ICS 35.020
L 80

中华人民共和国国家标准

GB/T 28447—2012

信息安全技术
电子认证服务机构运营管理规范

Information security technology—Specification on the operation management of a certificate authority

2012-06-29 发布　　2012-10-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准主要起草单位:北京天威诚信电子商务服务有限公司、顾信科技有限公司。

本标准主要起草人:唐志红、李延昭、魏一才、徐虎、龙毅宏、刘旭、许蕾、赵宏科、张海松、郭宏杰。

引　言

本标准是为贯彻执行《中华人民共和国电子签名法》(以下简称《电子签名法》),规范电子认证服务机构的运营管理而制定。

本标准覆盖了电子认证服务机构运营管理的主要方面,提供公共认证服务的电子认证服务机构应按本标准的规定开展相关的工作。本标准涉及面多,但对每方面只做重点的、关键的、必要的要点性规定,确保电子认证服务机构执行本标准时在具体技术上、策略上和方案上有很大的灵活性。比如,对于认证系统安全方面,本标准只规定需要采用的安全防护技术和手段及需要考虑的关键点,对具体实现技术并未做规定。

信息安全技术
电子认证服务机构运营管理规范

1 范围

本标准规定了电子认证服务机构在业务运营、认证系统运行、物理环境与设施安全、组织与人员管理、文档、记录、与介质管理、业务连续性、审计与改进等多方面应遵循的要求。

本标准适用于在开放互联环境中提供数字证书服务的电子认证服务机构的建设、管理及评估。

对于在封闭环境中(如在特定团体或某个行业内)运行的电子认证服务机构可根据自身安全风险评估以及国家有关的法律法规有选择性地参考本标准。国家有关的测评机构、监管部门也可以将本标准作为测评和监管的依据。

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 2887 计算机场地通用规范

GB/T 9361 计算机场地安全要求

GB/T 25056—2010 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 26855—2011 信息安全技术 公钥基础设施 证书策略与认证业务声明框架

GB 50045 高层民用建筑设计防火规范

GB 50057 建筑物防雷设计规范

GB 50174 电子信息系统机房设计规范

GB 50343 建筑物电子信息系统防雷技术规范

SJ/T 10796 防静电活动地板通用规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子认证服务机构 certificate authority

负责创建、分发证书并在必要时提供验证以证实用户身份的机构,一般是受用户信任的权威机构,用户可以选择该机构为其创建密钥。通常将电子认证服务机构简称为CA,也称为CA中心、CA机构、认证机构、证书认证机构等。

3.2

电子认证服务 electronic certification service

电子认证服务是指为电子签名相关各方提供真实性、可靠性验证的活动。

3.3

证书策略 certificate policy

命名的一组规则,指出证书对具有共同安全要求的特定团体和/或应用的适用性。

3.4

电子认证业务规则　certification practice statement

电子认证服务机构在提供电子认证服务时，在责任范围、作业操作规范、信息安全保障措施等方面所遵循的业务规则。

3.5

证书撤销列表　certificate revocation list

由电子认证服务机构签署的一个失效证书列表，它给出了一套证书发布者认为无效的证书。

3.6

数字证书　digital certificate

由电子认证服务机构采用非对称密码技术签发的、证实主体身份与特定公钥间对应关系的数据电文。

3.7

公钥基础设施　public key infrastructure

支持公开密钥体制的安全基础设施，提供身份鉴别、信息加密、数据完整性和交易抗抵赖的技术支撑。

3.8

注册机构　registration authority

具有下列一项或多项功能的实体：识别和鉴别证书申请者，同意或拒绝证书申请，在某些环境下主动撤销或挂起证书，处理用户撤销或挂起其证书的请求，同意或拒绝用户更新其证书或密钥的请求。通常将注册机构简称为 RA 或 RA 机构。

3.9

秘密共享　secret sharing

秘密共享指将一个秘密在一组参入者间进行分发的方法，其中每个参入者被分配了该秘密经分割后的一份(称为秘密份额或秘密分割)。只有足够数量的秘密份额才能恢复原秘密，单个的秘密份额本身是无法恢复秘密的。

注：在本标准中，被分担的秘密可能是 CA 私钥备份恢复数据或 CA 私钥。

4　缩略语

下列缩略语适用于本文件：

CA　证书认证机构，本标准中称为电子认证服务机构 Certificate Authority

CP　证书策略 Certificate Policy

CPS　电子认证业务规则 Certification Practice Statement

CRL　证书撤销列表 Certificate Revocation List

OCSP　在线证书状态查询协议 Online Certificate Status Protocol

PKI　公钥基础设施 Public Key Infrastructure

RA　注册机构 Registration Authority

5　电子认证服务机构运营的业务

5.1　用户证书服务

5.1.1　证书申请与审核

用户通过认证系统在线提交证书申请或通过注册机构申请证书，应按照电子认证服务机构的要求

提供相应的申请信息，如申请者姓名、域名、公司名、地址、联系方式等。

用户还应提供电子认证服务机构审核证书申请所需要的相关证明材料，如机构资质证明、域名所有权证明等。

电子认证服务机构的审核人员，依据用户提交的证明材料，对证书申请者的身份进行审核。

电子认证服务机构在证书申请审核过程中，应保留完整的审核记录，以供日后审计、审查、责任追踪和界定使用。

5.1.2 证书签发

电子认证服务机构必须在完成规定的证书申请审核后，通过认证系统批准、签发证书。证书签发应有记录。

5.1.3 证书存储与发布

电子认证服务机构通过认证系统为用户提供数字证书的存储与发布功能，使得依赖方可以查询、获取。

5.1.4 证书更新

证书用户在证书有效期到达前，可以申请更新证书，已过期或撤销的证书不能更新。

对证书用户提交的证书更新请求，电子认证服务机构必须进行审核，审核的方式包括手工和自动两种方式。手工审核的过程，要求在安全保障方面应与证书申请等同。对于自动审核方式，证书更新请求必须用原证书私钥签名，认证系统验证签名的有效性并自动签发更新证书。

5.1.5 证书撤销

证书撤销有下列3种发起方式：

a) 由证书用户发起——用户申请撤销证书，电子认证服务机构必须明确规定撤销证书申请的接受方式，如通过电话、邮件、在线申请等，以及审核程序。

b) 由电子认证服务机构发起——电子认证服务机构如发现用户证书申请资料存在虚假信息、不能满足证书签发条件等情况，或者发生(或怀疑发生)电子认证服务机构CA私钥泄露、认证系统存在安全隐患威胁用户证书安全等情况，可以不经过证书用户本人同意，予以撤销证书。

c) 由依赖方发起——当依赖方提出证书撤销申请时，如证书仅用于依赖方的系统，可以不经过证书用户本人同意，予以撤销证书。

证书撤销后，电子认证服务机构必须在周期性签发的CRL中，于最近的下次更新时间发布所撤销证书，或签发临时CRL发布所撤销证书；电子认证服务机构如提供OCSP服务，必须立即更新OCSP查询数据库，确保实时发布所撤销证书。

证书撤销后，应通过电话、邮件、在线等方式，及时告知用户或依赖方证书撤销结果。

电子认证服务机构必须记录所有证书撤销请求和相关操作结果。

5.1.6 证书冻结

证书冻结有下列3种发起方式：

a) 由证书用户发起——用户申请冻结证书，电子认证服务机构必须明确规定冻结证书申请的接受方式，如通过电话、邮件、在线申请等，以及审核程序。

b) 由电子认证服务机构发起——电子认证服务机构如发现用户证书申请资料存在虚假信息、不能满足证书签发条件等情况，或者发生(或怀疑发生)电子认证服务机构CA私钥泄露、认证系统存在安全隐患威胁用户证书安全等情况，可以不经过证书用户本人同意，予以冻结证书。

c) 由依赖方发起——当依赖方提出证书冻结申请时，如证书仅用于依赖方的系统，可以不经过证书用户本人同意，予以冻结证书。

冻结的证书需在 CRL 中发布，当被冻结证书失效后，将不再出现在 CRL 中。

在证书有效期内，对被冻结的证书有 3 种处理方式：

a) 被冻结证书有效性无法验证，用户和依赖方不能使用证书；

b) 被冻结证书转为正式撤销；

c) 被冻结证书解冻，从 CRL 中删除，重新转为有效证书。

证书冻结后，电子认证服务机构必须在周期性签发的 CRL 中，于最近的下次更新时间发布所冻结证书，或签发临时 CRL 发布所冻结证书；电子认证服务机构如提供 OCSP 服务，必须立即更新 OCSP 查询数据库，确保实时发布所冻结证书。

冻结的证书解冻后，电子认证服务机构应在周期性签发的 CRL 中，于最近的下次 CRL 更新中删除冻结的证书，电子认证服务机构如提供 OCSP 服务，应立即更新 OCSP 查询数据库，确保解冻的证书变为有效。

证书冻结和解冻后，应通过电话、邮件、在线等方式，及时告知用户或依赖方冻结和解冻结果。

电子认证服务机构必须记录所有证书冻结请求和相关操作结果。

5.1.7 证书状态查询

电子认证服务机构应为用户和依赖方提供如下 2 种证书状态查询服务（包括证书撤销列表和/或在线证书状态查询）：

a) CRL 查询。电子认证服务机构必须能够提供证书撤销列表（CRL）查询服务，CRL 发布必须符合标准；必须明确规定 CRL 发布周期和发布时间，宜每天签发 CRL；根据证书策略或当发生严重私钥泄露情况时，电子认证服务机构可签发临时 CRL；根据证书策略和依赖方协议，用户和依赖方应及时检查、下载临时 CRL。

在证书有效期内的，被撤销证书必须一直保留在 CRL 中直至证书过期失效，被冻结证书在冻结期内必须保留在 CRL 中直至解冻。当被撤销或被冻结证书过期时，应从 CRL 中删除。

电子认证服务机构发布的所有 CRL 必须定期归档保存，在证书失效后至少保留 5 年。

b) OCSP 查询。电子认证服务机构必须能够提供在线证书状态查询（OCSP）服务，查询数据格式和响应查询结果必须符合国家有关标准；必须保证查询服务响应速度和并发查询性能满足服务要求；必须保证查询结果的实时性和准确性。

5.1.8 证书归档

电子认证服务机构应定期对过期失效以及被撤销的证书进行归档。

在证书失效至少 5 年后，方可销毁归档数据。

5.2 用户证书密钥服务

电子认证服务机构必须说明所提供的证书类型及密钥对产生的方式，并告知证书用户和依赖方电子认证服务机构是否保存有用户证书私钥的备份。

5.2.1 用户证书密钥的产生、传递和存储

通常情况下，用户的签名证书的密钥对由用户自己在其密码设备中生成，并由用户控制。

用户加密证书密钥对可由用户自己产生，或者由电子认证服务机构通过密钥管理中心集中生成，并通过安全的途径传送给用户。若加密证书密钥对由电子认证服务机构通过密钥管理中心集中生成，则加密证书私钥在传送给用户的过程中，不能以明文形式出现。当电子认证服务机构通过密钥管理中心

为用户生成加密证书密钥对时，电子认证服务机构可将加密证书私钥的备份加密保存在密钥库中，以便在必要的时候恢复用户加密证书私钥。

5.2.2 用户证书私钥激活数据的产生、传递和存储

用户加密证书密钥对及其私钥激活数据可由用户自己产生和保存，或者由电子认证服务机构通过密钥管理中心集中生成。在后者的情况下，电子认证服务机构代用户产生的私钥激活数据必须有足够的安全强度并通过一定的安全方式传送给用户，确保激活数据在传递过程中不被泄漏，并对传递过程进行跟踪和记录。

5.2.3 用户证书私钥恢复

电子认证服务机构不应保存用户签名证书的私钥备份。

若电子认证服务机构保留有用户加密证书的私钥备份，则只能应用户自己要求或司法恢复需要，电子认证服务机构才能对用户加密证书的私钥进行恢复。

私钥恢复应有多人参与才能完成，且应对操作过程及结果进行记录。

5.2.4 用户证书密钥对的更新

用户在进行证书更新时应同时更新证书的密钥对。若出于特别的原因和安排，允许用户在进行证书更新时不更新证书的密钥对，那么电子认证服务机构必须确保这种方式是安全的，且必须为不更新的密钥对规定一个适合的、安全的最大期限，在这个期限后，该密钥不能再使用。

5.2.5 用户证书私钥的归档和销毁

电子认证服务机构不得拥有用户签名证书私钥，用户签名证书的私钥由用户自己根据需要进行管理和销毁。用户加密证书的密钥对由电子认证服务机构的密钥管理中心产生，在用户密钥对、证书失效后，电子认证服务机构应以加密的方式归档保留；所有归档密钥对，应至少在证书失效5年后方可销毁，销毁方式应能可靠地、彻底地销毁密钥信息。

5.3 认证系统功能要求

电子认证服务机构使用的认证系统应符合GB/T 25056—2010中的要求，能够提供用户证书的申请、签发、存储、发布、更新、撤销、冻结、状态查询、归档以及用户证书密钥管理等功能。

5.4 认证业务流程要求

认证业务流程应符合如下要求：

a) 对于证书申请审核过程，电子认证服务机构应根据认证业务规则，制定严格的证书申请审核流程和规范，鉴别证书申请者提供的身份信息的真伪，验证证书申请者的身份，确认是证书申请者所声称的人、机构在申请证书。

b) 对于证书更新的自动审核方式，电子认证服务机构必须确保能够通过一定的方式控制哪些证书可自动更新，防止非授权的更新。

c) 电子认证服务机构应制定证书撤销管理策略和流程，确保撤销过程的规范和撤销结果的准确、及时。

d) 电子认证服务机构可根据具体业务需要，制定证书冻结策略和流程，包括冻结请求、条件、宽限期及冻结状态的发布等。

e) 电子认证服务机构应在CP和CPS中发布证书状态查询服务策略，并在相关协议中明确提示证书用户和依赖方，使用证书时必须使用证书状态查询服务。

f) 电子认证服务机构应制定证书归档策略，以保证对过期失效以及被撤销的证书及时归档。

g) 电子认证服务机构应制定用户证书密钥和私钥激活数据的传递策略，以保障传递过程中的安全性。

h) 电子认证服务机构应制定严格的用户证书私钥恢复的管理规定和流程，确保用户私钥恢复的规范性和安全性。

i) 电子认证服务机构应制定用户证书私钥归档、销毁流程，保证私钥被安全地归档或销毁，确保私钥不会泄漏。

6 业务运营中的风险

电子认证服务机构在业务运营过程中面临着各类风险，包括系统风险、物理环境风险以及管理风险等。附录 A 对各类风险进行了举例说明，以供参考。

本标准后面各章节描述了电子认证服务机构为应对各类风险所应采取的控制措施。

7 认证系统运行要求

7.1 网络系统安全

网络系统安全应符合如下要求：

a) 电子认证服务机构及其注册机构的认证系统运行网络，必须采用独立的接入链路与公共网络连接，并与办公网络隔离，网段划分应符合 GB/T 25056—2010 中的要求。

b) 网络访问策略应只允许必需的访问，设定允许访问的主体（主机、端口）和对应的访问对象（主机、端口）以及连接方向，其他访问禁止。

c) 应对网络中的实体设备进行网络漏洞扫描，根据检测结果及时发现存在的不安全网络协议、网络服务，将不需要的网络协议、网络服务关闭，对于因业务需要而开启的不安全网络协议、网络服务应采取相应措施，使用更安全的网络协议、网络服务进行替换。

d) 应在关键网段安装入侵检测系统，能够及时检测到并报告常见的入侵模式，能够且应该及时更新入侵模式知识库，具备完善的日志与审计功能。

e) 实施网络服务安全配置与加固，只开启必需的网络服务，关闭其他的网络服务；对开启了的网络服务进行优化配置，定期打补丁。

f) 网络应采用通过安全检测、安全认证的网络设备，如路由器、各类安全网关、交换机等。

g) 若网络设备账户使用用户名/口令方式进行身份鉴别，则口令应具有足够的安全强度。

h) 网络设备应有完备的审计日志。

i) 采取其他必要的安全措施，保障运营网络的安全。

7.2 主机系统安全

主机系统安全应符合如下要求：

a) 应通过主机漏洞扫描系统发现系统存在的安全漏洞，并采取应对措施，包括进行系统安全优化等。

b) 应及时对系统安全漏洞打补丁，并采取防病毒措施，同时考虑采用其他系统安全加固技术，保障主机系统安全。

c) 主机系统应只创建、开启必需账户，关闭不需要的默认账户，账户口令应具有足够的安全强度，确保只有授权用户、进程和应用才能访问相应的资源。

7.3 系统冗余与备份

7.3.1 系统冗余

应采用设备冷/热备份、单机逻辑备份、双机备份等方式，对于生产系统的重要设备进行备份/冗余设置和容错设计。

应采用冗余技术、路由选择技术、路由备份技术等技术手段，实现网络备份与冗余。

a） 网络链路冗余

认证系统的网络对外应采用双路接入，并且两路网络接入来自不同的网络设施运营商，一路网络接入作为主服务线路，另一路接入作为备用线路，当主服务线路出现故障时能够迅速切换到备用线路。

b） 主机冗余

认证系统对关键业务、功能所在主机必须采用双机热备措施。对非关键业务、功能的设备，应该至少采用硬盘冷备份的方式进行系统备份。

c） 电源冗余与后备发电

对电子认证服务机构的电源有如下要求：

1） 放置有认证系统的数据中心宜采用双路供电系统，即从建筑外至数据中心内至少具有两条供电线路；

2） 必须为认证系统及安全设备提供不间断电源（UPS），且不间断电源设备应该具有冗余，不间断电源提供的电力必须足够支持通常的断电时间；

3） 有条件的电子认证服务机构应配置备用发电机，当出现停电且不间断电源不能提供持续的电力时，能够提供电力。

7.3.2 系统备份

电子认证服务机构应采用完全备份与增量备份相结合的方式对生产系统数据和信息进行备份。

应制定备份数据收集、保管、押运、恢复的管理策略，确保备份数据的安全，防止泄露和未经授权的使用。备份数据宜实行同城异地保管，如租用银行保管箱保存数据备份。

应定期检查备份系统和设备的可靠性和可用性，定期检查备份介质可靠性和数据完整性。

应根据设备的重要程度、故障频率、供应难度、库存数据量、设备金额等因素，综合评估运营风险，确定并建立关键设备和系统备份管理办法。应对关键设备做备份或采取有效办法保证供应的及时性（如与供应商签订应急维修或紧急供货合同）。

a） 软件与数据备份

软件与数据备份包括如下内容：

1） 主机操作系统；

2） 系统应用软件，如邮件系统、Web 服务程序、数据库系统等；

3） 认证系统软件；

4） 系统上的客户定制数据；

5） 系统配置；

6） 数据库用户数据。

对软件与数据备份有如下要求：

1） 必须采用专门的备份系统对整个认证系统进行备份，备份数据可以保存在磁带、硬盘或其他介质上；

2） 备份策略采用全备份与增量备份相结合的方式；

3） 备份策略应该保证没有数据丢失或数据丢失不会造成实质性的影响；

4) 在系统出现故障、遭遇灾难时，备份方案能够在最短的时间内从备份数据中恢复出原系统及数据；
5) 选择的备份介质应能保证数据的长期可靠，否则应定期更新；
6) 备份数据应存放在电子认证服务机构以外安全的地方，比如银行保管箱、灾难恢复中心等。

b) 硬件设备备份

电子认证服务机构硬件设备必须具有冗余、备份，在系统设备出现故障、损坏时能够及时更换。

7.4 系统运营维护安全管理

7.4.1 系统权限管理

电子认证服务机构应制定系统访问控制方面的管理规定，制定访问控制权限分配表，正确设置系统的用户角色和相应权限，所有运营维护只被赋予必须的、最小的权限，并对关键的、敏感的操作进行权限分割。

7.4.2 系统操作管理

系统操作管理应符合如下要求：

a) 应根据生产系统建设厂商的维护要求，制定运营维护策略和流程。
b) 不经批准不得在服务器上安装任何软件和硬件；不经批准不得删除服务器上的任何文件。
c) 应正确配置安全设备、网络设备、业务系统，定期检查、测试配置策略的有效性。应及时分析入侵检测系统的日志和所发现的问题，及时响应安全事件，调整安全策略。
d) 应有与生产系统功能相一致的测试系统，用于功能、补丁的部署、升级等测试用途。测试系统中不得使用生产系统的业务数据。
e) 应及时升级系统和数据库补丁包、安全包；及时升级防病毒软件病毒库；及时升级入侵检测系统、防火墙及网络设备固件等。只有在测试系统中经测试合格后，方能在生产系统上正式部署。
f) 应监控系统容量需求，制定未来容量需求的项目计划，保持适当的处理能力和存储能力。
g) 生产系统的任何调整和升级，应先制定详细的技术实施方案，经电子认证服务机构的安全策略管理组织审核批准后，方可实施，并应有完整的实施记录。
h) 对系统的任何操作，应做好操作记录。系统的事件和日志应及时归档保存。

7.4.3 系统变更和升级

应制定严谨的系统变更和升级的申请及审批策略、操作流程及验收标准，明确管理责任和程序，严格遵守管理控制程序，防止因为系统的变更和升级影响认证系统的正常运行。系统变更和升级应遵循如下准则：

a) 对设备、软件或程序的所有变更制定严格的程序。
b) 变更、升级前，对原系统业务数据和业务系统进行全备份。
c) 保证原有系统中的数据到变更、升级后系统的平稳过渡。
d) 系统变更和升级的实施方案和过程不应对已有客户、用户产生严重的影响。

7.4.4 账户、口令管理

应对网络设备和主机系统的账户口令的安全强度、使用期限、更换频率、保管手段、传输方式等进行要求和管理；应确保网络设备、主机和应用程序中没有设置默认的用户名、口令。

7.4.5 系统安全监控

电子认证服务机构应在系统的各个重要环节设置各类监测、防护设备，实时监测网络数据流量，监视并记录内部、外部用户的操作行为，监测并记录各类安全事件，如攻击、入侵、病毒等，能对异常的行为和安全事件采取相应的控制并及时报警。

电子认证服务机构应在运营场地管理区建立专门的系统监控室，由系统安全监控人员通过监控系统和设备对运营系统的运行状况、安全状况进行实时监控。当安全监控人员发现异常情况或安全事件后，应及时采取措施进行处理和记录，并报告安全主管，对于严重的安全事件，须上报安全策略管理组织。

7.5 密码设备安全管理

7.5.1 认证系统密码设备管理

认证系统所使用的密码设备应符合如下要求：

a) 购买和运输

电子认证服务机构及其注册机构购买、使用的密码设备，必须是通过国家密码管理机构审查的设备。

密码设备从制造商到电子认证服务机构的运输过程应安全可靠，防止篡改或非授权地接触。

电子认证服务机构收到密码设备后，应及时确认密码设备没有被替换或改动。

b) 保管和存储

电子认证服务机构应委派可信人员负责密码设备的接收、存储、保管、领用等流程，并留有完整的记录。

c) 安装、升级和维修

电子认证服务机构的密码设备，在运营环境中的安装、拆卸、硬件更换、固件和软件升级等过程中应有两名以上可信人员现场监督。

对密码设备进行故障诊断时，必须有两名以上可信人员在场；密码设备的维修必须始终处于电子认证服务机构可信人员的控制中。

d) 功能测试

新设备或密码设备修复后，在安装到认证系统使用前，应进行功能测试，只有测试正常方能投入使用。

认证系统所有密码设备应做周期性测试和校验，并做好相应记录。

e) 报废和销毁

生产系统中的密码设备不再使用后，应进行报废。所有报废必须经过审批，然后在安全环境中进行删除或归零操作，清除其中的密钥信息，并实施硬件销毁。报废和销毁必须有相应的记录。

7.5.2 用户密码设备管理

电子认证服务机构为用户提供的、用于生成和存储用户私钥的密码设备，在管理上应符合如下要求：

a) 用户密码设备应是经国家密码管理机构批准生产和销售的密码设备。

b) 电子认证服务机构应建立采购、测试、保管、使用、废弃等管理制度。

c) 用户密码设备的管理应由可信雇员执行。

d) 用户密码设备经测试功能正常后，方可进入生产流程。

e) 电子认证服务机构应采用适当措施，保证用户能安全地获得密码设备和激活数据。

f) 电子认证服务机构应对密码设备各阶段的管理信息进行记录。

7.6 CA 密钥和证书管理

7.6.1 CA 密钥的生成和存储

电子认证服务机构 CA 密钥(含根密钥)必须使用通过国家密码管理机构审查的设备生成,并在其中存储。

电子认证服务机构必须制定认证系统 CA 密钥的生成流程、操作等文档,在安全的(包括物理环境安全、流程安全以及参与的人员安全控制等)环境中操作。操作过程中应有操作员、见证人以及 CA 私钥激活数据保管员同时在场,并应对 CA 密钥的生成操作过程进行录像或拍照。

在整个 CA 密钥生成过程中,所有关键步骤都要进行记录,以备审计。

离线 CA 私钥必须保存在核心区;存放在线 CA 私钥的密码设备必须位于屏蔽区域。

7.6.2 CA 私钥激活数据的管理

电子认证服务机构应确保 CA 私钥激活数据在生成、保管及分发过程中安全可靠。

7.6.3 CA 密钥的使用

应建立管理制度对 CA 密钥及其激活数据的使用权限进行严格控制,每次使用应有书面记录,记录应包括每次使用的时间、用途及操作人员等内容。

7.6.4 CA 密钥的备份与恢复

为了防止存储 CA 密钥的硬件发生损坏导致数据丢失,CA 密钥在生成之后,应进行克隆备份,以便在必要时进行恢复。

a) CA 密钥备份

电子认证服务机构应制定 CA 密钥备份策略,对 CA 密钥进行备份。备份必须使用秘密共享和加密存储机制,确保 CA 私钥不会以明文形式出现在密码硬件之外。被分割的秘密可以是 CA 私钥备份恢复数据(如口令)或 CA 私钥本身,秘密共享采用公开的 m of n 算法($m \geqslant 60\% \times n$),各秘密份额保存在不同的 IC 卡或智能密码钥匙中,并分发给不同的可信人员持有。

密钥备份必须妥善保存在核心区内,并实行双人访问控制存取。可保存于具有防火、防热、防潮、防尘、防磁、防静电功能的保险柜中。保险柜应能保证在 1 000 ℃火灾现场,纸张防火柜内温度保持≤180 ℃、磁盘防火柜内温度保持≤52 ℃不少于 1 h。

b) CA 密钥恢复

当需要进行 CA 密钥恢复时,应有操作员、见证人、私钥恢复秘密份额保管员同时在场,由满足恢复要求的数量的秘密份额保管员输入分割数据,按照一定的算法进行合成并恢复 CA 密钥到密码设备中。应将恢复操作全程进行记录。

7.6.5 CA 密钥的销毁

电子认证服务机构必须制定彻底清除或销毁存储 CA 私钥密码设备的操作流程和办法,对因退出产品系统、超过归档期限或其他原因需要销毁的 CA 密钥对进行安全销毁,即销毁或归零存放私钥的密码设备。

7.6.6 CA 证书的创建和发布

CA 证书的创建,应事先进行审批,过程中做好记录,并在创建后适时发布,以保证用户和依赖方能

及时、安全的获取。

7.6.7 CA 证书的更新

电子认证服务机构的 CA 证书可能会因为如下原因进行重新签发，称为“CA 证书更新”：

——延长有效期；

——更换密钥对；

——改变证书的其他信息(如签名算法、扩展项等)。

CA 证书更新时，应采取与生成初始证书相同的流程和方法。

对于更换密钥对的证书更新，则应采取与生成 CA 密钥相同的流程和方法。

7.6.8 CA 证书的撤销

CA 证书可能会被撤销的原因包括不再使用、私钥损坏、私钥泄漏或怀疑泄漏以及被认为需要撤销的其他原因。

CA 证书的撤销操作，应如创建操作一样，事先进行审批，并做好撤销操作的记录；在被撤销后，相关信息被纳入到 CA 的 CRL 中，并及时发布。

7.6.9 CA 密钥和证书的归档

CA 证书失效后，必须将失效的 CA 密钥及 CA 证书归档并妥善保存。在证书失效至少 5 年后，方可销毁归档的 CA 密钥；归档数据和操作宜做签名。

8 物理环境与设施

8.1 运营场地

电子认证服务机构及其注册机构提供电子认证服务必须有固定和适宜的运营场地(数据中心)。

电子认证服务机构的场地环境建设应符合以下标准：

a) 计算机机房(数据中心)的安全建设应符合 GB/T 9361 的要求；

b) 活动地板应该具有稳定的抗静电性能和承载能力，同时应耐油、耐腐蚀、柔光、不起尘，具体应符合 SJ/T 10796 的要求；

c) 计算机系统的供电电源技术指标、相对湿度控制、接地系统设置等应按 GB/T 2887 中的规定执行；

d) 计算机机房的耐火等级应符合 GB 50045 及 GB/T 9361 的规定；

e) 计算机机房设计应符合 GB 50174 的规定。

8.2 运营区域划分及要求

8.2.1 基本要求

电子认证服务机构机房场所为安全控制区域，必须在机房场所的周边建立明确和清晰的安全边界(设置标志、物理障碍、门禁管理系统等)，进行物理保护；安全边界应完善和完整，能及时发现任何入侵企图；安全边界应设置向外开启的消防通道防火门，并应能快速关闭；消防门应有防误开启标识和报警装置，开启时应能以声、光或电的方式向安全监控中心报警。

安全区域应使用合格门锁，门应坚固，保证关闭安全；应使用合适的门禁系统和辅助设备，如加装闭门器、门位置状态检测器和门开启报警器等；采取必要措施，在各个区域防止尾随进入。

安全区域物理环境的任何变更，如设备或系统的新增、撤销、部署调整等，必须事先完成风险评估和

安全分析，形成正式文档向电子认证服务机构的安全策略管理组织申报，经审核批准后，方可实施，同时应做好完整的过程记录。

8.2.2 区域划分

电子认证服务机构机房场地根据业务功能分为公共区、服务区、管理区、核心区，各功能区域对应的安全级别为控制区、限制区、敏感区、机密区，安全等级和要求逐级提高。安全等级要求越高，安全防护措施和配套设施要求越严格。

宜使用层级式安全区域防护进行安全区域隔离和物理保护。层级式安全区域防护是指将安全区域按照安全等级的重要程度，由外向内安全级别逐步提高，且只有经由较低级别的区域方能进入更高级别安全区域。

不宜划分层级式安全区域的机房场所，应按照安全等级功能等同的原则保护各安全区域。

a) 公共区(控制区)

电子认证服务机构场地的入口处、办公区域、辅助和支持区域属于公共区，应采用访问控制措施，如使用身份标识门禁卡控制出入。

b) 服务区(限制区)

服务区是提供证书审批、证书管理等电子认证服务的区域，必须使用身份标识门禁卡控制出入。

c) 管理区(敏感区)

该区域是电子认证系统运营管理区域，系统监控室、场地安全监控中心、配电室等均属于该区域。此区域必须使用身份标识门禁卡控制出入，推荐使用人体特征鉴别控制出入。

d) 核心区(机密区)

证书认证系统、密钥管理系统、离线私钥和私钥激活数据存放房间属于核心区。核心区必须使用身份标识门禁卡和人体特征鉴别身份，控制出入，且在核心区内必须采取职责分离与权限分割的方案和措施，使得单个人员在核心区内无法完成敏感操作。

在核心区内，放置有在线签发数字证书的CA私钥的密码设备的区域，必须是至少符合GB/T 9361要求的屏蔽区域，该区域必须有安全的出入控制，且必须采取职责分离与权限分割的方案和措施，使得单个人员在屏蔽区域内无法完成敏感操作。

8.3 安全监控系统

宜设置专门用途的安全监控中心，对机房建筑整个区域发生的出入访问进行实时监控。

8.3.1 门禁

电子认证服务机构机房区域必须采用适宜的门禁管理系统进行物理场地访问控制管理。

门禁系统应能支持以电子身份识别卡、生物特征、PKI/CA技术等单独或以组合形式的方式鉴别身份；应能控制电子认证服务机构整个运营场地的所有出入口；应能识别、区分正确进出方式，如未刷卡进入，则不能刷卡离开；应能与安全侦测布防系统结合，对各个区域进行安全布防，侦测到异常活动时，应具备报警功能(如声光报警、短信/电话报警、门禁联动锁止等)；门禁系统应有备用电源，能保证不间断进行访问控制；系统应有完善的事件记录和审计控制；门禁系统控制中心应位于安全监控中心或相同安全等级的区域内。

在发生紧急情况(如电力故障、消防报警)时，所有消防疏散通道受控门应处于开启状态，重要区域如核心机房、资料室等区域应处于外部关闭、内部可手工开启的状态；前述重要区域应有应急开启装置，且当应急开启装置开启时，必须以声、光、电的方式发出报警信号，同时系统应显示报警区域并记录应急情况发生的详细信息。

应定期将门禁记录整理归档，并保存合理时间。

8.3.2 入侵检测

在机房场所建筑区域内应安装入侵检测报警系统，进行安全布防。安全区域窗户上应安装玻璃破碎报警器，建筑内天花板上应安装活动侦测器，发生非法入侵应立即报警。

入侵检测系统应有应急备用电源提供电力支持，保证在出现外部供电中断时系统能够不间断地运行。

8.3.3 监控录像

必须设置合适的监控点，采用录像集中监控对整个机房的活动区域进行 24h 不间断的监控。录像记录可以采用两种方式，一种为不间断录像；另一种为采用活动侦测系统与录像相结合的方式，不间断监控，间断（活动侦测）录像。

合理调整录像监控镜头位置，应能有效识别进出人员和记录操作行为；录像记录应安全保管并定期归档，录像记录的查阅必须经安全主管批准。录像记录最少保留 3 个月；重大活动记录应保留 1 年以上，可采用刻盘备份等形式。

监控录像系统应配有应急备用电源提供电力支持，保证在出现外部供电中断时系统不间断运行。

8.4 环境保护与控制设施

8.4.1 空气和温湿度控制

必须有完备的空调系统，保证机房有充足、新鲜和洁净的空气供应；保证机房各个区域的温湿度能满足系统运行、人员活动和其他辅助设备的要求。

8.4.2 防雷击和接地

必须采用符合国家标准的防雷措施。

必须设置综合地线系统；屏蔽机房必须设立保护地线，应经常检测接地电阻，确保人身、设备运行的安全；应设置交流电源地线，交流供电应采用符合规范的三芯线，即相线、中线、地线。

计算机系统安全保护地电阻值、计算机系统防雷保护地电阻值应符合 GB 50057 和 GB 50343 的有关规定。

8.4.3 静电防护

机房的地板或地面应有静电泄放措施和接地构造，防静电地板、地面的表面电阻或体积电阻应为 $2.5\times10^{4}\ \Omega\sim1.0\times10^{9}\ \Omega$，且应具有防火、环保、耐污耐磨性能。

8.4.4 水患防治

应正确安装水管和密封结构，合理布置水管走向，防止发生水害损失。机房内应进行防水检测，发现水害能及时报警。

8.4.5 消防设施

建筑材料耐火等级应符合 GB 50045 的规定。

办公区域必须设置火灾自动报警系统和灭火系统，可以使用水喷淋灭火装置，并应配备合理数量的手持灭火器具。

认证系统所在机房必须安装火灾自动报警系统和自动灭火系统，火灾探测系统应能同时通过检测温度和烟雾发现火灾的发生，且火灾报警系统应与灭火系统联动。

火灾报警系统包括火灾自动探测、区域报警器、集中报警器和控制器等，能够对火灾发生区域以声、光或电的方式发出报警信号，并能以手动或自动的方式启动灭火设备。用于生产系统的灭火系统，不得

使用水作为灭火介质，必须使用洁净气体灭火装置。宜使用惰性气体如 IG541 作为灭火介质。

凡设置洁净气体灭火系统的机房区域，应配置一定数量的专用空气呼吸器或氧气呼吸器。

8.5 支撑设施

8.5.1 供配电系统

供配电系统布线应采用金属管、硬质塑料管、塑料线槽等；塑料件应采用阻燃型材料；强电与弱电线路应分开布设；线路设计容量应大于设备总用量；应设立独立的配电室，通过配电柜控制供电系统。

应使用双路供电，并配备适当设备（如在线式 UPS），保障机房（数据中心）有不间断的供电。当出现意外情况导致供电中断时，应至少持续向机房提供 8 h 的供电。

8.5.2 照明

机房工作区域主要照明应采用高效节能荧光灯，照度标准值为 500 lx，照明均匀度不应小于0.7 lx；主要通道应设置通道疏散照明及疏散指示灯，主机房疏散照明照度值不应低于 5 lx，其他区域通道疏散照明的照度值不应低于 0.5 lx。

8.6 场地访问安全管理

电子认证服务机构应制定物理场地授权与访问规定，合理控制物理场地权限，保障场地安全。

内部人员因工作需要，可被赋予访问相应物理场地的权限。没有访问物理场地某区域权限而确因工作需要访问该场地区域的内部人员，在访问该区域时，必须由具有相应权限的人员全程陪同，并做好访问记录。

外来人员出入日志由电子认证服务机构陪同员工负责填写。所有外来人员进入、离开电子认证服务机构应有记录，能审计全部访问行为，并应定期将访问控制记录归档保存。

8.7 场地监控安全管理

电子认证服务机构必须安排安全人员通过场地安全监控设备对运营场地进行 7×24 h 监控，发现可疑问题或安全事件应及时处理，记录并及时报告上级安全主管。对于严重的安全事件，必须上报安全策略管理组织。

安全监控人员不得擅离职守，运营场地任何时候都必须有安全人员值守。

8.8 注册机构场地安全

RA 系统可在电子认证服务机构中建立、运行，也可在注册机构中建立、运行。运行 RA 系统并开展 RA 业务的机构，其运营场地和设施应符合如下要求：

a) 注册机构场地应有门禁监控系统，及为 RA 系统的各类设备提供电力、空气和温湿度控制、消防报警和灭火功能的支撑系统和环境保护设施；注册机构也可选择符合上述条件的 IDC 放置 RA 系统设备。

b) 使用了密码设备的 RA 系统，应另设专门的控制区域，对密码设备进行适当保护。

9 组织与人员管理

9.1 职能与角色设置

9.1.1 必需的部门职能

电子认证服务机构应设立开展电子认证服务所需的职能部门：

a） 安全策略管理部门

负责制定、批准、发布、实施、废止电子认证服务机构总体信息安全策略、安全管理制度，并监督、检查安全运营和生产活动。

b） 安全管理部门

监督生产系统、密钥管理、物理场地、设备、电力和网络基础设施的安全运作，对员工可信的控制等，规避主要风险。

c） 运营管理部门

负责对生产系统进行维护，协调和监督生产系统、密钥管理和运营物理环境等基础设施正常运行。

d） 人事管理部门

建立可信人员策略（包括岗位可信人员要求、背景调查内容和程序执行等内容），执行可信人员背景调查，并对可信人员进行管理。

e） 认证服务部门

对证书用户的身份真实性、过程真实性进行鉴别和验证，以及对证书用户资料进行规范管理。

f） 技术服务部门

解决用户在证书使用过程中的各种技术问题，为用户提供相关技术支持服务。

9.1.2 必需的岗位角色

电子认证服务机构应设置如下必需的岗位角色：

a） 安全策略管理组织负责人

负责安全策略管理组织的管理工作。

b） 安全管理人员

包括安全经理和负责网络与系统安全管理、场地安全管理的专业人员。

c） 密钥管理员

负责 CA 密钥和证书管理，以及核心区的密码设备管理。

d） 系统维护员

负责办公系统和认证系统的维护。

e） 鉴别与验证员

负责确认用户身份的真实性，确认用户证书服务请求的真实性，确保证书签发给正确的实体。

f） 客户档案管理员

负责管理客户资料档案。

g） 客户服务员

为客户提供技术咨询、技术支持和售后服务。

h） 审计员

负责对涉及系统安全的事件、各类管理和操作人员的行为进行审计和监督，确保遵从法律法规以及本机构安全策略要求，降低运营风险，提高服务质量，保证经营的可持续性。

i） 人事经理

负责制定可信人员政策，对关键岗位人员进行管理。

9.2 安全组织

电子认证服务机构应设立安全策略管理组织，如安全策略管理委员会，通过电子认证服务机构跨部门的执行层、业务管理层和行政管理层等不同部门管理人员协同完成电子认证服务机构整体的运营管理、风险控制和发展战略。

电子认证服务机构应设立贯彻安全策略、执行安全制度的安全管理部门，设置安全经理、网络与系

统安全管理人员、场地与设施安全管理人员、及审计员等安全管理岗位，建立覆盖企业内部和外部业务活动的信息安全组织架构。

9.3 人员安全管理

9.3.1 人员安全策略

电子认证服务机构应制定人员安全策略，对正式员工和临时人员进行有效的安全管理。应在策略中明确定义关键岗位的职责和关键岗位管理要求，对关键岗位应采用职责分割、双重控制、岗位轮换、最小权限等安全管理措施。

9.3.2 可信背景调查

应制定可信人员策略，对正式雇佣的新员工进行可信背景调查。背景调查可分为基本调查和高级调查。对普通雇员执行基本调查，调查内容如教育背景、工作经历等；对关键岗位雇员执行高级调查，调查内容如犯罪记录、信用记录等。

9.3.3 人员可信保障

电子认证服务机构应与员工签订保密协议，并定期对员工进行安全教育和专业培训，确保员工在从事电子认证服务的过程中，知悉自身责任，遵守相关制度，达到所从事岗位的安全要求。

9.3.4 人员异动处理

所谓人员异动是指由于不可预测的事件导致员工不能履行职责或员工不辞而别。电子认证服务机构应制定人员异动管理策略，要求关键岗位必须设置备份人员，以便在意外情况下关键业务职能得到延续，避免人员异动发生而影响企业运营。

10 文档、记录与介质管理

10.1 文档管理

10.1.1 文档归类

电子认证服务机构应对需要管理的文档进行归类，需要归类的文档包括但不限于如下文档。

a) 企业管理类

本类文档包括常规的企业管理文档，如公司组织管理、财务管理、人事管理、资产与设备管理等方面的文档。

b) 安全策略类

本类文档包括人员安全策略、物理环境安全策略、信息系统安全策略、通信系统安全策略、密钥管理策略、审计策略等。

c) 运营管理类

本类文档包括证书策略(CP)、电子认证业务规则(CPS)、认证服务流程与规范、客户服务流程与规范、用户协议、依赖方协议、隐私保护协议、应急响应计划、灾难恢复计划、业务连续性计划等文档。

电子认证服务机构应制定证书策略(CP)与电子认证业务规则(CPS)。证书策略要对电子认证服务机构签发的证书的类型、适用的环境、适用的应用、认证要求、安全保障要求等方面做出广泛而全面的规定。电子认证业务规则须阐述电子认证服务机构如何贯彻实施其证书策略。

认证业务规则的编写应符合 GB/T 26855—2011 的要求。

电子认证服务机构应对证书策略和电子认证业务规则进行有效管理，设有负责撰写、修改、审核、发

布和管理的部门，并制定相应的管理流程。

电子认证服务机构应根据其业务内容的变化，及时修改、调整其证书策略与电子认证业务规则。

证书策略与电子认证业务规则及其修改版本，必须经过电子认证服务机构的安全策略管理组织批准后才能公开发布。

d） 客户类

本类文档包括客户合同、客户资料、审批材料等开展电子认证业务过程中产生的文档。

提供公共服务的电子认证服务机构，应对其提供的证书业务同客户签订或通过某种方式向客户明示相应的法律协议，这些协议对客户和电子认证服务机构所承担的责任和义务以协议的形式给出明确的规定和说明。通常的法律协议有订户协议、依赖方协议、服务协议等。

当电子认证服务机构以外的实体要作为电子认证服务机构的一个注册机构提供认证业务时，电子认证服务机构与该实体须通过相应的协议明确规定双方，特别是作为注册机构的一方，应该承担的责任和义务，还包括该证书拥有者（证书用户）和依赖方应承担的责任和义务。

10.1.2 注册机构的文档

注册机构应制定与电子认证服务机构一致的安全策略及运营管理规范，如认证服务流程与规范、系统运行维护流程与规范、人员管理规范等。相关安全策略及运营管理规范需经过电子认证服务机构的安全策略管理组织批准才能实施。

对于授权承担 RA 职能的机构，电子认证服务机构应与其签订相应的协议，明确双方的权利、义务和责任。

10.1.3 人员与制度

电子认证服务机构应制定专门的文档管理制度，并指派专门人员负责管理各类文档。

10.1.4 文档保存

对于重要的纸质文档，如资质文档、重要文件等，应设置专门地点保存，防止文件受潮、损坏及遗失、被盗。

电子文档应放置在专门的服务器上，并设置有相应权限，由专人负责管理。

10.1.5 使用控制

根据策略和文档不同的安全等级，必须制定保管、借阅审批、登记、专控制度；对于机密和敏感文档，应限定借阅范围，并应经过相应级别负责人审批，同时做好登记。

作为可信第三方的电子认证服务机构会获得用户的各种信息，电子认证服务机构应制定严格的客户信息保密政策和制度，确定哪些客户信息是保密的，哪些客户信息是可公开的，对于需要公开的信息应该让客户事先知晓。无论电子认证服务机构还是其员工，都不能在未经客户许可的情况下向其他机构或个人透露客户信息。如因某种原因确实需要公开或向其他机构提供客户的信息，则事先应让客户知晓并获得客户同意。

为了配合国家的行政和执法的需要，电子认证服务机构有可能需要在客户不知晓的情况下向国家有关行政、执法机构提供客户的涉密信息，对此，电子认证服务机构应事先向客户说明电子认证服务机构有责任和义务提供这种协助。

10.1.6 文档销毁

应制定文档销毁流程，对机密和敏感文档的销毁应经过审批，并由专门人员销毁。

10.2 记录管理

10.2.1 记录种类

电子认证服务机构应保存完整的系统运行、安全监控、证书和密钥生命周期管理、设备管理、人员管理等方面的记录，具体的需保存的记录包括但不限于如下记录类别：

a） 物理场地与设施日常管理记录

场地值班巡检日志、场地安全事件日志、人员进出登记、设备维护巡检日志等。

b） 安全监控记录

物理场地的监控录像、门禁进出电子记录、场地入侵检测记录等，特别是报警记录。

c） 密码设备管理记录

密码设备购置、运输、测试、使用、存放、维修、销毁等方面的记录。

d） 密码设备操作使用记录

与认证业务有关的密码设备的操作使用记录，包括什么人、什么原因、在什么地方、使用了什么密码设备，进行了哪些操作，其他在场的参与人员或见证人员等。

e） CA 证书和密钥维护记录

CA 证书与密钥生命周期管理的相关记录。

f） 认证系统运行日志

记录认证系统的运行状况，如启动、运行是否正常，是否出现错误以及错误的类别，系统性能数据等。认证系统运行日志主要用于系统故障的监测和诊断，以及系统性能的分析。

g） 运营网络安全监测记录

对网络、主机、安全设备、以及软件的监测记录，特别是安全事件记录。

h） 认证系统操作日志

证书管理员在证书服务过程中使用认证系统的各种操作记录。

i） 认证服务记录

认证服务过程中的各类操作记录，如证书申请的鉴别与验证、批准或拒绝等。

除认证系统运行日志、运营网络安全监测记录根据需要设定合理的保存期限外，所有与运营有关的记录，包括运营网络安全监测记录中与安全事故、事件有关的记录，都需至少保留 1 年以上至完成运营审计。

10.2.2 记录管理要求

记录的查阅应仅限于特定人、特定目的，如审计人员进行周期性审计时方可查阅。

电子认证服务机构应定期对记录进行归档处理，并应防止归档记录被未授权的修改或销毁。对于归档的电子记录，可进行数字签名保证数据的完整性，防止被修改或置换。

记录的销毁应经过审批，并由具有相应权限的人员实施。对于纸质记录可使用粉碎机销毁；对于电子记录可采用不可逆、不可恢复的彻底删除方法，包括物理销毁电子记录存储介质的方法。所有的销毁操作过程应记录。

10.3 介质管理

应妥善控制和保管各类介质，包括光盘、硬盘、软盘、移动存储介质以及磁带等，并应完整记录介质的使用、库存、维修、销毁等信息，防止被盗、毁坏、被篡改、未授权访问、信息泄露等情况发生。

10.3.1 保管

应制定介质保管策略与制度，包括购买、存储等过程的管理要求。

10.3.2 使用

应制定介质使用管理策略与制度，明确便携介质进出机房的管理办法。

10.3.3 销毁

介质销毁应经审批，由 2 名可信人员实施，1 人执行 1 人监督，并记录销毁过程。

应采用介质厂家建议的清理或销毁敏感数据的方法。若介质厂家未规定销毁方法，则根据不同的介质，可以采用下列方法清理敏感数据。

a) 覆盖：指将非保密数据写入以前存有敏感数据的存储位置的过程，应注意覆盖的次数能够彻底消除恢复敏感数据的可能性。

b) 消磁：磁介质被擦除的过程，即还原其最初的退磁状态。

c) 销毁：以物理方式销毁存储介质，主要手段有熔炼、瓦解、粉碎。

11 业务连续性要求

为保证向客户提供连续、安全、稳定的服务，防止在发生意外事件、自然灾害后导致服务长时间中断，电子认证服务机构必须制订业务连续性计划。

业务连续性计划应涉及系统冗余与备份、应急处理、灾难恢复，以及建立灾备中心等方面的内容。

电子认证服务机构应设立部门负责业务连续性计划的制订、更新、维护以及相关员工的培训。业务连续性计划应由安全策略管理组织审批。

11.1 业务连续性计划

应对可能引起业务中断的事件进行风险评估，确定中断可能造成的影响（破坏程度和恢复时间），然后根据风险评估结果建立业务连续性战略和计划。

业务连续性计划应规定启动计划的条件、应急流程、恢复流程、培训要求和人员的职责。

业务连续性计划应覆盖电子认证业务的所有关键要素的恢复过程。

业务连续性计划应定义可接受的业务中断时间，恢复时间和故障间的平均时间，并在电子认证业务规则中披露。

业务连续性计划应定期演练、测试和更新，保证其持续有效、可执行。每年应至少组织一次灾难恢复演练，根据演练情况，发现存在的问题和潜在风险，及时更新计划。

11.2 应急处理预案

电子认证服务机构应针对影响认证业务正常运营的故障与意外事件，如黑客攻击、网络系统瘫痪、病毒、系统数据破坏或丢失、系统严重故障、CA 私钥损坏、水灾、停电或电力系统故障、人员异动等，制定应急处理预案。

应急处理预案应根据事件的严重程度、紧急程度和事件类别，分别规范告警、报告、保护、处置、善后、总结等处理流程和处置措施。

故障消除或意外事件处理后，应对应急处理过程进行总结，总结中应详细记录事件起因、处理过程、经验教训、改进建议等。

应针对应急事件处理中暴露的问题，不断修改和完善应急处理预案。

11.3 灾难恢复计划

灾难是指由人为因素或不可抗力产生的、对认证业务正常运营产生重大影响的严重故障、事件、事故、自然灾害等。

电子认证服务机构应进行风险分析，确定可能出现的灾难及造成的影响，确定灾难恢复目标，包括

关键业务功能和恢复的优先顺序、灾难恢复的时间范围(恢复时间目标、恢复点目标),制定灾难恢复方案和计划,以便在出现灾难性故障、事件、事故时,能够尽快恢复认证业务。

灾难恢复计划主要包括目标和范围、组织和职责、联络与通讯、应急响应流程、恢复和重续运行流程、灾后重建和回退、计划保障条件、计划附录等内容。

灾难恢复方案必须考虑如何把对用户的影响降到最低。

为保证灾难恢复计划的实施,应设立灾难恢复响应团队,明确具体职责分工,并将团队成员联系方式进行通告和备案。

特别地,当电子认证服务机构发生 CA 私钥泄漏事故时,必须重新生成 CA 密钥、签发 CA 证书、并进行发布,应在 24 h 内通过有效途径(如网站、媒体、电话、邮件等)告知用户和依赖方。

11.4 灾备中心

有条件的电子认证服务机构应建立灾备中心,在主运营场地出现灾难而不能正常运营时,在最短时间内,利用备份数据和设备在灾备中心恢复认证系统的部分或全部数据和功能。

灾备系统应使用与正常运营系统相同的认证系统,并配置独立的数据备份系统、备用数据处理系统和备用网络系统;灾备中心应具有与主运营中心功能上相等同的物理和运行环境,安全管理和控制亦应与主运营场地相等同,其中密码设备和 CA 密钥的保护等级应符合本标准要求;灾备系统可建设于同城或异地灾备中心,建议使用异地灾备中心。

12 审计与改进

12.1 审计

12.1.1 系统审计

系统审计的目的是发现电子认证服务机构业务系统运行和操作中存在的风险和问题,并依此采取相应的措施和手段,防止安全事故的产生,杜绝问题再发生。

系统审计对象包括与认证业务有关的软件与硬件设备,包括但不限于证书认证系统、密钥管理系统、应用软件系统、数据库系统、操作系统、密码设备、防火墙、路由器、交换机、入侵检测系统、防病毒系统及其他与认证业务有关的系统。

系统审计的内容是系统审计范围内各审计对象的系统运行日志和管理人员操作日志。系统运行日志审计主要用于发现外部或非人为的风险,而管理人员操作日志审计主要用于发现内部或人为的风险。

系统运行日志应该每周审计一次。管理人员操作日志应该每月审计一次。

12.1.2 运营审计

运营审计是为了检查、确认电子认证服务机构是否按照其电子认证业务规则、业务规范、管理制度和安全策略开展业务,发现存在的风险。

运营审计分内部审计和独立第三方审计。

内部审计即由电子认证服务机构自己组织内部人员进行的审计,审计的结果可供电子认证服务机构改进、完善业务,也可以为第三方审计做准备。对于内部审计应从组织制度上保证审计过程的独立性和有效性。

独立第三方审计是电子认证服务机构聘请具有审计资格和相关审计经验的审计机构进行的审计,审计的结果既可供电子认证服务机构改进、完善业务,也是主管部门监管电子认证服务机构的依据。

运营审计包括如下内容:

a) 安全策略是否得到充分的实施;

b） 工作流程和制度是否得到严格遵守；

c） 是否严格按电子认证业务规则、业务规范和安全规定开展认证业务；

d） 各种日志、记录是否完整，是否存在问题；

e） 是否存在其他安全风险。

运营审计的依据包括电子认证服务机构所有与业务有关的安全策略、电子认证业务规则、业务规范、管理制度，以及国家或行业的相关标准。

应定期对电子认证服务机构进行运营审计，一般审计间隔周期为1年。

内部审计结果一般不需对外公开发布。外部审计结果，应根据审计目的和用途，由电子认证服务机构自行决定是否对外公开发布。

12.1.3 注册机构审计

电子认证服务机构应对注册机构进行定期监督检查，监督检查的内容主要包括法律法规符合性、安全运营管理、风险管理等，检查其是否严格按照相关的安全策略及运营管理规范开展业务活动。监督检查可采取报告审查和现场核查相结合的方式，具体检查方式根据注册机构的实际运营情况进行选择。

12.2 改进

电子认证服务机构应制定安全调整策略和规程。

在审计时发现与安全要求不相符的事项，应按照相应的调整策略和规程进行适当调整，必要时对调整后的事项进行评估，然后实施调整后的事项。

电子认证服务机构对注册机构实施审计时，若发现违反策略、规范的情况，应通知注册机构限期改正；若超期不改，则电子认证服务机构应立即暂停甚至中止注册机构的业务，并及时通知相关的用户。

附 录 A
（资料性附录）
业务运营风险举例

A.1 系统风险

A.1.1 系统技术风险

下面列出了系统主要面临的四种威胁，以及可能导致的部分风险。

a) 截获，即未授权获得了访问资源的权利。例如：
   1) 未进行网段隔离，易导致网络攻击，敏感数据被窃取，以及未授权的访问。
   2) 使用默认设置，使得系统、网络开放了非必要端口或运行了非必要的网络服务，易被黑客用来实施攻击。

b) 中断，即系统资源丢失、不可用或不可得。例如：
   1) 缺乏入侵检测机制，则无法发现网络中的非法扫描行为，也易使系统受到服务拒绝(DOS)攻击，导致授权访问被拒绝。
   2) 运营系统的网络采用单一链路接入公网，易因网络运营商故障导致断网，影响对外提供业务。
   3) 系统关键设备没有冗余，出现单点故障时，会导致服务中断。
   4) 关键数据未备份，易导致数据丢失无法恢复。

c) 篡改，即未授权方不仅访问了资源而且修改了其内容。
   1) 未安装防病毒软件或未升级防病毒软件病毒库，易导致系统数据被窃取、篡改或删除。
   2) 未及时给系统打补丁或补丁未更新，易被黑客利用系统漏洞发动攻击。

d) 伪造，即未授权方在系统中创建假冒对象。例如：
   1) 认证系统未对通信实体采用相应的鉴别技术，易导致非授权的访问以及信息泄露。
   2) 系统存在默认账户和口令，或口令强度不够，或没有定期审查用户的权限是否有变化，易被内部或外部人员猜测弱密码入侵系统。

A.1.2 系统运行风险

系统运行风险包括但不限于如下方面：

a) 缺乏测试系统，系统变更直接应用于产品系统，易导致系统故障。
b) 没有存储容量计划，不能应变数据量超过容量的情形。
c) 缺乏对系统硬件、软件、固件以及文档的变更控制，则如果出现不完善的变更，将对系统产生不良影响。
d) 对设备的账户和口令缺乏设置要求和管理措施，无法保障账户和口令的安全有效，存在未授权访问的风险。
e) 未设专门人员对系统状态和各类日志进行监控，无法及时发现和响应系统异常情况。
f) 对密码设备缺乏管理，无法确保密码设备在生命周期各环节内的安全可靠。
g) 没有 CA 密钥管理策略、申报和审批流程制度，对涉及 CA 密钥和证书的所有关键操作和记录缺乏管理，无法确保 CA 密钥的可信性。

A.2 物理环境风险

物理环境风险包括但不限于如下方面：

a) 未对运营场地进行合理的区域划分，无法保障核心设备的访问安全。

b) 物理场地没有门禁系统，可能导致未授权人员对系统设备的物理访问，致使数据或设备被盗、损坏。

c) 缺乏常规安全监控，则无法及时发现、处理未授权人员的访问、场地设施的损坏等安全事件，可能会加重损失。

d) 缺乏环境控制设施，系统设备过热，易导致系统关闭、设备损坏或服务中断。

e) 没有防雷击、漏水报警、静电防护等环境保护设施，无法保障系统运行环境的安全可靠。

f) 没有后备电源，易因断电导致系统关闭，中断对外服务。

A.3 管理风险

管理风险包括但不限于如下方面：

a) 岗位角色划分不清，部门职能不明确，无法保障关键业务流程的有效执行。

b) 没有设立专门的安全管理组织，无法实施有效的安全规划和运营安全管理。

c) 安全策略和规程的缺失无法保障对运营风险的有效控制，如没有职责分割策略，单人即可完成敏感操作，易因疏忽导致重要业务受损。

d) 对从业人员的背景缺乏必要了解，无法保障人员的可信性，存在内部人员恶意入侵系统、泄露敏感信息等风险。

e) 缺乏整体的安全意识培训和专业岗位培训，易因疏忽、错误操作而造成损失，也无法保障安全事件发生时能够及时响应。

f) 关键岗位人员流失可能影响业务的正常运营。

g) 缺乏对文档和介质的管理，易导致信息被盗、数据丢失。

h) 未正确保存日志，无法确认导致安全事件发生的原因。

i) 没有对系统操作记录实施独立审计，无法确定系统安全控制的充足性以及与安全策略和规程的符合性，同时也无法检测系统安全方面的漏洞，进而提升安全控制能力。

j) 未建立业务连续性计划，没有异地备份站点，如发生地震、洪水等自然灾害，将导致长时间业务中断以及数据丢失。