《证券业商用密码应用上线指南》

编制说明

为全面贯彻落实总体国家安全观，构建以密码技术为核心、多种技术相互融合的新网络安全体系，保障网络与信息安全，维护国家安全和社会公共利益。中国证券业协会证券科技委员会成员单位银河证券、广发证券和兴业证券联合编写了《证券业商用密码应用上线指南》（以下简称《商用密码上线指南》），《商用密码上线指南》结合相关规定及证券行业发展特点，将证券公司商用密码工作改造上线工作进一步标准化，建立商用密码上线标准，指导证券公司商用密码改造上线工作。团体标准供会员单位及社会组织自愿采用。现就相关情况说明如下：

1. 起草背景

密码工作是党和国家的一项特殊重要工作,直接关系国家政治安全、经济安全、国防安全和信息安全。2019年10月26日,十三届全国人大常委会第十四次会议审议通过《中华人民共和国密码法》，自2020年1月1日起施行。国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，以促进密码技术进步、产业发展,切实维护国家安全、社会公共利益以及公民、法人和其他组织的合法权益。

证券业各机构在中国证监会统一组织、协调管理下，2015年开始着力密码算法的技术研究和设计等工作。中国证券业协会指导团标起草组通过梳理行业商用密码改造上线成果，形成方便使用的上线标准，为证券业信息系统摆脱底层安全通讯对国际算法（RSA、AES、MD5等）的过度依赖提供保障，符合国家层面从国家安全和长远战略高度考虑的信息安全要求，同时增强行业信息系统“安全可控”的能力。

为进一步加快推进商用密码在证券业的应用，团标起草组通过综合分析整个证券业信息系统共性特点，结合当前证券业商用密码应用已上线现状，对商用密码改造上线工作进行规范化、标准化，保障行业机构顺利开展密码应用上线工作。该标准对于降低市场参与者成本，指导相关单位信息系统商密改造按标准上线、按规范管理具有重要意义。

1. 主要内容：

《商用密码上线指南》共七部分，主要涵盖商用密码应用上线的基本要求、系统上线和应急管理三方面。其中基本要求是关于商用密码应用上线的基本性保障的概述，涵盖组织、经费和制度等要求，为推进系统顺利上线提供基础保障。系统上线分别给出上线前、上线中和上线后三阶段的实施概述，包括制定上线所需的系统测试方案、上线策略、上线实施方案等。应急管理则描述商用密码应用上线的应急实施方式，通过应急准备、应急处理和调查处理三部分，给出应急事件的事前、事中和事后的实施概述。附录则提供信息系统商用密码改造首次引入的安全模块应急案例，包括SSL VPN接入网关、数字证书认证系统和密钥管理系统（KMS）各类故障的应急措施。

1. 意见收集情况

由中国证券业协会信息科技部牵头，组织行业单位针对《商用密码上线指南》进行意见收集，团标起草组充分采纳相关意见建议，最终完成《商用密码上线指南（送审稿）》。

主要的意见建议包括“组织保障”中增加“工作小组组织相关人员持续开展商用密码相关知识及标准规范学习培训，落实系统上线后的运维和管理保障工作”，“上线后监控和质量保证措施”中增加“系统容量”的监控，“密码应用安全性评估”中增加“网络安全等级二级以上和二级以下系统”的改造要求，“安全测试”中增加“个人信息保护安全”内容等。

1. 主要试验（或验证）分析

本标准在起草时，参考了行业内的优秀改造实例，全面考量了应用改造的稳定性、完整性、兼容性以及扩展性，三家起草单位在本单位的商用密码应用上线过程中，均已按照本标准的内容进行了实践，三家单位的验证结果证明了相关内容在实际应用中的有效性、可行性和可靠性。