.1 系统要求 ..... 6

    7.2 密钥生成服务设计 ..... 7

    7.3 安全要求 ..... 8

    7.4 数据备份要求 ..... 8

8 注册服务系统要求 ..... 9

    8.1 系统要求 ..... 9

    8.2 注册服务设计 ..... 10

    8.3 用户密钥载体 ..... 10

    8.4 安全要求 ..... 10

    8.5 数据备份要求 ..... 10

9 发布服务系统要求 ..... 11

    9.1 系统要求 ..... 11

    9.2 发布服务设计 ..... 12

    9.3 安全要求 ..... 12

    9.4 数据备份要求 ..... 12

10 安全要求 ..... 12

    10.1 概述 ..... 12

    10.2 系统安全 ..... 12

    10.3 密钥安全 ..... 13

    10.4 通信安全 ..... 13

    10.5 安全审计 ..... 13

11 密钥管理要求 ..... 14

11.1	密钥安全 .....	14
11.2	用户密钥申请认证 .....	16
11.3	密钥生成 .....	16
11.4	密钥传输 .....	16
11.5	密钥存储 .....	16
11.6	密钥更新 .....	17
11.7	密钥注销 .....	17
11.8	密钥备份 .....	17
11.9	密钥恢复 .....	17
11.10	主密钥管理 .....	17
11.11	系统标识管理 .....	17
12	密钥管理安全操作流程要求 .....	17
12.1	系统初始化流程 .....	17
12.2	用户密钥载体初始化 .....	18
12.3	用户密钥生成流程 .....	18
12.4	标识状态发布流程 .....	19
12.5	更新用户密钥状态流程 .....	20
12.6	司法取证密钥恢复流程 .....	20
12.7	用户信息状态查询与响应流程 .....	21
12.8	主密钥更新流程 .....	21
附录 A (规范性)	发布服务消息格式 .....	22
A.1	公开参数数据格式 .....	22
A.2	标识吊销列表数据格式 .....	22
A.3	服务信息查询 .....	22
A.4	公开参数查询 .....	22
A.5	标识查询 .....	22
附录 B (资料性)	用户密钥申请流程和消息格式 .....	23
B.1	用户申请密钥流程 .....	23
B.2	用户申请密钥消息格式 .....	24
附录 C (规范性)	标识数据格式要求 .....	28
C.1	标识数据格式 .....	28
C.2	扩展项定义 .....	28
C.3	带签名的标识数据格式 .....	29
附录 D (规范性)	密码算法的 OID 与算法标识 .....	30
参考文献	.....	31

# 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。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：北京国脉信安科技有限公司、深圳奥联信息技术有限公司、格尔软件股份有限公司、兴唐通信科技有限公司、中国电子技术标准化研究院、北京海泰方圆科技股份有限公司、广东省电子商务认证有限公司、三未信安科技股份有限公司、智巡密码(上海)检测技术有限公司、金盾检测技术股份有限公司、中电科网络安全科技股份有限公司、厦门民航凯亚有限公司、长春吉大正元信息技术股份有限公司、济南三泽信息安全测评有限公司、北京时代亿信科技股份有限公司、华为技术有限公司、浙江国利信安科技有限公司、南方电网数字电网集团(广东)有限公司、国网新疆电力有限公司、新疆华电苇湖梁新能源有限公司、北京中科卓信软件测评技术中心、上海势炎信息科技有限公司、北京建恒信安科技有限公司、北京数字认证股份有限公司、中国网络空间研究院、企知道科技有限公司、郑州信大捷安信息技术股份有限公司、数安时代科技股份有限公司、工业和信息化部网络安全产业发展中心、中金数据(武汉)超算技术有限公司、工信通(北京)信息技术有限公司、国网区块链科技(北京)有限公司、中科信息安全共性技术国家工程研究中心有限公司、中国人民解放军国防科技大学、奇安信网神信息技术(北京)股份有限公司、中国电子信息产业集团有限公司第六研究所、陕西省信息化工程研究院。

本文件主要起草人：袁峰、封维端、蔡先勇、郑强、孙皇龙、但波、王立欣、李晓千、郑丽娟、黄晶晶、罗影、张立圆、药乐、陈树乐、李雪雁、王现方、曾光、匡云、尹文基、王迎、丁肇伟、张荣泽、刘伟丰、陈洁、邢伟、黄福飞、艾微、张玉柱、林培桂、杨延栋、刘海明、杨伟、张磊、王兵、乔梦宇、王震、刘中、梁松涛、林浩、周蔚林、王进、王斌、石竹玉、胡建勋、邢倩倩、安锦程、王龙、赵晓荣。



# 网络安全技术 标识密码认证系统 密码及其相关安全技术要求

## 1 范围

本文件规定了标识密码认证系统密钥生成、管理以及公开参数查询等服务的安全要求和技术要求。  
本文件适用于标识密码认证系统的设计、开发、使用和检测。

## 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 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 25069 信息安全技术 术语
- 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（所有部分） 信息安全技术 SM2 椭圆曲线公钥密码算法
- GB/T 37092 信息安全技术 密码模块安全要求
- GB/T 38635—2020（所有部分） 信息安全技术 SM9 标识密码算法
- GM/T 0016—2023 智能密码钥匙密码应用接口规范
- GM/T 0018—2023 密码设备应用接口规范
- GM/T 0057—2018 基于 IBC 技术的身份鉴别规范
- GM/T 0081—2020 SM9 密码算法加密签名消息语法规范
- GM/T 0090—2020 标识密码应用标识格式规范

## 3 术语和定义

GB/T 38635—2020（所有部分）和 GB/T 25069 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的过程。

### 3.2

**标识 identity**

可唯一确定实体身份且不可否认的信息。

注 1：本文件中标识为符合 GM/T 0090—2020 中 Identifier 定义的数据。

注 2：GM/T 0090—2020 中 Identifier 的 identityData 为实体的可识别名称、电子邮箱、身份证号、电话号码、设备编号、街道地址等。

[来源：GB/T 38635.1—2020, 3.1, 有修改]

### 3.3

#### 标识密码 identity-based cryptography

公钥由标识和公共参数唯一确定,私钥根据标识、公共参数和主私钥计算得出的公钥密码技术。

### 3.4

#### 标识密码认证系统 identity-based cryptographic authentication system

使用标识和主密钥生成用户密钥,并对标识和用户密钥的生成、发布、更新、撤销等全生存周期进行管理的系统。

### 3.5

#### 密钥生成中心 key generation center

负责选择系统参数、生成主密钥并产生用户密钥的可信机构。

注:本文件中指密钥生成服务的运营机构。

[来源:GB/T 38635.1—2020,3.3,有修改]

### 3.6

#### 签名主密钥 signature master key

由签名主私钥和签名主公钥组成,处于标识密码密钥分层结构最顶层的密钥。

注:其中签名主公钥公开,签名主私钥由密钥生成中心秘密保存,密钥生成中心用签名主私钥和用户的标识生成用户的签名私钥,签名主私钥一般由密钥生成中心通过随机数发生器产生,签名主公钥由签名主私钥结合系统参数产生。

[来源:GB/T 38635.2—2020,3.8,有修改]

### 3.7

#### 加密主密钥 encryption master key

由加密主私钥和加密主公钥组成,处于标识密码密钥分层结构最顶层的密钥。

注1:其中加密主公钥公开,加密主私钥由密钥生成中心秘密保存,密钥生成中心用加密主私钥和用户的标识生成用户的加密私钥,加密主私钥一般由密钥生成中心通过随机数发生器产生,加密主公钥由签名主私钥结合系统参数产生。

注2:签名主密钥和加密主密钥简称为主密钥,签名主私钥和加密主私钥简称为主私钥,签名主公钥和加密主公钥简称为主公钥。

[来源:GB/T 38635.2—2020,3.1,有修改]

### 3.8

#### 用户签名密钥 signature user key

使用用户标识和签名主私钥进行计算产生,并下发给用户用于数字签名的密钥。

注:也称为用户的签名私钥。

### 3.9

#### 用户加密密钥 encryption user key

使用用户标识和加密主私钥进行计算产生,并下发给用户用于密钥协商、密钥解封装和解密的密钥。

注1:也称为用户的加密私钥。

注2:用户签名密钥和用户加密密钥简称为用户密钥。

### 3.10

#### 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。



4 缩略语

下列缩略语适用于本文件。

KGS:密钥生成服务(Key Generation Service)

LA:本地代理(Local Agent)

PS:发布服务(Publish Service)

RA:注册服务(Registration Authority service)

5 标识密码认证系统

5.1 系统组成

5.1.1 系统架构

标识密码认证系统架构包含密钥生成服务(KGS)、注册服务(RA)、发布服务(PS)、安全审计、用户密钥载体以及可选的本地代理,见图 1。

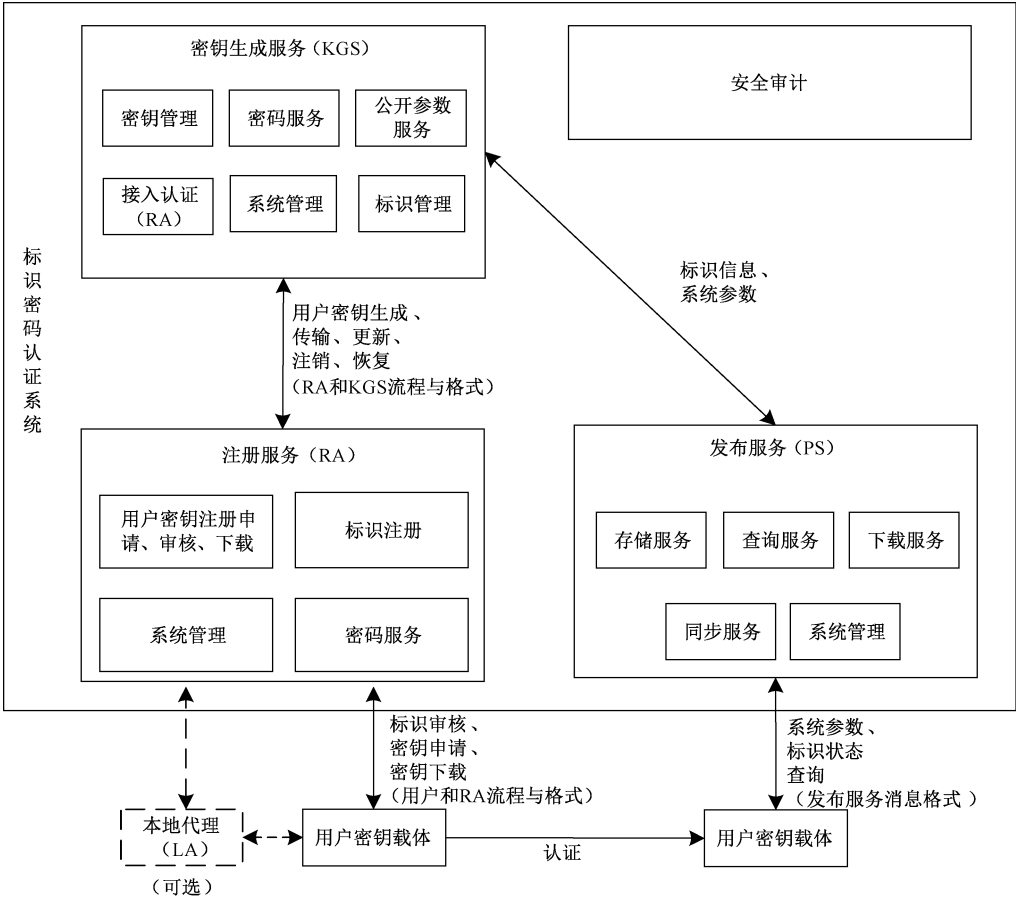


图 1 标识密码认证系统架构

其中：

- a) 密钥生成服务(KGS),是标识密码认证系统的核心组成部分,为用户生成用户密钥,并进行管理。KGS系统使用签名主密钥、加密主密钥和系统参数,生成用户密钥。KGS系统接收RA发来的用户密钥生成申请,生成并返回用户密钥和相关参数,其组成设计见5.1.2。KGS将系统参数和用户密钥的状态发布到PS中。KGS还应提供司法取证密钥恢复的服务。
- b) 发布服务(PS),是面向用户的信息服务,向用户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。公开参数包括可公开共享的密码参数、用户标识状态目录等,其组成设计见5.1.4;发布服务消息格式应符合附录A中的规定。
- c) 注册服务(RA),用于用户密钥注册申请和本地代理接入,承担用户密钥申请注册、申请审核、申请管理、与KGS系统进行业务交流工作,在向KGS系统申请密钥时,为接入认证提供用户标识和身份一致性的验证服务,其组成设计见5.1.3;用户密钥申请流程见附录B中B.1,用户和RA、RA和KGS之间的消息格式见B.2。
- d) 用户密钥载体,是用户密钥的载体,直接或通过LA向RA申请用户密钥,并对用户密钥进行存储和使用,其组成设计见5.1.5。用户密钥载体中的系统参数和主公钥可从PS中获取,并可从PS中查询用户标识状态。
- e) 本地代理,可作为RA的代理实体,承担为远程用户代理注册并申请密钥,其组成设计见5.1.6。
- f) 安全审计,应按照GB/T 22239—2019规定的要求设置安全审计机制,其组成设计见5.1.7。

### 5.1.2 密钥生成服务

KGS是标识密码认证系统的核心组成部分,为用户生成用户密钥,并进行管理与查询服务。KGS使用主密钥和系统参数,根据用户标识生成用户密钥。KGS接收RA发来的用户密钥生成申请,生成并返回用户所需密钥以及参数。

### 5.1.3 注册服务

#### 5.1.3.1 概述

RA用于用户密钥的注册申请和LA接入服务。

#### 5.1.3.2 用户密钥申请

用户密钥申请可采用在线或离线两种方式:

- 在线方式:用户通过LA或通过网络登录到用户注册管理系统申请;
- 离线方式:用户到指定的注册机构申请。

#### 5.1.3.3 身份审核

审核人员通过RA对申请者进行身份审核。

#### 5.1.3.4 身份与用户标识的一致性审核

RA应对用户密钥申请中的用户身份和用户标识进行一致性审核,确保该标识为申请者标识。

#### 5.1.3.5 密钥下载

密钥下载可采用在线或离线两种方式:

- 在线方式:用户通过LA或通过网络登录到RA下载用户密钥;
- 离线方式:用户到指定的RA线下获取用户密钥。

在线方式下载应保证传输信息的机密性和完整性。

离线方式下载应保证用户密钥载体符合 6.2 的要求。

5.1.4 发布服务

PS 面向终端用户提供信息服务查询,包括可公开的密码参数、用户标识状态目录等。

5.1.5 用户密钥载体

用户密钥载体是终端用户的密钥载体,通过 RA 或 LA 向 KGS 申请用户密钥,并向应用系统提供用户密钥的使用接口,可为智能密码钥匙或密码模块。

5.1.6 本地代理

LA 可分担 RA 的本地业务,主要面向终端用户进行资料录入和检查,最终审核结果由 RA 确定。

远程用户可通过 LA 向 RA 提交注册申请,并接收 RA 的返回信息,以及密钥下载。

LA 设置于 RA 外部,用户可通过 LA 接入 RA。LA 作为 RA 的远程注册终端,承担为用户代理注册并申请密钥的功能。

5.1.7 安全审计

安全审计服务提供事件级审计功能,对涉及系统安全的行为、人员、时间等记录进行跟踪、统计和分析。

5.2 标识管理

在标识密码认证系统中,应确保用户的标识在整个系统中的唯一性。RA 和 KGS 分别负责标识的注册和标识管理。

a) 标识注册

- 在 RA 注册时应检查用户的身份标识,确保在同一主密钥下标识信息和用户身份的一致性和唯一性;
- RA 应向 KGS 确认标识的唯一性;
- RA 应记录用户注册的标识信息,对标识信息进行增、删、改、查管理操作;
- RA 可对无效注册标识长期保留。

b) 标识管理

- KGS 应确保同一主密钥下标识的唯一性,当新注册标识出现重复时,应向对应的 RA 发出警告并拒绝生成用户密钥;
- KGS 应响应 RA 对标识的管理操作;
- KGS 应对无效注册标识长期保留。

5.3 标识格式

标识格式应符合附录 C 的规定。

## 6 密码算法、密码设备及接口要求

### 6.1 密码算法

标识密码认证系统使用对称密码算法、非对称密码算法和密码杂凑算法三类算法实现有关密码服务各项功能,其中,对称密钥密码算法实现数据加/解密以及消息鉴别;非对称密钥密码算法实现签名/验证以及密钥交换;密码杂凑算法实现待签名消息的杂凑运算。

标识密码认证系统支持使用的密码算法如下:

- 对称密码算法应符合 GB/T 32907 中规定的密码算法;
  - 非对称密码算法应符合 GB/T 32918(所有部分)和 GB/T 38635—2020(所有部分)中规定的密码算法;
  - 密码杂凑算法应符合 GB/T 32905 中规定的密码杂凑算法。
- SM9 的密码算法的 OID 与算法标识应符合附录 D 中的规定。

### 6.2 密码设备

#### 6.2.1 通则

应采用符合国家密码管理主管部门认证合格的密码设备,包括:

- 应用类密码设备:提供签名/验签、数据加密/解密、数据杂凑、数字信封、密钥生成和管理等密码服务;
- 通信类密码设备:提供通信双方的鉴别和数据加密服务;
- 用户密钥载体:提供数字签名/验证、数据加密/解密的智能密码钥匙或密码模块,用于用户标识和密钥存储及密码服务。

#### 6.2.2 密码设备的安全要求

密码设备应符合下列要求:

- 接口安全:不执行规定命令以外的任何命令和操作;
- 协议安全:所有命令的任意组合,不能得到私钥的明文;
- 密钥安全:私钥不以明文形式出现在密码设备之外;
- 物理安全:硬件密码设备应具有物理防护措施,任何情况下的拆卸均应立即销毁设备内保存的私钥。

### 6.3 密码设备服务接口

密码设备的服务接口应符合 GM/T 0018—2023 的规定,智能密码钥匙的服务接口应符合 GM/T 0016—2023 的规定。

## 7 密钥生成服务系统要求



### 7.1 系统要求

#### 7.1.1 功能

KGS 系统应提供下列服务功能:

- a) 依据主私钥和用户标识等数据生成用户密钥；
- b) 为司法机关提供用户加密私钥恢复服务；
- c) 为用户提供用户密钥更新、恢复、注销服务；
- d) 对 RA 提交的标识进行标识管理；
- e) RA 向 KGS 登录时，检查 RA 的标识的有效性。

### 7.1.2 性能

KGS 系统的性能应符合如下要求：

- a) 支持多并发服务请求；
- b) 系统各模块的状态信息保存在配置文件和数据库内部，保证系统的部署方便性和配置方便性，当系统需改变配置时无需中断系统的服务；
- c) 各模块的功能可通过配置文件进行控制，系统可根据不同的需求进行设置；
- d) 系统有冗余设计，保证系统的不间断运行。

### 7.1.3 管理员配置

KGS 系统应设置下列管理和操作人员：

- a) 超级管理员：负责 KGS 系统的策略设置，设置各子系统的业务管理员并对其管理的业务范围进行授权；
- b) 审计管理员：负责产生审计员并进行审计策略管理；
- c) 审计员：负责对涉及系统安全的事件、各类管理和操作人员的行为进行审计和监督；
- d) 业务管理员：负责 KGS 系统的业务管理，设置业务操作员并对其操作的权限进行授权；
- e) 业务操作员：按其权限进行具体的业务操作。

应对上述各类人员登录系统进行身份鉴别，其中“超级管理员”和“审计管理员”应在系统进行初始化时同时产生。

KGS 应按照 GB/T 22239—2019 规定的要求设置专门的安全管理人员负责系统的安全工作。

### 7.1.4 初始化

KGS 系统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；
- b) 配置系统参数，生成主密钥并安全备份；
- c) 为各管理员分配标识，管理员标识数据格式应符合 C.1 的规定，并且标识数据 identityData 应具有统一的格式；
- d) 完成超级管理员和审计管理员认证密钥的签发；
- e) 完成其他管理员认证密钥的签发。

## 7.2 密钥生成服务设计

### 7.2.1 密钥管理

包括用户密钥的生成、更新、恢复、注销和主密钥备份功能。

- a) 用户密钥生成：依据主私钥和用户标识等数据生成用户密钥，并通过安全协议或安全通道进行传输与下载，用户密钥的生成应在密码设备内实现。用户密钥生成后将用户标识状态等信息发布到 PS 中。

- b) 用户密钥更新:可通过更改用户标识数据结构中的有效期或序列号的方式更新用户标识数据结构内容,KGS依据主私钥和新的用户标识数据结构内容更新用户密钥,标识数据结构格式应符合附录 C 中的规定。
- c) 用户密钥恢复:用户密钥恢复可按照用户密钥重新申请方式实现;司法取证密钥恢复应依据特定文件规定,设置专用接口,专用凭证,并设置安全访问控制技术和载体。
- d) 用户密钥注销:依据用户要求或系统策略实现用户密钥注销,注销后应在公开参数服务中标明已注销的标识状态。
- e) 主密钥备份:主密钥应使用加密、秘密共享机制或其他安全方式进行备份。

#### 7.2.2 密码服务

包括主密钥生成、存储、用户密钥生成功能,并且为私钥生成模块、公开参数模块、系统管理模块、接入认证模块提供对称密码、非对称密码以及杂凑密码算法服务。

#### 7.2.3 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 PS 推送数据,或者撤销发布的信息。发布的数据应由 KGS 进行数字签名,保证数据的可认证和完整性。

#### 7.2.4 接入认证

包括 KGS 对 RA 的接入认证。

#### 7.2.5 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。

- a) 系统初始化,包括主密钥生成或导入、KGS 自身的用户密钥生成、系统参数配置、服务系统参数配置以及初始管理员生成等。
- b) 管理员管理,包括各类管理员生成、权限管理、身份鉴别等。
- c) 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。审计日志处理情况应做标记。
- d) 系统配置与监测,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。

#### 7.2.6 标识管理

标识管理见 5.2。

### 7.3 安全要求

安全要求见第 10 章。

### 7.4 数据备份要求

数据备份的目的是确保 KGS 关键业务数据在发生灾难性破坏时,系统能及时和尽可能完整地恢复被破坏的数据。应选择适当的存储备份系统对重要数据进行备份。

不同的应用环境可有不同的备份方案,但应符合以下基本要求:

- a) 在不中断数据库使用的前提下实施;

- b) 提供人工和自动备份功能；
- c) 提供实时和定期备份功能；
- d) 提供增量备份功能；
- e) 提供日志记录功能；
- f) 提供归档检索与恢复功能；
- g) 至少每天进行一次增量备份,定期进行全量备份。

KGS 系统应至少对主密钥、系统管理员信息、日志数据进行备份。

## 8 注册服务系统要求



### 8.1 系统要求

#### 8.1.1 功能

RA 系统应提供下列服务功能：

- a) 为用户提供密钥申请服务；
- b) 提供申请信息审核服务；
- c) 提供密钥下载服务。

#### 8.1.2 性能

RA 系统性能应符合如下要求：

- a) 系统对用户接口采用标准的互联网协议,确保各种用户都能使用本系统服务；
- b) 系统各模块的状态信息保存在配置文件和数据库内部,保证系统的部署方便性和配置方便性,当系统需改变配置时无需中断系统的服务；
- c) 各模块的功能可通过配置文件进行控制,系统可根据不同的需求进行设置；
- d) 系统某一功能模块可有多个实例,并且多个实例可运行在一台或多台计算机上；
- e) 系统有冗余设计,保证系统的不间断运行。

#### 8.1.3 管理员配置

RA 系统应设置下列管理和操作人员：

- a) 超级管理员:负责 RA 的策略设置,设置各子系统的业务管理员并对其管理的业务范围进行授权；
- b) 审计管理员:负责产生审计员并进行管理；
- c) 审计员: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；
- d) 业务管理员:负责 RA 的业务管理,设置业务操作员并对其操作的权限进行授权；
- e) 业务操作员:按其权限进行具体的业务操作。

应对上述各类人员登录系统进行身份鉴别,鉴别方式应符合 GM/T 0057—2018 的规定,其中“超级管理员”和“审计管理员”应在系统进行初始化时同时产生。

RA 应按照 GB/T 22239—2019 规定的要求设置专门的安全管理人员负责系统的安全工作。

#### 8.1.4 初始化

RA 系统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；



- b) 配置系统参数,初始化系统密钥,由 KGS 签发后导入并安全备份;
- c) 为各管理员分配标识,管理员标识数据格式应符合 C.1 的规定,并且标识数据 identityData 应具有统一的格式;
- d) 完成超级管理员和审计管理员认证密钥的签发;
- e) 完成其他管理员认证密钥的签发;
- f) 如有本地代理应继续进行下列工作:通过注册管理系统对本地代理进行注册,并分配本地代理的标识,签发相应本地代理的密钥。

## 8.2 注册服务设计

### 8.2.1 用户密钥注册申请、审核、下载

包括用户密钥申请服务、申请信息审核服务、密钥下载服务。

- a) 用户密码申请服务:依据注册表录入用户信息并存入数据库,用户申请信息中的标识信息可为基本标识数据(如手机号、设备号等),由 RA 将基本标识数据封装成符合 GM/T 0090—2020 的标识格式数据;也可为基于 GM/T 0090—2020 封装的标识格式数据。用户注册申请功能包括密钥申请、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功能。
- b) 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 KGS。
- c) 密钥下载服务:接收 KGS 返回的密钥数据包,通过认证后,将密钥数据包写入指定的用户密钥载体中,分发给用户。

### 8.2.2 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 LA 操作员签发密钥,实现 LA 操作员的注册等功能。

### 8.2.3 密码服务

为注册系统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。

### 8.2.4 标识注册

标识注册见 5.2。

## 8.3 用户密钥载体

用于安全存储用户密钥和进行密码计算。

用户密钥载体中应支持存储系统公开参数和主公钥。

用户密钥载体可包括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。

## 8.4 安全要求

安全要求见第 10 章。

## 8.5 数据备份要求

RA 的数据备份按照 7.4 的基本要求,并且 RA 应对系统管理员信息、用户密钥申请数据、审核



数据、密钥下载记录等数据进行备份。

## 9 发布服务系统要求

### 9.1 系统要求

#### 9.1.1 功能

PS 系统应提供下列服务功能：

- a) 用户标识状态查询；
- b) 系统公开参数查询；
- c) 系统公开参数下载；
- d) 标识状态信息批量下载。

PS 应对发布的信息进行数字签名。访问 PS 的用户应对获取的信息验证数字签名。PS 发布服务消息格式应符合附录 A 中的规定。

使用 SM9 密码算法的标识密码认证系统，其数字签名和验证应符合 GB/T 38635.2—2020 中第 6 章的规定。PS 发布的系统公开参数应符合 GB/T 38635.1—2020 中附录 A 的规定。

数字签名验证者应通过离线或在线的方式获取 PS 的标识，PS 的标识管理见 11.11。

#### 9.1.2 性能

PS 系统的性能应符合如下要求：

- a) 系统支持多并发服务请求；
- b) 系统各模块的状态信息保存在配置文件和数据库内部，保证系统的部署方便性和配置方便性，当系统需改变配置时无需中断系统的服务；
- c) 各模块的功能可通过配置文件进行控制，系统可根据不同的需求进行设置；
- d) 系统有冗余设计，保证系统的不间断运行。

#### 9.1.3 管理员配置

PS 系统应设置下列管理和操作人员：

- a) 超级管理员：负责 PS 系统的策略设置，设置各子系统的业务管理员并对其管理的业务范围进行授权；
- b) 审计管理员：负责产生审计员并进行管理；
- c) 审计员：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；
- d) 业务管理员：负责公开参数服务系统的某个子系统的业务管理，设置本子系统的业务操作员并对其操作的权限进行授权；
- e) 业务操作员：按其权限进行具体的业务操作。

应对上述各类人员登录系统进行身份鉴别，鉴别方式应符合 GM/T 0057—2018 的规定，其中“超级管理员”和“审计管理员”应在系统进行初始化时同时产生。

PS 系统应按照 GB/T 22239—2019 规定的要求设置专门的安全管理人员负责系统的安全工作。

#### 9.1.4 初始化

PS 系统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；

- b) 配置系统参数；
- c) 为各管理员分配标识,管理员标识数据格式应符合 C.1 的规定,并且标识数据 identityData 应具有统一的格式；
- d) 完成超级管理员和审计管理员认证密钥的签发；
- e) 完成其他管理员认证密钥的签发。

## 9.2 发布服务设计

### 9.2.1 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,在公开参数服务中存储的信息。这些公开信息由相应的 KGS 自身的用户密钥签名后,推送到 PS,以明确 PS 中的公开信息的来源。

### 9.2.2 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。用户状态查询应提供标识有效性、有效期、变更信息等信息;系统公开参数查询应提供系统公开参数、参数变更、目前支持的所有其他参数域等信息。

### 9.2.3 下载服务

支持系统公开参数下载、标识状态信息批量下载。

### 9.2.4 同步服务

PS 可采用主 PS 将数据推送到从 PS 中,或从 PS 向主 PS 拉取的方式同步。

### 9.2.5 系统管理

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。

## 9.3 安全要求

安全要求见第 10 章。

## 9.4 数据备份要求

PS 系统的数据备份按照 7.4 的基本要求进行,并且 PS 系统应对系统管理员信息、用户标识状态数据、系统公开参数进行备份。

# 10 安全要求

## 10.1 概述

安全要求包括系统安全、密钥安全、通信安全 and 安全审计。

## 10.2 系统安全

系统应具备系统管理和安全防护能力,保护系统本身的安全性,应按照 GB/T 22239—2019 规定的要求采取防火墙、病毒防治、漏洞扫描、入侵监测或入侵防御、数据备份、灾难恢复等安全防护措施保障

标识密码认证系统安全。

### 10.3 密钥安全

密钥安全见 11.1。

### 10.4 通信安全

KGS 与 PS 之间、RA 与 KGS 之间应采用密码技术保证通信过程中的机密性和完整性。

### 10.5 安全审计

#### 10.5.1 概述

在标识密码认证系统运行过程中涉及大量功能模块之间的相互调用,以及各种管理员的操作,这些调用和操作以日志的形式进行记载,以便用于系统错误分析、风险分析和安全审计等工作。

#### 10.5.2 功能要求

提供事件级审计功能,对涉及系统安全的行为、人员、时间的记录进行跟踪、统计和分析。

日志记录的主要内容要求:

- a) 操作员姓名;
- b) 操作项目;
- c) 操作起始时间;
- d) 操作终止时间;
- e) 序列号;
- f) 操作结果。

日志管理的主要内容要求:

- a) 日志参数设置:设置日志保存的最大规模和日志备份的目录;
- b) 日志查询:查询操作员、操作事件信息;
- c) 日志备份:当日志保存到日志参数设置的最大规模时,将保存的日志备份;
- d) 日志处理:对日志记录的正常业务流量和各类事件进行分类整理;
- e) 证据管理:对证据数据进行审计、统计和记录。

#### 10.5.3 功能模块审计要求

系统内的各功能模块在运行过程中会调用其他功能模块或被操作人员或其他功能模块所调用,对于这些相互之间的功能调用,各模块应记录如下数据:

- a) 调用请求的接收时间;
- b) 调用请求的来源网络地址;
- c) 调用请求发起者的身份;
- d) 调用请求的内容;
- e) 处理结果等。

各类管理员操作系统时,应记录关键操作步骤和信息:

- a) 登录信息,主要涉及管理员类型、名称、时间等;
- b) 操作内容,主要涉及增加、修改、删除和导出等操作。

#### 10.5.4 超级管理员审计

超级管理员的下列操作应被记录：

- a) 主密钥加载；
- b) 系统配置；
- c) 权限分配。

#### 10.5.5 审计管理员审计

审计管理员的下列操作应被记录：

- a) 审计员分配；
- b) 审计员授权。


#### 10.5.6 业务管理员审计

业务管理员的下列操作应被记录：

- a) 业务操作员分配；
- b) 业务操作员授权。

#### 10.5.7 业务操作员审计

业务操作员的下列操作应被记录：

- a) 用户密钥生成请求批准；
- b) 用户密钥生成请求拒绝；
- c) 用户密钥下载；
- d) 用户密钥更新；
- e) 用户密钥恢复；
- f) 用户密钥注销。

### 11 密钥管理要求

#### 11.1 密钥安全

##### 11.1.1 基本要求

密钥安全的主要目标是保障标识密码认证系统所涉及的密钥，在其生成、存储、使用、更新、注销、归档、销毁、备份和恢复整个生命周期中的安全。应采取硬件密码设备、密钥管理安全协议、密钥存取访问控制、密钥管理操作审计等多种安全措施。密钥安全的基本要求包括：

- a) 私钥的生成和使用应在硬件密码设备中完成；
- b) 私钥的生成和使用应有安全可靠的管理机制；
- c) 存在于硬件密码设备之外的所有私钥应加密；
- d) 密钥应有安全可靠的备份恢复机制；
- e) 对密码设备操作应由多个操作员实施。

##### 11.1.2 主密钥

主密钥的安全性除了满足基本要求外，还应符合下列要求。

- a) 主密钥的产生：  
主密钥应由硬件密码设备生成并存放在该密码设备中，并且硬件密码设备应至少达到 GB/T 37092 中密码模块二级要求。
- b) 主密钥的备份：  
应对主私钥的密文进行备份。应采用 SM2、SM4 或 SM9 加密算法加密或秘密共享机制将密钥份额分享给多个分管者保管。若使用秘密共享机制，宜使用参数为 (3, 5) 的门限秘密共享机制，分管的密钥份额应存放在硬件密码设备中，并对产生过程进行记录。秘密共享机制的算法本文件不做规定。
- c) 主密钥的恢复：  
应将备份的主私钥密文或密钥份额导入到密码设备中，在密码设备中恢复主私钥并计算出主公钥。
- d) 主密钥的更新：  
主密钥的更新，应重新生成主密钥，其过程同主密钥的产生。
- e) 主密钥的注销：  
主密钥的注销应与主密钥的更新同步。
- f) 主密钥的销毁：  
主密钥的销毁应与备份的主密钥一同销毁。

### 11.1.3 用户密钥

用户密钥的安全性除了满足基本要求外，还应符合下列要求。

- a) 用户密钥的产生：  
用户密钥的生成包括签名私钥和加密私钥。其中使用 SM9 标识密码算法的生成方法应符合 GB/T 38635—2020 的规定。
- b) 用户密钥的传输：  
用户密钥应通过加密或者安全通道方式传送到用户密钥载体。KGS 对用户密钥进行签名和加密保护，通过 RA 安全下载到用户密钥载体。  
用户申请密钥的流程和协议见附录 B。
- c) 用户密钥的检查：  
当用户密钥载体完成密钥下载后，应解密用户密钥，并验证用户密钥与标识的一致性，如验证失败，应拒绝接收该用户密钥。
- d) 用户密钥的恢复：  
用户密钥恢复按照用户密钥重新申请方式实现，重新申请的审核流程与第一次申请时一致，并且 RA 应审核用户身份与用户标识的一致性。
- e) 用户密钥的更新：  
用户密钥的更新可通过修改标识数据结构中的有效期或序列号的方式修改标识信息数据结构。  
用户密钥更新申请的审核流程与第一次申请时一致，并且 RA 应审核用户身份与用户标识的一致性。
- f) 用户密钥的注销：  
用户密钥的注销由用户到 RA 申请，RA 审核用户身份和用户标识的一致性，通过后提交 KGS 对该密钥对应的标识进行注销签名，更改该标识的状态标志，并推送到 PS。

g) 用户密钥的销毁:

用户密钥的销毁可由保存用户密钥的密码设备进行销毁。

#### 11.1.4 管理员认证密钥

管理员包括超级管理员、审计管理员、审计员、业务管理员和业务操作员等。管理员对应的认证密钥应存储在密码设备(如智能密码钥匙或密码模块)中。

管理员认证密钥的安全性应符合下列要求:

- a) 管理员认证密钥的使用应在硬件载体中完成;
- b) 管理员认证密钥所在的密码设备的口令复杂度应至少 8 个字符,并包含大小写字母、数字和特殊字符中的三种;
- c) 管理员的标识应与普通用户标识分开管理。

#### 11.2 用户密钥申请认证

用户通过 RA 申请私钥,应进行登录身份鉴别和密钥申请认证,具体要求包括:

- a) 对申请用户的真实性和有效性验证,应提供相应有效材料,有条件的采用现场面对面方式验证;
- b) 核实用户标识与用户身份的绑定关系;
- c) 申请用户密钥的数据包应保证完整性。

#### 11.3 密钥生成

##### 11.3.1 主密钥生成

主密钥生成要求见 11.1.2,其中基于 SM9 密码算法的标识密码认证系统的主密钥的生成算法见 GB/T 38635.2—2020 的 6.1 和 7.1。

##### 11.3.2 用户密钥生成

用户密钥的生成包括生成用户签名密钥和用户加密密钥,其中基于 SM9 密码算法的标识密码认证主密钥的生成见 GB/T 38635.2—2020 的 6.1 和 7.1。



#### 11.4 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,KGS 对用户密钥进行签名、加密保护,通过 RA 安全下载到用户密钥载体;
- b) 附录 B 给出了用户密钥下载的传输协议。

#### 11.5 密钥存储

密钥存储包括:

- a) 标识密码认证系统可只存储标识信息(用户标识、名称、相应的主私钥版本号、有效期,生成时间以及其他参数)。如需存储用户密钥,则用户密钥应采用加密算法加密保护;
- b) 对于安全要求高的客户端使用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) 注销的用户密钥目录应安全存储于历史库,保留年限由系统策略确定。

## 11.6 密钥更新

### 11.6.1 主密钥更新

标识密码认证系统可支持主密钥更新。主密钥更新时,应同时销毁签名主密钥,并将加密主密钥加密备份,主密钥更新流程见 12.8。

### 11.6.2 用户密钥更新

用户更新自己的密钥,先注销原密钥,再申请新密钥。申请新密钥时,可通过改变标识数据结构中的有效期或序列号的方式申请新密钥。标识数据格式应符合 C.1 中的规定。

## 11.7 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,进行密钥注销操作,并将信息传给 KGS。KGS 将该用户标识从在用库中注销,并将其转移到历史库。对该密钥对应的标识进行撤销签名,改变该标识的状态标志,并送入 PS。历史库的数据可依据安全策略,定期转存安全保留或销毁。

## 11.8 密钥备份

主私钥备份应采用加密或秘密共享机制备份。备份数据格式应至少包括私钥版本号、私钥实体、有效时间。

## 11.9 密钥恢复

标识密码认证系统应设置司法取证密钥恢复。司法取证密钥恢复可到 KGS 实施,或经过 KGS 认证控制实施。

用户密钥恢复可按照用户密钥重新申请方式实现,重新申请的审核流程与第一次申请时一致,并且 RA 应审核用户身份与用户标识的一致性。

### 11.10 主密钥管理

密钥生成服务的签名主公钥和加密主公钥应能通过在线或离线的方式获取。通过在线方式获取应保证通信信息的机密性和完整性。

主密钥注销策略要求包括到期注销主密钥和主动注销主密钥。电子认证服务方宜制定主密钥注销策略。

### 11.11 系统标识管理

密钥生成服务、发布服务和注册服务的标识应符合附录 C 的规定,并能通过在线或离线的方式获取。通过在线方式获取应保证通信信息的机密性和完整性。

## 12 密钥管理安全操作流程要求

### 12.1 系统初始化流程

KGS 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 KGS 的软、硬件系统(预先实施)；
- c) 首先,进行 PS 系统初始化,配置公开系统参数,等待 KGS 生成主密钥,并将主公钥导入 PS 用于验证 KGS 信息,由 KGS 为 PS 生成管理员,当主公钥导入完成后 PS 系统初始化完成；
- d) 再次,进行 KGS 初始化,配置系统参数(包括秘密参数和公开参数),生成主密钥(需将主公钥导入到 PS 中),并安全备份；KGS 完成自身初始化管理员私钥的签发,生成初始化管理员,向 PS 发布自签的 KGS 标识、主公钥、对应的系统参数和公开参数标识包,KGS 初始化完成,并由 KGS 初始化管理员完成 KGS 其他管理员私钥签发和角色配置；
- e) 最后,进行 RA 系统初始化,由 KGS 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) KGS 初始化完成；
- g) 如果有 LA 应继续进行下列工作:通过 RA 对 LA 进行注册,并签发相应 LA 的标识私钥。

## 12.2 用户密钥载体初始化

应预先对用户密钥载体进行初始化,将系统运行所需必要内容安全预制并下载到用户密钥载体。其中,基于 SM9 标识密码算法的认证系统公开参数的定义见 GB/T 38635.1—2020。

## 12.3 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 12.2；
- b) 将用户密钥载体与申请终端设备连接,进行用户密钥载体的确认,获取载体序列号 SN 和载体密钥密文；
- c) 用户直接或通过 LA 向 RA 系统发出用户密钥申请,如果通过 LA 向 RA 申请,LA 应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 对申请信息进行鉴别；
- e) RA 审核用户身份数据真实性、完整性；
- f) 若审核通过,RA 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,生成申请用户密钥消息,发送给 KGS；
- g) KGS 和 RA 做双向身份鉴别,验证 RA 签名,利用系统参数生成用户密钥,并把用户标识状态信息发布到 PS 上；
- h) KGS 对用户密钥密文和信息组成响应数据包并进行数字签名,回送给 RA；
- i) RA 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 下发到用户密钥载体内；
- j) 在用户密钥载体内安全解密,验证私钥正确性,如果正确,安全存储用户密钥。

用户密钥申请流程如图 2 所示。



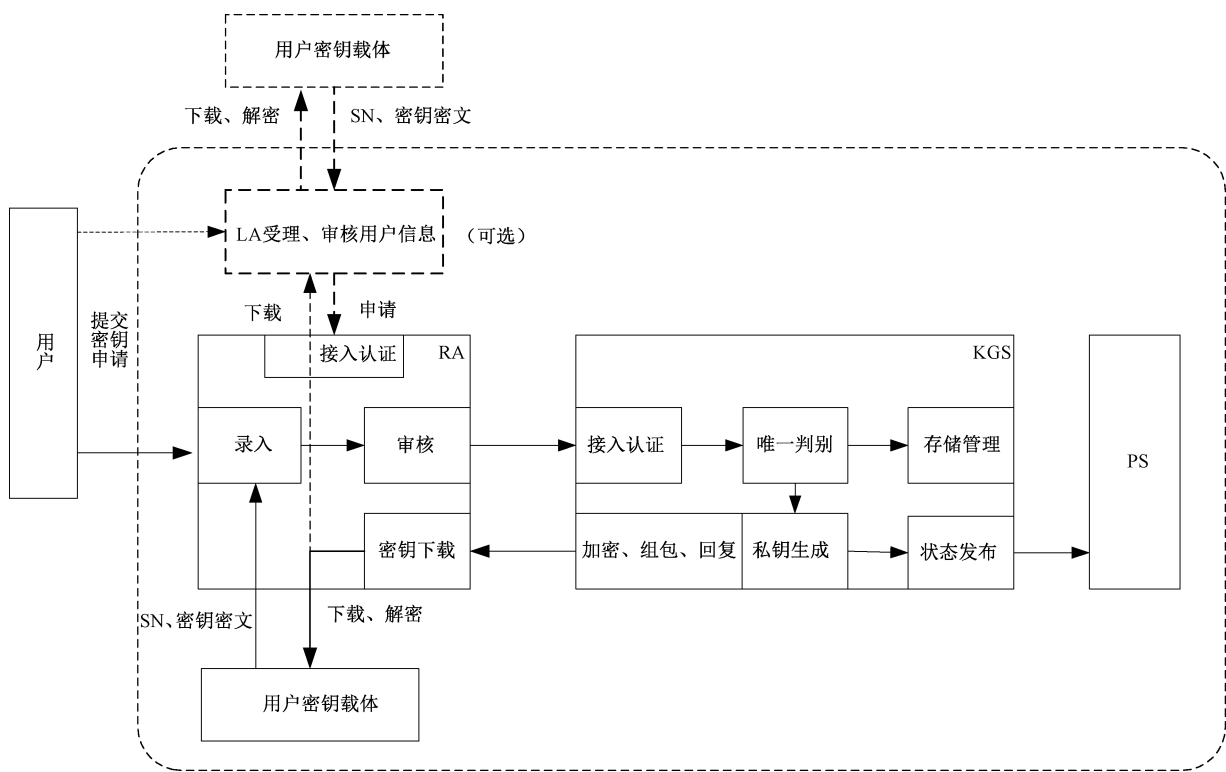


图 2 用户密钥申请流程图示

12.4 标识状态发布流程

12.4.1 新增用户密钥状态发布流程

新增用户密钥状态发布流程如下：

- a) 用户申请密钥完成后,KGS 系统对该用户的身份标识、有效状态、有效期等数据进行签名,发布到 PS;
- b) PS 对 KGS 的数据进行验证后,由 PS 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。

12.4.2 注销用户密钥状态发布流程

注销用户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能使用,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,申请办理者应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 KGS,KGS 对该标识信息进行注销处理,并将状态及时间数据进行签名,发布到 PS。
- c) PS 对 KGS 的数据进行验证后,由 PS 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。

12.4.3 冻结用户密钥状态流程

冻结用户密钥状态流程如下。

- a) 由 RA 或 LA 办理标识密钥冻结申请。申请办理者应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 KGS,KGS 对该标识信息进行冻结处理,并将状态及  
时间数据进行签名,发布到 PS。
- c) PS 对 KGS 的数据进行验证后,由 PS 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。

#### 12.4.4 恢复用户密钥状态流程

恢复用户密钥状态流程如下。

- a) 由 RA 或 LA 办理标识密钥恢复申请。申请办理者应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 KGS,KGS 对该标识信息进行恢复处理,并将状态及  
时间数据进行签名,发布到 PS。
- c) PS 对 KGS 的数据进行验证后,由 PS 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。

#### 12.5 更新用户密钥状态流程

更新用户密钥状态流程如下。

- 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 办理用户密钥更新申请。用原用户密钥变更信息表签名,并附上申请办理者身  
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 KGS,KGS 先将原标  
识及其对应的密钥注销,然后签发新标识对应的密钥,并将更新变化数据送给 PS 系统,更新  
标识状态库。
- d) KGS 加密新密钥安全传送 RA,后续过程与 12.3 中 g)~j)过程相同。

#### 12.6 司法取证密钥恢复流程

司法取证密钥恢复可在 KGS 办理,其操作流程依据 11.9 的要求实施。

司法取证密钥恢复应设置司法取证密钥恢复管理平台,配置必需的安全应用软件,建立严格的安全  
审计程序、工作流程和工作制度,切实保护国家利益,保护公民隐私。

司法取证密钥恢复还应满足下列要求。

- a) 系统结构:  
司法取证密钥恢复可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:  
司法取证密钥恢复管理系统可设置在 KGS 中。具体实现方式如下。
  - 1) 各个地区或部门的应用系统到私钥生成系统实施司法取证密钥恢复申请,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  
开恢复通道,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，不应向外泄露。

## 12.7 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 PS, 提出查询申请；
- b) 用户发送查询申请, 可通过注册的名称、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) PS 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。

## 12.8 主密钥更新流程

主密钥更新应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, 也可视为直接区分不同 KGS 的特征标识, 主密钥更新流程如下。

- a) 主密钥更新由 KGS 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) 由原主私钥生成的 KGS 标识密钥签名将更新的主公钥, 推送到 PS 中。
- c) PS 中应保留原主密钥和公开参数信息, 用于验证历史数据。
- d) KGS 将 KGS 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 PS 中。
- e) PS 将原主公钥和系统参数进行注销操作。
- f) PS 发布新主公钥和系统参数。

电子认证服务方宜制定主密钥更新后用户密钥的更新策略, 用户密钥根据需要可更新为新主密钥生成的用户密钥; 也可保留用户密钥, 新用户生成新主密钥产生的用户密钥。两种方式均不影响验证。

附 录 A  
(规范性)  
发布服务消息格式

**A.1 公开参数数据格式**

PS 发布的公开参数 IBCSysParams 的 ASN.1 数据格式定义应符合 GM/T 0081—2020 中 A.2 的规定。

**A.2 标识吊销列表数据格式**

PS 发布标识吊销列表 IdentifierRevocationList 的 ASN.1 数据格式定义应符合 GM/T 0081—2020 中 A.1 的规定。

**A.3 服务信息查询**

获取 PS 支持的标识密码认证系统的数量和类型等服务信息的请求数据格式应符合 GM/T 0057—2018 中 A.2 的规定,应答数据格式应符合 GM/T 0057—2018 中 A.3 的规定。

**A.4 公开参数查询**

向 PS 查询标识密码认证系统的公开参数的请求数据格式应符合 GM/T 0057—2018 中 A.4 的规定,应答数据格式应符合 GM/T 0057—2018 中 A.5 的规定。

**A.5 标识查询**

向 PS 查询标识信息的请求数据格式应符合 GM/T 0057—2018 中 A.6 的规定,应答数据格式应符合 GM/T 0057—2018 中 A.7 的规定。

## 附录 B

(资料性)

## 用户密钥申请流程和消息格式

## B.1 用户申请密钥流程

本条中使用的数学符号的定义见 GB/T 38635—2020，离线方式的用户密钥申请流程如下。

## 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  $r_1$  作为对称密钥。用 KGS 公钥加密生成  $P(r_1)$ ，送给注册点。

2) 注册点提取用户注册表中相关项数据和  $P(r_1)$ ，生成  $Data_1$ 。

$Data_1 = [\text{用户注册名} \parallel \text{用户标识 ID} \parallel \text{终端载体号 EID} \parallel P(r_1)]$ 。

3) 注册点对  $Data_1$  做数字签名  $sign = \text{SIGN}(Data_1)$ ，并生成数据包  $Data_2$ 。

$Data_2 = [\text{用户注册名} \parallel \text{用户标识 ID} \parallel \text{终端载体号 EID} \parallel P(r_1) \parallel sign]$ 。

4) 注册点生成随机数  $r_2$  作为对称密钥，用 KGS 公钥加密  $r_2$ ，生成  $P(r_2)$ 。

5) 注册点用对称密钥  $r_2$  对  $Data_2$  加密，生成数据包  $Data_3$ 。

$Data_3 = E_{r_2}(Data_2)$ 。

6) 注册点发送申请数据包  $Data_4$  给 KGS。

$Data_4 = P(r_2) \parallel Data_3$ 。

## d) KGS 验证申请数据包。

1) KGS 收到数据包  $Data_4$ 。用本方私钥  $d_{KGS}$  解密  $P(r_2)$ 。 $Dd_{KGS}(P(r_2)) = r_2$ ，得到对称密钥  $r_2$ 。

2) KGS 用  $r_2$  解密数据包  $Data_3$ ， $Dr_2(Data_3) = Data_2 = [\text{用户实名} \parallel \text{用户标识 ID} \parallel \text{终端载体号 EID} \parallel \text{电话号码} \parallel \text{电子邮箱} \parallel \text{通信地址} \parallel P(r_1) \parallel sign]$ 。

3) KGS 验证  $Data_2$  数字签名  $sign$ 。

4) KGS 用本方私钥解密  $Data_2$  中的  $P(r_1)$ 。 $Dd_{KGS}(P(r_1)) = r_1$ ，得到对称密钥  $r_1$ 。

## e) KGS 生成并发送用户密钥：

1) KGS 生成标识为  $ID_A$  的用户密钥  $d_A$ ；

2) KGS 用  $r_1$  对  $d_A$  加密，生成  $E(d_A)$ ，并计算 SM3 杂凑  $H = \text{Hash}(d_A)$ ；

3) KGS 生成  $Data_5$ ，用本方的私钥  $d_{KGS}$  对  $Data_5$  做数字签名  $sign$ ；

$Data_5 = [\text{用户名} \parallel \text{用户标识 } ID_A \parallel E(d_A \parallel H) \parallel \text{有效期}]$

$sign = \text{SIGN}_{d_{KGS}}(Data_5) = (h, S)$ ；

4) KGS 生成随机数  $r_3$ ，作为对称密钥；

5) KGS 用密钥  $r_3$  对数字签名  $sign$  和签发时间  $t$  等数据进行加密，生成  $Data_6$ ；

6)  $Data_6 = E_{r_3}[\text{用户名} \parallel \text{用户标识 } ID_A \parallel E(d_A \parallel H) \parallel \text{有效期} \parallel sign \parallel t]$ ；

7) KGS 用注册点的公钥对  $r_3$  加密，生成  $P(r_3)$ ；

8) KGS 发送给注册点： $[\text{注册点} \parallel \text{用户名} \parallel \text{用户 ID} \parallel P(r_3) \parallel Data_6]$ ；

## 9) 注册点接收与验证数据

注册点接收 KGS 发送来的数据: [注册点 || 用户名 || 用户 ID ||  $P(r_3)$  ||  $Data_6$ ]。

注册点用本方的私钥做解密  $E_{d_{RA}}(P(r_3))$ 。  $E_{d_{RA}}(P(r_3)) = r_3$ ，得到对称密钥  $r_3$ 。

注册点用  $r_3$  解密  $Data_6$ 。  $D_{r_3}(Data_6) = [\text{用户名} || \text{用户标识 } ID_A || E(d_A || H) || \text{有效期} || \text{sign} || t]$ 。

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  $E(d_A || H) || \text{有效期} || t$  送入用户载体。

用户载体内用  $r_1$  解密  $E(d_A)$ ，并存储:  $D_{r_1}(E(d_A)) = d_A$ 。

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

**B.2 用户申请密钥消息格式****B.2.1 用户向 RA 请求数据格式**

用户向 RA 请求的数据格式如下：


```
UserRequest ::= SEQUENCE {
    version                Version DEFAULT v1,
    userName               UTF8STRING,
    identifier              Identifier,
    eid                    [0] IMPLICIT OCTET STRING OPTIONAL,
    sm9Cipher              SM9Cipher
    extensions              [1] IMPLICIT Extensions OPTIONAL
}
```

Version ::= INTEGER { v1(0) }

version 为版本号，本文件定义为 v1，值为 0；

userName 为用户名；

identifier 为用户标识，其定义见 GM/T 0090—2020；

 eid 为用户密码终端载体号；

SM9Cipher 为使用 KGS 标识加密的由用户载体生成的随机对称密钥  $r_1$  的密文，其定义见 GB/T 41389；

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

```
Extension ::= SEQUENCE {
    extnID                  OBJECT IDENTIFIER,
    extnValue               [0] EXPLICIT ANY DEFINED BY extnID OPTIONAL
}
```

**B.2.2 RA 向 KGS 请求数据格式**

RA 使用自己的私钥和 KGS 的标识，对内容 UserRequest 生成 SignedAndEnvelopedData 类型的请求数据 RRequest，其中 SignedAndEnvelopedData 及类型定义见 GM/T 0081—2020 的 9.1。

RRequest ::= SignedAndEnvelopedData

```
SignedAndEnvelopedData ::= SEQUENCE {
    version                Version DEFAULT v1, -- 版本号 v1，值为 0。
```

```

    recipientInfos          RecipientInfos,
    digestAlgorithms        DigestAlgorithmIdentifiers,
    encryptedContentInfo    EncryptedContentInfo,
    signerInfos             SignerInfos
}
RecipientInfos ::= SET OF RecipientInfo
RecipientInfo ::= SEQUENCE{
    version                 Version DEFAULT v1,
    issuerIdentifier         Identifier,
    keyEncryptionAlgorithm  KeyEncryptionAlgorithmIdentifier,
    encryptedKey             SM9cipher
}
DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier
DigestAlgorithmIdentifier ::= OBJECT IDENTIFIER
EncryptedContentInfo ::= SEQUENCE {
    contentType             ContentType,
    contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier,
    encryptedContent         [0] IMPLICIT EncryptedContent OPTIONAL
}
EncryptedContent ::= OCTET STRING
SignerInfos ::= SET OF SignerInfo
SignerInfo ::= SEQUENCE {
    version                 Version DEFAULT v1,
    issuerIdentifier         Identifier,
    digestAlgorithm          DigestAlgorithmIdentifier,
    authenticatedAttributes [0] IMPLICIT Attributes OPTIONAL,
    digestEncryptionAlgorithm DigestEncryptionAlgorithmIdentifier,
    encryptedDigest          SM9Signature,
    unauthenticatedAttributes [1] IMPLICIT Attributes OPTIONAL
}

```

其中,RecipientInfo 为内容接收者 KGS 信息,各项含义如下:

- version 为版本号,本文件定义为 v1,值为 0;
- issuerIdentifier 为 KGS 标识;
- keyEncryptionAlgorithm 为用 KGS 标识加密数据加密密钥的算法标识,为 SM9 加密算法;
- encryptedKey 为内容加密密钥的 SM9 密文。

digestAlgorithms 为签名使用的杂凑算法标识集合,为 SM3 杂凑算法;

encryptedContentInfo 为内容使用内容加密密钥的密文,各项含义如下:

- contentType 为内容的类型,为 GM/T 0081—2020 第 5 章中的 data 类型;
- contentEncryptionAlgorithm 为内容加密算法标识;
- encryptedContent 为使用内容加密密钥加密内容后的密文。内容为用户向 RA 发送的 User-Request 数据。

signerInfos 为签名者信息,各项含义如下:

- version 为版本号,本文件定义为 v1,值为 0;
- issuerIdentifier 为 RA 的标识;
- digestAlgorithm 为对内容数据进行杂凑计算的杂凑算法,为 SM3 算法;
- authenticatedAttributes 是经由签名者签名的属性的集合,可选;如果该域存在,该域中摘要的计算方法是对原文进行摘要计算结果;
- digestEncryptionAlgorithm 签名算法标识,为 SM9 数字签名算法,其定义见 GM/T 0086—2020 的附录 D;
- encryptedDigest 是签名者对内容的 SM9 签名值。

### B.2.3 KGS 响应 RA 数据格式

KGS 收到 RA 发送的 RAResponse,使用 RA 的标识和 KGS 的私钥验证并解密出内容 UserRequest,再解密 UserRequest 的 sm9Cipher 得到用户的对称密钥  $r_1$ 。

KGS 为用户标识 identifier 生成签名和加密私钥数据:

```
UserKeys ::= SEQUENCE{
    keys      SEQUENCE{
        sm9SignPrivateKey    SM9SignPrivateKey,
        sm9EncPrivateKey      SM9EncPrivateKey
    },
    hash      OCTET STRING,
    signedIdentifier SignedIdentifier OPTIONAL
}
```

其中 SM9SignPrivateKey 和 SM9EncPrivateKey 见 GB/T 41389,hash 为 keys 的 SM3 杂凑值。

KGS 使用  $r_1$  加密 UserKeys,生成 data<sub>1</sub>,其类型为 EncryptedContentInfo,其中:

- contentType 为 GM/T 0081—2020 第 5 章中的 data 类型;
- contentEncryptionAlgorithm 为对称加密算法标识;
- encryptedContent 为使用  $r_1$  加密 UserKeys 的密文数据。

KGS 向 RA 发送的响应数据格式如下:

```
KGSRespondRaw := SEQUENCE{
    userName      UTF8STRING,
    userIdentifier Identifier,
    eid            [0] IMPLICIT OCTET STRING OPTIONAL,
    notBefore      GeneralizedTime,
    notAfter       GeneralizedTime,
    issueTime      GeneralizedTime,
    data1          EncryptedContentInfo
}

KGSRespond ::= SEQUENCE{
    raIdentifier  Identifier,
    userName      UTF8STRING,
    userIdentifier Identifier,
```



signedAndEnvelopedData SignedAndEnvelopedData  
}

userName 为用户名；

userIdentifier 为用户标识；

eid 为用户终端载体号；

notBefore、notAfter 为有效期；

issueTime 为密钥签发时间；

raIdentifier 为 RA 标识；

signedAndEnvelopedData 为 KGS 使用自己的用户密钥和 RA 的标识,对 KGSRespondRaw 生成的 SignedAndEnvelopedData 数据,其中各项含义如下：

——RecipientInfo 为接收者 RA 信息,其中：

- issuerIdentifier 为 RA 标识；
- keyEncryptionAlgorithm 为用 RA 标识加密数据加密密钥的算法标识,为 SM9 加密算法；
- encryptedKey 为内容加密密钥的 SM9 密文。

digestAlgorithms 为签名使用的杂凑算法标识集合,为 SM3 杂凑算法；

encryptedContentInfo 为使用内容加密密钥加密的密文,各项含义如下：

——contentType 为 GM/T 0081—2020 第 5 章中的 data 类型；

——contentEncryptionAlgorithm 为对称加密算法标识；

——encryptedContent 为使用内容加密密钥加密 KGSRespondRaw 的密文数据。

signerInfos 为签名者信息,各项含义如下：

——issuerIdentifier 为 KGS 的标识；

——digestAlgorithm 为对内容数据进行杂凑计算的杂凑算法,为 SM3 算法；

——authenticatedAttributes 是经由签名者签名的属性的集合,可选；如果该域存在,该域中摘要的计算方法是对原文进行摘要计算结果；

——digestEncryptionAlgorithm 签名算法标识,为 SM9 数字签名算法,其定义见附录 D；

——encryptedDigest 是签名者对 KGSRespondRaw 的 SM9 签名值。

signedIdentifier 为可选项,KGS 可根据需要对用户标识进行签名并返回带签名的标识数据格式,其结构见附录 C.3。

**B.2.4 RA 向用户响应数据格式**

RA 接收 KGS 的响应数据并进行验证和解密,得到 KGSRespondRaw。RA 向用户发送的响应数据格式如下：

RARespond ::= KGSRespondRaw

用户使用  $r_1$  解密  $data_1$  得到 userKeys 并验证 hash 值。若验证通过,则将用户密钥及有关数据存入安全区；反之,则返回申请失败。

## 附 录 C

### (规范性)

### 标识数据格式要求

#### C.1 标识数据格式

标识的 ASN.1 数据格式定义 Identifier 应符合 GM/T 0090—2020 中第 4 章的规定。

使用 SM9 标识密码算法的认证系统,其 Identifier 的 identityType 为 1.2.156.10197.1.302, alias 为“SM9”,标识数据 identityData 在 ASN.1 编码前的数据长度应不超过 256 字节,其 KGS 的标识中 identityData 项应为“SM9-KGC-××××”,PS 的标识中 identityData 应为“SM9-PS-××××”,其中“××××”应为数字或字母,同一个标识密码系统的 KGS 和 PS 的标识中的“××××”应一致。

#### C.2 扩展项定义

##### C.2.1 idExtensions

Identifier 的扩展项 idExtensions 为 Extensions 的 DER 编码内容:

Extensions ::= SEQUENCE SIZE(1..MAX) OF Extension

Extension ::= SEQUENCE{  
     extnID OBJECT IDENTIFIER,  
     extnValue OCTET STRING  
 }

extnID:表示扩展的 OID;

extnValue:表示扩展的值。

各扩展的 OID 应是 id-ext 的成员,定义如下:

id-ext OBJECT IDENTIFIER ::= {iso(1) member-body(2) cn(156) ccstc(10197) sm-scheme  
 (1) sm9(302) identifier(6) extension(1)}

##### C.2.2 IdentifierExtensionKGS

该扩展表示 KGS 的标识,extnID 定义为:

id-ext-kgs OBJECT IDENTIFIER ::= {id-ext 1}

extnValue 的内容为 DistricInfo 的 DER 编码数据,DistrictInfo 定义为:

DistrictInfo ::= SEQUENCE{  
     district IA5String,  
     districtNo INTEGER  
 }

district:表示该标识的发布服务的地址;

districtNo:表示在发布服务中存在多个 KGS 的发布信息时,生成该标识密钥的发布服务的唯一编号。

##### C.2.3 IdentifierExtensionPublisher

该扩展表示发布服务查询地址,extnID 定义为:

id-ext-ps OBJECT IDENTIFIER ::= {id-ext 2}  
extnValue 的内容为 DistricInfos 的 DER 编码数据, DistrictInfos 定义为:  
DistrictInfos ::= SET SIZE (1..MAX) OF DistrictInfo  
DistrictInfo ::= SEQUENCE{  
    district IA5String,  
    districtNo INTEGER  
}

district:表示该标识的发布服务的地址;

districtNo:表示在发布服务中存在多个 KGS 的发布信息时,生成该标识密钥的发布服务的唯一编号。

C.3 带签名的标识数据格式

KGS 可对用户的标识进行签名,其结果为带签名的标识数据格式,定义如下:

SignedIdentifier ::= SEQUENCE{  
    identifier Identifier,  
    signatureAlgorithm AlgorithmIdentifier,  
    signatureValue BIT STRING  
}  
AlgorithmIdentifier ::= SEQUENCE{  
    algorithm OBJECT IDENTIFIER,  
    parameters ANY DEFINED BY algorithm OPTIONAL  
}

identifier 标识数据,应符合 A.1 的规定。

signatureAlgorithm 是签名算法,包括 KGS 对 identifier 签名所使用的签名算法,本文件中为 1.2.156.10197.1.302.1。

signatureValue 是签名值,其签名者是 identifier 的扩展项 IdentifierExtensionKGS 中指定的 KGS。

附 录 D

(规范性)

密码算法的 OID 与算法标识

基于 SM9 标识密码算法的认证系统相关的 OID 定义见表 D.1、表 D.2、表 D.3 和表 D.4。

表 D.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
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 和 SM3 的数字签名
1.2.156.10197.1.302.6.1.1	基于 SM9 的标识扩展项 IdentifierExtensionKGS
1.2.156.10197.1.302.6.1.2	基于 SM9 的标识扩展项 IdentifierExtensionPublisher

表 D.2 非对称密码算法的标识

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

表 D.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 D.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

参 考 文 献

[1] GB/T 15843.3—2023 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—2025 信息技术 抽象语法记法—(ASN.1) 第 1 部分:基本记法规范


[3] GB/T 33560 信息安全技术 密码应用标识规范

[4] GB/T 41389 信息安全技术 SM9 密码算法使用规范

[5] GM/T 0086—2020 基于 SM9 标识密码算法的密钥管理系统技术规范

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

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



---



