ICS 35.240.01
A16

SF

中华人民共和国司法行政行业标准

SF/T 0036—2019

公证信息安全技术规范

Technical specification for notarization information security

2019-5-5 发布　　2019-5-20 实施

中华人民共和国司法部　　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由司法部公共法律服务管理局、中国公证协会提出。

本标准由司法部信息中心归口。

本标准起草单位：中国公证协会。

公证信息安全技术规范

1 范围

本标准规定了公证信息安全对象和内容、信息安全建设、物理安全、网络安全、系统安全、应用安全、数据安全及备份恢复和公证PKI系统安全保护要求。

本标准适用于司法行政公证管理部门、公证协会及各公证机构对公证信息安全的规划、设计、建设和管理。

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 17859 计算机信息系统安全保护划分准则

GB/T 19713 信息技术 安全技术 公钥基础设施 在线证书状态协议

GB/T 20269 信息安全技术 信息系统安全管理要求

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 信息安全技术 公钥基础设施 数字证书格式

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 50052 供配电系统设计规范

SF/T 0034-2019 公证数据要求与规范

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

公证 notarization

公证机构根据自然人、法人或者其他组织的申请，依照法定程序对民事法律行为、有法律意义的事实和文书的真实性、合法性予以证明的活动。

3.1.2

公证机构 notarial institutions

依法设立、不以营利为目的、依法独立行使公证职能、承担民事责任的证明机构。

3.1.3

公证事项 notarized matters

公证机构依据《中华人民共和国公证法》第十一条的规定，按照公证证明对象对所办理的公证业务的细化分类。

3.1.4

公证事务 notarial affairs

依据《中华人民共和国公证法》第十二条的规定，公证机构所办理的非证明业务。

3.1.5

公证信息安全 notarization information security

公证数据和信息化设施的安全。

3.1.6

数据保密性 data confidentiality

非授权的用户、实体或过程对于信息无访问权限，从而保证涉密信息具有不被盗取或利用的特性。

3.1.7

消息摘要算法 message-digest algorithm

一种加密过程不需要密钥，并且经过加密的数据无法被解密，只有输入相同的明文数据经过相同的算法才能得到相同的密文的算法。

3.1.8

区块链 block chain

一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

注：事务处理包括但不限于可信数据的产生、存取和使用等。

[GB/T 37043-2018，定义2.5.8]

3.1.9

数字签名 digital signature

附加在数据单元上的一些数据，或是对数据单元所作的密码交换（见“密码学”），这种数据或变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人（例如接收者）进行伪造。

[GB/T 9387.2—1995，定义3.3.26]

3.1.10

非对称密码技术 asymmetric cryptographic technique

使用两种相关变换的密码技术。

注：一种是由公开密钥定义的公开变换，另一种是由私有密钥定义的私有变换。

3.2 缩略语

下列缩略语适用于本文件。

CA 证书认证机构（Certificate Authority）

CRL 证书撤销列表（Certificate Revocation List）
IDS 入侵检测系统（Intrusion Detection Systems）
IPSec 因特网协议安全性（Internet Protocol Security）
OCSP 在线证书状态协议（Online Certificate Status Protocol）
PKI 公钥基础设施（Public Key Infrastructure）
RA 证书注册机构（Registration Authority）
SSL 安全套接层（Secure Sockets Layer）

4 公证信息安全对象和内容

4.1 信息安全对象

信息安全对象包括公证事项、公证事务、公证数据和公证信息化设施。

4.2 信息安全内容

信息安全内容包括技术安全和管理安全。其中：

a) 技术安全包括物理安全、网络安全、系统安全、应用安全、数据安全、PKI 安全等内容，具体如下：
   1) 物理安全：公证数据中心及电子公证信息化设施，包括机房、服务器、网络设备、存储设备、PC 机、移动设备等免受非法的物理访问、自然灾害和环境灾害；
   2) 网络安全：身份认证、通信过程中数据的保密性、完整性、可用性、可控性、真实性及可审查性保障等；
   3) 系统安全：操作系统、数据库、中间件等；
   4) 应用安全：公证信息化相关系统、平台、工具和应用，例如公证业务办证系统、公证业务管理系统、公证电子档案管理系统、公证在线受理系统、公证电子数据保管工具、屏幕录像工具等；
   5) 数据安全：公证数据存储安全、通信安全、权限安全（具体内容见 SF/T 0034-2019），以及电子公证中存储的工作人员数据、用户数据及其他数据；
   6) PKI 安全：公证行业 PKI 系统安全与安全管理。
b) 管理安全应遵循 GB/T 20269 内容，具体内容如下：
   1) 安全规章制度的制定内容；
   2) 机构和人员管理内容；
   3) 风险与应急管理内容；
   4) 运行和维护管理内容；
   5) 监督和检查管理内容；
   6) 安全教育培训内容。

5 公证信息安全建设

5.1 信息安全建设基本要求

信息安全建设要求如下：

a) 应遵循 GB/T 17859、GB/T 22240、GB/T 22239 和公通字[2007]43 号的相关规定，并符合公证行业所需要的其他要求；

b) 应根据信息的重要程度和不同类别，采取不同的保护措施，实施分类保护；
c) 应根据信息系统和数据的重要程度，进行分域存放，实施分域保护和域间安全交换，实施分域控制。

5.2 信息安全建设实施方法

信息安全建设应按照以下实施方法：

a) 依据信息安全等级保护的定级规则，确定电子公证信息的安全等级；
b) 按照信息安全等级保护要求，确定与电子公证信息安全等级相对应的基本安全要求；
c) 依据信息系统基本安全要求，并综合电子公证信息安全技术要求、信息系统所面临风险和实施安全保护措施的成本，进行安全保护措施的制定，确定适用于电子公证信息的安全保护措施，并依照本标准相关要求完成规划、设计、实施、验收和运行工作。

5.3 信息安全防护等级

信息安全防护等级应按照GB/T 22239-2008中第三级要求进行规划和建设。

6 物理安全

6.1 物理安全基本要求

应遵循GB/T 22240-2008中7.1.1的相关规定，并符合公证行业所需要的其他要求；

6.2 环境安全

环境安全主要对机房环境给出以下要求：

a) 应满足场地防火、防污染、防潮、防雷、防震动、防强电场、防强磁场、防地震、防水灾、防公众干扰的要求；
b) 应只设一个出入口，未经允许的人员不准进入机房；机房物品未经允许不得擅自带出，不得将磁铁、私人计算机或电设备、食品等无关物品带入机房。机房应设有门禁设备，所有出入机房的人员应经过门禁系统的识别；
c) 应设有空调设备，使机房温度达到计算机运行所允许的范围；
d) 应保证通信线路安全，采取必要措施，防止线路截获事件发生；
e) 应提供可靠的电力供应，电源应符合 GB/T 50052 的要求，采取多种供电方式，定期维护和检查供电设备，如进行有计划地停电，停电计划应提前通知有关部门。

6.3 设备安全

设备安全要求如下：

a) 应妥善放置计算机、网络基础设施，机房内部应设有电视监控，安排专人值守，加强保护以降低被破坏的风险，防止非法入侵；
b) 应为设备提供可靠的运行支持，并通过容错和故障恢复等措施，支持信息系统实现不间断运行；
c) 应采取严格的保护措施存放核心数据的各类记录介质，防止被盗、被毁和受损。核心数据应长期保存，并采取有效措施，防止被非法拷贝。

7 网络安全

7.1 网络安全基本要求

应遵循GB/T 22240-2008中7.1.2的相关规定，并符合公证行业所需要的其他要求；

7.2 网络访问控制

网络访问控制要求如下：

a) 应使用经过授权的网络服务，防止不安全的网络连接影响电子公证的安全；
b) 应制定有关网络及网络服务的使用策略，并与访问控制策略保持一致。具体策略应规定以下内容：
   1) 应明确用户允许访问的网络和网络服务；
   2) 应规定对用户访问网络和网络服务进行授权的程序；
   3) 应具有对网络连接和网络服务的访问进行保护的管理控制措施和程序；
   4) 应保留对网络服务的访问日志，并根据信息的敏感程度确定日志的具体内容。
c) 应基于访问控制策略和访问需求，根据不同的业务、应用及其所处理信息的敏感性和重要性，并按照国家信息安全等级保护要求，将网络与信息系统划分成不同的逻辑安全区域，采取重点防护、边界隔离的办法，重点加强安全域关键边界的安全保护和监控。同时通过隔离措施，过滤域间业务，控制域间通信；
d) 应制定并实施有效的端口保护措施，保护网络与信息系统的远程操作管理所使用的端口，防止端口被未经授权访问或非法访问，并记录各端口的访问日志。

7.3 网络传输安全

网络传输安全要求如下：

a) 应采取 SSL、IPSec 等加密控制措施，保障通过公共网络传输的数据机密性和完整性；
b) 应对网络安全状态进行持续监控，记录有关错误、故障和补救措施。

7.4 网络安全审计与监控

网络安全审计与监控要求如下：

a) 应对网络访问和使用情况进行审计和监控，以检测违反访问控制策略的活动；
b) 应记录相关证据。

7.5 网络设备安全管理

网络设备安全管理要求如下：

a) 应明确许可设备管理权限，否则应禁止；
b) 应明确限定设备管理权限的变更，包括系统自动生效的变更和管理员批准生效的变更；
c) 应经管理人员审查批准访问控制规则，方可执行；
d) 应依照每个系统的安全要求制定访问控制策略；
e) 应依照与该系统相关的业务信息的类型制定访问控制策略。

8 系统安全

8.1 系统安全基本要求

应遵循GB/T 22240-2008中7.1.3的相关规定，并符合公证行业所需要的其他要求。

8.2 身份鉴别

身份鉴别要求如下：

a) 每个用户应使用唯一的用户标识符，用户与其操作关联，并对其行为负责；
b) 因业务需要时允许使用用户组，应采取控制措施；
c) 授权用户访问的级别应给予业务目的，并符合安全策略，用户授权应遵循最小授权原则；
d) 用户访问权限应得到上级批准；
e) 应及时修改或注销已经转岗或离职用户的访问权限；
f) 应定期核查并删除多余、闲置或非法的账户。

8.3 操作系统安全

操作系统安全应提供以下访问控制功能：

a) 验证用户身份；
b) 记录所有系统访问日志；
c) 限制用户连接时间。

8.4 数据库安全

数据库安全涉及到数据的完整性、保密性，应包括以下内容：

a) 用户身份鉴别；
b) 访问控制；
c) 数据标记；
d) 数据流控制；
e) 安全审计；
f) 备份与恢复。

8.5 中间件安全

中间件安全要求如下：

a) 应选用符合安全要求的中间件产品；
b) 应制定符合安全规范的用户身份鉴别方式、用户权限设置、操作规范、安全审计等相关措施；
c) 应实时监控中间件运行状态和通过中间件的数据。

8.6 恶意代码防范

恶意代码防范要求如下：

a) 应制定软件使用规定，遵守软件许可协议，不应使用非法软件；
b) 通过互联网或不明来源获取的文件和软件，应采取防护措施；
c) 应安装并定期更新防病毒软件和补丁程序；
d) 应定期检查支持关键业务系统的软件和数据，发现任何未经批准的文件或者未经授权的修改，并进行调查；
e) 应检查所有来源不明和来源非法的存储介质上的文件、通过外部网络接收的文件，以确认是否含有恶意软件；
f) 应检查所有电子邮件的附件及下载内容是否含有恶意软件，应在用户端和电子邮件服务器端进行检查；

g) 应进行用户安全教育和培训，进行恶意软件攻击通报，制定系统恢复的管理程序，落实相关责任；
h) 应从权威发布部门接受恶意软件相关信息，对可疑问题应及时上报。

9 应用安全

9.1 应用安全基本要求

应遵循GB/T 22240-2008中7.1.4的相关规定，并符合公证行业所需要的其他要求。

9.2 身份鉴别

身份鉴别分为口令管理、用户访问权限审核，具体要求如下：

a) 口令管理
   1) 所有口令的信息应为保密信息；
   2) 系统向用户提供临时口令时，应确保提供安全的初始口令，并要求用户限期修改；用户忘记口令时，系统应在正确识别用户身份后才能向用户提供重置的临时口令；
   3) 应以安全方式向用户提供临时口令，禁止使用明文的电子邮件等未经保护的方式传递，并要求用户确认接收到临时口令；
   4) 口令应以加密方式存入用户数据库，通过加密、解密方式实现其存储、读取。
b) 用户访问权限审核
   1) 用户访问权限应由管理人员、系统责任人及系统维护人员共同确认；
   2) 用户账户、特殊权限账户、超级权限账户的访问权应定期检查；
   3) 发生非法入侵事件、发生人员变动后应进行审核；
   4) 对审核中发现的问题，应采取必要措施予以纠正。

9.3 应用访问控制

应用访问控制要求如下：

a) 应根据访问控制策略，控制用户访问应用系统和信息；
b) 应防止用户在未经授权的情况下使用能够超越系统或应用控制措施的工具和系统软件；
c) 系统所有人和授权用户可对应用系统中的信息进行访问；
d) 应用系统对共享信息资源的访问应对其它系统的安全无影响；
e) 应确保处理敏感信息的应用系统只输出必要信息，输出结果只能被发送至授权的终端，应定期检查此类输出。

9.4 应用数据完整性

应用数据完整性包括输入数据验证、内部处理控制和输出控制验证，具体要求如下：

a) 输入数据验证
   1) 进行口令修改等输入操作时，应双重输入，并确认两次输入的口令一致才接受修改；
   2) 应建立用于响应错误输入的程序；
   3) 应建立用于测试输入数据真实性的程序。
b) 内部处理控制
   1) 程序或进程中账户和口令应可修改；
   2) 应具备对口令猜测的防范机制和监控手段；

3) 应避免应用程序以错误的顺序运行，防止出现故障后程序以不正常的流程运行；
4) 应采用正确的故障恢复程序，确保正确处理数据；
5) 应采取会话控制或批次控制，确保更新前后数据文件状态的一致性；
6) 应检查执行操作前后对象是否正常；
7) 应验证系统生成的数据；
8) 应检查上传、下载的数据或软件的完整性；
9) 应检查文件与记录是否被篡改。

c) 输出数据验证
1) 应验证输出数据在规定的赋值范围内；
2) 输出数据应为用户或后续处理系统提供充足的信息，以确定信息的准确性、完整性、精确性和分类级别；
3) 应具有可以用来验证输出数据的测试程序。

9.5 应用通讯加密

应用通讯加密包括加密技术使用策略、加密技术、数字签名、抗抵赖服务、密钥管理，具体要求如下：

a) 加密技术使用策略
1) 应具有密钥管理方法，在密钥丢失、泄露或损坏时恢复信息原文；
2) 应具有策略实施、密钥管理的相关岗位和职责；
3) 应能正确确定合适的加密保护级别。

b) 加密技术
1) 应符合国家有关加密技术的使用和进出口限制等方面的法律法规；
2) 应根据风险评估确定保护级别，并以此确定加密算法的类型、属性，以及所用密钥的长度；
3) 应选择能够提供所需保护的合适的加密产品，加密产品应能实现安全的密钥管理。

c) 数字签名
1) 应充分保护私钥的机密性，防止窃取者伪造密钥持有人的签名；
2) 应使用公钥证书保护公钥完整性；
3) 用于数字签名的密钥应不同于用来加密内容的密钥；
4) 应符合有关数字签名的法律法规。

d) 抗抵赖服务
1) 应根据公证业务流程规范与加密技术使用策略；
2) 应使用抗抵赖服务的业务并使用抗抵赖服务。

e) 密钥管理
1) 应采取加密等安全措施来有效保护密钥；
2) 应对生成、存储和归档保存密钥的设备采取物理保护；
3) 应使用经过批准的加密机制进行密钥分发，应记录密钥的分发过程；
4) 应制定确切的密钥生存期，应在生存期内有效。生存期的长短应取决于使用环境及加密技术；
5) 应全国进行统一设计密匙管理。

9.6 应用安全管理

应用安全管理包括应用程序的部署及更新、应用系统源代码安全，具体要求如下：

a) 应用程序的部署及更新

1） 应用程序的软件版本升级或数据更新应由制定的管理员在获取授权后完成；
2） 运行应用程序的操作系统中应只保留应用程序的可执行代码；
3） 历史版本的软件应予以保留；
4） 应采用软件补丁消除或削弱安全缺陷；
5） 应对应用系统进行兼容性测试。

b） 应用系统源代码安全
1） 应用系统源代码应从操作系统中移除；
2） 应用系统开发过程中源代码版本应有严格的控制，对源代码的访问权限应实现分级访问控制；
3） 应用系统程序源代码应保存在安全环境中；
4） 对应用程序源代码的所有访问都应保留审计日志；
5） 应用程序源代码的维护和拷贝应严格遵从变更控制程序。

10 数据安全及备份恢复

10.1 数据安全及备份恢复基本要求

应遵循GB/T 22240-2008中7.1.5的相关规定，并符合公证行业所需要的其他要求。

10.2 存储安全

存储安全要求如下：

a） 应采用加密或其他保护措施实现公证数据和系统数据的存储保密性；
b） 应能检测到公证数据和系统数据在存储过程中完整性受到破坏，应在检测到完整性错误时采取必要的恢复措施；
c） 可使用消息摘要算法生成公证数据的数据指纹信息，用以验证数据的完整性；
d） 可采用区块链技术存储公证数据的数据指纹信息，使相关数据的存储具有防篡改性，当提取数据时需与相应的数据指纹信息进行比对，确定数据的原始性和完整性；
e） 应建立审计日志，记录所有数据存储和修改操作、数据库身份鉴别失败事件、重复性登陆失败、连续访问尝试、及其它安全事件。审计日志应保留规定的时长，以便支持以后的事件调查和访问控制审核。对于审查出问题的数据应具有撤回功能，以确保数据的正确性；
f） 应建立完善的用户权限和管理权限设置；
g） 应使用数字签名等技术，使相关数据的生成、修改、删除等操作具有抗抵赖性。

10.3 传输安全

传输安全要求如下：

a） 应采用加密、身份鉴别或其他保护措施实现公证数据和系统数据的传输保密性；
b） 应对重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用通信协议的攻击破坏数据保密性和完整性；
c） 应能够检测到公证数据和系统数据在传输过程中完整性受到破坏，应在检测到完整性错误时采取恢复措施；
d） 传输数据应使用时间戳或数字签名技术，以防范重放攻击；
e） 应使用数字签名等技术，使数据的传输操作具有抗抵赖性。

10.4 数据交换安全

数据交换安全要求如下：

a) 应进行分类存档所有数据；
b) 应保证数据完整性，应能够检测出数据受到破坏，并能进行恢复；
c) 应保证数据保密性，实现系统管理数据、鉴别信息和重要业务数据的传输和存储的保密性；
d) 应实现本地完全数据备份，宜建立数据异地备份。

10.5 数据权限安全

数据权限安全要求如下：

a) 应保护用户隐私数据，为用户数据提供仅供多种保密权限设置功能，应采用满足要求的加密算法，保证用户的保密信息除非经用户授权等法定事由，公证机构和技术公司不应查看用户保密数据；
b) 用户保密数据可由用户自行设置加密密钥来加密存储；
c) 应制定完善的访问控制策略，应控制用户访问数据范围，系统所有人和授权用户可访问对应的数据。

10.6 数据备份

数据备份包括数据备份策略、数据备份实施和数据备份管理，具体要求如下：

a) 数据备份策略
   1) 应包含系统和数据的名称、备份的频率和类型、备份介质、备份软件、异地存放周期以及制定备份方案的实施原则等；
   2) 应将备份操作安排在不影响业务的时间段里，严格遵照备份策略执行；
   3) 应至少保留两个版本或两个备份周期的重要的业务系统备份信息，备份信息应包含完整的备份记录、备份拷贝、恢复程序文档和清单；
   4) 应在本地保留备份信息，宜进行异地备份；
   5) 应定期检查和测试备份信息，保持其可用性和完整性，应在规定时间内完成恢复工作；
   6) 应明确规定备份信息的保留时间。
b) 数据备份实施
   1) 信息系统维护人员应根据业务需要定期进行备份计划的符合，并进行相关修订；
   2) 备份操作人员应根据备份计划定期执行备份工作，并检查备份日志，确认备份有效性，进行记录；
   3) 如发现备份失败，备份操作人员应检查失败原因，编写故障报告，并尽快安排重新备份；
   4) 备份完成后应保存备份介质，备份操作人员应在标签上按要求记录备份信息，应移交备份介质管理人员；
   5) 应定期进行恢复性测试，如恢复性测试失败，应检查失败原因，编写故障报告，应尽快安排重新测试。
c) 数据备份介质管理，其中：
   1) 应安排专人负责保管备份介质，进行登记并按照规定妥善存放。存有备份数据的备份介质应贴好标签，明确标示备份介质编号、有效期、备份日期、操作人员、备份内容、备份用途、备份数据保存时间等；
   2) 存有备份数据的备份介质需异地存放的，应存放在安全的备用场所内，应在执行完异地存放后进行记录，并签字确认；
   3) 应对备份介质的访问进行记录，并由保管人员签字确认；
   4) 应定期检查备份介质的情况，保证备份介质数量完整。

11 公证 PKI 系统安全保护要求

11.1 公证 PKI 系统安全保护基本要求

应遵循GB/T 22240-2008中7.2的相关规定，并符合公证行业所需要的其他要求。

11.2 角色与责任

系统应具备使主体与角色相关联的能力，一个主体应保证至多拥有一个角色的权限。角色与责任要求如下：

a) 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；
b) 管理员
   1) 安装、配置、维护系统；
   2) 建立和管理用户账户；
   3) 配置轮廓和审计参数；
   4) 生成部件密钥。
c) 操作员：签发和撤销证书；
d) 审计员：查看和维护审计日志；
e) 安全员：执行系统的备份和恢复。

11.3 访问控制

访问控制要求如下：

a) 能够访问 PKI 系统信息和服务的用户应按正规的程序执行；
b) 分配或使用系统特权时，应进行限制和控制；
c) 进行口令分配时，应通过正规的程序控制；
d) 应定期审核系统用户的访问权限，检查权限分配的合理性；
e) 应分类管理系统用户账号和终端用户账号；
f) 针对不同的功能，角色及其访问控制权限分配见表 1；
g) 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；
h) 进行远程访问时，PKI 系统应提供访问控制；
i) 远程用户应被认证通过后才允许访问，并应对授权用户提供被授权使用的服务；
j) 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，并应采取防火墙、IDS 等安全保护措施。

表 1 功能、角色及其访问控制权限的分配关系

功　能	角色及其访问权限
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数据和安全相关数据。
密钥生成	仅管理员可以请求生成部件密钥。

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	a) 仅操作员可以提出对证书私钥的请求； b) 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； c) 至少应有两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。
私钥和对称私钥销毁	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。
私钥和对称私钥输出	a) 仅管理员有权输出部件私钥； b) 仅操作员有权输出证书私钥； c) 输出证书私钥至少应获得两个人的同意，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	a) 仅操作员和证书主体有权申请使证书进入挂起状态； b) 仅操作员有权批准证书进入挂起状态； c) 仅操作员和证书主体有权申请撤销证书； d) 仅操作员有权批准撤销证书和所有被撤销信息。

11.4 审计功能及事件

审计功能及事件见表2。

表 2 审计功能及事件

功能	事件	附加信息
安全审计	所有审计变量的改变	
	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	若输入的数据与其他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	审计日志应保存非对称密钥的公钥部分
私钥生成	部件私钥的载入	
私钥存储	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	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	私钥和对称密钥的输出	
证书注册	所有证书请求	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	所有对于OCSP轮廓的更改	在日志记录中保存对轮廓更改的内容

11.5 密钥管理

密钥管理包括密钥生成、密钥传送与分发、密钥有效期、密钥存储、密钥备份、密钥更新、密钥回复、密钥归档和密钥销毁，具体要求如下：

a) 密钥生成
   1) 如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；
   2) 如密钥生成方法需要从随机数发生器输入随机数，随机数的生成应采用国家密码行政管理部门认可的方法；
   3) 如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；
   4) 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安全密钥的产生的难度应至少和断定产生的密钥的值的难度一样大；
   5) CA 签名公私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应符合统计规律；
   6) 应采用分割知识或其他分布式生成方法，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；
   7) 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；
   8) PKI 系统的文档中应明确规定系统密钥生成方法。
b) 密钥传送与分发
   1) 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；
   2) 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；
   3) 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，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；
   4) PKI 系统的文档中应明确说明 CA 公钥分发方法。
c) 密钥有效期
   1) PKI 系统应提供密钥有效期设置功能；

2) 应根据密钥长度、加密算法的攻击难度、加密对象的价值、合同或者法律等外部环境的需求进行设置，应符合国家密码行政管理部门的规定。

d) 密钥存储

1) 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；

2) CA 签名公私钥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，各模块应分散存放。

e) 密钥备份

1) 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。

2) 对于 CA 签名私钥备份，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，各模块应分散存放。

3) PKI 系统密钥备份应采用热备份、冷备份和异地备份等措施。

f) 密钥更新

1) 新密钥的生成应符合 11.5 a)的规定；

2) 新 CA 公钥的传送与分发应符合 11.5 b)的规定；

3) 旧 CA 公钥的归档应符合 11.5 h)的规定；

4) 旧 CA 私钥的销毁应符合 11.5 i)的规定；

5) PKI 系统应采取明确的方法更新 CA 密钥及证书。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，防止各种攻击行为（例如:替换 CA 私钥和证书等）；

6) PKI 系统文档中，应说明 CA 密钥及证书的更新方法，应确保 CA 密钥及证书更新时，按照文档中规定的方法操作。

g) 密钥恢复

1) 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；

2) CA 签名私钥恢复需多个被授权的人同时使用存有私钥信息的部件，在安全可信的环境中恢复，恢复后私钥仍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。

h) 密钥归档

1) 私钥归档中区分用于签名的私钥和用于解密数据的私钥。签名私钥不应归档，解密私钥可归档；

2) CA、RA、终端用户或其他系统部件的公钥都应归档。

i) 密钥销毁

1) 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，应保证销毁过程不可逆；

2) 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；

3) CA 签名私钥的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。

11.6 证书管理

证书管理包括证书注册和证书撤销，具体要求如下：

a) 证书注册

1) PKI 系统所签发的公钥证书应与 GB/T 20518 相一致。任何整数所包含的字段或扩展应被 PKI 系统根据 GB/T 20518 生成或经由颁发机构验证以保证其与标准的一致性；
2) 输入证书字段和扩展中的数据应被批准。

b) 证书撤销
1) 发布 CRL 的 PKI 系统应验证所有强制性字段的值符合 GB/T 20518；
2) 发布 OCSP 基本响应的 PKI 系统应验证所有强制性字段的值符合 GB/T 19713。

11.7 配置管理

配置管理应符合 GB/T 20271-2006 中 6.4.5.1 的要求，PKI 系统的配置管理要求如下：

a) 在配置管理自动化方面要求部分的配置管理应自动化；
b) 在配置管理能力方面应实现声称支持和验收过程的要求；
c) 应在 PKI 系统的配置管理范围方面，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，应对开发工具配置管理范围的管理；
d) 在系统的整个生存期，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。被授权的代码和代码修改应被加进已经交付的源码中。所有改变应被记载和检查。

11.8 指导性文档

指导性文档应符合 GB/T 20271-2006 中 6.4.5.4 的要求，具体要求如下：

a) 应提供指导性文档；
b) 应提供系统用户文档，系统用户文档应包含以下内容：
1) 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，应含有如何安装或终止安装的说明；
2) 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；
3) 如何用安全的方法重建 PKI 系统的方法；
4) 说明审计跟踪机制，使系统用户可以有效地使用审计跟踪来执行本地的安全策略；
5) 必要时，说明如何调整系统的安全默认配置。

c) 应提供终端用户文档，应包含以下内容：
1) 提供关于不同用户可见的安全机制以及如何利用它们的信息；
2) 描述没有明示用户的保护结构；
3) 解释它们的用途；
4) 使用指南。

d) 应提供系统用户文档，应包含以下内容：
1) 有关设置、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；
2) 管理员功能关于安全方面的详细描述，包括增加和删除一个用户、改变用户的安全特征等；

e) 应提供审计工具的文档，应包含以下内容：
1) 为检查和保持审计文件所推荐的过程；
2) 针对每种审计事件的详细审计记录文件；
3) 为周期性备份和删除审计记录所推荐的过程等。

参 考 文 献

[1] GB/T 9387.2-1995 信息处理系统 开放系统互连 基本参考模型 第2部分:安全体系结构
[2] GB/T 37043-2018 智慧城市 术语
[3] 公通字[2007]43号 关于印发《信息安全等级保护管理办法》的通知