ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31508—2015

信息安全技术　公钥基础设施
数字证书策略分类分级规范

Information security techniques—Public key infrastructure—Digital certificate policies classification and grading specification

2015-05-15 发布　　2016-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

GB/T 31508—2015

中华人民共和国
国家标准
信息安全技术　公钥基础设施
数字证书策略分类分级规范
GB/T 31508—2015
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 3.25　字数 87 千字
2015年5月第一版　2015年5月第一次印刷
*
书号:155066·1-51451　定价 45.00 元

GB/T 31508-2015

表 42　证书策略对内部审计周期的要求

类别	级别	内部审计周期要求
基线	基线	每年
商业交易	商业交易普通级	每年
	商业交易中级	每半年
	商业交易高级	每 3 个月
设备	设备普通级	每半年
	设备可信级	每 3 个月
公众服务	公众服务非实名级	每半年
	公众服务实名级	每半年

12.2　评估者的身份/资质

进行合规性审计和评估的机构，应是电子认证服务管理部门认可的机构。

参与电子认证服务机构评估的人员应证明其具备计算机安全方面的相关专业知识，在信息安全和PKI审计评估方面有丰富的经验。

12.3　评估者与被评估者的关系

评估者和电子认证服务机构之间应是相互独立的，没有任何利益关系。

12.4　对不足采取的措施

电子认证服务机构完成内部评估后，评估人员应列出所有问题条目的详细清单，由评估人员和被评估对象共同讨论有关问题，并将结果书面通知电子认证服务机构，进行后续处理。

外部评估完成后，电子认证服务机构应根据评估的结果检查缺失和不足，根据提出的整改要求，提交修改和预防措施以及整改计划书，并接受对整改计划的审查，以及对整改情况的再次评估。

对于整改计划不完善或者限期整改后不能达到要求的电子认证服务机构，电子认证服务管理部门有权终止其签发本标准中策略证书的服务。

12.5　评估结果的传达

审计评估机构在完成评估后，应在 15 d 内向电子认证服务管理部门提交评估结果。电子认证服务管理部门根据需要发布评估结果。

目　　次

表 40（续）

类别	级别	电子认证服务软件完整性验证要求
商业交易	商业交易高级	软件安装前验证软件的完整性。电子认证服务机构应有相应的机制监视电子认证服务系统的配置变化，并有文档化记录。电子认证服务机构至少每天进行一次完整性校验
设备	设备普通级	软件安装前验证软件的完整性。电子认证服务机构应有相应的机制监视电子认证服务系统的配置变化，并有文档化记录。电子认证服务机构至少每两天进行一次完整性校验
	设备可信级	软件安装前验证软件的完整性。电子认证服务机构应有相应的机制监视电子认证服务系统的配置变化，并有文档化记录。电子认证服务机构至少每天进行一次完整性校验
公众服务	公众服务非实名级	软件安装前验证软件的完整性。电子认证服务机构应有相应的机制监视电子认证服务系统的配置变化，并有文档化记录。电子认证服务机构至少每两天进行一次完整性校验
	公众服务实名级	软件安装前验证软件的完整性。电子认证服务机构应有相应的机制监视电子认证服务系统的配置变化，并有文档化记录。电子认证服务机构至少每两天进行一次完整性校验

10.7 网络的安全控制

电子认证服务机构应配备网络防火墙、过滤路由等设备，以阻止非法访问。

电子认证服务机构内部网络上传输的敏感信息应进行加密和完整性保护。

本标准中证书策略对电子认证机构和注册机构在线状态的要求，如表 41 所示。

表 41 证书策略对网络安全控制的要求

类别	级别	电子认证服务机构	注册机构
基线	基线	不作要求	不作要求
商业交易	商业交易普通级	不作要求	不作要求
	商业交易中级	可以短时在线	不作要求
	商业交易高级	不允许在线	不允许在线
设备	设备普通级	可以短时在线	不作要求
	设备可信级	不允许在线	不允许在线
公众服务	公众服务非实名级	可以短时在线	不作要求
	公众服务实名级	可以短时在线	不作要求

10.8 时间标记

证书、证书撤销列表、日志和其他关键信息应包含准确的时间和日期信息。

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：中国科学院数据与通信保护研究教育中心、北京数字证书认证中心有限公司、中国科学院软件所。

本标准主要起草人：荆继武、高能、林璟锵、王展、马存庆、向继、王跃武、夏鲁宁、查达仁、王平建、王琼霄、詹榜华、连一峰。