



# 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 发布  
国家标准化管理委员会



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]

3.6

电子签章 electronic seal signature

使用电子印章签署电子文件的过程。

[来源:GB/T 25069—2022,3.120]

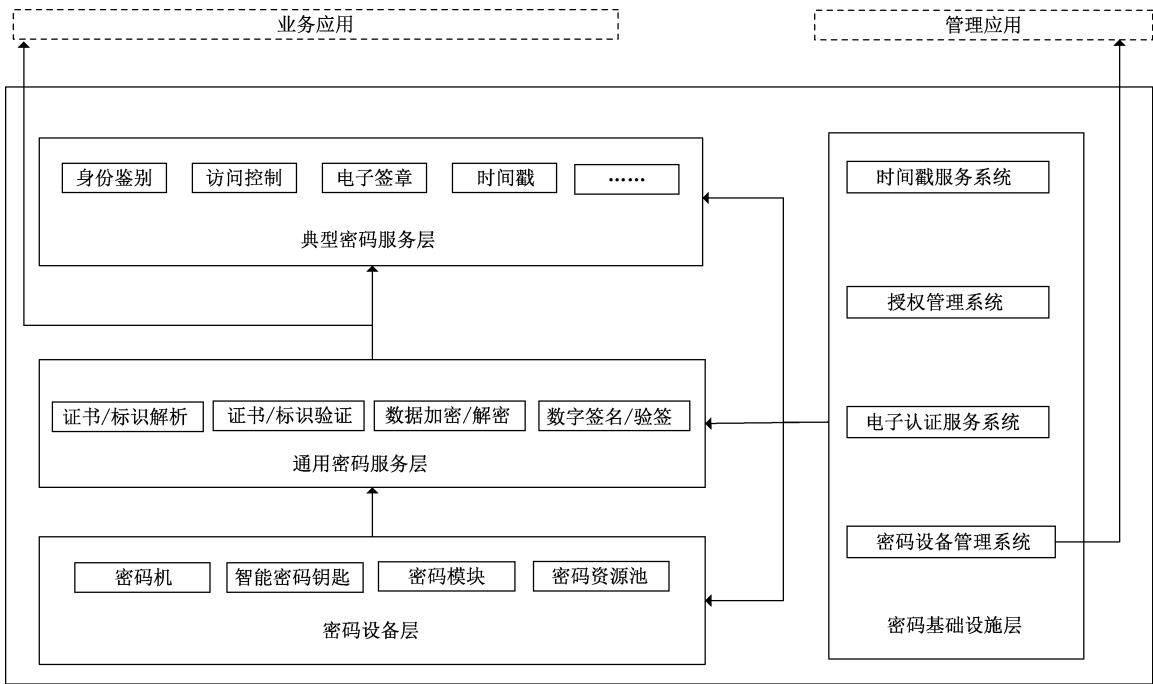
4 公钥密码应用技术体系框架

4.1 概述

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。技术体系框架为上层各业务应用提供统一的密码服务。在该框架内,密码设备层面向通用密码服务层提供密钥管理和基础密码运算服务;通用密码服务层面向典型密码服务层和业务应用提供数字证书及标识的解析、数据加解密、数字签名及验证等通用的密码功能服务;典型密码服务层面向业务应用提供身份鉴别、访问控制、电子签章及时间戳等一些典型的密码应用服务;密码基础设施层面向上述三层提供时间管理、权限管理、证书及标识管理和设备远程管理应用等基础服务。

该框架中,通用密码服务层和典型密码服务层可实体化实现,也可虚拟化实现。

公钥密码应用技术体系框架如图 1 所示,大的实线框为公钥密码应用技术体系框架图。



注：虚框不属于公钥密码应用技术体系框架。箭头表示支撑关系。

图 1 公钥密码应用技术体系框架图



4.2 密码设备层

密码设备层包括密码机、智能密码钥匙等密码模块类设备,或由密码模块构成的密码资源池,通过标准接口向通用密码服务层提供密钥生成、密码运算等基础密码服务。

密码设备具备密钥的加载、存储、更新、备份和恢复等功能,并保障密钥在密码设备中的安全。

服务端密码设备可通过密码设备管理系统提供的标准接口来接受远程管理。



### 4.3 通用密码服务层

通用密码服务层通过标准接口,向上层业务应用和典型密码服务层提供与密码设备、密码算法和具体密钥无关的密码功能服务。

通用密码服务层提供证书/标识解析、证书/标识验证,数据加密/解密及数字签名/验签等通用的密码服务功能。

通用密码服务层将上层的密码服务请求转化为具体的基础密码操作请求,通过调用密码设备实现具体的密码运算和密钥操作。

### 4.4 典型密码服务层

典型密码服务层包括但不限于身份鉴别、访问控制、电子签章和时间戳等服务,面向上层应用提供统一的共性密码应用服务。

典型密码服务层需要的密码功能由通用密码服务层提供。

身份鉴别通过标准接口为上层业务应用提供身份查询、身份解析、身份验证等身份鉴别服务。

访问控制通过标准接口为上层业务应用提供系统资源的访问控制,实现用户角色管理、系统资源管理、访问控制策略管理和用户授权管理等功能。

电子签章通过标准接口为上层业务应用提供电子印章制作、电子印章验证、电子签章生成和电子签章验证功能。

时间戳通过标准接口为上层业务应用和典型密码服务层中的其他组成部分提供时间戳加盖、验证等时间认证服务。

### 4.5 密码基础设施层

密码基础设施层由时间戳服务系统、授权管理系统、电子认证服务系统及密码设备管理系统等组成,为通用密码服务层、典型密码服务层、密码设备层提供基础服务。

时间戳服务系统对时间戳典型应用提供标准的接口调用,提供时间戳的产生和管理服务。

授权管理系统对访问控制典型应用提供标准的接口调用,实现授权与访问控制的机制。

电子认证服务系统包括证书认证系统和标识密码认证系统,对通用密码服务层提供标准的接口调用,实现应用对证书或标识密钥的访问与管理。

密码设备管理系统对密码设备进行管理,实现将上层管理应用的管理请求转换为标准的消息调用,通过安全通道实现管理应用与密码设备间的消息传递(例如密码设备远程配置、远程监控与合规性检验等)。

## 5 框架内各部分间的关系

公钥密码应用技术体系框架内各部分间的关系如图 1 所示。

密码设备层面向通用密码服务层,一般不直接面向典型密码服务层和业务应用。密码设备包括客户端密码设备和服务端密码设备。密码设备接口包括客户端密码设备接口、移动终端密码模块接口和服务端密码设备接口。服务端的密码设备可通过密码设备管理接口接受远程管理。

通用密码服务层面向典型密码服务层和业务应用,提供的接口包括通用密码服务接口和证书应用综合服务接口。

典型密码服务层面向业务应用,提供的接口包括身份鉴别接口、访问控制接口、电子签章服务接口和时间戳服务接口。

密码设备层、通用密码服务层和典型密码服务层提供的接口函数命名及错误代码区间见表 1。

表 1 接口的函数命名及错误代码区间表

框架内各层	接口名称	函数命名前缀	错误代码区间
密码设备层	智能密码钥匙接口	SKF_	0x0A000000~0x0AFFFFFF
	移动终端密码模块接口	SSF_	0x0D000000~0x0DFFFFFF
	密码设备应用接口	SDF_	0x01000000~0x01FFFFFF
通用密码服务层	通用密码服务接口	SAF_	0x02000000~0x02FFFFFF
	证书应用综合服务接口	SOF_	0x0B000000~0x0BFFFFFF
典型密码服务层	身份鉴别接口	SIF_	0x05000000~0x05FFFFFF
	访问控制接口	SPF_	0x07000000~0x07FFFFFF
	时间戳服务接口	STF_	0x04000000~0x04FFFFFF
	电子签章服务接口	SEF_	0x0C000000~0x0CFFFFFF
密码基础设施层	密码设备管理接口	SMF_	0x03000000~0x03FFFFFF



参 考 文 献

[1] GB/T 20520 网络安全技术 公钥基础设施 时间戳规范  
[2] GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范  
[3] GB/T 46798 网络安全技术 标识密码认证系统密码及其相关安全技术要求  
[4] GM/T 0032 基于角色的授权与访问控制技术规范  
[5] GM/T 0050 密码设备管理 设备管理技术规范

---

