山东 CA CPS

电子认证业务规则

版本 4.0.3

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

电子认证业务规则

山东省数字证书认证管理有限公司版权所有

版权声明

注意：《电子认证业务规则》服从于中国的法律法规，包括且不限于：《中华人民共和国电子签名法》、《电子认证服务管理办法》以及其他相关法律、行政法规。

对任何已经或即将涉嫌犯罪而影响山东省数字证书认证管理有限公司证书服务的组织、单位和个人，山东省数字证书认证管理有限公司将保留依法追诉的权利。

电子认证业务规则修订表

版本	生效日期	修订说明	发布者
1.0	2001年5月8日	采用RFC2527结构	安全管理委员会
2.0	2004年5月1日	采用RFC3647结构	安全管理委员会
2.0	2005年08月18日	《山东CA电子认证业务规则》根据《中华人民共和国电子签名法》、《电子认证服务管理办法》和中华人民共和国信息产业部颁布的《电子认证业务规则规范（试行）完全版》进行修改	安全管理委员会
2.1	2008年3月27日	根据信息产业部电子认证服务管理办公室年审意见修改	安全管理委员会
3.0	2011年1月1日	根据信息产业部电子认证服务管理办公室意见、最新山东CA证书策略和公司现有运营情况修改	安全管理委员会
4.0	2022年9月1日	增加事件证书应用的描述，根据新的业务模式修订身份鉴别、证书生命周期管理的业务规则	安全管理委员会
4.0.1	2023年3月27日	增加域名、IP 地址等的鉴别方法	安全管理委员会
4.0.3	2025年11月7日	增加对内设机构和内部人员的身份鉴别方法	安全管理委员会

目　录

第一章 概括性描述

1.1 概述

1.1.1 公司简介

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。

1.1.2 电子认证业务规则

山东省数字证书认证管理有限公司电子认证业务规则（以下简称 CPS）根据国家相关法律法规的要求，详细阐述了山东 CA 提供的电子认证服务整个过程、电子认证业务所遵循的规范以及电子认证服务各方所承担的责任范围等。

本规范适用于山东 CA 以及授权的注册机构，并通过公开发布的渠道告知电子签名订户、依赖方等相关参与者，以确保山东 CA 所提供的电子认证服务是权威、安全、可靠的规范化第三方服务。对于山东 CA 所提供的认证服务过程的责任范围，本业务规则也给予了明确的规定

1.2 文档名称与标识

1.2.1 名称

本文档称为《山东省数字证书认证管理有限公司电子认证业务规则》（简称 CPS），是山东 CA 对所提供的认证及相关业务的全面描述，对象标识符 CPS 为“Certificate Practice Statement”的缩写。本文档中，CPS 等同于本节中定义的文

档名称和适用名称。

1.2.2 标识

山东 CA 是山东省数字证书认证管理有限公司（Shandong Certificate Authority Co.Ltd）的简称形式。

山东 CA 所拥有的品牌的商标为：

1.2.3 发布

以电子的方式，在山东 CA 网站发布。网站地址：https://www.sdca.com.cn。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

山东 CA 是根据《中华人民共和国电子签名法》、《电子认证服务管理办法》规定，依法设立的第三方电子认证服务机构。山东 CA 通过给从事电子交易活动的各方主体颁发数字证书、提供证书验证服务等手段而成为电子认证活动的参与主体。

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（Registration Authority）

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（Business Terminal）

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、电子邮件、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（sponsor）

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。

1.3.5 订户（Certificates Applicant）

指接受并持有山东 CA 颁发的证书终端实体，包括个人、企业和组织机构。

1.3.6 依赖方（Relying Party）

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。

1.3.7 其他参与者（Other Participants）

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 证书应用

1.4.1 适合的证书应用

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。在不违背相关法律法规、本 CPS 以及订户协议的情况下，此类证书也可以用于其他用途。

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，在不违背相关法律法规、本 CPS 以及订户协议的情况下，此类证书也可以用于其他用途。

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，在不违背相关法律法规、本 CPS 以及订户协议的情况下，此类证书也可以用于其他用途。

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 限制的证书应用

证书禁止在任何违反国家法律、法规或破坏国家安全的情形下使用。否则，由此造成的法律后果由订户自己承担。

山东 CA 签发的数字证书禁止的应用范围包括：

1）国家法律法规所规定的不允许使用的范围；

2）破坏国家安全、环境安全和人身安全的危险环境；

3）山东 CA 与订户约定的证书禁止应用的范围。

1.5 策略管理

1.5.1 策略文档管理机构

本 CPS 的管理机构是山东 CA 安全管理委员会。由山东 CA 安全管理委员会负责本 CPS 的制订、发布、更新和解释等事宜。

本 CPS 由山东省数字证书认证管理有限公司拥有完全版权。

1.5.2 联系人

山东 CA 安全管理委员会为本 CPS 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 决定 CPS 符合策略的机构

决定 CPS 符合策略的机构为：山东 CA 安全管理委员会。

1.5.4 CPS 批准程序

按照工业和信息化部公布的《电子认证业务规则规范》的要求，在本 CPS 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，在山东 CA 网站予以公布，自公布之日起三十日内向工业和信息化部备案。

1.6 定义与缩写

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。它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，提供互联网环境的身份鉴别、信息加解密、数据完整性和不可否认性服务。

电子认证服务机构（CA）

电子认证服务机构（Certification Authority，简称 CA）是受订户信任的，负责签发数字证书的权威机构，又称为数字证书认证中心。作为电子交易中受信任

的第三方，负责为电子认证业务中各个实体颁发数字证书，以证明各实体身份的真实性，并负责在交易中检验和管理证书。

注册机构（RA）

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

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。数字证书提供了一种在 Internet 上验证身份的方式，其作用类似于日常生活中的身份证。

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。CRL 是证书撤销状态的公布形式，就像信用卡的黑名单，它通知其他证书订户某些电子证书不再有效。

在线证书状态协议（OCSP）

在线证书状态协议是用于检查数字证书在某一交易时间是否有效的标准。

证书策略（CP，Certificate Policy）

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。

电子认证业务规则（Certificate practice Statement，简称 CPS）

电子认证业务规则（Certificate 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。

私钥（Private key）

私钥（Private key）是在公钥基础设施 PKI 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。在数字签名中又称为电子签名制作数据，是在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。

公钥(Public key)

公钥(Public key)是在公钥基础设施（PKI）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。在数字签名中又称为电子签名验证数据，是用于验证电子签名的数据，包括代码、口令等。

甄别名(DN, Distinguished Name)

甄别名(DN，Distinguished Name)是在数字证书的主体名称域中，用来唯一标识订户的 X.500 名称。此域需要填写反映订户真实身份的、具有实际意义的、与法律不冲突的内容。

第二章 信息发布与信息管理

2.1 认证信息的发布

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。

根据我国法律法规的要求以及 X.509 标准，山东 CA 在对外的目录服务器公布证书相关信息，并定期公布证书撤销列表 CRL。

2.2 公众信息的发布

2.2.1 CPS 的发布

山东 CA 通过公司网站（https://www.sdca.com.cn）发布本机构制定的 CPS，并负责本规范的解释，一经山东 CA 在网站发布，即时生效，并对一切仍有效的数字证书的使用者、新的数字证书及相关业务的申请者均具备约束力。

本 CPS 的发布及更改一律须经山东 CA 核准和发布。如有需要可访问山东 CA 网站查看本 CPS，对具体个人不另行通知。

2.2.2 山东 CA 公众信息的发布

山东 CA 在公司网站 https://www.sdca.com.cn 上发布与其相关的公众信息，并对旧信息进行处理。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 发布时间及频率

2.3.1 电子认证业务规则的发布时间及频率

山东 CA 根据认证业务需要进行 CPS 的不定期变更，山东 CA 将通过文档版本升级的形式，以原有公布方式予以及时发布，一经发布，即时生效，并对一切仍有效的数字证书的使用者、新的数字证书及相关业务的申请者均具备约束力。

2.3.2 山东 CA 公众信息的发布时间及频率

山东 CA 在公司网站（https://www.sdca.com.cn）上发布与其相关的公众信息，处理旧信息。山东 CA 的网站实时更新，并在第一时间发布信息。

2.3.3 证书的发布时间及频率

山东 CA 的目录服务器实时更新目录，通常在 24 小时内发布最新 CRL。证书订户可在山东 CA 网站（https://www.sdca.com.cn）上查询或下载数字证书和 CRL。

2.4 信息库访问控制

2.4.1 信息的发布与处理

对于公开发布的 CP、CPS、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。

2.4.2 信息访问控制和安全审计

山东 CA 设置了信息访问控制和安全审计措施，保证了 CP、CPS、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。

第三章 身份标识与鉴别

3.1 命名规则

3.1.1 名称类型

山东 CA 采用 X.500 定义的唯一甄别名 DN（Distinguished Name）来标识订户身份信息，该甄别名包含于证书主体中。

3.1.2 对名称意义化的要求

订户的甄别名（DN）必须具有一定的意义，能够与证书主体所对应的实体建立确定联系。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 理解不同名称形式的规则

山东 CA 签发的数字证书符合 X.509 标准，甄别名格式遵守 X.500 标准，甄别名的命名规则由山东 CA 定义与解释。

3.1.5 名称的唯一性

在山东 CA 信任域内，不同订户证书的主题甄别名不能相同，必须是唯一的。但对于同一订户，可以用其主体名为其签发多张证书，但证书的密钥用法扩展项不同。当证书申请中出现不同订户存在相同名称时，遵循先申请者优先使用，后申请者增加附加识别信息予以区别的原则。

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 初始身份确认

3.2.1 证明拥有私钥的方法

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。山东 CA 在签发证书前，系统将自动使用订户的公钥验证其私钥签名的有效性和申请数据的完整性，以此来判断证书使用者拥有私钥。

3.2.2 组织机构身份的鉴别

对于组织机构订户，山东 CA 或授权的注册机构需要鉴别：

1）订户提交的组织身份信息

鉴别方法包括核对订户提交的组织有效身份证件或证件的具体信息。必要时可以通过权威第三方数据源对身份证件信息进行比对。组织有效身份证件指政府部门签发的证件或文件，包括但不限于营业执照、事业单位法人证书、社会团体登记证、政府批文等。

2）组织授予经办人的授权证明

鉴别方法包括但不限于检查组织或组织的法定代表人授权给经办人办理证书事宜的授权文件或授权条款，也可以通过法定代表人手机短信验证方式核实。

3）经办人的个人身份证明材料

鉴别方式可以采用面对面现场鉴别或线上远程鉴别。当山东 CA 或授权的注册机构认为有需要时，可以增加其他方式，包括但不限于鉴别组织的法定代表人身份或要求经办人提交法定代表人有效身份证件证明。

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，例如要求提交所有权文件，归属权证明文件、查询第三方数据库等。

5）针对政府、医院、学校等内设机构这类特定用户，其数字证书主要服务于机构内部的业务系统。CA 机构或其授权的注册机构，可依据内设机构审核确认后提供的证书用户发放名单，作为用户身份核验的基础依据。还可通过短信验证码、单位官方邮箱，或对接权威第三方数据库等补充方式，核验用户身份的真实性，进而完成证书申请的审批或驳回操作。

鉴别审核批准后，山东 CA 或注册机构按照相关法律法规的要求妥善保存订户申请材料，山东 CA 保存订户申请材料可以是纸质或电子数据形式。

本 CPS 简要说明了如何进行组织身份鉴别。山东 CA 保留根据最新国家政策法规的要求更新组织身份鉴别方法与流程的权利。

3.2.3 个人身份的鉴别

对于个人订户，山东 CA 或授权的注册机构将验证个人有效身份证件或证件的具体信息，核实个人订户身份的真实性。个人有效身份证件指政府部门签发的证件，包括但不限于：身份证、港澳台居民身份证、户口簿、护照、军官证等。

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，例如要求提交所有权文件，归属权证明文件、查询第三方数据库等。

鉴别方式可以采用面对面现场鉴别或线上远程鉴别。必要时，可以通过权威第三方数据源信息比对、手机短信验证等其他可靠的方式鉴别。

对于政府、医院、学校等内部人员这类订户，与 3.2.2 组织机构身份的鉴别章节中对于政府、医院、学校等内设机构的身份鉴别方式相同。

鉴别审核批准后，山东 CA 或授权的注册机构按照相关法律法规的要求妥善保存订户申请材料，山东 CA 保存订户申请材料可以是纸质或电子数据形式。

本 CPS 简要说明了如何进行个人身份鉴别。山东 CA 保留根据最新国家政策法规的要求更新个人身份鉴别方法与流程的权利。

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 没有验证的订户信息

除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，山东 CA 不对申请时的其他信息予以验证。

对于没有验证过的订户信息，山东 CA 将不承诺此类信息的真实性，并不承担由于此类信息引起的任何责任和解决纠纷的义务。

3.2.6 授权确认

个人在山东 CA 的数字证书申请表上写明经办人的身份信息并签名确认，或采用权威第三方数据源信息比对、手机短信验证等其他安全有效方式体现申请人真实意愿的方式，则证明本人对经办人的授权确认。

代表组织获取数字证书，需要出具组织授权其为该组织办理数字证书事宜的授权文件。组织在山东 CA 的数字证书申请表上加盖单位公章或采用权威第三方数据源信息比对、法定代表人手机短信验证等其他安全有效方式体现申请机构真实意愿的方式，则证明本组织对经办人的授权确认。

3.2.7 互操作准则

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 常规密钥更新的标识与鉴别

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。

山东 CA 授权的注册机构的审核人员合理、审慎地核对申请资料，根据审核

人员的管理规定对申请者的资料的真实性进行审查，并进行批准或拒绝的操作。

密钥更新会造成使用原密钥对加密的文件或数据无法解密，因此，订户在申请密钥更新前，必须确认使用原密钥对加密的文件或数据已经解密，由此造成的损失，山东 CA 将不承担责任。

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 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证书时，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。

第四章 证书生命周期操作要求

山东 CA 授权的注册机构提供完整的数字证书周期，包括证书申请、申请处理、签发、接受、密钥对和证书的使用、证书更新、证书密钥更换、证书变更、证书撤销和挂起、证书状态服务、密钥生成备份和恢复等服务，提供身份认证、电子签名、数据加密、密钥管理等与数字证书密切相关的配套服务。自 CA 认证系统签发之日算起，山东 CA 签发的个人类型证书、机构类型证书的默认有效期为 1 年；设备类型证书的默认有效期为 1 年；山东 CA 保留根据业务需要重新设置订户证书有限期的权利。

4.1 证书申请

4.1.1 证书申请实体

证书申请实体包含个人、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 申请过程与责任

证书申请人按照本 CPS 所规定的要求，通过现场面对面或在线方式提交证书申请，包括相关的身份证明材料。山东 CA 或注册机构应明确告知证书订户所需承担的相关责任和义务，证书申请人表达申请证书的意愿后，山东 CA 或注册机构依据身份鉴别规范对证书申请人的身份进行鉴别，并决定是否受理申请。

证书申请流程如下：

订户：订户需要提供本 CPS 第 3.2 节所述的有效身份证明材料，并确保材料真实准确。配合山东 CA 或授权的注册机构完成对身份信息的采集、记录和审核。

山东 CA：山东 CA 参照本 CPS 第 3.2 节的要求对订户的身份信息进行采集、记录，审核。通过鉴证后，山东 CA 向订户签发证书。如果订户身份信息的鉴别由授权的注册机构完成，山东 CA 应对授权的注册机构进行监督管理。

注册机构：授权的注册机构参照本 CPS 第 3.2 节的要求对订户的身份信息进行采集、记录和审核。通过鉴证后，注册机构向山东 CA 提交证书申请，由山东 CA 向订户签发证书。注册机构须接受山东 CA 的监督管理。授权的注册机构应

当按照山东 CA 的要求，向山东 CA 提交身份鉴证资料或自行妥善保存。

订户的申请表和相关证明文件至少保存到证书失效后五年。

证书申请人应当提供真实、完整和准确的信息，山东 CA 或其注册机构须按本 CPS 第 3.2 节的要求和流程对申请人身份材料信息进行审查。如证书申请人未向山东 CA 提供真实、完整和准确的信息，或者有其他过错，给山东 CA 或电子签名依赖方造成损失的，由证书申请人承担赔偿责任。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

山东 CA 或授权的注册机构按照本 CPS 所规定的身份鉴别流程对申请人的身份进行识别与鉴别。具体的鉴别流程详见本 CPS 第 3.2 节初始身份确认。

4.2.2 证书申请批准和拒绝

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 处理证书申请的时间

山东CA授权的注册机构将在1个工作日内对证书申请者提交的证书信息进行识别，并处理证书申请。

事件证书申请为即时处理。

4.3 证书签发

4.3.1 证书签发中注册机构和电子认证服务机构的行为

订户一旦提交了证书申请，尽管事实上还没有接受证书，但该订户仍被视为已同意山东 CA 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），将为证书申请者签发证书。

证书的签发意味着山东 CA 最终完全正式地批准了证书申请。证书从订户接受证书（参见第 4.4 节）之日起将被视为有效证书。

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 构成接受证书的行为

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 电子认证服务机构对证书的发布

一旦证书订户接受证书，山东 CA 将在目录服务器或其他合理的方式来发布证书。

山东 CA 不提供事件证书的发布。

4.4.3 电子认证服务机构对其他实体的通告

山东 CA 不具有向其他实体进行单独通告的义务，但使用证书的各类实体可以通过山东 CA 查询服务获得所需证书信息。

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超过其规定使用范围，否则山东 CA 不承担由订户违规使用而造成的任何责任。

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。

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 依赖方公钥和证书的使用

依赖方只能在接受山东 CA 协议要求的前提下，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。

当依赖方需要发送加密信息给接受方时，须先通过适当的途径获得接受方的加密证书，然后使用证书上的公钥对信息加密并发送给接受方。

获得对方的证书和公钥，可以通过查看证书以了解对方的身份，通过公钥验证对方电子签名的真实性，实现通信的不可抵赖性，并实现通信双方数据传输的保密性和完整性。

4.6 证书更新

证书更新指在不改变证书注册信息的情况下，为订户签发一张新证书。

4.6.1 证书更新的情形

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 请求证书更新的实体

订户本人或其授权代表。

4.6.3 证书更新请求的处理

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。注册机构审核通过后，为订户制作证书；证书签发后，注册机构将证书当面发给订户。订户接受证书（参见第 4.4 节）；新证书签发后原有证书将被撤销（参见第 4.9 节）。山东 CA 将实时在 LDAP 上发布订户的新证书。订户被撤销的原有证书将在 24 小时内通过 CRL 发布。

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 构成接受更新证书的行为

同第 4.4.1 节“构成接受证书的行为”。

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“电子认证服务机构对证书的发布”。

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“电子认证服务机构对其他实体的通告”。

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 证书密钥更换的情形

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 请求证书密钥更换的实体

订户本人或其授权代表。

4.7.3 证书密钥更换请求的处理

同第 4.6.3 节“证书更新请求的处理”。

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 构成接受密钥更换证书的行为

同第 4.4.1 节“构成接受证书的行为”。

4.7.6 电子认证服务机构对密钥更换证书的发布

同第 4.4.2 节“电子认证服务机构对证书的发布”。

4.7.7 电子认证服务机构对其他实体的通告

同第 4.4.3 节“电子认证服务机构对其他实体的通告”。

4.8 证书变更

4.8.1 证书变更的情形

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 请求证书变更的实体

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 颁发新证书时对订户的通告

同第 4.7.4 节“订户新证书签发的通知”。

4.8.5 构成接受变更证书的行为

同第 4.4.1 节“构成接受证书的行为”。

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“电子认证服务机构对证书的发布”。

4.8.7 电子认证服务机构对其他实体的通告

同第 4.4.3 节“电子认证服务机构对其他实体的通告”。

4.9 证书撤销和挂起

4.9.1 证书撤销的情形

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他安全威胁；

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 请求证书撤销的实体

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 撤销请求的流程

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。

订户证书在 24 小时内进入 CRL 或被直接签发 CRL，向外界公布。

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，其他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限

山东 CA 从收到证书撤销请求起 24 小时内完成请求的处理。

4.9.6 依赖方检查证书撤销的要求

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 CRL 发布频率

山东CA将通过证书撤销列表在24小时内公布被撤销的证书，特殊紧急情况下可以立即签发公布。山东CA 每年发布一次电子认证服务机构的CA证书撤销列表(ARL)。

4.9.8 CRL 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 在线状态查询的可用性

山东CA向证书订户提供7×24小时在线证书状态查询服务（OCSP）。

4.9.10 撤销状态查询要求

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 撤销信息的其他发布形式

山东CA网站（https://www.sdca.com.cn）提供CRL文件下载。

4.9.12 密钥损害的特别要求

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 证书挂起的情形

证书挂起是证书撤销的一种特殊情形， 由于某种原因暂停使用证书。例如：订户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 请求证书挂起的实体

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 挂起请求的流程

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。

订户证书在24小时内进入CRL或被直接签发CRL，向外界公布。

4.9.16 挂起的期限限制

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方式的查询证书服务和获取CRL服务，符合LDAP V3标准。

4.10.2 服务可用性

山东CA至少24小时发布一次CRL。

山东CA的OCSP（在线证书状态查询）服务，对依赖方提供7×24小时服务。

4.10.3 可选特征

无。

4.11 订购结束

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 密钥生成、备份与恢复

4.12.1 密钥备份与恢复的策略与行为

证书订户的加密密钥由山东省密钥管理中心（KMC）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，由山东CA通过相应程序从KMC为其取得相应的加密密钥。

通用证书的签名私钥由订户的密码设备（如智能USB Key、智能IC卡、SIM Key等）生成，协同签名证书的签名私钥由基于密钥分割的软件密码模块生成。为保证订户签名私钥的安全性，山东CA不保管签名私钥。因此，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不负责。

4.12.2 会话密钥的封装与恢复的策略与行为

用非对称算法封装会话密钥，可以用解密密钥来解开并恢复会话密钥。

第五章 认证机构设施、管理和操作控制

5.1 物理控制

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 场地位置与建筑

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，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不间断电源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系统设备与服务正常运转。

山东CA系统使用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 水患防治

山东CA在机房设计建设时已充分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 火灾防护

山东CA在设备机房内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，并建立消防灭火等应急响应措施，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按照相关流程经审批通过后，通过粉碎、焚烧或其他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，所有处理行为将进行记录。

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山东省委机要局安全保管。以上所有操作流程将进

行记录。

5.2 程序控制

5.2.1 可信角色

在山东CA提供的电子认证服务过程中，能从本质上影响证书的颁发、使用、管理和撤销等涉及密钥操作的职位都被山东CA视为可信角色。这些角色包括但不限于：密钥和密码设备的管理员、系统管理员、安全审计人员、业务管理人员及业务操作人员等，具体岗位名称和要求以山东CA的岗位说明书为准。

5.2.2 每项任务需要的人数

山东CA确保单个角色不能接触、导出、恢复、更新、废止山东CA的电子认证系统存储的根证书对应的私钥。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。

至少两个可信角色才能使用一项对参加操作人员保密的密钥分割和合成技术来进行任何钥匙恢复的操作。

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

所有山东CA的在职人员，必须通过认证后，根据作业性质和职位权限的需要，发放门禁卡、登录密码、操作证书、作业帐号等安全令牌。对于使用安全令牌的员工，山东CA系统将独立完整地记录其所有的操作行为。

所有山东CA职位人员必须确保：

1）根据岗位安全等级的不同，进行不同程度层次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，为其发放安全令牌；

4）发放的安全令牌只直接属于个人或组织所有；

5）发放的安全令牌不允许共享。

山东CA的系统和程序通过识别不同的令牌，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。山东CA对如下人员进行了职责分割：

1）安全管理员；

2）密钥管理员；

3）证书受理员；

4）证书审核员；

5）根CA证书管理员；

6）系统维护人员；

7）秘密分割持有者。

5.3 人员控制

5.3.1 资格、经历和无过失要求

山东CA员工的录取经过严格的审查，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，核心和关键部位的员工考察期为半年，根据考察的结果安排相应的工作或者辞退。山东CA根据需要对员工进行职责、岗位、技能、政策、法律、安全等方面的培训。

山东CA会对其关键的CA职员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。

注册机构和受理点操作员的审查，可以参照山东CA对可信任员工的考察方式。受理点责任机构可以在此基础上增加考察和培训条款，但不得违背山东CA电子认证业务规则。

山东CA确立流程管理规则，所有的员工与山东CA签定保密协议，据此CA员工受到合同和章程的约束，不得泄露山东CA证书服务体系的敏感信息。

5.3.2 背景审查程序

山东CA制定了严格的员工背景审查程序，与有关的政府部门和调查机构合作，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）下列情形之一，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）虚假声称具有某种技能、能力的证件；

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）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

根据山东CA策略调整、系统更新等情况，山东CA将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，每年对员工进行一次以上的培训，对于相关业务技能培训应每年进行一次以上的业务技能培训。

5.3.5 工作岗位轮换周期和顺序

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 审计日志程序

5.4.1 记录事件的类型

山东CA的CA和RA运行系统，记录所有与系统相关的事件，以备审查。这些记录，无论是纸质或电子文档形式，都包含事件日期、事件的内容、事件的发生时间段、事件相关的实体等。

山东CA应记录的内容包括（但不限于）：

1）系统安全事件，包括： CA系统、RA系统和其他服务系统的活动，系统崩溃，硬件故障和其他异常。

2）电子认证系统操作事件，包括系统的启动和关闭。

3）认证机构设施的访问，包括授权人员进出认证机构设施、非授权人员及陪同人进入认证机构设施。

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将定期进行内部检查、审计和处理。

5.4.3 审计日志的保存期限

山东CA会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执行严格的保护和管理，确保只有山东CA授权的人员才能对审计日志进行操作。审计日志处于严格的保护状态，严禁未经授权的任何操作。

5.4.5 审计日志备份程序

山东CA保证所有的审查记录和审查总结都按照山东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 审计收集系统

山东CA审查采集系统涉及：

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）网络安全等其他有必要审查的系统。

5.4.7 对导致事件实体的通告

对于审计收集系统中记录的事件，对导致该事件的个人、机构等主体，山东CA不进行通告。

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 归档记录的类型

山东CA按照制度和流程定期对电子生成和（或者）手工生成的重要数据定期存档。存档的内容包括订户资料、电子认证系统签发的系统证书和订户证书、证书撤销列表CRL、电子认证系统维护操作记录、可信人员进出机房操作记录、外来人员进出记录、数据备份记录、涉及电子认证安全的事件记录及审计数据等。

5.5.2 归档记录的保存期限

山东CA针对归档记录将保存至订户证书失效后五年。

5.5.3 归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的

工作人员按照特定的安全方式才能获取。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 归档文件的备份程序

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 记录时间戳要求

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。系统产生的记录按照要求添加时间标识。

5.5.6 归档收集系统

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 获得和检验归档信息的程序

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每年验证存档信息的完整性。

5.6 电子认证服务机构密钥更替

在CA的密钥对遭受攻击或因为密钥生命期而需要更新密钥对的情况下，所有密钥管理员在场，共同启动密钥管理程序，执行密钥更新指令，硬件加密设备重新生成根密钥。山东CA密钥更替方式如下：

1）在CA证书生命周期结束前停止签发新的订户证书，确保在CA证书到期时所有订户证书也全部到期。

2）产生新的密钥对，签发新的CA证书。

3）使用新的CA密钥签发订户证书。

山东CA将继续使用旧的私钥签发CRL，直到旧的私钥签发的证书全部到期为止。

5.7 损害与灾难恢复

在出现异常或灾难等不可抗力情况时，为能够在最短的时间内重新恢复电子认证系统的运行，对外提供安全可靠的电子认证服务，山东CA制定了损害和灾难恢复计划，以应对突发事故导致的系统问题。

5.7.1 事故和损害处理程序

为了及时响应和处理事故和损害的发生，山东CA已制定各种应急处理方案，规定了相应的应急响应、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/或数据的损坏

山东CA对业务系统及其他重要系统的资源、软件和/或数据进行了备份，并制定了相应的应急处理流程。当出现计算资源、软件或数据的损坏时，能在最短的时间内恢复被损害的资源、软件和/或数据，保证系统重新正常运行对外提供电子认证服务。

5.7.3 实体私钥损害处理程序

对于实体私钥出现损毁、遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，山东CA有如下处理要求和程序：

1）当证书订户发现实体证书私钥损害时，订户必须立即停止使用其私钥，并立即通知山东CA或注册机构撤销其证书。山东CA按本CPS第4.9节发布证书撤销信息。

2）当山东CA或注册机构发现证书订户的实体私钥受到损害时，山东CA或注册机构将立即撤销证书，并通知证书订户，订户必须立即停止使用其私钥。山东CA按本CPS第4.9节发布证书撤销信息。

3）当山东CA的证书出现私钥损害时，山东CA将立即撤销CA 证书并及时通过有效途径通知依赖方，然后生成新的CA 密钥对、签发新的CA 证书。

5.7.4 灾难后的业务连续性能力

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

5.8 电子认证服务机构或注册机构的终止

当山东CA打算终止经营时，会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。

山东CA会按照相关法律的规定来安排好档案和证书的存档工作。

在CA终止期间，采用以下措施终止业务：

1）起草CA终止声明；

2）通知与CA停止相关的实体；

3）关闭从目录服务器；

4）证书撤销；

5）处理存档文件记录；

6）停止认证中心的服务；

7）存档主目录服务器；

8）关闭主目录服务器；

9）处理山东CA系统管理员和业务管理员；

10）处理加密密钥；

11）处理和存储敏感文档；

12）清除CA主机硬件。

根据山东CA与RA签订的协议终止RA的业务。

由于密钥受损和非密钥受损原因而终止山东CA，要完成相似的操作，唯一不同在发送山东CA终止通知的时间限制上：由于密钥受损原因终止山东CA，要求山东CA通知订户的过程尽快完成；由于非密钥受损的原因终止山东CA，在通知所有订户后，采取适当的步骤减轻山东CA终止对订户的影响。

第六章 认证系统技术安全控制

6.1 密钥对的生成和安装

由于密钥对是安全机制的关键，所以在电子认证业务规则中制定了相应的规定，通过物理安全控制和密钥安全存储控制来确保密钥对的产生、传送、安装、存储、运算等过程中符合保密性、完整性和不可否认性的需求。

6.1.1 密钥对的生成

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 加密私钥传送给订户

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 公钥传送给证书签发机构

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。

订户从KMC取得加密公私钥对的，由CA系统从KM返回的通信协议数据包中提取公钥。

6.1.4 电子认证服务机构公钥传送给依赖方

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 密钥的长度

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的要求。

6.1.6 公钥参数的生成和质量检查

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 密钥使用用途

在山东CA证书服务体系中的密钥用途和证书类型紧密相关，被分为签名和加密两大类。

1）山东CA的根密钥用于签发证书撤销列表（CRL）、订户证书、通信证书、管理员和操作员证书等；

2）管理员和操作员密钥用于CA、RA系统业务系统身份认证、操作完整性和不可抵赖性以及日志审计等操作；

3）通信密钥用于CA系统体系内各通信双方关键操作数据签名和加密；

4）订户的签名密钥用于提供网络安全服务，如信息在传输过程中不被篡改、接收方能够通过数字证书来确认发送方的身份、发送方对于自己发送的信息不能抵赖等；

5）订户加密密钥用于对需在网络上传送的信息进行加密，保证信息除发送方和接受方外不被其他人窃取、篡改。

更多与协议和应用相关的密钥使用限制请参阅X.509标准中的密钥用途扩展域。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块的标准和控制

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（m 选 n）

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的私钥，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

订户加密私钥由山东省密钥管理中心生成并负责存储、备份以及在发生法律纠纷时提供司法取证的依据。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

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

山东省密钥管理中心提供过期的托管私钥的存档服务；保存期为五年。当私钥过了保存期，将依据相关规定对其进行销毁。

6.2.6 私钥导入、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 私钥在密码模块的存储

山东CA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签发的订户加密证书私钥，在其生命周期结束后，KMC对该密钥进行归档妥善保存一定期限，以便于解开加密信息。对于山东CA签发的订户签名私钥，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 密码模块的评估

山东CA使用国家密码主管部门批准和许可的密码产品。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

对于生命周期外的CA和订户证书，山东CA将进行归档。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

存放有山东CA根密钥的加密卡的激活信息（秘密分割），其产生按山东CA密钥生成规程参考指南中的规定进行。所有秘密分割的创建和分发有相应的记录，包括产生时间、持有人等信息。

山东CA根私钥的激活数据由硬件加密卡内部产生，并分割保存在5个智能卡中，需通过专门的读卡设备和软件读取。

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）由订户产生；

2）至少6位字符或数字；

3）不能包含很多相同的字符；

4）不能和操作员的名字相同；

5）不能使用生日、电话等数字；

6）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

保存有山东CA根私钥的激活数据的5个智能卡，由山东CA 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 激活数据的其他方面

1）激活数据的传送

存有山东CA根私钥的激活数据的智能卡，通常保存在山东CA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，其传送过程需在山东CA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，订户应保护它们在传送过程中免于丢失、偷窃、修改、非授权泄露、或非授权使用。

2）激活数据的销毁

存有山东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在山东CA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 特别的计算机安全技术要求

山东CA的电子认证系统的数据文件和设备由山东CA系统管理员维护，未经授权，其他人员不能操作和控制系统；其他普通用户无系统账号和密码。系统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，系统管理员定期更改系统密码。

6.5.2 计算机安全评估

山东CA的电子认证系统已通过国家密码管理局组织的安全性审查。

6.6 生命周期技术控制

6.6.1 系统开发控制

山东CA的系统由符合国家相关安全标准和具有商用密码产品生产资质的可靠开发商开发，其开发过程符合国家密码主管部门的相关要求。

6.6.2 安全管理控制

山东CA的配置以及任何修改和升级都会记录并进行控制，并且山东CA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。

电子认证系统只开放与业务相关的功能，只有山东CA授权的员工能够进入山东CA的系统或设备。

6.6.3 生命周期的安全控制

山东CA的电子认证系统在系统设计过程中进行了安全性论证，在开发过程中有严格的流程进行代码安全管理，在开发完成后进行了严格的安全测试，在正式使用前通过了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网络中有防火墙、入侵检测、漏洞扫描和网络防病毒等安全机制保护，其配置只允许已授权的机器和账号访问。只有经过授权的山东CA员工才能够进入山东CA设备或系统。

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。

第七章 证书、证书撤销列表和在线证书状态协议

7.1 证书

山东CA签发的证书均符合X.509 V3证书格式，遵循RFC5280标准。

7.1.1 版本号

X.509 V3

7.1.2 证书标准项及扩展项

证书标准项：

1）证书版本号（Version）

指明X.509证书的格式版本，值为V3。

2）证书序列号（SerialNumber）

山东CA分配给证书的唯一的数字标识符。

3）证书签名标识符（Signature）

符合国家密码主管部门批准的算法对象标识符。

4）签发机构名（Issuer）

用来标识签发证书的CA的 DN名字。

5）证书有效期（Validity）

指证书的起止时间。

6）主题（Subject）

指为证书订户申请证书时所填写的申请信息。即订户的甄别名。

详细请参看第3.1节。

7）公钥（subjectPublicKeyInfo）

证书持有者公开密钥信息域包含两个重要信息：证书持有者的公开密钥的值；公开密钥使用的算法标识符。

证书扩展项：

1）颁发机构密钥标识符

颁发机构密钥标识符与验证签名的公开密钥相联系。山东CA根证书公钥

与此标识符相联系。

2）主题密钥标识符

通过主题密钥标识符识别相对应证书的公钥。

3）密钥用法

指定各种密钥的用法：电子签名、不可抵赖、密钥加密、数据加密、密钥协议、验证证书签名、验证CRL签名、只加密、只解密、只签名。

4）增强型密钥用法

指明公钥的多种用途，对密钥用法中指明的基本用途的补充或替代，如：服务器验证、客户端验证、代码签名、安全电子邮件、时间戳、智能卡登录。

5）主题替换名称

主题替换名称允许把附加身份加到证书的主体上，包括DNS名称、IP地址、因特网电子邮件地址等。

6）基本限制

用于鉴别证书持有者身份，如最终订户等。

7）CRL发布点

由山东CA定义的CRL发布点。

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。

统一社会信用代码：用于标识组织的证件号码。

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 名称形式

山东CA签发证书的甄别名符合 X.500 关于甄别名的规定。详情参见第3.1节内容。

7.1.5 名称限制

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

没有定义。

7.1.7 策略限制扩展项的用法

没有使用。

7.1.8 策略限定符的语法和语义

没有规定。

7.1.9 关键证书策略扩展项的处理规则

与X.509和PKI相关规定一致。

7.2 证书撤销列表

山东CA定期签发证书撤销列表（CRL），其所签发的CRL遵循RFC5280标准。

7.2.1 版本号

采用X.509 V2格式。

7.2.2 CRL 和 CRL 条目扩展项

与X.509和PKI规定一致。

1）版本号：用来指定CRL的版本信息。

2）签名算法：山东CA采用符合国家密码主管部门批准的算法。

3）颁发者：指定签发机构的DN名。

4）生效时间：指定一个日期/时间值，用以表明本CRL发布的时间。

5）下次更新时间：指定一个日期/时间值，用以表明下一次CRL将要发布的时间。

6）撤销证书列表：指定已经撤销或挂起的证书列表。本列表中含有证书的序列号和证书被撤销的日期和时间。

7）颁发机构密钥标识符：本项标识用来验证在CRL上签名的公开密钥。

8）扩展

7.3 在线证书状态协议

RFC2560中定义了在线证书状态协议（Online Certificate Status Protocol, OCSP），它克服了基于CRL的撤销方案的局限性，并且为证书状态查询提供即时的最新响应。

7.3.1 版本号

OCSP：V1。

7.3.2 OCSP 扩展项

与RFC2560一致。

第八章 认证机构审计和其他评估

8.1 评估的频率或情形

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，检验其是否符合本CPS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 评估者的资质

山东CA无条件接受国家主管部门的评估，评估者所具有的资质由主管部门决定。

对山东CA实施规范审计的第三方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进行审计的第三方，必须是一个独立于山东CA的合法审计实体。

山东CA内部审计员不能与系统管理员、业务管理员、业务操作员等岗位重叠。

8.4 评估内容

审计工作包括：

1）安全策略是否得到充分实施；

2）运营工作流程和制度是否严格遵守；

3）电子认证业务规范是否符合证书策略的要求；

4）是否严格按照本CPS、业务规范和安全要求开展业务；

5）各种日志、记录是否完整，是否存在问题；

6）是否其他可能存在的安全风险；

7）山东CA支持的证书认证操作规程是否完全与本CPS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；

8）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；

9）审计者或山东CA认为有必要审计的其他方面。

8.5 对问题与不足采取的措施

如果在审计过程中发现执行有不足之处，将会提交到安全管理委员会，责任职能部门进行业务改进和完善，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一般不公开审计结果。在必要的情况下，山东CA可依照与关联单位（例如垫付商、注册机构、受理点）签订的协议中有关规定，向关联单位通知审计结果。

第九章 法律责任和其他业务条款

9.1 费用

证书相关费用在实际应用证书的网站上公布，山东CA也可以通过柜台等其他方式告知订户相关费用。山东CA根据市场情况和提供的电子认证服务内容确定收费标准,并向订户收取费用。

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 证书撤销或状态信息的查询费用

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 退款策略

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保证具有维持、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，并依据本CPS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有专门的信息保密策略，保护自身和订户的敏感信息、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 不属于保密的信息

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具备严格的管理制度、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 个人隐私保密

9.4.1 隐私保密方案

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 作为隐私处理的信息

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 其他信息披露情形

对其他信息的披露受制于法律、订户协议。

9.5 知识产权

山东CA保留对本CPS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CPS。

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

除非山东CA作出特别约定，若本CPS的规定与其他山东CA制定的相关规定、指导方针相互抵触，订户必须接受本CPS的约束。在山东CA与包括订户在内的其他方签订的仅约束签约双方的协议中，对协议中未约定的内容，视为双方均同意按本CPS的规定执行；对协议中有不同于本CPS内容的约定，按双方协议中约定的内容执行。

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。

针对上述内容补充解释如下：

1）除上述所规定的职责条款，山东CA、山东CA授权的注册机构、山东CA的员工不承担其他任何义务。必须指出，本CPS的内容，没有任何信息可以暗示或解释成山东CA必须承担其他的义务或山东CA必须对其行为作出其他的承诺。

2）在上述内容中所罗列不可抗力的任何情况下，山东CA由于受到影响，可免除本节所述的责任和相应的证书策略规定的责任和义务。

3）由于技术的进步与发展，为保证证书的安全性，山东CA会要求证书持有者及时更换证书以保证山东CA能更好地履行本节所述之责任。

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，并在本CPS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。

注册机构必须遵守和符合本CPS的条款。具体内容详见本文档9.6.1。

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）订户需熟悉本CPS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

依赖方确认，在任何信赖行为发生之前，阅读了本CPS，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CPS的所有规定。

9.7 担保免责

有下列情形之一的，应当免除山东CA之责任：

1）订户在申请和使用山东CA数字证书时，有违反如下义务之一的：

a）订户应当提供真实、完整、准确的材料和信息，不得提供虚假、无效的材料和信息；

b）订户应当妥善保管山东CA所签发的数字证书载体和保护PIN码，不得泄漏PIN码或将数字证书载体随意交付他人；

c）订户在应用自己的密钥或使用数字证书时，应当使用可依赖的、安全的系统；

d）订户知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告

知山东CA及相关各方，并终止使用该电子签名制作数据；

e）订户在使用数字证书时必须遵守国家的法律、法规和行政规章制度，不得将数字证书在山东CA规定使用范围之外的其他任何用途使用；

f）订户必须在证书有效安全期内使用该证书，不得使用已失密或可能失密、已过有效期、被挂起、被撤销的数字证书；

g）订户应当根据规定按时向山东CA及当地业务受理点缴纳服务费用。

2）由于不可抗力原因而导致数字证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的；本项所规定之“不可抗力”，是指不能预见、不能避免并不能克服的客观情况，包括（但不限于）：

a）自然灾害，包括地震、火山爆发、滑坡、泥石流、雪崩、洪水、台风等；

b）社会异常或者政府行为，包括政府颁发新的政策、法律和行政法规，或战争、罢工、骚乱等社会异常事件。

3）山东CA已遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的。

9.8 有限责任

在与订户和依赖方签定的协议中，对于因订户或依赖方的原因造成的损害不具有赔偿义务。

9.9 赔偿

CA机构按照本CPS承担赔偿责任。证书订户和依赖方在使用或信赖证书时，若有任何行为或疏漏而导致CA机构和注册机构产生损失，订户和依赖方应承担赔偿责任。

订户接受证书就表示同意在以下情况下承担赔偿责任。

1）未向CA机构提供真实、完整和准确的信息，而导致CA机构或有关各方损失。

2）未能保护订户的私钥，或者没有使用必要的防护措施来防止订户的私钥遗失、泄密、被修改或被未经授权的人使用时。

3）在知悉证书密钥已经失密或者可能失密时，未及时告知CA机构，并未终止使用该证书，而导致CA机构或有关各方损失。

4）订户如果向依赖方传递信息时表述有误，而依赖方用证书验证了一个或多个电子签名后理所当然地相信这些表述，订户必须对这种行为的后果负责。

5）证书的非法使用，即违反CA机构对证书使用的规定，造成了CA机构或有关各方的利益受到损失。

山东CA承担赔偿责任（法定或约定免责除外）的赔偿限制如下：

山东CA对任何证书订户、依赖方等实体有关证书赔偿的合计责任限制在不超出下述数量的范围内：

证书类型	赔偿金额上限（人民币）
自然人证书	800 元
机构（企业）证书	4000 元
设备证书	8000 元

这种赔偿上限可以由山东CA根据情况重新制定，并通知相关当事人。

9.10 有效期限与终止

9.10.1 有效期限

本CPS自发布之日起生效。

9.10.2 终止

当新版本的CPS生效时或山东CA终止业务时，旧版本CPS自动终止；当山东CA中止业务时，山东CA CPS自动终止。

9.10.3 效力的终止与保留

本CPS终止后，已签发符合本CPS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，将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 修订程序

CPS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CPS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，审批通过后正式发布生效。

9.12.2 通知机制和期限

本CPS在山东CA的网站（https://www.sdca.com.cn）上发布。

版本更新时，最新版本的CPS在山东CA的网站发布，对具体个人不做另行通知。

9.12.3 必须修改业务规则的情形

当本CPS 描述的规则、流程和相关技术已经不能满足山东CA电子认证业务要求或当管辖法律、适用标准及操作规范等有重大改变时，山东CA将依照有关规定修改本CPS的相关内容。

9.13 争议处理

订户、依赖方等关联实体在电子认证活动中产生争端可按照以下步骤解决：

1）当事人首先通知，根据本CPS中的规定，明确责任方；

2）由相关部门负责与当事人协调；

3）若协调失败，可以通过司法途径解决；

4)任何因与山东CA或其授权的注册机构和合作方就本CPS所产生的任何争议而提起诉讼的，受山东CA工商注册所在地的人民法院管辖。

9.14 管辖法律

本CPS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、规则、规章、法令和政令的约束和解释。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CPS的使用必须遵从中华人民共和国的相关法律和法规。

9.16 一般条款

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信任域参与者之间的完整协议。

9.16.2 转让

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

在山东CA、注册机构、订户和依赖方之间出现纠纷、诉讼时，胜讼可以要求对方支付有关诉讼费作为对其补偿的一部分。免除一方对某次合同违约的赔偿，不意味着免除对其他合同违约的赔偿。

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。

9.17 其他条款

山东CA对本CPS具有最终解释权。