山东 CA CPS

电子认证业务规则

版本 3.0

生效日期： 2011 年 1 月 1 日

SDCA CPS

Certification Practice Statement

Version 3.0

Effective Date：Jan 1, 2011

山东省数字证书认证管理有限公司
Shandong Certification 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，山东数字证书认证管理有限公司将保留依法追诉的权利。

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（Shandong Certification Authority Co.,Ltd），是山东省数字证书认证中心的企业化运作实体，简称山东 CA。山东 CA 于 2001 年 2 月 14 日注册成立，在 2003 年通过了国家密码管理局的建设论证和安全性审查，在 2004 年 7 月 14 日通过了国家密码管理局组织的技术鉴定，成为全国首批通过国家技术鉴定的数字证书认证中心，在 2005 年 6 月 17 日通过了国家信息产业部的电子认证服务机构现场资质审查，成为全国第一家获得《电子认证服务许可证》的电子认证服务机构之一。

本着“志存高远 科技为先 诚信规范 合作发展”的运营宗旨，山东 CA 致力于为电子政务、电子商务及社会信息化等应用提供优质的电子认证服务。

1.1.2 电子认证业务规则

本电子认证业务规则（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 以及分支机构，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

山东 CA 标识

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

山东 CA 所拥有的品牌的商标为：

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《山东 CA 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 版本

本规则为山东 CA 发布的第三个版本，即《山东 CA 电子认证业务规则》V3.0，是在《山东 CA 电子认证业务规则》V2.1 的基础上根据山东 CA CP 和公司运营现状修改整理形成的。

1.2.3 发布

本电子认证业务规则文档的发布有以下三种形式：

1）以电子的方式，在山东 CA 网站发布。网站地址：

http://www.sdca.com.cn

2）以电子的方式，通过电子邮件发布。电子邮箱地址：

webmaster@sdca.com.cn

3）以文件形式，从以下地址索取：

邮编：250011

地址：山东省济南市趵突泉北路 24 号

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。

山东 CA 的认证系统是所有山东 CA 下层机构和实体的根。在十分严密的保密和安全机制控制下，山东 CA 根据根证书有效的安全策略，自己生成密钥对，自己签发根证书。山东 CA 根据授权和协议，签发下一级的证书，这些下级也必须遵守本证书策略的要求。山东 CA 的认证系统所签发的证书，与每一个证书申领实体的公钥绑定。

1.3.2 注册机构（Registration Authority）

注册机构作为电子认证服务机构授权的下属机构，负责证书订户信息的审核、整理汇总、统计分析，与上级 CA 进行数据交换，管理和服务下层注册分支机构和下层受理点。每个注册机构可以按照行业或行政地域分成多个注册分支机构，或直接连接受理点，可以直接对最终订户提供服务。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。

注册机构可以由山东 CA 自建或授权的第三方机构建立。当注册机构由第三方机构建立时，山东 CA 必须与其签订协议，明确双方的权利和义务。

1.3.3 注册分支机构（Registration Authority Branch）

注册分支机构与注册机构功能类似。当注册机构服务的群体超过一定程度时，在注册机构下面设注册分支机构。注册分支机构的上级是注册机构，下级是受理点。注册分支机构由山东 CA 授权建立或撤消。注册分支机构是可选项，即根据客户数量决定是否设立。

1.3.4 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 授权的注册机构或山东 CA 授权的注册分支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。

1.3.5 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。

1.3.6 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。

1.3.7 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。

1.3.8 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

数字证书可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。

山东 CA 数字证书已经广泛的在电子政务社会管理和公共服务、电子交易、电子办公、电子公证、公共服务等领域应用，为建设互联网络的信任环境开展了基础性的服务。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。

此类证书通常用于数字签名、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。此类证书通常用于数字签名、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，此类证书通常用于网上设备的身份认证，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。

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

管理本文档的机构是：山东 CA 安全中心。

1.5.2 联系人

山东 CA 将对电子认证业务规则进行严格的版本控制，并由山东 CA 指定专人负责。

联系人：安全中心

电　话：86-0531-86019278，传真：86-0531-86019278

地　址：山东省济南市趵突泉北路 24 号（250011）

电子邮件：webmaster@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

按照信息产业部公布的《电子认证业务规则规范》的要求，在山东 CA 电子认证业务规则做出任何变动之前，山东 CA 安全中心将对提供的变动建议进行研究，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。山东 CA 根据《电子认证服务管理办法》中规定，在本机构网站予以公布，并在公布之日前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做规范的描述，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：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（Directory Server）公布证书相关信息，并以定期和实时的方式公布证书撤销列表 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（http://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 在网站或以书面声明形式发布、更改，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。

本规则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 网站查看本电子认证业务规则，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 http://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。

电子认证业务规则的变更，必须在被认定后三十日内发布。

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（http://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 的目录服务器实施更新目录，通常在 24 小时内发布最新 CRL。证书订户可在山东 CA 网站（http://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

对于以网站方式公布的信息，山东 CA 允许任何公众进行查询和访问。证书和 CRL 除公司网站外，还可通过 LDAP 方式发布，同时提供 OCSP 在线验证方式。但只有山东 CA 有权对公布的各类旧信息进行处理。

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 CPS、证书、CRL 等电子认证信息库只有经过授权的山东 CA 工作人员才能登陆、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 颁发的数字证书，根据证书对应实体的类型不同，其实体名字可以是人员姓名、组织机构名称、部门名、域名等，证书包含订户和颁发机构主题甄别名，对证书申请者的身份和其他属性进行鉴别，并以不同的标识记录其信息。证书持有者的标识命名，以甄别名（Distinguished Name）形式包含在证书主体内，是证书持有者的唯一识别名。

山东CA的证书符合X.509标准，分配给证书持有者实体的甄别名，采用X.500标准命名方式，格式如下：

属性	值	举例
Country（C） =	国家	CN
Organization（O） =	组织	山东 CA
Organizational Unit （OU） =	组织机构	运行部
State or Province （S） =	省	山东省
Locality （L） =	市	济南市
Common Name （CN） =	通用名	张三
Email=	邮件地址	san.zhang@sdca.com.cn

山东 CA 的证书包含颁发者的甄别名称，格式如下：

属性	值	举例
Country（C） =	国家	CN
Common Name （CN） =	通用名	SDCA Root Authority

3.1.2 对名称意义化的要求

山东 CA 签发的个人实体证书、组织机构通用数字证书、服务器证书等包含的命名应具有通常理解的语义，用它可以确定证书主题中的个人、机构或设备的身份。对于具有特殊要求的应用中，山东 CA 可以按照一定的规则为订户指定特殊的名称，并且能够把该类特殊的名称与一个确定的实体（个人、单位或设备）唯一联系起来。

3.1.3 订户的匿名或假名

订户在证书中的名称可以是假名，但不能使用匿名，并在山东 CA 的数据库中记录订户的相关信息。

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

山东 CA 证明拥有私钥的方法是根据证书申请信息进行验证。首先利用数据摘要算法进行计算，再用申请信息中的公钥对申请信息中的签名解密，然后进行比较，如果相等则证明数字证书的申请者拥有与签名验证公钥对应的签名私钥。

3.2.2 组织机构身份的鉴别

组织机构申请者填写书面申请表（一式二份），经过单位授权代表的签署及单位盖章，表示接受书申请的有关条款，并承担相应的责任。山东 CA 授权的发证机构必须对订户进行以下资料的鉴别：

1）申请机构的组织机构代码证的复印件；

2）申请机构的营业执照副本及复印件，如果没有营业执照，则提供书面申请

表上可选的其他有效证件的副本及复印件。部分有效证件如下：

- 营业执照
- 企业法人营业执照
- 事业单位法人登记证
- 税务登记证
- 社会团体法人登记证
- 政府批文
- 其他有效证件

3）经办人身份证原件与复印件。

山东 CA 授权的发证机构的审核人员合理、审慎地核对申请资料的原件与复印件，并通过电话、邮政信函等方式确认该机构资料信息的真实性，以及代表机构进行证书申请的个人是否得到足够的授权。

3.2.3 个人身份的鉴别

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。

个人申请者填写书面申请表（一式二份），签字确认，表示接受证书申请的有关条款，并承担相应的责任。

3.2.4 没有验证的订户信息

在初始身份认证中，不作验证的订户信息列表如下：

个人订户信息	机构订户信息	设备信息
● 电话/移动电话 ● 地址/邮政编码 ● 传真	● 单位英文或拼音 ● 地址/邮政编码 ● 电话/移动电话 ● 联系人、传真	● 不作验证的个人或机构订户信息 ● 设备类型 ● MAC 地址

3.2.5 授权确认

山东 CA 签发证书前，将确认证书申请必须获得授权。山东 CA 通过可信第三方获得申请者所在组织机构电话号码，然后联系组织机构的有关人员，确认申请者获得了所在组织机构的授权。

3.2.6 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 授权的发证机构的审核人员合理、审慎地核对申请资料的原件与复印件，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。

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 授权的发证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。如果由于条件的限制无法进行现场审核时，山东 CA 可以通过电话、传真、邮政信函或其他第三方证明等合理方式对申请者的身份予以鉴别验证。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 授权的发证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

山东 CA 目前只接受离线申请方式，申请程序根据山东 CA 证书的种类不同而不同，但都应遵守证书操作所规定的步骤。

证书申请流程如下：

- 对于个人证书（包括个人身份证书，个人安全电子邮件证书，个人代码签名证书），申请者到山东 CA 授权的发证机构领取证书申请表（一式二份）或到山东 CA 网站下载相应的申请表（一式二份），并提供个人身份证明文件及其复印件一份，例如：身份证、军官证、学生证、护照等。详细内容请见第 3.2 节。
- 对于单位证书（包括单位身份证书，单位安全电子邮件证书，单位代码签名证书），申请者到山东 CA 授权的发证机构领取单位证书申请表（一式二份）或到山东 CA 网站下载相应的申请表（一式二份），申请者应提供单位对经办人的授权委托书，单位的营业执照、税务登记证、组织机构代码证、经办人的身份证和山东 CA 可能需要的其他文件。详细内容

请见第 3.2 节。

- 对于服务器证书，与单位的申请相同，还需要提供服务器域名的所有权的证明，详细内容请见第 3.2 节。
- 对于软件代码，提供合法拥有该软件的证明或授权文件，软件拥有者的身份证明。
- 对于支付网关证书，与单位的申请相同，还需要提供与支付网关相关的证明。详细内容请见第 3.2 节。
- 对于其他类型证书，山东 CA 网站上发布申请要求，并且山东 CA 拥有解释权。
- 对于山东 CA 测试证书、内部通讯证书、管理员证书、操作员证书或注册机构、注册分支机构的通讯证书、管理员证书，要填写山东 CA 内部证书申请表；对于注册机构、注册分支机构下的所有证书申请表，需一式二份。

订户的申请表和相关证明文件的复印件存档 7 年。

山东 CA 作为电子认证服务的发证机构有责任对申请人的身份进行充分的验证。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。详细内容请见第 3.2 节。

申请者必须真实填写证书申请信息，并遵守《山东 CA 数字证书用户责任书》。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。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

山东 CA 授权的发证机构遵循第 3 章对证书申请者提交的信息进行识别，并由双人复合鉴别验证。

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 授权的发证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 授权的发证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 授权的发证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 授权的发证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 授权的发证机构必须在 1 个工作日内对证书申请者提交的证书信息进行识别，并完成证书申请处理。

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发证机构签发其证书。

山东 CA 授权的发证机构批准证书申请后（参见第 4.2 节），接收参考码、授权码，为证书申请者制作证书，并提供给订户。

证书的发行意味着山东 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 直接通知订户或发证机构证书已签发，并将证书提供给申请者。

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。

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，发证机构将在目录服务器及由山东 CA 和其授权发证机构决定的其它合理的方式来发布证书。

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。

证书应用范围：

编号	订户	证书类型	订户私钥与证书的用途
1	个人	个人身份证书	订户使用此证书来向对方表明个人的身份，同时应用系统也可以通过证书获得订户的其他身份信息。 主要用于：文档签名、个人网上购物、网上炒股等。
2		个人安全邮件证书	个人Email证书使订户个人可以在重要的邮件通信中对信件内容进行加密和签名操作。
3	单位	单位身份证书	颁发给独立的单位、组织，在互联网上证明该单位、组织的身份。 主要用于：文档签名、网上工商事务、网上招标投标、网上签约、安全网上公文传送、网上缴费、网上缴税、网上购物和网上报关等。

4		单位安全邮件证书	单位Email证书使单位订户可以在重要的邮件通信中对信件内容进行加密和签名操作。
编号	**订户**	**证书类型**	**订户私钥与证书的用途**
5	代码签名	个人代码签名证书	为软件开发者提供对软件代码做电子签名的技术，可以有效防止软件代码被篡改，使软件用户免遭病毒与黑客程序的侵扰，同时可以保护软件开发者的版权利益。
6		单位代码签名证书	单位代码签名证书颁发给具有企业行为的软件开发商或提供商，通过对其提供的软件代码进行电子签名，可以有效防止该软件代码被篡改，并且能够保护软件开发商的版权利益。当用户在网上下载经过代码签名的软件时，将会得到提示，从而确认： 1．软件的来源真实、可靠。 2．软件从签名到下载前，未遭到修改或破坏。
7	服务器	WEB 服务器证书	Web服务器证书通过在客户端浏览器和Web服务器之间建立起一条SSL安全通道，来保证用户在网络通讯中的安全性。它可以和网站的IP地址、域名绑定，目前支持多种主流的Web Server，包括：IIS、Lotus Domino、Weblogic、Apache、iPlant、NetScape等。 主要用于：实现安全站点、配合个人证书、单位证书、单位员工证书等客户端的证书实现安全购物站点、安全电子业务综合服务平台、安全公文报送系
8		服务器身份证书	主要颁发给需要安全鉴别的服务器，以便于标识证书持有服务器的身份。应用服务器证书中包含服务器信息和服务器的公钥，其和对应的私钥可以存放在服务器硬盘或加密硬件设备上。
9	VPN	网关证书	通过配置VPN（虚拟专用网），企业的远程雇员、分支机构、合作伙伴以及客户就可以在互联网上透明、安全的连接到公司网络。VPN网关证书即是作为一种在VPN隧道中鉴别设备身份的强有力方式。
10		客户端证书	VPN客户端证书主要用于认证远程雇员、商务合作伙伴和客户身份，以确保在VPN网络中只有指定人员才能有权访问传递的信息。

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

为保证证书及其密钥对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一个月内，到山东 CA 授权的发证机构申请更新证书。

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 授权的发证机构通过 PIN 码验证和身份信息核查，进行更新请求；或在山东 CA 授权的发证机构书面填写《山东 CA 数字证书申请表》。山东 CA 授权的发证机构按照第 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。发证机构审核通过后，为订户制作证书；证书签发后，发证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：

- 证书的密钥泄露。对此，订户负有立即告知山东 CA 的责任；
- 证书到期时，要求更换证书密钥；
- 证书丢失；
- 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：

- 证书订户甄别名更改；
- 证书订户 Email 更改；
- 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：

- 新的密钥对替代旧的密钥对；
- 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；
- 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；
- 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）；
- 证书到期：到期后订户未续约；
- 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；
- 订户申请初始注册时，提供不真实材料；
- 证书已被盗用、未经授权的泄漏和其它安全威胁；
- 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；
- 订户自动提出撤销请求；
- 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

订户到山东 CA 授权的发证机构书面填写《山东 CA 数字证书申请表》，并注明撤销的原因。山东 CA 授权的发证机构按照第 3 章识别与鉴定的规定对订户提交的证书撤销申请进行审核。山东 CA 撤销订户证书后，发证机构将当面通知订户证书被撤销。

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 授权的发证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。

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（http://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

申请者到山东CA授权的发证机构书面填写《山东CA数字证书申请表》，并注明挂起的原因。山东CA授权的发证机构按照第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授权的发证机构。

山东CA挂起订户证书后，发证机构将当面通知或通过发送E-mail邮件或邮寄等方式通知订户证书被挂起。

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授权的发证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，在需要恢复时到山东CA授权的发证机构书面填写《山东CA数字证书申请表》，并注明恢复的原因。山东CA授权的发证机构按照第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，为用户恢复证书，并通知用户证书已恢复。

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LDAPv3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：

- 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。

- 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。加密密钥被加密存放在KMC管理中心。

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：

- 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。

- 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安全区、CA操作区、CA DMZ区，CA安全区屏蔽机房与外界区域利用通顶隔墙进行保护，防止通过天花板下面的假平顶进入。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。

CA其他区域采用通顶隔墙进行隔离，便于维护管理。

CA出入门由门禁出入卡系统进行控制，并在安全区采用指纹识别与智能卡结合的方式实施。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：

包括消防间、UPS配电间、监控室、机房中心通道、办公区域、制证中心等。

消防间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，并且由门禁出入系统进行管理。

UPS配电间、监控室采用实墙隔断，监控室在办公区一侧开窗口。需要通过

门禁出入卡系统才能进入房间。

5.1.2 物理访问

山东CA的核心机房和各功能区域的访问控制系统是与控制各区域进出的门禁系统相结合的，并实现了以下安全功能：

- 进出每一区域的门都有记录作为审计依据；
- 核心机房的安全区域采用身份鉴别卡和指纹验证的结合方式控制，其他区域采用双人、同时身份鉴别卡控制每道门的进出；
- 其他功能区域只采用身份鉴别卡控制门的进出；
- 授权人员进出每一道门都会有时间记录；
- 只有相关授权人员使用授权口令才可以登录访问物理设备；
- 根据操作性质及安全性的不同，物理设备设置多种权限级别账户（组）对人员进行访问控制，确保物理设备系统安全性；
- 涉及物理设备密码及重大系统操作的，必须两人以上同时在场才可操作；
- 高安全级别的重要系统设备的操作与维修，必须在机房内多人现场监控下现场完成且有相关记录。

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，并通过与专业消防部门协调，实施消防灭火等应急响应措施，避免

火灾的威胁，防止明火或者烟雾对系统造成损害或不利影响，充分保障系统安全。

5.1.6 介质存储

山东CA对存储有系统程序、订户数据、维护记录、审计记录、日志文件、备份数据等信息的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数据和记录销毁流程经安全中心审批通过后，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备份。在异地备份时按照策略和流程由专人送交到山东省机要局安全保管。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

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。

山东CA明确执行CA系统的关键职能职位，他们包括：

- **山东CA安全中心**

  享有以下权限：

  1）提出山东CA安全管理策略方面的建议；

  2）负责安全措施的制定和定期进行安全审计；

  3）定期对CA中心安全问题进行讨论，并对安全问题提供相应的解决方

案；

4）及时对系统的安全问题做出响应，减少因处理不及时所造成的损失；

5）发布并维护山东CA中心电子认证业务规则；

6）保障山东CA电子认证业务规则的政策能够通过技术解决方式得到实施；

7）保障山东CA认证系统的运营同电子认证业务规则保持一致；

8)任命山东CA认证系统的超级管理员；

- **山东CA超级管理员**

享有以下权限：

1）负责输入启动各个服务（CA、RA-SERVER）的超级管理员口令；

2）监督系统管理员维护各个模块的服务；

3）签发系统管理员；

4）如果系统管理员忘记口令，可重新签发一个系统管理员；

5）授权数据库管理员备份数据、重新加密以及在必要的时候对山东CA的数据库进行恢复。

- **山东CA系统管理员**

享有以下权限：

1）建立和变更山东CA系统的安全策略；

2）增加和减免其他管理员，及山东CA订户；

3）对于敏感操作的授权，诸如增加和减免业务管理员等；

4）管理交叉认证，发布山东CA交叉认证协议，更新及撤销交叉认证；

5）处理系统审计日志；

6）享有山东CA所有管理员的权限；

7）管理CRL、证书模板的制定。

- **山东CA录入员（SOO：System Operation Operator）**

1）负责订户证书申请信息的录入；

2）协助客户办理数字证书申请、作废、更新等手续。

- **山东CA审核员（RAO：Registry Approval Operator）**

1）负责数字证书的审批受理；

2）如实向上级机构传送证书申请者的信息；

3）协助客户办理数字证书申请、作废、更新等手续。

- **山东CA审计员（auditor）**

  1）负责CA、RA数字证书的统计、审计；

  2）负责CA、RA日志的备份、恢复。

- **山东CA制证员（CertMaker）**

  1）证书的制作、发放；

  2）协助客户办理数字证书申请、作废、更新等手续。

- **其他管理员**

  包含：

  - 网络管理员；
  - 数据库管理员；
  - 加密机管理员；
  - 目录服务管理员；
  - 证书发布系统管理员。

安排上述职位是为了确保责任明确，建立有效的安全机制，保证内部管理和操作的安全。

山东CA根据受理点的章程，规范受理点操作人员的操作。在受理点的软件设计中，充分考虑安全因素。山东CA对受理点的责任进行合理划分，并在系统、技术实现以及管理上允予体现。

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CA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，发放系统操作卡、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：

- 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；
- 基本的身份审查措施，确保符合岗位可信资格；
- 赋予可信员工相应的权限区分，为其发放安全令牌；
- 发放的安全令牌只直接属于个人或组织所有；
- 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：

- 安全管理员；
- 密钥管理员；
- 证书申请录入员；
- 证书申请审核员；
- 证书制证员；
- 根CA证书管理员；
- 系统维护人员；
- 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、注册分支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：

- 山东CA安全原则和机制；
- 山东CA使用的软件介绍；
- 山东CA操作的系统和网络；
- 岗位职责；
- 山东CA政策、标准和程序；
- 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员工进行了未授权或越权操作，山东CA在确认后将立即中止该员工进入山东CA证书服务体系，根据情节严重程度实施包括提交司法机关处理等措施。

一旦发现上述情况，山东CA立即作废或终止该人员的安全令牌。

5.3.7 独立合约人的要求

山东CA的独立合约人及顾问执行与普通员工一致的可信资格确认，此外独立合约人及顾问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

在培训或再培训期间，山东CA提供给员工的培训文档包括（但不限于）以下几类：

1)员工手册；

2)电子认证业务规则；

3)岗位说明书；

4)安全管理制度等。

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）电子认证服务系统操作事件，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、非授权人员进入认证机构设施及陪同人和安全存储设施的访问。

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，山东CA将一个季度进行一次内部检查、审计。

对系统安全事件和系统操作事件日志，山东CA将每月进行一次检查、处理。

对物理设施的访问日志，山东CA将每月进行一次检查、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，本地保存期限至少两个月，离线存档为七年。

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授权的人员才能访问这些审查记录。并且实现异地备份，并禁止访问、阅读、修改和删除等操作。

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：

- 证书签发系统；
- 证书注册系统；
- 证书目录系统；
- 证书审批受理系统；

- 访问控制系统（包括防火墙）；
- 专网办公系统；
- 客户服务系统；
- 网站、数据库安全保障系统；
- 其他山东CA认为有必要审查的系统。

5.4.7 对导致事件实体的通告

山东CA将依据法律、法规的监管要求，对一些恶意行为，如网络攻击等，通知相关的主管部门，并且山东CA保留进一步追究责任的权利。

5.4.8 脆弱性评估

根据审计记录，山东CA定期进行系统、物理场地、运营管理、人事管理等方面的安全脆弱性评估，并根据评估报告采取措施。

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归档存档期限一般规定为七年。订户资料保存期限为订户证书过期后七年。

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。

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，由安全中心授权，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。密钥更换及自签名证书按照规定报告上级管理机构。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

山东CA已制定各种应急处理方案，规定了相应的事故和损害处理程序，应急处理方案包括：

- 认证系统应急方案；
- 电力系统应急方案；
- 消防应急方案；
- 网络与信息系统应急方案；
- 安全事故应急处理方案等。

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。当出现计算机资源、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。

5.7.3 实体私钥损害处理程序

对于实体私钥的损害，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CPS §4.9 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CPS §4.9 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 证书并及时通过广达的途径通知依赖方，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

除非物理场地出现了毁灭性的、无法恢复的灾难，山东CA能够在出现灾难后最短时间内恢复其业务能力。山东CA目前正计划建立省际异地灾难恢复中心，灾难恢复中心的建立，将进一步增强山东CA的灾后业务存续能力。

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授权的发证机构、垫付商和证书持有者书面通知，并在终止服务六十日前向国务院信息产业主管部门报告,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：

- 起草CA终止声明；
- 通知与CA停止相关的实体；
- 关闭从目录服务器；
- 证书撤销；
- 处理存档文件记录；
- 停止认证中心的服务；

- 存档主目录服务器；
- 关闭主目录服务器；
- 处理山东CA系统管理员和业务管理员；
- 处理加密密钥；
- 处理和存储敏感文档；
- 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

- 加密密钥对是由中华人民共和国国家密码管理局许可的、山东CA数字证书签发系统支持的加密机设备生成的，由山东省密码管理局所属的KMC控制管理。
- 签名密钥对是由客户端产生，证书申请者可使用山东省密码管理局认可的、山东CA数字证书签发系统支持的介质生成签名密钥对。签名密钥存储在介质中不可导出，保证山东CA无法复制签名密钥对。

  山东CA支持多种介质，如智能密码钥匙、智能IC卡等。山东CA可根据证书申请者要求或自身选择签名密钥对生成介质。
- 服务器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，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

山东CA从KMC取得订户加密公钥后为其签发证书，在此过程中采用国家密码管理局许可的对称密钥算法加密，保证了传输中密钥的安全。

自生成密钥对证书订户向山东CA提交证书申请时，该请求信息内的公钥，使

用安全通道保证信息的机密性和完整性。

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（http://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、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

为了保证加密/解密的安全性，山东CA所使用的密钥对长度为1024位。如果国家法律法规、政府主管机构等对密钥长度有明确的规范和要求，山东CA将会完全遵从。

6.1.6 公钥参数的生成和质量检查

公钥参数由国家密码管理局许可、山东CA数字证书签发系统支持的硬件产生；质量检查由国家密码管理局具体实施。

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。

- 山东CA的签名密钥用于签发RA证书和证书撤销列表（CRL）；
- RA的签名密钥用于确认RA所做的审批证书等操作；
- 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；
- 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

KMC可以根据客户和法律的需要，对加密密钥进行托管。签名私钥由订户自己保管，以保证其不可否认性。

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。

KMC备份托管的订户加密私钥，确保加密私钥的安全。

6.2.5 私钥归档

KMC提供过期的托管私钥的存档服务；保存期为七年。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或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。

山东CA所签发的服务器类证书，证书的私钥由专有的密码模块提供和保存，

当服务程序要加载私钥时需求通过保护口令的验证才能访问密码模块中的私钥。

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。

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。

如果订户证书私钥的激活数据是口令，这些口令必须：

- 由订户产生；
- 至少6位字符或数字；
- 不能包含很多相同的字符；
- 不能和操作员的名字相同；
- 不能使用生日、电话等数字；
- 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

- 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。

- 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是在山东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的数字证书签发系统的数据文件和设备由山东CA系统管理员维护，未经山东CA管理员授权，其它人员不能操作和控制山东CA系统；其它普通订户无系统账号和密码。山东CA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。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，山东CA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CA系统及其运营环境通过了中国国家信息安全测评认证中心的运营系统安全测评。

山东CA根据法律法规和主管部门的规定，按照国家计算机安全等级的要求，实现安全等级制度。

6.6 生命周期技术控制

6.6.1 系统开发控制

按照山东CA内部系统开发流程进行控制。

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在案并进行控制，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。

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的证书认证系统在系统设计过程中充分进行了安全性考虑，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访问。只有经过授权的山东CA员工才能够进入山东CA签发系统、山东CA注册系统、山东CA目录服务器、山东CA证书发布系统等设备或系统。所有授权订户必须有合法的安全令牌，并且通过密码验证。

CA系统只开放与申请证书、查询证书等相关操作功能，其他端口和服务全部关闭。

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认证系统的各种系统日志、操作日志有对应的记录时间。

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RFC3280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：

- 证书版本号（Version）

  指明X.509证书的根式版本，值为V3。

- 证书序列号（SerialNumber）

  指唯一标识该证书的一组32位字符。

- 证书签名标识符（Signature）

  指定签发证书时所使用的签名算法。

- 签发机构名（Issuer）

  用来标识签发证书的CA的 DN名字。

  CN = SDCA Root Authority

  C = CN

- 证书有效期（Validity）

  指证书的起止时间。

- 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。

- 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。

- 微缩图算法

证书内容的签名算法。

- 微缩图

  证书内容的签名值。

证书扩展项：

- 授权密钥标识符

  授权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。

- 主题密钥标识符

  通过主体密钥标识符识别相对应证书的公钥。

- 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。

- 密钥扩展使用

  暂无。

- 证书策略

  暂无。

- 基本限制

  用于鉴别证书持有者身份，如最终订户等。

- CRL发布点

  由山东CA定义的CRL发布点。如：

  Directory Address：

  CN=crl396，OU=crl，OU=5 OU=1，O=SDCA，L=JINAN，S=SHANDONG，C=cn

7.1.3 算法对象标识符

山东CA签发的证书按照RFC 3280标准，用 sha1RSA算法签名。

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

订户在证书中的名称可以是假名，但不能使用匿名，并在山东CA的数据库中记录订户的相关信息。山东CA可以按照一定的规则为订户指定特殊名称，并且能够把该类特殊的名称与一个确定的实体（个人、单位或设备）唯一联系起来。

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RFC3280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。

- 版本号：用来指定CRL的版本信息。
- 签名算法：山东CA采用sha1RSA签名算法。
- 颁发者：指定签发机构的DN名。
- 生效时间：指定一个日期/时间值，用以表明本CRL发布的时间。
- 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。
- 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。
- 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。

- 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的撤消方案的局限性，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、安全时间发生后的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、注册分支机构、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 评估者的资质

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：

- 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的审计人员或审计评估机构，且在业界享有良好的声誉；
- 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；
- 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：

- 安全策略是否得到充分实施；
- 运营工作流程和制度是否严格遵守；
- 电子认证业务规范是否符合证书策略的要求；
- 是否严格按照本CPS、业务规范和安全要求开展业务；
- 各种日志、记录是否完整，是否存在问题；
- 是否其它可能存在的安全风险；
- 山东CA支持的证书认证操作规程是否完全与本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；
- 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；
- 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，由安全中心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中心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、注册分支机构、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

证书相关费用在山东CA的网站上公布（http://www.sdca.com.cn）。价目表按山东CA明确指定的时间生效，若没有指定生效时间的，自价目表公布之日起生效。山东CA也可以通过其他方法通知证书持有者或其他各方费用变化。

9.1.1 证书签发和更新费用

根据山东CA的价目确定。

9.1.2 证书查询费用

山东CA目前不对证书查询收取专门的费用。

9.1.3 证书撤销或状态信息的查询费用

证书撤销列表（CRL）的获取不收取任何费用。山东CA有可能根据需要将OCSP服务作为增值服务收取费用。

9.1.4 其他服务费用

根据山东CA的价目确定。

9.1.5 退款策略

如果由于山东CA违背了本证书策略所规定的责任，造成订户合同无法履行、订户证书无法使用，山东CA对订户证书进行撤销并将订户为申请证书所支付的费用退还给订户。

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。

9.2.1 保险范围

出现下列情形并经公司确认后，证书订户、依赖方等实体可以申请赔偿（法定或约定免责除外）。

1）山东CA在批准证书前没有严格按业务程序确认证书申请，造成证书的错误签发，并导致订户或依赖方遭受损失的；

2）山东CA将证书错误的签发给订户以外的第三方，导致订户或者依赖方遭受损失的；

3）由于山东CA的原因导致证书私钥被破译、窃取，导致订户或者依赖方遭受损失的；

4）山东CA未能及时撤销证书，导致订户或者依赖方遭受损失的。

9.2.2 其他资产

山东CA目前有能力维护运营和应对可能出现的赔付。

9.2.3 对最终实体的保险或担保

山东CA承担订户或依赖方在使用证书过程中造成损失时的举证责任，如无证据证明订户或依赖方使用过程中存在错误操作，则山东CA将按照发布的赔偿办法予以赔偿。

9.3 业务信息保密

山东CA有专门的信息保密制度，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

山东CA保密的信息包括（但不限于）：

- 系统方面

- 认证系统结构、配置，包括系统、网络、数据库等；
- 认证系统安全策略和方案；
- 系统操作、维护记录；
- 各类系统操作口令。

- 运营管理方面

- 物理安全策略与实施方案，包括场地、访问控制、入侵检测等实施方案；
- 密钥管理策略与操作记录；
- CA 或RA 批准或拒绝的申请纪录；
- 可信人员名单；
- 内部安全管理策略与制度。

- 审计记录。

● 订户信息

- 订户的注册信息；
- 订户系统、应用访问CRL、OCSP 的记录（时间、频度）；
- 订户与认证机构、注册机构签订的协议。

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 个人隐私保密

9.4.1 隐私保密方案

山东CA制定有隐私保护制度并签定保密协议，保证证书订户的个人信息不被滥用、未授权使用或出售，同时采取必要措施防止客户资料被遗失、盗用与篡改。

9.4.2 作为隐私处理的信息

作为隐私处理的信息包括：最终订户注册申请证书中提交的信息，包括联系电话、地址等；订户与山东CA、注册机构签订的协议。

9.4.3 不被视为隐私的信息

不被认为是隐私信息包括：用来构成证书内容的信息，证书及证书状态。

9.4.4 保护隐私的责任

除非执法、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和授权，订户同意和授权信息以下列

方式之一传送给山东CA或其注册机构：

1）将手写签名的同意和授权文件邮寄、快递到山东CA或其注册机构；

2）将手写签名的同意和授权文件传真到山东CA或其注册机构；

3）以签名电子邮件的形式同意并授权。

9.4.6 依法律或行政程序的信息披露

当山东CA在任何法律、法规或规章条款的要求下，或在司法机关的要求下必须披露本电子认证业务规则中具有保密性质的信息时，山东CA可以按照法律、法规或规章条款以及司法机关的要求，向执法部门公布相关的保密信息。这种披露不视为违反了保密的要求和义务。

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相应的依赖方协议。

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，若本电子认证业务规则的规定与其他山东CA制定的相关规定、指导方针相互抵触，订户必须接受本电子认证业务规则的约束。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电子认证业务规则的规定执行；对协议中有不同于本电子认证业务规则内容的约定，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：

- 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；
- 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；
- 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：

第一：除上述所规定的职责条款，山东CA、山东CA的服务机构、山东CA授权的发证机构、山东CA的雇员不承担其它任何义务。必须指出，本电子认证业务规则的内容，没有任何信息可以暗示或解释成山东CA必须承担其它的义务或山东CA必须对其行为作出其它的承诺。

第二：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。

第三：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，并在本电子认证业务规则或相应的注册机构协议中规定，以后山东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电子认证业务规则的条款。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：

- 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；
- 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；

- 订户需熟悉本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；
- 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授权的发证机构，申请采取挂失、废除等处理措施。

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，阅读了依赖方协议，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：

- 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;
- 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；
- 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；
- 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；
- 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；
- 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；
- 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）：

- 自然灾害，包括地震、火山爆发、滑坡、泥石流、雪崩、洪水、台风等；
- 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已谨慎地遵循了国家法律、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

1）对于由如下原因造成的订户或依赖方损失，山东CA对订户或依赖方进行赔偿：

（1）山东CA在批准证书前没有严格按业务程序确认证书申请，造成证书的错误签发；

（2）由于山东CA的原因，使得证书中出现了错误信息；

2）在如下情况，订户对自身原因造成的山东CA、依赖方损失承担责任：

（1）订户在证书申请中对事实的虚假或错误描述；

（2）在证书申请中订户没有披露重要的事实，如果这种错误表述或遗漏是因为粗心或故意欺骗任何一方；

（3）订户没有使用可信系统保护私钥，或者没有采取必要的注意防止订户私钥的安全损害、丢失、泄漏、修改或非授权的使用；

（4）订户使用的名字（包括但不限于通用名、域名和e-mail 地址）破坏了第三方的知识产权法。

3）在如下情况，依赖方对自身原因造成的山东CA损失承担责任：

（1）依赖方没有执行依赖方职责义务；

（2）依赖方在不合理的环境下信赖一个证书；

（3）而依赖方没有检查证书状态确定证书是否过期或撤销。

4）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：

（1）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
自然人证书	800 元 RMB
机构（企业）证书	4000 元 RMB
设备证书	8000 元 RMB

这种赔偿上限可以由山东CA根据情况重新制定，山东CA会将重新制定后的情况立刻通知相关当事人。

（2）对于由订户或依赖方的原因造成的损失，山东CA不承担责任，由订户或依赖方自行承担。

（3）山东CA只有在其证书有效期限内承担损失损害赔偿。

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，已签发符合本证书策略的证书，效力作用直到证书到期或撤消。

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，会通过适当方式，如电话、电邮、信函、传真等，个别通知订户、依赖方。

9.12 修订

山东CA有权在合适的时间修订本电子认证业务规则中任何术语、条件和条款，而且无须预先通知任何一方。

山东CA有权在山东CA的自主数据库中设置和公布修改结果，或以其他方式（如修改CPS版本的形式或在网站上）公布。

所有的修订在公布后立刻生效。

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。

本CPS的修订，由安全中心组织讨论，提出修订报告，经山东CA安全管理委员会批准后，由安全中心负责组织修订，修订后的CPS经过山东CA安全管理委员会审查通过后正式实施。

9.12.2 通知机制和期限

修改后的CPS经批准后将立即在山东CA信息库更新通告栏发布。对于需要通过电子邮件、信件、媒体等方式通知的修改，山东CA将在合理的时间内通知有关各方，合理的时间保证有关方面受到的影响最小。

山东CA保留随时对CPS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。

9.12.3 必须修改业务规则的情形

由山东CA安全中心根据公司业务情况提出，山东CA安全管理委员会审批。

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

本规则在各方面服从《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的使用也必须遵从使用地的相关法律和法规。

9.16 一般条款

9.16.1 完整协议

CP、CPS、订户协议及依赖方协议及其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

法律允许的范围内，在山东CA订户协议、依赖方协议和其他订户协议内出现可以同其他条款分割的条款时，协议中的可分割条款的无效不应该影响协议中其他条款效力。

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等，造成山东CA、注册机构无法提供正常的服务时，山东CA、注册机构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。