ICS 35.020
L 80

中华人民共和国国家标准

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

Information security techniques—Public key infrastructure—Evaluation criteria 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 系统安全等级保护评估准则》按五级划分的原则,制定 PKI 系统安全等级保护评估准则,详细说明了参照 GB 17859 所提出的安全等级保护对 PKI 系统的评估要素。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评估要素也随之递增。正文中字体为黑体加粗的内容为本级新增部分的要求。本标准用以指导评估者如何对 PKI 系统的安全保护等级进行评估,主要从对 PKI 系统的安全保护等级进行划分的角度来说明其评估内容。评估者可以根据各级别的具体要求,对评估对象进行评估,确定评估对象的安全保护级别。对于实现本标准中规定的评估内容的安全技术与采取的安全保证措施,应参照 GB/T 21053—2007 中的规定进行设计和开发。

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

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 系统所需要满足的评估内容。

本标准适用于 PKI 系统的安全保护等级的评估，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 20518—2006　信息安全技术　公钥基础设施　数字证书格式

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

GB/T 21052—2007　信息安全技术　信息系统物理安全技术要求

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

安全级别　security level

分层的安全等级与表示对象的敏感度或个人的安全许可的安全种类的组合。

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

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。

3.7

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

以下缩略语在本标准各部分通用：

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
SF	安全功能 Security Function
ST	安全目标 Security Target
TOE	评估对象 Target of Evaluation
TSF	TOE 安全功能 TOE Security Function

5　评估内容

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。结构上，PKI 系统的 CA、RA、证书资料库可没有明确的分化。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

应按照 GB/T 21052—2007 第 4 章所描述的要求，对 PKI 系统硬件及相关环境进行评估。

5.1.3　角色与责任

PKI 系统应对系统用户提供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。

系统用户应按照角色的安全功能管理进行权限限制。

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；

b)　标识与鉴别系统用户的过程；

c)　角色的职能分割。

5.1.4.2　网络访问控制

用户可以且只能直接访问被授权使用的服务。远程用户只有被认证后，PKI 系统才允许访问。连接到远程计算机系统应被认证。

5.1.5 标识与鉴别

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。

5.1.5.2 用户鉴别

在用户身份被鉴别之前，PKI 系统可执行与安全功能无关的动作。在执行其他的安全功能引起的动作之前，用户应成功鉴别自己。

5.1.5.3 用户标识

在用户标识自己身份之前，PKI 系统可代表用户执行与安全功能无关的动作。用户在成功标识自己之后，才能执行其他的安全功能引起的操作动作。

5.1.5.4 用户主体绑定

PKI 系统应通过用户主体绑定建立和维护用户与用户主体之间的关联，使用户的身份与该用户的所有可审计行为相关联。

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。

5.1.7 密钥管理

5.1.7.1 密钥生成

PKI 系统的系统用户密钥应由相应级别的 CA 或 RA 等机构生成。在密钥生成时应采取安全控制。

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。在密钥生成时应采取安全控制，只有管理员才能启动 CA 密钥生成过程。

终端用户密钥可由用户生成，也可委托 CA、RA 等 PKI 系统的服务机构生成。生成方法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

PKI 系统的系统用户密钥的传送与分发应当以加密形式安全进行。CA 公钥分发方法应当切实可行。

如果终端用户自己生成密钥对，终端用户应将公钥安全地提交给 PKI 系统。

如果终端用户委托 CA 生成密钥对，那么不需要签发前的公钥传送，CA 向用户传送与分发私钥应当以加密形式安全进行。

5.1.7.3 密钥存储

PKI 系统的系统用户密钥与 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以加密的形式存储，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

PKI 系统应具备证书轮廓，并保证发行的证书与证书轮廓中的描述一致。

5.1.8.2 证书撤销列表轮廓管理

若 PKI 系统发布 CRL，TSF 应具备证书撤销列表轮廓，并保证发行的 CRL 与该轮廓中的规定相一致。

5.1.8.3 在线证书状态协议轮廓管理

OCSP 轮廓应规定 PKI 系统可能产生的字段类型和字段类型可接受的变量值。

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由 PKI 系统根据 GB/T 20518—2006 生成，或经由证书颁发机构验证以保证其与标准的一致性。

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) 评估者应检查 PKI 系统产生的证书是否满足实际要求。

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。

5.1.9.2.2 OCSP 基本回应的审核

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。

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。结构上，PKI 系统的 CA、RA 可不进行明确的分化，证书资料库应独立设计。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

应按照 GB/T 21052—2005 第 5 章所描述的要求，对 PKI 系统硬件及相关环境进行评估。

5.2.3 角色与责任

PKI 系统应对系统用户提供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。

操作员角色：负责签发和撤销证书。

系统用户应按照角色的安全功能管理进行权限限制。

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。

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照已定义的策略和程序进行。

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；

b) 标识与鉴别系统用户的过程；

c) 角色的职能分割。

5.2.4.2 网络访问控制

用户可以且只能直接访问被授权使用的服务。用户终端到 PKI 系统服务的路径应是受控的。远程用户只有被认证后，PKI 系统才允许访问。连接到远程计算机系统应被认证。对 PKI 系统诊断分析端口的访问应进行安全控制。

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。

经过指定时间的不活动状态，正在访问 PKI 服务系统的终端应超时进入保护状态，以防未授权用户访问。对高风险的应用应限制连接次数以提供额外的保护。

5.2.5 标识与鉴别

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。

5.2.5.2 用户鉴别

在用户身份被鉴别之前，PKI 系统可执行与安全功能无关的动作。在执行其他的安全功能引起的动作之前，用户应成功鉴别自己。

5.2.5.3 用户标识

在用户标识自己身份之前，PKI 系统可代表用户执行与安全功能无关的动作。用户在成功标识自己之后，才能执行其他的安全功能引起的操作动作。

5.2.5.4 用户主体绑定

PKI 系统应通过用户主体绑定建立和维护用户与用户主体之间的关联，使用户的身份与该用户的所有可审计行为相关联。

5.2.5.5 鉴别失败处理

PKI 系统的安全功能应能检测到与鉴别事件相关的不成功的鉴别尝试。

5.2.6 审计

5.2.6.1 审计数据产生

PKI 系统安全功能应能为系统的可审计事件生成一个审计记录，并在每一个审计记录中记录基本信息。

PKI 系统安全功能应能维护系统的可审计事件。

5.2.6.2 审计查阅

PKI 系统安全功能应为管理员提供从审计记录中读取一定类型的审计信息的能力。

5.2.6.3 选择性审计

审计功能部件应可根据基本属性选择或排除审计事件中的可审计事件。

5.2.6.4 审计事件存储

审计功能部件应能够防止对审计记录的非授权修改，并可检测对审计记录的修改；当审计踪迹存储已满时，审计功能部件应能够阻止除由管理员发起的以外的所有审计事件的发生。

5.2.7 数据输入输出

5.2.7.1 TOE 内部用户数据传送

在 PKI 系统的物理分隔部件间传递用户数据时，PKI 系统应执行访问控制策略，以防止安全相关的用户数据被篡改以及机密性用户数据的泄露。

5.2.7.2 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。

5.2.7.3 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。

5.2.7.4 TOE 内 TSF 数据的传送

PKI 系统应保护安全相关的 TSF 数据在分离的 PKI 部件间传送时不被篡改，保护机密性 TSF 数据在分离的 PKI 部件间传送时不被泄露。

5.2.8 备份与恢复

PKI 系统应具有备份和恢复功能，并可在需要时调用备份功能。在系统备份数据中应保存足够的信息使系统能够重建备份时的系统状态。

5.2.9 密钥管理

5.2.9.1 密钥生成

PKI 系统的部件密钥和系统用户密钥应由相应级别的 CA 或 RA 等机构生成。在密钥生成时应采取安全控制。

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。在密钥生成时应采取安全控制，只有管理员才能启动 CA 密钥生成过程。

终端用户密钥可由用户生成，也可委托 CA、RA 等 PKI 系统的服务机构生成。生成方法应符合国家密码行政管理部门的规定。

5.2.9.2 密钥传送与分发

PKI 系统的**部件密钥**和系统用户密钥的传送与分发应当以加密形式安全进行。CA 公钥分发方法应当切实可行，**并应当保证 CA 公钥的完整性**。

如果终端用户自己生成密钥对，终端用户应将公钥安全地提交给 PKI 系统。

如果终端用户委托 CA 生成密钥对，那么不需要签发前的公钥传送，CA 向用户传送与分发私钥应当以加密形式安全进行。

5.2.9.3 密钥存储

PKI 系统的**部件密钥**、系统用户密钥与 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以加密的形式存储，终端用户密钥由用户自行存储。

5.2.9.4 密钥导入导出

所有密钥导入导出 PKI 系统，应采用国家密码行政管理部门认可的加密算法或加密设备。私钥不应以明文形式导入导出 PKI 系统。PKI 系统应把导入导出的密钥与正确实体相关联，并赋予相应的权限。

5.2.9.5 密钥销毁

PKI 系统应提供销毁明文对称密钥和私有密钥的方法。

5.2.10 轮廓管理

5.2.10.1 证书轮廓管理

5.2.10.1.1 基本证书轮廓管理

PKI 系统应具备证书轮廓，并保证发行的证书与证书轮廓中的描述一致。

5.2.10.1.2 扩展的证书轮廓管理

管理员应为证书扩展指定可能的值。

5.2.10.2 证书撤销列表轮廓管理

5.2.10.2.1 基本证书撤销列表轮廓

若 PKI 系统发布 CRL，TSF 应具备证书撤销列表轮廓，并保证发行的 CRL 与该轮廓中的规定相一致。

5.2.10.2.2 扩展的证书撤销列表轮廓

若 PKI 系统发布 CRL，管理员应指定 CRL 和 CRL 扩展可接受的值。

5.2.10.3 在线证书状态协议轮廓管理

OCSP 轮廓应规定 PKI 系统可能产生的字段类型和字段类型可接受的变量值。

5.2.11 证书管理

5.2.11.1 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由

PKI 系统根据 GB/T 20518—2006 生成，或经由证书颁发机构验证以保证其与标准的一致性。

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) 评估者应检查 PKI 系统产生的证书是否满足实际要求。

5.2.11.2 证书撤销

5.2.11.2.1 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。

5.2.11.2.2 OCSP 基本回应的审核

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。

5.3 第三级

5.3.1 概述

第三级的 PKI 系统，所保护的资产价值较高，面临的安全威胁较大，应提供全面的安全保护。结构上，PKI 系统的 CA、RA、证书资料库应独立设计，并采用双证书（签名证书和加密证书）机制，建设双中心（证书认证中心和密钥管理中心）。第三级 PKI 系统的安全要素要求列表见附录 A。

5.3.2 物理安全

5.3.2.1 核心部件物理安全

应按照 GB/T 21052—2007 第 6 章所描述的要求，对 PKI 系统硬件及相关环境进行评估。

5.3.2.2 RA 物理安全

RA 可有多种建设方式。

RA 应设置专门的区域来接待日常业务。

RA 应妥善保管私钥。

RA 设备应有安全人员和电子监控设备保护防盗。

所有的活动都应被授权人员或安全人员监控。

RA 对外服务的时间应被严格限制。

维修和服务人员在工作区域应受监控。

5.3.3 角色与责任

PKI 系统应对系统用户提供管理员、操作员和审计员的角色定义。

管理员角色：负责安装、配置、维护系统；建立和管理用户账户；配置轮廓和审计参数；生成部件密钥；执行系统的备份和恢复。

操作员角色：负责签发和撤销证书。

审计员角色：负责查看和维护审计日志。

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。

系统用户应按照角色的安全功能管理进行权限限制。

5.3.4 访问控制

5.3.4.1 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。应定期审核系统用户的访问权限。选取和使用口令时系统用户应按照已定义的策略和程序进行。对无人值守的设备应有适当的保护措施。

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；

b) 标识与鉴别系统用户的过程；

c) 角色的职能分割；

d) **进行 PKI 系统的特定操作时需要的最小系统用户人数。**

5.3.4.2 **网络访问控制**

用户可以且只能直接访问被授权使用的服务。用户终端到 PKI 系统服务的路径应是受控的。远程用户只有被认证后，PKI 系统才允许访问。连接到远程计算机系统应被认证。对 PKI 系统诊断分析端口的访问应进行安全控制。**PKI 系统内部网络和外部网络之间应设置安全控制。**

按照 PKI 系统的访问控制策略，应限制用户可用的服务。路由控制应保证计算机连接和信息流不违背系统的访问控制策略。PKI 系统所有网络服务的安全属性要求在 PKI 系统文档中有相关说明。

5.3.4.3 **操作系统访问控制**

PKI 系统的访问应使用安全的登录过程。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。**系统的口令管理应提供工具确保生成高质量的口令。对系统工具的使用应进行严格的控制。**经过指定时间的不活动状态，正在访问 PKI 服务系统的终端应超时进入保护状态，以防未授权用户访问。对高风险的应用应限制连接次数以提供额外的保护。

5.3.4.4 **应用访问控制**

应根据访问控制策略，严格限制对信息和应用系统功能访问。

5.3.5 **标识与鉴别**

5.3.5.1 **用户属性定义**

PKI 系统应维护每个用户的安全属性。

5.3.5.2 **用户鉴别**

在用户身份被鉴别之前，PKI 系统可执行与安全功能无关的动作。在执行其他的安全功能引起的动作之前，用户应成功鉴别自己。

PKI 系统应提供多鉴别机制，对不同身份的用户使用不同的鉴别机制。

当进行鉴别时，PKI 系统的安全功能应避免提供给用户的反馈泄露用户的鉴别数据。

5.3.5.3 **用户标识**

在用户标识自己身份之前，PKI 系统可代表用户执行与安全功能无关的动作。用户在成功标识自己之后，才能执行其他的安全功能引起的操作动作。

5.3.5.4 **用户主体绑定**

PKI 系统应通过用户主体绑定建立和维护用户与用户主体之间的关联，使用户的身份与该用户的所有可审计行为相关联。

5.3.5.5 **鉴别失败处理**

PKI 系统的安全功能应能检测到与鉴别事件相关的不成功的鉴别尝试。

当用户自从上次鉴别成功以来不成功的鉴别尝试的次数达到或超过了定义的界限时，PKI 系统应采取应对措施。

5.3.5.6 **秘密的规范**

当用来对用户身份鉴别的口令、密钥等秘密信息由用户产生时，PKI 系统应对可接受的秘密信息的质量做出要求，并检查。秘密信息质量量度由管理员制定。

当用来对用户身份鉴别的口令、密钥等秘密信息由 PKI 系统产生时，PKI 系统应可生成符合秘密信息质量要求的秘密信息。秘密信息质量量度由管理员制定。

5.3.6 **审计**

5.3.6.1 **审计数据产生**

PKI 系统安全功能应能为系统的可审计事件生成一个审计记录，并在每一个审计记录中至少记录

基本信息。

PKI 系统安全功能应能维护系统的可审计事件。

5.3.6.2 **审计查阅**

PKI 系统安全功能应为审计员提供从审计记录中读取一定类型的审计信息的能力。

5.3.6.3 **选择性审计**

审计功能部件应可根据基本属性选择或排除审计事件中的可审计事件。

5.3.6.4 **审计事件存储**

审计功能部件应能够防止对审计记录的非授权修改，并可检测对审计记录的修改；当审计踪迹存储已满时，**审计功能部件应能够阻止除由审计员发起的以外的所有审计事件的发生。**

5.3.6.5 **审计日志签名**

审计功能部件应定期对审计日志做完整性保护。

对审计日志签名的时间周期应是可配置的。

对审计日志签名的事件应写入审计日志中，签名结果应包含在其中。

5.3.7 **数据输入输出**

5.3.7.1 **TOE 内部用户数据传送**

在 PKI 系统的物理分隔部件间传递用户数据时，PKI 系统应执行访问控制策略，以防止安全相关的用户数据被篡改以及机密性用户数据的泄露。

5.3.7.2 **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。

5.3.7.3 **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。

5.3.7.4 **TOE 内 TSF 数据的传送**

PKI 系统应保护安全相关的 TSF 数据在分离的 PKI 部件间传送时不被篡改，保护机密性 TSF 数据在分离的 PKI 部件间传送时不被泄露。

5.3.7.5 **原发抗抵赖**

PKI 系统在任何时候都应对证书状态信息和其他安全相关信息强制产生原发证据。

PKI 系统应能为所有安全相关的信息提供验证信息原发证据的能力。

5.3.8 **备份与恢复**

PKI 系统应具有备份和恢复功能，并可在需要时调用备份功能。在系统备份数据中应保存足够的信息使系统能够重建备份时的系统状态。**并通过完整性保护措施防止备份数据受到未授权的修改。关键安全参数和其他机密信息应以加密形式存储。**

5.3.9 **密钥管理**

5.3.9.1 **密钥生成**

PKI 系统部件密钥和系统用户密钥应由相应级别的 CA 或 RA 等机构生成。在密钥生成时应采取安全控制。

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。在密钥生成时应采取安全控制，只有管理员才能启动 CA 密钥生成过程，**而且生成过程中应有多个管理员同时在场。**

终端用户密钥可由用户生成，也可委托 CA、RA 等 PKI 系统的服务机构生成。生成方法应符合国家密码行政管理部门的规定。

PKI 系统的文档中应明确规定密钥生成方法。

5.3.9.2 **密钥传送与分发**

PKI 系统的部件密钥和系统用户密钥的传送与分发应当以加密形式安全进行。CA 公钥分发方法

应当切实可行，并应当保证 CA 公钥的完整性。

PKI 系统的文档中应明确说明 CA 公钥分发方法。

如果终端用户自己生成密钥对，终端用户应将公钥安全地提交给 PKI 系统。

如果终端用户委托 CA 生成密钥对，那么不需要签发前的公钥传送，CA 向用户传送与分发私钥应当以加密形式安全进行。

PKI 系统的文档中应明确规定用户公钥传送方法。

5.3.9.3 密钥存储

PKI 系统部件密钥和系统用户密钥应存储于国家密码行政管理部门规定的密码模块中或以加密的形式存储，CA 签名公私钥对应以加密的形式存储于硬件密码设备中。

如果终端用户密钥在 PKI 系统服务部件中存储，则应以加密的形式存储。如果终端用户密钥由用户自行存储，则由其选择存储方式。

PKI 系统的文档中应明确规定密钥存储方法。

5.3.9.4 密钥备份

对 PKI 系统部件密钥和系统用户密钥备份，应以加密形式进行。

对于 CA 签名私钥备份，应以加密的形式进行，且只有特定权限的人才能访问私钥信息存放部件。

用户签名私钥由用户自行备份。用户用于机密性目的的密钥由 PKI 系统备份时，应以加密形式进行。

PKI 系统的文档中应明确规定密钥备份方法。

5.3.9.5 密钥导入导出

所有密钥导入导出 PKI 系统，应采用国家密码行政管理部门认可的加密算法或加密设备。私钥不应以明文形式导入导出密码模块。PKI 系统应把导入导出的密钥与正确实体相关联，并赋予相应的权限。

PKI 系统的文档中应明确规定密钥导入导出方法。

5.3.9.6 密钥更新

PKI 系统应采取明确的方法更新 CA 密钥及证书。在更新过程中应采取安全措施保证 PKI 系统服务的安全性和连续性。CA 新密钥对的产生、新公钥的分发、旧公钥归档以及旧私钥的销毁应符合本级别中各自的相关规定。

用户密钥由 PKI 系统自动更新时，PKI 系统应采取明确的方法更新用户密钥及证书，在更新过程中应采取安全措施保证用户密钥和证书的安全。新密钥对的产生、新公钥的分发、旧公钥的归档、旧的用户私钥的销毁应符合 5.3.9 中的相关规定。

PKI 系统的文档中应明确规定密钥更新方法。

5.3.9.7 密钥恢复

对于备份的密钥，应仅由密钥所有者恢复；对于归档的密钥，则根据法律、规章或合同规定，由执法机关或管理部门恢复。PKI 系统应在恢复密钥前验证申请者的身份。

密钥恢复应保证密钥不被未授权地泄露或修改。其中 CA 签名私钥恢复需要特定权限的人在安全可信的环境中恢复。

PKI 系统的文档中应明确规定密钥恢复方法。

5.3.9.8 密钥归档

签名私钥不应被归档，用于解密数据的私钥应被归档。

CA、RA、终端用户或其他系统部件的公钥都应归档。

PKI 系统的文档中应明确规定密钥归档方法。

5.3.9.9 密钥销毁

PKI 系统密钥销毁需要特定权限的人执行密钥销毁程序，并应符合国家密码行政管理部门对密钥

销毁的相关规定。

终端用户密钥的销毁一般由用户自己执行销毁程序。

PKI 系统的文档中应明确规定密钥销毁方法。

5.3.10 轮廓管理

5.3.10.1 证书轮廓管理

5.3.10.1.1 基本证书轮廓管理

PKI 系统应具备证书轮廓，并保证发行的证书与证书轮廓中的描述一致。

5.3.10.1.2 扩展的证书轮廓管理

管理员应为证书扩展指定可能的值。

5.3.10.2 证书撤销列表轮廓管理

5.3.10.2.1 基本证书撤销列表轮廓

若 PKI 系统发布 CRL，TSF 应具备证书撤销列表轮廓，并保证发行的 CRL 与该轮廓中的规定相一致。

5.3.10.2.2 扩展的证书撤销列表轮廓

若 PKI 系统发布 CRL，管理员应指定 CRL 和 CRL 扩展可接受的值。

5.3.10.3 在线证书状态协议轮廓管理

OCSP 轮廓应规定 PKI 系统可能产生的字段类型和字段类型可接受的变量值。

5.3.11 证书管理

5.3.11.1 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由 PKI 系统根据 GB/T 20518—2006 生成，或经由证书颁发机构验证以保证其与标准的一致性。

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) 评估者应检查 PKI 系统产生的证书是否满足基本要求。

5.3.11.2 证书撤销

5.3.11.2.1 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。

5.3.11.2.2 OCSP 基本回应的审核

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。

5.4 第四级

5.4.1 概述

第四级的 PKI 系统，所保护的资产价值很高，面临的安全威胁很大。结构上，PKI 系统的 CA、RA、证书资料库应独立设计，并采用双证书（签名证书和加密证书）机制，建设双中心（证书认证中心和密钥管理中心）。第四级 PKI 系统的安全要素要求列表见附录 A。

5.4.2 物理安全

5.4.2.1 核心部件物理安全

应按照 GB/T 21052—2007 第 7 章所描述的要求，对 PKI 系统硬件及相关环境进行评估。

5.4.2.2 RA 物理安全

RA 可有多种建设方式。

RA 应设置专门的区域来接待日常业务。

RA 应妥善保管私钥。

RA 设备应有安全人员和电子监控设备保护防盗。

所有的活动都应被授权人员或安全人员监控。

RA 对外服务的时间应被严格限制。

维修和服务人员在工作区域应受监控。

5.4.3 角色与责任

开发者应提供 PKI 系统管理员、操作员、审计员和安全员的角色定义。

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

操作员角色：负责签发和撤销证书。

审计员角色：负责查看和维护审计日志。

安全员角色：负责执行系统的备份和恢复。

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。

系统用户应按照角色的安全功能管理进行权限限制。

5.4.4 访问控制

5.4.4.1 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。应定期审核系统用户的访问权限。选取和使用口令时系统用户，应按照已定义的策略和程序进行。对无人值守的设备应有适当的保护措施。

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；

b) 标识与鉴别系统用户的过程；

c) 角色的职能分割；

d) 进行 PKI 系统的特定操作时需要的最小系统用户人数。

5.4.4.2 网络访问控制

用户可以且只能直接访问被授权使用的服务。用户终端到 PKI 系统服务的路径应是受控的。远程用户只有被认证后，PKI 系统才允许访问。连接到远程计算机系统应被认证。对 PKI 系统诊断分析端口的访问应进行安全控制。PKI 系统内部网络和外部网络之间应设置安全控制。

按照 PKI 系统的访问控制策略，应限制用户可用的服务。路由控制应保证计算机连接和信息流不违背系统的访问控制策略。PKI 系统所有网络服务的安全属性要求在 PKI 系统文档中有相关说明。

5.4.4.3 操作系统访问控制

PKI 系统的访问应使用安全的登录过程。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。系统的口令管理应提供工具确保生成高质量的口令。对系统工具的使用应进行严格的控制。经过指定时间的不活动状态，正在访问 PKI 服务系统的终端应超时进入保护状态，以防未授权用户访问。对高风险的应用应限制连接次数以提供额外的保护。

5.4.4.4 应用访问控制

应根据访问控制策略，严格限制对信息和应用系统功能访问。

5.4.5 标识与鉴别

5.4.5.1 用户属性定义

PKI 系统应维护每个用户的安全属性。

5.4.5.2 用户鉴别

当进行鉴别时，PKI 系统的安全功能应避免提供给用户的反馈泄露用户的鉴别数据。

在用户身份被鉴别之前，PKI 系统不允许执行代表该用户的任何行动。

PKI 系统应提供多鉴别机制，对不同身份的用户使用不同的鉴别机制。

PKI 系统应定义鉴别机制如何提供鉴别以及每一种鉴别机制将在何时使用。

5.4.5.3 用户标识

在用户被标识之前，PKI 系统不允许执行代表该用户的任何行动。

5.4.5.4 用户主体绑定

PKI 系统应通过用户主体绑定建立和维护用户与用户主体之间的关联，使用户的身份与该用户的所有可审计行为相关联。

5.4.5.5 鉴别失败处理

PKI 系统的安全功能应能检测到与鉴别事件相关的不成功的鉴别尝试。

当用户自从上次鉴别成功以来不成功的鉴别尝试的次数达到或超过了定义的界限时，PKI 系统应采取应对措施。

5.4.5.6 秘密的规范

当用来对用户身份鉴别的口令、密钥等秘密信息由用户产生时，PKI 系统应对可接受的秘密信息的质量做出要求，并检查。秘密信息质量量度由管理员制定。

当用来对用户身份鉴别的口令、密钥等秘密信息由 PKI 系统产生时，PKI 系统应可生成符合秘密信息质量要求的秘密信息。秘密信息质量量度由管理员制定。

5.4.6 审计

5.4.6.1 审计数据产生

PKI 系统安全功能应能为系统的可审计事件生成一个审计记录，并在每一个审计记录中至少记录基本信息。

PKI 系统安全功能应能维护系统的可审计事件。

5.4.6.2 审计查阅

PKI 系统安全功能应为审计员提供从审计记录中读取一定类型的审计信息的能力。

5.4.6.3 选择性审计

审计功能部件应可根据基本属性选择或排除审计事件中的可审计事件。

5.4.6.4 审计事件存储

审计功能部件应能够防止对审计记录的非授权修改，并可检测对审计记录的修改；当审计踪迹存储已满时，审计功能部件应能够阻止除由审计员发起的以外的所有审计事件的发生。

5.4.6.5 可信的时间戳

PKI 系统应获得可信的时间戳功能供审计部件使用。

5.4.6.6 审计日志签名

审计功能部件应定期从第三方获得数字签名的时间戳。时间戳不应由审计功能部件签名。

审计功能部件获得时间戳的时间周期应是可配置的。

对审计日志做时间戳的事件应写入日志中，时间戳应包含在其中。

5.4.7 数据输入输出

5.4.7.1 TOE 内部用户数据传送

在 PKI 系统的物理分隔部件间传递用户数据时，PKI 系统应执行访问控制策略，以防止安全相关的用户数据被篡改以及机密性用户数据的泄露。

在 PKI 系统的物理分隔部件间传递用户数据时，PKI 系统应执行访问控制策略，以检测是否有用户数据的完整性错误出现。检测到完整性错误时，PKI 系统应采取行动进行处理。

5.4.7.2 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。

5.4.7.3 **TSF 间用户数据传送的完整性**

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，使得能以某种方式传送和接收用户数据时，保护数据以避免完整性错误。

5.4.7.4 **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。

5.4.7.5 **输出 TSF 数据的完整性**

PKI 系统应提供检测与远程可信 IT 产品间传送的所有 TSF 数据是否被修改的能力。检测到完整性错误时，PKI 系统应采取行动进行处理。

5.4.7.6 **TOE 内 TSF 数据的传送**

PKI 系统应保护安全相关的 TSF 数据在分离的 PKI 部件间传送时不被篡改，保护机密性 TSF 数据在分离的 PKI 部件间传送时不被泄露。

PKI 系统能检测在系统分离部件间传送的 TSF 数据的完整性错误出现。检测到完整性错误时，PKI 系统应采取行动进行处理。

5.4.7.7 **原发抗抵赖**

PKI 系统在任何时候都应对证书状态信息和其他安全相关信息强制产生原发证据。

PKI 系统应能为所有安全相关的信息提供验证信息原发证据的能力。

对初始化证书注册消息，PKI 系统只接受经过完整性算法保护的。

对所有其他安全相关信息，PKI 系统只接受经过数字签名算法保护的。

5.4.8 **备份与恢复**

PKI 系统应具有备份和恢复功能，并可在需要时调用备份功能。在系统备份数据中应保存足够的信息使系统能够重建备份时的系统状态。**这些数据应以稳定可靠的方式存储，使其在掉电的情况下仍然能够保存。**并通过完整性措施防止备份数据受到未授权的修改。关键安全参数和其他机密信息应以加密形式存储。

5.4.9 **密钥管理**

5.4.9.1 **密钥生成**

PKI 系统部件密钥和系统用户密钥应由相应级别的 CA 或 RA 等机构生成。在密钥生成时应采取安全控制。

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。在密钥生成时应采取安全控制，只有管理员才能启动 CA 密钥生成过程，而且生成过程中应有多个管理员同时在场，**使用知识分割或其他分布式生成方法生成。**

终端用户签名私钥只能由其自己生成；终端用户加密密钥可由用户生成，也可委托 CA、RA 等 PKI 系统的服务机构生成。生成方法应符合国家密码行政管理部门的规定。

PKI 系统的文档中应明确规定密钥生成方法。

5.4.9.2 **密钥传送与分发**

PKI 系统的部件密钥和系统用户密钥的传送与分发应当以加密形式安全进行。CA 公钥分发方法应当切实可行，并应当保证 CA 公钥的完整性。

PKI 系统的文档中应明确说明 CA 公钥分发方法。

如果终端用户自己生成密钥对，终端用户应将公钥安全地提交给 PKI 系统。

如果终端用户委托 CA 生成密钥对，那么不需要签发前的公钥传送，CA 向用户传送与分发私钥应当以加密形式安全进行。

PKI 系统的文档中应明确规定用户公钥传送方法。

5.4.9.3 密钥存储

PKI 系统部件密钥和系统用户密钥应存储于国家密码行政管理部门规定的密码模块中或以加密的形式存储，**其中 CA 签名私钥应采用分割知识方法或其他分布存储方案**。

如果终端用户密钥在 PKI 系统服务部件中存储，则应以加密的形式存储。如果终端用户密钥由用户自行存储，则由其选择存储方式。

PKI 系统的文档中应明确规定密钥存储方法。

5.4.9.4 密钥备份

对 PKI 系统部件密钥和系统用户密钥备份，应以加密形式进行。

对于 CA 签名私钥备份，应以加密的形式**采用分割知识等方法分布存储于硬件密码设备中**，且只有特定权限的人才能访问私钥信息存放部件。

用户签名私钥由用户自行备份。用户用于机密性目的的密钥由 PKI 系统备份时，应以加密形式进行。

PKI 系统的文档中应明确规定密钥备份方法。

5.4.9.5 密钥导入导出

所有密钥导入导出 PKI 系统，应采用国家密码行政管理部门认可的加密算法或加密设备。私钥不应以明文形式导入导出 PKI 系统。**对关键的密钥导入导出，应采用分割知识的方法进行**。PKI 系统应把导入导出的密钥与正确实体相关联，并赋予相应的权限。

PKI 系统的文档中应明确规定密钥导入导出方法。

5.4.9.6 密钥更新

PKI 系统应采取明确的方法更新 CA 密钥及证书。在更新过程中应采取安全措施保证 PKI 系统服务的安全性和连续性。CA 新密钥对的产生、新公钥的分发、旧公钥归档以及旧私钥的销毁应符合本级别中各自的相关规定。

用户密钥由 PKI 系统自动更新时，PKI 系统应采取明确的方法更新用户密钥及证书，在更新过程中应采取安全措施保证用户密钥和证书的安全。**新密钥对的产生、新公钥的分发、旧公钥的归档、旧的用户私钥的销毁应符合 5.4.9 中的相关规定**。

5.4.9.7 密钥恢复

对于备份的密钥，应仅由密钥所有者恢复；对于归档的密钥，则根据法律、规章或合同规定，由执法机关或管理部门恢复。PKI 系统应在恢复密钥前验证申请者的身份。

密钥恢复应保证密钥不被未授权地泄露或修改。其中 CA 签名私钥恢复**需要多个特定权限的人同时使用存有密钥信息的部件在安全可信的环境中进行，恢复后私钥仍然采用分割知识程序或其他分布式方案存放**。

PKI 系统的文档中应明确规定密钥恢复方法。

5.4.9.8 密钥归档

签名私钥不应被归档，用于解密数据的私钥应被归档。

CA、RA、终端用户或其他系统部件的公钥都应归档。

PKI 系统的文档中应明确规定密钥归档方法。

5.4.9.9 密钥销毁

PKI 系统密钥销毁需要特定权限的人执行密钥销毁程序，**CA 签名私钥销毁需要多个管理员同时在场执行多道销毁程序**，并应符合国家密码行政管理部门对密钥销毁的相关规定。

终端用户密钥的销毁一般由用户自己执行销毁程序。

PKI 系统的文档中应明确规定密钥销毁方法。

5.4.10 轮廓管理

5.4.10.1 证书轮廓管理

5.4.10.1.1 基本证书轮廓管理

PKI 系统应具备证书轮廓，并保证发行的证书与证书轮廓中的描述一致。

5.4.10.1.2 扩展的证书轮廓管理

管理员应为证书扩展指定可能的值。

5.4.10.2 证书撤销列表轮廓管理

5.4.10.2.1 基本证书撤销列表轮廓

若 PKI 系统发布 CRL，TSF 应具备证书撤销列表轮廓，并保证发行的 CRL 与该轮廓中的规定相一致。

5.4.10.2.2 扩展的证书撤销列表轮廓

若 PKI 系统发布 CRL，管理员应指定 CRL 和 CRL 扩展可接受的值。

5.4.10.3 在线证书状态协议轮廓管理

OCSP 轮廓应规定 PKI 系统可能产生的字段类型和字段类型可接受的变量值。

5.4.11 证书管理

5.4.11.1 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由 PKI 系统根据 GB/T 20518—2006 生成，或经由证书颁发机构验证以保证其与标准的一致性。

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) 评估者应检查 PKI 系统产生的证书是否满足基本要求。

5.4.11.2 证书撤销

5.4.11.2.1 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。

5.4.11.2.2 OCSP 基本回应的审核

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。

5.5 第五级

5.5.1 概述

第五级的 PKI 系统，所保护的资产价值极高，面临的安全威胁极大。本标准中规定了最基本的安全要求，实际运营的 PKI 系统应满足并不限于本标准中的规定。结构上，PKI 系统的 CA、RA、证书资料库应独立设计，并采用双证书（签名证书和加密证书）机制，建设双中心（证书认证中心和密钥管理中心）。第五级 PKI 系统的安全要素要求列表见附录 A。

5.5.2 物理安全

5.5.2.1 核心部件物理安全

应按照 **GB/T 21052—2007 第 8 章**所描述的要求，对 PKI 系统硬件及相关环境进行评估。

5.5.2.2 RA 物理安全

RA 可有多种建设方式。

RA 应设置专门的区域来接待日常业务。

RA 应妥善保管私钥。

RA 设备应有安全人员和电子监控设备保护防盗。

所有的活动都应被授权人员或安全人员监控。

RA 对外服务的时间应被严格限制。

维修和服务人员在工作区域应受监控。

5.5.3 角色与责任

PKI 系统应对系统用户提供管理员、操作员、审计员和安全员的角色定义。

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

操作员角色：负责签发和撤销证书。

审计员角色：负责查看和维护审计日志。

安全员角色：负责执行系统的备份和恢复。

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。

系统应具备防范特权主体危害 PKI 系统安全的能力，每个角色的行为都应受到限制，使各个角色都无法越权完成任何非法操作，也不能对系统进行任何恶意活动。

系统用户应按照角色的安全功能管理进行权限限制。

5.5.4 访问控制

5.5.4.1 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。应定期审核系统用户的访问权限。选取和使用口令时系统用户应按照已定义的策略和程序进行。对无人值守的设备应有适当的保护措施。

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；

b) 标识与鉴别系统用户的过程；

c) 角色的职能分割；

d) 进行 PKI 系统的特定操作时需要的最小系统用户人数。

5.5.4.2 网络访问控制

用户可以且只能直接访问被授权使用的服务。用户终端到 PKI 系统服务的路径应是受控的。远程用户只有被认证后，PKI 系统才允许访问。连接到远程计算机系统应被认证。对 PKI 系统诊断分析端口的访问应进行安全控制。PKI 系统内部网络和外部网络之间应设置安全控制。

按照 PKI 系统的访问控制策略，应限制用户可用的服务。路由控制应保证计算机连接和信息流不违背系统的访问控制策略。PKI 系统所有网络服务的安全属性要求在 PKI 文档中有相关说明。

5.5.4.3 操作系统访问控制

对连接到特定位置或移动设备的认证应当使用自动终端标识过程。PKI 系统的访问应使用安全的登录过程。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。系统的口令管理应提供工具以确保生成高质量的口令。对系统工具的使用应进行严格的控制。

经过指定时间的不活动状态，正在访问 PKI 服务系统的终端应超时进入保护状态，以防未授权用户访问。对高风险的应用应限制连接次数以提供额外的保护。

5.5.4.4 应用访问控制

应根据访问控制策略，严格限制对信息和应用系统功能访问。**敏感系统应有独立的计算环境。**

5.5.5 标识与鉴别

5.5.5.1 用户属性定义

PKI 系统应维护每个用户的安全属性。

5.5.5.2 用户鉴别

当进行鉴别时，PKI 系统的安全功能应避免提供给用户的反馈泄露用户的鉴别数据。

在用户身份被鉴别之前，PKI 系统不允许执行代表该用户的任何行动。

PKI 系统应提供多鉴别机制，对不同身份的用户使用不同的鉴别机制。

PKI 系统应定义鉴别机制如何提供鉴别以及每一种鉴别机制将在何时使用。

5.5.5.3 用户标识

在用户被标识之前，PKI 系统不允许执行代表该用户的任何行动。

5.5.5.4 用户主体绑定

PKI 系统应通过用户主体绑定建立和维护用户与用户主体之间的关联，使用户的身份与该用户的所有可审计行为相关联。

5.5.5.5 鉴别失败处理

PKI 系统的安全功能应能检测到与鉴别事件相关的不成功的鉴别尝试。

当用户自从上次鉴别成功以来不成功的鉴别尝试的次数达到或超过了定义的界限时，PKI 系统应采取应对措施。

5.5.5.6 秘密的规范

当用来对用户身份鉴别的口令、密钥等秘密信息由用户产生时，PKI 系统应对可接受的秘密信息的质量做出要求，并检查。秘密信息质量量度由管理员制定。

当用来对用户身份鉴别的口令、密钥等秘密信息由 PKI 系统产生时，PKI 系统应可生成符合秘密信息质量要求的秘密信息。秘密信息质量量度由管理员制定。

5.5.6 审计

5.5.6.1 审计数据产生

PKI 系统安全功能应能为系统的可审计事件生成一个审计记录，并在每一个审计记录中至少记录基本信息。

PKI 系统安全功能应能维护系统的可审计事件。

5.5.6.2 审计查阅

PKI 系统安全功能应为审计员提供从审计记录中读取一定类型的审计信息的能力。

5.5.6.3 选择性审计

审计功能部件应可根据基本属性选择或排除审计事件中的可审计事件。

5.5.6.4 审计事件存储

审计功能部件应能够防止对审计记录的非授权修改，并可检测对审计记录的修改；当审计踪迹存储已满时，审计功能部件应能够阻止除由审计员发起的以外的所有审计事件的发生。

5.5.6.5 可信的时间戳

PKI 系统应获得可信的时间戳功能供审计部件使用。

5.5.6.6 审计日志签名

审计功能部件应定期从第三方获得数字签名的时间戳。

时间戳不应由审计功能部件签名。

审计功能部件获得时间戳的时间周期应是可配置的。

对审计日志做时间戳的事件应写入日志中，时间戳应包含在其中。

5.5.7 数据输入输出

5.5.7.1 TOE 内部用户数据传送

在 PKI 系统的物理分隔部件间传递用户数据时，PKI 系统应执行访问控制策略，以防止安全相关的用户数据被篡改以及机密性用户数据的泄露。

在 PKI 系统的物理分隔部件间传递用户数据时，PKI 系统应执行访问控制策略，以检测是否有用

户数据的完整性错误出现。检测到完整性错误时，PKI 系统应采取行动进行处理。

5.5.7.2 **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。

5.5.7.3 **TSF 间用户数据传送的完整性**

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，使得能以某种方式传送和接收用户数据时，保护数据以避免完整性错误。

5.5.7.4 **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。

5.5.7.5 **输出 TSF 数据的完整性**

PKI 系统应提供检测与远程可信 IT 产品间传送的所有 TSF 数据是否被修改的能力。检测到完整性错误时，PKI 系统应采取行动进行处理。

对于 PKI 系统与远程可信 IT 产品间传送的所有 TSF 数据，如被修改，PKI 系统应提供改正的能力。

5.5.7.6 **TOE 内 TSF 数据的传送**

PKI 系统应保护安全相关的 TSF 数据在分离的 PKI 部件间传送时不被篡改，保护机密性 TSF 数据在分离的 PKI 部件间传送时不被泄露。

PKI 系统能检测在系统分离部件间传送的 TSF 数据的完整性错误出现。检测到完整性错误时，PKI 系统应采取行动进行处理。

5.5.7.7 **原发抗抵赖**

PKI 系统在任何时候都应对证书状态信息和其他安全相关信息强制产生原发证据。

PKI 系统应能为所有安全相关的信息提供验证信息原发证据的能力。

对初始化证书注册消息，PKI 系统只接受经过完整性算法保护的。

对所有其他安全相关信息，PKI 系统只接受经过数字签名算法保护的。

5.5.8 **备份与恢复**

PKI 系统应具有备份和恢复功能，并可在需要时调用备份功能。**在系统备份数据中应保存足够的信息使系统能够重建上一次完整事务完成后的系统状态**。这些数据应以稳定可靠的方式存储，使其在掉电的情况下仍然能够保存。并通过完整性措施防止备份数据受到未授权的修改，关键安全参数和其他机密信息应以加密形式存储。

5.5.9 **密钥管理**

5.5.9.1 **密钥生成**

PKI 系统部件密钥和系统用户密钥应由相应级别的 CA 或 RA 等机构生成。在密钥生成时应采取安全控制。

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。在密钥生成时应采取安全控制，只有管理员才能启动 CA 密钥生成过程，而且生成过程中应有多个管理员同时在场，使用知识分割或其他分布式生成方法生成。

终端用户签名私钥只能由其自己生成；终端用户加密密钥可由用户生成，也可委托 CA、RA 等 PKI 系统的服务机构生成。生成方法应符合国家密码行政管理部门的规定。

PKI 系统的文档中应明确规定密钥生成方法。

5.5.9.2 **密钥传送与分发**

PKI 系统的部件密钥和系统用户密钥的传送与分发应当以加密形式安全进行。CA 公钥分发方法应当切实可行，并应当保证 CA 公钥的完整性。

PKI 系统的文档中应明确说明 CA 公钥分发方法。

如果终端用户自己生成密钥对，终端用户应将公钥安全地提交给 PKI 系统。

如果终端用户委托 CA 生成密钥对，那么不需要签发前的公钥传送，CA 向用户传送与分发私钥应当以加密形式安全进行。

PKI 系统的文档中应明确规定用户公钥传送方法。

5.5.9.3 密钥存储

PKI 系统部件密钥和系统用户密钥应以加密的形式存储于硬件密码设备中，CA 签名私钥应采用分割知识方法或其他分布存储方案。

如果终端用户密钥在 PKI 系统服务部件中存储，则应由硬件密码设备加密后存储。如果终端用户密钥由用户自行存储，则应以加密的形式存储于硬件密码设备中。

PKI 系统的文档中应明确规定密钥存储方法。

5.5.9.4 密钥备份

对 PKI 系统部件密钥和系统用户密钥备份，应以加密的形式存储于硬件密码设备中。

对于 CA 签名私钥备份，应以加密的形式采用分割知识等方法分布存储于硬件密码设备中，且只有特定权限的人才能访问私钥信息存放部件。

用户签名私钥由用户自行备份，以加密的形式存储于硬件密码设备中。用户用于机密性目的的密钥由 PKI 系统备份时，应由硬件密码设备加密后备份。

PKI 系统的文档中应明确规定密钥备份方法。

5.5.9.5 密钥导入导出

所有密钥导入导出 PKI 系统，应采用国家密码行政管理部门认可的加密算法或加密设备。私钥不应以明文形式导入导出 PKI 系统。对关键的密钥导入导出，应采用分割知识的方法进行。PKI 系统应把导入导出的密钥与正确实体相关联，并赋予相应的权限。

PKI 系统的文档中应明确规定密钥导入导出方法。

5.5.9.6 密钥更新

PKI 系统应采取明确的方法更新 CA 密钥及证书。在更新过程中应采取安全措施保证 PKI 系统服务的安全性和连续性。CA 新密钥对的产生、新公钥的分发、旧公钥归档以及旧私钥的销毁应符合本级别中各自的相关规定。

用户密钥由 PKI 系统自动更新时，PKI 系统应采取明确的方法更新用户密钥及证书，在更新过程中应采取安全措施保证用户密钥和证书的安全。**新密钥对的产生、新公钥的分发、旧公钥的归档、旧的用户私钥的销毁应符合 5.5.9 中的相关规定。**

5.5.9.7 密钥恢复

对于备份的密钥，应仅由密钥所有者恢复；对于归档的密钥，则根据法律、规章或合同规定，由执法机关或管理部门恢复。PKI 系统应在恢复密钥前验证申请者的身份。

密钥恢复应保证密钥不被未授权地泄露或修改。其中 CA 签名私钥恢复需要多个特定权限的人同时使用存有密钥信息的部件在安全可信的环境中进行，**在恢复过程中不应在任何一点出现 CA 签名私钥的完整形式**，恢复后私钥仍然采用分割知识程序或其他分布式方案存放。

PKI 系统的文档中应明确规定密钥恢复方法。

5.5.9.8 密钥归档

签名私钥不应被归档，用于解密数据的私钥应被归档。

CA、RA、终端用户或其他系统部件的公钥都应归档。

PKI 系统的文档中应明确规定密钥归档方法。

5.5.9.9 密钥销毁

PKI 系统密钥销毁需要特定权限的人执行密钥销毁程序，CA 签名私钥销毁需要多个管理员同时在场执行多道销毁程序，并应符合国家密码行政管理部门对密钥销毁的相关规定。

终端用户密钥的销毁由用户自己执行多道销毁程序。

PKI 系统的文档中应明确规定密钥销毁方法。

5.5.10 **轮廓管理**

5.5.10.1 **证书轮廓管理**

5.5.10.1.1 **基本证书轮廓管理**

PKI 系统应具备证书轮廓，并保证发行的证书与证书轮廓中的描述一致。

5.5.10.1.2 **扩展的证书轮廓管理**

管理员应为证书扩展指定可能的值。

5.5.10.2 **证书撤销列表轮廓管理**

5.5.10.2.1 **基本证书撤销列表轮廓**

若 PKI 系统发布 CRL，TSF 应具备证书撤销列表轮廓，并保证发行的 CRL 与该轮廓中的规定相一致。

5.5.10.2.2 **扩展的证书撤销列表轮廓**

若 PKI 系统发布 CRL，管理员应指定 CRL 和 CRL 扩展可接受的值。

5.5.10.3 **在线证书状态协议轮廓管理**

OCSP 轮廓应规定 PKI 系统可能产生的字段类型和字段类型可接受的变量值。

5.5.11 **证书管理**

5.5.11.1 **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由 PKI 系统根据 GB/T 20518—2006 生成，或经由证书颁发机构验证以保证其与标准的一致性。

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) 评估者应检查 PKI 系统产生的证书是否满足基本要求。

5.5.11.2 **证书撤销**

5.5.11.2.1 **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。

5.5.11.2.2 **OCSP 基本回应的审核**

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。

附　录　A
（规范性附录）
安全要素要求级别划分

本附录给出的表 A.1 对安全要素要求的级别划分进行了总结。

表 A.1　安全功能要求级别划分

安全要素	第一级	第二级	第三级	第四级	第五级
物理安全	+	++	+++	++++	+++++
角色	+	++	+++	++++	+++++
访问控制	+	++	+++	+++	++++
标识与鉴别	+	++	+++	++++	++++
审计		+	++	+++	+++
数据输入输出	+	++	+++	++++	+++++
备份与恢复		+	++	+++	++++
密钥管理	+	++	+++	++++	+++++
轮廓管理	+	++	++	++	++
证书管理	+	+	+	+	+
表中“+”表示对安全要素的要求，“+”数量的增加表示安全要素要求的提高。					

参 考 文 献

[1] ISO/IEC 15408-1:1999 Information technology—Security techniques—Evaluation Criteria for IT Security—Part 1:Introduction and general model,Version 2.0

[2] ISO/IEC 15408-2:1999 Information technology—Security techniques—Evaluation Criteria for IT Security—Part 2:Security functional requirements,Version 2.0

[3] ISO/IEC 15408-3:1999 Information technology—Security techniques—Evaluation Criteria for IT Security—Part 3:Security assurance requirements,Version 2.0

[4] PKI Assessment Guidelines—PAG v3.0 Public Draft for Comment

GB/T 21054—2007

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 公钥基础设施
PKI 系统安全等级保护评估准则
GB/T 21054—2007
*
中国标准出版社出版发行
北京西城区复兴门外三里河北街 16 号
邮政编码:100045
http://www.spc.net.cn
http://www.gb168.cn
电话:(010)51299090、68522006
2008 年 1 月第一版
*
书号:155066·1-30415

GB/T 21054-2007