国家标准《信息安全技术 公钥基础设施 PKI系统安全技术要求》（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系统安全等级保护技术要求》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、北京创原天地科技有限公司、北京奇虎科技有限公司、北京中电华大电子设计有限责任公司、格尔软件股份有限公司、公安部第一研究所、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、郑州信大捷安信息技术股份有限公司、中国汽车工程研究院股份有限公司、中国信息通信研究院。工作组主要成员包括：张立武、张严、....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系统安全等级保护技术要求》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 系统安全技术要求》。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 系统安全技术要求》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 系统安全技术要求》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 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》的修订，旨在令本标准适用于技术的发展以及生产现状。现行国家标准 GB/T 21053.2-2007 发布已超过十年，在此期间，等级保护标准体系、公钥基础设施以及我国密码行业的应用情况均发生了较大的变化，亟需对标准进行修订。

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：

《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》为修订标准，现行标准的技术内容规定了 PKI 系统产品的等级及相应等级的安全技术要求，主要应用于 PKI 系统产品的测评。自标准发布后，由于信息系统等级保护技术体系的发展，“等级保护”一词已有了较为严格和规范的内涵，主要针对实际部署运行的信息系统，与本标准针对产品的技术范围存在差异，继续沿用原名称会造成名词定义冲突。为避免歧义，明确标准对象，更好地支持本标准的实际应用工作，将标准项目名称修改为《信息安全技术 公钥基础设施 PKI 系统安全技

术要求》。

根据本标准的实际应用情况，对标准的技术要求进行修订，删除与实际部署相关的技术要求。

明确本标准中规定的安全等级为 PKI 系统的等级划分，并给出相应等级 PKI 系统的安全功能要求和安全保障要求。根据系统产品安全技术要求相关标准的写作惯例，将安全级别划分由原有的五个级别修改为两个级别（基本级和增强级）。

本文件适用于 PKI 系统的设计和实现，对于 PKI 系统安全功能的研制、开发、测试和产品采购亦可参照使用。

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 21053-2007。

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系统安全技术要求》
标准编制组
二〇二一 年 五 月