ICS 35.040
L 80

中华人民共和国国家标准

GB/T 21053—2007

信息安全技术　公钥基础设施 PKI系统安全等级保护技术要求

Information security techniques—Public key infrastructure—Technology requirement for security classification protection of PKI system

2007-08-23 发布　　2008-01-01 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

目　　次

前　言

本标准的附录 A 为规范性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：中国科学院软件研究所、中国电子技术标准化研究所。

本标准主要起草人：张凡、冯登国、张立武、路晓明、庄涌、王延鸣。

引　言

公开密钥基础设施(PKI)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 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,详细说明了为实现 GB/T 21054—2007 所提出的 PKI 系统五个安全保护等级应采取的安全技术要求,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,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。正文中字体为黑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
PKI 系统安全等级保护技术要求

1　范围

本标准依据 GB/T 21054—2007 的五个安全保护等级的划分，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/T 19713—2005　信息安全技术　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

GB/T 21054—2007　信息安全技术　公钥基础设施　PKI 系统安全等级保护评估准则

GB/T 21052—2007　信息安全技术　信息系统物理安全技术要求

GB/T 20984—2007　信息安全技术　信息安全风险评估规范

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；PKI

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

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 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，包括从本标准中派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。