ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 43578—2023

信息安全技术　通用密码服务接口规范

Information security technology—Universal cryptography service interface specification

2023-12-28 发布　　2024-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件由全国信息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：北京数字认证股份有限公司、无锡江南信息安全工程技术中心、中国电力科学研究院、中国电子技术标准化研究院、博雅中科(北京)信息技术有限公司、山东得安信息技术有限公司、上海市数字证书认证中心有限公司、北京信安世纪科技股份有限公司、智巡密码(上海)检测技术有限公司、格尔软件股份有限公司、中科信息安全共性技术国家工程研究中心有限公司、数安时代科技股份有限公司、阿里云计算有限公司、郑州信大捷安信息技术股份有限公司、中电科网络安全科技股份有限公司、中移(杭州)信息技术有限公司、浙江九州量子信息技术股份有限公司、航天信息股份有限公司、OPPO广东移动通信有限公司、深圳市不动产登记中心。

本文件主要起草人：赵松、王银平、程磊、夏鲁宁、侯鹏亮、李述胜、刘平、李智虎、黄晶晶、程科伟、浦雨三、马洪富、袁中林、许涛、王玉林、焦靖伟、韩玮、谭武征、高振鹏、杜志强、肖淑婷、梁松涛、刘为华、王中武、王晨光、张文科、董亮亮、李根、路晓明、杨倩媚、颜海龙。

信息安全技术　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。

本文件适用于公开密钥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，密码设备的应用系统的开发。

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 20518　信息安全技术　公钥基础设施数字证书格式

GB/T 25069　信息安全技术　术语

GB/T 32918.1　信息安全技术　SM2 椭圆曲线公钥密码算法　第 1 部分：总则

GB/T 33560　信息安全技术　密码应用标识规范

GB/T 35275　信息安全技术　SM2 密码算法加密签名消息语法规范

GB/T 35276　信息安全技术　SM2 密码算法使用规范

GB/T 35291　信息安全技术　智能密码钥匙应用接口规范

GB/T 36322　信息安全技术　密码设备应用接口规范

GB/T 41389　信息安全技术　SM9 密码算法使用规范

GM/T 0094—2020　公钥密码应用技术体系框架规范

GM/Z 4001　密码术语

PKCS＃1　RSA 密码编译标准(RSA Cryptography Standard)

PKCS＃7　密码消息语法标准(Cryptographic Message Syntax Standard)

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

密钥容器　key container

密码设备中用于保存密钥唯一性存储空间。

4　缩略语

下列缩略语适用于本文件。

CA：证书认证机构(Certification Authority)

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