国家标准《信息安全技术 公钥基础设施 PKI系统安全测评方法》（征求意见稿）编制说明

一、 工作简况

1.1 任务来源

根据全国信息安全标准化技术委员会2020年下达的国家标准制修订计划，国家标准《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》由中国科学院软件研究所负责。

1.2 主要起草单位和工作组成员

本标准的主要起草单位为：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、成都卫士通信息产业股份有限公司、北京信安世纪科技有限公司、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、北京百度网讯科技有限公司、北京奇虎科技有限公司、北京软件产品质量检测检验中心、格尔软件股份有限公司、国网区块链科技（北京）有限公司、华为技术有限公司、天津南大通用数据技术股份有限公司、同智伟业软件股份有限公司、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、中国汽车工程研究院股份有限公司、中国信息通信研究院、中金金融认证中心有限公司。工作组主要成员包括：张严、张立武、....等。

1.3 编制过程

标准起草过程如下：

2019年10月 - 2020年10月：组建标准编制组，结合GB/T 22239-2019修订情况和GB/T 20153现行版本在应用中的反馈对当前PKI系统等级保护技术进行了调研，提出了《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》修订稿草案初稿，并以多种形式征求专家和相关单位意见。

2020年10月26日：参加了全国信息安全标准化技术委员会WG4工作组召开的组内专家评审会，工作组汇报标准编制情况，专家组审阅了相关文档，质询了有关问题，并提出了修改意见。**参会专家一致同意通过对该项标准草案的评审**，建议标准编制单位根据本次会议的意见修改后提交工作组。

2020年11月10日，参加了全国信息安全标准化技术委员会第二次会议周，

经工作组讨论建议本标准保持草案阶段，会后，标准编制单位根据本次会议的意见形成了新一版的工作组草案。

2021 年 3 月 9 日，参加了全国信息安全标准化技术委员会组织召开的“2020 年网络安全国家标准项目阶段性检查”会议，编制组针对标准编制过程中发现的标准名称和范围与当前标准实际应用情况进行了说明，经专家讨论，建议将本标准的名称修改为《信息安全技术 公钥基础设施 PKI 系统安全测评方法》。之后，标准牵头单位向 WG4 工作组提交了名称修改申请，WG4 工作组经讨论，同意名称修改申请提交至 TC260 秘书处。

2021 年 3 月至 4 月，编制组根据修改后的标准名称和范围，对标准草案进行了修改，形成了《信息安全技术 公钥基础设施 PKI 系统安全测评方法》标准草案（2021 年 4 月版本）。

2021 年 5 月 12 日，参加了在武汉召开的全国信息安全标准化技术委员会 2021 年第一次会议周，经 WG4 组全体成员单位投票决定，**同意本标准形成征求意见稿。**会后，标准编制单位根据本次会议的意见形成了《信息安全技术 公钥基础设施 PKI 系统安全测评方法》征求意见稿。

二、 标准编制原则和确定主要内容的论据及解决的主要问题

本标准是对国家标准 GB/T 21054-2007《信息安全技术 公钥基础设施 PKI 系统安全等级保护技术要求》的修订，旨在令本标准适用于技术的发展以及生产现状。由于本标准所依据的国家标准 GB/T 21053.2-2007 正在进行修订，需要对标准进行修订，以保证本标准评估准则与相应技术要求的一致性。

根据对相关标准、技术更新情况以及现行标准在应用中的反馈情况进行调研和编制组内部讨论，本标准拟主要修订以下内容：

1）明确本标准的定位为《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》的下位标准，针对《PKI 系统安全等级保护技术要求》提出的技术要求，一一对应地给出相应的测评方法。

2）由于《PKI 系统安全等级保护技术要求》的名称需要进行修改，为保持相关标准名称的一致性，同时考虑到网络安全产品国家标准命名的惯例，将标准项目名称修改为《信息安全技术 公钥基础设施 PKI 系统安全测评方法》。

3）对技术内容和框架进行修订，以保持本标准与 GB/T 20153 标准的一致性；

4）对现行标准的技术内容进行调整，给出具体的评估流程和预期结果，解决现行版本中技术内容与范围存在不一致的情况。

本文件依据GB/T 21053-XXXX中对不同等级PKI系统所提出的技术要求，给出了对应的测评方法。

本文件适用于PKI系统的安全保护等级的评估，对于PKI系统安全功能的研制、开发、测试和产品评估亦可参照使用。

三、 主要试验[或验证]情况分析

暂无

四、 知识产权情况说明

本标准未涉及已知的专利等知识产权内容。

五、 产业化情况、推广应用论证和预期达到的经济效果

暂无

六、 采用国际标准和国外先进标准情况

暂无

七、 与现行相关法律、法规、规章及相关标准的协调性

本标准在编制过程中，已经查阅了《中华人民共和国网络安全法》、《中华人民共和国电子签名法》等相关法规，确保本标准内容遵守相关法律规定。确保相关内容和术语与这些标准的内容保持一致。

本标准在编制过程中，保持与 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》以及 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的协调性，使符合本标准要求的 PKI 系统能够支持构建符合上述标准要求的证书认证系统。

八、 重大分歧意见的处理经过和依据

编制过程中未出现重大分歧。

九、 标准性质的建议

建议本标准作为推荐性国家标准发布实施。

十、 贯彻标准的要求和措施建议

暂无

十一、 替代或废止现行相关标准的建议

本部分替代 GB/T 21054-2007。

十二、 其它应予说明的事项

无。

《信息安全技术 公钥基础设施 PKI 系统安全测评方法》
标准编制组
二〇二一 年 五 月