



中华人民共和国国家标准

GB/T 28447—2012

信息安全技术 电子认证服务机构运营管理规范

Information security technology—Specification on the operation management of a
certificate authority

2012-06-29 发布

2012-10-01 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

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 电子认证服务机构运营的业务	2
5.1 用户证书服务	2
5.2 用户证书密钥服务	4
5.3 认证系统功能要求	5
5.4 认证业务流程要求	5
6 业务运营中的风险	6
7 认证系统运行要求	6
7.1 网络系统安全	6
7.2 主机系统安全	6
7.3 系统冗余与备份	7
7.4 系统运营维护安全管理	8
7.5 密码设备安全管理	9
7.6 CA 密钥和证书管理	10
8 物理环境与设施	11
8.1 运营场地	11
8.2 运营区域划分及要求	11
8.3 安全监控系统	12
8.4 环境保护与控制设施	13
8.5 支撑设施	14
8.6 场地访问安全管理	14
8.7 场地监控安全管理	14
8.8 注册机构场地安全	14
9 组织与人员管理	14
9.1 职能与角色设置	14
9.2 安全组织	15
9.3 人员安全管理	16
10 文档、记录与介质管理	16
10.1 文档管理	16
10.2 记录管理	18

10.3 介质管理	18
11 业务连续性要求	19
11.1 业务连续性计划	19
11.2 应急处理预案	19
11.3 灾难恢复计划	19
11.4 灾备中心	20
12 审计与改进	20
12.1 审计	20
12.2 改进	21
附录 A (资料性附录) 业务运营风险举例	22

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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。

本标准主要起草单位:北京天威诚信电子商务服务有限公司、颐信科技有限公司。

本标准主要起草人:唐志红、李延昭、魏一才、徐虎、龙毅宏、刘旭、许蕾、赵宏科、张海松、郭宏杰。

引 言

本标准是为贯彻执行《中华人民共和国电子签名法》(以下简称《电子签名法》),规范电子认证服务机构的运营管理而制定。

本标准覆盖了电子认证服务机构运营管理的主要方面,提供公共认证服务的电子认证服务机构应按本标准的规定开展相关的工作。本标准涉及面多,但对每方面只做重点的、关键的、必要的要点性规定,确保电子认证服务机构执行本标准时在具体技术上、策略上和方案上有很大的灵活性。比如,对于认证系统安全方面,本标准只规定需要采用的安全防护技术和手段及需要考虑的关键点,对具体实现技术并未做规定。

信息安全技术

电子认证服务机构运营管理规范

1 范围

本标准规定了电子认证服务机构在业务运营、认证系统运行、物理环境与设施安全、组织与人员管理、文档、记录、与介质管理、业务连续性、审计与改进等多方面应遵循的要求。

本标准适用于在开放互联环境中提供数字证书服务的电子认证服务机构的建设、管理及评估。

对于在封闭环境中(如在特定团体或某个行业内)运行的电子认证服务机构可根据自身安全风险评估以及国家有关的法律法规有选择性地参考本标准。国家有关的测评机构、监管部门也可以将本标准作为测评和监管的依据。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 2887 计算机场地通用规范

GB/T 9361 计算机场地安全要求

GB/T 25056—2010 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 26855—2011 信息安全技术 公钥基础设施 证书策略与认证业务声明框架

GB 50045 高层民用建筑设计防火规范

GB 50057 建筑物防雷设计规范

GB 50174 电子信息系统机房设计规范

GB 50343 建筑物电子信息系统防雷技术规范

SJ/T 10796 防静电活动地板通用规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子认证服务机构 **certificate authority**

负责创建、分发证书并在必要时提供验证以证实用户身份的机构,一般是受用户信任的权威机构,用户可以选择该机构为其创建密钥。通常将电子认证服务机构简称为CA,也称为CA中心、CA机构、认证机构、证书认证机构等。

3.2

电子认证服务 **electronic certification service**

电子认证服务是指为电子签名相关各方提供真实性、可靠性验证的活动。

3.3

证书策略 **certificate policy**

命名的一组规则,指出证书对具有共同安全要求的特定团体和/或应用的适用性。