ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 19771—2025
代替 GB/T 19771—2005

网络安全技术　公钥基础设施 PKI 组件最小互操作规范

Cybersecurity technology—Public key infrastructure—Specification for minimum interoperability for PKI components

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 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　最小互操作基本功能要求 …… 3
5.1　概述 …… 3
5.2　CA 系统 …… 3
5.3　RA 系统 …… 4
5.4　证书持有者 …… 5
5.5　证书验证者 …… 5
5.6　密码算法 …… 6
6　互操作事务数据格式要求 …… 6
6.1　总体要求 …… 6
6.2　注册请求 …… 6
6.3　证书密钥更新 …… 10
6.4　撤销请求 …… 11
6.5　访问资料库 …… 13
7　测试评价方法 …… 13
7.1　通用测试评价方法 …… 13
7.2　最小互操作基本功能测试评价方法 …… 13
7.3　互操作数据格式测试评价方法 …… 15

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 19771—2005《信息技术　安全技术　公钥基础设施PKI组件最小互操作规范》，与GB/T 19771—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“范围”的内容，重新界定了文件的标准化对象和所覆盖的各个方面，并更改了文件的适用界限（见第1章，2005年版的第1章）；

b) 更改了PKI四个组件的基本功能要求（见第5章，2005年版的第5章），增加了对BYOD请求证书的功能要求（见5.3.2、5.4.2），增加了验证证书的最小步骤要求（见5.2.2），增加了对商用密码算法的支持（见5.6）；

c) 更改了互操作事务数据格式的要求，将对数字证书的数据结构、证书扩展、证书撤销列表的格式要求修改为符合GB/T 20518—2018（见6.1，2005年版的6.1、6.2、6.3）；将对PKI事务消息格式的内容的要求修改为符合GB/T 19714—2025（见6.1，2005年版的6.5）；更改了PKI事务的消息内容（见第6章，2005年版的6.6）；

d) 增加了对CA系统、RA系统、证书持有者、证书验证者功能的测试评价方法，增加了互操作数据格式测试评价方法（见第7章）；

e) 删除了规范性附录A、规范性附录B、规范性附录C、规范性附录D（见2005版的附录A、附录B、附录C、附录D）。

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：中国科学院大学、北京数字认证股份有限公司、公安部第三研究所、中国科学院软件研究所、长春吉大正元信息技术股份有限公司、安徽信科共创信息安全测评有限公司、清华大学、广东省电子商务认证有限公司、深圳市电子商务安全证书管理有限公司、亚数信息科技（上海）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、联通在线信息科技有限公司、北京中关村实验室、奇安信网神信息技术（北京）股份有限公司、陕西省信息化工程研究院、国家信息技术安全研究中心、中孚信息股份有限公司、杭州海康威视数字技术股份有限公司、中国电子信息产业集团有限公司第六研究所、长扬科技（北京）股份有限公司。

本文件主要起草人：冯登国、荆继武、刘丽敏、郑亚杰、陈妍、丁肇伟、张建国、寇春静、张立武、贾珂婷、张严、秦岭月、李强、陈树乐、郑会涛、魏一才、胡建勋、梁斌、赵博鑫、孟佳颖、安锦程、赵晓荣、梁利、陈腾、王滨、王龙、赵华。

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 19771—2005；

——本次为第一次修订。

网络安全技术　公钥基础设施 PKI组件最小互操作规范

1　范围

本文件规定了公钥基础设施组件最小互操作的基本功能要求和数据格式要求，描述了测试评价方法。

本文件适用于电子签名、电子签章、身份管理等活动中PKI的设计、开发、测试及其应用。

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 15852.2　网络安全技术　消息鉴别码　第2部分：采用专门设计的杂凑函数的机制

GB/T 19714—2025　网络安全技术　公钥基础设施　证书管理协议

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—2018　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 32905　信息安全技术　SM3密码杂凑算法

GB/T 32907　信息安全技术　SM4分组密码算法

GB/T 32918.2　信息安全技术　SM2椭圆曲线公钥密码算法　第2部分：数字签名算法

GB/T 37092　信息安全技术　密码模块安全要求

GB/T 43694　网络安全技术　证书应用综合服务接口规范

GM/Z 0001—2013　密码术语

3　术语和定义

GB/T 25056—2018、GM/Z 0001—2013界定的以及下列术语和定义适用于本文件。

3.1

PKI组件　public key infrastructure component

构成PKI系统的组成要素，用于进行证书相关活动的实体。

3.2

数字证书　digital certificate

由证书认证机构对用户的公钥和身份信息进行确认，并用私钥进行签名的数据。

注：也称公钥证书。

3.3

签名证书　signature certificate

用于证明签名公钥的数字证书。

[来源：GM/Z 0001—2013，2.90]