ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0110—2021

密钥管理互操作协议规范

Key management interoperability protocol specification

2021-10-18 发布　　2022-05-01 实施

国家密码管理局　　发布

目　　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　概述 …… 3
6　密钥管理互操作协议 …… 3
6.1　协议模型 …… 3
6.2　对象 …… 4
6.3　属性 …… 17
6.4　操作 …… 50
6.5　消息 …… 81
7　安全要求 …… 116
7.1　密码算法 …… 116
7.2　密钥生成 …… 117
7.3　存储安全 …… 117
7.4　传输安全 …… 117
7.5　身份认证 …… 117
7.6　访问控制 …… 117
附录 A（资料性）　标准应用示例 …… 118
附录 B（规范性）　TTLV 编码 …… 120
附录 C（规范性）　错误处理 …… 123
附录 D（资料性）　配置文件示例 …… 140
参考文献 …… 142
索引 …… 146

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。

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：三未信安科技股份有限公司、北京数字认证股份有限公司、北京信安世纪科技股份有限公司、上海众人网络安全技术有限公司、中金金融认证中心有限公司、兴唐通信科技有限公司、成都卫士通信息产业股份有限公司、北京赛博兴安科技有限公司、北京融通高科科技发展有限公司、北京数码视讯科技股份有限公司、北京江南天安科技有限公司、北京宏思电子技术有限责任公司、北京智芯微电子科技有限公司、数安时代科技股份有限公司、格尔软件股份有限公司、山东大学、中国移动通信集团设计院有限公司、暨南大学。

本文件主要起草人：高志权、董坤朋、鹿淑煜、刘晓东、李向锋、汪宗斌、李坤、刘海涛、姜晓新、成明、韩浩、王亚伟、张向辉、马晓艳、王妮娜、罗俊、张旭、张妍、张钊、张永强、谭武征、张高山。

引　言

在密码系统中，密钥的生成、使用和管理至关重要，密钥的安全是密码系统安全的基础。密钥管理是指根据安全策略，对密钥的产生、分发、存储、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期的管理。在密码应用方案中，应用服务器、数据库系统、云计算平台、大数据平台等多种环境中需要对数据进行加密保护，都需要使用密钥管理系统对数据加密密钥等密钥的全生命周期进行安全管理，亟需定义统一的密钥管理接口规范。

本文件目标是为密码应用系统和密钥管理系统之间通信制定统一的密钥管理协议。通过该密钥管理协议，解决需要使用密钥的应用系统与生成和管理这些密钥的密钥管理系统之间的通信标准化问题。

本文件制定的密钥管理协议为密钥管理系统的开发、使用及检测提供依据和指导，有利于提高密钥管理系统的产品化和规范化。

密钥管理互操作协议规范

1 范围

本文件规定了密钥客户端和密钥管理服务端之间通信的密钥管理协议，通过该协议完成密钥管理服务端中对象的生成、存储和状态转换等操作，并规定了协议应用的安全要求。

不涉及密钥管理服务端的内部逻辑结构和安全性设计，也不涉及密钥客户端的业务逻辑。

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 15852.1 信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制

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 35276 信息安全技术 SM2密码算法使用规范

GM/T 0024 SSL VPN技术规范

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

归档 archive

将不会被频繁访问的信息放进长期存储区。

3.2

授权 authorization

授予实体的访问权限；表达了对执行某项安全功能或活动的“正式”许可。

3.3

失信 compromise

未经授权泄露、篡改、替换或使用敏感数据(例如密钥材料和与安全相关的其他信息)。

3.4

消息摘要 message digest

消息经过密码杂凑运算得到的结果。

3.5

密钥封装(封装) key wrapping(wrapping)

一种对密钥进行加密、MAC/签名或加密与MAC/签名都执行的一种方法。