ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 21053—XXXX

信息安全技术 公钥基础设施 PKI 系统安全技术要求

Information security technques—Public key infrastructure—Security technology requirement for PKI system

（征求意见稿）

（本稿完成日期：2021 年 8 月 6 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－　－　实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 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》。与 GB/T 21053-2007 相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 将名称修改为《信息安全技术 公钥基础设施 PKI 系统安全技术要求》，本文件规定了 PKI 系统产品的等级及相应等级的安全技术要求。

b) 增加了 5 概述，对 PKI 系统的基本框架和本文件规定的 PKI 系统的安全等级进行了概述；

c) 根据系统产品安全技术要求相关标准的写作惯例，将原有 5.1 至 5.5 的内容调整至 6 基本级要求和 7 增强级要求；

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：中国科学院软件研究所、中国科学院大学、公安部第三研究所、成都卫士通信息产业股份有限公司、北京信安世纪科技有限公司、北京数字认证股份有限公司、长春吉大正元信息技术股份有限公司、北京百度网讯科技有限公司、北京创原天地科技有限公司、北京奇虎科技有限公司、北京中电华大电子设计有限责任公司、格尔软件股份有限公司、公安部第一研究所、国网区块链科技（北京）有限公司、华为技术有限公司、天津南大通用数据技术股份有限公司、郑州信大捷安信息技术股份有限公司、中国汽车工程研究院股份有限公司、中国信息通信研究院。

本文件主要起草人：张立武、张严、顾健、陈妍、邱梓华、刘丽敏、张立廷、汪宗斌、傅大鹏、王榕、李健、郑强、张屹、董晶晶。

本文件及其所替代的文件的历次版本发布情况为：

——GB/T 21053-2007。

信息安全技术 公钥基础设施 PKI 系统安全技术要求

1 范围

本文件提出了PKI系统产品的安全等级划分，并给出了相应安全等级PKI系统产品的安全功能要求和安全保障要求。

本文件适用于 PKI 系统产品的测试和评估，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

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

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

GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求

GB/T 20518-2018 信息安全技术 公钥基础设施 数字证书格式

GB/T 20984-2007 信息安全技术 信息安全风险评估规范

GB/T 21052-2007 信息安全技术 信息系统物理安全技术要求

GB/T 25056-2018 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GM/T 0014-2012 数字证书认证 系统密码协议规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

公钥基础设施 public key infrastructure

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。

[GB/T 20518-2018 3.1]

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

拆分知识 split knowledge

一种密钥保存方法，由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。

注：拆分知识方法可以是门限式的，即当获取了拆分保存的N个部分密钥中的M个部分（M<N）时，即可得到密钥的全部信息，但对于任何少于M个部分密钥信息，都无法从中恢复密钥的明文。

3.4

拆分知识过程 split knowledge procedure

用来实现拆分知识的过程。

3.5

关键性扩展 critical extension

证书或CRL中不能被忽略的扩展项，证书或CRL的应用系统如果不能识别关键性扩展时，应拒绝接受该证书或CRL。

3.6

审计踪迹 audit trail

记录一系列审计信息和事件的日志。

3.7

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。例如：管理员、审计员、操作员等。

3.8

终端用户 terminal user

使用PKI系统所提供服务的远程普通用户。

3.9

PKI 系统部件密钥 PKI system component key

由PKI系统中各部件使用的密钥。

3.10

系统密钥 system key

PKI系统部件密钥和PKI系统的系统用户使用的密钥。

4 缩略语

下列缩略语适用于本文件。

CA：认证机构(Certification Authority)
CRL：证书撤销列表(Certificate Revocation List)
OCSP：在线证书状态协议(Online Certificate Status Protocol)
PKI：公钥基础设施(Public Key Infrastructur)
RA：注册机构(Registration Authority)

5 概述

5.1 PKI 系统框架

本文件规定的PKI系统的基本框架如图1所示，主要包括CA、RA和证书资料库等基本逻辑部件和OCSP等可选服务部件。其中：

——RA 与终端用户进行交互，接收证书请求，并将证书请求发送给 CA 部件。当 CA 完成证书签发后，RA 将签发后的终端用户证书及 CA 证书等发送给终端用户；
——CA 根据证书请求和 CRL 请求，签发对应的证书和 CRL，并将证书和 CRL 存储至证书资料库；
——证书资料库提供证书和 CRL 的存储和查询等服务；
——密钥管理中心提供 PKI 系统中各类密钥的管理功能；
——如果 PKI 系统支持 OCSP 功能，则还应具备 OCSP 服务部件，实现 OCSP 请求的接收和响应。

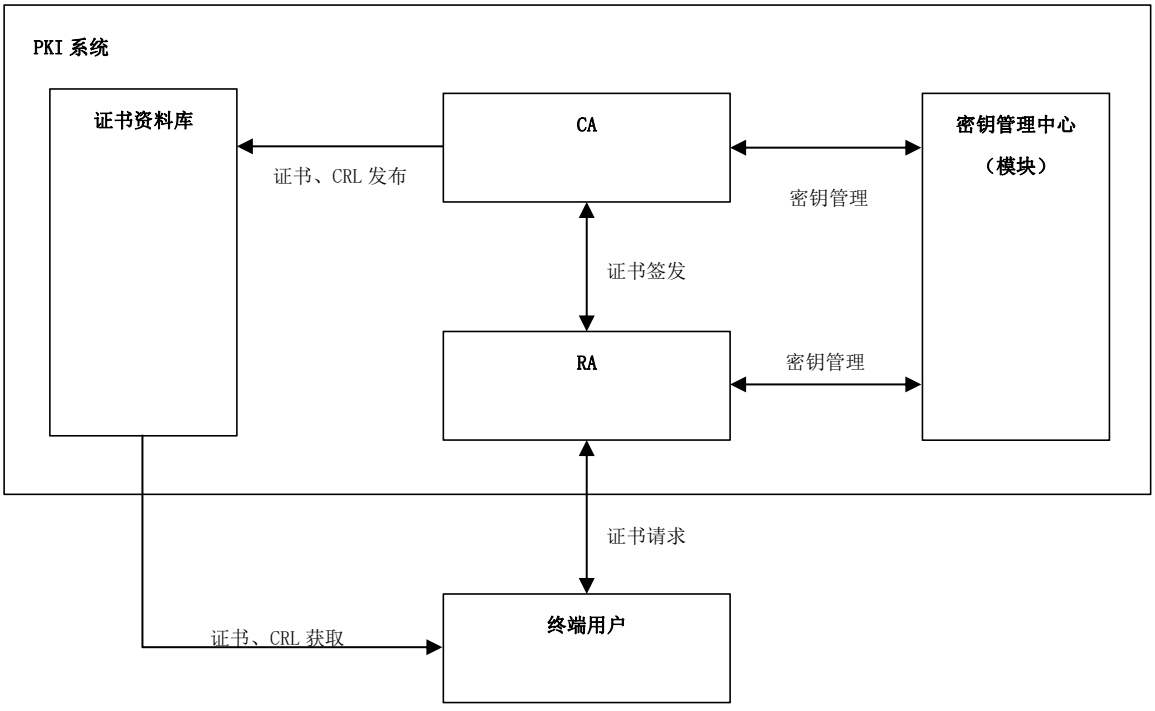

图 1 PKI 系统框架

关于PKI系统各部件的功能和事务描述，参见GB/T 19771-2005。

5.2 PKI 系统安全级别划分

本文件规定的PKI系统的安全级别包括基本级和增强级，安全功能的强弱以及安全保障要求的高低是等级划分的具体依据。对于基本级的PKI系统，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。对于增强级的PKI系统，PKI系统的CA、RA和证书资料库都应独立设计。

基本级的PKI系统产品适用于基于GB 17859-1999的第二级系统中的PKI系统的安全性测评，增强级的PKI系统产品适用于基于GB 17859-1999的第三级、第四级系统中的PKI系统的安全性测评。在安全要求上，基本级与GB/T 21053-2007中第二级基本对应，增强级与GB/T 21053-2007中第三级基本对应。

6 基本级安全要求

6.1 安全功能要求

6.1.1 密钥管理通用要求

6.1.1.1 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。如果PKI系统支持密钥导入导出，应提供密钥导入导出功能。并遵循以下要求：

a) 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。
b) PKI 系统的各类私钥不应以明文形式导入导出 PKI 系统。
c) 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。

6.1.2 PKI 系统密钥管理

6.1.2.1 PKI 系统密钥生成

PKI系统应提供系统密钥生成功能，并遵循以下要求：

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。

6.1.2.2 PKI 系统密钥传送与分发

PKI系统应提供系统密钥传送与分发功能，并遵循以下要求：

a) 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。
b) 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。
c) 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，例如：通过嵌入应用软件、使用安全信道传递、手工传递等方法分发。

6.1.3 用户密钥管理

6.1.3.1 终端用户密钥传送与分发

PKI系统应提供终端用户密钥传送与分发功能，并遵循以下要求：

a) 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，PKI 系统应实现终端密钥传送与分发功能来实现终端用户向 CA 的安全密钥提交。终端用户应将公钥安全地提交给 CA，如使用证书载体等方法进行面对面传送。

b) 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，PKI系统应实现终端密钥传送与分发功能来实现CA向终端用户的安全密钥分发。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。

6.1.4 轮廓管理

6.1.4.1 证书轮廓管理

PKI系统应具备证书轮廓，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 20518-2018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。
e) keyUsage；
f) basicConstraints；
g) certificatePolicies。

管理员还应为证书扩展指定可能的值。

6.1.4.2 证书撤销列表轮廓管理

若PKI系统发布CRL，则应具备证书撤销列表轮廓，证书撤销列表轮廓用于定义CRL中字段和扩展中可接受的值，这些字段和扩展应与GB/T 20518-2018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。

PKI系统发布CRL时，应保证发布的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。

6.1.4.3 在线证书状态协议轮廓管理

若PKI系统发布OCSP响应，应遵循以下要求：

a) 若 PKI 系统发布 OCSP 响应，PKI 系统应具备 OCSP 轮廓。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。
b) PKI 系统发布 OCSP 响应时，PKI 系统应保证 OCSP 响应与轮廓一致；
c) 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；
d) 若 PKI 系统允许使用基本相应类型（basic response type）的 OCSP 响应，则 PKI 系统管理员应为 ResponderID 指定可接受的值。

6.1.5 证书管理

6.1.5.1 证书注册

PKI系统所签发的公钥证书的格式应符合GB/T 20518-2018中的规定。任何证书所包含的字段或扩展应被PKI系统根据GB/T 20518-2018生成或由颁发机构验证以保证其与标准的一致性。

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

a) 数据被操作员手工批准；
b) 自动过程检查和批准数据；
c) 字段或扩展的值由 PKI 系统自动生成；
d) 字段或扩展的值从证书轮廓中获得。

进行证书生成时：

a) 应仅产生与 GB/T 20518-2018 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 系统应保证所生成的数字证书满足以下要求：
   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 字段在 CA 系统内应是全局唯一的；
   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。

6.1.5.2 证书撤销

6.1.5.2.1 证书撤销列表审核

发布CRL的PKI系统应提供CRL验证功能，验证CRL的所有强制性字段的值符合GB/T 20518-2018。并至少进行以下字段的审核：

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) signature 和 signatureAlgorithm 字段应为许可的数字签名算法的 OID；
d) thisUpdate 应包含本次 CRL 的发布时间；

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

6.1.5.2.2 OCSP 基本响应的审核

发布OCSP响应的PKI系统应提供OCSP响应验证功能，验证OCSP响应所有强制性字段的值符合GM/T 0014-2012 5.6中的规定。并至少进行以下字段的审核：

a) version 字段应为 0；
b) signatureAlgorithm 字段应为许可的数字签名算法的 OID；
c) thisUpdate 字段应指出证书状态正确的时间；
d) producedAt 字段应指出 OCSP 响应者发出响应的时间；
e) nextUpdate 字段的时间不应早于 thisUpdate 字段的时间。

6.1.6 身份鉴别

6.1.6.1 用户属性定义

PKI系统应提供安全属性维护功能，实现对每个用户安全属性的维护。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。

6.1.6.2 用户身份鉴别

PKI系统应在用户身份鉴别方面遵循以下要求：

a) PKI 系统应预先设定 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：
   1) 响应查询公开信息（如：在线证书状态查询等）；
   2) 接收用户发来的数据，但直到系统用户批准之后才处理。
b) PKI 系统应定义其所支持的用户鉴别机制的类型。
c) 当进行用户鉴别时，PKI 系统的安全功能应仅仅将最少的反馈提供给用户，并避免泄露用户的鉴别数据。例如：当用户进行口令字符输入时，应只显示星号，而不显示原始字符；对于鉴别结果仅显示鉴别的成功或失败，等等。

6.1.6.3 鉴别失败处理

PKI系统应在鉴别失败处理方面遵循以下要求：

a) PKI 系统应实现鉴别失败次数检测功能，当用户自最近一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够检测到。
b) PKI 系统应提供鉴别失败检测参数配置功能。管理员可配置的参数包括：失败的鉴别次数和失效时间值等。

6.1.7 访问控制

6.1.7.1 角色与责任

PKI系统应在角色与责任方面遵循以下要求：

a) PKI 系统开发者应依据以下责任分配提供 PKI 系统的管理员、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

操作员：签发和撤销证书。

b) PKI 系统应提供主体与角色关联功能，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。

c） 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
数据输入和输出	私钥输出应由管理员执行，其余数据的输入输出应由系统用户执行
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助过程和相关信息。
PKI系统配置	对于PKI系统功能的任何配置权应仅授予管理员。（除了在本标准中其他地方所定义的分配给其他角色的TSF功能，这一要求应用于所有的配置变量。）
证书轮廓管理	更改证书轮廓的权限应仅授予管理员。
撤销轮廓管理	更改撤销轮廓的权限应仅授予管理员。
证书撤销列表轮廓管理	更改证书撤销列表轮廓的权限应仅授予管理员。
在线证书状态查询轮廓管理	更改在线证书状态查询轮廓的权限应仅授予管理员。

6.1.7.2　系统用户访问控制

PKI系统应在系统用户访问控制方面遵循以下要求：

a） PKI 系统应提供用户注册、注销及口令分配功能，为用户分配或者使用系统特权时，应对该操作进行严格的限制和控制。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。

b） PKI 系统应实现系统用户访问控制功能，访问控制权限的分配应依据表 2；

c） PKI 系统应在文档中提供访问控制的相关文档，访问控制文档中的应包含如下几个方面内容：

1） 角色及其相应的访问权限

应提供角色及其相应的访问权限的说明，角色及其相应的访问权限的分配应与表 2 一致。

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证书撤销的主体所完成。
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。

表 2 角色及其相应的访问权限（续）

私钥和对称密钥销毁	仅管理员有权产生将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。

2） 标识与鉴别系统用户的过程

应提供标识与鉴别系统用户的过程，该过程应符合 7.1.1 的要求。

3） 角色的职能分割

应提供角色职能分割的说明，职能分割应符合 7.1.3 的要求。

6.1.7.3 网络访问控制

PKI系统应在网络访问控制方面遵循以下要求：

a） PKI 系统应具备网络访问控制能力。使得用户进行远程访问时，远程用户只有通过鉴别后，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。

b） 远程计算机系统与 PKI 系统的连接应被鉴别，鉴别方法使用的凭据可包括计算机地址、访问时间、拥有的密钥等等。

c） PKI 系统应具备网络访问控制策略配置能力。

d） PKI 系统应对诊断分析端口的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。

6.1.8 安全审计

6.1.8.1 审计数据产生

PKI系统应在审计数据产生方面遵循以下要求：

a） PKI 系统应通过审计功能部件实现审计数据产生功能，审计数据产生功能应对下列事件产生审计记录：

1） 审计功能的启动和结束；

2） 表 3 中列出的事件。

表 3 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操作	
	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	若输入的数据与其他数据相关，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（成果或失败）。
PKI系统部件的配置	所有与安全相关的对于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。

b) 对于每一个事件，审计数据产生功能生成的审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，以及**表 3** 中附加信息栏中要求的内容。

c) 审计数据产生功能生成的审计记录中不应出现明文形式的私钥、对称密钥和其他安全相关的参数。

d) 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。

6.1.8.2 审计查阅

a) 审计功能部件应为审计员提供查看所有日志信息的能力。

b) 审计功能部件应以适于阅读和解释的方式向读者提供日志信息。

6.1.8.3 选择性审计查阅

审计功能部件应实现选择性审计查阅功能，使得管理员在查阅审计日志时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。

6.1.8.4 审计事件存储

审计功能部件在存储审计记录时，应具备以下能力：

a) 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) 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，以防止审计数据丢失。

6.1.9 备份和恢复

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他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。

6.2 安全保障要求

6.2.1 开发

6.2.1.1 安全架构

开发者应提供产品安全功能的安全架构描述，安全架构描述应与产品设计文档中对安全功能的描述范围相一致。

6.2.1.2 功能规范

开发者应提供完备的功能规范说明，功能规范说明应满足以下要求：

a) 清晰描述 7.1、7.2 章中定义的安全功能；
b) 提供部件和安全功能接口间的对应关系；
c) 通过实现模块描述安全功能，标识和描述实现模块的目的、相关接口及返回值等，并描述实现模块间的相互作用及调用的接口；
d) 提供实现模块和子系统间的对应关系。

6.2.1.3 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求：

a) 通过子系统描述产品结构，标识和描述产品安全功能的所有子系统，并描述子系统间的相互 作用；
b) 提供子系统和安全功能接口间的对应关系；

6.2.2 指导性文档

6.2.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，对每一种用户角色的描述应满足以下要求：

a) 描述用户能访问的功能和特权，包含适当的警示信息；
b) 描述产品安全功能及接口的用户操作方法，包括配置参数的安全值等；
c) 标识和描述产品运行的所有可能状态，包括操作导致的失败或者操作性错误；
d) 描述实现产品安全目的必需执行的安全策略。

6.2.2.2 准备程序

开发者应提供产品及其准备程序，准备程序描述应满足以下要求：

a) 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b) 描述安全安装产品及其运行环境必需的所有步骤。

6.2.3 生命周期支持

6.2.3.1 配置管理能力

开发者的配置管理能力应满足以下要求:

a) 为产品的不同版本提供唯一的标识;
b) 使用配置管理系统对组成产品的所有配置项进行维护,并进行唯一标识;
c) 提供配置管理文档,配置管理文档描述用于唯一标识配置项的方法;

6.2.3.2 配置管理范围

开发者应提供产品配置项列表,并说明配置项的开发者。配置项列表应包含以下内容:

a) 产品及其组成部分、安全保障要求的评估证据;

6.2.3.3 交付程序

开发者应使用一定的交付程序交付产品,并将交付过程文档化。在给用户方交付产品的各版本时,交付文档应描述为维护安全所必需的所有程序。

6.2.4 测试

6.2.4.1 测试覆盖

开发者应提供测试覆盖文档,测试覆盖描述应满足以下要求:

a) 表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性;

6.2.4.2 功能测试

开发者应测试产品安全功能,将结果文档化并提供测试文档。测试文档应包括以下内容:

a) 测试计划,标识要执行的测试,并描述执行每个测试的方案,这些方案包括对于其他测试结果的任何顺序依赖性;
b) 预期的测试结果,表明测试成功后的预期输出;
c) 实际测试结果和预期的测试结果的对比。

6.2.4.3 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源,以用于安全功能的抽样测试。

6.2.5 脆弱性评定

基于已标识的潜在脆弱性,产品能抵抗具有**基本攻击潜力**的攻击者的攻击。

6.2.6 代码安全

开发者应采用代码审计等方式，对PKI系统进行安全性测试并提供相关测试文档，确保PKI系统的代码安全。

7 增强级安全要求

7.1 安全功能要求

7.1.1 密钥管理通用要求

7.1.1.1 密钥有效期设置

PKI系统应具备密钥有效期设置能力，并遵循以下要求：

a) **PKI 系统在生成系统密钥和终端用户密钥时应为密钥设置有效期，有效期的设置应考虑以下因素：**
   1) **密钥长度；**
   2) **加密算法的攻击难度；**
   3) **加密对象的价值；**
   4) **合同或者法律等外部环境的需求；**
b) **密钥有效期的设定应符合国家密码行政管理部门相关规定。**

7.1.1.2 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。如果PKI系统支持密钥导入导出，应提供密钥导入导出功能。

a) PKI 系统的密钥导入导出应遵循以下要求：
   1) 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。
   2) PKI 系统的各类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。**
   3) 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。
b) **PKI 系统的文档中应明确说明是否支持密钥导入导出，如果支持，应明确规定密钥导入导出方法。**

7.1.1.3 密钥归档

7.1.1.3.1 私钥归档

PKI系统应具备私钥归档能力，对需要被归档的私钥进行归档。并遵循以下要求：

a) **PKI 系统在私钥归档中应区分用于签名的私钥和用于解密数据的私钥。签名私钥不应被归档，仅用于解密数据的私钥可被归档。**

注：私钥归档与备份类似，同样保存一份私钥的拷贝，但用于不同的目的。备份用于保证系统运作的连续性，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。

b) **PKI 系统的文档中应明确规定私钥归档方法。**

7.1.1.3.2 公钥归档

PKI 系统应具备公钥归档能力，并遵循以下要求：

a) **PKI 系统应确保 CA、RA、终端用户或其他系统部件的公钥能够被归档，以支持在数字证书从目录中移除后验证数字签名。**
b) **PKI 系统的文档中应明确规定公钥归档方法。**

7.1.2 PKI 系统密钥管理

7.1.2.1 PKI 系统密钥生成

PKI系统应提供系统密钥生成功能，并遵循以下要求：

a) 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并确保密钥生成环境的安全可信；
b) CA 签名公私钥对应采用国家行政管理部门认可在硬件密码设备中生成；
c) 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，且应有多于一个管理员同时在场；
d) 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；
e) 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；
f) 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；
g) 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；
h) 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；
i) PKI 系统的文档中应明确规定系统密钥生成方法。

7.1.2.2 PKI 系统密钥传送与分发

PKI系统应提供系统密钥传送与分发功能，并遵循以下要求：
a) 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。
b) 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。
c) 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，例如：通过嵌入应用软件、使用安全信道传递、手工传递等方法分发。

7.1.2.3 PKI 系统密钥存储

PKI 系统应提供系统密钥存储功能，并遵循以下要求：
a) 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 系统部件密钥应存储于国家密码行政管理部门认可的硬件密码中。CA 签名公私钥对应采用分隔知识方法或其它分布存储方案以密文形式存储于专门的硬件密码模块中,且各模块应物理分散存放。
b) PKI 系统的文档中应明确规定系统密钥存储方法。

7.1.2.4 PKI 系统密钥备份

PKI系统应提供系统密钥备份功能，对PKI系统部件密钥和系统用户密钥备份，并遵循以下要求：
a) 备份的系统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后存储。
b) 对于 CA 签名私钥备份，应以加密的形式存储，并对存放部件进行访问控制，只有特定权限的人才能访问私钥信息存放部件。
c) PKI 系统的文档中应明确规定系统密钥备份方法。

7.1.2.5 PKI 系统密钥更新

PKI系统应具备有效的CA私钥及证书更新能力。当CA签名密钥过期，或者CA签名私钥的安全性受到威胁时，对CA密钥和证书进行更新，并遵循以下要求：

a) 新密钥对的产生应符合 7.1.2.1 中 CA 密钥对产生的规定。
b) 新的 CA 公钥的分发应符合 7.1.2.2 中 CA 公钥分发的规定。
c) 旧的 CA 公钥的归档应符合 7.1.1.3 中 CA 密钥归档的规定。
d) 旧的 CA 私钥的销毁应符合 7.1.2.7 中 CA 密钥销毁的规定。
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。

7.1.2.6 PKI 系统密钥恢复

PKI系统应具备系统密钥恢复能力，并遵循以下要求：

a) 对于因备份存储的密钥，应仅由密钥所有者恢复；
b) 对于因归档存储的密钥，则应根据法律、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。
c) PKI 系统在密钥恢复过程中应保证密钥以密文形式存在，且无法被未授权地泄露或修改。
d) 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拆分知识过程或其他分布式方案存放，恢复过程不应危及密钥信息的安全性，不应暴露签名私钥。
e) PKI 系统的文档中应明确规定系统密钥恢复方法。

7.1.2.7 PKI 系统密钥销毁

PKI系统应具备系统密钥销毁能力，并遵循以下要求：

a) PKI 系统的密钥销毁应设置为只允许具有特定权限的人才能执行，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 系统密钥销毁方法应符合国家密码行政管理部门对密钥销毁的相关规定。
b) PKI 系统文档中应明确规定系统密钥销毁方法。

7.1.3 用户密钥管理

7.1.3.1 终端用户密钥生成

PKI系统应提供终端用户密钥生成功能，并遵循以下要求：

a) 终端用户签名私钥应由其自己生成；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。
b) 终端用户自己生成密钥时，PKI 系统应提供终端用户密钥生成机制，确保采用国家密码行政管理部门认可的硬件设备生成。
c) PKI 系统的文档中应明确规定终端用户密钥生成方法。

7.1.3.2 终端用户密钥传送与分发

PKI系统应提供终端用户密钥传送与分发功能，并遵循以下要求：

a) 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，PKI 系统应实现终端密钥传送与分发功能来实现终端用户向 CA 的安全密钥提交。终端用户应将公钥安全地提交给 CA，如使用证书载体等方法进行面对面传送。
b) 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，PKI 系统应实现终端密钥传送与分发功能来实现 CA 向终端用户的安全密钥分发。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。
c) PKI 系统的文档中应明确规定用户密钥传送方法。

7.1.3.3 终端用户密钥存储

PKI系统应提供终端用户密钥存储功能，并遵循以下要求：

a) 如果终端用户的密钥在 PKI 系统服务部件中存储，PKI 系统应提供终端用户密钥存储功能，可使用软件加密后存储在数据库中，如使用软件加密，加密算法应符合国家密码行政管理部门的规定。
b) PKI 系统的文档中应明确规定终端用户密钥存储方法。

7.1.3.4 终端用户密钥备份

PKI系统的用户签名私钥可由用户自行备份。用户用于实现机密性保护的密钥可由PKI服务机构提供备份服务或由用户自行备份。PKI系统的文档中应明确规定终端用户密钥备份方法。

如果终端用户密钥由PKI系统备份，PKI系统应提供终端用户密钥备份功能，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。

7.1.3.5 终端用户密钥更新

终端用户密钥更新指对对过期或者私钥的安全性受到威胁的终端用户密钥进行更新。终端用户密钥可由PKI系统通过提供更新功能进行自动更新，也可手工更新。如果PKI系统提供终端用户密钥更新功能，应遵循以下要求：

a) 新密钥对的产生应符合 7.1.3.1 中终端用户密钥对产生的规定。
b) 新的用户公钥的分发应符合 7.1.3.2 中终端用户公钥分发的规定。
c) 旧的用户公钥的归档应符合 7.1.1.3 中密钥归档的规定。
d) 旧的用户私钥的销毁应符合 7.1.3.7 中终端用户密钥销毁的规定。
e) 如果终端用户密钥由 PKI 系统自动更新，则 PKI 系统应采取明确的方法更新终端用户密钥及证书。在更新过程中应采取安全措施保证终端用户密钥和证书的安全，防止例如替换终端用户私钥和证书等的各种攻击行为。
f) 如果终端用户密钥由 PKI 系统自动更新，则 PKI 系统的文档中，应说明终端用户密钥及证书的更新方法；并确保终端用户密钥及证书更新时，严格按照文档中规定的方法操作。

7.1.3.6 终端用户密钥恢复

如果终端用户密钥由PKI系统备份，PKI系统应提供终端用户密钥恢复功能，并遵循以下要求：

a) 终端用户密钥恢复应保证密钥不被未授权地泄露或修改，恢复过程中密钥应以加密形式存在。
b) PKI 系统的文档中应明确规定终端用户密钥恢复方法。

7.1.3.7 终端用户密钥销毁

PKI系统文档中应明确规定终端用户密钥销毁方法。

7.1.4 轮廓管理

7.1.4.1 证书轮廓管理

PKI系统应具备证书轮廓，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 20518-2018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。
e) keyUsage；
f) basicConstraints；
g) certificatePolicies。

管理员还应为证书扩展指定可能的值。

7.1.4.2 证书撤销列表轮廓管理

若PKI系统发布CRL，则应具备证书撤销列表轮廓，证书撤销列表轮廓用于定义CRL中字段和扩展中可接受的值，这些字段和扩展应与GB/T 20518-2018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。

PKI系统发布CRL时，应保证发布的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，管理员应指定 CRL 和 CRL 扩展可接受的值。

7.1.4.3 在线证书状态协议轮廓管理

若PKI系统发布OCSP响应，应遵循以下要求：

a) 若 PKI 系统发布 OCSP 响应，PKI 系统应具备 OCSP 轮廓。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。
b) PKI 系统发布 OCSP 响应时，PKI 系统应保证 OCSP 响应与轮廓一致；

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

7.1.5 证书管理

7.1.5.1 证书注册

PKI系统所签发的公钥证书的格式应符合GB/T 20518-2018中的规定。任何证书所包含的字段或扩展应被PKI系统根据GB/T 20518-2018生成或由颁发机构验证以保证其与标准的一致性。

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

a) 数据被操作员手工批准；
b) 自动过程检查和批准数据；
c) 字段或扩展的值由 PKI 系统自动生成；
d) 字段或扩展的值从证书轮廓中获得。

进行证书生成时：

a) 应仅产生与 GB/T 20518-2018 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 系统应保证所生成的数字证书满足以下要求：
   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 字段在 CA 系统内应是全局唯一的；
   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。

7.1.5.2 证书撤销

7.1.5.2.1 证书撤销列表审核

发布CRL的PKI系统应提供CRL验证功能，验证CRL的所有强制性字段的值符合GB/T 20518-2018。并至少进行以下字段的审核：

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) signature 和 signatureAlgorithm 字段应为许可的数字签名算法的 OID；
d) thisUpdate 应包含本次 CRL 的发布时间；
e) nextUpdate 字段的时间不应早于 thisUpdate 字段的时间。

7.1.5.2.2 OCSP 基本响应的审核

发布OCSP响应的PKI系统应提供OCSP响应验证功能，验证OCSP响应所有强制性字段的值符合GM/T 0014-2012 5.6中的规定。并至少进行以下字段的审核：

a) version 字段应为 0；
b) signatureAlgorithm 字段应为许可的数字签名算法的 OID；
c) thisUpdate 字段应指出证书状态正确的时间；
d) producedAt 字段应指出 OCSP 响应者发出响应的时间；
e) nextUpdate 字段的时间不应早于 thisUpdate 字段的时间。

7.1.6 身份鉴别

7.1.6.1 用户属性定义

PKI系统应提供安全属性维护功能，实现对每个用户安全属性的维护。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。

7.1.6.2 用户身份鉴别

PKI系统应在用户身份鉴别方面遵循以下要求：

a) PKI 系统应预先设定 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：
   1) 响应查询公开信息（如：在线证书状态查询等）；
   2) 接收用户发来的数据，但直到系统用户批准之后才处理。
b) PKI 系统应定义其所支持的用户鉴别机制的类型。
c) 当进行用户鉴别时，PKI 系统的安全功能应仅仅将最少的反馈提供给用户，并避免泄露用户的鉴别数据。例如：当用户进行口令字符输入时，应只显示星号，而不显示原始字符；对于鉴别结果仅显示鉴别的成功或失败，等等。
d) **PKI 系统安全功能应提供一个以上的鉴别机制，应能够支持对不同身份的用户使用不同的鉴别机制，以及对一个用户同时使用多个鉴别过程进行多因素鉴别。**
e) **PKI 系统应支持基于数字证书的鉴别机制，当对一个用户同时使用多个鉴别过程进行鉴别时，所使用的鉴别机制中应包含基于数字证书的鉴别机制。**

7.1.6.3 鉴别失败处理

PKI系统应在鉴别失败处理方面遵循以下要求：

a) PKI 系统应实现鉴别失败次数检测功能，当用户自最近一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够检测到。
b) PKI 系统应提供鉴别失败检测参数配置功能。管理员可配置的参数包括：失败的鉴别次数和失效时间值等。
c) **PKI 系统应实现鉴别失败处理功能，当用户自最近一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：**
   1) 使终端失效一段随次数增加的时间；
   2) 使一个用户帐号失效一段时间或失效直到管理员解除；
   3) 向 PKI 系统的管理员报警；
   4) 允许用户重新建立会话过程。
d) **为了防止拒绝服务攻击，PKI 系统实现鉴别失败处理功能时，至少保证有一个用户账号不应失效。**

7.1.6.4 秘密的规范

PKI系统应在秘密的规范方面遵循以下要求：

a) 当被用来进行用户身份鉴别的秘密信息（如口令、密钥等）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。秘密信息质量量度由管理员制定，可包括：字母数字结构、密钥长度限制等。

b) 当被用来进行用户身份鉴别的秘密信息（如口令、密钥等）由 PKI 系统产生时，PKI 系统应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，可包括：字母数字结构、密钥长度限制等。

c) PKI 系统应保证生成或接受的秘密信息质量满足以下要求：

1) 终端用户口令应包括字母和数字的组合，且不少于 6 个字符。

2) 系统用户口令和系统部件密钥解密口令应包括字母和数字的组合，且不少于 8 个字符。

3) 使用的密钥算法和长度应符合密码国家标准和行业标准的要求。

d) PKI 系统应的秘密信息质量规范功能应支持用户配置策略，实现对具有特殊意义的数字和组合的口令的拒绝，例如：姓名、生日、电话号码、机构名称等。

7.1.7 访问控制

7.1.7.1 角色与责任

PKI系统应在角色与责任方面遵循以下要求：

a) PKI 系统开发者应依据以下责任分配提供 PKI 系统的管理员、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系统要求新增审计员角色，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。

b) PKI 系统应提供主体与角色关联功能，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。

c) 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 4 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
数据输入和输出	私钥输出应由管理员执行，其余数据的输入输出应由系统用户执行
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助过程和相关信息。
PKI系统配置	对于PKI系统功能的任何配置权应仅授予管理员。（除了在本标准中其他地方所定义的分配给其他角色的TSF功能，这一要求应用于所有的配置变量。）
证书轮廓管理	更改证书轮廓的权限应仅授予管理员。
撤销轮廓管理	更改撤销轮廓的权限应仅授予管理员。
证书撤销列表轮廓管理	更改证书撤销列表轮廓的权限应仅授予管理员。
在线证书状态查询轮廓管理	更改在线证书状态查询轮廓的权限应仅授予管理员。

7.1.7.2 系统用户访问控制

PKI系统应在系统用户访问控制方面遵循以下要求：

a) PKI 系统应提供用户注册、注销及口令分配功能，为用户分配或者使用系统特权时，应对该操作进行严格的限制和控制。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。

b) **PKI 系统应具备对系统用户开展定期审核的能力，定期审核系统用户的权限分配是否适当，审核可自动执行或告知管理员手动执行。**

c) PKI 系统应实现系统用户访问控制功能，访问控制权限的分配应依据表 2；

d) **PKI 系统应定义系统关键操作，关键操作应包括：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。PKI 系统应确保仅有多个系统用户同时在场，并符合表 3 的要求时，才能执行相应的关键操作。**

e) PKI 系统应在文档中提供访问控制的相关文档，访问控制文档中的应包含如下几个方面内容：

1) 角色及其相应的访问权限

应提供角色及其相应的访问权限的说明，角色及其相应的访问权限的分配应与表 2 一致。

表 5 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证书撤销的主体所完成。
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。 **至少应有两个人才可请求解密证书私钥，其中一个是操作员，另一个是操作员、管理员或审计员。**
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	仅管理员有权产生将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两个人的同意，其中一个是操作员，另一个是操作员、管理员或审计员。**
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。

2） 标识与鉴别系统用户的过程

应提供标识与鉴别系统用户的过程，该过程应符合 7.1.1 的要求。

3） 角色的职能分割

应提供角色职能分割的说明，职能分割应符合 7.1.3 的要求。

7.1.7.3 网络访问控制

PKI系统应在网络访问控制方面遵循以下要求：

a） PKI 系统应具备网络访问控制能力。使得用户进行远程访问时，远程用户只有通过鉴别后，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。

b） 远程计算机系统与 PKI 系统的连接应被鉴别，鉴别方法使用的凭据可包括计算机地址、访问时间、拥有的密钥等等。

c） PKI 系统应具备网络访问控制策略配置能力。

d） PKI 系统应对诊断分析端口的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。

e） **根据 PKI 系统的访问控制策略，PKI 系统应具备对于不合理的服务请求应进行限制和过滤的能力。**

f） **PKI 系统所有网络服务的安全属性要求应在 PKI 文档中有相关说明。**

7.1.8 安全审计

7.1.8.1 审计数据产生

PKI系统应在审计数据产生方面遵循以下要求：

a） PKI 系统应通过审计功能部件实现审计数据产生功能，审计数据产生功能应对下列事件产生审计记录：

1） 审计功能的启动和结束；

2） **表 3** 中列出的事件。

表 6 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操作	
	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	若输入的数据与其他数据相关，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（成果或失败）。
PKI系统部件的配置	所有与安全相关的对于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。

b) 对于每一个事件，审计数据产生功能生成的审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，以及**表 3** 中附加信息栏中要求的内容。

c) 审计数据产生功能生成的审计记录中不应出现明文形式的私钥、对称密钥和其他安全相关的参数。

d) 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。

7.1.8.2 审计查阅

a) 审计功能部件应为审计员提供查看所有日志信息的能力。

b) 审计功能部件应以适于阅读和解释的方式向读者提供日志信息。

7.1.8.3 选择性审计查阅

审计功能部件应实现选择性审计查阅功能，使得管理员在查阅审计日志时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。

7.1.8.4 审计事件存储

审计功能部件在存储审计记录时，应具备以下能力：

a) 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) 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，以防止审计数据丢失。

7.1.8.5 审计日志完整性保护

PKI系统应具备审计日志完整性保护能力，并遵循以下要求：

a) **审计功能部件应具备审计日志完整性保护能力，实现定期对审计日志进行完整性保护运算的功能，完整性保护运算机制包括数字签名、带密钥的杂凑计算、消息鉴别码等。**

b) 进行完整性保护运算时,运算的对象应包括从上次运算后加入的所有审计日志条目以及上次运算的结果。
c) 对审计日志进行完整性保护运算的时间周期应是可配置的。
d) 对审计日志进行完整性保护运算的事件应写入审计日志中,审计日志完整性保护运算结果应包含在其中。

7.1.9 原发抗抵赖

PKI系统应具备原发抗抵赖能力，并遵循以下要求：
a) PKI 系统应提供原发抗抵赖权标生成功能，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 系统应能使信息原发者的身份等属性，与证据使用信息的安全相关部分相关联。
b) 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。

7.1.10 备份和恢复

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他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。关键安全参数和其他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。

7.2 安全保障要求

7.2.1 开发

7.2.1.1 安全架构

开发者应提供产品安全功能的安全架构描述,安全架构描述应与产品设计文档中对安全功能的描述范围相一致。

7.2.1.2 功能规范

开发者应提供完备的功能规范说明，功能规范说明应满足以下要求：
a) 清晰描述 7.1、7.2 章中定义的安全功能；
b) 提供部件和安全功能接口间的对应关系；
c) 通过实现模块描述安全功能，标识和描述实现模块的目的、相关接口及返回值等，并描述实现模块间的相互作用及调用的接口；
d) 提供实现模块和子系统间的对应关系。

7.2.1.3 产品设计

开发者应提供产品设计文档,产品设计文档应满足以下要求:

a) 通过子系统描述产品结构,标识和描述产品安全功能的所有子系统,并描述子系统间的相互 作用;
b) 提供子系统和安全功能接口间的对应关系;
c) **通过实现模块描述安全功能,标识和描述实现模块的目的、相关接口及返回值等,并描述实现模块间的相互作用及调用的接口;**
d) **提供实现模块和子系统间的对应关系。**

7.2.1.4 实现表示

开发者应提供产品安全功能的实现表示,实现表示应满足以下要求:
a) **详细定义产品安全功能,包括软件代码、设计数据等实例;**
b) **提供实现表示与产品设计描述间的对应关系。**

7.2.2 指导性文档

7.2.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南,对每一种用户角色的描述应满足以下要求:
a) 描述用户能访问的功能和特权,包含适当的警示信息;
b) 描述产品安全功能及接口的用户操作方法,包括配置参数的安全值等;
c) 标识和描述产品运行的所有可能状态,包括操作导致的失败或者操作性错误;
d) 描述实现产品安全目的必需执行的安全策略。

7.2.2.2 准备程序

开发者应提供产品及其准备程序,准备程序描述应满足以下要求:
a) 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤;
b) 描述安全安装产品及其运行环境必需的所有步骤。

7.2.3 生命周期支持

7.2.3.1 配置管理能力

开发者的配置管理能力应满足以下要求:
a) 为产品的不同版本提供唯一的标识;
b) 使用配置管理系统对组成产品的所有配置项进行维护,并进行唯一标识;
c) 提供配置管理文档,配置管理文档描述用于唯一标识配置项的方法;
d) **配置管理系统提供自动方式来支持产品的生成,通过自动化措施确保配置项仅接受授权变更;**
e) **配置管理文档包括一个配置管理计划,描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。配置管理计划描述应描述如何使用配置管理系统开发产品,开发者实施的配 置管理应与配置管理计划相一致。**

7.2.3.2 配置管理范围

开发者应提供产品配置项列表,并说明配置项的开发者。配置项列表应包含以下内容:
a) 产品及其组成部分、安全保障要求的评估证据;
b) **实现表示、安全缺陷报告及其解决状态。**

7.2.3.3 交付程序

开发者应使用一定的交付程序交付产品,并将交付过程文档化。在给用户方交付产品的各版本时,交付文档应描述为维护安全所必需的所有程序。

7.2.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在产品的开发环境中,为保护产品设计和实现 的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

7.2.3.5 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制,并提供生命周期定义文档描述用于开发和维护产品的模型。

7.2.3.6 工具和技术

开发者应明确定义用于开发产品的工具,并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

7.2.4 测试

7.2.4.1 测试覆盖

开发者应提供测试覆盖文档,测试覆盖描述应满足以下要求:

a) 表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性;
b) 表明上述对应性是完备的,并证实功能规范中的所有安全功能接口都进行了测试。

7.2.4.2 测试深度

开发者应提供测试深度的分析。测试深度分析描述应满足以下要求:

a) 证实测试文档中的测试与产品设计中的安全功能子系统和实现模块之间的一致性;
b) 证实产品设计中的所有安全功能子系统、实现模块都已经进行过测试。

7.2.4.3 功能测试

开发者应测试产品安全功能,将结果文档化并提供测试文档。测试文档应包括以下内容:

a) 测试计划,标识要执行的测试,并描述执行每个测试的方案,这些方案包括对于其他测试结果的任何顺序依赖性;
b) 预期的测试结果,表明测试成功后的预期输出;
c) 实际测试结果和预期的测试结果的对比。

7.2.4.4 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源,以用于安全功能的抽样测试。

7.2.5 脆弱性评定

基于已标识的潜在脆弱性,产品能抵抗具有**中等攻击潜力**的攻击者的攻击。

7.2.6 代码安全

开发者应采用代码审计等方式，对PKI系统进行安全性测试并提供相关测试文档，确保PKI系统的代码安全。

参 考 文 献

[1]GB/T 20281-2020 信息安全技术 防火墙安全技术要求和测试评价方法