ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 21054—2023
代替 GB/T 21054—2007

信息安全技术　公钥基础设施 PKI 系统安全测评方法

Information security techniques—Public key infrastructure—Security testing assessment approaches 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 21054—2007《信息安全技术　公钥基础设施　PKI 系统安全等级保护评估准则》。与 GB/T 21054—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 系统安全测评方法》；

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“ 概述”一章，对 PKI 系统通用的测评方法进行了描述（见第 5 章）；

e) 将 2007 年版的第 5 章评估内容调整至新增的第 6 章安全功能测评方法和第 7 章安全保障测评方法（见第 6 章和第 7 章，2007 年版的第 5 章）；

f) 删除了 2007 年版中关于物理安全的测评方法，将其中“数据输入输出”中关于原发抗抵赖的测评方法调整为 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、北京百度网讯科技有限公司、同智伟业软件股份有限公司、北京软件产品质量检测检验中心、天津南大通用数据技术股份有限公司、西安西电捷通无线网络通信股份有限公司、郑州信大捷安信息技术股份有限公司、华为技术有限公司、国网区块链科技（北京）有限公司、北京中电华大电子设计有限责任公司、中国电子科技集团公司第十五研究所、北京奇虎科技有限公司、北京创原天地科技有限公司、数安时代科技股份有限公司、中国信息通信研究院、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：张严、张立武、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、张立廷、傅大鹏、郑强、张宝欣、汪宗斌、寇春静、刘金华、李健、丁肇伟、王现方、韩长青、金健、孟祥振、毛巨辉、李琴、韩秀德、褚超、石竹玉、黄钰、董晶晶、唐占国、肖青海、周蔚林、王榕、魏一才、朱晓宇、钟清华、李达、刘为华。

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 21054—2007；

——本次为第一次修订。

信息安全技术　公钥基础设施
PKI 系统安全测评方法

1　范围

本文件依据 GB/T 21053—2023 规定了 PKI 系统的安全测评方法，包括安全功能测评方法和安全保障要求测评方法。

本文件适用于 PKI 系统的安全测评。

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 21053—2023　信息安全技术　公钥基础设施 PKI 系统安全技术要求

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 21053—2023 和 GB/T 25069 界定的术语和定义适用于本文件。

4　缩略语

GB/T 21053—2023 界定的缩略语适用于本文件。

5　概述

本文件依据 GB/T 21053—2023 规定的 PKI 系统的安全级别及相应级别的安全技术要求，给出了对应的安全测评方法。

PKI 系统的典型框架、安全功能及安全级别划分见 GB/T 21053—2023 中第 5 章。对于基本级的 PKI 系统，依据本文件第 6 章和第 7 章中与基本级安全要求对应的测评方法进行测评；对于增强级的 PKI 系统，依据本文件第 6 章和第 7 章中与增强级安全要求对应的测评方法进行测评。完成所有安全要素测评后，所有测评结论均为“符合”的，可给出被测评 PKI 系统“符合相应安全等级”的测评结论。其他情况，测评结论应记为“不符合相应安全等级”。

本文件中，使用**“宋体加粗”**的文字表示增强级 PKI 系统在基本级 PKI 系统基础上增加的安全要求对应的测评方法。

6　安全功能测评方法

6.1　密钥管理通用要求测评方法

密钥管理通用要求部分的测试方法、预期结果和结果判定如下。