国家标准《信息安全技术 信息系统密码应用设计技术要求》（征求意见稿）编制说明

一、工作简况

1、任务来源

本标准由国家标准化管理委员会下达的国家标准编制计划，项目名称为《信息安全技术 信息系统密码应用设计技术要求》（计划号：20210986-T-469），项目类型为标准制定，项目所属工作组为 WG3 工作组。本项目由鼎铉商用密码测评技术（深圳）有限公司牵头编制。

2、主要起草单位和工作组成员

项目编制组成员单位主要包括：鼎铉商用密码测评技术（深圳）有限公司等。

3、主要工作过程

2020 年 5 月，项目组在信安标委 WG3 工作组召开的 2020 年申报项目和在研项目推进工作会议上，向专家和工作组其他成员单位汇报了《信息安全技术 信息系统密码应用设计技术要求》（投票草案稿）工作情况，收集了各位专家的立项反馈意见。WG3 专家及成员工作组成员单位同意该标准立项，与密码行业标准同步制定。

2020 年 6 月-7 月，本标准项目牵头单位根据立项反馈意见对标准进行修订，并在项目组内征求意见。此阶段主要对标准框架、设计原则、密钥管理、产品选用细粒度、是否纳入安全管理等问题进行了明确。

2020 年 8 月-11 月，本标准项目牵头单位多次参与密标委组织的专家评审会议，收集各评审专家的专业意见，并在会后组织项目组各成员单位开展研讨，对草案稿进行修改完善，并于 2020 年 11 月 5 日形成新标准草案提交 WG3 工作组审查。根据此次会议的专家评审意见，建议标准名称变更为《信息安全技术 信息系统密码应用设计技术指南》。

2020 年 12 月-2021 年 3 月，本标准项目牵头单位 WG3 工作组专家评审意见，优化了标准框架，增加设计要点、设计活动、密码应用需求分析方法等内容，优化了密码应用方案模板。

2021 年 4 月-2021 年 6 月，本标准项目牵头单位根据 2021 年 4 月 WG3 工作组专家评审意见，进一步加大标准工作推进力度，并对专家意见对标准进行修改。

2021 年 7 月-2021 年 8 月，召集 2 次参编工作会议，1 次责任专家工作会议，多次内部工作讨论会议，将标准主要核心部分调整成：设计原则、设计概要、信息系统应用层设计指南、密码支撑层设计指南、密码产品部署、密钥管理安全设计指南。附录增加密码服务支撑技术架构设计示例。

2021 年 11 月，标准周会议上向各位专家汇报了标准情况，并组织了国密局商密办等内部专家参与的专题会议，讨论标准内容，根据两次会议专家意见，修改和完善标准文本。

2021 年 12 月，信安标委秘书处组织了标准征求意见稿的专家审查会，会上专家对如何完善文本的内容提出了建议。会后编制组根据专家意见，对标准文本进行了修改完善。

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

1、标准编制原则

本标准的编制原则是：合规性、安全性、协调性、可行性

1) 合规性：本标准依据《信息安全技术 信息系统密码应用基本要求》（征求意见稿），指导信息系统实现密码功能、密钥管理所使用的密码算法、密码技术、密码产品和密码服务均符合相关国家标准、行业标准；

2) 安全性：本标准指导信息系统运营者从信息安全风险评估和依据《信息安全技术 信息系统密码应用基本要求》（征求意见稿）两个角度充分分析密码应用需求。

3) 协调性：本标准与《信息安全技术 信息系统密码应用基本要求》（征求意见稿）、《信息安全技术 信息系统密码应用测评要求》（草案）、《信息系统密码应用实施指南》等标准中的相关内容保持一致；

4) 可行性：本标准可用于指导信息系统密码应用方案的设计，指导信息系统运营者设计出具备总体性、科学性、完备性和可行性的密码应用方案。

2、确定主要内容的论据及解决的主要问题

本标准制定参考以下国家标准、行业标准：

1) GB/T 15843（所有部分） 信息技术 安全技术 实体鉴别

2) GB/T 22239 信息安全技术 网络安全等级保护基本要求

3) GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

4) 信息安全技术 术语（征求意见稿）

5） GB/T 35273　信息安全技术 个人信息安全规范

6） 信息安全技术 信息系统密码应用基本要求（征求意见稿）

7） 信息安全技术 信息系统密码应用测评要求（草稿）

解决的主要问题：信息系统密码应用方案设计直接决定着信息系统密码应用能否合规、正确、有效的部署实施。当前正在制定中的国标《信息安全技术 信息系统密码应用基本要求》提出了信息系统中密码应用的基本要求。《信息安全技术 信息系统密码应用设计技术要求》与同步制定的密码行业标准作为对《信息安全技术 信息系统密码应用基本要求》的补充，将有力指导密码技术在信息系统中合规、正确和有效的应用。

3、本部分在确定主要内容时主要基于如下几个方面：

1） 进行信息系统密码应用设计框架研究，明确信息系统密码应用方案顶层设计方法，形成包括信息系统现状分析、密码应用需求分析和密 码应用设计等内容的总体设计思路，给予方案设计方法论上的指导，并制定密码应用方案模板；

2） 开展信息系统密码应用设计中的密码应用技术研究，将密码安全需求落实到密码功能上，将密码功能落实到具体算法、技术、产品、服务上；

3） 开展信息系统密码应用设计中的密钥管理研究，同时给出密钥管 理的方法和措施，给予具体的密码应用设计指导。

三、主要试验[或验证]情况分析

暂无。

四、知识产权情况说明

本标准不涉及专利及知识产权问题。

五、产业化情况、推广应用论证和预期达到的经济效果

本标准将从规划、建设、应急等方面对密码应用方案设计进行规范和约束，将有力指导密码技术在信息系统合规、正确、有效应用：首先，本标准可以服务信息系统运营者，指导其完成密码应用方案设计，同时也可能为评审密码应用方案的专家或测评机构提供参考；其次，本标准可以帮助制定出合理的密码应用实施方案，可以方便信息系统集成建设方正确实施和部署密码应用；最后，本标准有助于制定出合理的密码应用方案，合理的密码应用方案可以作为密码应用安全性评估的有力参考，有效降低评估成本、提升评估质量，推进密码应用工作的实

际落地。

六、采用国际标准和国外先进标准情况

无。

七、与现行相关法律、法规、规章及相关标准的协调性

本标准与相关法律、《信息安全技术 信息系统密码应用基本要求》（征求意见稿）、《信息安全技术 信息系统密码应用测评要求》（草案）、《信息系统密码应用实施指南》中的相关内容保持一致。

八、重大分歧意见的处理经过和依据

无。

九、标准性质的建议

建议作为国家推荐性标准发布。

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

无。

十二、其它应予说明的事项

无。

《信息安全技术 信息系统密码应用设计技术指南》编制工作组

2021-11-28