SDCA CPS

电子认证业务规则

版本 2.1

发布日期：2008 年 4 月 15 日

生效日期： 2008 年 5 月 1 日

SDCA CPS

Certification Practice Statement

Version 2.1

The Issuing Date：April 15, 2008

The Effective Date：May 1, 2008

山 东 省 数 字 证 书 认 证 管 理 有 限 公 司
Shandong Certification Authority Co.,Ltd

山东 CA 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： **山东 CA 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 CA 证书服务的组织、单位和个人，山东 CA 将保留依法追诉的权利。

修订表

版本	日期	备注
1.0	2001年5月8日	采用RFC2527结构
2.0	2004年5月1日	采用RFC3647结构
	2005年4月8日	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
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。

目　录

第一章 概括性描述

1.1 概述

1.1.1 山东 CA

山东 CA 是指山东省数字证书认证中心，是由山东省数字证书认证管理有限公司（Shandong Certification Authority Co.,Ltd，简称**山东 CA**）提出、设计、建设、运行，可实现跨地区、跨行业统一认证和安全服务的电子认证服务机构。该机构遵循 PKI 体系标准，在地域或行业两方面进行全方位的布局，可实现交叉认证。山东 CA 自成立以来，严格按照国家规定的各项要求，2003 年 9 月 28 日，山东省数字证书认证中心建设实施方案通过了国家密码管理委员会办公室组织的专家论证。2003 年 11 月 22 日，山东 CA 通过了国家密码管理委员会办公室组织的安全性审查。2004 年 7 月 14 日，山东 CA 圆满通过国家密码管理委员会办公室组织的技术鉴定，成为全国第五家通过国家技术鉴定的数字证书认证中心。

山东 CA 为互联网络的交易和作业方建立信任关系，保证交易主体身份的真实性，为信息的保密性、完整性以及交易的不可抵赖性提供全面的服务。其宗旨是保证互联网络提供的服务和享受服务的客户实现安全交易，为互联网络的客户提供网上身份认证和信任服务。

山东 CA 作为被信任的第三方，为网上交易和网上安全作业的参与方颁发数字证书。在山东 CA 或山东 CA 授权的发证机构确定参与方的真实身份后，由山东 CA 或山东 CA 授权的发证机构发放数字证书，山东 CA 数字证书（以下简称证书）遵循 X.509V3 的规范。山东 CA 承诺，在证书有效的情况下，保证证书能唯一地与身份明确的实体相关联，公钥能与身份确定的实体唯一相对应。

为了配合证书业务的正常开展，山东 CA 建立了山东 CA 电子认证业务规则，电子认证业务规则的建立并保障其完整正确地得到贯彻和实施将为电子政务公共服务、电子交易和其他网上安全服务提供强有力的支持。

1.1.2 电子认证业务规则

山东 CA、山东 CA 授权的注册机构、注册分支机构、受理点、山东 CA 授权或协议的单位等实体，统称为山东 CA 认证体系内的实体或山东 CA 关联实体。山东 CA 认证体系内的实体和山东 CA 数字证书持有者，必须完整地理解和执行山东 CA 电子认证业务规则所规定的条款，承担相应的责任和义务。

山东CA电子认证业务规则详细阐述了山东CA实际工作和运行应遵循的各项规范。它支持多种山东 CA 制定的证书策略。证书策略是证书管理、证书应用、证书

分类、证书授权、证书责任等政策规则的集合。

电子认证业务规则作为实际应用和操作的文件依据，适用于山东 CA、山东 CA 授权机构、山东 CA 数字证书签约单位、山东 CA 实体内员工、申请证书的单位和个人。作为公告，向社会公布山东 CA 关于证书服务的基本立场和观点。在证书有效期内为证书申请者提供相关的咨询服务。山东 CA 认证体系中涉及的单位和个人，必须完整理解和准确解释山东 CA 电子认证业务规则的内容。

1.2 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）的缩写形式。

山东 CA 所拥有的品牌的商标为：

1.3 文档名称与标识符

1.3.1 名称

本文档名称为山东 CA 电子认证业务规则，是山东 CA 对所提供的认证及相关业务的全面描述。

1.3.2 版本

本电子认证业务规则为山东 CA 发布的 2.1 版本，在《山东 CA 电子认证业务规则 V2.0》的基础上修改整理。

1.3.2 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

1.4 电子认证活动参与者

1.4.1 电子认证服务机构

山东 CA 和山东 CA 下层 CA 统称为**电子认证服务机构**。

山东 CA 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。山东 CA 将决定在什么时间，什么地点、由什么人监督、怎么实施山东 CA 根密钥对的更新和切换。山东 CA 的运作单位是山东省数字证书认证管理有限公司即**山东 CA**。山东 CA 必须建立完善的安全机制，以保证根私有密钥的安全性。在时机成熟的时候，山东 CA 将建立异地备份中心。

山东 CA 所签发的证书与每一个证书申领实体的公钥绑定。山东 CA 承诺，在有效期内的证书,将采用证书目录服务器和证书黑名单服务器CRL SERVER(Certificate Revocation List Server)，公布该证书可以公开的信息和状态。

山东 CA 将根据业务需要，与山东 CA 服务框架体系中未涉及的其它电子认证服务机构建立交叉认证关系。交叉认证是指两个完全独立的，采用各自认证策略的证书认证中心建立相互信任关系，从而使双方的客户可以实现互相认证。当山东 CA 需要建立某 CA 交叉认证关系时，即信任某电子认证服务机构发放的证书，山东 CA 将审查该电子认证服务机构目前已在执行的证书业务相关文件、承诺以及操作规程。所有信任山东 CA 的机构，如果要接受与山东 CA 建立交叉认证关系的 CA 所发放的证书，必须自行检查该 CA 的电子认证业务规则及其他证书业务相关的文件。交叉认证并不表示山东 CA 批准了或赋予了其它独立电子认证服务机构的任何权力。

1.4.2 注册机构（Registration Authority）

注册机构作为电子认证服务机构授权委托的下属机构，负责证书用户信息的审核、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，可以直接对最终用户提供服务。注册机构可以根据客户群体的发展需要，遵循山东 CA 认证体系地域或行业的划分情况，授权建立相应的受理点或注册分支机构。注册机构有责任妥善保存客户的数据，不允许将客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。注册机构必须获得电子认证服务机构的授权。地区、行业、机构均可以申请成为山东 CA 的注册机构。注册机构性质包含授权、品牌、独立法人等。山东 CA 注册机构于 2004 年通过国家密码管理委员会办公室组织的技术鉴定，并成为全国第一家通过国家密码管理委员会办公室技术鉴定的远程注册机构。

1.4.3 注册分支机构（Registration Authority Branch）

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。注册分支机构由注册机构或电子认证服务机构授权建立或撤消。注册分支机构是可选项，即根据客户群体大小决定是否设注册分支机构。注册分支机构性质包含授权、品牌、独立法人等。

1.4.4 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 正在实施的数字证书政策（CP），电子认证业务规则以及山东 CA 的 CA 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、电子邮件信箱、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（§1.4.5）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。

1.4.5 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。

1.4.6 证书持有者（Subscriber）

证书持有者包括个人、单位、服务器、网站等提供网上服务和享受网上服务的各种实体，以及其他持有山东 CA 各类证书的人、物或组织单位。

证书持有者分为两类：

- 被垫付的证书持有者，其证书费用由证书垫付商承担；
- 自支付的证书持有者，自行承担证书费用。

1.4.7 信任体（Relying Party）

在山东 CA 证书服务体系范围内，用证书进行网上作业的证书持有者，称为山东 CA 的信任体。

信任体必须是山东 CA 证书服务体系中证书持有者，享有相应的利益，包括山东 CA 可能提供的证书保障，以及山东 CA 电子认证业务规则或证书政策中涉及的权益。

1.4.8 证书申请者（Certificates Applicant）

请求山东 CA 颁发证书的个人、企业和组织机构。

1.4.9 用户（Subscriber）

指由山东 CA 签发的各种类型证书的持有者。

1.4.10 其他参与者（Other Participants）

为以上未提及的隶属于山东 CA 证书体系的实体。如目录服务提供者等与 PKI 服务相关的参与者。

1.5 证书应用

1.5.1 适合的证书应用

山东 CA 数字证书目前已经在电子政务公共服务、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。具体请参阅 http://www.sdca.com.cn/。证书申请者可以根据实际需要，自主判断和决定采用相应合适的证书种类。

1.5.2 限制的证书应用

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

由于证书的使用可能导致人员死亡、伤残的情形。

由于证书的使用可能导致环境破坏的情形。

1.6 策略管理

1.6.1 版权

1.6.2 电子认证业务规则批准程序

在山东 CA 电子认证业务规则做出任何变动之前，山东省数字证书认证管理有限公司将对提供的变动建议进行研究，做出变更决定。在征询山东 CA 律师有关法律方面的意见后，形成决议。山东 CA 将在决议形成后，在山东 CA 网站公布变更后的山东 CA 电子认证业务规则正式文档。

1.6.3 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：运营安全管理小组

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：webmaster@sdca.com.cn

1.6.4 公告

所有公告和通知被山东 CA 电子签名后，将在山东 CA 网站上公布。

山东 CA 网站地址：http://www.sdca.com.cn。

第二章 信息发布与信息管理

2.1 目录服务

山东 CA 通过目录服务发布证书的使用和废止的相关信息。用户可以通过访问山东 CA 的目录服务器获取证书的信息。山东 CA 同时提供在线证书状态查询、证书废除列表查询服务。

2.2 信息发布

2.2.1 CPS 的发布

《山东CA电子认证业务规则 V2.0》版权由**山东CA**完全拥有，并负责本规范的解释，一经山东CA在网页http://www.sdca.com.cn/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。

本电子认证业务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 网页 http://www.sdca.com.cn/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 在山东 CA 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。

2.2.3 证书的发布

证书在签发成功后，山东 CA 通过目录服务器自动将该证书发布，并可到山东 CA 网站上进行查询。山东 CA 定期公布在证书有效期内被废止的数字证书。证书用户都可以在山东 CA 的网站中查询获得有关信息。

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 电子认证业务规则 V2.0》是山东 CA 最新发布的版本，山东 CA 有权利对其进行改动，其发布时间及频率由山东 CA 决定。如有任何改动，山东 CA 会以电子形式把最新版本的电子认证业务规则或是相应条目的修改即时发布。

2.3.2 山东 CA 公众信息的发布时间及频率

山东CA在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，会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的目录服务器上每日更新目录，通常在 24 小时内自动发布最新CRL，也可人工发布最新CRL。证书用户可在山东CA网页http://www.sdca.com.cn/上查询或下载数字证书和CRL。

2.4 信息访问控制

2.4.1 信息的发布与处理

山东 CA 将及时在网站上公布新的信息。只有山东 CA 有权对网站上的旧信息进行处理。

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，保证只有经过授权的山东 CA 工作人员才能编写和修改山东 CA 在线的公告版本和公布信息。

2.4.3 信息资料权限管理

山东 CA 在必要时可自主选择是否实行信息的权限管理，以确保只有证书用户才有权阅读受山东 CA 控制的信息资料。

第三章 身份标识与鉴别

3.1 命名规则

3.1.1 甄别名

甄别名（Distinguished Name）包含于每张证书中含有的用户信息，唯一标识证书用户的身份。

山东 CA 证书符合 X509.3 标准，甄别名格式遵守 X500 标准。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	王超

3.1.2 E-mail

E-mail 标识个人、单位安全电子邮件证书中的电子邮件。

3.1.3 通用名命名方式

各类证书通用名命名方式不同，但是所有证书用户的通用名都需要严格审查。命名方式如下：

编号	证书类型	通用名
1	个人身份证书	个人姓名（与身份证上标明的一致）
2	单位身份证书	单位名称（与营业执照等有效证件上标明的一致）
3	WEB 服务器证书	域名或者 IP 地址
4	服务器身份证书	服务器主机名或 IP 地址
5	单位安全电子邮件证书	单位名称（同单位证书），单位电子邮件地址
6	个人安全电子邮件证书	个人姓名（同个人证书），个人电子邮件地址
7	个人代码签名证书	个人姓名（与身份证上标明的一致）
8	单位代码签名证书	单位名称（与营业执照等有效证件上标明的一致）
9	VPN 网关证书	根据实际情况
10	VPN 客户端证书	根据实际情况

3.2 初始身份验证

3.2.1 单位身份证书申请验证

单位申请者填写书面申请表（一式三份），经过单位授权代表的签署及单位盖章后，携带以下资料到山东 CA 授权的发证机构进行身份审核及交费手续 （以下证件的复

印件和申请表需要单位盖章证明）：

a）申请单位的组织机构代码证的复印件；

b）申请单位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
- 事业单位登记证
- 事业单位法人登记证
- 税务登记证
- 组织机构代码证
- 社会团体登记证
- 社会团体法人登记证
- 人民团体登记证
- 人民团体法人登记证
- 政府批文
- 其他有效证件

c）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，根据审核人员的管理规定对申请者的资料的真实性进行表面审查，并进行批准或拒绝的操作。

3.2.2 单位 Email 证书申请验证

由于山东 CA 无法验证申请者提供的 Email 是否为单位所属，无法验证申请者提供的 Email 的真实性。因此，山东 CA 对单位 Email 证书的 Email 地址的有效性不承担任何责任。

申请者填写书面申请表（一式三份），经过单位授权代表的签署及单位盖章后，携带相关资料（同§3.2.1）到山东 CA 授权的发证机构进行身份审核及交费手续。

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，根据审核管理规定对申请者的资料的真实性进行表面审查，并进行批准或拒绝的操作。

3.2.3 个人用户身份验证

山东 CA 的个人证书签发给合法的个人申请者，山东 CA 需要审核个人申请者的身份。

个人申请者填写书面申请表（一式三份），个人签字后，携带个人身份证（或军官证、或学生证或护照等）原件与复印件到山东 CA 授权的发证机构进行身份审核及

办理交费手续。

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表面审查，并进行批准或拒绝的操作。

3.2.4 个人Email证书申请验证

山东CA无法验证个人Email是否为申请者所属，无法验证Email的真实性。因此，山东CA对个人Email证书的Email地址的有效性不承担任何责任。

个人申请者填写书面申请表(一式三份)，个人签字后，携带相关资料(同§3.2.3节）到山东CA授权的发证机构进行身份审核及办理交费手续。

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表面审查，并进行批准或拒绝的操作。

3.2.5 Web服务器证书申请验证

申请者的提交服务器证书请求（CSR）文件。

申请者提交相关证明确认服务器已经申请了有效的Internet DNS名称(即域名)或IP地址。

申请者填写书面申请表（一式三份），经过单位授权代表的签署及单位盖章后，携带相关资料（同§3.2.1）到山东 CA 授权的发证机构进行身份审核及办理交费手续；

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表面审查，并进行批准或拒绝的操作。

3.2.6 服务器身份证书申请验证

申请者填写书面申请表(一式三份)，经过单位授权代表的签署及单位盖章后(如为个人申请则需要个人签名)，携带相关资料（同§3.2.1或§3.2.3）到山东CA授权的发证机构进行身份审核及办理交费手续。

山东 CA 无法验证服务器身份的真实性，因此山东 CA 不对服务器身份的有效性负责。山东CA仅提供服务器身份证书的加密、签名服务。

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表面审查，并进行批准或拒绝的操作。

3.2.7 单位代码签名证书申请验证

同第 3.2.1 节

3.2.8 个人代码签名证书申请验证

同第 3.2.3 节

3.2.9 VPN 网关证书申请验证

同第 3.2.1 节

3.2.10 VPN 客户端证书申请验证

同第 3.2.1 节

3.2.11 审核认证体系成员身份

山东 CA 认证机构的管理员、操作员必须是山东 CA 认证机构的正式职员。

认证机构管理员的身份除了必须符合个人证书申请者的条件外，还必须符合各认证机构协议中的有关规定。

认证机构资格由山东 CA 根据各认证机构协议来审查批准。

单位和个人身份或 EMAIL 证书用户的身份验证方式由山东 CA 来定义和验证。山东 CA 有权利选择用户身份验证的方式和方法，以达到全面准确验证用户身份的目的。

3.3 更新请求确认

3.3.1 更新申请情况

- 证书到期；
- 证书补发；
- 证书 DN 或 EMAIL 更改；
- 密钥更新。

出现以上情况时证书用户可以到山东 CA 授权的发证机构申请更新证书。

3.3.2 更新操作

证书用户申请更新证书时，填写证书更新表（一式三份），按照初始身份验证步骤提交相关资料（同§3.2）并由山东 CA 授权的发证机构审核。

3.3.3 更新申请的确认

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表面审查，并进行批准或拒绝的操作。

3.4 废止请求确认

3.4.1 证书废止情况

- 密钥泄漏；
- 证书有效期内用户终止使用证书；
- 其它。

证书废止包括证书废除、证书挂起。

3.4.2 废止操作

证书用户申请废止证书时，填写证书废止表（一式三份），按照初始身份验证步骤提交相关资料（同§3.2）并由山东 CA 授权的发证机构审核。

3.4.3 废止申请的确认

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表面审查，并进行批准或拒绝的操作。

3.5 恢复请求确认

3.5.1 恢复情况

只能恢复被挂起的证书。

3.5.2 恢复操作

证书用户申请恢复证书时，填写证书恢复表（一式三份），按照初始身份验证步骤提交相关资料（同§3.2）并由山东 CA 授权的发证机构审核。

3.5.3 恢复申请的确认

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表面审查，并进行批准或拒绝的操作。

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数字证书授权、申请、发放、修改、查询和管理等服务，提供网络安全及身份认证、电子公正、密钥管理等与数字证书密切相关的配套服务。本章节描述的证书包括 CA 证书、RA 证书、终端用户证书。本章节主要以终端用户中的证书申请者为模板，描述证书业务规范。

4.1 证书申请

4.1.1 证书申请对象

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、LRA、受理点和 CA 机构或 RA 机构的系统及相应的管理员。

4.1.2 证书申请流程

山东 CA 接受离线申请和在线申请（目前只提供测试证书）这两种申请方式。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。

4.1.2.1 离线申请

对于离线申请，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），申请者提交一份内容完整的带个人签名的申请书。可以从山东 CA 的网站下载或到山东 CA 授权的发证机构领取。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（一式三份）或到山东 CA 网站下载相应的申请表（一式三份），申请者应提供单位对经办人的委托书，单位的工商注册、税务、登记组织机构代码证件、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，需一式三份；
- 客户的申请表和相关证明文件的复印件存档 7 年，或直到申请人与山东 CA 终止合作为止。两者中以时间长的为准；
- 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。

4.1.2.2　在线证书申请

在线证书申请，目前只针对测试证书。在安全性得到保证的情况下，允许申请者到山东 CA 或山东 CA 授权的发证机构申请测试证书。对于测试证书，山东 CA 不承担由于测试证书的使用而带来的任何责任。

4.1.3　证书申请注意事项

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。以及由此造成的后果，山东 CA 不承担。

4.2　证书审核

4.2.1　证书申请的识别与鉴定

山东 CA 授权的发证机构遵循第三章对证书申请者提交的信息进行审核。

4.2.2　证书申请的通过与拒绝

山东 CA 授权的发证机构根据验证的信息审核通过或拒绝证书申请者的申请。若通过申请，则提交 CA。

4.2.3　证书审核时间

山东 CA 授权的发证机构必须在 24 小时内对证书申请者提交的证书信息进行审核。

4.3　证书签发

4.3.1　签发证书

- 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 § 4.2），山东 CA 将为证书申请者颁发证书。生成参考码、授权码并返还给发证机构；

- 山东 CA 授权的发证机构接收到参考码、授权码后，为证书申请者制作证书，并随同密码信封一起提供给用户；
- 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。证书从用户接受证书（参见§4.4 关于证书接受）那天起将被视为有效证书。

4.3.2 证书签发通知

山东 CA 直接通知用户或发证机构证书已签发。并将证书及密码信封直接提供给申请者。

4.3.3 拒绝签发证书

山东 CA 授权的发证机构可以根据其独立判断，拒绝给任何人签发证书，并且不对因此而导致的任何损失或费用承担任何责任和义务。除非证书申请者提交了欺骗性的或伪造的信息，山东 CA 在拒绝签发证书后，将立即归还证书申请者所付的所有证书购买费用。

4.4 证书接受

4.4.1 证书接受

在山东 CA 数字证书签发完成后，山东 CA 将把数字证书及密码信封当面或寄送给证书申请者，证书申请者从获得证书起就被视为已同意接受证书。证书申请者接受数字证书后，应妥善保存其证书对应的私有密钥。证书申请者可以从山东 CA 网站 http://www.sdca.com.cn/中下载个人或其他数字证书。

4.4.2 证书申请者陈述

一旦接受山东 CA 发证机构签发的证书，从接受之时起直至证书的整个使用有效期内，如果证书申请者不另行通知，那么证书申请者被视为向山东 CA、发证机构及所有合理信赖证书中所含信息的个人、实体作出如下保证：

- 用与证书中所含公钥相对应的私有密钥所进行的每一次电子签名，都是证书申请者自己的电子签名，并且在进行电子签名时，证书是有效证书并已被证书申请者接受（证书没有过期、废止）；
- 未经授权的人员从未访问过证书申请者私有密钥；
- 证书申请者向发证机构陈述的所有包含在证书中的有关信息是真实的；
- 就证书申请者所知道的或注意到的包含在证书中的信息，都是真实的（如果证书申请者发现了证书中信息存在某些错误，但证书申请者还没有及时通知给发证机构，那么，发证机构认为：证书申请者认为上述信息都是真实的）；
- 证书将按山东 CA 电子认证业务规则的规定，只用于经过授权的或其它合法的使用目的；
- 证书申请者是最终证书申请者而不是发证机构。除非经证书申请者和发证机构间的书面协议明确批准，证书申请者保证不从事发证机构（或类似机构）

所从事的功能，例如：把与证书中所含的公钥所对应的私有密钥用于签发任何证书（或认证其他任何形式的公钥）或证书吊销列表。

一经接受证书，既表示证书申请者知悉和接受山东 CA 电子认证业务规则中的所有条款和条件，并知悉和接受相应的证书申请者协议。

4.4.3 证书申请者责任

一经接受证书，证书申请者就应承当如下责任：既始终保持对其私有密钥的控制，使用可信的系统，和采取合理的预防措施来防止私有密钥的遗失、泄露、被篡改或被未经授权使用。

4.4.4 申请者的赔偿

一经接受证书，证书申请者即同意山东 CA、山东 CA 授权的发证机构以及他们的代理商、签约商对于由下列原因直接或间接造成的任何责任和损失不承担法律责任：

- 证书申请者（或其授权的代理人）虚假地或错误地陈述了事实；
- 证书申请者未能披露重要事实，而证书申请者的这种有意或无意的错误陈述或失职造成了对发证机构、山东 CA、或任何信任其证书的人的欺骗；
- 证书申请者没有使用可信系统或没有采用必要的合理措施防止其私有密钥被损害、丢失、泄露、被篡改或被未经授权使用。

证书申请者对山东 CA 和山东 CA 授权的 CA 发证机构以及他们的代理商、签约商造成的责任和损失包括：由于上述原因直接或间接造成的责任、损失、任何诉讼、仲裁及一切相关费用，包括但不限于诉讼费用、仲裁费用以及律师费等。对于此处的责任和损失，证书申请者将予以经济赔偿。

当证书是应证书申请者代理人的要求签发时，代理人和证书申请者应向发证机构、山东 CA 和它们的代理商和签约商，依照本节规定进行连带赔偿。证书申请者有责任就代理商的疏忽和错误陈述通知证书签发者。

4.4.5 发布

一旦证书申请者接受证书，发证机构将在目录服务器及由山东 CA 和发证机构决定的其它一个或多个方式发布证书的副本。证书申请者也可以在其它资料库中公布他们的由山东 CA 签发的数字证书。

4.5 密钥与证书的使用

4.5.1 用户私有密钥和证书的使用

证书应用范围：

编号	用户	证书类型	用户私有密钥与证书的用途

1	个人	个人身份证书	用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用户的其他身份信息。 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证书使用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证书使单位用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。
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、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、安全公文报送系统等。
8		服务器身份证书	主要颁发给需要安全鉴别的服务器，以便于表征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，其和对应的私有密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），企业的远端用户、分支机构、合作伙伴以及用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 密钥及证书的使用说明

申请者接受到数字证书后，应妥善保存其证书对应的私有密钥。申请者可以从山东 CA 证书目录服务器中下载个人或其他数字证书。

4.5.3 信赖体证书和公钥的用途

获得对方的证书和公钥后，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

为保证证书及其密钥对的安全有效，山东 CA 会为签发的证书设置有效期，一般为一年。这也是为了保证证书用户的权利。证书用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。更新证书时发证机构根据用户的要求决定新证书是否使用原证书密钥。出于安全考虑建议证书用户更新证书时更新密钥。

4.6.1 证书更新的原因

- 证书的使用期限将要到期；
- 其他。

4.6.2 证书更新的用户类型

由山东 CA 颁发的原有证书有效期限未到的个人、单位、服务器、企业、组织、网站等提供网上服务和享受网上服务的各种实体，以及其他凡是山东 CA 各类证书（包括测试证书）的有效期限未到的证书持有者。

4.6.3 证书更新的流程

- 申请者到山东 CA 授权的发证机构书面填写“证书更新申请表单”，并注明更新的原因。如果申请人是 RA 或 LRA，由 RA 或 LRA 填写表单。如果申请人是终端用户，则由终端用户填写表单；
- 山东 CA 授权的发证机构按照第三章识别与鉴定对用户提交的证书更新申请进行审核；
- 发证机构审核通过后，提交申请至山东 CA，山东 CA 为用户颁发新的参考码、授权码；
- 发证机构取得新的参考码、授权码后为用户制作证书；
- 证书签发后，发证机构将证书及其密码信封当面发给用户。用户接受证

书（详看§4.4节）；

- 新证书签发后旧的证书将被注销(§4.10)。山东CA将在1小时内在LDAP上发布用户的新证书。用户旧的证书在24小时内通过CRL发布。

4.6.4 证书更新的注意事项

请用户在进行证书更新之前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。

如用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概不负责。

4.7 密钥更新

由于技术的不断更新，为了加密的安全性与灵活性，山东CA有权定期更换证书用户的密钥。

4.7.1 私有密钥有效期

最终用户的私有密钥有效期一般均与其证书的有效期一致。但对于CA的签名根密钥而言，有效期应比其证书有效期短。其原因是为了防止电子认证服务机构签发的证书出现刚签发不久即失效的情况。如果CA签名密钥的证书有效期与私有密钥有效期一致，则在其证书有效期最后几天签发的证书会因签发证书的失效而无法使用。

CA签名私有密钥和证书有效期之间的关系除与下级证书有效期有关外，还与CA系统的层次结构有关。

4.7.2 密钥更新的原因

- 原有证书的密钥泄露。对此，证书持有者负有立即告知山东CA的义务；
- 原有证书到期，证书更新；
- 其他。

4.7.3 密钥更新的用户类型

由山东CA颁发的原有证书有效期限未到的个人、单位、服务器、企业、组织、网站等提供网上服务和享受网上服务的各种实体,以及其他凡是山东CA各类证书(包括测试证书）的有效期限未到的证书持有者。

4.7.4 密钥更新的流程

同第4.6节“证书更新的流程”。

4.7.5 密钥更新的注意事项

请用户在进行密钥更新之前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密钥的更新。

如用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 概不负责。

4.8 证书修改

4.8.1 证书修改原因

- 证书用户甄别名更改；
- 证书用户 Email 更改；
- 其他：如通用名、组织、角色改变等原因。

4.8.2 证书修改的用户类型

由山东 CA 颁发的原有证书有效期限未到的个人、单位、服务器、企业、组织、网站等提供网上服务和享受网上服务的各种实体，以及其他凡是山东 CA 各类证书（包括测试证书）的有效期限未到的证书持有者。

4.8.3 证书修改流程

- 申请者到山东 CA 授权的发证机构书面填写“证书更新申请表单”，并注明修改的原因。如果申请人是 RA 或 LRA，由 RA 或 LRA 填写表单。如果申请人是终端用户，则由终端用户填写表单；
- 山东 CA 授权的发证机构按照第三章识别与鉴定对用户提交的证书修改申请进行审核；
- 发证机构审核通过后，提交申请至山东 CA。山东 CA 为用户颁发新的参考码和授权码；
- 发证机构取得新的参考码、授权码后为用户制作证书；
- 证书签发后，发证机构将证书及其密码信封当面发给用户。用户接受证书（详看 §4.4 节）；
- 新证书签发后旧的证书将被注销（§4.10）。山东 CA 将在 1 小时内在 LDAP 内发布用户的新证书。用户旧的证书在 24 小时内通过 CRL 发布。

4.8.4 证书修改的注意事项

证书修改后，证书的有效期并没有改变，仍然为原证书有效期。

请用户在进行证书更新之前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。

如用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 概不负责。

4.9 证书挂起

4.9.1 证书挂起原因

- 证书用户暂停使用证书；
- 其他，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。

4.9.2 证书挂起的用户类型

由山东 CA 颁发的原有证书有效期限未到的个人、单位、服务器、企业、组织、网站等提供网上服务和享受网上服务的各种实体，以及其他凡是山东 CA 各类证书（包括测试证书）的有效期限未到的证书持有者。

4.9.3 证书挂起的流程

- 申请者到山东 CA 授权的发证机构书面填写“证书废止申请表单”，并注明挂起的原因。如果申请人是 RA 或 LRA，由 RA 或 LRA 填写表单。如果申请人是终端用户，则由终端用户填写表单；
- 山东 CA 授权的发证机构按照第三章识别与鉴定对用户提交的证书挂起申请进行审核；
- 强制挂起：山东 CA 授权的发证机关管理员可以依法对用户证书进行强制挂起，挂起后必须立即通知该证书用户。强制挂起的命令来源于：山东 CA 或山东 CA 授权的发证机构；
- 山东 CA 挂起用户证书后，发证机构将当面通知或通过发送 E-mail 邮件或邮寄的方式通知用户证书被挂起；
- 用户证书被挂起后，用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注销证书。对此造成的任何后果，山东 CA 不负任何责任。

4.9.4 证书挂起的注意事项

用户在申请证书挂起时，需在填写证书废止申请表时注明原因。并在以后，对进行挂起的证书进行恢复。

4.10 证书注销

注意此处：与证书挂起区分使用。

4.10.1 证书注销的原因

- 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有密钥被泄密或用户怀疑自己的密钥失密；

- 从属关系改变：与密钥相关的用户的主题信息改变，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（例如用户离开了某个组织）；
- 证书的更新费用未收到；
- 用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；
- 用户申请初始注册时，提供不真实材料；
- 证书已被盗用、冒用、伪造或者篡改；
- 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；
- 其他情况。这些情况可以是因法律或政策的要求山东 CA 采取的临时注销措施，也可以是用户申请注销证书时填写的其他原因。

4.10.2 证书注销的用户类型

由山东 CA 颁发的原有证书有效期限未到的个人、单位、服务器、企业、组织、网站等提供网上服务和享受网上服务的各种实体，以及其他凡是山东 CA 各类证书（包括测试证书）的有效期限未到的证书持有者。

4.10.3 证书注销的流程

- 申请者到山东 CA 授权的发证机构书面填写“证书废止申请表单”，并注明注销的原因。如果申请人是 RA 或 LRA，由 RA 或 LRA 填写表单。如果申请人是终端用户，则由终端用户填写表单；
- 山东 CA 授权的发证机构按照第三章识别与鉴定对用户提交的证书注销申请进行审核；
- 强制注销：山东 CA 授权的发证机关管理员可以对用户证书进行强制注销，注销后必须立即通知该证书用户。强制注销的命令来自于：山东 CA 或山东 CA 授权的发证机构；
- 山东 CA 注销用户证书后，发证机构将当面通知用户证书被注销。用户证书在 24 小时内进入 CRL 或被直接签发 CRL，向外界公布。

4.10.4 CRL 发布频率

山东 CA 将通过证书黑名单列表在 24 小时内公布被注销的证书，特殊紧急情况下可以立即生效（假使网络传输条件能够保证）。对于测试证书的注销，不提供黑名单公布服务。

4.10.5 CRL 检查要求

信任体应经常检查 CRL，包括：

- 在认证各方的数字证书前，根据山东 CA 最新公布的 CRL 检查该证书的状

态；

- 在使用证书前根据山东 CA 最新公布的 CRL 检查证书的状态；
- 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。

信任体应根据山东 CA 公布的最新 CRL 确认使用的证书是否被注销。如果黑名单公布证书已经注销，而信任体没有查黑名单，由此造成的损失由信任体本身承担。

4.10.6 证书注销的注意事项

- 山东 CA 没有公开数字证书注销原因的业务；
- 证书更新、证书修改、密钥更新后原有证书将被注销；
- 提交请求时需要指明注销原因，只有注销原因是“证书挂起”的证书将来才有可能通过“恢复证书”来被恢复使用；
- 请用户在进行证书注销之前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注销。

注意：此处的证书注销是永久性注销，不可以进行证书恢复。

4.11 证书恢复

4.11.1 证书恢复原因

- 证书被挂起。

证书恢复，只是针对挂起的证书。

4.11.2 证书恢复的用户类型

由山东 CA 颁发的原有证书有效期限未到的个人、单位、服务器、企业、组织、网站等提供网上服务和享受网上服务的各种实体，以及其他凡是山东 CA 各类证书（包括测试证书）的有效期限未到的证书持有者。

4.11.3 证书恢复的流程

- 申请者到山东 CA 授权的发证机构书面填写“证书恢复申请表单”。如果申请人是 RA 或 LRA，由 RA 或 LRA 填写表单。如果申请人是终端用户，则由终端用户填写表单；
- 山东 CA 授权的发证机构按照第三章“识别与鉴定”对用户提交的证书恢复申请进行审核；
- 发证机构审核通过后，为用户恢复证书。并通知用户证书已被恢复；
- 用户得到恢复通知，证书恢复完成。

4.12 密钥恢复

4.12.1 密钥恢复原因

- 加密密钥丢失；
- 加密密钥损坏；
- 司法取证密钥恢复；
- 其他。

4.12.2 密钥恢复的用户类型

由山东 CA 颁发的原有证书有效期限未到的个人、单位、服务器、企业、组织、网站等提供网上服务和享受网上服务的各种实体，以及其他凡是山东 CA 各类证书（包括测试证书）的有效期限未到的证书持有者。

4.12.3 密钥恢复流程

- 申请者书面填写“密钥恢复申请表单”，并注明恢复的原因。如果申请人是 RA 或 LRA，由 RA 或 LRA 填写表单。如果申请人是终端用户，则由终端用户填写表单；
- 山东 CA 授权的发证机构按照第三章识别与鉴定对用户提交的密钥恢复申请进行审核；
- 审核通过后，提交申请至山东 CA。山东 CA 为用户颁发新的参考码和授权码；
- 发证机构取得新的参考码、授权码后为用户恢复密钥，生成新的证书，并提交用户；
- 新证书签发后，旧的证书将被自动注销（§4.10）。山东 CA 将在 1 小时内在 LDAP 内发布用户的新证书。用户旧的证书在 24 小时内通过 CRL 发布。

4.12.4 密钥恢复的注意事项

- 密钥恢复只能恢复用户的加密密钥；
- 当证书用户接受证书后，应妥善保管签名证书，为其备份；
- 由用户丢失签名证书而造成的后果，山东 CA 概不负责；
- 加密密钥恢复后将生成新的证书，旧证书被废除。

4.12.4 司法取证密钥恢复

司法取证人员按照有关法律规定向山东省密钥管理中心提出密钥恢复申请，经审核后，由山东省密钥管理中心执行密钥恢复操作。

4.13 证书状态查询

山东 CA 提供以下服务为证书用户提供证书状态查询。

4.13.1 CRL

CRL 通过 LDAP 发布服务器进行发布，其可信度及安全性由根证书的签名来保证。用户需要将 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。

4.13.2 OCSP

山东 CA 提供 OCSP（在线证书状态查询）服务，用户可以通过访问山东 CA 网站 http://www.sdca.com.cn/获得证书的状态信息。

4.14 服务终止

服务终止是指证书用户终止与山东 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，证书用户不再延长证书使用期或者不再重新申请证书时，证书用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，由于证书用户的原因而单方面要求终止证书服务。山东 CA 将根据证书用户的要求挂起或废除证书。证书用户与山东 CA 的服务终止。

4.15 密钥托管与恢复

4.15.1 加密密钥的托管与恢复

证书用户的加密密钥由 KMC 管理中心托管备份，当证书用户需要恢复加密密钥时，由山东 CA 通过 KMC 为用户取得相应的加密密钥。加密密钥被加密存放在 KMC 管理中心。

4.15.2 注意

为保证用户签名私有密钥的安全性，山东 CA 不保管签名私有密钥。因此，要求用户妥善保管，对 WEB 站点证书签名私有密钥的备份由用户自行完成。由于签名私有密钥遗失所造成的损失由证书用户自己承担。山东 CA 概不负责。

第五章 设备、管理与操作安全控制

5.1 物理安全控制

5.1.1 机房安全

➢ 机房基本情况

山东 CA 主机房位于济南市区，分为七层安全级别，其中第一层、第二层是监控和管理机房（山东 CA Network Operation Center，简称 NOC）的物理通道。山东 CA 还将在济南以外的地区建立异地备份中心。所有机房的建设和管理严格按照山东 CA 的规定要求，采用高安全性的监控技术，包括视频实时监测、指纹、身份识别卡等监控技术，以确保物理通道的安全。机房内部一律禁止参观，只有经过山东 CA 授权的人员才能进入授权的部门和工作地点。在进入山东 CA NOC 时，必须经过身份识别。NOC 实行全年 24 小时自动监控。

➢ 监控记录

监控记录文件包括对 NOC 通道上的所有踪迹的记录。山东 CA 的员工经授权后，两人以上才能进入 NOC。对于要进入 NOC 的来访者，要经山东 CA 运营安全管理小组批准后，指定并授权一位山东 CA 的员工陪同。

➢ 受理点网络系统保护

所有山东 CA 受理点的网络系统也必须受到保护，确保只有经授权的员工才能进入受理点的系统。山东 CA 的管理员负责设置和检查受理点管理员的权限。受理点操作员的权限和责任在受理点协议中已作出了规定。

➢ 根证书的安全

山东 CA 根证书和山东 CA 的证书持有者保证根证书的安全，根证书对应的私有密钥受到严格的保护。

5.1.2 电源和空调

山东 CA 系统采用双电源供电，在单路电源中断时，可以维持系统正常运转。同时，使用一个不间断电源（UPS），避免电源波动。

山东 CA 系统使用中央空调和冷却设备。

山东 CA 对电源，空调等要求，按照电信设施管理的规定严格要求，并且每年对是否符合要求进行检查。

5.1.3 防水

山东 CA 在机房建设时已采取相应措施，防止水侵蚀，充分保障系统安全。

5.1.4 防火

山东 CA 通过与专业防火部门协调，实施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。

5.1.5 存储介质保护

存储介质必须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。具体的要求在山东 CA 的技术标准和规程中作出了规定。

5.1.6 过期数据处理

当电子认证服务机构保存的相关数据已不再需要或存档的期限已满时，山东 CA 将完全销毁这些数据。

所有处理行为将记录在案，以供审查的需要，销毁行为遵守我国的法律。

5.1.7 异地备份介质

山东 CA 将提供异地的备份。异地备份介质安全要求应符合山东 CA 备份标准和程序。

5.2 流程安全控制

5.2.1 职位分配

山东 CA 明确执行 CA 系统的关键职能职位，他们包括：

- 山东 CA 运营安全管理小组

  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）要定期对 CA 中心安全问题进行讨论，对于安全问题提供相应的解决方案；

  4）能够及时地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；

  8）开发并维护山东 CA 中心电子认证业务规则；

  9）确保山东 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；

  10）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；

  11）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/Authority 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 安全策略；
  2）增加和减免其他安全官员，管理员，及山东 CA 用户；
  3）对于敏感操作的授权，诸如增加和减免安全官员及管理员；
  4）管理交叉认证，发布山东 CA 交叉认证协议，更新及注销交叉认证；处理审计日志；
  5）享有山东 CA 所有管理员的特权；
  6）管理 CRL、证书模板的制定。

- 山东 CA 录入员（SOO：System Operation Operator）
  1）负责用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，充分考虑安全的牵制和约束。山东 CA 对受理点的责任进行合理划分，并在系统、技术实现以及管理的责任义务上保证。

5.2.2 每一项任务需要的人数

山东 CA 确保单个人不能接触、导出、恢复、更新、废止山东 CA 的 CA 系统存储的根证书对应的私有密钥。

至少两个人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，进行 CA 系统中密钥恢复的操作。

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。

5.2.3 安全令牌控制

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：

- 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。

5.3 人事安全控制

5.3.1 人员背景审查

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、技术、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。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。受理点责任单位可以在此基础上，增加考察和培训条款，但不得违背山东 CA 证书受理的规程和山东 CA 电子认证业务规则。

山东 CA 确立流程管理规则，据此 CA 员工受到合同和章程的约束，不许泄露山东 CA 证书服务体系的敏感信息。所有的员工与山东 CA 签定保密协议，合同期满以后 3 年内仍然不得从事与山东 CA 相类似的工作，报第三方公证。

5.3.2 背景审查的实现

山东 CA 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。

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；
- 山东 CA 质量控制体系；
- 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。

5.3.4 继续培训要求

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。

5.3.5 岗位分离

山东 CA 负责 CA 系统运行的员工和负责 CA 系统设计、开发、维护的员工承担不同的职责，双方的岗位互相分离，即开发员工和运行员工分离的原则。为了保证安全，后者不能成为前者。

5.3.6 未授权行为的制裁

当山东 CA 员工进行了未授权或越权操作，山东 CA 在确认后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 系统抢修的要求

山东 CA 在系统遇到紧急情况需要联合抢修时，应至少有壹名山东 CA 安全事务专员在场，抢修人员在运行人员的陪同下，所有操作、修改都留记录。

非山东 CA 员工因物理修理、消防、强电故障等情况，需要进入山东 CA 数据中心实施修理时，必须报安全事务专员，经同意后，认证修理者的身份，由山东 CA 规定的可信任员工始终陪同和监护，完成约定部位的修理。

5.4 日志审计

5.4.1 记录事件种类

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，无论是手写、书面或电子文档形式，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 记录其它与 CA 系统本身不相关的事件，例如：物理通道参观记录、人事变动等。

5.4.2 审查的频率

山东 CA 每周对记录进行审查，对审查记录行为备案。

5.4.3 审查记录的保存期限

山东 CA 在数据库保存审查记录至少两个月，离线存档至少七年。

5.4.4 审查记录的保护

山东 CA 执行严格的通道管理，确保只有山东 CA 授权的人员才能接近这些审查记录。这些记录处于严格的保护状态，并且有异地备份，严格禁止访问、阅读、修改和删除等操作。

5.4.5 审查记录备案步骤

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 审查采集系统（内部和外部）

山东 CA 审查采集系统涉及：

- 证书管理系统；
- 证书签发系统；
- 证书目录系统；
- 远程通信系统；
- 证书审批受理系统；
- 应急反应系统；
- 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。

山东 CA 全天候准备上述系统的检查管理和审查工具。在需要的时候，山东 CA 会随时应用这些工具来满足各项审查的要求。

5.4.7 对攻击者的处理

山东 CA 对审查中发现的攻击现象将做详细记录，在法律许可的范围内追溯攻击者，并保留采取相应对策措施的权利，如：切断对攻击者已经开放的服务、递交司法部门处理等措施。

山东 CA 有权决定是否通知在审查中发现的攻击者或肇事者。如果是个人系统或应用程序使用第 5.4.6 中的系统引发的事件，又被山东 CA CSF 的审查系统记录下来的，山东 CA 没有义务通知他们。

5.5 归档策略

5.5.1 记录的事件类型

山东 CA 会对 CA 的数据库定期存档，间隔时间由山东 CA 自行决定，存档的内容包括山东 CA 发行的证书和 CRL、审查数据记录、证书申请审批资料等。(签名私有密钥由实体本身保存，有关私有密钥的责任由实体本身承担)。

5.5.2 存档的保留期限

山东 CA CSF 中的存档期限一般规定为七年。

5.5.3 档案的保护

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接近它们。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 存档备份

所有存档文件的数据库除了保存在山东 CA 的主要存储库，还将在异地保存其备份。存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有授权的工作人员才能在监督的情况下，对档案进行读取操作。山东 CA 在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

5.5.5 为记录加上时间标识

所有 5.5.1 条款所述的存档内容都要加时间标识。

5.5.6 档案收集系统（内部或外部）

山东 CA CSF 中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 验证档案信息

山东 CA 每年会验证存档信息的完整性。

5.6 密钥转换

5.6.1 密钥转换定义

在这里密钥转换是指当山东 CA 根证书到期而需要更换根密钥对时所采取的措施。山东 CA 根密钥对由加密机产生。证书到期更换密钥时将签发 3 张证书。

- 使用旧的私有密钥对新的公钥及信息签名生成证书；
- 使用新的私有密钥对旧的公钥及信息签名生成证书；
- 使用新的私有密钥对新的公钥及信息签名生成证书。

通过以上 3 张证书达到密钥更换的目的，使新旧证书之间互相认证、信任。

5.6.2 根证书有效期

山东 CA 根证书有效期为 10 年。在山东 CA 证书到期之前，山东 CA 将对根私有密钥进行更换。密钥转换程序在旧密钥对向新密钥对的转换起着过渡的作用。山东 CA 密钥转换采用以下方式：

- 山东 CA 将在证书到期前的 60 天内停止颁发新的证书；
- 旧的山东 CA 证书到期后，山东 CA 将用新的 CA 密钥对签发证书。

5.6.3 CRL

新的山东 CA 将继续使用旧的 CA 根私有密钥签发的 CRL，直到由旧的 CA 根私有密钥签发的证书到期为止。

5.7 灾难恢复

灾难恢复情况如下：

- 山东 CA 遭到攻击，造成灾难时的恢复；
- 山东 CA 遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，山东 CA 将按照灾难恢复计划实施恢复。具体由山东 CA 灾难恢复计划决定；
- 根证书公钥被作废；
- 当山东 CA 证书被作废时，山东 CA 应根据本电子认证业务规则相关规定通知证书持有者，证书将被作废；
- 根私有密钥被攻破；
- 当山东 CA 的根私有密钥作废时，山东 CA 应根据山东 CA 灾难恢复计划规定的灾难恢复步骤进行操作；
- 自然灾难或其他灾难后采取的安全措拖；

- 按照山东 CA 灾难恢复计划实施。

5.8 CA 或 RA 业务终止

5.8.1 CA 终止原因

CA 终止事件的原因可以分为密钥受损原因和非密钥受损原因。

5.8.2 终止通知

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。

5.8.3 终止归档

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。

5.8.4 终止措施

在 CA 中止期间，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；
- 证书注销；
- 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；
- 管理山东 CA 系统管理员和山东 CA 安全官员；
- 处理加密密钥；
- 处理和存储敏感文档；
- 清除 CA 主机硬件。

5.8.5 RA 的终止根据

根据山东 CA 与 RA 签订的协议终止 RA 的业务。

第六章 认证系统技术安全控制

6.1 密钥对的产生和安装

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，确保密钥对的产生、传送、安装等具备保密性、完整性和不可否认性。

6.1.1 密钥对的产生

- 加密密钥对

  加密密钥对是由中华人民共和国国家密码管理委员会办公室（以下简称国密办）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，由山东省国家密码管理委员会办公室所属的 KMC 控制管理。

- 签名密钥对

  签名密钥对由客户端产生，证书申请者可使用山东省国家密码管理委员会办公室认可的、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。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用户自己产生，用户应妥善保管。

- 山东 CA 在技术、流程和管理上保证密钥对产生的安全性。

6.1.2 私有密钥的传递

证书用户的加密私有密钥是在 KMC 产生的，该私有密钥只保存在 KMC。在加密私有密钥从 KMC 到用户的传递过程中采用国密办许可的对称密钥算法加密。山东 CA 无法获得，保证了证书用户的密钥安全。

6.1.3 公钥的传递

山东 CA 从 KMC 取得用户公钥后为其签发证书，在此过程中也采用国密办许可的对称密钥算法加密，保证传输中数据的安全。

6.1.4 CA 公钥的传递

山东 CA 的根公钥包含在山东 CA 自签的根证书中。证书用户可以从山东 CA 的网站上下载山东 CA 根证书。

6.1.5 密钥长度

山东 CA 所使用的密钥对长度支持 RSA 1024 位。

6.1.6 公钥参数的产生

公钥参数由国密办许可、山东 CA 数字证书签发系统支持的硬件产生。

6.1.7 密钥用途

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。

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

6.1.8 公钥的存档

公钥属于安全数据，由山东省国家密码管理委员会办公室所属的 KMC 定期存档、管理。

6.1.9 证书与密钥对的有效期限

山东 CA 根证书有效期为 10 年，用户证书由于考虑到安全性，目前提供的证书有效期一般为一年，但系统支持在根证书有效期内的任意期限，最短可定制到一天。

6.2 私有密钥保护与密码模块的控制

6.2.1 密码模块标准与控制

山东 CA 使用国密办许可的产品，密码模块的标准符合国家规定的要求。

6.2.2 私有密钥的分割管理

山东 CA 采用多人控制策略激活、使用、停止山东 CA 的签名密钥。

6.2.3 私有密钥托管

KMC 可以根据客户和法律的需要，对加密密钥进行托管。签名私有密钥从不进行托管，以保证其不可否认性。

6.2.4 私有密钥备份

证书的持有者可以备份他们的私有密钥，以确保这些私有密钥的安全。

KMC 备份托管的加密私有密钥，确保加密私有密钥的安全。

6.2.5 私有密钥存档

KMC 提供过期的托管私有密钥的存档服务。

6.2.6 私有密钥的导入/导出

在山东 CA 证书服务体系中，使用山东 CA 的软件可以把私有密钥导入密码模块中。

私有密钥无法从硬件及软件密码模块中导出。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有密钥进行加解密操作。

6.2.7 私有密钥的保存

证书的持有者可以将私有密钥保存在硬件密码模块中，也可以保存在软件密码模块中。

山东 CA 的签名私有密钥必须保存在硬件密码模块中。

6.2.8 激活私有密钥

在山东 CA 证书服务体系中，必须通过密码验证后，方可激活私有密钥。

6.2.9 停止私有密钥

在山东 CA 证书服务体系中，通过终止程序来停止私有密钥，并且把私有密钥从内存中清除。

6.2.10 销毁私有密钥

凡用户需要销毁私有密钥，应通知山东 CA，由 KMC 进行销毁。

6.3 敏感数据的保护

6.3.1 敏感数据的产生

敏感数据包括山东 CA 提供的证书私有密钥口令、被加密的数据等。山东 CA 提供唯一的不可猜测的证书私有密钥口令。这些私有密钥口令由山东 CA 根据授权和操作的许可实施批准并且仅发放给授权用户。

6.3.2 敏感数据的保护

山东 CA 采取加解密机制等多种方式保护敏感数据，以避免为授权的使用。未授权 用户企图使用敏感数据达到预定的数目时，敏感数据会自动锁定。

6.4 计算机安全控制

6.4.1 计算机安全性要求

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；其它普通用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。

6.4.2 计算机的安全等级

山东 CA 使用的密码设备是通过国密办批准生产的密码设备。

6.5 系统升级与相关安全性控制

6.5.1 系统升级控制

山东 CA 的软件设计和开发过程遵循以下原则：

- 第三方的验证和审核
- 安全风险和可靠性设计

6.5.2 安全性管理控制

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。

6.6 网络安全性控制

山东 CA 有防火墙以及其他访问控制机制保护，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。所有授权用户必须有合法的安全令牌，并且通过密码验证。

6.7 数字时间戳

数字时间戳（DTS：Digital Time Stamp）是对时间信息的电子签名，主要用于实现确定在某一时间某个文件确实存在和确定多个文件在时间上的逻辑关系功能。

第七章 证书、CRL 及 OCSP 结构

7.1 证书

山东 CA 签发的证书均符合 X.509V3 证书格式。遵循 RFC3280 标准。

7.1.1 证书版本号

- X.509：V3

7.1.2 证书标准项

- 证书序列号

  唯一标识该证书的一组 32 位字符。
- 证书有效期

  证书的起止时间。
- 主题

  为证书用户申请证书时所填写的申请信息。即用户的甄别名。详细请参看第 3.1 节。
- 发行者

  CN = SDCA Root Authority

  C = CN

7.1.3 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。
- 密钥使用

  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。
- 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，如最终用户等。
- CRL 发布点

  由山东 CA 定义的 CRL 发布点。如：

  Directory Address：

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

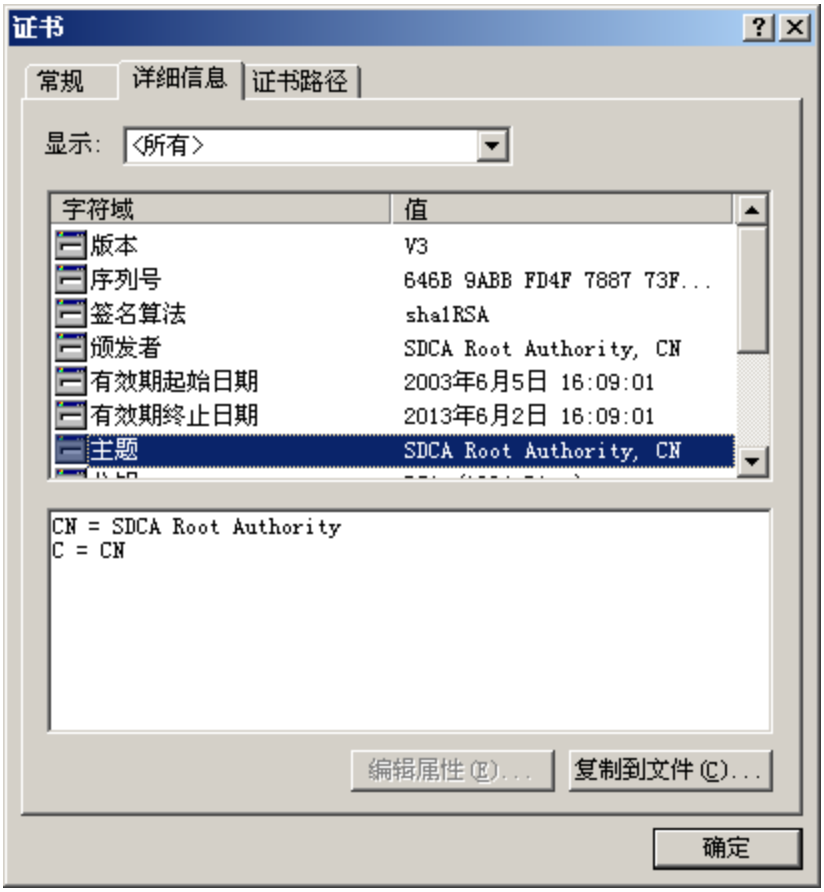
7.1.4 命名格式

采用 X.500 甄别名格式，详看第 3.1 节。

- 策略标识

  暂无。

- 示图



7.2 CRL

山东 CA 定期签发 CRL（证书废除列表），其所签发的 CRL 遵循 RFC3280 标准。采用 X.509V2 格式。

7.2.1 CRL 版本号

- X.509：V2。

7.2.2 CRL 项

- 颁发者

  CN = SDCA Root Authority

  C = CN

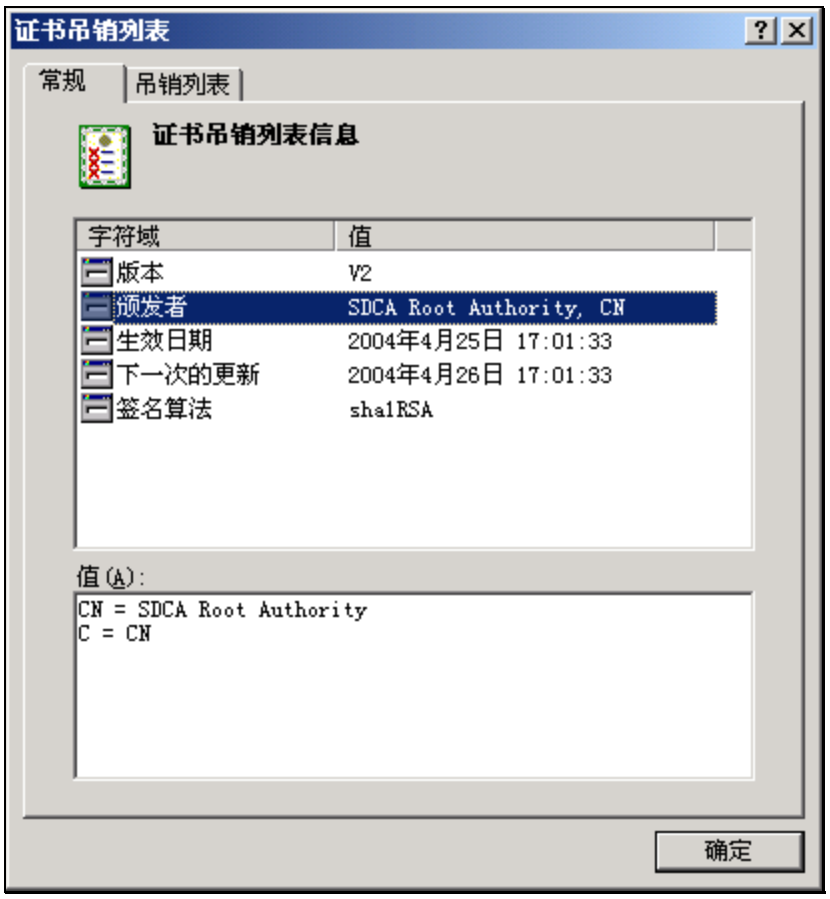
- CRL 发布

山东 CA 每隔 24 小时自动发布最新的 CRL。

- 签名算法

  山东 CA 采用 sha1RSA 签名算法。

7.2.3 示图



7.2.4 CRL 下载

山东CA证书用户可以通过山东CA网站http://www.sdca.com.cn/下载CRL。

7.3 OCSP

山东 CA 为证书用户提供 OCSP（在线证书状态查询服务），OCSP 为 CRL 的有效补充，方便证书用户及时查询证书状态信息。山东 CA OCSP 服务遵循 RFC2560 标准。

7.3.1 OCSP 版本号

- OCSP：V1。

7.3.2 OCSP 扩展

- 暂无。

7.3.3 OCSP 查询

山东CA证书用户可以通过山东CA网站Http://www.sdca.com.cn/在线查询证书

状态。

第八章 认证机构审计与评估

8.1 审计的频率与环境

8.1.1 山东 CA 的审计

由山东 CA 或法律主管部门指定审计者。审计者对山东 CA 进行审计。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。

8.1.2 山东 CA 对关联单位的审计

山东 CA 对其关联单位实行定期审计（一般为 1 年）。审计人员由山东 CA 指派。审计人员必须熟悉山东 CA 的规范和信任服务的相关知识，了解保证安全的基本知识，按照山东 CA 的规范、协议、履行责任业务等情况，独立、公正地对关联单位作出合格或不合格的结论。

山东 CA 可以根据协议对下属的关联机构和单位进行安全审计，有权根据上级的审计结果和自己的审计结果，取消对下属单位的授权或重新授权。

山东 CA 的关联单位，一年被审计的次数一般情况下为一次，特殊情况也不得超过 2 次。上级机构和单位，不得对下属单位和机构重复审计和重复收费。审计结果根据被审计单位的要求而决定是否公布。

山东 CA 对关联单位的审计将收取审计费。审计费用在山东 CA 与关联单位的协议书中体现。

8.2 审计者的身份与资质

8.2.1 山东 CA 的内部审计

内部审计组织为山东 CA 运营安全管理小组，主要是审查实际运营操作是否与山东 CA CPS V2.0 中规定的一致。

8.2.2 山东 CA 的外部审计

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：

- 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 审计者与山东 CA 的关系

8.3.1 审计者与山东 CA 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。

8.3.2 审计报告与山东 CA 的关系

山东 CA 不是这些审计报告的作者，所以对其内容不负任何责任，同时山东 CA 也不对这些审计报告发表任何观点，也不会对由于信任审计报告中有关山东 CA 的内容而导致的任何损失负责。

8.4 审计内容

对山东 CA 规范审计应包括：

- 山东 CA 支持的证书认证操作规程是否完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 审计结果

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，向山东 CA 关联单位（例如垫付商、注册机构、注册分支机构、受理点）通知审计结果的具体规定将在山东 CA 和关联单位的协议中写明。

8.6 不足信息的处理

如果在审计过程中发现执行规范有不足之处，山东 CA 将根据审计报告的内容准备一份解决方案，明确对此采取的相应行动。山东 CA 将根据普遍认可的国际惯例或监管法律迅速解决问题。

第九章 法律责任和其他业务条款

9.1 费用

9.1.1 费用支付

山东 CA 对证书持有者和所有使用山东 CA 的各方（山东 CA 体系的关联单位包括山东 CA 注册机构、注册分支机构、证书制作受理点等）收取服务费用。证书持有者和山东 CA 关联单位有义务根据山东 CA 的价目表支付给山东 CA 费用。

9.1.2 证书费用

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七天后生效。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。费用的变化包括：

- 证书认购的费用——根据山东省物价局收费文件及山东 CA 的价目表；
- 证书更新的费用——根据山东省物价局收费文件及山东 CA 的价目表；
- 密钥更新的费用——根据山东省物价局收费文件及山东 CA 的价目表；
- 证书废止的费用——根据山东省物价局收费文件及山东 CA 的价目表；
- 证书恢复的费用——根据山东省物价局收费文件及山东 CA 的价目表；
- 其他与证书相关的费用——根据山东省物价局收费文件及山东 CA 的价目表。

退款政策——山东 CA 数字证书一旦发放，山东 CA 不办理退证、退款手续。

9.2 支付能力

山东 CA 授权的发证机关（如注册机构、注册分支机构、受理点等）应具有维持其运作和履行其责任的经济实力，它应该有能力承担对订户、接收方以及其他信任其签发的证书和时间戳的人造成的责任风险，除非获得山东 CA 的书面同意，发证机关应该购买针对可能产生的错误和疏忽的责任保险。

9.3 商业信息的保密

9.3.1 保密的商业信息

山东 CA 与山东 CA 授权的发证机关之间、山东 CA 与证书持有者之间、山东 CA 授权的发证机构与证书持有者之间的协议、往来函和商务协定等，除非法律明确规定，一般不能在未经另一方许可的前提下擅自公开。

对山东 CA 或山东 CA 对发证机构的审计报告、审计结果等相关信息是保密信息，除了山东 CA 授权和信任的员工，不能泄露给其他任何人。这些信息除了用于审查目的或法律规定的目的外，不能用于其他用途。

有关山东 CA 电子认证服务机构运作的信息只能在严格指定的情况下，才能传授给山东 CA 授权的员工。

突发事件的应对计划和灾难事件的恢复计划。

控制发证机关软硬件操作的安全措施和管理证书服务及注册服务的安全措施。

除非法律明文规定，山东 CA 没有义务公布或透露证书持有者证书以外的信息。

9.3.2 非保密的商业信息

与证书有关的申请流程、申请需要的手续、申请操作指南等书中公布的信息是可以公开的。而且山东 CA 在处理申请业务时可利用这些信息，包括发布上述信息给第三方。

山东 CA 在山东 CA 的目录服务器中公布证书的作废信息，供网上查询。

当山东 CA 在任何法律、法规或规章条款的要求下，或在法院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法院的判定的要求，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 个人信息的保密

9.4.1 保密的个人信息

与证书持有者证书公钥配对的私有密钥是保密的，证书持有者应该认真保管，不能公布给他人。如果证书持有者擅自泄露私有密钥，则由此引起的后果由证书持有者自负。

存在于 CA、RA、和数据库中，在申请证书时提供的私人信息，无论该申请是否被批准。

9.4.2 非保密的个人信息

与证书持有者证书相关的信息，证书的相关信息是可以公开的，通过山东 CA 目录服务等方式向外公布。

证书被作废/暂停使用的信息披露。

向法律执行机关披露。

当保密信息的所有者出于某种原因，要求山东 CA 公开或披露他所拥有的保密信息，山东 CA 应满足其要求。如果这种披露保密的行为涉及或有可能引起对任何其他方的赔偿义务，山东 CA 有权拒绝其请求，且不应承担任何与此相关的或由于公开保密信息引起的损失和损坏的赔偿责任。保密信息的所有者应负责山东 CA 与此相关的或由于公开保密信息引起的所有损失、损坏的赔偿责任。

9.5 知识产权

山东 CA 享有并保留对证书以及山东 CA 提供的全部软件的独一无二的一切知识产权，包括保证证书和软件的完整权、名称权和利益分享权等。因此，山东 CA 有权决定关联机构采用什么软件系统，选择采取的形式、方法、时间、过程和模型，以便保证系统的兼容和互通。

按本电子认证业务规则的规定，所有与山东 CA 发行的证书和山东 CA 提供的软件相关的一切版权、商标和其他知识产权均属于山东 CA 的产权，这些知识产权包括所有相关的文件和使用手册。电子认证服务机构在征得山东 CA 的同意后，可以使用相关的文件和手册，并有责任和义务提出修改意见。

在没有山东 CA 预先书面同意的情况下，任何使用者不能在任何证书到期、作废或终止后，使用或接受任何山东 CA 使用的名称、商标、交易形式或可能与之相混淆的名称、商标、交易形式或商务称号。

9.6 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，用户必须接受本电子认证业务规则的约束。在山东 CA 与包括用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。

9.7 免责

山东 CA 不对由于不可抗力造成的操作失败或延迟承担任何损失、损坏或赔偿责任。

山东 CA 在提供给证书持有者的“山东 CA 数字证书用户责任书”中，都有事先告知证书持有者的免责条款的规定：山东 CA 发放的各类型数字证书只能用于网络上

标识身份、加密数据、保证网络安全通讯等相应证书规定的用途，不能作为其他任何用途。若证书持有者将其数字证书用于其他的用途，山东 CA 不承担任何责任。

山东 CA 在进行申请者身份认证或证书制作时，将充分遵守山东 CA 的安全操作流程。如果由于非山东 CA 的原因而造成的山东 CA 设备故障、线路中断，导致签发数字证书错误、延误、中断或者无法签发，山东 CA 不负任何赔偿责任。

山东 CA 在签发数字证书之前，证书申请者已同意遵守“山东 CA 数字证书用户责任书”中的各项规定。用户责任书中明确规定山东 CA 不承担任何形式的担保和义务。如果证书申请者故意或无意地提供不完整、不可靠或已过期的信息，而又根据正常的流程提供了必须的审核文件，由此得到了山东 CA 签发的数字证书，由此引起的法律和经济责任由证书申请者全部承担，山东 CA 不承担与证书内容相关的法律和经济责任，但可以根据受害者的请求提供协查帮助。山东 CA 也不承担任何其他未经授权的人或组织以山东 CA 名义编撰、发表或散布不可信赖的信息所引起的法律责任。山东 CA 仅仅提供电子沟通或交易中签名的“不可抵赖”的依据，但并不表明有对此承担法律责任等方面的约定。

9.8 责任范围

9.8.1 CA 的责任

山东 CA 应承担的唯一和绝对的责任和义务是：

- 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 的签名私有密钥在山东 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。

9.8.2 注册机构的职责

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第三章。

9.8.3 注册分支机构的职责

同注册机构的职责。

9.8.4 受理点的职责

同注册机构的职责。

9.8.5 证书持有者的职责

所有的证书持有者必须严格遵守关于证书申请以及私有密钥的所有权和安全保存相关的程序：

- 证书持有者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；
- 证书持有者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；
- 证书持有者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，还需遵守证书持有者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，如证书持有者遗失私有密钥、遗忘或泄密以及其他情况，证书持有者应立刻通知山东 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。

9.9 理赔

9.9.1 山东 CA 承担责任的限制

如山东 CA 违反了前文第 9.8 款条例规定的职责，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 所有的赔偿义务不得高于这种证书适用的赔偿责任上限。
  赔偿责任上限为该种证书签发费、管理费和应用服务费总和的拾倍，最高不超过伍万元人民币。
  证书签发费、管理费、应用服务费按山东省物价局核准颁发的《收费许可证》中的规定执行。

- 山东 CA 只有在山东 CA 证书有效期限内承担损失损害赔偿。

9.9.2 注册机构承担责任的限制

注册机构的责任在注册机构和山东 CA 之间签订的注册机构协议中表明。

9.9.3 注册分支机构责任的限制

注册分支机构的责任在注册分支机构和山东 CA 之间签订的注册分支机构协议中表明。

9.9.4 受理点承担责任的限制

受理点的责任在受理点和山东 CA 之间签订的受理点协议中表明。

9.10 有效期和终止

本 CPS 中已详细注明版本号及生效日期，新版本在对外发布后 15 日正式生效，自生效之日起，旧版本自动失效。山东 CA 需要终止本 CPS 或其中某些部分时，将在公司网站上进行公布，对具体某方不再做另行通知。

9.11 信任体间的责任关系

9.11.1 信任体和证书持有者的赔偿责任

第一：信任体和证书持有者在使用或信赖证书时，若有任何行为或疏漏而致使山东 CA、山东 CA 授权的发证机构产生损失，信任体和证书持有者应承担连带赔偿的责任、相应的损失及诉讼、仲裁等费用。山东 CA 及山东 CA 授权的发证机构有权要求赔偿。

第二：证书持有者的责任并不仅限于本电子认证业务规则的规定，证书持有者如果向第三方传递信息时表述有误，而第三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，证书持有者必须对这种行为的后果负责。

第三：证书持有者接受证书就表示同意在以下情况下承担赔偿责任：

- 证书持有者（或由证书持有者授权，按证书持有者指示行事的人）对事实表达有误或曲解时；
- 证书持有者没有公开一项实质性的事实，而且造成这种错误或遗漏的原因是出于他的疏忽或是他有意欺瞒山东 CA、山东 CA 授权的发证机构或其授权的其他代理机构和山东 CA 签约单位时；
- 证书持有者没有采取必要的防护措施来防止私有密钥的遗失、泄密、被修改或被未经授权的人使用时。

第四：当一个证书应证书持有者的代理人要求被签发后，代理人和证书持有者

两者负有连带责任。如出现第三中所述的情况，他们负共同赔偿责任。证书持有者有责任就代理人所做任何不实陈述与遗漏，通知山东 CA 或山东 CA 授权、代理的机构。

9.11.2 信托关系

电子认证服务机构与证书持有者和信任体之间的关系不存在代理和信托关系。证书持有者和信任体都没有权利以合同形式或其他方法让山东 CA 承担信托责任。

9.12 修订

山东 CA 有权在合适的时间修订、修改和改变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、修改和改变在公布后立刻生效。证书持有者如不在修改结果后公布的限定时间内申请废止证书，就视为同意这种修正、修改和变化。所有以书面形式提供给证书持有者的内容，按以下规则发送：

- 接受者是公司或其它单位组织则向其登记的联系地址或办公室发送信息；
- 接受者是个人则向其申请书上规定的地址发送；
- 这些通知可能用快递或挂号信的方式发送。山东 CA 有权选择通过电子邮件或其他方式向证书持有者发送通知，邮件地址在证书持有者申请证书时已注明。

所有发送给山东 CA 的通知应以书面形式传递。所有这些通知应采用快递或挂号信的方式发送。若通过电子邮件方式发送通知给山东 CA，则这种通知只有在山东 CA 收到证书持有者的电子邮件通知后 24 小时内，收到证书持有者书面确认材料，方为有效。

9.13 修订程序

1）发现 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；
2）将现存问题反馈 CPS 编写小组；
3）经过 CPS 编写小组讨论后，提出具体的修改意见；
4）修改意见提交运营安全管理小组；
5）运营安全管理小组审查修改意见，如果不通过则提出修改见反馈 CPS 编写小

组；

6）CPS 修改意见经运营安全管理小组审查通过，由 CPS 编写小组发布更新。

9.14 争议解决

如果当事人之间无法很好的解决出现的问题和争端，应该提交仲裁机构（约定为“济南仲裁委员会”），根据仲裁条例在时效内裁决。仲裁的决定是终决性的，对每个当事人都有约束力。

9.15 监管法律

本电子认证业务规则在各方面服从中华人民共和国法律的管制和解释。

9.16 适用的法律

无论合同或其他法律条款的选择及无论是否在中国建立商业关系，山东 CA 电子认证业务规则的执行、解释、翻译和有效性均适用中华人民共和国和法律。法律的选择是确保对所有订户有统一的程序和解释，而不管他们在何地居住以及在何处使用证书。

9.17 其他规定

9.17.1 各种规范的冲突

若本电子认证业务规则的规定与其他规定、指导方针相互抵触，用户必须接受本电子认证业务规则的约束，除非本电子认证业务规则的规定在法律所禁止的范围内，或有关规定、指导方针明确地言明优于本电子认证业务规则。

9.17.2 安全资料的财产权益

下列与安全相关的资料视为下列指定的当事人所拥有：

- 证书：证书的权利行使受山东 CA 的管理约束。本规范旨在保护用户的隐私，避免未经授权者公布其证书；
- 电子认证业务规则：本电子认证业务规则的产权为山东 CA 所有；
- 甄别名：甄别名归命名实体所有(或他们的雇主和负责人所有)；
- 私有密钥：不论该密钥是以何种实体媒介存放或保护，私有密钥为合法使用或有权使用该密钥用户（或其雇主或委托人）所有；
- 公开密钥：不论该密钥以何种实现媒介存放或保护，公开密钥为用户（或其雇主或委托人）所有；
- 山东 CA 的公开密钥：山东 CA 作为自身的根节点的公开密钥，是山东 CA 的财产。这个公钥由山东 CA 授权分配，放在值得信任的硬体或软件上。

9.18 补充说明

暂无。

第十章 定义与缩写

10.1 山东 CA

山东 CA（山东省数字证书认证中心、SDCA）是山东 CA 认证体系的根，由山东 CA 派生出山东 CA 认证体系和电子认证服务机构。目前山东 CA 由**山东 CA** 负责运营。

10.2 山东 CA 认证委员会

由山东 CA 牵头，由加入到山东 CA 认证体系的各地区、各行业单位代表组成，旨在协调各地区、行业之间的相互关系，统一布局山东 CA 的认证服务市场，制订山东 CA 认证体系的政策和标准，研究和开发山东 CA 认证体系的关键技术，解决争议和纠纷，共同推进电子政务公共服务、电子交易市场。山东 CA 认证委员会是各地各行业实体的联合体。

10.3 电子认证服务机构

山东 CA 及下层机构统称为电子认证服务机构。

10.4 注册机构

CA 注册机构（Registration Authority），简称 RA。与山东 CA 签署注册机构协议，被山东 CA 授权发行山东 CA 证书的代理机构。注册机构负责处理证书申请者提出的证书申请信息，并提交 CA。

10.5 注册分支机构

CA 注册分支机构，简称 LRA。与山东 CA 签署注册分支机构协议，被山东 CA 授权发行山东 CA 证书的代理机构，隶属于注册机构。功能同 CA 注册机构。

10.6 受理点

与山东 CA 签署受理点协议，被山东 CA 授权发行山东 CA 证书的代理机构，其功能比注册机构小。

10.7 发证机构

包含山东 CA 授权的注册机构、注册分支机构、受理点证书发放机构。发证机构为证书申请者发放山东 CA 证书。

10.8 山东 CA 运营安全管理小组

由山东 CA 任命的负责山东 CA 安全策略的制定以及执行的组织。

10.8 山东 CA 超级管理员

负责实施 CA 政策、增加新 CA 超级管理员、管理 CA 系统管理员、验证审计记录、电子认证业务规则的执行情况承诺，批准安全令牌的发放，是系统的最高层管

理者。

10.9 山东 CA 系统管理员

负责安装、配置和维护 CA 系统的软硬件系统，负责 CA 服务器的启动和中止，管理 CA 的操作员。

10.10 山东 CA 录入员

负责录入证书申请者提交的信息，协助客户办理数字证书申请、作废、更新等手续。

10.11 山东 CA 审核员

负责审核证书申请信息，协助客户办理数字证书申请、作废、更新等手续。

10.12 山东 CA 审计员

CA 审计员（Auditor）负责 CA 系统的证书统计，日志备份、恢复，日志审核的工作。

10.13 山东 CA 证书制作员

负责为证书申请者下载制作证书，并提交给用户。

10.14 安全令牌

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情况，发放需要的系统操作卡、身份识别卡、智能密码钥匙、指纹、登录密码、操作证书、作业帐号等，山东 CA 称之为安全令牌。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。安全令牌由山东 CA 的安全事务专员审批。

10.15 山东 CA 数字证书签发系统

为山东 CA 证书申请者签发、管理数字证书的软件系统。

10.16 山东 CA 白皮书

山东 CA 白皮书是山东 CA 的一个支持山东 CA 数字证书相应政策的详细的操作声明和操作步骤。

10.17 山东 CA 灾难恢复策略

山东 CA 灾难恢复策略指山东 CA 在灾难发生时执行的计划和程序，可以由山东 CA 独立的审查员或管理者验证。

10.18 对象标识符（OID）

对象标识符（OID）由一组整数构成，可以方便地指派特定的目的，而且在所有 OID 的空间里有各自独一无二的特殊性，可以区别其他对象。

10.19 注册机构协议

一份合同，它详细地概括了山东 CA 指定的注册机构的程序、责任和义务。

10.20 注册分支机构协议

一份合同，它详细地概括了山东 CA 指定的注册分支机构的程序、责任和义务。

10.21 受理点协议

一份合同，它详细地概括了山东 CA 指定的受理点的程序、责任和义务。

10.22 信任体

信任体（Relying Party）指山东 CA CSF 中证书持有者，信任山东 CA 颁发的数字证书。

10.23 证书持有者

个人、集体、单位、组织、服务器或者其他拥有任何山东 CA 证书的人或实体。

10.24 证书申请者

证书申请者（Certificate Applicant）请求山东 CA 颁发证书的个人、企业、组织机构。

10.25 用户

用户（Subscribers）指由 CA 山东签发的各种类型证书的持有者。

10.26 终端用户

山东 CA 中的终端用户包括所有证书申请者、终端管理员和操作人员及要求数字证书验证和加密服务的系统和服务器。所有终端用户由山东 CA 授予证书，并且是证书的主体。终端用户可以使用山东 CA 授予的证书为其他终端用户加密信息，也可校验其他终端用户的电子签名。这样，终端用户也可是山东 CA 中的可信赖方。

10.27 非垫付商的受理点

执行受理点职能但不承担任何垫付商支付义务的受理点。

10.28 垫付商受理点

垫付商受理点（Sponsor RA）是一个受理点，执行受理点的职能并承担每个它所发放山东 CA 证书的支付义务。

10.29 垫付商

垫付商（Sponsor）承担每个证书所有支付义务的对象，它有权如证书政策所述管理这些山东 CA 证书。

10.30 证书申请

由证书申请者提交给山东 CA 的请求，山东 CA 根据此请求为用户颁发证书。

10.31 参考码

山东 CA 为证书申请者颁发证书时生成的 32 位字符组合。唯一标识证书申请。与授权码相对应。

10.32 授权码

山东 CA 为证书申请者颁发证书时生成的 32 位字符组合。与参考码相对应。

10.33 证书口令

证书口令指证书中私有密钥的保护口令。

10.34 证书序列号

唯一标识证书的 32 位字符组合。

10.35 甄别名

甄别名（Distinguished Name）简称 DN，包含用户的属性信息。

10.36 密钥管理中心

密钥管理中心简称 KMC，负责密钥的产生、存储、归档等管理工作。

10.37 OCSP

OCSP（Online Certificate Status Protocol），即**在线查询数字证书状态协议**，用于支持实时查询数字证书状态。

10.38 LDAP

LDAP（Lightweight Directory Access Protocol），即**轻量级目录访问协议**，用于查询、下载数字证书以及数字证书废止列表（CRL）。

10.39 PKI

PKI（Public Key Infrastructure），公开密钥基础设施。

10.40 CRL

CRL（Certificate Rovocation List），即**数字证书废止列表**的英文简称。CRL 中记录所有在原定失效日期到达之前被废止的数字证书的用户数字证书序列号，供数字证书使用者在认证对方数字证书时查询使用。CRL 通常又被称为数字证书黑名单。内容通常还包含 CA 机构的名称、发行日期、下次废止列表的预定发行日期、更新或废止的数字证书序号，并说明更新或废止的时间与理由。

10.41 认证

认证（Certification）指不同实体在进行网上交易之前，通过可信赖的、中立的第三方（如山东 CA）对身份进行审核，并由第三方出具证明证实其身份的可靠性和合法性的过程。

10.42 电子签名

电子签名，是利用公开密钥算法等方法保证信息传输过程中信息的完整和提供信息发送者的身份认证及不可抵赖性的一种技术。

10.43 私有密钥

私有密钥（Private Key），是一种不能公开、由持有者秘密保管的数字密钥，用于创建电子签名、解密报文或与相应的公开密钥一起加密机要文件。

10.44 公开密钥

公开密钥（Public Key），可以公开的数字密钥，用于验证相应的私有密钥签名的报文，也可以用来加密报文、文件，由相应的私有密钥解密。

10.45 签名密钥对

证书申请者申请证书时由客户端产生。主要用于用户的签名和验证。包含一对私有密钥和公开密钥。

10.46 加密密钥对

证书申请者申请证书时由 KMC 产生。主要用于用户信息的加解密。包含一对私有密钥和公开密钥。

10.47 PKCS

PKCS （Public Key Cryptography Standard），公开密钥密码算法标准。

10.48 HTTP

HTTP （Hypertext Transfer Protocol），超文本传输协议。