山东 CA CP

证书策略

版本 2.0.3

发布日期：2025 年 11 月 7 日

生效日期：2025 年 11 月 7 日

山东省数字证书认证管理有限公司

Shandong Certificate Authority Co.,Ltd

目　录

1 概括性描述

山东省数字证书认证管理有限公司（简称“山东 CA”）成立于 2000 年 12 月，是依据我国《电子签名法》和《电子认证服务管理办法》，全国首家获得国家许可资质的合法第三方电子认证服务机构，是中国电子认证服务产业联盟副理事长单位。公司被认定为高新技术企业、首批山东省网络安全重点企业，通过了 CMMI3 级认证，并获得山东省科技型中小企业、省级“专精特新”企业和省级“一企一技术”研发中心等荣誉称号。

山东 CA 是专业的电子认证服务提供商、网络可信服务运营商和信息安全解决方案提供商，承担着山东省电子认证基础设施的建设和运营，通过确认网络主体行为、保障用户利益、认定法律责任，为电子签名相关各方提供真实性、可靠性验证，是国家网络信任体系建设和数字经济产业发展的坚实支撑。

本文是山东 CA 的证书策略（Certificate Policy，简称 CP）。山东 CA 按照公钥基础设施（Public Key Infrastructure，简称 PKI）体系标准向订户提供各种应用的数字证书。本证书策略阐明了山东 CA 在提供电子认证服务过程中，必须遵循的基本规范。

本证书策略由山东 CA 根据《中华人民共和国电子签名法》和《电子认证服务管理办法》修订完善，并实施执行。根据本证书策略制定的电子认证业务规则，不能出现与本证书策略内容冲突的条款。

本证书策略的结构符合 PKI 的行业标准即由互联网组织“互联网工程工作组”（Internet Engineering Task Force，简称 IETF）制定的 RFC3647 标准。

山东 CA 保证自己的证书策略与 RFC3647 标准尽可能一致，但保留必要时候采用不同结构的权利。

1.1 概要

本证书策略是山东 CA 实施电子认证服务需要符合的策略声明，为数字证书的申请、签发、管理、使用、撤销和更新提供依据，为电子认证活动的各参与者的权利和义务关系制定业务、技术要求和规范。本证书策略的适用对象包括：

1）山东 CA 及其下层认证服务机构，应遵循本证书策略的规范及根据本证

书策略制定的电子认证业务规则，并按照电子认证业务规则运营。

2）本证书策略的证书订户，需要了解身份鉴别要求、作为订户的权利和义务以及对其提供的保护。

3）本证书策略的证书依赖方，需要了解本证书策略的证书或者该证书对应的电子签名的可信程度。

本证书策略不适用于任何非山东 CA 内的任何服务，例如山东 CA 为某些企业或组织建立的自行运营的内部 CA。

1.2 文档名称与标识

本文档称为《山东省数字证书认证管理有限公司证书策略》。山东 CA 注册的 OID 为 1.2.156.112571，本文档的对象标识符为：1.2.156.112571.7.1。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

电子认证服务机构是颁发证书的实体。山东 CA 是依法设立的电子认证服务机构。山东 CA 建设和运营的认证系统是多层次的 CA 结构模式，山东 CA 及其下层 CA 统称电子认证服务机构，这些签发实体均可发放证书。

1.3.2 注册机构

注册机构是受理证书的申请、审核、更新、恢复、撤销和下载等业务的实体。注册机构有责任妥善保存订户的数据，不允许将订户的数据透露给与证书申请无关的任何单位或个人，不允许用作商业利益方面的用途。

山东 CA 可以授权下属机构或委托外部机构作为注册机构，负责提供证书业务办理、身份鉴别与审核等服务。当注册机构为第三方机构时，山东 CA 必须与其签订协议，明确双方的权利和义务，以及承担的法律责任。

1.3.3 受理点

经过山东 CA 审查，山东 CA 授权特定单位或实体负责办理和审批数字证书申请。数字证书申请手续、过程和要求，必须与山东 CA 正在实施的证书策略、电子认证业务规则以及受理点授权协议书相一致。受理点负责向山东 CA 授权的

注册机构提供证书申请实体的信息，包括申请实体的名称、可以表明身份的证件号码和联系方法（通信地址、电子邮箱、电话等）。受理点根据这些信息为申请实体制作证书或根据申请实体的要求，提供申请实体自行申请的技术支持。

根据是否承担证书申请者费用的不同情况，受理点可分为垫付型的受理点和非垫付型的受理点。除非特别声明，受理点通常指非垫付型的受理点。

如果受理点满足证书垫付商的条件，并实行证书垫付商证书受理相应的做法，则把该受理点称为垫付型证书受理点。

如果受理点没有承担证书申请者的费用（与垫付型证书受理点不同），则称该受理点为非垫付型受理点。

1.3.4 证书垫付商

证书垫付商指的是能够为其所属或所服务的证书申请群体承担所有证书费用的团体组织。证书垫付商根据情况，有权取缔其支付费用申请证书。垫付商必须预定证书数量并预先缴纳所有的证书费用，并享受一定的优惠政策。垫付商必须承担其代付证书申请者身份真实性的责任。

1.3.6 订户

指接受并持有山东 CA 颁发证书的终端实体，包括个人、企业和组织机构。

1.3.7 依赖方

指需要验证证书和签名的实体。依赖方可以是、也可以不是订户。

1.3.8 其他参与者

指为山东 CA 的电子认证活动提供相关服务的其他实体，如第三方权威机构、目录服务提供者等与 PKI 服务相关的参与者。

1.4 证书的用途

1.4.1 支持的证书应用

山东 CA 数字证书可广泛应用在电子政务、电子商务、企业信息化以及其他电子化社会化活动中，用以确保互联网上信息传递双方身份的真实性、信息的保密性和完整性、以及网上交易的不可否认性。根据证书的功能以及使用证书的实际应用，目前山东 CA 签发的主要证书类型包括：

1）个人证书：个人包括自然人或特定身份的人员，如公务员、企业员工等。此类证书包含个人通用证书、个人代码签名证书、安全电子邮件证书等，通常用于电子化、移动化应用下数字签名、加密解密、安全电子邮件以及网上身份认证等。

2）机构证书：机构包括企事业单位、政府机关、社会团体等。此类证书包括机构通用证书、机构岗位证书、机构代码签名证书等，通常用于电子化、移动化应用下数字签名、加密解密以及网上身份认证等。

3）设备证书：设备包括服务器、防火墙、路由器等，此类证书通常包括设备通信证书、SSL 服务器证书和时间戳证书。用于网上设备的身份认证、安全通道建立、设备之间安全信息的传递以及签发有效时间戳等。

4）事件证书：存在即时或者特定场景业务过程中，需要事件发生过程的信息进行数据签名情形，此类证书根据订户提交的信息签发事件证书，其私钥为一次性使用，对业务场景的信息数据，如事件参与者、手写笔迹、指纹、电子文档或者其他证据信息，进行电子签名，确保业务场景的信息未被篡改，脱离场景该证书就不能使用。适合应用在企业信息化、电子政务和电子商务等领域，用于证明业务场景中所进行的电子签名行为，不限签名场景、电子文档和签名次数，因事件证书私钥使用后即销毁，只用于一次性事件型电子签名场合，此类证书无法用于其他用途。

1.4.2 不支持的证书应用

证书禁止在任何违反国家法律、法规或破环国家安全的情形下使用。否则，任何不符合的应用不受本证书策略的保护，由此造成的法律后果由订户自己承担。

证书不能用于直接导致人员伤亡或者严重的环境破坏的应用，例如：核设备的操作、航天器的导航或通信系统、航空管制系统或者武器控制系统等。

1.5 策略管理

1.5.1 策略管理机构

山东 CA 安全管理委员会负责制订、修订和发布本证书策略。

1.5.2 联系人

山东 CA 安全管理委员会为本证书策略的联系人。

电　话：86-531-86019278，传真：86-531-86019278

地　址：山东省济南市趵突泉北路 24 号（250011）

电子邮件：sdca@sdca.com.cn

1.5.3 电子认证业务规则的审批机关

本证书策略由山东 CA 安全管理委员会组织制订，报山东 CA 安全管理委员会批准执行，并在中华人民共和国工业和信息化部（以下简称“工业和信息化部”）备案。

1.5.4 电子认证业务规则的审批流程

在本证书策略做出任何变动之前，山东 CA 安全管理委员会组织编写小组进行修订，在征询山东 CA 法律顾问有关方面的意见后，提交山东 CA 安全管理委员会审批。经山东 CA 安全管理委员会审批通过后三十日内向工业和信息化部备案。

1.6 定义与缩写

1、公钥基础设施（PKI）

公钥基础设施（Public Key Infrastructure，简称 PKI）是利用公钥加密技术为电子认证的开展提供一套安全基础平台的技术和规范。

2、电子认证服务机构（CA）

电子认证服务机构（Certification Authority，简称 CA）是负责签发数字证书的权威机构，又称为数字证书认证中心。

3、注册机构（RA）

注册机构（Registration Authority，简称 RA）是负责订户证书的申请、审批和证书管理等工作，面向证书订户。

4、数字证书（Digital Certificate）

数字证书是指经 CA 数字签名的包含数字证书使用者身份公开信息和公开密钥的电子文件。

5、证书撤销列表（CRL）

证书撤销列表(Certificate Revocation List，简称 CRL)，是一种包含撤销的证书列表的签名数据结构。

6、在线证书状态协议（OCSP）

在线证书状态协议（Online Certificate Status Protocol，简称 OCSP）用于检查数字证书在某一交易时间是否有效的标准。

7、证书策略（CP）

证书策略（Certificate Policy，简称 CP）是一套命名的规则集，用以指明证书对一个特定团体和（或者）具有相同安全需求的应用类型的适用性。

8、电子认证业务规则（CPS）

电子认证业务规则（Certification Practice Statement，简称 CPS）是关于 CA 的颁发和管理证书的运作规范的描述，包括 CA 整体运行规范和证书的颁发、管理、撤销和密钥以及证书更新的操作规范等事务。

10、私钥（Private key）

私钥在公钥基础设施中为一个密码串，由特定算法与公钥一起生成，用于解密信息或进行数字签名。

11、公钥(Public key)

公钥在公钥基础设施中为一个密码串，由特定算法与私钥一起生成，用于加密信息或验证数字签名。

12、甄别名(DN)

甄别名（Distinguished Name，简称 DN）在数字证书的主体名称域中，用来唯一标识订户信息的 X.500 名称。

2 信息发布和资料库

2.1 资料库

山东 CA 电子认证系统信息库包括以下内容：CP、CPS、证书、CRL。山东 CA 的职责是确保发布的认证信息及时、可靠。

2.2 信息发布

山东 CA 提供明确的访问位置和方法，通过在线的方式公布证书和证书状态信息，定期公布证书撤销列表。

山东 CA 在网站（https://www.sdca.com.cn）上发布证书策略、电子认证业务规则、证书和证书状态等信息。已有旧信息与山东 CA 新发布的信息不一致的，以山东 CA 新发布的信息为准。

2.3 发布信息的时间及频率

山东 CA 及时发布电子认证业务规则、证书服务等文档以及文档的修订信息。

对于终端订户的证书撤销列表，至少每 24 小时内签发一次。

2.4 资料库的访问控制

对于公开发布的证书策略、电子认证业务规则、证书和 CRL 等信息，山东 CA 允许公众通过网站或目录服务器进行查询和访问。

山东 CA 保证证书策略、电子认证业务规则、证书、CRL 等电子认证信息库只有经过授权的山东 CA 工作人员才能登录、访问和控制。

3 身份标识与鉴别

3.1 命名

3.1.1 名称类型

山东 CA 证书符合 X.509 标准，命名规则必须使用 X.500 甄别名。

3.1.2 名称意义化的要求

山东 CA 签发证书的命名应具有通常理解的语义，用它可以确定证书主体中的个人、机构或设备的身份。事件证书的甄别名还可包含其他与场景有关的信息。

3.1.3 订户的匿名或假名

在山东 CA 证书服务体系中，除在特定场景下的证书以外，原则上订户不能使用匿名或假名。

3.1.4 不同名字格式的解释规则

依照 X.500 甄别名命名规则解释。

3.1.5 名称的唯一性

山东 CA 签发给某个实体的证书，其主题甄别名在整个 CA 信任域内是唯一的。

3.1.6 商标的识别、鉴别和角色

证书申请者不应使用任何可能侵犯知识产权的名称。山东 CA 不对证书申请者是否拥有命名的知识产权进行判断和决定，也不负责解决证书中任何关于域名、商标等知识产权的纠纷。山东 CA 没有权利，也没有义务拒绝或者质疑任何可能导致产生知识产权纠纷的证书申请。

3.2 初始身份验证

3.2.1 证明拥有私钥的方法

山东 CA 通过证书请求中所包含的电子签名来证明申请人持有与注册公钥对应的私钥。

3.2.2 机构身份的鉴别

任何组织（政府机构、企事业单位等），在以组织名义申请证书时，其身份应当被进行严格的验证。至少需要进行如下的鉴别：

1）订户提交的组织身份信息；

2）组织授予经办人的授权证明；

3）经办人的个人身份证明材料；

4）在域名、设备名称或者 IP 被作为证书主题内容申请证书时，还需要合理验证该组织是否拥有该权利；

5）审核确认后提供的内设机构证书用户发放名单。

组织身份的鉴别流程应当明确记录在按照本证书策略制定的电子认证业务规则中。

3.2.3 自然人身份的鉴别

山东 CA 的个人证书签发给合法的个人申请者，山东 CA 需要严格审核个人申请者的身份。至少需要进行如下的一种鉴别：

1）利用权威第三方提供的身份证明或数据库服务；

2）政府机构发放的合法性文件，如：居民身份证、军官证、护照等证明订户的身份。若委托他人进行证书申请的，应同时提供被委托人的身份证明；

3）在域名、设备名称或者 IP 被作为证书主题内容申请证书时，还需要合理验证该个人是否拥有该权利；

4）审核确认后提供的内部人员证书用户发放名单。

自然人身份的鉴别流程应当明确记录在按照本证书策略制定的电子认证业务规则中。

3.2.4 事件证书订户身份的鉴别

事件证书订户身份的鉴别参照个人或组织身份鉴别方法进行鉴别，也可以采取包括录音、录像、可信数据源等有效的身份核验方式进行自动鉴别。

3.2.5 不需验证的订户信息

通常，除了该类型证书所必须要求的身份信息需要得到明确、可靠的验证以外，其他信息是可以不被要求验证的。

3.2.6 授权确认

山东 CA 签发证书前，需确认证书申请者必须获得授权。山东 CA 通过有效方式确定授权信息，并将授权信息妥善保存。

3.2.7 互操作规范

对于山东 CA 外的其他证书服务机构颁发的证书，可以与山东 CA 进行互操作，但是必须符合山东 CA 的证书策略的要求，并且与山东 CA 签署了相应的协议。

3.3 密钥更新请求的身份标识与鉴别

在订户证书到期前，订户需要获得新的证书以保持证书使用的连续性。山东 CA 一般要求订户产生一个新的密钥对代替过期的密钥对，称作“密钥更新”。然而，在某些情况下，也允许订户为一个现存的密钥对申请一个新证书，称作“证书更新”。对于密钥更新而言，订户证书除公钥、有效期和序列号改变外，其他信息都没改变；对于证书更新而言，和密钥更新相比，订户证书公钥也不改变。对于山东 CA 的证书认证业务，在证书有效期到期前只能通过密钥更新或证书更新签发有相同签发者、主体名和证书用途的证书。通常，我们在表述证书更新时包含了密钥更新和证书更新。

3.3.1 常规密钥更新请求的身份标识与鉴别

对于常规密钥更新，订户可以用原有的私钥对更新请求进行签名。山东 CA 认证系统会对订户的签名和更新请求进行鉴别。

订户也可以选择一般的初始证书申请流程，按照初始身份验证步骤（详细内容请见第 3.2 节）进行常规密钥更新，按照要求提交相应的证书申请和身份证明资料。

事件证书没有密钥更新。

3.3.2 撤销后密钥更新的标识与鉴别

山东 CA 不提供证书被撤销后的密钥更新。订户必须重新进行身份鉴别，按照初始身份验证步骤向山东 CA 申请重新签发证书。

3.4 证书撤销请求的标识与鉴别

在山东 CA 的证书业务中，证书撤销请求可以来自订户，也可以来自山东 CA。当山东 CA 授权的注册机构有充分的理由撤销订户时，有权依法撤销证书，这种情况无须进行鉴证。如果订户主动要求撤销证书，则需要递交初始身份验证时的申请材料。如果是司法机关依法提出撤销，山东 CA 将直接以司法机关提供的书面撤销请求文件作为鉴别依据，不再进行其他方式的鉴别。

4 证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请者

证书申请者包含个人、企业单位、事业单位、社会团体、人民团体等各类组织机构以及 CA、RA、受理点和 CA 机构或 RA 机构的系统及相应的管理员。

4.1.2 登记过程与责任

订户必须提供真实的身份信息，并如实填写证书申请信息，遵守电子认证业务规则及用户协议，否则，山东 CA 有权拒绝签发证书、停止证书的使用、废止证书，且由此造成的后果，山东 CA 不承担任何责任。

山东 CA 的注册机构对申请人的身份进行充分的验证并对证书申请进行处理。出于安全性和审查的需要，申请表应由验证人签名并注明日期。

4.2 证书申请处理

4.2.1 标识与鉴别过程

山东 CA 或授权的注册机构遵循第 3 章对证书申请者提交的信息进行识别。注册机构须保留足以识别申请者身份的文档记录。

4.2.2 接受或拒绝证书申请

依据识别与鉴别的信息，山东 CA 授权的注册机构有权决定接受或拒绝订户的申请。

如果符合下述条件，山东 CA 授权的注册机构接受订户的证书申请：

1）成功标识和鉴别了订户的身份信息；

2）订户接受订户协议的内容和要求；

3）订户按照规定支付了相应的费用，另有协议规定的情况除外。

如果发生下列情形之一，山东 CA 授权的注册机构有权拒绝订户的证书申请：

1）该申请未完成标识和鉴别的过程；

2）订户不能提供所需要的补充文件；

3）订户不接受或者反对订户协议的内容和要求；

4）没有或者不能够按照规定支付相应的费用；

5）山东 CA 授权的注册机构认为批准该申请将会对山东 CA 带来争议、法律纠纷或者损失。

4.2.3 证书申请的处理期限

山东 CA 授权的注册机构应在一个工作日内对证书申请者提交的证书信息进行处理。

4.3 证书签发

4.3.1 证书签发期间电子认证服务机构的行为

证书申请者一旦提交了证书申请，尽管事实上还没有接受证书，但仍被视为该订户已同意注册机构签发其证书；

山东 CA 授权的注册机构批准证书申请后（参见第 4.2 节），将为证书申请者颁发证书，并提供给订户。

4.3.2 订户证书签发的通知

山东 CA 通过注册机构对证书订户的通过有以下几种方式：

1）通过面对面的方式，通知订户到注册机构领取数字证书；注册机构将证书直接交给订户，来通知订户证书信息已经正确生成；

2）邮政信函或电子邮件通知订户；

3）山东 CA 认为其他安全可行的方式通知订户。

对于事件证书，订户成功完成电子签名，即视为山东 CA 证书签发成功，山东 CA 不再就证书签发向订户进行其他方式的通告。

4.4 证书接受

4.4.1 证书接受的行为

在山东 CA 数字证书签发完成后，山东 CA 将把数字证书当面或寄送给订户，订户从获得证书起就被视为已同意接受证书。订户接受数字证书后，应妥善保存

其证书对应的私钥。

事件证书签发完成后，将证书应用于对应的电子签名时起，就被视为同意接受证书。

4.4.2 电子认证服务机构发布证书

山东 CA 将已签发的证书发布到可以被公开访问的信息库中，包括 LDAP 目录发布、HTTP 方式发布等。

4.4.3 电子认证服务机构通知其他实体关于证书的签发

山东 CA 应在公开访问信息库中提供证书的查询服务，使用山东 CA 证书的各类实体可以通过查询服务获得所需证书，通常情况下，山东 CA 不对其他实体进行专门通知。

4.5 密钥对和证书的使用

山东 CA 要求订户密钥对和证书的使用不能应用于其规定的用途之外的目的，否则其应用不受相关法律和本证书策略的保护。

4.5.1 订户私钥和证书的使用

订户接受到数字证书后，应妥善保存其证书对应的私钥。订户可以从山东 CA 证书目录服务器中下载个人或其他数字证书。

对于签名证书，其私钥仅用于对信息的签名。在可能的情况下，签名证书应同被签名信息一起提交给依赖方。订户使用私钥对信息签名时，应该确认被签名的内容。对于加密证书，其私钥可用于对采用对应公钥加密的信息解密。

订户使用证书时应妥善保存其证书对应的私钥，免受未授权的使用。

在证书到期或者撤销之后，订户必须停止使用私钥。

事件证书订户只能在指定的场景应用证书对应私钥进行签名，完成签名后须停止使用证书对应私钥并进行销毁。

4.5.2 依赖方对公钥和证书的使用

依赖方只能在接受山东 CA 证书策略要求的情况下，才能依赖山东 CA 订户证书。在信任证书和签名前，依赖方必须根据环境和条件进行合理地判断并做出决定。

在依赖证书前，依赖方必须独立的进行如下评估和判断：

1）证书是否由可信任的 CA 所签发；

2）证书被适当的使用，判断该证书没有被用于电子认证业务规则或者法律法规禁止或限制的使用范围；

3）证书的使用与证书密钥用途包含内容是否一致；

4）查询证书及其证书信任链中的证书状态，如果订户证书或其信任链内的任何证书已经被撤销，依赖方必须独立去了解该订户证书对应的私钥所做的签名是否是在撤销之前做的，是否可以依赖，并独立承担相应的风险。

4.6 证书更新

4.6.1 证书更新的情况

为保证证书的安全有效和订户的权利，山东 CA 会为签发的证书设置有效期。订户必须在证书有效期到期前三十天内，到山东 CA 授权的注册机构申请更新证书。

4.6.2 证书更新请求者

订户本人或其授权代表可以请求证书更新。

4.6.3 处理证书更新请求

订户或其授权人通过已有私钥，在山东 CA 授权的注册机构通过 PIN 码验证和身份信息核查，进行更新请求；或在山东 CA 授权的注册机构书面填写《山东 CA 数字证书申请表》。山东 CA 授权的注册机构按照第 3 章识别与鉴定的规定对订户提交的证书更新申请进行审核。

提出更新申请的订户在进行证书更新之前应将加密邮件等加密过的文件进行解密，同时备份（例如将邮件内容复制以明文方式存储或将邮件附件保存），然后将证书删除。以上操作完成后才能进行证书的更新。如订户未解密文件而进行证书更新，由此造成的可能损失，山东 CA 不承担任何责任。

4.6.4 通知订户新证书签发

同第 4.3.2 节“订户证书签发的通知”。

4.6.5 构成更新证书接受的行为

同第 4.4.1 节“证书接受的行为”。

4.6.6 电子认证服务机构对更新证书的发布

同第 4.4.2 节“电子认证服务机构发布证书”。

4.6.7 电子认证服务机构对其他实体的通告

同第 4.4.3 节“电子认证服务机构通知其他实体关于证书的签发”。

4.7 证书密钥更换

证书密钥更换是指不改变证书中包含的信息的情况下，产生新的密钥对，并由山东 CA 签发新证书。

4.7.1 证书密钥更换的情况

证书订户申请更换密钥的情形主要有：

1）证书的密钥泄露。对此，订户负有立即告知山东 CA 的责任；

2）证书到期时，要求更换证书密钥；

3）证书丢失；

4）其他。例如，由于信息技术的不断更新，为了保证证书的安全性，山东 CA 有权要求订户更换证书的密钥。

4.7.2 证书密钥更换请求者

订户本人或其授权代表可以请求证书密钥更换。

4.7.3 证书密钥更换请求的处理

同第 4.6.4 节“通知订户新证书签发”。

4.7.4 订户新证书签发的通知

同第 4.6.4 节“通知订户新证书签发”。

4.7.5 构成密钥更换证书接受的行为

同第 4.4.1 节“证书接受的行为”。

4.7.6 电子认证服务机构对密钥更新证书的发布

同第 4.4.2 节“电子认证服务机构发布证书”。

4.7.7 电子认证服务机构通知其他实体证书的签发

同第 4.4.3 节“电子认证服务机构通知其他实体关于证书的签发”。

4.8 证书变更

4.8.1 证书变更的情况

证书变更指改变证书中除订户公钥之外的信息而签发新证书的情形。订户证书只有在有效期内，才可能发生证书变更的情况。

证书变更的原因有：

1）证书订户甄别名更改；

2）其他：如通用名、组织、角色改变等原因。

4.8.2 证书变更请求者

订户本人或其授权代表。

4.8.3 证书变更请求的处理

对于要求证书变更的，需确认证书变更请求是被订户或订户授权的代表提出的，并对其身份进行鉴别。证书处理过程同第 4.6.3 节“证书更新请求的处理”。证书变更后，证书的有效期并没有改变，仍然为原证书有效期。

4.8.4 订户新证书签发的通知

同第 4.3.2 节“订户证书签发的通知”。

4.8.5 构成变更证书接受的行为

同第 4.4.1 节“证书接受的行为”。

4.8.6 电子认证服务机构对变更证书的发布

同第 4.4.2 节“电子认证服务机构发布证书”。

4.8.7 电子认证服务机构通知其他实体证书的签发

同第 4.4.3 节“电子认证服务机构通知其他实体关于证书的签发”。

4.9 证书撤销和挂起

4.9.1 撤销的情况

证书撤销是指由于各种原因导致证书不能再继续使用，必须废除的情况。

证书撤销的原因主要有：

1）新的密钥对替代旧的密钥对；

2）密钥失密：与证书中的公钥相对应的私钥被泄密或订户怀疑自己的密钥失密；

3）从属关系改变：与密钥相关的订户的主题信息改变，证书中的相关信息有所变更；

4）操作中止：由于证书不再需要用于原来的用途，但密钥并未失密，而要求中止（例如订户离开了某个组织）；

5）证书到期：到期后订户未续约；

6）订户不能履行电子认证业务规则或其他协议、法律及法规所规定的责任和义务；

7）订户申请初始注册时，提供不真实材料；

8）证书已被盗用、未经授权的泄漏和其它安全威胁；

9）CA 失密：电子认证服务机构因运营问题，导致 CA 内部重要数据或 CA 根密钥失密等原因；

10）订户自动提出撤销请求；

11）其他情况。这些情况可以是因法律或政策的要求山东 CA 采取的临时撤销措施，也可以是订户申请撤销证书时填写的其他原因。

4.9.2 证书撤销请求者

请求证书撤销的实体包括：

1）订户本人或其授权代表；

2）山东 CA 或其授权机构的授权代表；

3）司法机关等公共权力部门的授权代表。

4.9.3 证书撤销请求的处理

请求证书撤销的实体向山东 CA 授权的注册机构提交《山东 CA 数字证书申请表》，并注明撤销的原因。山东 CA 授权的注册机构按照第 3 章识别与鉴定的规定对提交的证书撤销申请进行审核。山东 CA 撤销证书后，注册机构将当面通知请求证书撤销的实体证书被撤销。

如是强制撤销，山东 CA 授权的发证机关管理员可以对订户证书进行强制撤销，撤销后必须立即通知该证书订户。强制撤销的命令来自于：山东 CA、山东 CA 授权的注册机构或司法机关等公共权力部门。

4.9.4 撤销请求宽限期

当最终订户发现出现第 4.9.1章节中的情况时，应该尽快提出证书撤销请求，撤销请求必须在密钥泄密或有泄密嫌疑8小时以内发现提出，其它撤销原因从发现需要撤销证书到向山东CA或注册机构提出撤销请求的时间间隔必须在24小时以内提出。

4.9.5 电子认证服务机构处理撤销请求的时间要求

山东 CA 应在收到证书撤销请求起 24 小时内完成请求的处理。

4.9.6 依赖方进行撤销检查的要求

依赖方在信任证书前，必须对证书的状态进行检查，包括：

1）在使用证书前根据山东CA最新公布的CRL检查证书的状态；

2）验证CRL的可靠性和完整性，确保它是经山东CA发行并电子签名的。

依赖方应根据山东CA公布的最新CRL或提供的OCSP服务确认使用的证书是否被撤销。如果公布证书已经撤销，而依赖方没有检查，由此造成的损失由依赖方本身承担。

4.9.7 证书撤销列表签发频率

对于订户证书撤销列表，至少每24小时签发一次；对于电子认证服务机构的CA证书撤销列表(ARL)，至少每年签发一次。特殊紧急情况下应立即签发公布。

4.9.8 证书撤销列表发布的最大滞后时间

山东CA撤销的证书从被撤销到被发布到CRL上的滞后时间最大为24小时。

4.9.9 在线撤销/状态查询的可用性

山东CA向依赖方提供7×24小时在线证书状态查询服务。

4.9.10 在线撤销检查的要求

依赖方在信赖一个证书前必须通过证书状态查询检查该证书的状态。如果依赖方不希望通过最新的相关证书撤销列表来检查证书状态，则应通过可用的OCSP服务对证书状态进行在线检查。

4.9.11 可获得撤销公告的其他方式

无规定。

4.9.12 针对密钥泄露的特殊要求

山东CA所有订户在发现证书密钥受到损害时，应立即通知山东CA撤销证书。

4.9.13 证书挂起的情况

证书挂起是证书撤销的一种特殊情况，当证书订户想暂停使用证书时的证书处理方式。例如：证书持有者由于某种原因如长期出差，短期内无法使用证书，可以申请证书挂起。

4.9.14 证书挂起请求者

请求证书挂起的人包括：

1）订户本人或其授权代表；

2）山东 CA 或其授权机构的授权代表；

3）司法机关等公共权力部门的授权代表。

4.9.15 挂起请求的程序

申请者向山东CA授权的注册机构提交《山东CA数字证书申请表》，并注明挂起的原因。山东CA授权的注册机构按照第3章识别与鉴定对订户提交的证书挂起申请进行审核。

如是强制挂起，山东CA授权的发证机关管理员可以依法对订户证书进行强制挂起，挂起后必须立即通知该证书订户。强制挂起的命令来源于：司法机关、山东CA或山东CA授权的注册机构。

4.9.16 挂起的期限

订户证书被挂起后，订户必须在证书有效期到期前恢复证书，否则山东CA或山东CA授权的注册机构有权自行撤销证书。对此造成的任何后果，山东CA不负责任。

4.9.17 证书恢复

证书挂起订户或其授权者，在需要恢复时向山东CA授权的注册机构提交《山东CA数字证书申请表》，并注明恢复的原因。山东CA授权的注册机构按照第3章识别与鉴定对订户提交的证书恢复申请进行审核。审核通过之后，为订户恢复证书，并通知订户证书已恢复。

4.10 证书状态服务

山东CA通过CRL、OCSP、LDAP提供证书状态服务。

4.10.1 操作特征

山东CA提供以下三种方式为证书订户提供证书状态查询。

1）通过发布服务器采用http方式发布CRL，其可信度及安全性由根证书的签名来保证。订户需要将CRL下载到本地后进行验证，包括CRL的合法性验证和检查CRL中是否包含待检验证书的序列号。

2）提供OCSP（在线证书状态查询）服务，以网络服务的方式提供证书状态信息，符合RFC2560标准。

3）提供LDAP目录查询证书状态服务，符合LDAP V3标准。

4.10.2 服务可用性

山东CA提供7×24小时证书状态查询服务。

4.11 订购的结束

订购结束即服务终止，是指证书订户终止与山东CA的服务，它包含以下两种情况：

1）证书到期时终止与山东CA的服务；

当证书到期时，证书订户不再延长证书使用期或者不再重新申请证书时，证

书订户可以提出服务终止。

2）证书未到期时中止与山东CA的服务；

在证书的有效期内，由于证书订户的原因而单方面要求终止证书服务。山东CA将根据证书订户的要求撤销证书，证书订户与山东CA的服务终止。

4.12 密钥托管与恢复

4.12.1 密钥托管与恢复的策略与实施

证书订户的加密密钥由密钥管理中心托管备份，当证书订户本人、国家执法机关、司法机关或其他管理部门因管理需要提出恢复加密密钥时，按照密钥托管和恢复服务的流程取得相应的加密密钥。

为保证订户签名私钥的安全性，签名私钥不进行托管，要求订户妥善保管签名私钥。由于签名私钥遗失所造成的损失由证书订户自己承担，山东CA对此不承担任何责任。

4.12.2 会话密钥的封装与恢复的策略与实施

无规定。

5 设施、管理和运作控制

5.1 物理安全控制

山东CA电子认证服务机构的物理环境满足以下安全要求：

1）防止物理非法进入

山东CA通过入侵报警、视频监控等安防设施对定义的七层管理区域进行实时监测，并建立完善的安全管理制度，保护山东CA的电子认证服务设施。

2）防止未授权访问

山东CA通过门禁系统和权限分割的管理模式，确保不发生未经过授权或越权的区域访问。

5.1.1 场所位置和建筑

山东CA电子认证服务业务的运行场地位于山东省济南市趵突泉北路24号。

核心机房：

包括CA核心区、CA服务区、CA管理区，其中CA核心区为屏蔽机房，屏蔽机房采用了六面钢板及专用屏蔽门进行屏蔽处理，以防止电磁泄漏，增加系统的安全性。

机房出入由门禁系统进行控制，并在核心区采用双人指纹加门禁卡的方式进行认证。每个区域都安装视频监控系统、防侵入报警系统、机械组合锁等装置。

其他功能区域：

包括消防室、配电室、监控室、机房中心通道等。

消防室按照当地消防部门的要求采用通顶实体砖墙与其他区域分割，并能直通室外。

机房中心通道与办公区域连接部位采用玻璃门，UPS配电室、监控室采用实墙隔断，并且由门禁系统进行管理。

5.1.2 物理访问

山东CA的核心机房和各功能区域的访问通过门禁系统和防侵入报警系统等方式进行控制的，进出每一区域的门都有记录，进出核心机房采用双人身份鉴别

卡和生物特征结合的方式控制。

5.1.3 电力与空调

山东CA系统采用市电供电、UPS不间断和电力发电车三种电源方式供电，在市电供电中断时，UPS不间断电源系统和电力发电车可以持续维持电子认证服务系统设备与服务正常运转。

山东CA系统需要中央空调冷却设备和新风系统控制机房内重要设备的温度和湿度。

5.1.4 防水措施

山东CA机房设计必须考虑水患，进行防水设计和建设，并采取相应措施，防止水侵蚀，充分保障系统安全。

5.1.5 火灾预防和保护

山东CA设备机房必须按照国家标准建设安装有火灾报警系统和消防应急联动处理系统，避免火灾的威胁，充分保障系统安全。

5.1.6 介质存储

山东CA将存储介质保存到相应的安全区域中，介质得到安全可靠的保护，避免诸如温度、湿度和磁力等环境变化可能产生的危害和破坏，并且只有授权人员才能访问。

5.1.7 废物处理

山东CA对作废的相关业务文件和材料应按照相关流程经审批通过后，通过粉碎、焚烧或其它不可恢复的方法处理，废弃的密码设备在销毁处置前根据产品提供商的操作指南将其物理销毁或初始化，其他废物处理按照山东CA的相关处理要求进行，所有处理行为将记录在案。

5.1.8 异地备份

山东CA对业务系统中的程序、数据等关键信息应按照数据备份策略和流程进行安全备份。备份介质按照备份策略和流程保存在本地机房和异地。在异地备份时按照策略和流程由专人送交到指定地点安全保管。以上所有操作流程将记录在案。

5.2 程序控制

5.2.1 可信角色

山东CA明确各级员工的可信资格，在入职时应根据其拟从事岗位关键等级的安全要求执行仔细有效的身份背景调查，确保其从事相应岗位的可信资格，只有在通过背景调查后才能确定其可信资格，并授予相应的权限，从事电子认证服务业务。

5.2.2 每项任务需要的人数

山东CA确保单个人不能接触、导出、恢复、更新、废止电子认证系统根证书对应的私有密钥。对于关键的操作进行物理与逻辑上的分割控制，使掌握设备物理权限的人不能再拥有逻辑权限。

山东CA在具体业务规范中对关键任务进行严格控制，确保至少两个可信角色共同参与完成。

山东CA对与运行和操作相关的职能有明确的分工，贯彻互相牵制的安全机制，保证至少一人操作，一人监督记录。

5.2.3 每个角色的识别与鉴别

对于即将成为山东CA可信雇员的人员必须进行严格的身份审查措施，通过证件材料等的缴验及其他途径的询证，来保证其安全级别的可信程度。

所有山东CA工作人员必须确保：

1）根据岗位安全等级的不同，进行不同程度的身份识别和鉴别措施；

2）基本的身份审查措施，确保符合岗位可信资格；

3）赋予可信员工相应的权限区分；

山东CA系统和程序通过识别不同的安全令牌，对操作者进行权限控制。

5.2.4 需要职责分割的角色

所谓职责分割，是指如果一个人担任了完成某一职能的角色，就不能再担任完成另一特定职能的角色。CA必须（但不限于）对以下角色进行职责分割：

1）负责对证书申请、撤销或更新的相关信息的录入人员；

2）负责对证书申请、撤销或更新请求的审核人员；

3）负责处理订户信息的人员；

4）负责签发和撤销CA认证系统证书的人员；

5）负责维护CA认证系统的人员。

5.3 人员控制

5.3.1 资历和安全要求

山东CA员工的录取必须经过严格的审查，根据岗位需要增加相应可信任的员工。一般员工需要有3个月的考察期，核心和关键岗位的员工有半年的考察期，根据考察的结果安排相应的工作或者辞退。

山东CA对其员工应进行严格的背景调查。背景调查主要通过（但不限于）以下方式：

1）身份验证，包括个人身份证件、户籍证件等；

2）学历、学位等其他资格、资历证书；

3）个人履历，包括家庭状况、教育经历、工作经历及相关证明人等；

4）无犯罪记录证明材料。

5.3.2 背景审查流程

山东CA必须制定员工背景审查程序并严格执行，对担当可信角色和重要岗位的人员进行调查，完成对山东CA可信任员工的背景调查。

身份背景调查过程中，存在（但不限于）下列情形的不得通过可信审查：

1）伪造相关证件材料的；

2）伪造工作经历及工作证明人虚假的；

3）虚假声称证件具有某种技能、能力的；

4）以往工作中存在重大不诚实行为的；

5）有犯罪记录的。

5.3.3 培训要求

山东CA应对山东CA员工进行以下内容的综合性培训：

1）山东CA安全原则和机制；

2）山东CA使用的软件介绍；

3）山东CA操作的系统和网络；

4）山东CA岗位职责；

5）山东CA政策、标准和程序；

6）相关法律、仲裁规则、管理办法等。

针对关键岗位员工进行相关职责、安全机制、工作操作说明等方面内容的培训。

5.3.4 再培训周期和要求

山东CA必须对员工进行继续培训，以适应新的变化。对于公司安全管理策略，至少每年对员工进行一次培训，对于相关业务技能培训应每年进行一次业务技能培训。

5.3.5 岗位轮换的频率和顺序

根据岗位人员和业务上的实际情况内部自行安排。

5.3.6 未授权行为的处罚

当山东CA员工被怀疑，或者已进行了未授权的操作，例如滥用权利或超出权限使用CA系统或进行越权操作，山东CA得知后将立即对该员工进行工作隔离，随后对该员工的未授权行为进行评估，如经评估后，未授权操作得到确认，立即作废或终止该员工的安全令牌，采取必要的防范处理措施，并对该员工进行相应处罚，情节严重的，依法追究相应责任。

5.3.7 独立合约人的要求

山东CA的独立合约人执行与普通员工一致的可信资格确认，此外独立合约人进入关键区域必须有专人的陪同与监督。

5.3.8 提供给员工的文档

为使得系统正常运行，山东CA向员工提供完成其工作所必须的文档。

5.4 审计流程

5.4.1 被记录事件的类型

山东CA的运行系统必须记录所有与系统相关的事件，以备审查。这些记录，

无论是纸质或电子形式，都应包含事件日期、事件内容、事件发生时间、引发事件的相关实体等。

山东CA应记录的内容包括（但不限于）：

1）电子认证服务系统安全事件；

2）电子认证服务系统操作事件；

3）认证机构设施的访问事件；

4）证书生命周期相关事件。

5.4.2 处理日志的周期

对于CA 和订户证书生命周期内的管理事件日志、系统安全事件、系统操作事件日志、物理设施访问日志，山东CA应定期进行内部检查、审计和处理。

5.4.3 审计日志的保存期限

山东CA应妥善保存认证服务的审计日志，与证书相关的审计日志至少保存到证书失效后五年。

5.4.4 审计日志的保护

山东CA必须严格执行审计流程，确保审计日志不被未授权的访问、复制、修改和删除等操作。

5.4.5 审计日志的备份

山东 CA 应保证所有的审计记录和审计总结都按照山东 CA 备份标准和程序进行。根据记录的性质和要求，采用在线和离线的各种备份工具，有实时、每天、每周、每月和每年等各种形式的备份。

5.4.6 审计日志收集系统

山东CA审计采集系统应涉及：

1）证书签发系统；

2）证书注册系统；

3）证书受理系统；

4）网站、数据库系统；

5）网络安全等其它有必要审查的系统。

5.4.7 事件引发主体的通知

无规定。

5.4.8 脆弱性评估

山东CA定期对系统进行漏洞扫描和渗透测试等脆弱性评估，降低系统运行的风险。

5.5 记录归档

5.5.1 归档的记录类型

山东CA应按照制度和流程对电子生成和（或者）手工生成的重要数据定期存档。存档的内容至少包括：

1）所有在5.4节涉及的审计数据；

2）证书申请的相关信息；

3）证书生命周期的相关信息。

5.5.2 归档记录的保存期限

山东CA归档记录存档期限规定为五年以上。

5.5.3 归档记录的保护

存档记录既要有物理安全措施的保证，也要有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能访问。山东CA保护相关的档案免遭恶劣环境的威胁，例如温度、湿度和磁力等的破坏。

5.5.4 归档记录的备份流程

所有纸质归档记录按照备份策略和流程由专人定期执行，备份介质在山东CA公司本地备份管理。按照备份策略和流程，电子存档文件除了在山东CA内本地备份外，还将在异地保存其备份。

5.5.5 归档记录的时间戳要求

所有5.5.1条款所述的存档内容都按照归档策略和流程分别由专人收集、归档、审核和保管。所有归档记录上均有参与归档操作的人员与时间记录。

5.5.6 归档记录收集系统（内部或外部）

山东CA的档案收集系统由人工操作和自动操作两部分组成。

5.5.7 获得和检验归档记录的流程

只有被授权的可信人员能够访问归档记录。所有记录被访问后，需验证其完整性。此外，山东CA每年应验证存档信息的完整性。

5.6 电子认证服务机构密钥的更替

CA的根密钥在遭受攻击或因为密钥生命期而需要更新根密钥的情况下，密钥管理员应在场，启动密钥管理程序，执行密钥更新指令，硬件加密设备重新生成根密钥。

5.7 事故和灾难恢复

5.7.1 事故处理流程

山东CA应制定各种应急处理方案，规定相应的事故和损害处理程序，规定相应的应急响应、应急处置、应急恢复、保障措施。

涉及电子认证机构的重大事故应按照规定及时上报管理机构。

5.7.2 计算资源、软件和/或数据遭到破坏

山东CA应对业务系统及其他重要系统的资源、软件和/或数据进行备份，并制定相应的应急处理流程。当出现计算机资源、软件或数据的损坏时，能在最短的时间内完整有效的恢复被损害的资源、软件和/或数据。

5.7.3 电子认证服务机构私钥的泄露处理流程

当山东CA根证书出现私钥泄露时，应立即撤销根证书，上报电子认证服务管理部门并及时通过合适的途径和方式通知订户和依赖方，然后生成新的根密钥、签发新的根证书。

5.7.4 灾难发生后的业务连续性

山东CA应进行异地数据备份，发生自然灾害或其它不可抗力灾难后，将利用备份数据重建系统恢复业务。

5.8 电子认证服务机构的终止

当山东CA打算终止经营时，应按照相关政策规定在终止经营前三个月给山东CA授权的注册机构、垫付商和证书持有者书面通知，并在终止服务六十日前向行业主管部门报告，按照相关法律规定的步骤进行操作。

6 技术安全控制

6.1 密钥对的生成和安装

6.1.1 密钥对的生成

6.1.1.1 电子认证服务机构的密钥的生成

加密密钥对是通过国家密码管理局安全性审查的密钥管理系统中获取，采用国家密码管理局认可的加密机设备生成的，接受山东省密码管理局监督管理。

签名密钥对是由国家密码管理局认可的密码设备、密码模块的介质或者软件模块生成签名密钥对，签名密钥安全存储在密码设备、密码模块中不可导出，保证山东CA无法复制签名密钥对。

山东CA支持符合国家密码管理局相关规范的密码设备、密码模块产生签名密钥对，如智能密码钥匙USB Key、智能IC卡、SIM Key硬件密码设备或协同签名等密码模块等，订户可根据证书应用场景要求选择签名密钥对生成介质。

服务器端设备证书的密钥对由订户自己产生，订户应妥善保管。

山东CA通过物理安全控制和密钥安全存储控制，在技术、流程和管理上保证密钥对产生的安全性。

6.1.2 递交私钥给订户

订户自己生成的密钥对的情况下，不需要将私钥传给订户。

证书订户的加密私钥是在KMC产生的，该私钥只保存在KMC。在加密私钥从KMC到订户的传递时，采用国家密码管理局许可的对称密钥算法加密，对称密钥通信时为临时密钥，由订户的签名公钥进行加密，山东CA无法获得，这样就保证了证书订户加密私钥的安全。

6.1.3 传送公钥给证书签发机构

证书订户产生的公钥向山东CA提交证书签发申请时，采用PKCS#10格式证书请求信息或者其他约定格式的数据包提交给山东CA，山东CA证书签发前验证所提交的请求，并从该请求信息内提取对应公钥。

6.1.4 传送电子认证服务机构公钥给依赖方

山东CA的根公钥包含在山东CA自签发的根证书中。证书订户可以从山东CA的网站（https://www.sdca.com.cn）上下载山东CA根证书，也可以由山东CA通过目录系统、软件安装、业务系统的安装、电子邮件和软件绑定等方式提供给依赖方。

6.1.5 密钥长度

山东CA所采用的密钥算法和密钥长度符合国家密码管理部门的规定，遵从国家法律法规、政府主管机构等对密钥长度有明确的规范和要求。

6.1.6 公钥参数的生成和资格检查

公钥参数的生成和质量检查由国家密码管理局许可的密码设备或密码模块进行。

6.1.7 密钥用途

山东CA签发的证书应包含密钥用法扩展项，其用法符合RFC5280标准。

6.2 私钥保护和密码模块的工程控制

6.2.1 密码模块标准和控制

山东CA使用国家密码管理局许可的产品，密码模块的标准符合国家规定的要求。

6.2.2 私钥多人控制

山东CA采用多人控制策略激活、使用、备份、停止和恢复山东CA的签名密钥，采取5个管理人员中至少3个在场才可进行操作的原则。

6.2.3 私钥托管

密钥管理中心根据客户和法律的需要，对加密密钥进行托管。通用证书的签名私钥由订户自己保管；协同签名证书的签名私钥由订户终端和协同签名系统协同计算产生并分别保管。

6.2.4 私钥备份

6.2.4.1 电子认证服务机构私钥的备份

山东CA对其签名私钥通过专门的备份加密卡进行备份，私钥的备份采用多人

控制策略。

山东省密钥管理中心备份托管的订户加密私钥，确保加密私钥的安全。

订户的签名私钥山东CA和山东省密钥管理中心都不进行保存和备份。

6.2.5 私钥归档

密钥管理中心提供托管私钥的存档服务，保存期为五年。

6.2.6 私钥导入或导出密码模块

在山东CA业务系统中，可以把订户的私钥导入指定的密码模块中。私钥无法从硬件密码模块中导出，必须通过密码验证之后，才可能使用存储在密码模块中的私钥进行加解密操作。

山东CA的根CA私钥在硬件密码模块上生成、保存和使用。山东CA对根CA私钥进行严格的密钥管理和备份、恢复控制，有效防止了根CA私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

6.2.7 保存在密码模块的私钥

CA根私钥以加密的形式存放在硬件密码设备中，并在该设备中使用。

6.2.8 激活私钥的方法

山东CA将订户证书的私钥保存在USB Key、智能卡等硬件密码模块中，只有输入PIN码，私钥才能被激活使用。

CA私钥存放在密码设备中，具有激活私钥权限的管理员使用含有自己身份的智能IC卡登录，启动密钥管理程序，进行激活私钥的操作，需要半数以上的管理员同时在场。

6.2.9 解除私钥激活状态的方法

对于存放在软件密码模块中的证书的私钥，当软件密码模块被下载、订户退出登录状态、操作关闭或计算机断电时，私钥被解除激活状态。对于存放在硬件密码模块中的订户证书私钥，通过PIN码激活私钥后仅活动一次后即解除其激活状态。

解除CA私钥激活状态的方法包括激活私钥权限的管理员退出、关闭密码模块设备、停止私钥服务应用等。

6.2.10 销毁私钥的方法

对于山东CA签发的最终订户加密私钥，在其生命周期结束后，密钥管理中心对该私钥进行归档妥善保存一定期限，以便于解开加密信息。对于订户签名私钥，在其生命周期结束后，无需再保存，可以通过私钥的删除、系统或密码模块的初始化来销毁。

6.2.11 加密模块定级

山东CA应使用国家密码主管部门批准和许可的密码产品，接受其颁布的各类标准、规范、评估结果、评价证书等各类要求。

6.3 密钥对管理的其它方面

6.3.1 公钥归档

对于生命周期外的CA和最终订户证书，山东CA应进行归档。归档的证书存放在归档数据库中。

6.3.2 证书操作期和密钥对使用期限

证书操作期终止于证书过期或者被撤销。山东CA为订户颁发的证书操作周期通常与密钥对的使用周期是相同的。

对于签名用途的证书，其私钥只能在证书有效期内才可以用于数字签名，私钥的使用期限不超过证书的有效期限。为了保证能够验证在证书有效期内的签名的信息，公钥的使用期限可以在证书的有效期限之外。

对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公钥的使用期限不超过证书的有效期限。为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。

6.4 激活数据

6.4.1 激活数据的产生和安装

CA根私钥的激活信息由存放有CA根私钥加密卡的产生，并分割保存在5个智能卡中，通过专门的读卡设备和软件读取。所有秘密分割的创建和分发应有相应

的记录，包括产生时间、持有人等信息。

订户证书私钥激活数据可以是口令或者指纹等识别方式。如果订户证书私钥的激活数据是口令，这些口令必须：

1）至少 6 位字符或数字；

2）不能包含很多相同的字符；

3）不能和操作员的名字相同；

4）不能使用生日、电话等数字；

5）不能包含订户名信息中的较长的子字符串。

6.4.2 激活数据的保护

保存有CA根私钥的激活数据的5个智能卡，由5个不同的超级管理员掌管，而且超级管理人员必须符合山东CA职责分割的要求，签署协议确认他们知悉秘密分割掌管者责任。

如果证书订户使用口令或 PIN 码保护私钥，订户应妥善保管好其口令或 PIN 码，防止泄露或窃取。

6.4.3 激活数据的其它方面

1）激活数据的传送

存有CA根私钥的激活数据的智能卡，通常应保存在认证机构的安全设施中，不能携带外出或传送。如因某种特殊情况确实需要传送时，其传送过程需在安全管理人员的监督下进行。

当订户证书私钥的激活数据需要进行传送时，应保护它们在传送过程中免于丢失、偷窃、修改、非授权泄露、非授权使用等。

2）激活数据的销毁

存有CA根私钥的激活数据的智能卡，其销毁所采取的方法包括将智能卡初始化，或者彻底销毁智能卡，保证不会残留有任何秘密信息。CA根私钥激活数据的销毁是在安全管理人员的监督下进行。

当订户证书私钥的激活数据不需要时应该销毁，订户应该确保无法通过残余信息、介质直接或间接恢复激活数据的部分或全部，比如记录有口令的纸页必须粉碎。

6.5 计算机安全控制

6.5.1 特定的计算机安全技术要求

山东CA的证书签发系统的数据文件和设备由系统管理员维护，未经授权，其他人员不能操作和控制。山东CA系统密码有最小密码长度要求，而且必须符合复杂度要求，系统管理员应定期更改系统密码。

山东CA系统应部署在多级不同厂家的防火墙之内，确保系统网络安全。系统逻辑上与其他组件系统和信息访问进行隔离，只允许已经定义的应用进程进行访问。

6.5.2 计算机安全等级

山东CA的计算机安全等级不应低于三级。

6.6 生命周期技术控制

6.6.1 系统开发控制

系统开发控制包括可信人员管理、开发环境安全管理、产品设计和开发评估、使用可靠的开发工具等。应参考国家相关标准制定软件开发规范，并在实施中严格执行。

6.6.2 安全管理控制

山东CA电子认证系统的使用必须具有严格的控制措施，所有的系统都应经过严格的测试验证后才进行使用，山东CA的任何配置以及任何修改和升级都要记录在案并进行控制，并且需要采取一种灵活的管理体系来控制和监视系统的配置，以防止未授权的修改。认证机构还对认证系统进行定期和不定期的检查和测试。

6.6.3 生命期的安全控制

山东CA电子认证系统在系统设计过程中要充分考虑安全性，在开发过程中应有严格的流程进行代码安全管理，开发完成后进行严格的安全测试，在正式使用前必须通过国家有关部门的系统安全性审查和技术鉴定。

6.7 网络的安全控制

山东CA应采用防火墙、入侵检测、漏洞扫描和网络防病毒等安全机制对网络进行安全控制，只允许已授权的机器和账号访问。只有经过授权的山东CA员工才能够进入授权的设备和CA系统。

CA系统只开放与证书业务及管理相关的端口和服务。

CA系统的边界控制设备应拒绝一切非电子认证业务的服务。

6.8 时间戳

山东CA系统使用可信时间源保证系统时间的准确性。

7 证书、证书吊销列表和在线证书状态协议

7.1 证书

7.1.1 版本号

山东CA签发的证书均符合X.509 V3证书格式，遵循RFC5280标准。

7.1.2 证书扩展项

山东CA签发的证书应符合RFC5280和国家相关标准、规范的要求。

山东CA签发证书应支持（但不限于）以下证书标准扩展项：

1）颁发机构密钥标识符（authorityKeyIdentifier）

本项提供了一种识别与证书签名私钥相应的公钥的方式。山东CA产生的所有证书都应包括该扩展，以便于链的建立。本扩展标记为非关键的。

2）主题密钥标识符（subjectKeyIdentifier）

本项提供一种识别包含有一个特定公钥的证书的方法。山东CA产生的所有证书必须包括本扩展，而且山东CA自签名证书必须把本扩展的值赋给终端实体证书的颁发机构密钥标识符的扩展项中。此扩展项标记为非关键的。

3）密钥用法（keyUsage）

本项说明证书已认证的公开密钥的用途，包括：验证数字签名（digitalSignature）、不可抵赖（nonRepudiation）、密钥加密（keyEncipherment）、数据加密（dataEncipherment）、密钥协商（keyAgreement）、验证证书签名（keyCertSign）、验证CRL签名（CRLSign）、只加密（encipherOnly）、只解密（decipherOnly）。

如果密钥的用法只限于所指示的用途时标记为关键的，否则标记为非关键的。

4）增强密钥用法（extKeyUsage）

本项可以作为对密钥用法扩展项中指明的基本用途的补充和替代。山东CA可以根据证书应用服务需求标记此扩展的关键度。

5）主题替换名称（subjectAltName）

本项包含一个或者多个替换名供实体使用。山东CA可以根据证书应用服务需求标记此扩展的关键度，如果标记为关键的，至少应能识别和处理一个条目。

6）基本限制（basicConstraints）

本项用于标识证书的主体是否是一个CA，通过该CA可能存在的认证路径有多长。山东CA证书必须包括此项扩展，根证书主题类型被设为CA，最终订户证书的主题类型被设为End-Entity。本扩展项根据应用标记关键度。

7）证书撤销列表分发点（CRLDistributionPoints）

CRL分发点扩展用来标识如何获得CRL信息。本扩展项根据应用标记关键度。

8）其他

针对不同的证书应用服务需求，还应支持的扩展项包括（但不限于）：

个人身份识别码：用于标识个人身份证件的号码，此扩展项标记为非关键的。

统一社会信用代码：用于标识组织的证件号码，此扩展项标记为非关键的。

山东CA所签发的证书还应支持自定义的私有扩展项，且必须标记为非关键扩展。

7.1.3 算法对象标识符

符合国家密码主管部门批准的算法对象标识符。

7.1.4 命名形式

山东CA签发证书的甄别名符合 X.500 关于甄别名的规定。详细内容请见第3.1节内容。

7.1.5 名称约束

在山东CA 证书服务体系中，除在特定场景下的证书以外，原则上订户不能使用匿名或假名。

7.1.6 证书策略对象标识符

没有使用。

7.1.7 策略限制扩展项的使用

无规定。

7.1.8 策略限定符的语法和语义

无规定。

7.1.9 关键证书策略扩展项的处理规则

关键扩展项不能识别，拒绝处理证书。

7.2 证书撤销列表

7.2.1 版本号

山东CA签发X.509 V2版本的证书撤销列表。所签发的CRL遵循RFC5280标准。

7.2.2 证书撤销列表和 CRL Entry 扩展

与X.509和PKI规定一致。

7.3 OCSP 服务

山东CA对外提供OCSP服务，作为CRL的有效补充，为证书状态查询提供即时的最新响应，应符合RFC2560标准的要求。

8 合规性审计和相关评估

8.1 评估的频率或情况

根据情况而定，有年度评估、运营前评估和随时进行评估。

山东CA本身也需要对山东CA的关联单位（包含山东CA授权的注册机构、受理点等证书体系成员）所有的流程和操作进行审计，检验其是否符合电子认证业务规则和相应的证书政策的规定，其频率可由山东CA决定或由法律制定的监管机构决定。

根据《中华人民共和国电子签名法》、《电子认证服务管理办法》等的要求，每年一次接受上级主管部门的合规性审计。

根据审计结果，需要整改后复审的，应接受复审。

8.2 评估者的身份/资质

对山东CA实施规范审计的审计者所具有的资质和经验必须符合监管法律和行业准则规定的要求，包括：

1）必须是经许可的、有营业执照的、具有计算机安全专门技术知识的审计人员或审计评估机构，且在业界享有良好的声誉；

2）了解计算机信息安全体系、通信网络安全要求、PKI技术、标准和操作；

3）具备检查系统运行性能的专业技术和工具。

8.3 评估者与被评估者之间的关系

对山东CA进行审计的审计者，必须是一个独立于山东CA的实体。

8.4 评估内容

评估应包括以下内容：

1）电子认证业务规则是否符合证书策略的要求；

2）山东CA是否有能力来实施电子认证业务规则中制订的相关操作流程和运作协议；

3）山东CA支持的证书认证操作规程是否完全与电子认证业务规则表达一致，

包括山东CA的技术、手续和员工的相关管理政策和电子认证业务规则；

4）山东CA是否实施了相关技术、管理、相关政策和电子认证业务规则；

5）评估者或山东CA认为有必要评估的其他方面。

8.5 对不足采取的措施

如果在内部评估过程中发现执行有不足之处，由安全管理委员会负责监督这些问题的责任职能部门进行业务改进和完善的情况，完成对评估结果的改进后，各职能部门必须向安全管理委员会提交业务改进工作总结报告。

如果在外部评估过程中发现执行有不足之处，山东CA必须根据评估的结果检查缺失和不足，根据提出的整改要求，提交修改和预防措施以及整改方案，并接受对整改方案的审查，以及对整改情况的再次评估。

8.6 评估结果的传达与发布

除非法律明确要求，山东CA一般不公开评估结果。

9 商业和法律相关事务

9.1 费用

9.1.1 证书签发和更新费用

山东CA收取合理的证书签发和更新费用，并在订户订购时提前告知。

9.1.2 证书查询费用

查询在有效期内的证书，山东CA目前不收取任何费用。

9.1.3 撤销和状态信息查询费用

通过山东CA网站对证书撤销和状态查询，目前不收取任何费用。

9.1.4 其他服务费用

山东CA保留收取其他服务费的权利。

9.1.5 退款条件说明

在实施证书操作和签发证书的过程中，山东CA遵守并保持严格的操作程序和策略。一旦订户接受数字证书，山东CA将不办理退证、退款手续。

如果订户在证书服务期内退出数字证书服务体系，山东CA将不退还剩余时间的服务费用。

9.2 财务责任

山东CA应具有维持、运作和履行其责任的经济基础，有能力承担对订户、依赖方因合法使用数字证书时而造成的责任风险，根据电子认证业务规则规定的方式和范围进行有过错时的赔偿。

9.3 业务信息保密

山东CA应有专门的信息保密制度，保护自身和客户的敏感信息、商业秘密。

9.3.1 保密信息范围

保密的业务信息包括但不限于以下方面:

1）在双方披露时标明为保密(或有类似标记)的;

2）在保密情况下由双方披露的或知悉的;

3）双方根据合理的商业判断应理解为保密数据和信息的;

4）以其他书面或有形式确认为保密信息的;

5）或从上述信息中衍生出的信息。

对于CA机构来说，保密信息包括但不限于以下方面:

1）保存在审计记录中的信息;

2）年度审计结果也同样视为保密;

3）除非有法律要求，由CA机构掌握的，除作为证书、CRL、认证策略被清楚发布之外的个人和公司的信息需要保密。

CA机构不保存任何证书应用系统的交易信息。

除非法律明文规定,CA机构没有义务公布或透露订户数字证书以外的信息。

9.3.2 非保密信息范围

山东CA电子认证业务规则、证书申请流程、手续、申请操作指南、证书撤销列表等。

9.3.3 保护保密信息的责任

山东CA应有各种严格的管理制度、流程和技术手段保护自身的商业秘密，每个员工都必须接受信息保密方面的培训，并与公司签订保密协议。任何参与方有责任保证不泄露保密信息。

9.4 个人隐私保护

9.4.1 隐私保护方案

在数字证书生命周期中，山东CA在订户个人隐私信息的收集、使用、存储环节中，采取有效手段，保护个人隐私信息。

山东CA保护证书申请人所提供的、证明其身份的资料，并采取必要的安全措施防止证书申请人资料被遗失、盗用与篡改。

山东CA实施信息安全管理制度以及行业通行的安全技术和程序来确保订户的个人信息不被丢失、泄露、篡改、毁损或滥用。

9.4.2 视为隐私的信息

订户提供的不构成数字证书内容的资料被视为隐私信息。

9.4.3 不被视为隐私的信息

订户提供的用来构成证书内容的信息不被视为隐私信息。法律和行政法规另有规定的除外。

9.4.4 保护隐私信息的责任

除执法、司法方面的强制需要，山东CA及其注册机构在没有获得客户授权的情况下，不会将客户隐私信息透露给第三方。

9.4.5 使用隐私信息的告知与同意

山东CA或其注册机构如果需要将客户隐私信息用于双方约定的用途以外的目的，则需要事先告知订户并获得订户同意。

9.4.6 依法律或行政程序的信息披露

在以下情况下，山东CA可以向特定的对象公布隐私信息，山东CA无需承担由此造成的任何责任：

1）基于法律法规而提供的；

2）司法机关通过合法程序；

3）经订户书面授权或同意提供的。

9.4.7 其他信息披露情况

对其他信息的披露应遵循国家的相关规定与订户相关协议。

9.5 知识产权

山东CA保留对本证书策略的所有知识产权。

山东CA保留其签发的证书和证书撤销信息的所有知识产权。任何人可以免费地复制、分发证书和证书撤销列表，只要他们进行完整复制并且证书和证书撤销列表的使用符合本证书策略。

证书申请者保留证书申请中包含的申请者拥有的商标、服务标志或商业名称以及签发给该证书申请者的证书中的可辨识名的所有权利。

证书所有者拥有其证书相关的密钥对的知识产权。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

山东CA承担的责任和义务是：

1）保证电子认证服务机构本身使用和发放的公钥算法在现有通常技术条件下不会被攻破；

2）保证山东CA的签名私钥在山东CA内部得到安全的存放和保护；

3）山东CA建立和执行的安全机制符合国家政策的规定。

山东CA不对由于客观意外或其他不可抗力事件造成的操作失败或延迟承担任何损失、损坏或赔偿责任。这些事件包括劳动纠纷、交易一方故意或无意的行为、罢工、暴动、骚动、战争、火灾、爆炸、地震、水灾或其他大灾难等。

9.6.2 注册机构的陈述与担保

注册机构必须遵守所有的登记程序和安全保障措施。这些程序和保障由山东CA决定，并在电子认证业务规则或相应的注册机构协议中规定，山东CA可以根据情况修改有关内容，并及时公布。

9.6.3 订户的陈述与担保

所有的订户必须严格遵守关于证书申请以及私钥的所有权和安全保存相关的程序：

1）订户在证书申请表上填列的所有声明和信息必须是完整、精确、真实和正确的，可供山东CA或受理点检查和核实；

2）订户必须严格遵守和服从电子认证业务规则规定的或者由山东CA推荐使用的安全措施；

3）订户需熟悉电子认证业务规则的条例和与证书相关的证书政策，遵守订户证书使用方面的有关限制；

4）一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘或泄密以及其他情况，订户应立刻通知山东CA或山东CA授权的注册机构，申请采取挂失、撤销等处理措施。

9.6.4 依赖方的陈述与担保

依赖方确保在任何信赖行为发生之前，阅读了电子认证业务规则，并评估了在特定应用中信赖证书的适当性，不在证书适用目的以外的应用中信任证书。

9.6.5 其他参与者的陈述与担保

遵守本证书策略的所有规定。

9.7 免责声明

在法律允许的范围内，电子认证业务规则包含山东CA的免责声明。

9.8 有限责任

在法律允许的范围内，山东CA只承担对外声明的、在电子认证业务规则中规定和对外签署的任何协议中所规定的有限责任。在电子认证业务规则中明确规定合理的赔付标准。

9.9 赔偿

山东CA如违反了第9.6.1节中的陈述，订户和依赖方等实体可申请山东CA承担赔偿责任（法定或约定免责的除外），具体赔偿的范围、限额、免赔等在电子认证业务规则中进行规定。

9.10 有效期限与终止

9.10.1 有限期限

本证书策略自发布之日起生效。

9.10.2 终止

当新版本的证书策略生效时或山东CA终止业务时，旧版本证书策略自动终止。

9.10.3 终止与生存的效力

本证书策略终止后，已签发符合本证书策略的证书，效力作用直到证书到期或撤销。

当由于某种原因，如内容修改、与适用法律相冲突，证书策略、电子认证业务规则、订户协议、依赖方协议和其他协议中的某些条款失效后，不影响文件中其他条款的法律效力。

9.11 对各参与者的个别通告与沟通

山东CA及其注册机构在必要的情况下，如在主动撤销订户证书、发现订户将证书用于规定外用途及订户其他违反订户协议的行为时，会通过法律认可的通信方式，个别通知订户、依赖方。

9.12 修订

9.12.1 修订流程

证书策略中所列条款不能适应运营的实际需求，或者与现行法律相抵触时，山东CA有权在合适的时间修订本证书策略中任何术语、条件和条款，而且无须预先通知任何一方。

山东CA安全管理委员会组织编写小组进行修订，在征询山东CA法律顾问有关方面的意见后，提交山东CA安全管理委员会审批，审批通过后正式实施。

9.12.2 通知机制和期限

山东CA保留随时对证书策略进行修订的权利，进行下列（但不限于）不重要的修订后将不作通知：对印刷错误的更正、URL的改变和联系人信息的变更等。

修订后的证书策略经批准后将及时生效。

9.12.3 必须更换 OID 的情况

由山东CA安全管理委员会根据公司业务情况决定。

9.13 争议处理

如果各参与方之间无法协商解决出现的问题和争端，可通过法律途径解决。

9.14 管辖法律

本证书策略在各方面服从《中华人民共和国电子签名法》、《电子认证服务管理办法》等中华人民共和国法律、法规、规章的约束和解释。山东CA的任何业务

活动受有关法律、法规的制约，任何业务和法律文件、合同的解释、执行不能同有关法律、法规相冲突。

9.15 与适用法律的符合性

本证书策略的使用必须遵从中华人民共和国的相关法律和法规。

9.16 杂项条款

9.16.1 完整协议

证书策略、电子认证业务规则、订户协议及其他补充协议将构成山东CA电子认证参与者之间的完整协议。

9.16.2 转让

山东CA、山东CA注册机构、订户及依赖方之间的责任、义务不能通过任何形式转让给其他方。

9.16.3 分割性

当法庭判定协议中的某一条款由于某种原因无效或不具执行力时，不会出现因为某一条款的无效导致整个协议无效。

9.16.4 强制执行

无规定。

9.16.5 不可抗力

当由于不可抗力，如地震、洪灾、雷电等自然灾害和战争、社会异常事件、政府行为、互联网或其他基础设施无法使用等，造成山东CA、注册机构无法履行合同，不能提供正常的服务时，山东CA、注册机构可免除违约责任，不承担由此给客户造成的损失。