



中华人民共和国公共安全行业标准

GA/T 687—2007

信息安全技术 公钥基础设施安全技术要求

Information security techniques—
Technology requirements of public key infrastructure security

2007-03-20 发布

2007-05-01 实施

中华人民共和国公安部 发布

目 次

前言	V
引言	VI
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 安全等级保护技术要求	2
5.1 第一级	2
5.1.1 概述	2
5.1.2 物理安全	2
5.1.3 角色与责任	2
5.1.4 访问控制	3
5.1.5 标识与鉴别	4
5.1.6 数据输入输出	4
5.1.7 密钥管理	4
5.1.8 轮廓管理	5
5.1.9 证书管理	6
5.1.10 配置管理	7
5.1.11 分发和操作	7
5.1.12 开发	7
5.1.13 指导性文档	8
5.1.14 生命周期支持	8
5.1.15 测试	8
5.2 第二级	8
5.2.1 概述	8
5.2.2 物理安全	8
5.2.3 角色与责任	8
5.2.4 访问控制	9
5.2.5 标识与鉴别	10
5.2.6 审计	11
5.2.7 数据输入输出	12
5.2.8 备份与恢复	12
5.2.9 密钥管理	13
5.2.10 轮廓管理	14
5.2.11 证书管理	15
5.2.12 配置管理	16
5.2.13 分发和操作	16
5.2.14 开发	16

5.2.15	指导性文档	17
5.2.16	生命周期支持	17
5.2.17	测试	17
5.2.18	脆弱性评定	17
5.3	第三级	17
5.3.1	概述	17
5.3.2	物理安全	18
5.3.3	角色与责任	18
5.3.4	访问控制	19
5.3.5	标识与鉴别	20
5.3.6	审计	21
5.3.7	数据输入输出	23
5.3.8	备份与恢复	23
5.3.9	密钥管理	24
5.3.10	轮廓管理	27
5.3.11	证书管理	28
5.3.12	配置管理	29
5.3.13	分发和操作	30
5.3.14	开发	31
5.3.15	指导性文档	31
5.3.16	生命周期支持	32
5.3.17	测试	32
5.3.18	脆弱性评定	32
5.4	第四级	32
5.4.1	概述	32
5.4.2	物理安全	32
5.4.3	角色与责任	33
5.4.4	访问控制	33
5.4.5	标识与鉴别	35
5.4.6	审计	36
5.4.7	数据输入输出	38
5.4.8	备份与恢复	38
5.4.9	密钥管理	39
5.4.10	轮廓管理	43
5.4.11	证书管理	44
5.4.12	配置管理	45
5.4.13	分发和操作	45
5.4.14	开发	46
5.4.15	指导性文档	46
5.4.16	生命周期支持	47
5.4.17	测试	47
5.4.18	脆弱性评定	47

5.5 第五级	48
5.5.1 概述	48
5.5.2 物理安全	48
5.5.3 角色与责任	48
5.5.4 访问控制	49
5.5.5 标识与鉴别	51
5.5.6 审计	52
5.5.7 数据输入输出	53
5.5.8 备份与恢复	54
5.5.9 密钥管理	54
5.5.10 轮廓管理	58
5.5.11 证书管理	59
5.5.12 配置管理	60
5.5.13 分发和操作	61
5.5.14 开发	62
5.5.15 指导性文档	62
5.5.16 生命周期支持	63
5.5.17 测试	63
5.5.18 脆弱性评定	63
附录 A (规范性附录) 安全要素要求级别划分	64
参考文献	65

前 言

本标准的附录 A 为规范性附录。

本标准由公安部公共信息网络安全监察局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：中国科学院研究生院信息安全国家重点实验室。

本标准主要起草人：冯登国、张凡、张立武、路晓明、庄涌。

引 言

公开密钥基础设施是集机构、系统(硬件和软件)、人员、程序、策略和协议为一体,利用公钥概念和技术来实施和提供安全服务的、具有普适性的安全基础设施。PKI 系统是通过颁发与管理公钥证书的方式为终端用户提供服务的系统,包括 CA、RA、资料库等基本逻辑部件和密钥托管、OCSP 等可选服务部件以及所依赖的运行环境。

《PKI 系统安全等级保护技术要求》按五级划分的原则,制定 PKI 系统安全等级保护技术要求,详细说明了 PKI 系统五个安全保护等级应采取的安全技术要求,以及为确保这些安全技术所实现的安全功能能够达到其应具有的安全性而采取的保证措施,从技术要求方面进行详细描述,即主要说明为实现每一个保护等级的评估要素应采取的安全技术措施,以及各安全技术要求在不同安全级中具体实现上的差异。第一级为最低级别,第五级为最高级别,随着等级的提高,PKI 系统安全等级保护的要求也随之递增。正文中字体加粗的内容为本级新增部分的要求。

信息安全技术

公钥基础设施安全技术要求

1 范围

本标准参照 GB 17859—1999 的五个安全保护等级的划分,对 PKI 系统安全保护进行等级划分,规定了不同等级 PKI 系统所需要的安全技术要求。

本标准适用于 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。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 19713—2005 信息技术 安全技术 公钥基础设施 在线证书状态协议

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB/T 20518—2006 信息安全技术 公钥基础设施 数字证书格式

3 术语和定义

下列术语和定义适用于本标准。

3.1

公开密钥基础设施 public key infrastructure

公开密钥基础设施是支持公钥管理体制的基础设施,提供鉴别、加密、完整性和不可否认性服务。

3.2

PKI 系统 PKI system

PKI 系统是通过颁发与管理公钥证书的方式为终端用户提供服务的系统,包括 CA、RA、资料库等基本逻辑部件和密钥托管、OCSP 等可选服务部件以及所依赖的运行环境。

3.3

安全策略 security policy

一系列安全规则的准确规定,包括从本文档中衍生出的规则和供应商添加的规则。

3.4

分割知识 split knowledge

两个或两个以上实体分别保存密钥的一部分,密钥的每个部分都不应泄露密钥的明文有效信息,而当这些部分在加密模块中合在一起时可以得到密钥的全部信息,这种方法就叫分割知识。

3.5

分割知识程序 split knowledge procedure

用来实现分割知识的程序。

3.6

保护轮廓 protection profile

一系列满足特定用户需求的、为一类评估对象独立实现的安全要求。