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 IV
引　言 V
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 7
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 10
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 12
5.2.10 轮廓管理 13
5.2.11 证书管理 14
5.2.12 配置管理 15
5.2.13 分发和操作 15
5.2.14 开发 16
5.2.15 指导性文档 16

5.2.16 生命周期支持 16
5.2.17 测试 16
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 17
5.3.3 角色与责任 17
5.3.4 访问控制 18
5.3.5 标识与鉴别 20
5.3.6 审计 21
5.3.7 数据输入输出 22
5.3.8 备份与恢复 23
5.3.9 密钥管理 23
5.3.10 轮廓管理 26
5.3.11 证书管理 27
5.3.12 配置管理 28
5.3.13 分发和操作 28
5.3.14 开发 29
5.3.15 指导性文档 29
5.3.16 生命周期支持 30
5.3.17 测试 30
5.3.18 脆弱性评定 30
5.4 第四级 31
5.4.1 概述 31
5.4.2 物理安全 31
5.4.3 角色与责任 31
5.4.4 访问控制 32
5.4.5 标识与鉴别 33
5.4.6 审计 34
5.4.7 数据输入输出 36
5.4.8 备份与恢复 37
5.4.9 密钥管理 37
5.4.10 轮廓管理 40
5.4.11 证书管理 41
5.4.12 配置管理 42
5.4.13 分发和操作 43
5.4.14 开发 43
5.4.15 指导性文档 44
5.4.16 生命周期支持 44
5.4.17 测试 45
5.4.18 脆弱性评定 45
5.5 第五级 45
5.5.1 概述 45
5.5.2 物理安全 45

5.5.3 角色与责任 45
5.5.4 访问控制 46
5.5.5 标识与鉴别 48
5.5.6 审计 49
5.5.7 数据输入输出 50
5.5.8 备份与恢复 51
5.5.9 密钥管理 52
5.5.10 轮廓管理 55
5.5.11 证书管理 56
5.5.12 配置管理 57
5.5.13 分发和操作 57
5.5.14 开发 58
5.5.15 指导性文档 58
5.5.16 生命周期支持 59
5.5.17 测试 59
5.5.18 脆弱性评定 59
附 录 A（规范性附录）安全要素要求级别划分 61
参考文献 62

前　言

（略）

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 AAA—200×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 AAA—200×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，提倡使用本标准的各方探讨使用其最新版本的可能性。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/T20984-2007　信息安全技术　信息安全风险评估指南

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（PKI） public key infrastructure (PKI)

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。（除了在本标准中其它地方所定义的分配给其它角色的 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的提交给 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 标准相一致。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

证书撤消列表轮廓用于定义 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 标准相一致。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 系统自动的生成；**
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：
——提供分发的过程；
——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消或修改，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的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。**
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消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。(除了在本标准中其它地方所定义的分配给其它角色的 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。
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。

5.2.5.4 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。

5.2.5.5 鉴别失败处理

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 系统的安全功能应能检测到。这个界限是管理员可配置的。管理员可配置的参数包括但不限于，失败的鉴别次数和时间门限值。

鉴别不成功尝试的次数不必连续，但应与鉴别事件相关。

5.2.6 审计

5.2.6.1 审计数据产生

审计功能部件应对下列事件产生审计记录：

a) 审计功能的启动和结束；

b) 表 5 中的事件。

表5 可审计事件

功能	事件	附加信息
安全审计	**所有对审计变量（如：时间间隔、审计事件的类型）的改变**	
	所有删除审计记录的企图	
	对审计日志签名	**审计日志记录中应保存数字签名、Hash 结果或认证码。**
本地数据输入	**所有的安全相关数据输入系统**	**若输入的数据与其它数据相关应验证用户访问相关数据的权限。**
远程数据输入	**所有被系统所接受的安全相关信息**	
数据输出	**所有对关键的或安全相关的信息进行输出的请求**	
密钥生成	**PKI 系统生成密钥的要求（用作一次性会话密钥的对称密钥生成除外）**	**审计日志记录中应保存非对称密钥对的公钥部分。**
私钥载入	**部件私钥的载入**	
私钥的存储	**对为密钥恢复而保存的证书主体私钥的读取**	
可信公钥的输入，删除和存储	**所有对于可信公钥的改变（如：添加、删除）**	**审计日志记录中应包括公钥和与公钥相关的信息。**
私钥和对称密钥的输出	**私钥和对称密钥（包括一次性会话密钥）的输出**	
证书注册	**所有的证书请求**	**若成功，保存证书的拷贝在日志中； 若拒绝，保存原因在日志中。**
证书状态变更的审批	**所有更改证书状态的请求**	**在日志中保存请求结果（成功或失败）。**
PKI 系统部件的配置	**所有的与安全相关的对于 PKI 系统安全功能的配置**	
证书轮廓管理	**所有的对于证书轮廓的更改**	**在日志记录中保存对轮廓更改的内容。**
撤销轮廓管理	**所有的对于撤销轮廓的更改**	**在日志记录中保存对轮廓更改的内容。**
证书撤销列表轮廓管理	**所有的对于证书撤销列表轮廓的更改**	**在日志记录中保存对轮廓更改的内容。**
在线证书状态协议轮廓管理	**所有的对于 OCSP 轮廓的更改**	**在日志记录中保存对轮廓更改的内容。**

对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，以及表 5 中附加信息栏中要求的内容。

日志记录中不应出现明文形式的私钥、对称密钥和其它安全相关的参数。

审计功能部件应能将可审计事件与发起该事件的用户身份相关联。

5.2.6.2 审计查阅

审计功能部件应为管理员提供查看日志所有信息的能力。

审计功能部件应以适于阅读和解释的方式向阅读者提供日志信息。

5.2.6.3 选择性审计

审计功能部件应可根据下列属性选择或排除审计事件集中的可审计事件：

用户标识、事件类型、主体标识、客体标识等。

5.2.6.4 审计事件存储

审计功能部件应具有以下能力：

a) 受保护的审计踪迹存储，能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；

b) 防止审计数据丢失，要求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，以防止对安全相关的用户数据的篡改。

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。

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。

5.2.7.4 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；

PKI 系统应保护机密性 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，使在系统失败或者其它严重错误的情况下能够重建系统。执行备份的频率取决于系统或者应用的重要性。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

5.2.9.1.1 PKI 系统密钥生成

PKI 系统部件密钥和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。

5.2.9.1.2 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。

5.2.9.2 密钥传送与分发

5.2.9.2.1 PKI 系统密钥传送与分发

PKI 系统部件密钥的传送与分发应以加密形式直接发送到 PKI 系统部件中，加密算法等应符合国家密码行政管理部门的规定。

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。**CA 公钥分发还应保证 CA 公钥的完整性，可通过嵌入应用软件、SSL、手工等方法分发。**

5.2.9.2.2 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的提交给 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。

5.2.9.3 密钥存储

系统部件密钥和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。

5.2.9.4 密钥导入导出

密钥被导出到 PKI 系统之外可能基于以下的原因：密钥备份、复制，以及将 PKI 系统部件产生的密钥传送到用户手中。

密钥导入或导出 PKI 系统时，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 系统用户密钥、系统部件密钥、终端用户密钥可使用软件加密，CA 签名私钥应使用软件方法或硬件密码设备进行加密。

PKI 系统应提供合适的方法把导入或导出 PKI 系统的对称密钥、私有密钥或公有密钥与正确实体相关联，并赋予相应的权限，其中实体可能是一个人、一个组或一个过程。

5.2.9.5 密钥销毁

PKI 系统应提供销毁对称密钥和私有密钥的适当方法，PKI 系统文档中应规定这些密钥销毁方法，保证销毁过程应是不可逆的，密钥销毁方法应符合国家密码行政管理部门规定。

5.2.10 轮廓管理

5.2.10.1 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 标准相一致。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；
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。

PKI 系统管理员还应为以下的字段和扩展指定可能的取值：

a) keyUsage；

b) basicConstraints；

c) certificatePolicies。

管理员还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

证书撤消列表轮廓用于定义 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 标准相一致。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；

c) NextUpdate。

若 PKI 系统发布 CRL，管理员还应指定 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

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。

5.2.11 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 系统自动的生成；

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。

5.2.11.2 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。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。

5.2.11.2.2 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。

5.2.12 配置管理

应按 **GB/T 20271-2006 中 6.2.5.1** 的要求，从以下方面实现 PKI 系统的配置管理：

a) 在配置管理能力方面应实现对版本号等方面的要求；
b) **在 PKI 系统的配置管理范围方面，应将 PKI 系统的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下**；
c) **在系统的整个生存期，即在它的开发、测试和维护期间，应有一个软件配置管理系统处于保持对改变源码和文件的控制状态。只有被授权的代码和代码修改才允许被加进已交付的源码的基本部分。所有改变应被记载和检查，以确保未危及系统的安全。在软件配置管理系统中，应包含从源码产生出系统新版本、鉴定新生成的系统版本和保护源码免遭未授权修改的工具和规程。通过技术、物理和保安规章三方面的结合，可充分保护生成系统所用到的源码免遭未授权的修改和毁坏**。

5.2.13 分发和操作

应按 **GB/T 20271-2006 中 6.2.5.2** 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：
——提供分发的过程；
——安全启动和操作的过程；
——**建立日志的过程**。

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。

5.2.14 开发

应按 **GB/T 20271-2006 中 6.2.5.3** 的要求，从以下方面进行 PKI 系统的开发：

a) 按**非形式化安全策略模型、完全定义的外部接口**、描述性高层设计、TSF 子集实现、**TSF 内部结构层次化**、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。

5.2.15 指导性文档

应按 **GB/T 20271-2006 中 6.2.5.4** 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；

d) **应提供关于所有审计工具的文档，包括为检查和保持审计文件所推荐的过程、针对每种审计事件的详细审计记录文件、为周期性备份和删除审计记录所推荐的过程等**；

e) **应提供如何进行系统自我评估的章节（带有网络管理、口令要求、意外事故计划的安全报告）和为灾害恢复计划所做的建议，以及描述普通侵入技术和其它威胁，并查出和阻止入侵的方法**。

5.2.16 生命周期支持

应按 **GB/T 20271-2006 中 6.2.5.5** 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和**明确定义开发工具的要求**进行开发，并提供**开发过程中的安全措施说明**；

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消或修改，说明在故障或系统出错时如何恢复系统至安全状态；

c) **如果系统含有加强安全性的硬件，那么管理员、其他用户或自动的诊断测试，应能在各自的操作环境中运行它并详细说明操作过程**。

5.2.17 测试

应按 **GB/T 20271-2006 中 6.2.5.6** 的要求，从以下方面对 PKI 系统进行测试：

a) 应通过**测试范围的证据、测试的范围分析、高层设计的测试**、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，**包括查找漏洞，如违反系统访问控制要求、违反资源访问控制要求、拒绝服务、对审计或验证数据进行未授权访问等**。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。

5.2.18 脆弱性评定

应按 GB/T 20271-2006 中 6.2.5.7 的要求，从以下方面对所开发的 PKI 系统进行脆弱性评定：

a) **指南检查**；

b) **PKI 系统安全功能强度评估**；

c) **开发者脆弱性分析**。

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，适用于运营级的 PKI 系统或者安全要求极高的企业级 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 和证书资料库都应独立设计，并采用终端用户证书分为签名证书和加密证书的双证书机制，建设包括证书认证中心和密钥管理中心的双中心系统。证书认证中心和密钥管理中心的基本功能要求、建设要求和运行管理要求等相关安全技术要求应符合国家相关标准的规定。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

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 6 章**所描述的要求。

5.3.2.2 RA 物理安全

RA 可全部托管在 CA 系统，也可部分托管在 CA 系统，部分建在远端。

RA 应设置专门的区域来接待日常业务，只有被授权者才能接触 RA 工作站和相关敏感数据、设备。

RA 应妥善保管私钥，在 RA 设备不使用时应锁存私钥。

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在指定的时间。

维修和服务人员在工作区域应受监控。

5.3.3 角色与责任

开发者应提供 PKI 系统管理员、操作员和**审计员**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；执行系统的备份和恢复。本级 PKI 系统新增审计员角色，与审计相关的权限只应分配给审计员。

操作员：签发和撤销证书。

审计员：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。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 6 中的配置对授权的角色修改安全功能的能力进行限制。

表6 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。
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。（除了在本标准中其它地方所定义的分配给其它角色的 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。

5.3.4 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，检查不应有的权限分配。**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。**对无人值守的设备应有适当的保护措施，用户登录时应严格控制和记录。**

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 7。

表7 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消证书的主体所完成。
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； **至少应有 2 个人才可请求解密证书私钥，这两个人中一个是操作员，另一个是操作员、管理员、审计员中的一人。**
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的请求。
私钥和对称密钥销毁	仅管理员、**审计员、操作员**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； **输出证书私钥至少应获得 2 个人的同意，这两个人中一个是操作员，另一个是操作员、管理员、审计员中的一人。**
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 5.3.5 的要求。

c) 角色的职能分割

应符合 5.3.3 的要求。

d) 进行 PKI 系统的特定操作时需要的最小系统用户人数最少应满足以下要求：

CA 私钥和关键部件密钥的生成、备份、更新、导入导出、密钥恢复、密钥销毁等操作要求有多个系统用户同时在场，并符合表 7 的要求。

5.3.4.2 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。PKI 系统内部网络和外部网络之间应设置安全控制，并设置网关、网闸、防火墙等保护措施。**

按照 PKI 系统的访问控制策略，应限制用户可用的服务，对于不合理的服务请求应进行限制和过滤。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，不合理的信息流和网络连接应进行限制和过滤。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。

5.3.4.3 操作系统访问控制

PKI 系统的访问应使用安全的登录过程，自动登录等应被严格限制。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。

系统的口令管理应提供有效的、交互式的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。

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。

5.3.4.4 应用程序访问控制

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。无关的应用程序应进行删除，不适当的应用程序行调用应检查权限并记录。系统应采取病毒防治、漏洞扫描、入侵检测等安全防护措施。

5.3.5 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。

5.3.5.1 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。

5.3.5.2 用户鉴别

当进行鉴别时，PKI 系统的安全功能应仅仅将最少的反馈提供给用户（如打入的字符数、鉴别的成功或失败），不应给用户更多的信息。

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。

PKI 系统安全功能应提供一个以上的鉴别机制，对不同身份的用户使用不同的鉴别机制，并对一个用户使用多个鉴别过程。

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，口令字符输入时，应只显示星号，而不显示原始字符。

5.3.5.3 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。

5.3.5.4 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。

5.3.5.5 鉴别失败处理

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 系统的安全功能应能检测到。这个界限是管理员可配置的。管理员可配置的参数包括但不限于，失败的鉴别次数和时间门限值。

鉴别不成功尝试的次数不必连续，但应与鉴别事件相关。

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，例如：

a) 使终端失效一段随次数增加的时间；

b) 使一个用户帐号失效一段时间或失效，直到管理员解除；

c) 向管理员报警；

d) 重新允许用户会话建立过程。

为了防止拒绝服务，至少保证有一个用户帐号不应失效。

5.3.5.6 秘密的规范

当用来对用户身份鉴别的口令、密钥等秘密信息由终端用户自己产生时，PKI 系统应对可接受的秘密信息的质量作出要求，并检查。秘密信息质量包括字母数字结构或者密钥长度等。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。秘密信息质量包括字母数字结构或者密钥长度等。当使用伪随机生成器时，应能提供具有高度不可预见性的随机数。秘密信息质量量度由管理员制定。

终端用户口令应是字母和数字的组合，不少于 6 个字符。系统用户口令和系统部件密钥解密口令应是字母和数字的组合，不少于 8 个字符。口令不应采用有特殊意义的数字和组合，如姓名、生日、电话号码等。

5.3.6 审计

5.3.6.1 审计数据产生

审计功能部件应对下列事件产生审计记录：

a) 审计功能的启动和结束；

b) 表 8 中的事件。

表8 可审计事件

功能	事件	附加信息
安全审计	所有对审计变量（如：时间间隔、审计事件的类型）的改变	
	所有删除审计记录的企图	
	对审计日志签名	审计日志记录中应保存数字签名、Hash 结果或认证码。
本地数据输入	所有的安全相关数据输入系统	若输入的数据与其它数据相关则应验证用户访问相关数据的权限。
远程数据输入	所有被系统所接受的安全相关信息	
数据输出	所有对关键的或安全相关的信息进行输出的请求	
密钥生成	PKI 系统生成密钥的要求（用作一次性会话密钥的对称密钥生成除外）	审计日志记录中应保存非对称密钥对的公钥部分。
私钥载入	部件私钥的载入	
私钥的存储	对为密钥恢复而保存的证书主体私钥的读取	
可信公钥的输入，删除和存储	所有对于可信公钥的改变（如：添加、删除）	审计日志记录中应包括公钥和与公钥相关的信息。
私钥和对称密钥的输出	私钥和对称密钥（包括一次性会话密钥）的输出	
证书注册	所有的证书请求	若成功，保存证书的拷贝在日志中； 若拒绝，保存原因在日志中。
证书状态变更的审批	所有更改证书状态的请求	在日志中保存请求结果（成功或失败）。
PKI 系统部件的配置	所有的与安全相关的对于 PKI 系统安全功能的配置	
证书轮廓管理	所有的对于证书轮廓的更改	在日志记录中保存对轮廓更改的内容。

撤销轮廓管理	所有的对于撤销轮廓的更改	在日志记录中保存对轮廓更改的内容。
证书撤销列表轮廓管理	所有的对于证书撤销列表轮廓的更改	在日志记录中保存对轮廓更改的内容。
在线证书状态协议轮廓管理	所有的对于 OCSP 轮廓的更改	在日志记录中保存对轮廓更改的内容。

对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，以及表 8 中附加信息栏中要求的内容。

日志记录中不应出现明文形式的私钥、对称密钥和其它安全相关的参数。

审计功能部件应能将可审计事件与发起该事件的用户身份相关联。

5.3.6.2 审计查阅

审计功能部件应为审计员提供查看日志所有信息的能力。

审计功能部件应以适于阅读和解释的方式向阅读者提供日志信息。

5.3.6.3 选择性审计

审计功能部件应可根据下列属性选择或排除审计事件集中的可审计事件：

用户标识、事件类型、主体标识、客体标识等。

5.3.6.4 审计事件存储

审计功能部件应具有以下能力：

a) 受保护的审计踪迹存储，能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；

b) 防止审计数据丢失，要求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数字签名、Keyed Hash、认证码等完整性保护运算。

完整性保护运算的对象是从上次签名后加入的所有审计日志条目以及上次签名的结果。

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，审计日志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，以防止对安全相关的用户数据的篡改。

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。

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。

5.3.7.4 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；

PKI 系统应保护机密性 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

要求 PKI 系统在任何时候都应对证书状态信息和其它安全相关信息强制产生原发证据。PKI 系统应能使信息原发者的身份等属性，与证据适用信息的安全相关部分相关联。

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，按正规的程序来进行验证。

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，使在系统失败或者其它严重错误的情况下能够重建系统。执行备份的频率取决于系统或者应用的重要性。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。系统应**通过数字签名、Hash 等方式防止备份数据受到未授权的修改。关键安全参数和其它机密信息应以加密形式存储。**

备份方案取决于应用环境，但至少应满足以下基本要求：

a) 备份要在不中断数据库使用的前提下实施；

b) 备份方案应符合国家有关信息数据备份的标准要求；

c) 备份方案应提供人工和自动备份功能；

d) 备份方案应提供实时和定期备份功能；

e) 备份方案应提供增量备份功能；

f) 备份方案应提供日志记录功能。

5.3.9 密钥管理

5.3.9.1 密钥生成

5.3.9.1.1 PKI 系统密钥生成

PKI 系统部件密钥和系统用户密钥生成应由相应级别的 CA 或 RA 等机构进行，**应使用硬件密码设备产生。进行密钥生成时，PKI 系统应在安全可信的环境中生成。**

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，**应使用硬件密码设备产生**。进行密钥生成时，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，**且应有多于一个管理员同时在场**。

密钥生成过程应满足以下要求：

a) 如果在密码模块内部产生密钥，密码模块应使用国家密码行政管理部门认可的算法或安全函数、按国家密码行政管理部门认可的密钥生成方法生成密钥；

b) 如果密钥生成方法需要从随机数发生器输入随机数，那么随机数的生成应采用国家密码行政管理部门认可的方法；

c) 如果在密钥生成过程中加入随机种子，随机种子导入应符合国家密码行政管理部门的规定；

d) 猜测一个初始化确定性随机数发生器的随机种子值等危及密钥产生方法安全的难度，应至少和断定产生的密钥的值的难度一样大；

e) CA 签名公私密钥对生成应在可信的、安全的环境中产生，用于密钥对生成的随机数发生器产生的随机数要符合统计规律；

f) PKI 系统的文档中应明确规定系统密钥生成方法。

5.3.9.1.2 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。

PKI 系统的文档中应明确规定终端用户密钥生成方法。

5.3.9.2 密钥传送与分发

5.3.9.2.1 PKI 系统密钥传送与分发

PKI 系统部件密钥的传送与分发应以加密形式直接发送到 PKI 系统部件中，加密算法等应符合国家密码行政管理部门的规定。

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。CA 公钥分发还应保证 CA 公钥的完整性，

可通过嵌入应用软件、SSL、手工等方法分发。

PKI 系统的文档中应明确说明 CA 公钥分发方法。

5.3.9.2.2 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的提交给 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。

PKI 系统的文档中应明确规定用户密钥传送方法。

5.3.9.3 密钥有效期

PKI 系统应提供密钥有效期设置功能，并根据以下几点进行设置：

a) **密钥长度**；

b) **加密算法的攻击难度**；

c) **加密对象的价值**；

d) **合同或者法律等外部环境的需求**；

e) **密钥有效期的设定应符合国家密码行政管理部门规定。**

5.3.9.4 密钥存储

5.3.9.4.1 PKI 系统密钥存储

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由硬件密码设备加密后存储。CA 签名公私钥对应以加密的形式存储于国家密码行政管理部门认可的硬件密码设备中。

PKI 系统的文档中应明确规定系统密钥存储方法。

5.3.9.4.2 终端用户密钥存储

如果终端用户的密钥在 PKI 系统服务部件中存储，可用软件加密后存储在数据库中，加密算法应符合国家密码行政管理部门的规定。

如果终端用户的密钥由用户自行存储，则由用户选择存储方式。

PKI 系统的文档中应明确规定终端用户密钥存储方法。

5.3.9.5 密钥备份

5.3.9.5.1 PKI 系统密钥备份

对 PKI 系统部件密钥和系统用户密钥备份，应由国家密码行政管理部门认可的硬件密码设备加密后存储。

对于 CA 签名私钥备份，应以加密的形式备份于国家密码行政管理部门认可的硬件密码设备中，并进行访问控制，只有特定权限的人才能访问私钥信息存放部件。

PKI 系统密钥备份可采用热备份、冷备份和异地备份等措施。

PKI 系统的文档中应明确规定系统密钥备份方法。

5.3.9.5.2 终端用户密钥备份

用户签名私钥可由用户自行备份。用户用于机密性目的的密钥可由 PKI 服务机构提供备份服务或由用户自行备份。

如果由 PKI 系统备份，可用软件加密后存储在数据库中。如果用户自行备份，应用软件加密后存储。加密算法应符合国家密码行政管理部门的规定。

终端用户密钥备份可采用热备份、冷备份和异地备份等措施。

PKI 系统的文档中应明确规定终端用户密钥备份方法。

5.3.9.6 密钥导入导出

密钥被导出到 PKI 系统之外可能基于以下的原因：密钥备份、复制，以及将 PKI 系统部件产生的密钥传送到用户手中。

密钥导入或导出 PKI 系统时，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 系统用户密钥和系统部件密钥应由国家密码行政管理部门认可的硬件密码设备加密，终端用户密钥可使用软件加密，CA 签名私钥应使用硬件密码设备加密。**

PKI 系统应提供合适的方法把导入或导出 PKI 系统的对称密钥、私有密钥或公有密钥与正确实体相关联，并赋予相应的权限，其中实体可能是一个人、一个组或一个过程。

PKI 系统的文档中应明确规定密钥导入导出方法。

5.3.9.7 密钥更新

5.3.9.7.1 PKI 系统密钥更新

当 CA 签名密钥过期，或者 CA 签名私钥的安全性受到威胁时，带来了 CA 密钥和证书更新的问题。PKI 系统应提供有效的 CA 私钥及证书更新方式。要求：

a) **新密钥对的产生应符合5.3.9.1中的规定**；
b) **新的CA公钥的分发应符合5.3.9.2中的规定**；
c) **旧的CA公钥的归档应符合5.3.9.9中的规定**；
d) **旧的CA私钥的销毁应符合5.3.9.10中的规定**；
e) **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，防止例如替换CA私钥和证书等的各种攻击行为**；
f) **PKI系统的文档中，应说明CA密钥及证书的更新方法；并确保CA密钥及证书更新时，严格按照文档中规定的方法操作**。

5.3.9.7.2 用户密钥更新

用户密钥对过期或者私钥的安全性受到威胁时应更新密钥。用户密钥可由 PKI 系统自动更新，也可手工更新。要求：

a) **新密钥对的产生应符合5.3.9.1中的规定**；
b) **新的用户公钥的分发应符合5.3.9.2中的规定**；
c) **旧的用户公钥的归档应符合5.3.9.10中的规定**；
d) **旧的用户私钥的销毁应符合5.3.9.11中的规定**；
e) **如果用户密钥由PKI系统自动更新，则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，防止例如替换用户私钥和证书等的各种攻击行为**；
f) **如果用户密钥由PKI系统自动更新，则PKI系统的文档中，应说明用户密钥及证书的更新方法；并确保用户密钥及证书更新时，严格按照文档中规定的方法操作**。

5.3.9.8 密钥恢复

5.3.9.8.1 PKI 系统密钥恢复

对因密钥备份或密钥归档等不同原因存储在 PKI 系统中的密钥，在恢复时，应有不同的条件。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。

PKI 系统密钥恢复应保证密钥不被未授权的泄露或修改，恢复过程中密钥应以加密形式存在。

CA 签名私钥恢复需要特定权限的用户使用存有密钥信息的部件，在安全可信的环境中恢复，恢复过程不应危及密钥信息的安全性，不应暴露签名私钥。

PKI 系统的文档中应明确规定系统密钥恢复方法。

5.3.9.8.2 用户密钥恢复

用户密钥恢复应保证密钥不被未授权的泄露或修改，恢复过程中密钥应以加密形式存在。

PKI 系统的文档中应明确规定用户密钥恢复方法。

5.3.9.9 密钥归档

5.3.9.9.1 私钥归档

私钥归档中区分用于签名的私钥和用于解密数据的私钥。

签名私钥不允许被归档，用于解密数据的私钥允许被归档。

私钥归档如备份一样也保存一份私钥的拷贝，但用于不同的目的。备份用于系统运作的连续性，以防意外事故造成的私钥损坏、丢失、删除等。而归档用于长期的、将来为解密历史数据提供服务。

PKI 系统的文档中应明确规定私钥归档方法。

5.3.9.9.2 公钥归档

CA、RA、终端用户或其它系统部件的公钥都应归档，归档公钥为数字证书从目录中移除后验证数字签名提供了便利。

PKI 系统的文档中应明确规定公钥归档方法。

5.3.9.10 密钥销毁

5.3.9.10.1 PKI 系统密钥销毁

PKI 系统的密钥销毁应设置为只有特定权限的人才能执行销毁程序，并保证销毁过程应是不可逆的。PKI 系统提供的销毁程序可包括：用随机数据覆盖存储密钥的媒介、存储体，销毁存储密钥的媒介等。PKI 系统密钥销毁应符合国家密码行政管理部门对密钥销毁的相关规定。

PKI 系统的文档中应明确规定系统密钥销毁方法。

5.3.9.10.2 用户密钥销毁

终端用户密钥的销毁一般由用户自己执行销毁程序，并保证销毁过程应是不可逆的。用户可执行的销毁程序包括：用随机数据覆盖存储密钥的媒介、存储体，销毁存储密钥的媒介等。

PKI 系统的文档中应明确规定用户密钥销毁方法。

5.3.10 轮廓管理

5.3.10.1 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 标准相一致。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。

PKI 系统管理员还应为以下的字段和扩展指定可能的取值：

a) keyUsage；
b) basicConstraints；
c) certificatePolicies。

管理员还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

证书撤消列表轮廓用于定义 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 标准相一致。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；

c) NextUpdate。

若 PKI 系统发布 CRL，管理员还应指定 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

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。

5.3.11 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系统自动的生成；

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。

5.3.11.2 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。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。

5.3.11.2.2 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。

5.3.12 配置管理

应按 **GB/T 20271-2006 中 6.3.5.1** 的要求，从以下方面实现 PKI 系统的配置管理：

a) **在配置管理自动化方面要求部分的配置管理自动化**；
b) 在配置管理能力方面应实现对版本号、**配置项、授权控制**等方面的要求；
c) 在PKI系统的配置管理范围方面，应将PKI系统的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下，**要求实现对配置管理范围内的问题跟踪，特别是安全缺陷问题进行跟踪**；
d) 在系统的整个生存期，即在它的开发、测试和维护期间，应有一个软件配置管理系统处于保持对改变源码和文件的控制状态。只有被授权的代码和代码修改才允许被加进已交付的源码的基本部分。所有改变应被记载和检查，以确保未危及系统的安全。在软件配置管理系统中，应包含从源码产生出系统新版本、鉴定新生成的系统版本和保护源码免遭未授权修改的工具和规程。通过技术、物理和保安规章三方面的结合，可充分保护生成系统所用到的源码免遭未授权的修改和毁坏。

5.3.13 分发和操作

应按 **GB/T 20271-2006 中 6.3.5.2** 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、启动和**修改检测**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：
——提供分发的过程；
——安全启动和操作的过程；
——建立日志的过程；
——**修改内容的检测**；
——**对任何安全加强功能在启动、正常操作维护时能被撤消或修改的阐述**；
——**在故障或硬件、软件出错后恢复系统至安全状态的规程**；
——**对含有加强安全性的硬件部件，应说明用户或自动的诊断测试的操作环境和使用方法**；
——**所有诊断测试过程中，为加强安全性的硬件部件所提供例证的结果**；
——**在启动和操作时产生审计踪迹输出的例证**。

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；

f) **以安全方式开发并交付系统后，仍应提供对产品的长期维护和评估的支持，包括产品中的安全漏洞和现场问题的解决**；

g) **应采用书面说明的方式向客户通告新的安全问题**；

h) **对可能受到威胁的所有的安全问题，均应描述其特点，并作为主要的问题对待，直到它被解决**；

i) **为了支持已交付的软件的每个版本，对所有已有的安全漏洞都应有文档书面说明，并且客户能在限制的基础上得到该文档**；

j) **对安全漏洞的修改不必等到系统升级到下一个版本。安全功能的增加和改进应独立于系统版本的升级，也就是说，应存在适应性独立于系统其它功能的改进**；

k) **只有经过客户授权，才允许在生产性运行的系统上进行新特性和简易原型的开发、测试和安装**；

l) **新的版本应避免违反最初的安全策略和设想，也应避免在维护、增加或功能升级中引入安全漏洞，所有功能的改变和安全结构设置的默认值都应作记录。在新版本交付给客户使用前，客户应能得到相应的文档**。

5.3.14 开发

应按 **GB/T 20271-2006 中 6.3.5.3** 的要求，从以下方面进行 PKI 系统的开发：

a) 按非形式化安全策略模型、完全定义的外部接口、**安全加强的高层设计、TSF完全实现**、TSF内部结构层次化、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；

f) **在PKI系统开发的敏感阶段，应保持一个安全环境，该安全环境要求：**

——描述PKI系统开发所使用的计算机系统的安全使用和维护情况的安全策略和措施应有书面记载，并可供检查；

——系统开发过程中使用的所有计算机系统应接受定期的和有书面记载的内部安全审计，描述审计过程的文件和真实的审计报告应可供检查；

——除授权的分发机构外，不应在开发环境外部复制或分发内部文档；

——开发环境的计算机系统使用的所有软件应合法地从确定的渠道获得；

——开发者个人独自开发的软件，应在被开发管理者审核后才能用于开发的系统。

5.3.15 指导性文档

应按 **GB/T 20271-2006 中 6.3.5.4** 的要求，从以下方面编制 PKI 系统的指导性文档：

a) **应通过提供指导性文档，将如何安全使用和维护PKI系统的信息交付给系统的终端用户和系统用户。对文档的总体要求是：**

——应对所有的安全访问和相关过程、特权、功能等适当的管理加以阐述；

——应阐述安全管理和安全服务的交互，并提供指导；

——应详细给出每种审计事件的审计记录的结构，以便考察和维护审计文件和进程；

——应提供一个准则集用于保证附加的说明的一致性不受破坏。

b) **系统用户文档应提供系统用户了解如何用安全的方式管理系统，除了给出一般的安全忠告，还应明确：**

——在系统用安全的方法设置时，围绕管理员、操作员、审计员和安全员、主体和客体的属性等，应如何安装或终止安装；

——在系统的生命周期内如何用安全的方法维护系统，包括为了防止系统被破坏而进行的每天、每周、每月的安全常规备份等；

——如何用安全的方法重建PKI系统的方法；

——说明审计跟踪机制，使系统用户可有效地使用审计跟踪来执行本地的安全策略；

——必要时，如何调整系统的安全默认配置。

c) 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；

d) 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；

e) 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；

f) 应提供关于所有审计工具的文档，包括为检查和保持审计文件所推荐的过程、针对每种审计事件的详细审计记录文件、为周期性备份和删除审计记录所推荐的过程等；

g) 应提供如何进行系统自我评估的章节（带有网络管理、口令要求、意外事故计划的安全报告）和为灾害恢复计划所做的建议，以及描述普通侵入技术和其它威胁，并查出和阻止入侵的方法。

5.3.16 生命周期支持

应按 **GB/T 20271-2006 中 6.3.5.5** 的要求，从以下方面实现 PKI 系统的生命周期支持：

a) 按**标准的生命周期模型**和明确定义开发工具的要求进行开发，并提供开发过程中的安全措施说明；

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消或修改，说明在故障或系统出错时如何恢复系统至安全状态；

c) 如果系统含有加强安全性的硬件，那么管理员、其他用户或自动的诊断测试，应能在各自的操作环境中运行它并详细说明操作过程。

5.3.17 测试

应按 **GB/T 20271-2006 中 6.3.5.6** 的要求，从以下方面对 PKI 系统进行测试：

a) 应通过测试范围的证据、测试的范围分析、高层设计的测试、**低层设计测试、顺序的功能测试**、相符性独立测试和**抽样性独立测试**等，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，包括查找漏洞，如违反系统访问控制要求、违反资源访问控制要求、拒绝服务、对审计或验证数据进行未授权访问等。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。

5.3.18 脆弱性评定

应按 GB/T 20271-2006 中 6.3.5.7 的要求，从以下方面对所开发的 PKI 系统进行脆弱性评定：

a) **分析确认以防止误用**；

b) PKI系统安全功能强度评估；

c） 开发者脆弱性分析；

d） **独立脆弱性分析**。

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，适用于安全要求很高的运营级 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 和证书资料库都应独立设计，并采用终端用户证书分为签名证书和加密证书的双证书机制，建设包括证书认证中心和密钥管理中心的双中心系统。证书认证中心和密钥管理中心的基本功能要求、建设要求和运行管理要求等相关安全技术要求应符合国家相关标准的规定。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

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 7 章**所描述的要求。

5.4.2.2 RA 物理安全

RA 可全部托管在 CA 系统，也可部分托管在 CA 系统，部分建在远端。

RA 应设置专门的区域来接待日常业务，只有被授权者才能接触 RA 工作站和相关敏感数据、设备。

RA 应妥善保管私钥，在 RA 设备不使用时应锁存私钥。

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在指定的时间。

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：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。本级 PKI 系统新增安全员角色，与备份恢复相关的权限只应分配给安全员。

操作员：签发和撤销证书。

审计员：查看和维护审计日志。

安全员：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，并保证一个主体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 9 中的配置对授权的角色修改安全功能的能力进行限制。

表9 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。 **变更时间戳事件时间间隔和时间戳来源的权限仅授予管理员。**
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**安全员**。
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	**PKI 系统私钥的输出应得到至少两个管理员的认可，或一个管理员和一个操作员、审计员或安全员的认可。**

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。（除了在本标准中其它地方所定义的分配给其它角色的 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。

5.4.4 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，检查不应有的权限分配。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。对无人值守的设备应有适当的保护措施，用户登录时应严格控制和记录。

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 10。

表10 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消证书的主体所完成。
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； 至少应有 2 个人才可请求解密证书私钥，这两个人中一个是操作员，另一个是操作员、管理员、审计员和安全员中的一人。
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的请求。
私钥和对称密钥销毁	仅管理员、审计员、操作员有权将 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； 输出证书私钥至少应获得 2 个人的同意，这两个人中一

	个是操作员，另一个是操作员、管理员、审计员和安全员中的一人。
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 5.4.5 的要求。

c) 角色的职能分割

应符合 5.4.3 的要求。

d) 进行PKI系统的特定操作时需要的最小系统用户人数最少应满足以下要求：

CA 私钥和关键部件密钥的生成、备份、更新、导入导出、密钥恢复、密钥销毁等操作要求有多个系统用户同时在场，并符合表 10 的要求。

5.4.4.2 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。PKI 系统内部网络和外部网络之间应设置安全控制，并设置网关、网闸、防火墙等保护措施。

按照 PKI 系统的访问控制策略，应限制用户可用的服务，对于不合理的服务请求应进行限制和过滤。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，不合理的信息流和网络连接应进行限制和过滤。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。

5.4.4.3 操作系统访问控制

PKI 系统的访问应使用安全的登录过程，自动登录等应被严格限制。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。

系统的口令管理应提供有效的、交互式的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。

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。

5.4.4.4 应用程序访问控制

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。无关的应用程序应进行删除，不适当的应用程序调用应检查权限并记录。系统应采取病毒防治、漏洞扫描、入侵检测等安全防护措施。

5.4.5 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。

5.4.5.1 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。

5.4.5.2 用户鉴别

当进行鉴别时，PKI 系统的安全功能应仅仅将最少的反馈提供给用户（如打入的字符数、鉴别的成功或失败），不应给用户更多的信息。

在用户被成功鉴别之前，PKI 系统不允许执行代表该用户的任何行动。

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。

PKI 系统安全功能应提供一个以上的鉴别机制，对不同身份的用户使用不同的鉴别机制，并对一个用户使用多个鉴别过程。

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，口令字符输入时，应只显示星号，而不显示原始字符。

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

在标识用户的身份之前，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

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。

5.4.5.5 鉴别失败处理

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 系统的安全功能应能检测到。这个界限是管理员可配置的。管理员可配置的参数包括但不限于，失败的鉴别次数和时间门限值。

鉴别不成功尝试的次数不必连续，但应与鉴别事件相关。

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，例如：

a) 使终端失效一段随次数增加的时间；

b) 使一个用户帐号失效一段时间或失效，直到管理员解除；

c) 向管理员报警；

d) 重新允许用户会话建立过程。

为了防止拒绝服务，至少保证有一个用户帐号不应失效。

5.4.5.6 秘密的规范

当用来对用户身份鉴别的口令、密钥等秘密信息由终端用户自己产生时，PKI 系统应对可接受的秘密信息的质量作出要求，并检查。秘密信息质量包括字母数字结构或者密钥长度等。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。秘密信息质量包括字母数字结构或者密钥长度等。当使用伪随机生成器时，应能提供具有高度不可预见性的随机数。秘密信息质量量度由管理员制定。

终端用户口令应是字母和数字的组合，不少于 6 个字符。**系统用户口令和系统部件密钥解密口令应是字母、数字以及特殊字符的组合，不少于 10 个字符。**口令不应采用有特殊意义的数字和组合，如姓名、生日、电话号码等。

5.4.6 审计

5.4.6.1 审计数据产生

审计功能部件应对下列事件产生审计记录：

a) 审计功能的启动和结束；

b) 表11中的事件。

表11 可审计事件

功能	事件	附加信息
安全审计	所有对审计变量（如：时间间隔、审计事件的类型）的改变	
	所有删除审计记录的企图	
	对审计日志签名	审计日志记录中应保存数字签名、Hash 结果或认证码。
本地数据输入	所有的安全相关数据输入系统	若输入的数据与其它数据相关则应验证用户访问相关数据的权限。
远程数据输入	所有被系统所接受的安全相关信息	
数据输出	所有对关键的或安全相关的信息进行输出的请求	
密钥生成	PKI 系统生成密钥的要求（用作一次性会话密钥的对称密钥生成除外）	审计日志记录中应保存非对称密钥对的公钥部分。
私钥载入	部件私钥的载入	
私钥的存储	对为密钥恢复而保存的证书主体私钥的读取	
对称密钥存储	**手工导入用于认证的对称密钥**	
可信公钥的输入，删除和存储	所有对于可信公钥的改变（如：添加、删除）	审计日志记录中应包括公钥和与公钥相关的信息。
私钥和对称密钥的输出	私钥和对称密钥（包括一次性会话密钥）的输出	
证书注册	所有的证书请求	若成功，保存证书的拷贝在日志中； 若拒绝，保存原因在日志中。
证书状态变更的审批	所有更改证书状态的请求	在日志中保存请求结果（成功或失败）。
PKI 系统部件的配置	所有的与安全相关的对于 PKI 系统安全功能的配置	
证书轮廓管理	所有的对于证书轮廓的更改	在日志记录中保存对轮廓更改的内容。
撤销轮廓管理	所有的对于撤销轮廓的更改	在日志记录中保存对轮廓更改的内容。
证书撤销列表轮廓管理	所有的对于证书撤销列表轮廓的更改	在日志记录中保存对轮廓更改的内容。
在线证书状态协议轮廓管理	所有的对于 OCSP 轮廓的更改	在日志记录中保存对轮廓更改的内容。

对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，以及表 11 中附加信息栏中要求的内容。

日志记录中不应出现明文形式的私钥、对称密钥和其它安全相关的参数。

审计功能部件应能将可审计事件与发起该事件的用户身份相关联。

5.4.6.2 审计查阅

审计功能部件应为审计员提供查看日志所有信息的能力。

审计功能部件应以适于阅读和解释的方式向阅读者提供日志信息。

5.4.6.3 选择性审计

审计功能部件应可根据下列属性选择或排除审计事件集中的可审计事件：

用户标识、事件类型、主体标识、客体标识等。

5.4.6.4 审计事件存储

审计功能部件应具有以下能力：

a) 受保护的审计踪迹存储，能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；

b) 防止审计数据丢失，要求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。

数字签名时间戳签名的对象是从上次生成时间戳后加入的所有审计日志条目以及上次签名的时间戳的值。

对审计日志签名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，以防止对安全相关的用户数据的篡改。

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修改、替换、重排、删除等完整性错误出现。

检测到完整性错误时，PKI 系统应进行诸如重新请求数据、提醒管理员、记录发现的错误等处理。

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，保护数据避免篡改、删除、插入、重用错误。

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。

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。

5.4.7.5 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。

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

检测到完整性错误时，PKI 系统应进行诸如重新请求数据、提醒管理员、记录发现的错误等处理。

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；

PKI 系统应保护机密性 TSF 数据在分离的 PKI 部件间传送时不被泄露。

PKI 系统应能够检测在系统物理分离部件间传送的 TSF 数据的修改、替换、重排、删除等完整性

错误出现。

检测到完整性错误时，PKI 系统应进行诸如重新请求数据、提醒管理员、记录发现的错误等处理。

5.4.7.7 原发抗抵赖

要求 PKI 系统在任何时候都应对证书状态信息和其它安全相关信息强制产生原发证据。PKI 系统应能使信息原发者的身份等属性，与证据适用信息的安全相关部分相关联。

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，按照正规的程序来进行验证。

对初始化证书注册消息，PKI 系统只接受经过认证码、Keyed Hash 或者数字签名算法保护的。

对所有其它安全相关信息，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，使在系统失败或者其它严重错误的情况下能够重建系统。执行备份的频率取决于系统或者应用的重要性。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，例如磁盘或者磁带，使其在掉电的情况下仍然能够保存**。系统应通过数字签名、Hash 等方式防止备份数据受到未授权的修改。关键安全参数和其它机密信息应以加密形式存储。

备份方案取决于应用环境，但至少应满足以下基本要求：

a) 备份要在不中断数据库使用的前提下实施；

b) 备份方案应符合国家有关信息数据备份的标准要求；

c) 备份方案应提供人工和自动备份功能；

d) 备份方案应提供实时和定期备份功能；

e) 备份方案应提供增量备份功能；

f) 备份方案应提供日志记录功能。

5.4.9 密钥管理

5.4.9.1 密钥生成

5.4.9.1.1 PKI 系统密钥生成

PKI 系统部件密钥和系统用户密钥生成应由相应级别的 CA 或 RA 等机构进行，应使用硬件密码设备产生。进行密钥生成时，PKI 系统应在安全可信的环境中生成。

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，应使用硬件密码设备产生。进行密钥生成时，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，且应有多于一个管理员同时在场。

密钥生成过程应满足以下要求：

a) 如果在密码模块内部产生密钥，密码模块应使用国家密码行政管理部门认可的算法或安全函数、按国家密码行政管理部门认可的密钥生成方法生成密钥；

b) 如果密钥生成方法需要从随机数发生器输入随机数，那么随机数的生成应采用国家密码行政管理部门认可的方法；

c) 如果在密钥生成过程中加入随机种子，随机种子导入应符合国家密码行政管理部门的规定；

d) 猜测一个初始化确定性随机数发生器的随机种子值等危及密钥产生方法安全的难度，应至少和断定产生的密钥的值的难度一样大；

e) CA 签名公私密钥对生成应在可信的、安全的环境中产生，用于密钥对生成的随机数发生器产生的随机数要符合统计规律；

f) **应采用分割知识或其它分布式生成方法，每个管理员只能持有以加密形式存有一部分私钥信息的硬件密码设备。除非采用特殊的设备，私钥信息不应导出硬件密码设备**；

g) **在私钥产生过程中不应暴露私钥信息。CA签名密钥生成后，产生过程中使用的而签名过程中不再需要的密钥参数应销毁；**

h) PKI 系统的文档中应明确规定系统密钥生成方法。

5.4.9.1.2 终端用户密钥生成

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自己生成，也可委托 CA、RA 等 PKI 系统的服务机构生成。

用户自己生成密钥时，应采用国家密码行政管理部门认可的硬件设备。

PKI 系统的文档中应明确规定终端用户密钥生成方法。

5.4.9.2 密钥传送与分发

5.4.9.2.1 PKI 系统密钥传送与分发

PKI 系统部件密钥的传送与分发应以加密形式直接发送到 PKI 系统部件中，加密算法等应符合国家密码行政管理部门的规定。

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。CA 公钥分发还应保证 CA 公钥的完整性，可通过嵌入应用软件、SSL、手工等方法分发。

PKI 系统的文档中应明确说明 CA 公钥分发方法。

5.4.9.2.2 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的提交给 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。

PKI 系统的文档中应明确规定用户密钥传送方法。

5.4.9.3 密钥有效期

PKI 系统应提供密钥有效期设置功能，并根据以下几点进行设置：

a) 密钥长度；
b) 加密算法的攻击难度；
c) 加密对象的价值；
d) 合同或者法律等外部环境的需求；
e) 密钥有效期的设定应符合国家密码行政管理部门规定。

5.4.9.4 密钥存储

5.4.9.4.1 PKI 系统密钥存储

PKI 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由硬件密码设备加密后存储。PKI 系统部件密钥应以加密的形式存储于国家密码行政管理部门认可的硬件密码设备中。CA 签名公私钥对应采用分割知识方法或其它分布存储方案以密文的形式存储于专门的硬件密码模块中，且各模块应分散存放。

PKI 系统的文档中应明确规定系统密钥存储方法。

5.4.9.4.2 终端用户密钥存储

如果终端用户的密钥在 PKI 系统服务部件中存储，可用软件加密后存储在数据库中，加密算法应符合国家密码行政管理部门的规定。

如果用户的密钥由用户自行存储，则由用户选择存储方式。

PKI 系统的文档中应明确规定终端用户密钥存储方法。

5.4.9.5 密钥备份

5.4.9.5.1 PKI 系统密钥备份

对 PKI 系统部件密钥和系统用户密钥备份，应由国家密码行政管理部门认可的硬件密码设备加密后存储。

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备份于国家密码行政管理部门认可的硬件密码设备中，且各部件应分散存放于安全可信的环境中，**并进行访问控制，只有特定权限的人才能访问私钥信息存放部件。**只有在必要时，多个特定权限的人采用多个部件同时使用备份私钥信息恢复 CA 签名私钥**。

PKI 系统密钥备份应采用热备份、冷备份和异地备份等措施。

PKI 系统的文档中应明确规定系统密钥备份方法。

5.4.9.5.2 终端用户用户密钥备份

用户签名私钥可由用户自行备份。用户用于机密性目的的密钥可由 PKI 服务机构提供备份服务或由用户自行备份。

如果由 PKI 系统备份，可用软件加密后存储在数据库中。如果用户自行备份，应用软件加密后存储。加密算法应符合国家密码行政管理部门的规定。

终端用户密钥备份可采用热备份、冷备份和异地备份等措施。

PKI 系统的文档中应明确规定终端用户密钥备份方法。

5.4.9.6 密钥导入导出

密钥被导出到 PKI 系统之外可能基于以下的原因：密钥备份、复制，以及将 PKI 系统部件产生的密钥传送到用户手中。

密钥导入或导出 PKI 系统时，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 系统用户密钥和系统部件密钥应由国家密码行政管理部门认可的硬件密码设备加密，终端用户密钥可使用软件加密，**CA 签名私钥应使用硬件密码设备加密并进行知识分割**。

PKI 系统应提供合适的方法把导入或导出 PKI 系统的对称密钥、私有密钥或公有密钥与正确实体相关联，并赋予相应的权限，其中实体可能是一个人、一个组或一个过程。

PKI 系统的文档中应明确规定密钥导入导出方法。

5.4.9.7 密钥更新

5.4.9.7.1 PKI 系统密钥更新

当 CA 签名密钥过期，或者 CA 签名私钥的安全性受到威胁时，带来了 CA 密钥和证书更新的问题。PKI 系统应提供有效的 CA 私钥及证书更新方式。要求：

a) 新密钥对的产生应符合 5.4.9.1 中的规定；

b) 新的 CA 公钥的分发应符合 5.4.9.2 中的规定；

c) 旧的 CA 公钥的归档应符合 5.4.9.9 中的规定；

d) 旧的 CA 私钥的销毁应符合 5.4.9.10 中的规定；

e) 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，防止例如替换CA私钥和证书等的各种攻击行为；

f) PKI系统的文档中，应说明CA密钥及证书的更新方法；并确保CA密钥及证书更新时，严格按照文档中规定的方法操作。

5.4.9.7.2 用户密钥更新

用户密钥对过期或者私钥的安全性受到威胁时应更新密钥。用户密钥可由 PKI 系统自动更新，也可手工更新。要求：

a) 新密钥对的产生应符合 5.4.9.1 中的规定；

b) 新的用户公钥的分发应符合 5.4.9.2 中的规定；

c) 旧的用户公钥的归档应符合 5.4.9.10 中的规定；

d) 旧的用户私钥的销毁应符合 5.4.9.11 中的规定；

e) 如果用户密钥由PKI系统自动更新，则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，防止例如替换用户私钥和证书等的各种攻击行为；

f) 如果用户密钥由PKI系统自动更新，则PKI系统的文档中，应说明用户密钥及证书的更新方法；并确保用户密钥及证书更新时，严格按照文档中规定的方法操作。

5.4.9.8 密钥恢复

5.4.9.8.1 PKI 系统密钥恢复

对因密钥备份或密钥归档等不同原因存储在 PKI 系统中的密钥，在恢复时，应有不同的条件。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。

PKI 系统密钥恢复应保证密钥不被未授权的泄露或修改，恢复过程中密钥应以加密形式存在。

CA 签名私钥恢复**需要多个被授权的人同时使用存有密钥信息的部件，在安全可信的环境中恢复，恢复后私钥仍然采用分割知识程序或其它分布式方案存放**，恢复过程不应危及密钥信息的安全性，不应暴露签名私钥。

PKI 系统的文档中应明确规定系统密钥恢复方法。

5.4.9.8.2 终端用户密钥恢复

用户密钥恢复应保证密钥不被未授权的泄露或修改，恢复过程中密钥应以加密形式存在。

PKI 系统的文档中应明确规定用户密钥恢复方法。

5.4.9.9 密钥归档

5.4.9.9.1 私钥归档

私钥归档中区分用于签名的私钥和用于解密数据的私钥。

签名私钥是不允许被归档的，用于解密数据的私钥允许被归档。

私钥归档如备份一样也保存一份私钥的拷贝，但用于不同的目的。备份用于系统运作的连续性，以防意外事故造成的私钥损坏、丢失、删除等。而归档用于长期的、将来为解密历史数据提供服务。

PKI 系统的文档中应明确规定私钥归档方法。

5.4.9.9.2 公钥归档

CA、RA、终端用户或其它系统部件的公钥都应归档，归档公钥为数字证书从目录中移除后验证数字签名提供了便利。

PKI 系统的文档中应明确规定公钥归档方法。

5.4.9.10 密钥销毁

5.4.9.10.1 PKI 系统密钥销毁

PKI 系统的密钥销毁应设置为只有特定权限的人才能执行销毁程序，并保证销毁过程应是不可逆的。**CA 签名私钥的密钥销毁应设置为需要多个管理员同时在场，执行多道销毁程序**。PKI 系统提供的销毁程序可包括：用随机数据覆盖存储密钥的媒介、存储体，销毁存储密钥的媒介等。PKI 系统密钥销毁应符合国家密码行政管理部门对密钥销毁的相关规定。

PKI 系统的文档中应明确规定系统密钥销毁方法。

5.4.9.10.2 用户密钥销毁

终端用户密钥的销毁一般由用户自己执行销毁程序，并保证销毁过程应是不可逆的。用户可执行的销毁程序包括：用随机数据覆盖存储密钥的媒介、存储体，销毁存储密钥的媒介等。

PKI 系统的文档中应明确规定用户密钥销毁方法。

5.4.10 轮廓管理

5.4.10.1 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 标准相一致。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。

PKI 系统管理员还应为以下的字段和扩展指定可能的取值：

a) keyUsage；
b) basicConstraints；
c) certificatePolicies。

管理员还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

证书撤消列表轮廓用于定义 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 标准相一致。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；
c) NextUpdate。

若 PKI 系统发布 CRL，管理员还应指定 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

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。

5.4.11 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系统自动的生成；
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。

5.4.11.2 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。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。

5.4.11.2.2 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。

5.4.12 配置管理

应按 **GB/T 20271-2006 中 6.4.5.1** 的要求，从以下方面实现 PKI 系统的配置管理：

a) 在配置管理自动化方面要求部分的配置管理自动化；
b) 在配置管理能力方面应实现**生成支持和验收过程**的要求；
c) 在PKI系统的配置管理范围方面，应将PKI系统的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下，要求实现对**开发工具配置管理范围的管理**；

d) 在系统的整个生存期，即在它的开发、测试和维护期间，应有一个软件配置管理系统处于保持对改变源码和文件的控制状态。只有被授权的代码和代码修改才允许被加进已交付的源码的基本部分。所有改变应被记载和检查，以确保未危及系统的安全。在软件配置管理系统中，应包含从源码产生出系统新版本、鉴定新生成的系统版本和保护源码免遭未授权修改的工具和规程。通过技术、物理和保安规章三方面的结合，可充分保护生成系统所用到的源码免遭未授权的修改和毁坏。

5.4.13 分发和操作

应按 **GB/T 20271-2006 中 6.4.5.2** 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、启动和修改检测的过程进行说明，最终生成安全的配置。文档中所描述的内容应包括：
   ——提供分发的过程；
   ——安全启动和操作的过程；
   ——建立日志的过程；
   ——修改内容的检测；
   ——对任何安全加强功能在启动、正常操作维护时能被撤消或修改的阐述；
   ——在故障或硬件、软件出错后恢复系统至安全状态的规程；
   ——对含有加强安全性的硬件部件，应说明用户或自动的诊断测试的操作环境和使用方法；
   ——所有诊断测试过程中，为加强安全性的硬件部件所提供例证的结果；
   ——在启动和操作时产生审计踪迹输出的例证。
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；
f) 以安全方式开发并交付系统后，仍应提供对产品的长期维护和评估的支持，包括产品中的安全漏洞和现场问题的解决；
g) 应采用书面说明的方式向客户通告新的安全问题；
h) 对可能受到威胁的所有的安全问题，均应描述其特点，并作为主要的问题对待，直到它被解决；
i) 为了支持已交付的软件的每个版本，对所有已有的安全漏洞都应有文档书面说明，并且客户能在限制的基础上得到该文档；
j) 对安全漏洞的修改不必等到系统升级到下一个版本。安全功能的增加和改进应独立于系统版本的升级，也就是说，应存在适应性独立于系统其它功能的改进；
k) 只有经过客户授权，才允许在生产性运行的系统上进行新特性和简易原型的开发、测试和安装；
l) 新的版本应避免违反最初的安全策略和设想，也应避免在维护、增加或功能升级中引入安全漏洞，所有功能的改变和安全结构设置的默认值都应作记录。在新版本交付给客户使用前，客户应能得到相应的文档。

5.4.14 开发

应按 **GB/T 20271-2006 中 6.4.5.3** 的要求，从以下方面进行 PKI 系统的开发：

a) 按**半形式化功能说明、半形式化高层设计、TSF的结构化实现、TSF内部结构复杂度最小化、半形式化低层设计、半形式化对应性说明**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；
f) 在PKI系统开发的敏感阶段，应保持一个安全环境，该安全环境要求：
——描述PKI系统开发所使用的计算机系统的安全使用和维护情况的安全策略和措施应有书面记载，并可供检查；
——系统开发过程中使用的所有计算机系统应接受定期的和有书面记载的内部安全审计，描述审计过程的文件和真实的审计报告应可供检查；
——除授权的分发机构外，不应在开发环境外部复制或分发内部文档；
——开发环境的计算机系统使用的所有软件应合法地从确定的渠道获得；
——开发者个人独自开发的软件，应在被开发管理者审核后才能用于开发的系统。

5.4.15 指导性文档

应按 **GB/T 20271-2006 中 6.4.5.4** 的要求，从以下方面编制 PKI 系统的指导性文档：

a) 应通过提供指导性文档，将如何安全使用和维护PKI系统的信息交付给系统的终端用户和系统用户。对文档的总体要求是：
——应对所有的安全访问和相关过程、特权、功能等适当的管理加以阐述；
——应阐述安全管理和安全服务的交互，并提供指导；
——应详细给出每种审计事件的审计记录的结构，以便考察和维护审计文件和进程；
——应提供一个准则集用于保证附加的说明的一致性不受破坏。
b) 系统用户文档应提供系统用户了解如何用安全的方式管理系统，除了给出一般的安全忠告，还应明确：
——在系统用安全的方法设置时，围绕管理员、操作员、审计员和安全员、主体和客体的属性等，应如何安装或终止安装；
——在系统的生命周期内如何用安全的方法维护系统，包括为了防止系统被破坏而进行的每天、每周、每月的安全常规备份等；
——如何用安全的方法重建PKI系统的方法；
——说明审计跟踪机制，使系统用户可有效地使用审计跟踪来执行本地的安全策略；
——必要时，如何调整系统的安全默认配置。
c) 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；
d) 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；
e) 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；
f) 应提供关于所有审计工具的文档，包括为检查和保持审计文件所推荐的过程、针对每种审计事件的详细审计记录文件、为周期性备份和删除审计记录所推荐的过程等；
g) 应提供如何进行系统自我评估的章节（带有网络管理、口令要求、意外事故计划的安全报告）和为灾害恢复计划所做的建议，以及描述普通侵入技术和其它威胁，并查出和阻止入侵的方法。

5.4.16 生命周期支持

应按 **GB/T 20271-2006 中 6.4.5.5** 的要求，从以下方面实现 PKI 系统的生命周期支持：

a) 按标准的生命周期模型和**遵照实现标准-应用部分的工具和技术的要求**进行开发，并**提供充分的安全措施**；

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消或修改，说明在故障或系统出错时如何恢复系统至安全状态；

c) 如果系统含有加强安全性的硬件，那么管理员、其他用户或自动的诊断测试，应能在各自的操作环境中运行它并详细说明操作过程。

5.4.17 测试

应按 **GB/T 20271-2006 中 6.4.5.6** 的要求，从以下方面对 PKI 系统进行测试：

a) 应通过测试范围证据和**严格的范围分析**、高层设计测试、低层设计测试和**实现表示测试**、顺序的功能测试、相符独立性测试和抽样性独立测试等，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，包括查找漏洞，如违反系统访问控制要求、违反资源访问控制要求、拒绝服务、对审计或验证数据进行未授权访问等。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。

5.4.18 脆弱性评定

应按 GB/T 20271-2006 中 6.4.5.7 的要求，从以下方面对所开发的 PKI 系统进行脆弱性评定：

a) **一般性的隐蔽信道分析**；

b) **安全状态的检查和分析**；

c) PKI系统安全功能强度评估；

d) 开发者脆弱性分析；

e) 独立脆弱性分析；

f) **中级抵抗力分析**。

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，适用于安全要求极高的运营级 PKI 系统，是安全的理想状态。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 和证书资料库都应独立设计，并采用终端用户证书分为签名证书和加密证书的双证书机制，建设包括证书认证中心和密钥管理中心的双中心系统。证书认证中心和密钥管理中心的基本功能要求、建设要求和运行管理要求等相关安全技术要求应符合国家相关标准的规定。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

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 8 章**所描述的要求。

5.5.2.2 RA 物理安全

RA 可全部托管在 CA 系统，也可部分托管在 CA 系统，部分建在远端。

RA 应设置专门的区域来接待日常业务，只有被授权者才能接触 RA 工作站和相关敏感数据、设备。

RA 应妥善保管私钥，在 RA 设备不使用时应锁存私钥。

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在指定的时间。

维修和服务人员在工作区域应受监控。

5.5.3 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：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：签发和撤销证书。

审计员：查看和维护审计日志。

安全员：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，并保证一个主体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。

系统应具备防范系统用户危害 PKI 系统安全的能力，应使用分割知识程序等措施限制单个主体的权限。

角色的安全功能管理应按表 12 中的配置对授权的角色修改安全功能的能力进行限制。

表12　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； 变更时间戳事件时间间隔和时间戳来源的权限仅授予管理员。
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安全员。
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	PKI 系统私钥的输出应得到至少两个管理员的认可，或一个管理员和一个操作员，审计员或安全员的认可。
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。（除了在本标准中其它地方所定义的分配给其它角色的 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。

5.5.4　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，检查不应有的权限分配。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。对无人值守的设备应有适当的保护措施，用户登录时应严格控制和记录。

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 13。

表13　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消证书的主体所完成。
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； 至少应有 2 个人才可请求解密证书私钥，这两个人中一个是操作员，另一个是操作员、管理员、审计员和安全员中的一人。
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、审计员、操作员有权将 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； 输出证书私钥至少应获得 2 个人的同意，这两个人中一个是操作员，另一个是操作员、管理员、审计员和安全员中的一人。
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 5.5.5 的要求。

c） 角色的职能分割

应符合 5.5.3 的要求。

d） 进行PKI系统的特定操作时需要的最小系统用户人数最少应满足以下要求：

CA 私钥和关键部件密钥的生成、备份、更新、导入导出、密钥恢复、密钥销毁等操作应有多个系统用户同时在场，并符合表 13 的要求。

5.5.4.2 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。PKI 系统内部网络和外部网络之间应设置安全控制，并设置网关、网闸、防火墙等保护措施。

按照 PKI 系统的访问控制策略，应限制用户可用的服务，对于不合理的服务请求应进行限制和过滤。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，不合理的信息流和网络连接应进行限制和过滤。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

PKI 系统的访问应使用安全的登录过程，自动登录等应被严格限制。**对连接到特定位置或移动设备的认证应使用自动终端标识过程。**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有效的、交互式的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。

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。

5.5.4.4 应用程序访问控制

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。无关的应用程序应进行删除，不适当的应用程序调用应检查权限并记录。系统应采取病毒防治、漏洞扫描、入侵检测等安全防护措施。**敏感系统要求有独立的计算环境，不应与其它应用程序共享计算环境。**

5.5.5 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。

5.5.5.1 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。

5.5.5.2 用户鉴别

当进行鉴别时，PKI 系统的安全功能应仅仅将最少的反馈提供给用户（如打入的字符数、鉴别的成功或失败），不应给用户更多的信息。

在用户被成功鉴别之前，PKI 系统不允许执行代表该用户的任何行动。

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。

PKI 系统安全功能应提供一个以上的鉴别机制，对不同身份的用户使用不同的鉴别机制，并对一个用户使用多个鉴别过程。

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，口令字符输入时，应只显示星号，而不显示原始字符。

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

在标识用户的身份之前，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

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。

5.5.5.5 鉴别失败处理

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 系统的安全功能应能检测到。这个界限是管理员可配置的。管理员可配置的参数包括但不限于，失败的鉴别次数和时间门限值。

鉴别不成功尝试的次数不必连续，但应与鉴别事件相关。

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，例如：

a) 使终端失效一段随次数增加的时间；

b) 使一个用户帐号失效一段时间或失效，直到管理员解除；

c) 向管理员报警；

d) 重新允许用户会话建立过程。

为了防止拒绝服务，至少保证有一个用户帐号不应失效。

5.5.5.6 秘密的规范

当用来对用户身份鉴别的口令、密钥等秘密信息由终端用户自己产生时，PKI 系统应对可接受的秘密信息的质量作出要求，并检查。秘密信息质量包括字母数字结构或者密钥长度等。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。秘密信息质量包括字母数字结构或者密钥长度等。当使用伪随机生成器时，应能提供具有高度不可预见性的随机数。秘密信息质量量度由管理员制定。

终端用户口令应是字母和数字的组合，不少于 6 个字符。系统用户口令和系统部件密钥解密口令应是字母、数字以及特殊字符的组合，不少于 10 个字符。口令不应采用有特殊意义的数字和组合，如姓名、生日、电话号码等。

5.5.6 审计

5.5.6.1 审计数据产生

审计功能部件应对下列事件产生审计记录：

a) 审计功能的启动和结束；

b) 表14中的事件。

表14 可审计事件

功能	事件	附加信息
安全审计	所有对审计变量（如：时间间隔、审计事件的类型）的改变	
	所有删除审计记录的企图	
	对审计日志签名	审计日志记录中应保存数字签名、Hash 结果或认证码。
	获得第三方时间戳	**第三方数字签名的时间戳应包括在审计日志中。**
本地数据输入	所有的安全相关数据输入系统	若输入的数据与其它数据相关则应验证用户访问相关数据的权限。
远程数据输入	所有被系统所接受的安全相关信息	
数据输出	所有对关键的或安全相关的信息进行输出的请求	
密钥生成	PKI 系统生成密钥的要求（用作一次性会话密钥的对称密钥生成除外）	审计日志记录中应保存非对称密钥对的公钥部分。
私钥载入	部件私钥的载入	
私钥的存储	对为密钥恢复而保存的证书主体私钥的读取	

对称密钥存储	手工导入用于认证的对称密钥	
可信公钥的输入，删除和存储	所有对于可信公钥的改变（如：添加、删除）	审计日志记录中应包括公钥和与公钥相关的信息。
私钥和对称密钥的输出	私钥和对称密钥（包括一次性会话密钥）的输出	
证书注册	所有的证书请求	若成功，保存证书的拷贝在日志中； 若拒绝，保存原因在日志中。
证书状态变更的审批	所有更改证书状态的请求	在日志中保存请求结果（成功或失败）。
PKI 系统部件的配置	所有的与安全相关的对于 PKI 系统安全功能的配置	
证书轮廓管理	所有的对于证书轮廓的更改	在日志记录中保存对轮廓更改的内容。
撤销轮廓管理	所有的对于撤销轮廓的更改	在日志记录中保存对轮廓更改的内容。
证书撤销列表轮廓管理	所有的对于证书撤销列表轮廓的更改	在日志记录中保存对轮廓更改的内容。
在线证书状态协议轮廓管理	所有的对于 OCSP 轮廓的更改	在日志记录中保存对轮廓更改的内容。

对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，以及表 14 中附加信息栏中要求的内容。

日志记录中不应出现明文形式的私钥、对称密钥和其它安全相关的参数。

审计功能部件应能将可审计事件与发起该事件的用户身份相关联。

5.5.6.2 审计查阅

审计功能部件应为审计员提供查看日志所有信息的能力。

审计功能部件应以适于阅读和解释的方式向阅读者提供日志信息。

5.5.6.3 选择性审计

审计功能部件应可根据下列属性选择或排除审计事件集中的可审计事件：

用户标识、事件类型、主体标识、客体标识等。

5.5.6.4 审计事件存储

审计功能部件应具有以下能力：

a) 受保护的审计踪迹存储，能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；

b) 防止审计数据丢失，要求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 系统应提供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。

数字签名时间戳签名的对象是从上次生成时间戳后加入的所有审计日志条目以及上次签名的时间戳的值。

对审计日志签名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，以防止对安全相关的用户数据的篡改。

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修改、替换、重排、删除等完整性错误出现。

检测到完整性错误时，PKI 系统应进行诸如重新请求数据、提醒管理员、记录发现的错误等处理。

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 系统与其它 PKI 系统或 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 系统与其它 PKI 系统或 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，保护数据避免篡改、删除、插入、重用错误。

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。

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。

5.5.7.5 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。

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

检测到完整性错误时，PKI 系统应进行诸如重新请求数据、提醒管理员、记录发现的错误等处理。

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；

PKI 系统应保护机密性 TSF 数据在分离的 PKI 部件间传送时不被泄露。

PKI 系统应能检测在系统物理分离部件间传送的 TSF 数据的修改、替换、重排、删除等完整性错误出现。

检测到完整性错误时，PKI 系统应进行诸如重新请求数据、提醒管理员、记录发现的错误等处理。

5.5.7.7 原发抗抵赖

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

PKI 系统应能使信息原发者的身份等属性，与证据适用信息的安全相关部分相关联。

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，按照正规的程序来进行验证。

对初始化证书注册消息，PKI 系统只接受经过认证码、Keyed Hash 或者数字签名算法保护的。

对所有其它安全相关信息，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，使在系统失败或者其它严重错误的情况下能够重建系统。执行备份的频率取决于系统或者应用的重要性。**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，例如磁盘或者磁带，使其在掉电的情况下仍然能够保存。系统应通过数字签名、Hash 等方式防止备份数据受到未授权的修改。关键安全参数和其它机密信息应以加密形式存储。

备份方案取决于应用环境，但至少应满足以下基本要求：

a) 备份要在不中断数据库使用的前提下实施；

b) 备份方案应符合国家有关信息数据备份的标准要求；
c) 备份方案应提供人工和自动备份功能；
d) 备份方案应提供实时和定期备份功能；
e) 备份方案应提供增量备份功能；
f) 备份方案应提供日志记录功能。

5.5.9 密钥管理

5.5.9.1 密钥生成

5.5.9.1.1 PKI 系统密钥生成

PKI 系统部件密钥和系统用户密钥生成应由相应级别的 CA 或 RA 等机构进行，应使用硬件密码设备产生。进行密钥生成时，PKI 系统应在安全可信的环境中生成。

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，应使用硬件密码设备产生。进行密钥生成时，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，且应有多于一个管理员同时在场。

密钥生成过程应满足以下要求：

a) 如果在密码模块内部产生密钥，密码模块应使用国家密码行政管理部门认可的算法或安全函数、按国家密码行政管理部门认可的密钥生成方法生成密钥；
b) 如果密钥生成方法需要从随机数发生器输入随机数，那么随机数的生成应采用国家密码行政管理部门认可的方法；
c) 如果在密钥生成过程中加入随机种子，随机种子导入应符合国家密码行政管理部门的规定；
d) 猜测一个初始化确定性随机数发生器的随机种子值等危及密钥产生方法安全的难度，应至少和断定产生的密钥的值的难度一样大；
e) CA 签名公私密钥对生成应在可信的、安全的环境中产生，用于密钥对生成的随机数发生器产生的随机数要符合统计规律；
f) 应采用分割知识或其它分布生成方法，在私钥产生过程中不应暴露私钥信息，每个管理员只能持有以加密形式存有一部分私钥信息的硬件密码设备。除非采用特殊的设备，私钥信息不应导出硬件密码设备；
g) 在私钥产生过程中不应暴露私钥信息。CA 签名密钥生成后，产生过程中使用的而签名过程中不再需要的密钥参数应销毁；
h) PKI 系统的文档中应明确规定系统密钥生成方法。

5.5.9.1.2 终端用户密钥生成

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自己生成，也可委托 CA、RA 等 PKI 系统的服务机构生成。

用户自己生成密钥时，应采用国家密码行政管理部门认可的硬件设备。

PKI 系统的文档中应明确规定终端用户密钥生成方法。

5.5.9.2 密钥传送与分发

5.5.9.2.1 PKI 系统密钥传送与分发

PKI 系统部件密钥的传送与分发应以加密形式直接发送到 PKI 系统部件中，加密算法等应符合国家密码行政管理部门的规定。

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。CA 公钥分发还应保证 CA 公钥的完整性，可通过嵌入应用软件、SSL、手工等方法分发。

PKI 系统的文档中应明确说明 CA 公钥分发方法。

5.5.9.2.2 终端用户公钥传送与分发

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的提交给 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。

PKI 系统的文档中应明确规定用户密钥传送方法。

5.5.9.3 密钥有效期

PKI 系统应提供密钥有效期设置功能，并根据以下几点进行设置：

a) 密钥长度；

b) 加密算法的攻击难度；

c) 加密对象的价值；

d) 合同或者法律等外部环境的需求；

e) 密钥有效期的设定应符合国家密码行政管理部门规定。

5.5.9.4 密钥存储

5.5.9.4.1 PKI 系统密钥存储

PKI 系统部件密钥和系统用户密钥应以加密的形式存储于国家密码行政管理部门认可的硬件密码设备中。CA 签名公私钥对应采用分割知识方法或其它分布存储方案以密文的形式存储于专门的硬件密码模块中，且各模块应分散存放。

PKI 系统的文档中应明确规定系统密钥存储方法。

5.5.9.4.2 终端用户密钥存储

如果终端用户的密钥在 PKI 系统服务部件中存储，应由国家密码行政管理部门认可的硬件密码设备加密后存储。

如果终端用户的密钥由用户自行存储，则用户应以加密的形式存储于国家密码行政管理部门认可的硬件密码设备中。

PKI 系统的文档中应明确规定终端用户密钥存储方法。

5.5.9.5 密钥备份

5.5.9.5.1 PKI 系统密钥备份

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国家密码行政管理部门认可的硬件密码设备中。

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备份于国家密码行政管理部门认可的硬件密码设备中，且各部件应分散存放于安全可信的环境中，并进行访问控制，只有特定权限的人才能访问私钥信息存放部件。只有在必要时，多个特定权限的人采用多个部件同时使用备份私钥信息恢复 CA 签名私钥。

PKI 系统密钥备份应采用热备份、冷备份和异地备份等措施。

PKI 系统的文档中应明确规定系统密钥备份方法。

5.5.9.5.2 终端用户密钥备份

用户签名私钥可由用户自行备份。用户用于机密性目的的密钥可由 PKI 服务机构提供备份服务或由用户自行备份。

如果由 PKI 系统备份，应由国家密码行政管理部门认可的硬件密码设备加密后备份。如果用户自行备份，应以加密的形式备份于国家密码行政管理部门认可的硬件密码设备中。

终端用户密钥备份应采用热备份、冷备份和异地备份等措施。

PKI 系统的文档中应明确规定终端用户密钥备份方法。

5.5.9.6 密钥导入导出

密钥被导出到 PKI 系统之外可能基于以下的原因：密钥备份、复制，以及将 PKI 系统部件产生的

密钥传送到用户手中。

密钥导入或导出 PKI 系统时，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 系统用户密钥、系统部件密钥和终端用户密钥应由国家密码行政管理部门认可的硬件密码设备加密**，CA 签名私钥应使用硬件密码设备加密并进行知识分割。

PKI 系统应提供合适的方法把导入或导出 PKI 系统的对称密钥、私有密钥或公有密钥与正确实体相关联，并赋予相应的权限，其中实体可能是一个人、一个组或一个过程。

PKI 系统的文档中应明确规定密钥导入导出方法。

5.5.9.7 密钥更新

5.5.9.7.1 PKI 系统密钥更新

当 CA 签名密钥过期，或者 CA 签名私钥的安全性受到威胁时，带来了 CA 密钥和证书更新的问题。PKI 系统应提供有效的 CA 私钥及证书更新方式。要求：

a) 新密钥对的产生应符合 5.5.9.1 中的规定；

b) 新的 CA 公钥的分发应符合 5.5.9.2 中的规定；

c) 旧的 CA 公钥的归档应符合 5.5.9.9 中的规定；

d) 旧的 CA 私钥的销毁应符合 5.5.9.10 中的规定；

e) 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，防止例如替换CA私钥和证书等的各种攻击行为；

f) PKI系统的文档中，应说明CA密钥及证书的更新方法；并确保CA密钥及证书更新时，严格按照文档中规定的方法操作。

5.5.9.7.2 用户密钥更新

用户密钥对过期或者私钥的安全性受到威胁时应更新密钥。用户密钥可由 PKI 系统自动更新，也可手工更新。要求：

a) 新密钥对的产生应符合 5.5.9.1 中的规定；

b) 新的用户公钥的分发应符合 5.5.9.2 中的规定；

c) 旧的用户公钥的归档应符合 5.5.9.10 中的规定；

d) 旧的用户私钥的销毁应符合 5.5.9.11 中的规定；

e) 如果用户密钥由PKI系统自动更新，则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，防止例如替换用户私钥和证书等的各种攻击行为；

f) 如果用户密钥由PKI系统自动更新，则PKI系统的文档中，应说明用户密钥及证书的更新方法；并确保用户密钥及证书更新时，严格按照文档中规定的方法操作。

5.5.9.8 密钥恢复

5.5.9.8.1 PKI 系统密钥恢复

对因密钥备份或密钥归档等不同原因存储在 PKI 系统中的密钥，在恢复时，应有不同的条件。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。

PKI 系统密钥恢复应保证密钥不被未授权的泄露或修改，恢复过程中密钥应以加密形式存在。

CA 签名私钥恢复需要多个被授权的人同时使用存有密钥信息的部件，在安全可信的环境中恢复，**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它分布式方案存放，恢复过程不应危及密钥信息的安全性，不应暴露签名私钥。

PKI 系统的文档中应明确规定系统密钥恢复方法。

5.5.9.8.2 终端用户密钥恢复

终端用户密钥恢复应保证密钥不被未授权的泄露或修改，恢复过程中密钥应以加密形式存在。

PKI 系统的文档中应明确规定终端用户密钥恢复方法。

5.5.9.9 密钥归档

5.5.9.9.1 私钥归档

私钥归档中区分用于签名的私钥和用于解密数据的私钥。

签名私钥是不允许被归档的，用于解密数据的私钥允许被归档。

私钥归档如备份一样也保存一份私钥的拷贝，但用于不同的目的。备份用于系统运作的连续性，以防意外事故造成的私钥损坏、丢失、删除等。而归档用于长期的、将来为解密历史数据提供服务。

PKI 系统的文档中应明确规定私钥归档方法。

5.5.9.9.2 公钥归档

CA、RA、终端用户或其它系统部件的公钥都应归档，归档公钥为数字证书从目录中移除后验证数字签名提供了便利。

PKI 系统的文档中应明确规定公钥归档方法。

5.5.9.10 密钥销毁

5.5.9.10.1 PKI 系统密钥销毁

PKI 系统的密钥销毁应设置为只有特定权限的人才能执行销毁程序，并保证销毁过程应是不可逆的。CA 签名私钥的密钥销毁应设置为需要多个管理员同时在场，执行多道销毁程序。PKI 系统提供的销毁程序可包括：用随机数据覆盖存储密钥的媒介、存储体，销毁存储密钥的媒介等。PKI 系统密钥销毁应符合国家密码行政管理部门对密钥销毁的相关规定。

PKI 系统的文档中应明确规定系统密钥销毁方法。

5.5.9.10.2 用户密钥销毁

终端用户密钥的销毁由用户自己执行多道销毁程序，并保证销毁过程应是不可逆的。用户可执行的销毁程序包括：用随机数据覆盖存储密钥的媒介、存储体，销毁存储密钥的媒介等。

PKI 系统的文档中应明确规定用户密钥销毁方法。

5.5.10 轮廓管理

5.5.10.1 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 标准相一致。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。

PKI 系统管理员还应为以下的字段和扩展指定可能的取值：

a) keyUsage；
b) basicConstraints；

c) certificatePolicies。

管理员还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

证书撤消列表轮廓用于定义 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 标准相一致。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；

c) NextUpdate。

若 PKI 系统发布 CRL，管理员还应指定 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

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。

5.5.11 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系统自动的生成；

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。

5.5.11.2 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。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。

5.5.11.2.2 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。

5.5.12 配置管理

应按 **GB/T 20271-2006 中 6.5.5.1** 的要求，从以下方面实现 PKI 系统的配置管理：

a） 在配置管理自动化方面要求**完全的配置管理自动化**；

b） 在配置管理能力方面应实现生成支持和验收过程的要求；

c） 在PKI系统的配置管理范围方面，应将PKI系统的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下，要求实现对开发工具配置管理范围的管理；

d） 在系统的整个生存期，即在它的开发、测试和维护期间，应有一个软件配置管理系统处于保持对改变源码和文件的控制状态。只有被授权的代码和代码修改才允许被加进已交付的源码的基本部分。所有改变应被记载和检查，以确保未危及系统的安全。在软件配置管理系统中，应包含从源码产生出系统新版本、鉴定新生成的系统版本和保护源码免遭未授权修改的工具和规程。通过技术、物理和保安规章三方面的结合，可充分保护生成系统所用到的源码免遭未授权的修改和毁坏。

5.5.13 分发和操作

应按 **GB/T 20271-2006 中 6.5.5.2** 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、启动和修改检测的过程进行说明，最终生成安全的配置。文档中所描述的内容应包括：

——提供分发的过程；

——安全启动和操作的过程；

——建立日志的过程；

——修改内容的检测；

——对任何安全加强功能在启动、正常操作维护时能被撤消或修改的阐述；

——在故障或硬件、软件出错后恢复系统至安全状态的规程；

——对含有加强安全性的硬件部件，应说明用户或自动的诊断测试的操作环境和使用方法；

——所有诊断测试过程中，为加强安全性的硬件部件所提供例证的结果；

——在启动和操作时产生审计踪迹输出的例证。

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；

f) 以安全方式开发并交付系统后，仍应提供对产品的长期维护和评估的支持，包括产品中的安全漏洞和现场问题的解决；

g) 应采用书面说明的方式向客户通告新的安全问题；

h) 对可能受到威胁的所有的安全问题，均应描述其特点，并作为主要的问题对待，直到它被解决；

i) 为了支持已交付的软件的每个版本，对所有已有的安全漏洞都应有文档书面说明，并且客户能在限制的基础上得到该文档；

j) 对安全漏洞的修改不必等到系统升级到下一个版本。安全功能的增加和改进应独立于系统版本的升级，也就是说，应存在适应性独立于系统其它功能的改进；

k) 只有经过客户授权，才允许在生产性运行的系统上进行新特性和简易原型的开发、测试和安装；

l) 新的版本应避免违反最初的安全策略和设想，也应避免在维护、增加或功能升级中引入安全漏洞，所有功能的改变和安全结构设置的默认值都应作记录。在新版本交付给客户使用前，客户应能得到相应的文档。

5.5.14 开发

应按 **GB/T 20271-2006 中 6.5.5.3** 的要求，从以下方面进行 PKI 系统的开发：

a) 按**形式化的**TCB**安全策略模型、形式化功能说明、形式化高层设计**、TSF的结构化实现、TSF内部结构复杂度最小化、**形式化低层设计、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；

f) 在PKI系统开发的敏感阶段，应保持一个安全环境，该安全环境要求：

——描述PKI系统开发所使用的计算机系统的安全使用和维护情况的安全策略和措施应有书面记载，并可供检查；

——系统开发过程中使用的所有计算机系统应接受定期的和有书面记载的内部安全审计，描述审计过程的文件和真实的审计报告应可供检查；

——除授权的分发机构外，不应在开发环境外部复制或分发内部文档；

——开发环境的计算机系统使用的所有软件应合法地从确定的渠道获得；

——开发者个人独自开发的软件，应在被开发管理者审核后才能用于开发的系统。

5.5.15 指导性文档

应按 **GB/T 20271-2006 中 6.5.5.4** 的要求，从以下方面编制 PKI 系统的指导性文档：

a) 应通过提供指导性文档，将如何安全使用和维护PKI系统的信息交付给系统的终端用户和系统用户。对文档的总体要求是：

——应对所有的安全访问和相关过程、特权、功能等适当的管理加以阐述；

——应阐述安全管理和安全服务的交互，并提供指导；

——应详细给出每种审计事件的审计记录的结构，以便考察和维护审计文件和进程；

——应提供一个准则集用于保证附加的说明的一致性不受破坏。

b) 系统用户文档应提供系统用户了解如何用安全的方式管理系统，除了给出一般的安全忠告，还要明确：

——在系统用安全的方法设置时，围绕管理员、操作员、审计员和安全员、主体和客体的属性等，应如何安装或终止安装；

——在系统的生命周期内如何用安全的方法维护系统，包括为了防止系统被破坏而进行的每天、每周、每月的安全常规备份等；

——如何用安全的方法重建PKI系统的方法；

——说明审计跟踪机制，使系统用户可有效地使用审计跟踪来执行本地的安全策略；

——必要时，如何调整系统的安全默认配置。

c) 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；

d) 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；

e) 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；

f) 应提供关于所有审计工具的文档，包括为检查和保持审计文件所推荐的过程、针对每种审计事件的详细审计记录文件、为周期性备份和删除审计记录所推荐的过程等；

g) 应提供如何进行系统自我评估的章节（带有网络管理、口令要求、意外事故计划的安全报告）和为灾害恢复计划所做的建议，以及描述普通侵入技术和其它威胁，并查出和阻止入侵的方法。

5.5.16 生命周期支持

应按 **GB/T 20271-2006 中 6.5.5.5** 的要求，从以下方面实现 PKI 系统的生命周期支持：

a) 按**可测量的生命周期模型和遵照实现标准-所有部分的工具和技术的要求**进行开发，并提供充分的安全措施；

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消或修改，说明在故障或系统出错时如何恢复系统至安全状态；

c) 如果系统含有加强安全性的硬件，那么管理员、其他用户或自动的诊断测试，应能在各自的操作环境中运行它并详细说明操作过程。

5.5.17 测试

应按 **GB/T 20271-2006 中 6.5.5.6** 的要求，从以下方面对 PKI 系统进行测试：

a) 应通过测试范围证据和严格的范围分析、高层设计测试、低层设计测试和实现表示测试、顺序的功能测试、相符独立性测试、抽样性独立测试和**完全独立性测试**等，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，包括查找漏洞，如违反系统访问控制要求、违反资源访问控制要求、拒绝服务、对审计或验证数据进行未授权访问等。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。

5.5.18 脆弱性评定

应按 GB/T 20271-2006 中 6.5.5.7 的要求，从以下方面对所开发的 PKI 系统进行脆弱性评定：

a) **系统化的隐蔽信道分析**；
b) 安全状态的检查和分析；
c) PKI系统安全功能强度评估；
d) 开发者脆弱性分析；
e) 独立脆弱性分析；
f) **高级抵抗力分析**。

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 安全要素要求级别划分

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	+	+	+	+	+
配置管理	+	++	+++	++++	+++++
分发和操作	+	++	+++	++++	+++++
开发	+	++	+++	++++	+++++
指导性文档	+	++	+++	++++	+++++
生命周期支持	+	++	+++	++++	+++++
测试	+	++	+++	++++	+++++
脆弱性评定		+	++	+++	++++

注：“+”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 Part1:Introduction and general model Part 1:Introduction and general model，Version 2.0

[2] ISO/IEC 15408-2：1999 Information technology—Security techniques—Evaluation Criteria for IT Security Part2:Security functional requirements Part2:Security functional requirements，Version 2.0

[3] ISO/IEC 15408-3：1999 Information technology—Security techniques—Evaluation Criteria for IT Security Part3:Security assurance requirements Part3:Security assurance requirements，Version 2.0

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