ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0019—2023
代替 GM/T 0019—2012

通用密码服务接口规范

Universal cryptography service interface specification

2023-12-04 发布　　2024-06-01 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。

本文件代替GM/T 0019—2012《通用密码服务接口规范》，与GM/T 0019—2012相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 删除了“用户证书列表”中的“数据长度(字节)”列(见2012年版的表2)“密钥容器列表”中的“数据长度(字节)”列(见2012年版的表3)；

b) 删除了“证书中DN的结构(见表4)”内容(见2012年版的5.2.4)；

c) 删除了“通用密码服务在公钥密码应用技术体系框架内的位置”图；(见2012年版的图1)；

d) 增加了“解析PKCS ♯7格式的签名数据”接口(见7.4.16)；

e) 增加了“验证方法”(见第8章)；

f) 增加了“SM9密码算法应用接口”(见附录A)；

g) 增加了“证书被吊销的原因”错误码（见表B.1)；

h) 删除了“SAR_CertRevokedErr”的宏描述、预定义值、说明（见2012年版的附录A)。

请注意本文件的某些内容可能涉及专利。本文本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：北京数字认证股份有限公司、格尔软件股份有限公司、北京海泰方圆科技股份有限公司、无锡江南信息安全工程技术中心、上海数字证书认证中心有限公司、中电科网络安全科技股份有限公司、山东得安信息技术有限公司、北京国脉信安科技有限公司、中国电子技术标准化研究院。

本文件主要起草人：赵松、王银平、刘平、李述胜、郑强、谭武征、蒋红宇、柳增寿、王玉林、王中武、马洪富、高志权、孔凡玉、袁峰、上官晓丽、蔡一鸣、黄晶晶。

本文件及其所代替文件的历次版本发布情况为：

——2012年首次发布为GM/T 0019—2012；

——本次为第一次修订。

通用密码服务接口规范

1 范围

本文件规定了通用密码服务接口的数据结构、接口描述、函数定义要求，描述了相应验证方法。

本文件适用于公钥密码应用技术体系下密码应用服务的开发，密码应用支撑平台的研制及检测，密码设备应用系统的开发。

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 25069 信息安全技术 术语

GB/T 41389 信息安全技术 SM9 密码算法使用规范

GM/T 0003.1 信息安全技术 SM2 椭圆曲线公钥密码算法 第1部分：总则

GM/T 0006 密码应用标识规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0010 SM2 密码算法加密签名消息语法规范

GM/T 0015 数字证书格式

GM/T 0016 智能密码钥匙应用接口规范

GM/T 0018 密码设备应用接口规范

GM/T 0094 公钥密码应用技术体系框架规范

GM/Z 4001 密码术语

3 术语和定义

GB/T 25069、GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

容器 container

密码设备中用于保存密钥所划分的唯一性存储空间。

4 缩略语

下列缩略语适用于本文件。

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

CA：证书认证机构（Certification Authority）

CN：通用名（Common Name）

CRL：证书撤销列表（Certificate Revocation List）

DER：可区分编码规则（Distinguished Encoding Rules）