



中华人民共和国国家标准

GB/T 46795—2025

网络安全技术 公钥密码应用技术体系框架

Cybersecurity technology—
Public key cryptographic application technology framework

2025-12-02 发布

2026-07-01 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 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 公钥密码应用技术体系框架 2

 4.1 概述 2

 4.2 密码设备层 2

 4.3 通用密码服务层 3

 4.4 典型密码服务层 3

 4.5 密码基础设施层 3

5 框架内各部分间的关系 3

参考文献..... 5

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：格尔软件股份有限公司、北京国脉信安科技有限公司、北京信安世纪科技股份有限公司、中电科网络安全科技股份有限公司、赛西(深圳)电子信息产品标准化工程中心有限公司、广东省电子商务认证有限公司、兴唐通信科技有限公司、中国电子技术标准化研究院、智巡密码(上海)检测技术有限公司、中安云科科技发展(山东)有限公司、安徽问天量子科技股份有限公司、上海市数字证书认证中心有限公司、阿里云计算有限公司、新疆数字证书认证中心(有限公司)、中电信量子信息科技集团有限公司、飞天诚信科技股份有限公司、国民技术股份有限公司、上海势炎信息科技有限公司、长春吉大正元信息技术股份有限公司、浙江国利信安科技有限公司、北京天融信网络安全技术有限公司、深圳奥联信息安全技术有限公司、公安部第三研究所、中科信息安全共性技术国家工程研究中心有限公司、北京国泰网信科技股份有限公司、郑州信大捷安信息技术股份有限公司、北京中科卓信软件测评技术中心、北京数字认证股份有限公司、中安网脉(北京)技术股份有限公司、亚数信息科技(上海)有限公司、浙江云端保网络科技有限公司、渔翁信息技术股份有限公司、杭州海康威视数字技术股份有限公司、成都久信信息技术股份有限公司、北京启明星辰信息安全技术有限公司、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、华为技术有限公司。

本文件主要起草人：郑强、刘平、袁峰、汪宗斌、张立廷、陈树乐、赵敏、封维端、焦靖伟、王妮娜、韩玮、黄晶晶、郑海森、刘婧婧、王玉林、李世奇、谭瑞琥、罗俊、徐晓明、朱鹏飞、瓦里别克·吐达洪、尹文基、付月朋、赵丽丽、李红波、雷晓锋、安高峰、程朝辉、但波、傅大鹏、贾微微、孙健、胡建勋、李欣、付博雯、刘为华、刘中、黄福飞、李虹霖、王天顺、翟新元、王滨、陈萧宇、郭经宇、朱光剑、张彬、郑成龙、肖臻、王龙、曾光、陈加栋。

网络安全技术

公钥密码应用技术体系框架

1 范围

本文件确立了公钥密码应用技术体系框架,包括密码设备层、通用密码服务层、典型密码服务层和密码基础设施层,描述了该框架内各组成部分及其关系。

本文件适用于公钥密码技术和产品的研究、设计、开发和应用。

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—2022 信息安全技术 术语

3 术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

密码资源池 **cryptographic resource pool**

一组密码物理资源或虚拟密码资源的集合。

注：能够对密码资源进行实时监控、合理分配和负载均衡,具有可扩展性、高性能、低风险等特点。

3.2

密码模块 **cryptographic module**

实现密码运算功能,相对独立的软件、固件、硬件或这三者组合。

[来源:GB/T 25069—2022,3.379]

3.3

密码机 **cryptographic machine**

能独立运行,实现密码运算、密钥管理等功能,并提供密码服务的设备。

[来源:GB/T 25069—2022,3.377]

3.4

智能密码钥匙 **cryptographic smart token**

实现密码运算、密钥管理功能、提供密码服务的终端密码设备。

注：一般使用通用串行总线(USB)接口形态。

3.5

时间戳 **time stamp**

对时间和其他待签名数据进行签名得到的,用于表明数据属性的数据。

[来源:GB/T 25069—2022,3.542]