ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 19714—2025
代替 GB/T 19714—2005

网络安全技术　公钥基础设施 证书管理协议

Cybersecurity technology—Public key infrastructure—Certificate management protocol

2025-08-01 发布　　2026-02-01 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。

本文件代替GB/T 19714—2005《信息技术　安全技术　公钥基础设施　证书管理协议》。与GB/T 19714—2005相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了标准的范围（见第1章，2005年版的第1章）；
b) 删除了PKI管理概述内容（见2005年版的第5章）；
c) 删除了加密密钥私钥拥有证明（见2005年版的6.3.2、7.2.8）和协商密钥私钥拥有证明相关内容（见2005年版的6.3.3）；
d) 删除了根CA的更新的相关内容（见2005年版的6.4、8.2）；
e) 删除了终端实体初始化和初始注册/认证相关的前提与限制（见2005年版的第6章）；
f) 增加了“流程与消息结构”，描述各PKI组件间证书管理的流程与消息结构（见第6章）；
g) 增加了协议支持的国家标准算法以及算法OID（见附录A的表A.1）；
h) 增加了“transactionID”的相关描述（见附录C的C.1.2.1）；
i) 增加了协议版本字段取值的设置（见C.1.2.1）；
j) 增加了“隐式确认”数据结构（见C.1.2.2）和“确认等待时间”数据结构（见C.1.2.3）；
k) 在PKIHead的generalInfo扩展项增加了对证书模板标识“certTemplateID”字段的支持（见C.1.2.4）；
l) 增加了“多重保护”相关描述（见C.1.4）；
m) 更改了加密值数据结构，修改为“SM2EnvelopedKey”（见C.2.2，2005年版的7.2.2），协议中加密数据统一更改使用“SM2EnvelopedKey”（见C.3.2、6.2.2，2005年版的7.3.2、附录E）；
n) 增加了证书确认相关内容（见C.1.3、C.3.15）；
o) 增加了“轮询请求和响应”数据结构（见C.3.19）；
p) 增加了证书冻结和证书解冻请求与响应相关内容（见C.1.3、C.3.20、C.3.21）；
q) 增加了有关失败状况的更多信息（见C.2.3）；
r) 增加了利用CertReqMessages进行多个证书的申请与利用CertRepMessage进行多个证书的响应时，有多种实现方式的说明，明确了实现上可有多种选择（见C.3.1和C.3.2），明确了一种常见的实现方式（见A.5）；
s) 删除了交叉认证相关内容（见2005年版的7.3.11、7.3.12、8.6）；
t) 删除了CA初始化、终端实体初始化相关的PKI管理功能内容（见2005年版的第8章）；
u) 删除了CMP协议的传输相关内容（见2005年版的第9章和附录G）；
v) 删除了“请求消息行为说明”（见2005年版的附录D），将其主要内容纳入附录C中（见C.2.8、C.3.1）；
w) 更改了证书管理协议OID（见附录F，2005年版的附录F）。

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、中国电子技术标准化研究院、西安西电捷通无线网络通信股份有限公司、博雅中科（北京）信息技术有限公司、长春吉大正元信息技术股份有限公司、上海市数字证书认证中心有限公司、华为技术有限公司、武汉大学、公安部第一研究所、亚数信息科技（上海）

有限公司、长扬科技(北京)股份有限公司、深圳市电子商务安全证书管理有限公司、陕西省信息化工程研究院、江南信安(北京)科技有限公司、郑州信大捷安信息技术股份有限公司、清华大学、格尔软件股份有限公司、广东省电子商务认证有限公司、同智伟业软件股份有限公司、北京时代新威信息技术有限公司、北京中关村实验室、浙江大华技术股份有限公司、工业和信息化部网络安全产业发展中心(工业和信息化部信息中心)、工信通(北京)信息技术有限公司、中国电子信息产业集团有限公司第六研究所、国网区块链科技(北京)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、奇安信网神信息技术(北京)股份有限公司、中电科网络安全科技股份有限公司。

本文件主要起草人:高文华、高文举、李彦峰、李琴、王秉新、丁肇伟、王玉林、曾光、何德彪、胡光俊、林雪焰、夏鲁宁、夏冰冰、李向锋、傅大鹏、刘中、王月辉、张国强、李志勇、田玉存、李亮、郭燕飞、丁蓓菁、邓晨、刘斌、赵婧、张紫薇、魏一才、赵华、沈志淳、张鑫、苏金岩、王志辉、郑会涛、赵晓荣、徐剑南、王彤、汪海洋、刘为华、贾珂婷、郑强、陈树乐、焦正坤、俞政臣、朱威儒、赵博鑫、张剑青、陈子雄、王进、王斌、王龙、杨珂、高振鹏、杜志强、安锦程、寇建波。

本文件及其所代替文件的历次版本发布情况为:

——2005 年首次发布为 GB/T 19714—2005;

——本次为第一次修订。

网络安全技术　公钥基础设施　证书管理协议

1　范围

本文件给出了公钥基础设施(PKI)中证书管理协议的结构和内容,规定了证书产生和管理所需要的协议消息格式。

本文件适用于公钥基础设施相关产品的研制,以及用于指导公钥基础设施相关产品的设计、开发和管理。

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 19713　网络安全技术　公钥基础设施　在线证书状态协议

GB/T 20518—2018　信息安全技术　公钥基础设施　数字证书格式

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

GB/T 25069—2022　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 35276—2017　信息安全技术　SM2 密码算法使用规范

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

数字签名　digital signature

被数据单元的接收者用以确认数据单元的来源和完整性,达到保护数据,防止被伪造的目的,附加在数据单元上的一些数据,或是对数据单元所做的密码变换。

[来源:GB/T 25069—2022,3.576,有修改]

3.2

杂凑算法　hash-algorithm

基于杂凑函数实现的密码算法。

3.3

个人安全环境　personal security environment;PSE

终端用于安全存储证书及私钥的环境。

3.4

拥有证明　proof of possession;POP

终端用以证明自己拥有(即能使用)与其申请证书的公钥相对应的私钥。