ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 43694—2024

网络安全技术　证书应用综合服务接口规范

Cybersecurity technology—Certificate application integrated service interface specification

2024-04-25 发布　　2024-11-01 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：北京数字认证股份有限公司、博雅中科(北京)信息技术有限公司、北京奇虎科技有限公司、山东得安信息技术有限公司、中国电力科学研究院、北京信安世纪科技股份有限公司、无锡江南信息安全工程技术中心、中国电子技术标准化研究院、格尔软件股份有限公司、中电科网络安全科技股份有限公司、深圳市不动产登记中心、郑州信大捷安信息技术股份有限公司、阿里云计算有限公司、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、数安时代科技股份有限公司、智巡密码(上海)检测技术有限公司、中科信息安全共性技术国家工程研究中心有限公司、中国汽车工程研究院股份有限公司。

本文件主要起草人：刘伟、赵永省、夏鲁宁、李述胜、刘中、程科伟、浦雨三、张屹、张志磊、马洪富、袁中林、李智虎、焦靖伟、刘平、黄晶晶、谭武征、寇建波、颜海龙、刘献伦、刘为华、肖淑婷、张文科、杨倩媚、董亮亮、周蔚林、韩玮、高振鹏、胡建勋、刘冲、牟洁。

网络安全技术　证书应用综合服务接口规范

1　范围

本文件规定了面向证书应用的综合服务接口要求和定义，描述了相应验证方法。

本文件适用于公钥密码基础设施应用技术体系下证书应用中间件和证书应用系统的开发，以及密码应用支撑平台的研制和检测。

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 20518　信息安全技术　公钥基础设施　数字证书格式

GB/T 25061　信息安全技术　XML 数字签名语法与处理规范

GB/T 25069　信息安全技术　术语

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 43578　信息安全技术　通用密码服务接口规范

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

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

数字证书　digital certificate

由 CA 签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

注：数字证书也称公钥证书，按类别分为个人证书、机构证书和设备证书，按用途分为签名证书和加密证书。

［来源：GM/Z 4001—2013，2.115］

3.2

用户密钥　user key

存储在设备内部的用于应用密码运算的非对称密钥对。

注：用户密钥包含签名密钥对和加密密钥对。

3.3

密钥容器　key container

密码设备中用于保存用户密钥的唯一性存储空间。