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

中 华 人 民 共 和 国
国 家 标 准
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
GB/T 21053—2007
*
中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
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 4.5 字数 128 千字
2008 年 1 月第一版 2008 年 1 月第一次印刷
*
书号:155066·1-30419 定价 44.00 元

GB/T 21053-2007

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。

目　次

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。

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。

3.7

关键性扩展 critical extension

证书或 CRL 中一定能够被识别的扩展项，若不能识别，该证书或 CRL 就无法被使用。

3.8

审计踪迹 audit trail

记录一系列审计信息和事件的日志。

3.9

系统用户 system.user

对 PKI 系统进行管理、操作、审计、备份、恢复的工作人员，系统用户一般在 PKI 系统中被赋予了指定的角色。

3.10

终端用户 terminate user

使用 PKI 系统所提供服务的远程普通用户。

4 缩略语

以下缩略语适用于本标准：

CA	认证机构 Certification Authority
CPS	认证惯例陈述 Certification Practice Statement
CRL	证书撤销列表 Certificate Revocation List
OCSP	在线证书状态协议 Online Certificate Status Protocol
PP	保护轮廓 Protection Profile
RA	注册机构 Registration Authority
TOE	评估对象 Target Of Evaluation
TSF	TOE 安全功能 TOE Security Function

5 安全等级保护技术要求

5.1 第一级

5.1.1 概述

第一级的 PKI 系统，由用户自主保护，所保护的资产价值很低，面临的安全威胁很小，适用于安全要求非常低的企业级 PKI 系统。PKI 系统面临的风险，应按照 GB/T 20984—2007 进行评估。结构设计上，PKI 系统的 CA、RA、证书资料库可不进行明确的分化，所有功能软件模块可全部安装在同一台计算机系统上。第一级 PKI 系统的安全要素要求列表见附录 A。

5.1.2 物理安全

进行 PKI 系统硬件设备、相关环境和系统安全的设计时，应按照 GB/T 21052—2007 第 4 章所描述的要求。

5.1.3 角色与责任

开发者应提供 PKI 系统管理员和操作员的角色定义。

管理员角色负责：安装、配置、维护系统；建立和管理用户账户；配置轮廓；生成部件密钥。

操作员角色负责：签发和撤销证书。

角色的安全功能管理应按表 1 中的配置对授权的角色修改安全功能的能力进行限制。

表 1　授权的角色对于安全功能的管理

功　能	授权角色
证书注册	验证证书字段或扩展字段内容正确性的权限应授权给操作员； 若使用自动过程验证证书字段和扩展字段，那么，配置自动过程的权限应授权给操作员。
数据输入和输出	私钥输出应由管理员执行。
证书状态变更的许可	只有操作员可以配置用于撤销证书的自动过程和相关信息； 只有操作员可以配置用于证书挂起的自动过程和相关信息。
PKI 系统配置	对于 PKI 系统功能的任何配置权应仅授予管理员。（除了在本标准中其他地方所定义的分配给其他角色的 TSF 功能，这一要求应用于所有的配置变量。）
证书轮廓管理	更改证书轮廓的权限应仅授予管理员。
撤销轮廓管理	更改撤销轮廓的权限应仅授予管理员。
证书撤销列表轮廓管理	更改证书撤销列表轮廓的权限应仅授予管理员。
在线证书状态查询轮廓管理	更改在线证书状态查询轮廓的权限应仅授予管理员。

5.1.4　访问控制

5.1.4.1　系统用户访问控制

PKI 系统文档中，应有访问控制的相关文档，访问控制文档中的访问控制策略应包含如下几个方面：

a）　角色及其相应的访问权限

角色及其相应的访问权限的分配见表 2。

表 2　角色及其相应的访问权限

功　能	事　件
证书请求数据的远程和本地输入	证书请求数据的输入操作应仅由操作员和申请证书的主体所完成。
证书撤销请求数据的远程和本地输入	证书撤销请求数据的输入操作应仅由操作员和申请撤销证书的主体所完成。
数据输出	仅系统用户可以请求导出关键和安全相关数据。
密钥生成	仅管理员可以请求生成部件密钥（在多次连接或消息中用于保护数据）。
私钥载入	仅管理员可以请求向加密模块载入部件私钥。
私钥存储	仅操作员可以提出对证书私钥解密的请求； PKI 系统安全功能不应提供解密证书私钥以用来进行数字签名的能力。
可信公钥的输入、删除和存储	仅管理员有权更改（增加、修改、删除）信任公钥。
对称密钥存储	仅管理员有权产生将 PKI 系统对称密钥载入加密模块请求。
私钥和对称密钥销毁	仅管理员有权将 PKI 系统的私钥和对称密钥销毁。
私钥和对称密钥的输出	仅管理员有权输出部件私钥； 仅操作员有权输出证书私钥。
证书状态更改许可	仅操作员和证书主体有权申请使证书进入挂起状态； 仅操作员有权解除证书的挂起状态； 仅操作员有权批准证书进入挂起状态； 仅操作员和证书主体有权申请撤销证书； 仅操作员有权批准撤销证书和所有被撤销信息。

b) 标识与鉴别系统用户的过程

应符合 5.1.5 的要求。

c) 角色的职能分割

应符合 5.1.3 的要求。

5.1.4.2 网络访问控制

进行远程访问时，PKI 系统应提供访问控制。远程用户只有被认证通过后，PKI 系统才允许访问，并只对授权用户提供被授权使用的服务。远程计算机系统与 PKI 系统的连接应被认证，认证方法包括计算机地址、访问时间、拥有的密钥等。PKI 系统应定义网络访问控制策略。

5.1.5 标识与鉴别

标识与鉴别包括建立每一个用户所声称的身份，和验证每一个用户确实是他所声称的用户。确保用户与正确的安全属性相关联。

5.1.5.1 用户属性定义

PKI 系统应维护每个用户的安全属性。

安全属性包括但不限于身份、组、角色、许可、安全和完整性等级。

5.1.5.2 用户鉴别

PKI 系统的安全功能应预先设定 PKI 系统代表用户执行的、与安全功能无关的动作，在用户身份被鉴别之前，允许 PKI 系统执行这些预设动作，包括：

a) 响应查询公开信息(如：在线证书状态查询等)；

b) 接收用户发来的数据，但直到系统用户批准之后才处理。

管理员应对鉴别数据进行管理。

PKI 系统应定义所支持的用户鉴别机制的类型。

5.1.5.3 用户标识

PKI 系统的安全功能应预先设定 PKI 系统代表用户执行的、与安全功能无关的动作，在标识用户身份之前，允许 PKI 系统执行这些预设动作，包括：

a) 响应查询公开信息(如：在线证书状态查询等)；

b) 接收用户发来的数据，但直到系统用户批准之后才处理。

5.1.5.4 用户主体绑定

在 PKI 系统安全功能控制范围之内，对一个已标识与鉴别的用户，为了完成某个任务，需要激活另一个主体，这时，应通过用户主体绑定将该用户与该主体相关联，从而将用户的身份与该用户的所有可审计行为相关联，使用户对自己的行为负责。

5.1.6 数据输入输出

5.1.6.1 TSF 间用户数据传送的保密性

当用户数据通过外部信道在 PKI 系统之间或 PKI 系统用户之间传递时，PKI 系统应执行访问控制策略，使得能以某种防止未授权泄露的方式传送用户数据。

5.1.6.2 输出 TSF 数据的保密性

在 TSF 数据从 TSF 到远程可信 IT 产品的传送过程中，应保护机密数据不被未授权泄露。

这些机密数据可以是 TSF 的关键数据，如口令、密钥、审计数据或 TSF 的可执行代码。

5.1.7 密钥管理

5.1.7.1 密钥生成

5.1.7.1.1 PKI 系统密钥生成

系统用户密钥生成应由相应级别的 CA 或 RA 等机构进行，可用软件方法产生，生成算法和密钥长度等应符合国家密码行政管理部门的规定。在进行密钥生成时，PKI 系统应限制非授权人员的参与。

CA 签名公私钥对应采用国家密码行政管理部门认可的方法生成，可用软件方法或硬件密码设备

产生。在密钥生成时应检查用户角色，并设置为只有管理员才能启动 CA 密钥生成过程。

5.1.7.1.2 终端用户密钥生成

终端用户的密钥可由用户自己生成，也可委托 CA、RA 等 PKI 系统的服务机构生成。

终端用户密钥可用软件方法产生，生成算法和密钥长度等应符合国家密码行政管理部门的规定。

5.1.7.2 密钥传送与分发

5.1.7.2.1 PKI 系统密钥传送与分发

系统用户密钥的传送与分发应以加密形式直接发送到系统用户证书载体中，加密算法等应符合国家密码行政管理部门的规定。

CA 公钥分发方法应适当、切实可行，如提供根证书和 CA 证书下载、或与终端用户证书一起下载等，应符合国家密码行政管理部门对密钥分发的相关规定。

5.1.7.2.2 终端用户密钥传送与分发

如果终端用户自己生成密钥对，把公钥传送给 CA 是证书注册过程的一部分。终端用户应将公钥安全地提交给 CA，如使用证书载体等方法进行面对面传送。

如果终端用户委托 CA 生成密钥对，则不需要签发前的终端用户公钥传送。CA 向用户传送与分发私钥应以加密形式进行，加密算法等应符合国家密码行政管理部门的规定。

5.1.7.3 密钥存储

系统用户密钥可用软件加密的形式存储，加密算法应符合国家密码行政管理部门的规定。

CA 签名私钥应存储于国家密码行政管理部门规定的密码模块中或由硬件密码设备加密后存储。

终端用户密钥由用户自行存储。

5.1.8 轮廓管理

5.1.8.1 证书轮廓管理

证书轮廓定义证书中的字段和扩展可能的值，这些字段和扩展应与 GB/T 20518—2006 相一致。证书轮廓包括的信息有：

a) 与密钥绑定的用户的标识符；
b) 主体的公私密钥对可使用的加密算法；
c) 证书发布者的标识符；
d) 证书有效时间的限定；
e) 证书包括的附加信息；
f) 证书的主体是否是 CA；
g) 与证书相对应的私钥可执行的操作；
h) 证书发布所使用的策略。

PKI 系统应具备证书轮廓，并保证发布的证书与证书轮廓中的描述一致。PKI 系统管理员应为以下字段和扩展指定可能的值：

a) 密钥所有者的标识符；
b) 公私密钥对主体的算法标识符；
c) 证书发布者的标识符；
d) 证书的有效期。

5.1.8.2 证书撤销列表轮廓管理

证书撤销列表轮廓用于定义 CRL 中字段和扩展中可接受的值，这些字段和扩展应与 GB/T 20518—2006 相一致。CRL 轮廓可能要定义的值包括：

a) CRL 可能或者必须包括的扩展和每一扩展的可能的值；
b) CRL 的发布者；
c) CRL 的下次更新日期。

若 PKI 系统发布 CRL，则应具备证书撤销列表轮廓，并保证发布的 CRL 与该轮廓中的规定相一致。PKI 系统管理员应规定以下字段和扩展的可能的取值：

a) issuer；

b) issuerAltName。

5.1.8.3 在线证书状态协议轮廓管理

在线证书状态协议轮廓用于定义一系列在 OCSP 响应中可接受的值。OCSP 轮廓应规定 PKI 系统可能产生的 OCSP 响应的类型和这些类型可接受的值。

a) 若 PKI 系统发布 OCSP 响应，PKI 系统应具备 OCSP 轮廓并保证 OCSP 响应与轮廓一致；

b) 若 PKI 系统发布 OCSP 响应，PKI 系统应要求管理员为 responseType 字段指定可接受的值；

c) 若 PKI 系统允许使用基本响应类型(basic response type)的 OCSP 响应，则 PKI 系统管理员应为 ResponderID 指定可接受的值。

5.1.9 证书管理

5.1.9.1 证书注册

PKI 系统所签发的公钥证书应与 GB/T 20518—2006 相一致。任何证书所包含的字段或扩展应被 PKI 系统根据 GB/T 20518—2006 生成或经由颁发机构验证以保证其与标准的一致性。

输入证书字段和扩展中的数据应被批准。证书字段或扩展的值可有以下 4 种方式获得批准：

a) 数据被操作员手工批准；

b) 自动过程检查和批准数据；

c) 字段或扩展的值由 PKI 系统自动生成；

d) 字段或扩展的值从证书轮廓中获得。

进行证书生成时：

a) 应仅产生与 GB/T 20518—2006 中规定的证书格式相同的证书；

b) 应仅生成与现行证书轮廓中定义相符的证书；

c) PKI 系统应验证预期的证书主体拥有与证书中包含的公钥相对应的私钥，除非公私密钥对是由 PKI 系统所产生的；

d) PKI 系统应保证：

1) version 字段应为 0，1，2；

2) 若包含 issuerUniqueID 或 subjectUniqueID 字段，则 version 字段应为 1 或 2；

3) 若证书包含 extensions，那么 version 字段应为 2；

4) serialNumber 字段对 CA 应是唯一的；

5) validity 字段应说明不早于当时时间的 notBefore 值和不早于 notBefore 时间的 notAfter 值；

6) 若 issuer 字段为空，证书应包括一个 issuerAltName 的关键性扩展；

7) 若 subject 字段为空，证书应包括一个 subjectAltName 的关键性扩展；

8) subjectPublicKeyInfo 字段中的 signature 字段和 algorithm 字段应包含国家密码行政管理部门许可的或推荐的算法的 OID。

5.1.9.2 证书撤销

5.1.9.2.1 证书撤销列表审核

发布 CRL 的 PKI 系统应验证所有强制性字段的值符合 GB/T 20518—2006。至少以下字段应被审核：

a) 若包含 version 字段，应为 1；

b) 若 CRL 包含关键性的扩展，version 字段应出现且为 1；

c) 若 issuer 字段为空，CRL 应包含一个 issuerAltName 的关键性扩展；

d) signature 和 signatureAlgorithm 字段应为许可的数字签名算法的 OID；

e) thisUpdate 应包含本次 CRL 的发布时间；

f) nextUpdate 字段的时间不应早于 thisUpdate 字段的时间。

5.1.9.2.2 OCSP 基本响应的审核

发布 OCSP 响应的 PKI 系统应验证所有强制性字段的值符合 GB/T 19713—2005。至少应审核以下字段：

a) version 字段应为 0；

b) 若 issuer 字段为空，响应中应包含一个 issuerAltName 的关键性扩展；

c) signatureAlgorithm 字段应为许可的数字签名算法的 OID；

d) thisUpdate 字段应指出证书状态正确的时间；

e) producedAt 字段应指出 OCSP 响应者发出响应的时间；

f) nextUpdate 字段的时间不应早于 thisUpdate 字段的时间。

5.1.10 配置管理

应按 GB/T 20271—2006 中 6.1.5.1 的要求，在配置管理能力方面实现对版本号等方面的要求。

5.1.11 分发和操作

应按 GB/T 20271—2006 中 6.1.5.2 的要求，从以下方面实现 PKI 系统的分发和操作：

a) 以文档形式提供对 PKI 系统安全地进行分发的过程，并对安装、生成和启动的过程进行说明，最终生成安全的配置。文档中所描述的内容应包括：

1) 提供分发的过程；

2) 安全启动和操作的过程。

b) 对系统的未授权修改的风险，应在交付时控制到最低限度。在包装及安全分送和安装过程中，这种控制应采取软件控制系统的方式，确认安全性会由最终用户考虑，所有安全机制都应以功能状态交付。

c) 所有软件应提供安全安装默认值，在客户不做选择时，默认值应使安全机制有效地发挥作用。

d) 随同系统交付的全部默认用户标识码，应在交付时处于非激活状态，并在使用前由管理员激活。

e) 指导性文档应同交付的系统软件一起包装，并应有一套规程确保当前送给用户的系统软件是严格按最新的系统版本来制作的。

5.1.12 开发

应按 GB/T 20271—2006 中 6.1.5.3 的要求，从以下方面进行 PKI 系统的开发：

a) 按非形式化功能说明、描述性高层设计、TSF 子集实现、TSF 内部结构模块化、描述性低层设计和非形式化对应性说明的要求，进行 PKI 系统的开发；

b) 系统的设计和开发应保护数据的完整性，例如，检查数据更新的规则，返回状态的检查，中间结果的检查，合理值输入检查等；

c) 在内部代码检查时，应解决潜在的安全缺陷，关闭或取消所有的后门；

d) 所有交付的软件和文档，应进行关于安全缺陷的定期的和书面的检查，并将检查结果告知客户；

e) 系统控制数据，如口令和密钥，不应在未受保护的程序或文档中以明文形式储存，并以书面形式向客户提供关于软件所有权法律保护的指南。

5.1.13 指导性文档

应按 GB/T 20271—2006 中 6.1.5.4 的要求，从以下方面编制 PKI 系统的指导性文档：

a) 终端用户文档应提供关于不同用户的可见的安全机制以及如何利用它们的信息，描述没有明示用户的保护结构，并解释它们的用途和提供有关它们使用的指南；

b) 系统用户文档应提供有关如何设置、维护和分析系统安全的详细指导，包括当运行一个安全

设备时，需要控制的有关功能和特权的警告，以及与安全有关的管理员功能的详细描述，包括增加和删除一个用户、改变用户的安全特征等；

c) 文档中不应提供任何一旦泄露将会危及系统安全的信息。有关安全的指令和文档应划分等级分别提供给终端用户和系统用户。这些文档应为独立的文档，或作为独立的章节插入到终端用户指南和系统用户指南中。文档也可为硬拷贝、电子文档或联机文档。如果是联机文档，应控制对其的访问。

5.1.14 生命周期支持

应按 GB/T 20271—2006 中 6.1.5.5 的要求，从以下方面实现 PKI 系统的生命周期支持：

a) 按开发者定义生命周期模型进行开发；

b) 操作文档应详细阐述安全启动和操作的过程，详细说明安全功能在启动、正常操作维护时是否能被撤销或修改，说明在故障或系统出错时如何恢复系统至安全状态。

5.1.15 测试

应按 GB/T 20271—2006 中 6.1.5.6 的要求，从以下方面对 PKI 系统进行测试：

a) 应通过一般功能测试和相符性独立测试，确认 PKI 系统的功能与所要求的功能相一致。

b) 所有系统的安全特性，应被全面测试。所有发现的漏洞应被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

c) 应提供测试文档，详细描述测试计划、测试过程、测试结果。

5.2 第二级

5.2.1 概述

第二级的 PKI 系统，应提供审计能力，所保护的资产价值低，面临的安全威胁小，适用于安全要求较高的企业级 PKI 系统。PKI 系统面临的风险，应按照 GB/T 20984—2007 进行评估。结构设计上，PKI 系统的 CA、RA 可不进行明确的分化，但证书资料库应独立设计。RA 可全部由 CA 托管，软件功能模块可安装在同一台计算机系统上，而数据库系统应有独立的计算环境。第二级 PKI 系统的安全要素要求列表见附录 A。

5.2.2 物理安全

进行 PKI 系统硬件设备、相关环境和系统安全的设计时，应按照 GB/T 21052—2007 第 5 章所描述的要求。

5.2.3 角色与责任

开发者应提供 PKI 系统管理员和操作员的角色定义。

管理员：安装、配置、维护系统；建立和管理用户账户；配置轮廓和审计参数；生成部件密钥；查看和维护审计日志；执行系统的备份和恢复。本级的 PKI 系统要求提供审计和系统备份功能，管理员的职责也相应地多分配审计和系统备份权限。

操作员：签发和撤销证书。

系统应具备使主体与角色相关联的能力，并保证一个身份不应同时具备多个角色的权限。一个人不应同时拥有多个角色，开发者应在系统设计时对角色的管理进行相关限制。

角色的安全功能管理应按表 3 中的配置对授权的角色修改安全功能的能力进行限制。

表 3 授权的角色对于安全功能的管理

功 能	授权角色
安全审计	配置审计参数的权限应仅授予管理员； 变更审计日志签名时间间隔的权限应仅授予管理员。
备份与恢复	配置备份参数的权限应仅授予管理员； 初始化备份或恢复功能的权限应仅授予管理员。

表 3(续)

功　能	授权角色
证书注册	验证证书字段或扩展字段内容正确性的权限应授权给操作员。 若使用自动过程验证证书字段和扩展字段，那么，配置自动过程的权限应授权给操作员。
数据输入和输出	私钥输出应由管理员执行。
证书状态变更的许可	只有操作员可配置用于撤销证书的自动过程和相关信息； 只有操作员可配置用于证书挂起的自动过程和相关信息。
PKI 系统配置	对于 PKI 系统功能的任何配置权应仅授予管理员。(除了在本标准中其他地方所定义的分配给其他角色的 TSF 功能，这一要求应用于所有的配置变量。)
证书轮廓管理	更改证书轮廓的权限应仅授予管理员。
撤销轮廓管理	更改撤销轮廓的权限应仅授予管理员。
证书撤销列表轮廓管理	更改证书撤销列表轮廓的权限应仅授予管理员。
在线证书状态查询轮廓管理	更改在线证书状态查询轮廓的权限应仅授予管理员。

5.2.4　访问控制

5.2.4.1　系统用户访问控制

注册和注销能够访问 PKI 系统信息和服务的用户应按正规的程序执行。分配或者使用系统特权时，应进行严格的限制和控制。进行口令分配时，应通过正规的程序控制。选取和使用口令时系统用户应按已定义的策略和程序进行。系统用户账号和终端用户账号应严格分类管理。

PKI 系统文档中，应有访问控制的相关文档，访问控制文档中的访问控制策略应包含如下几个方面：

a)　角色及其相应的访问权限

角色及其相应的访问权限的分配见表 4。

表 4　角色及其相应的访问权限

功　能	事　件
证书请求数据的远程和本地输入	证书请求数据的输入操作应仅由操作员和申请证书的主体所完成。
证书撤销请求数据的远程和本地输入	证书撤销请求数据的输入操作应仅由操作员和申请撤销证书的主体所完成。
数据输出	仅系统用户可以请求导出关键和安全相关数据。
密钥生成	仅管理员可以请求生成部件密钥(在多次连接或消息中用于保护数据)。
私钥载入	仅管理员可以请求向加密模块载入部件私钥。
私钥存储	仅操作员可以提出对证书私钥解密的请求； PKI 系统安全功能不应提供解密证书私钥以用来进行数字签名的能力。
可信公钥的输入、删除和存储	仅管理员有权更改(增加、修改、删除)信任公钥。
对称密钥存储	仅管理员有权产生将 PKI 系统对称密钥载入加密模块请求。
私钥和对称密钥销毁	仅管理员有权将 PKI 系统的私钥和对称密钥销毁。
私钥和对称密钥的输出	仅管理员有权输出部件私钥； 仅操作员有权输出证书私钥。

表 4(续)

功　能	事　件
证书状态更改许可	仅操作员和证书主体有权申请使证书进入挂起状态； 仅操作员有权解除证书的挂起状态； 仅操作员有权批准证书进入挂起状态； 仅操作员和证书主体有权申请撤销证书； 仅操作员有权批准撤销证书和所有被撤销信息。

b)　标志和鉴别系统用户过程

应符合 5.2.5 的要求。

c)　角色的职能分割

应符合 5.2.3 的要求。

5.2.4.2　网络访问控制

进行远程访问时，PKI 系统应提供访问控制。远程用户只有被认证通过后，PKI 系统才允许访问，并只对授权用户提供被授权使用的服务。**系统开发者应提供对远程用户终端到 PKI 系统服务的路径进行控制的方法，并采取防火墙、入侵检测等安全保护措施。**对远程计算机系统与 PKI 系统的连接应被认证，认证方法包括计算机地址、访问时间、拥有的密钥等。PKI 系统应定义网络访问控制策略。**PKI 系统的诊断分析端口是重要的受控访问端口，开发者应对其访问进行严格的安全控制，能够检测并记录对这些端口的访问请求。**

5.2.4.3　操作系统访问控制

每个用户只有唯一的 ID，以便在 PKI 系统的操作能够被记录追踪。

当系统用户正在访问 PKI 服务系统，中途长期离开用户终端时，PKI 系统应能检测出这些终端经过了指定时间的不活动状态，并自动进入保护状态，采取锁屏、断开连接等措施，防止未授权用户访问。对高风险的应用应限制连接次数以提供额外的保护，对短时间内超过限制次数以上的连接应进行可配置的操作并记录。

5.2.5　标识与鉴别

标识与鉴别包括建立每一个用户所声称的身份，和验证每一个用户确实是他所声称的用户。确保用户与正确的安全属性相关联。

5.2.5.1　用户属性定义

PKI 系统应维护每个用户的安全属性。

安全属性包括但不限于身份、组、角色、许可、安全和完整性等级。

5.2.5.2　用户鉴别

PKI 系统的安全功能应预先设定 PKI 系统代表用户执行的、与安全功能无关的动作，在用户身份被鉴别之前，允许 PKI 系统执行这些预设动作，包括：

a)　响应查询公开信息(如：在线证书状态查询等)；

b)　接收用户发来的数据，但直到系统用户批准之后才处理。

管理员应对鉴别数据进行管理。

PKI 系统应定义所支持的用户鉴别机制的类型。

5.2.5.3　用户标识

PKI 系统的安全功能应预先设定 PKI 系统代表用户执行的、与安全功能无关的动作，在用户被标识之前，允许 PKI 系统执行这些预设动作，包括：

a)　响应查询公开信息(如：在线证书状态查询等)；

b)　接收用户发来的数据，但直到系统用户批准之后才处理。