ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 21053—2023
代替 GB/T 21053—2007

信息安全技术　公钥基础设施 PKI 系统安全技术要求

Information security techniques—Public key infrastructure—Security technology requirement for PKI system

2023-03-17 发布　　2023-10-01 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 21053—2007《信息安全技术　公钥基础设施　PKI系统安全等级保护技术要求》。与GB/T 21053—2007相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 将名称修改为《信息安全技术　公钥基础设施　PKI系统安全技术要求》；
b) 对范围的内容进行了修改（见第1章，2007年版的第1章）；
c) 调整修改了规范性引用文件（见第2章，2007年版的第2章）；
d) 增加了“PKI系统框架与安全级别”一章，对PKI系统的基本框架、各组件的功能和本文件规定的PKI系统的安全等级进行了描述（见第5章）；
e) 将安全级别划分由2007年版的五个级别修改为基本级和增强级两个级别（见5.3，2007年版的5.1.1、5.2.1、5.3.1、5.4.1、5.5.1）；
f) 将2007年版5.1～5.5的内容调整至新增的6安全功能要求和7安全保障要求（见第6章和第7章，2007年版的5.1～5.5）；
g) 删除了2007年版中与实际部署相关的内容（物理安全、数据输入输出）；将其中“数据输入输出”中关于原发抗抵赖的要求调整为6.9“原发抗抵赖”（见6.9，2007年版的5.1.2、5.3.2、5.1.6和5.3.7）。

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。

本文件由全国信息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：中国科学院软件研究所、中国科学院大学、公安部第三研究所、公安部第一研究所、成都卫士通信息产业股份有限公司、北京信安世纪科技股份有限公司、北京数字认证股份有限公司、长春吉大正元信息技术股份有限公司、格尔软件股份有限公司、中国信息通信研究院、数安时代科技股份有限公司、北京创原天地科技有限公司、北京奇虎科技有限公司、中国电子科技集团公司第十五研究所、北京中电华大电子设计有限责任公司、国网区块链科技（北京）有限公司、华为技术有限公司、郑州信大捷安信息技术股份有限公司、西安西电捷通无线网络通信股份有限公司、天津南大通用数据技术股份有限公司、北京软件产品质量检测检验中心、同智伟业软件股份有限公司、北京百度网讯科技有限公司、亚数信息科技（上海）有限公司、广州市百果园信息技术有限公司、广州市网星信息技术有限公司、中金金融认证中心有限公司。

本文件主要起草人：张立武、张严、王蕊、陈妍、冯登国、顾健、邱梓华、李景华、亢洋、李谦、刘丽敏、张妍、刘玉岭、郑强、张立廷、傅大鹏、汪宗斌、张宝欣、寇春静、刘金华、李健、丁肇伟、王现方、王榕、周蔚林、肖青海、张屹、刘健、黄钰、李达、褚超、周吉祥、杜志强、毛巨辉、孟祥振、焦正坤、韩长青、魏一才、朱晓宇、钟清华、李达。

本文件及其所代替文件的历次版本发布情况为：

——2007年首次发布为GB/T 21053—2007；
——本次为第一次修订。

信息安全技术　公钥基础设施
PKI系统安全技术要求

1　范围

本文件将PKI系统的安全级别划分为基本级和增强级，规定了相应安全级别的安全功能要求和安全保障要求。

本文件适用于PKI系统的研发，PKI系统产品的测评和采购参照使用。

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 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 25069　信息安全技术　术语

GM/T 0014—2012　数字证书认证系统密码协议规范

3　术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

PKI系统　PKI system

公钥基础设施中，基于公钥密码体制，实现数字证书的发布、撤销和管理等功能，并为订户（3.4）提供相应服务的信息系统。

3.2

拆分知识　split knowledge

将密码密钥拆分成多个密钥组件的如下过程：各单个组件并不共享原始密钥的知识，而能由分开的实体随后将其输入密码模块或从密码模块输出，经组合来重新创建原始密码密钥。

注：能请求组件的全部或其某一子集来完成此种组合。

［来源：GB/T 25069—2022，3.120］

3.3

系统用户　system user

在PKI系统中，通过系统操作界面进行特定操作，实现对系统特定功能进行控制的用户。

示例：PKI系统的管理员、审计员和操作员。

［来源：GB/T 25069—2022，3.652，有修改］