东方新诚信数字认证中心

电子政务电子认证服务业务规则

Ver 1.0

东方新诚信数字认证中心有限公司

二〇一二年四月

目录

1 概括性描述

1.1 概述

东方新诚信数字认证中心，简称“ 东方新诚信 CA ”（英文缩写为 DFCA）。东方新诚信 CA 面向全国市场，面向社会信息化、社会公共管理、基于互联网的在线服务等应用领域，提供证书管理、密钥管理等基础电子认证服务，提供涵盖“ 身份认证、授权管理、责任认证、数据安全 ”等扩展的电子认证应用支撑服务。

东方新诚信 CA 严格按照《中华人民共和国电子签名法》与《电子认证服务管理办法》的要求，遵循国家信息安全保障的总体政策要求，依据国家相关法律法规与标准规范，采用通过国家密码管理局鉴定的商用密码产品，使用创新的电子认证业务与服务模式，建立“ 东方新诚信电子认证系统 ”，面向社会信息化、社会公共管理、基于互联网的在线服务等应用领域提供安全、统一、有序的电子认证服务，解决应用系统的信息安全问题。

《东方新诚信数字认证中心电子政务电子认证服务业务规则》（以下简称为《电子认证服务业务规则》或“ DFCA-CPS ”）由东方新诚信 CA 根据《电子政务电子认证服务管理办法》，依据《电子政务电子认证业务规则规范》制定。

本《电子认证服务业务规则》详细阐述了东方新诚信 CA 在实际工作和运营中所遵循的各项规范，适用于东方新诚信 CA 及其员工、注册机构、证书申请方、订户和依赖方，各参与方须完整理解和执行《电子认证服务业务规则》所规定的条款并承担相应的责任和义务。

1.2 文档名称与标识

本文档名称是《东方新诚信数字认证中心电子政务电子认证服务业务规则》。

本文档版本 Version 1.0。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

东方新诚信 CA 是根据《中华人民共和国电子签名法》和《电子认证服务管理办法》规定，依法建设的第三方电子认证服务机构。

电子认证服务机构是受用户信任，负责创建和分配公钥证书的权威机构，是颁发数字证书的实体。

1.3.2 注册机构

注册机构（以下简称为“ RA ”）作为电子认证服务机构授权委托的下属机构，包括注册系统（RA 系统）和证书本地受理点，负责受理证书申请，负责对证书用户信息的审核、整理汇总、统计分析，负责与 CA 进行数据交换，实现各类证书业务的处理。

RA 有责任妥善保存与保管用户的数据，不允许将用户数据透露给与证书申请无关的任何单位或个人，不允许将用户数据用于商业利益方面的用途。RA 必须获得东方新诚信 CA 的授权，根据授权从事相关证书业务的办理。各类政府机构、企事业单位等均可申请成为东方新诚信 CA 的注册机构。

东方新诚信 CA 根据申请单位的性质、证书发展规模、场地和人员情况等，经过严格的评估审计，合格后由安全策略委员会最终决定，对其发放授权委托书，授权其成为注册机构。

1.3.3 订户

订户，即证书持有人，是指从东方新诚信 CA 接收证书的实体。包括已经申请并拥有东方新诚信 CA 签发的数字证书的单位、企业、组织、机构、个人、服务器、网站等各类主体或实体，以及其他任何具有确定的身份标识，并持有东方新诚信 CA 签发的数字证书的对象。

在电子签名应用中，订户即为电子签名人。

1.3.4 依赖方

依赖方是指任何使用东方新诚信 CA 签发的证书进行网络作业的证书持有者和按照 DFCA-CPS 合理信任证书真实性的任何实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个订户。

在东方新诚信 CA 的证书服务体系中，依赖方是信任东方新诚信 CA 所签发的数字证书（以下简称为“ 东方新诚信证书 ”），可以对使用东方新诚信数字证书机制生成的数字签名进行验证，使用其他东方新诚信证书的公钥的实体。依赖方可以在法律规定以及 DFCA-CPS 规定的范围内信任证书及其签名，并享有 DFCA-CPS 规定的各种权利。

对于依赖方，东方新诚信 CA 承诺，除了未经验证的用户信息外，证书中的或证书中合并参考到的所有信息都是准确的。

依赖方应合理地信任证书以及相关的数字签名。如果信任数字签名时需要额外的保证，依赖方必须得到这些保证后才能合理地信任该数字签名。

1.3.5 其他参与者

其他参与者是指其他为东方新诚信 CA 提供相关服务的实体。

1.4 证书应用

1.4.1 适合的证书应用

东方新诚信证书能够满足社会信息化、社会公共管理、基于互联网的在线服务等应用领域对电子认证服务的需要，例如，电子政务、电子商务、医药价格等应用。证书申请人根据实际需要，决定采用哪种类型的数字证书。

东方新诚信证书主要适合以下四方面的应用。

1. 身份认证

保证采用东方新诚信 CA 信任服务的证书持有者身份的合法性，主要包括对个人、机构和设备等网络实体的鉴别。

2. 电子签名

采用东方新诚信证书对信息进行电子签名，实现对信息的完整性保护，防止对信息的篡改。同时，还可实现提交信息的不可抵赖性。通过在电子签名时包含时间信息，还可形成时间戳签名，实现对关键操作的时间进行真实性验证。

3. 信息保护

对于信息化应用中存储与传输的重要信息、敏感信息，可以采用采用东方新诚信证书机制进行加密保护。

4. 权限管理

以东方新诚信证书作为用户身份认证的凭证，在此基础上，对用户进行分组划分，进而对其进行权限管理与访问控制。

1.4.2 限制的证书应用

限制东方新诚信证书应用的场合主要包括（但不限于）：

1. 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，由此造成的法律后果由用户自己承担；
2. 由于证书的使用可能导致人员死亡、伤残的情形；
3. 由于证书的使用可能导致环境破坏的情形。

违反本限制的证书应用要求所造成的法律后果由订户负责。

1.5 策略管理

1.5.1 策略文档管理机构

DFCA-CPS 的管理机构是东方新诚信 CA 安全策略委员会。由东方新诚信 CA 安全策略委员会负责对本 DFCA-CPS 的制定、发布、更新等事宜。

1.5.2 联系人

本《电子认证服务业务规则》通过内部文件发布，对具体个人不另行通知。

邮箱：dfca-cps@chinaonenet.com

联系地址：长沙高新开发区麓龙路 199 号麓谷商务中心 A 栋 1502 号

邮编：410205

联系电话：0731-88237505

传　　真：0731-88239600

1.5.3 决定 CPS 符合策略的机构

本《电子认证服务业务规则》由东方新诚信 CA 安全策略委员会组织制定，报东方新诚信 CA 安全策略委员会批准执行。

1.5.4 CPS 批准程序

东方新诚信 CA 安全策略委员会负责 CPS 的管理。东方新诚信 CA 安全策略委员会对 CPS 草案进行评审，如果符合证书策略，将批准 CPS，之后在对外公布。

1.6 定义和缩写

下列定义适用于本《电子认证服务业务规则》

1. 东方新诚信数字认证中心

受用户信任，负责创建和分配用户密钥和公钥证书的权威机构。

2. 东方新诚信数字认证中心电子政务电子认证服务业务规则

关于东方新诚信数字证书电子认证服务机构在签发、管理、注销或更新证书（或更新证书中的密钥）过程中采纳的业务实践的声明。

3. 注册机构

具有下列一项或多项功能的实体：识别和鉴别证书申请人，同意或拒绝证书申请，在某些环境下主动撤销或挂起证书，处理订户撤销或挂起证书的请求，同意或拒绝订户更新其证书或密钥的请求。

4. 数字证书

亦简称为证书，包含公开密钥拥有者的信息，公开密钥，签发者信息、有效期，以及一些扩展信息的数字文件。

5. 证书撤销列表（CRL）

一个已标识的列表，它指定了一套证书发布者认为无效的证书。除普通 CRL 外，还定义了一些特殊的 CRL 类型用于覆盖特殊领域的 CRL。

6. 私钥

私钥是指在公钥密码系统中，用户的密钥对中只能由用户持有并保持为秘密的密钥。

7. 公钥

公钥是指在公钥密码系统中，用户的密钥对中可以公开的密钥。

2 信息发布与信息管理

2.1 认证信息的发布

东方新诚信 CA 通过在线业务网站公布与其相关的信息。该网站是东方新诚信 CA 发布所有信息的最权威、最及时、最主要的渠道。

DFCA-CPS 发布在东方新诚信 CA 的在线业务网站上，供相关方查询、下载、查阅。

东方新诚信 CA 通过目录服务器发布订户的证书和 CRL。订户或依赖方可以通过访问东方新诚信 CA 的目录服务器获取证书和 CRL。同时，东方新诚信 CA 提供在线证书状态查询服务（OCSP 服务）。

2.2 发布的时间与频率

1. CPS 的发布时间与频率

(1) 按照 DFCA-CPS 的相关规定，东方新诚信 CA 对 DFCA-CPS、用户协议、相关方协议等进行修订。一旦对规则的修改、补充等获得批准，将首先在业务门户网站上发布，并即时生效。对证书的订户及证书申请人均具备约束力，对具体个人不另行通知；

(2) 根据电子认证服务业务开展的实际需要、相关技术的发展与改进升级以及相关法律法规的要求，东方新诚信 CA 决定对 CPS 进行修改、补充或调整，其发布时间与频率由东方新诚信 CA 独立做出决定。这种发布应该是及时、高效的，并符合国家法律法规的要求。

2. 证书/CRL 的发布时间与频率

(1) 证书一经签发，就即时在东方新诚信 CA 的证书服务目录服务器公布；

(2) 东方新诚信 CA 的 CRL 每 24 小时发布一次；在紧急情况下，东方新诚信 CA 可自行决定 CRL 的发布时间与频率；

(3) 通过 OCSP 对证书状态的查询是及时的；

(4) 用户可以通过业务门户网站查询证书的信息。

3. 其他公告、通知等信息的发布时间与频率

(1) 根据实际业务开展的需要，东方新诚信 CA 将实时在业务门户网站发布与东方新诚信电子认证服务相关的公告与通知；

(2) 这类信息是不定期发布的，东方新诚信 CA 将保证在第一时间发布信息。

2.3 信息库访问控制

对于公开发布的 DFCA-CPS、证书、CRL 等信息，东方新诚信 CA 允许公众自行通过网站和目录服务器进行查询与下载，其中，敏感信息的访问采用基于安全套接层协议（SSL 协议）的安全超文本传输协议（HTTPS 协议）。

东方新诚信 CA 设置了访问控制与安全审计措施，保证只有经授权的东方新诚信 CA 业务人员才能编写和修改东方新诚信 CA 在线公布的信息。

只有经授权的 RA/CA 管理员可以查询东方新诚信 CA 和注册机构数据库中的其他数据。

3 身份标识与鉴别

3.1 命名

3.1.1 名称类型

东方新诚信 CA 依照特定的签发程序，保存与订户相关的身份信息，对订户的身份进行鉴别。

每个订户按照 X.509 的规定，将对应一个可分辨的名称。该名称由甄别名（Distinguished Name，简称为 DN）和用户唯一标识项组成。DN 包含于证书的主题中。DN 遵从关于 DN 的 X.501 标准，并用 X.501 Printable String 格式。

东方新诚信 CA 负责确认公钥与已命名实体的对应关系。这种确认关系通过证书明确无误地表达。命名可以由申请者独立完成，也可以由申请者与东方新诚信 CA 协商解决。

3.1.2 对名称意义化的要求

订户的甄别名必须具有明确的、肯定的意义。

证书主体名称标识本证书所提到的最终实体的特定名称，描述了与主体公钥中的公钥绑定的实体信息。

3.1.3 订户的匿名或伪名

东方新诚信 CA 不允许和不接受任何匿名或伪名，仅接受有明确意义的名称作为 DN。

3.1.4 理解不同名称形式的规则

DN 由 CN、OU、O、C 等部分组成，其中 CN 表示用户名，OU、O 表示组织单位名称，C 用来表示国家。

3.1.5 名称的唯一性

在东方新诚信 CA 证书服务体系中，“ 证书主体名＋证书序列号 ” 必须是唯一的。

3.1.6 商标的识别、鉴别和角色

本 DFCA-CPS 受到完全的版权保护，本文件中涉及的“ 东方新诚信 CA ” 及其图标是东方新诚信 CA 独立持有的专有商标。其他参与者的商标为其拥有方所有。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

东方新诚信 CA 通过证书请求信息中所包含的数字签名来证明证书申请人持有与公钥对应的私钥。在用户申请证书时中，用户签名私钥由用户密码设备生成。证书请求信息中包含用该私钥进行的数字签名，可以用其对应的公钥来验证这个签名。

证书申请人应妥善保管自己的私钥。因此，证书申请人视作其签名私钥的唯一持有者。

3.2.2 组织机构身份的鉴别

对于组织机构的身份鉴别，需要验证组织的合法证件。证书申请人需持工商营业执照、事业单位法人证书与组织机构代码证书等证件，以及组织机构给经办人的授权和经办人的身份证件，向东方新诚信 CA 提出申请。若该组织需申请设备类型证书，还需提交相关使用权证明文件。

组织机构的身份鉴别规范简要说明了如何进行组织机构的身份鉴别。东方新诚信 CA 保留根据最新国家政策、法律、法规的要求更新组织机构身份鉴别规范的权利。

经办人经组织机构授权，通过邮寄或现场等方式，向东方新诚信 CA 的注册机构提交书面数字证书申请表以及下述组织机构的证明文件等申请资料，并缴纳相应的费用。

1. 组织机构代码证的副本及复印件；
2. 法人营业执照（或事业单位法人证书）副本及复印件；

3. 组织机构给经办人的授权书；

4. 经办人有效身份证件的原件和复印件；

5. 如该组织需申请设备类型证书，还需提交相关使用权证明文件。

以上各项证明文件需加盖申请单位的公章。

注册机构按照东方新诚信 CA 制定的组织机构身份鉴别规范，对申请资料的原件和复印件真实性进行审核，并进行批准申请或拒绝申请的操作。

批准申请后，东方新诚信 CA 或注册机构将保留相关盖单位公章的证明材料复印件，与证书申请表一并存档保存。

3.2.3 个人身份的鉴别

个人身份的鉴别可以使用以下有效的身份证件：居民身份证、港澳台居民身份证、户口簿、护照、外国人永久居留证、军官证、警官证、士兵证、士官证和文职干部证等。

个人身份的鉴别规范简要说明了如何进行个人身份鉴别。东方新诚信 CA 保留根据最新国家政策、法律、法规的要求更新个人身份鉴别规范的权利。

个人通过邮寄或现场等方式，向东方新诚信 CA 的注册机构提交书面数字证书申请表和上述有效身份证件的复印件等申请资料，并缴纳相关费用。

若申请人与证书持有人不是同一人时，还需提交申请人有效身份证件的原件（备查）与复印件。

注册机构按照东方新诚信 CA 个人身份鉴别规范对申请资料的原件和复印件真实性进行审核，并进行批准申请或拒绝申请的操作。

批准申请后，东方新诚信 CA 或注册机构将保留复印件，与证书申请表一并存档保存。

3.2.4 域名的确认

如果证书名称是域名（或互联网 IP 地址），除了在对申请者提交的书面材料进行审核外，还需要申请者额外提供域名使用权证明材料，以确定申请者有权使用相应的域名（或互联网 IP 地址）。东方新诚信 CA 还需采取其他独立的审查措施，以确认该域名（或互联网 IP 地址）

的归属权，并要求申请者提供相应的协助。申请者不得拒绝这种请求。

3.2.5 没有验证的订户信息

用户提交证明文件以外的信息为没有验证的用户信息。

3.2.6 授权确认

为确保办理人具有特定的许可，代表组织机构申请数字证书，需要出具组织机构授权其为该组织机构办理数字证书事宜的授权文件。

组织机构在东方新诚信 CA 的数字证书申请表以及授权书上加盖单位公章后，则证明本组织机构对办理人的授权确认。

3.2.7 互操作准则

互操作可能是交叉认证或其他形式的互操作。交叉认证是指两个完全独立的、采用各自认证策略的电子认证服务机构之间建立相互信任关系，使双方的用户可以实现互相认证。

东方新诚信 CA 将根据业务需要，在遵循本 DFCA-CPS 的各项控制要求的基础上，与东方新诚信 CA 证书服务体系中未涉及的其他电子认证服务机构建立交叉认证关系。

如果国家法律法规对此有规定，东方新诚信 CA 将严格予以执行。

3.3 密钥更新请求的身份标识与鉴别

3.3.1 密钥更新的标识与鉴别

通常，订户密钥的有效期是一年。密钥到期后，订户需更新密钥，并向注册机构申请重新签发证书。

在密钥更新过程中，通过用户使用当前有效私钥对包含新公钥的密钥更新请求进行签名，东方新诚信 CA 使用用户原有公钥验证确认签名来进行用户身份标识和鉴别。

国家主管部门对密钥的管理、更新等有规定的，东方新诚信 CA 将严格予以执行。

3.3.2 注销后密钥更新的标识与鉴别

东方新诚信 CA 不提供证书被注销后的密钥更新。订户必须重新进行身份鉴别和注册。对身份标识和鉴别的要求，使用初始身份确认相同的流程，详见 3.2.2 组织身份的鉴别、3.2.3 个人身份的鉴别与 3.2.4 域名的确认。

3.4 注销请求的标识与鉴别

用户本人注销时的身份标识和鉴别使用初始身份确认相同的流程，详见 3.2.2 组织身份的鉴别、3.2.3 个人身份的鉴别与 3.2.4 域名的确认。

如果是司法机关依法提出注销，东方新诚信 CA 将直接以司法机关书面的注销请求文件作为鉴别依据，不再进行其他方式的鉴别。

如果是因为用户没有履行本 DFCA-CPS 所规定的义务，由注册机构申请注销用户的证书时，不需要对用户身份进行标识和鉴别。

4 证书生命周期操作要求

本章阐述了东方新诚信 CA 根据公布的 DFCA-CPS 进行证书的申请、签发、管理、更新、注销等证书生命周期管理的全程过程，以及在这些过程中各参与方的责任与义务。

4.1 证书申请

4.1.1 证书申请实体

证书申请实体包括企业单位、事业单位、政府机构、社会团体等各类组织机构与个人用户。

4.1.2 申请过程与责任

证书申请人按照本 DFCA-CPS 所规定的要求，通过在线方式或离线方式，填写证书申请表，并准备相关的身份证明材料。东方新诚信 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。

申请过程中各方责任为：用户要按照本 DFCA-CPS 的要求准备证书申请材料，并确保申请材料真实准确。注册机构负责接收证书申请人的请求材料，当面对用户所提供的证书申请信息与身份证明资料进行鉴别验证。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

东方新诚信 CA 或授权的注册机构按照本 DFCA-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 3.2.2 组织身份的鉴别、3.2.3 个人身份的鉴别与 3.2.4 域名的确认。

4.2.2 证书申请批准和拒绝

东方新诚信 CA 或注册机构根据本 DFCA-CPS 所规定的身份鉴别流程对证书申请人身份进行识别与鉴别后，根据鉴别结果决定批准或拒绝证书申请。

如果证书申请人通过本 DFCA-CPS 所规定的身份鉴别流程且鉴证结果为合格，东方新诚信 CA 或注册机构将批准证书申请，为证书申请人制作并颁发数字证书。

证书申请人未能通过身份鉴别，东方新诚信 CA 或注册机构将拒绝申请人的证书申请，并通知申请人鉴证失败，同时向申请人提供失败的原因（法律禁止的除外）。

被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

4.2.3 处理证书申请的时间

东方新诚信 CA 的注册机构将做出合理努力来尽快确认证书申请信息。一旦注册机构收到了所有必须的相关信息，将在两个工作日内处理证书申请。

注册机构能否在上述时间期限内处理证书申请，取决于证书申请人是否真实、完整、准确地提交了相关信息和是否及时地响应了东方新诚信 CA 的管理要求。

4.3 证书签发

4.3.1 证书签发过程中东方新诚信 CA 的行为

东方新诚信 CA 在批准证书申请之后，将签发证书。证书的签发意味着东方新诚信 CA 最终完全正式地批准了证书申请。

通常东方新诚信 CA 签发的证书在 24 小时后才生效。

4.3.2 东方新诚信 CA 对订户的通告

东方新诚信 CA 通过注册机构，对订户的通告有以下几种方式：

1. 通过面对面的方式，通知订户到注册机构领取数字证书；
2. 注册机构把证书等直接提交给用户，来通知订户证书信息已经正确生成；

3. 邮政信函通知用户；

4. 其他东方新诚信 CA 认为安全可行的方式通知用户。

4.4 证书接受

4.4.1 构成接受证书的行为

数字证书签发完成后，东方新诚信 CA 或其注册机构将数字证书本身或者证书获得的方式或者与证书相关的授权码递送给证书申请人，证书申请人即被视为同意接受证书。

4.4.2 东方新诚信 CA 对证书的发布

东方新诚信 CA 在签发完证书后，将证书发布到证书服务系统中。

证书服务系统将证书发布到目录服务器中，供用户和依赖方查询和下载。

4.4.3 东方新诚信 CA 对其他实体的通告

其他实体可以通过从目录服务器中查询到东方新诚信 CA 已经签发的数字证书。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

用户在提交了证书申请并接受了东方新诚信 CA 所签发的证书后，均视为已经同意遵守与东方新诚信 CA、依赖方有关的权利和义务的条款。用户接收到数字证书，应妥善保存其证书对应的私钥。

用户只能在指定的应用范围内使用私钥和证书。只有在接受了相关证书之后，用户才能使用对应的私钥。在证书到期或被注销之后，用户必须停止使用该证书对应的私钥。

4.5.2 依赖方对公钥和证书的使用

依赖方只能在合法的应用范围内依赖于证书，并且与证书要求相一致（如密钥用途扩展

等）。依赖方获得对方的证书和公钥后，可以通过查看对方的证书了解对方的身份，并通过公钥验证对方电子签名的真实性。验证证书的有效性包括三个方面的内容：

1. 用东方新诚信 CA 的认证机构证书验证用户证书中的签名，确认该证书是东方新诚信 CA 签发的，并且证书的内容没有被篡改；
2. 检验证书的有效期，确认该证书在有效期之内；
3. 查询证书状态，确认该证书没有被注销。

在验证电子签名时，依赖方应准确知道什么数据已被签名。在公钥密码标准里，标准的签名信息格式被用来准确表示签名过的数据。

4.6 证书更新

4.6.1 证书更新的情形

证书更新是指在证书中信息（包括身份信息变动或密钥变动）发生变化的情况下，为订户签发一张新证书。

在证书上都有明确的证书有效期，表明该证书的起始日期与截至日期。订户应当在证书有效期到期前，向东方新诚信 CA 申请更新证书。

证书更新的具体情形如下：

1. 证书的有效期将要到期；
2. 密钥对的使用期将要到期；
3. 其他需要更新证书的情形。

在证书有效期内，如以下信息发生变更，应进行证书更新：

1. 机构用户的单位注册地，单位名称、单位组织机构代码号等关键信息；
2. 个人用户的姓名、住址、电子邮件等关键信息；
3. 设备的域名、IP、所有者等关键信息；
4. 东方新诚信 CA 规定的其他相关信息。

4.6.2 请求证书更新的实体

证书持有者、证书持有者的授权代表（例如，机构证书等）或者证书对应实体的拥有者（例如，设备证书等）可以请求证书更新。

4.6.3 证书更新请求的处理

东方新诚信 CA 支持下述处理证书更新请求方式：

对于证书信息发生改变的用户，由注册机构来处理证书更新请求，为用户制作新的证书。

注册机构对申请证书更新用户的身份进行鉴别与验证，鉴别要求同本 DFCA-CPS 的 3.2.2 组织身份的鉴别、3.2.3 个人身份的鉴别与 3.2.4 域名的确认。

4.6.4 颁发新证书时对订户的通告

对订户的通告有以下几种方式：

1. 通过面对面的方式，通知证书更新已完成，新证书已颁发；
2. 邮政信函通知用户；
3. 其他东方新诚信 CA 认为安全可行的方式通知用户。

4.6.5 构成接受更新证书的行为

当更新证书签发后，注册机构将证书当面或寄送给用户，就表示用户接受更新证书。

4.6.6 东方新诚信 CA 对更新证书的发布

东方新诚信 CA 在签发更新证书后，将证书发布到证书服务系统中。

证书服务系统将证书发布到目录服务器中，供用户和依赖方查询和下载。

4.6.7 东方新诚信 CA 对其他实体的通告

其他实体可以通过从目录服务器查询已更新的数字证书。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

证书密钥更新指订户或其他参与者生成一对新密钥并申请为新公钥签发一个新证书。

证书密钥更新的具体情形如下：

1. 因私钥泄漏而注销证书；
2. 证书无法继续获得信任；
3. 证书无法正常使用；
4. 证书丢失；
5. 证书密钥的有效期将要到期；
6. 其他需要更新证书密钥的情形。

4.7.2 请求证书密钥更新的实体

请求证书密钥更新的实体同 4.6.2 请求证书更新的实体。

4.7.3 证书密钥更新请求的处理

证书密钥更新请求的处理同 4.6.3 证书更新请求的处理

4.7.4 颁发新证书时对订户的通告

颁发新证书给用户的通告同 4.6.4 颁发新证书时对订户的通告。

4.7.5 构成接受密钥更新证书的行为

正式接受密钥更新证书的行为同 4.6.5 构成接受更新证书的行为。

4.7.6 东方新诚信 CA 对密钥更新证书的发布

对密钥更新证书的发布同 4.6.6 东方新诚信 CA 对更新证书的发布。

4.7.7 东方新诚信 CA 对其他实体的通告

在颁发证书时对其他实体的通告同 4.6.7 东方新诚信 CA 对其他实体的通告。

4.8 证书变更

在证书有效期内，当证书信息发生变化，用户或者其它参与者可以选择证书变更，保留原有公钥，申请签发新的证书。

4.8.1 证书变更的情形

证书变更指改变证书中除用户公钥之外的信息而签发新证书的情形。当用户实体身份信息发生改变，而影响证书项内容时，订户可以向东方新诚信 CA 申请证书变更。

4.8.2 请求证书变更的实体

东方新诚信 CA 颁发的证书有效期限未到的个人、单位、服务器设备、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，以及其他东方新诚信 CA 各类证书（包括测试证书）的有效期限未到的证书持有者均可向东方新诚信 CA 申请变更自己持有的证书。

4.8.3 证书变更请求的处理

订户在申请证书变更时，可以通过在线方式或离线方式填写相应的申请表。订户填写完后，向注册机构提交申请表以及相关的身份证明材料，并按时缴纳相应的费用。

注册机构按“ 证书申请处理 ”的流程，对证书变更申请进行身份鉴别与审核。东方新诚信 CA 确认并批准变更申请后，为订户签发新的证书。

4.8.4 证书变更时对订户的通告

证书变更完成后，颁发新证书给用户的通告同 4.6.4 颁发新证书时对订户的通告。

4.8.5 构成接受变更证书的行为

正式接受变更证书的行为同 4.6.5 构成接受更新证书证书的行为。

4.8.6 东方新诚信 CA 对变更证书的发布

对变更证书的发布同 4.6.6 东方新诚信 CA 对更新证书的发布。

4.8.7 东方新诚信 CA 对其他实体的通告

在颁发证书时对其他实体的通告同 4.6.7 东方新诚信 CA 对其他实体的通告。

4.9 证书注销和冻结

4.9.1 证书注销与冻结的情形

1. 发生下列情形之一的，用户应当申请注销与冻结数字证书：

   (1) 数字证书私钥安全已经受到损害；

   (2) 数字证书中的信息发生重大变更；

   (3) 认为本人不能实际履行本 DFCA-CPS；

   (4) 政务机构的证书持有者工作性质发生变化。

2. 发生下列情形之一的，东方新诚信 CA 可以注销和冻结其签发的数字证书：

   (1) 订户申请注销数字证书；

   (2) 订户提供的信息不真实；

   (3) 订户没有或无法履行双方合同规定的义务；

   (4) 数字证书的安全性得不到保证；

(5) 政务机构的证书持有者受到国家法律法规制裁；

(6) 证书仅用于依赖方主导的系统并由依赖方提出撤销申请；

(7) 法律、法规规定的其他情形。

4.9.2 请求证书注销的实体

根据不同的情况，订户、东方新诚信 CA、注册机构、订户所属组织机构或证书使用唯一依赖方可以请求注销与冻结订户证书。

4.9.3 注销请求的流程

证书注销与冻结请求的处理采用与原始证书签发相同的过程。

1. 证书注销或冻结的申请人通过在线方式或离线方式填写《证书注销/冻结申请表》，并注明注销或冻结原因；
2. 东方新诚信 CA 的注册机构根据“ 3.2 初始身份确认 ”的要求对订户提交的注销或冻结请求进行身份鉴别与审核，以确认为订户本人或得到了订户的授权；
3. 东方新诚信 CA 注销或冻结订户证书后，注册机构将通知订户证书被注销或冻结，订户的数字证书在 24 小时内进入 CRL，向外界公布；
4. 强制注销或冻结是指当东方新诚信 CA 或授权的注册机构确认订户有违反本 DFCA-CPS 的情况发生时，对订户证书进行强制注销或冻结，注销或冻结后将立即通知该订户。

4.9.4 注销请求宽限期

如果出现私钥泄露等事件，注销和冻结请求必须在发现泄露或有泄露嫌疑 8 小时内提出。其他注销和冻结原因的注销请求必须在 48 小时内提出。

4.9.5 东方新诚信 CA 处理注销/冻结请求的时限

东方新诚信 CA 接到注销/冻结请求后立即处理，24 小时生效。东方新诚信 CA 每日签

发一次 CRL，并将最新的 CRL 发布到证书服务系统的目录服务器，供请求者查询下载。

CRL 的结构如下：

1. 版本号(version)；
2. 签名算法标识符(signature)；
3. 颁发者名称(issue)；
4. 本次更新(this update)；
5. 下次更新(next update)；
6. 用户证书序列号/吊销日期(user certificate/revocation date)；
7. CRL 条目扩展项(crl entry extensions)；
8. CRL 扩展域(crl extensions)；
9. 签名算法(signature algorithm)；
10. 签名(signature value)。

4.9.6 依赖方检查证书注销/冻结的要求

在具体应用中，依赖方必须使用以下两种功能之一进行所依赖证书的状态查询：

1. CRL 查询：通过目录服务器提供的查询系统，查询并下载 CRL 到本地，进行证书状态的检验；
2. 在线证书状态查询（OCSP）：东方新诚信 CA 接受证书状态查询请求，查询证书的实时状态。查询结果经过签名后，返回给请求者。

4.9.7 CRL 发布频率

东方新诚信 CA 的订户证书的 CRL 的发布周期为一日，即每日发布一次 CRL。

东方新诚信 CA 机构证书的 CRL 至少每年签发一次，即每年至少重新发布一次。

4.9.8 CRL 发布的最大滞后时间

发布的最长滞后时间为 24 小时。

4.9.9 在线状态查询的可用性

东方新诚信 CA 向订户和依赖方提供在线证书状态查询服务。

4.9.10 在线状态查询要求

依赖方是否进行在线状态查询完全取决于应用的安全要求。很多的应用本身建有用户帐户数据库，并基于用户帐户进行应用控制，数字证书在此只起身份鉴别的作用。在这种情况下，在线状态查询不一定是必需的。对于安全保障要求高并且完全依赖数字证书进行身份鉴别与授权的应用，依赖方在信赖一个证书前，必须通过证书状态在线查询检查该证书的状态。

4.9.11 注销信息的其他发布形式

除了 CRL、OCSP 外，东方新诚信 CA 暂不提供注销/冻结信息的其他发布形式。

4.9.12 密钥损害的特别要求

无论是最终订户还是东方新诚信 CA 或其授权的注册机构，发现证书密钥受到安全损害时，应立即注销证书。

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

请求证书挂起的实体包括：证书有效期限未到的订户本人或其授权代表、东方新诚信 CA 或其授权机构的授权代表、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

申请者到东方新诚信 CA 授权的注册机构，书面填写《东方新诚信 CA 数字证书挂起申请表》，并注明挂起的原因。东方新诚信 CA 授权的注册机构按照“ 第 3 章身份标识与鉴别 ”对订户提交的证书挂起申请进行鉴别与验证。

如是是强制挂起，注册机构的管理员可以依法对数字证书进行强制挂起。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、东方新诚信 CA 或东方新诚信 CA 授权的注册机构。

东方新诚信 CA 挂起订户证书后，注册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，否则东方新诚信 CA 或东方新诚信 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，东方新诚信 CA 不负责任。

4.10 证书状态服务

4.10.1 操作特征

东方新诚信 CA 通过证书服务系统为用户提供证书状态服务。

4.10.2 服务可用性

原则上，东方新诚信 CA 提供 365 天×24 小时的证书状态查询服务，即在网络以及电力供应允许的情况下，每天用户能够实时获得证书状态查询服务。

4.10.3 可选特征

根据请求者的要求，在请求者支付相关费用后，东方新诚信 CA 可以提供以下通知服务：

1. 收到证书主题的电子签名消息的接受者要求，确认该证书是否已被注销；
2. 提供通知服务，当指定的证书被注销时，东方新诚信 CA 将通知请求该项服务的请求者。

4.11 订购结束

终止服务是指当证书有效期满或证书注销后，该证书的服务时间结束。

下列情况视为证书持有者终止使用东方新诚信 CA 提供的证书服务：

1. 证书到期后，用户不再延长证书使用期或者不再重新申请证书，则可以自动终止与东方新诚信 CA 的服务；
2. 在证书有效期内，证书持有者提出终止服务，即服务终止。

4.12 密钥生成、备份与恢复

4.12.1 密钥生成、备份与恢复的策略与行为

用户的签名密钥对由用户的密码设备生成，加密密钥对由密钥管理中心生成。

签名密钥对由用户的密码设备保管。加密密钥对由用户的密码设备保管，同时，密钥管理中心保存有加密密钥对的备份数据，以便于密钥恢复。

密钥恢复是指加密密钥对的恢复，密钥管理中心不负责签名密钥对的恢复。密钥恢复分为两类：用户密钥恢复和司法取证密钥恢复。

1. 用户密钥恢复

当用户的密钥损坏或丢失后，某些密文数据将无法还原，此时用户可申请密钥恢复。用户向东方新诚信 CA 申请进行密钥恢复。经审核后，通过东方新诚信 CA 向密钥管理中心请求密钥恢复 ,密钥管理中心接受用户的恢复请求,恢复用户的密钥并下载于用户证书载体中。

2. 司法取证密钥恢复

司法取证人员向东方新诚信 CA 申请。由东方新诚信 CA 的业务人员根据司法机关的书面材料，生成司法取证密钥恢复申请。经审核后，由密钥管理中心恢复所需的密钥并记录于

特定载体中。

具体策略在“ 6.1 密钥生成与安装 ”与“ 6.2 私钥的安全保证 ”中详细描述。

4.12.2 会话密钥的封装与恢复的策略与行为

会话密钥的封装采用数字信封的方式。数字信封使用接收者的公钥对会话密钥加密，接收者用自己的私钥解密，恢复会话密钥。

5 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

东方新诚信 CA 的建筑物和机房建设按照下列标准实施：

1. GB 50174-2008：《电子计算机机房设计规范》
2. GB 2887-2000：《电子计算机场地通用规范》
3. GB 9361-88：《计算站场地安全要求》
4. SJ/T 10796-2001：《防静电活动地板通用规范》
5. GB 50034-2004：《建筑照明设计标准》
6. GB 50054-95：《低压配电设计规范》
7. GB 50019-2003：《采暖通风与空气调节设计规范》
8. GB 157：《建筑防雷设计规范》
9. GBJ 79-1985：《工业企业通信接地设计规范》

东方新诚信 CA 机房位于长沙麓谷高新区标志麓谷坐标 A 栋 1502，实行分区访问的安全管理：

东方新诚信 CA 机房的功能区域划分为 CA 核心区、CA 管理区、CA 服务区、RA 管理区与监控管理区等区域。

CA 核心区位于屏蔽机房内，具有最高的安全级别。屏蔽机房设置了非接触 IC 卡指纹门禁系统，并设置了“双人同进、双人同出”策略，即需要两个持有相应 IC 卡的管理人员同时刷卡，方可进入该区域。

其它区域的进入权限授权给不同的管理人员，不能有一个管理人员可单独进入多个区域的情况。

5.1.2 物理访问

为了保证 CA 系统的安全，采取了一定的隔离、控制、监控手段。机房的所有门都足够结实，能防止非法的进入。机房通过设置门禁和侵入报警系统来重点保护机房物理安全。

物理访问控制包括如下几个方面：

1. 门禁系统：控制各层门的进出。工作人员需使用身份识别卡与指纹鉴定才能进出，进出每一道门应有时间记录和信息提示。
2. 报警系统：当发生任何非法闯入、非正常手段的开门、长时间不关门等异常情况，均会触发报警系统。报警系统明确指出报警位置。
3. 监控系统：与门禁和物理侵入报警系统配合使用的还有视频监控系统，对安全区域和操作区域进行录像。所有录像资料需要保留，以备查询。

门禁和物理侵入报警系统备有 UPS，并提供至少 8 小时的不间断供电。

5.1.3 电力与空调

机房电源供电系统包括机房区的动力、照明、监控、通讯、维护等用电系统。按负荷性质分为计算机设备负荷和辅助设备负荷，计算机设备和动力设备分开供电。供电系统的组成包括配电柜、动力线缆、线槽及插座、接地防雷、照明箱及灯具、应急灯、照明线管等。计算机设备专用配电柜和辅助设备配电柜独立设置。

目前，东方新诚信 CA 采用使用不间断电源系统（UPS）来保证供电的稳定性和可靠性，当市电停电时，UPS 可以保证供电 8 小时，维持系统正常运转。东方新诚信 CA 的市电由高开区的市电接入供电。高开区的市电提供了双市电供电，在第一路市电停电的情况下，将自动切换到第二路市电供电。

根据机房环境及设计规范要求，机房内设置了空气调节系统。空气调节系统包括空调、通风管路、新风系统。

东方新诚信 CA 对 CA 系统的电源、空调等物理要求，严格参照相关设施管理的规定进行维护和保养，而且每年对其中否符合要求进行检查。

5.1.4 水患防治

机房内无渗水、漏水现象，主要设备采用专用的防水插座，并采取必要措施防止下雨或水管破损，造成天花板漏水、地板渗水和空调漏水等现象。

东方新诚信 CA 的系统有充分保障，能够防止水侵蚀。

5.1.5 火灾防护

火灾预防与保护措施主要包括以下六个方面：

1. 敏感区、高度敏感区域，其建筑物的耐火等级必须符合 GB 50045-1995《高层民用建筑设计防火规范》中规定的二级耐火等级；
2. 东方新诚信 CA 的设施内设置火灾报警装置。在机房内、各物理区域内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位设置烟、温感探测器；
3. 敏感区及高敏区配置独立的气体灭火装置，使用专业的灭火系统，备有相应的气体灭火器。东方新诚信 CA 内除对纸介质等易燃物质进行灭火外，禁止使用水、干粉或泡沫等易产生二次破坏的灭火剂；
4. 火灾自动报警、自动灭火系统避开可能招致电磁干扰的区域或设备，同时配套设置消防控制室。还设有不间断的专用消防电源和直流备用电源，并具有自动和手动两种触发装置；
5. 火灾自动灭火设施的区域内，其隔墙和门的耐火极限不低于 1 小时，吊顶的耐火极限不得低于 15 分钟；
6. 在非敏感区及敏感区的办公区域内，须设置紧急出口，紧急出口必须设有消防门，消防门符合安全要求。紧急出口门需与门禁报警设备联动。

灭火系统采用电动，手动，紧急启动三种方式：

1. 电动方式：防护区报警系统第一次火警确认后，发出声光警示信号，切断非消防电源（如：空调电源、照明电源等）。并送排风（烟），防火阀关闭。第二次火警确认后，经延时，同时发出气体释放信号，并发出启动电信号，送给对应的管网启动钢瓶，喷气灭火；

2. 手动方式：人员对钢瓶或药剂瓶直接开启操作；

3. 紧急启动：防护区外设有紧急启动按钮供紧急时使用。

东方新诚信 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。

5.1.6 介质存储

数据的存储介质包括硬盘、软盘、磁带、光盘等，介质存储地点和系统分开并且保证物理安全，注意防磁、防静电干扰、防火、防水，由专人管理。

5.1.7 废物处理

当东方新诚信 CA 存档的敏感数据或密钥已不再需要或存档期限已满时，应当将这些数据进行销毁。写在纸张之上的，必须切碎或烧毁。如果保存在磁盘中，应多次重写覆盖磁盘的存储区域，其他介质以不可恢复原则进行相应的销毁处理。

5.1.8 异地备份

所备份的业务数据磁带（光盘、移动存储介质等）均送到位于异地的东方新诚信 CA 异地备份区，进行异地备份保存。

5.2 程序控制

5.2.1 可信角色

东方新诚信 CA 或其授权的注册机构、依赖方等组织中与密钥和证书生命周期管理操作有关的工作人员，都是可信角色，必须由可信人员担任。

东方新诚信 CA 明确规定 CA 关键职能的职位，主要包括但不限于以下部分：

1. 安全策略委员会主任

2. 可信人员管理员

3. 安全管理员

4. 物理环境安全管理员
5. 密钥管理员
6. 运行维护管理员
7. CA 系统管理员
8. 系统维护管理员
9. 数据库管理员
10. 网络管理员
11. 运行审计管理员
12. 鉴别与验证员
13. 信息录入员
14. 信息审核员
15. 档案管理员
16. 其他。

东方新诚信 CA 根据《电子认证服务机构从业人员岗位技能规范》等标准规范与本 CPS 的要求，制订其授权的证书服务机构（RA 等）的管理规范，规范证书服务机构和服务系统的管理人员、操作人员的操作。在与此相关的软件设计中，充分考虑安全的限制与约束。东方新诚信 CA 对授权的证书服务机构的责任进行合理划分，并通过系统和技术实现以及管理的责任义务上进行保证。

5.2.2 每项任务需要的人数

东方新诚信 CA 确保单个人不能接触、导出、恢复、更新、废止东方新诚信 CA 存储的私钥。

至少有两个人以上共同实施，使用对参加操作人员保密的密钥分割和合成技术，进行任何 CA 密钥的生成、恢复操作。

东方新诚信 CA 对与运行和操作相关的职能有明确的分工，贯彻职责分割、多人控制、

互相牵制和最小权益的安全管理原则。

对于重要的系统操作与维护，东方新诚信 CA 通常会安排一人进行操作，一人进行监督记录。

5.2.3 每个角色的识别与鉴别

所有东方新诚信 CA 的在职人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用门禁卡和指纹识别；进入系统需要使用数字证书进行身份鉴别。东方新诚信 CA 将独立完整地记录其所有的操作行为。

5.2.4 需要职责分割的角色

为保证系统安全，遵循可信角色分离的原则，即东方新诚信 CA 的可信角色由不同的人担任。

对于证书服务的受理，必须通过业务办理人员（或录入人员）、鉴别验证人员、业务执行人员等多个角色进行才能完成。

至少两个人以上才能使用对参加操作人员保密的密钥分割和合成技术，来进行任何密钥恢复的操作。

东方新诚信 CA 在系统遇到紧急情况需要联合抢修时，至少派遣 1 名东方新诚信 CA 工作人员在场。抢修人员需在东方新诚信 CA 工作人员陪同下，执行许可的操作。所有的操作、修改都保留记录。

非东方新诚信工作人员因基础装修、消防、强（弱）电故障等情形，需要进入数据机房实施修理时，必须经东方新诚信安全管理部门同意后，首先对修理者的身份进行验证，然后由东方新诚信 CA 指定的工作人员始终陪同和监督，完成约定部位的修理。

5.3 人员控制

5.3.1 资格、经历和无过失要求

所有的员工与东方新诚信 CA 签订保密协议。对于充当可信角色或其他重要角色的人

员，必须具备的一定的资格，具体要求在人事管理制度中规定。东方新诚信 CA 要求充当可信角色的人员至少必须具备忠诚、可信赖及工作的热诚度、无影响东方新诚信 CA 运行的其它兼职工作、无同行业重大错误记录、无违法记录等。

5.3.2 背景审查程序

东方新诚信 CA 与有关的政府部门和调查机构合作，完成对东方新诚信 CA 的可信任人员的背景调查。

所有目前的可信任人员和申请调入的可信任人员都必须书面同意对其进行背景调查。

背景调查分为基本调查和全面调查。基本调查包括对工作经历，职业推荐，教育，社会关系方面的调查；全面调查除基本调查项目外，还包括对犯罪记录，社会关系和社会安全方面的调查。

调查程序包括：

1. 人事部门负责对应聘人员的个人资料予以审查与确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明；
2. 人事部门通过电话、信函、网络、走访等形式对其提供的材料的真实性进行鉴定；
3. 用人部门通过现场考核、日常观察、情景考验等方式对其考察；
4. 经考核，人事部门和用人部门联合填写《可信人员调查表》，报主管领导批准后准予上岗。

5.3.3 培训要求

东方新诚信 CA 对所有人员按照其岗位和角色安排不同的培训。培训内容主要包括：

1. 东方新诚信 CA 的安全原则和机制、岗位职责；
2. 电子认证系统相关软、硬件的安装与维护；
3. 电子认证系统的操作与使用；
4. 东方新诚信 CA 的业务管理相关的流程、标准与规范；
5. 东方新诚信 CA 的运行管理相关的规章、制度与管理办法；

6. 国家电子认证相关的法律法规与政策；

7. 其他必要的培训。

对于运营人员，有关 CA 的相关知识与技能，每年至少要总结一次并由东方新诚信 CA 组织培训。技术的进步、系统功能更新或新系统的加入，都需要对相关人员进行培训。

5.3.4 再培训周期和要求

对于充当可信角色或其他重要角色的人员，每年至少接受东方新诚信 CA 组织的培训一次。

认证策略调整、系统更新时，应对相关人员进行再培训，以适应新的变化。

5.3.5 工作轮换周期和顺序

东方新诚信 CA 将根据业务的安排进行工作轮换。轮换的周期和顺序，视业务的具体情况而定。

工作岗位轮换遵循国家电子认证服务管理相关规范要求的职责分割的要求。

5.3.6 未授权行为的处罚

当东方新诚信 CA 的员工被怀疑，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东方新诚信 CA 或进行越权操作，东方新诚信 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，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施。对情节严重的，依法追究相应责任。

一旦发现上述情况，东方新诚信 CA 立即吊销或终止该人员的安全操作令牌（包括门禁卡、操作管理证书等）。

5.3.7 独立合约人的要求

对不属于东方新诚信 CA 内部的工作人员，但从事东方新诚信 CA 有关业务的人员等独立签约者，东方新诚信 CA 的统一要求如下：

1. 人员档案进行备案管理；
2. 签署保密协议；
3. 必须接受东方新诚信 CA 组织的相关知识与安全规范培训；
4. 由东方新诚信 CA 派专人监督和陪同从事相关在工作。

5.3.8 提供给员工的文档

为使得系统正常运行，必须提供给具有权限的相关人员各种文档，主要包括（但不限于）：

1. 认证系统相关软、硬件的操作手册，例如，认证系统操作手册、密码设备用户手册、目录服务器安装配置说明文件等；
2. 电子认证业务规则与相关的协议和规范；
3. 系统运行与维护相关的流程、管理办法，例如，机房设备管理办法；
4. 电子认证服务相关的宣传资料；
5. 内部操作文件，例如，灾难备份和恢复方案；
6. 其他文档。

5.4 审计日志程序

5.4.1 记录事件的类型

东方新诚信 CA 记录与系统相关的事件，这些记录信息称为日志。对于这些日志，无论其载体是纸张还是电子文档的形式，必须包含事件发生的日期、事件的发生时间段、事件的内容和事件相关的实体等。主要包括但不限于：

1. 订户服务申请和注销的申请表、协议、身份证明材料和其他相关信息等；
2. 电子认证系统密钥的生成、变化等记录；
3. 电子认证系统自身密钥的生成、配置、更新等成功和失败的记录；
4. 电子认证系统日常运行产生的各类日志记录；

5. CRL 操作记录；

6. 进出东方新诚信 CA 控制区域的表格、门禁卡进出敏感区域的记录、机房工作日志、系统日常维护记录、监控录像等；

7. 系统软硬件设备上线、更换、下线等记录；

8. 其他与系统不直接相关的事件，例如：物理通道参观记录、人事变动等。

5.4.2 处理日志的周期

东方新诚信 CA 定期对日志进行审查，并对审查日志的行为进行备案。每年进行的审查不少于 2 次。

5.4.3 审计日志的保存期限

东方新诚信 CA 在数据库保存审计日志至少 3 年，离线保存至少为 10 年。

监控录像资料保存 1 年，存档期限为 10 年。

5.4.4 审计日志的保护

东方新诚信 CA 执行严格的管理，确保只有东方新诚信 CA 授权的人员才能对审查日志进行相应操作。日志处于严格的保护状态，严禁在未授权的情况下被访问、阅读、修改和删除等操作，另外对日志进行异地备份。审计日志的制作和访问进行岗位分离。

东方新诚信 CA 将审计日志存储到磁带中，并存放到异地，实行安全保管。

5.4.5 审计日志备份程序

东方新诚信 CA 保证所有的审查记录和审查总结都按照东方新诚信 CA 备份标准和程序进行备份。根据记录的性质和要求，分为实时、按天、按周、按月和按年等多种形式的备份，可采用在线和离线两种方式的备份工具。

审计文档由管理员每周进行一次归档。所有档案安全存放在文档库内。

5.4.6 审计日志收集系统

审计日志收集系统涉及：

1. 证书管理系统；
2. 密钥管理系统；
3. 证书注册管理系统；
4. 证书服务系统；
5. 证书在线业务门户；
6. 网站、数据库安全管理系统；
7. 其他需要审计的系统。

东方新诚信 CA 使用审计工具满足对上述系统审计的各项要求。

5.4.7 对导致事件实体的通告

东方新诚信 CA 发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，东方新诚信 CA 保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

东方新诚信 CA 有权决定是否对导致事件的实体进行通告。

5.4.8 脆弱性评估

东方新诚信 CA 每年对系统进行脆弱性评估，以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

东方新诚信 CA 对以下记录（包括但不限于）进行归档保存

1. 电子认证系统的建设和升级文档；

2. 证书申请信息、证书服务批准与拒绝的信息、与订户的协议、证书和 CRL 等；

3. 系统运行所产生的日志；

4. 电子认证服务规划、各类服务规范和协议、规章制度、管理办法等；

5. 认证系统的数据库数据；

6. 人员进出记录和第三方人员服务记录；

7. 监控录像；

8. 员工资料，包括背景调查、录用、培训等资料；

9. 各类外部、内部审核评估文档。

5.5.2 归档记录的保存期限

所有归档记录的保存期一般规定为 10 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查询。东方新诚信 CA 保护相关的档案内容，免遭恶劣环境的威胁，如温度、湿度和强磁力等的破坏。

东方新诚信 CA 保存的申请信息、用户基本情况资料和身份鉴别资料，非经政府主管机构或司法机构经过合法途径予以申请，任何无关的第三方均无法获知。

5.5.4 归档文件的备份程序

所有存档的文件和数据库除了保存在东方新诚信 CA 的存储库，还在从银行租赁的保险柜中保存其备份。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。只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。东方新诚信 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 记录时间戳要求

东方新诚信 CA 暂不采用时间戳。

5.5.6 归档收集系统

认证系统的相关运营信息，由东方新诚信 CA 内部的工作人员或者具备完全控制措施的内部系统，依照人工和自动操作两部分进行产生的收集，并且由具备相关权限的人进行管理和分类。

由两个人分别来保留归档数据的两个拷贝，并且为了确保档案信息的准确，需要对这两个拷贝进行比较。

5.5.7 获得和检验归档信息的程序

东方新诚信 CA 每年会组织专人检验归档信息的完整性，也可根据业务需求不定期进行检查验证。

5.6 电子认证服务机构密钥更替

东方新诚信 CA 密钥更替指东方新诚信 CA 认证机构证书到期时，需要更换密钥而采取的措施。

东方新诚信 CA 的认证机构的签名密钥由密码机产生，有效期为 20 年，更替办法为：

1. 使用旧的私钥对新的公钥及信息签名生成证书；
2. 使用新的私钥对旧的公钥及信息签名生成证书；
3. 使用新的私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信任。

密钥更替时直接把当前 CA 证书注销，签发到 ARL 并发布，然后签发一个新的 CA 证书，通过证书库和 LDAP 方式下发给证书应用系统。

东方新诚信 CA 将继续使用旧的根私有密钥签发的 CRL，直到旧的私钥签发的证书到

期为止。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

发生故障时，东方新诚信 CA 将按照灾难恢复计划实施恢复。

5.7.2 计算机资源、软件和/或数据被破坏

东方新诚信 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，东方新诚信 CA 将按照灾难恢复计划实施恢复。

5.7.3 东方新诚信 CA 私钥损害处理程序

当东方新诚信 CA 的根私钥出现损毁、遗失、泄露、破解、被篡改、或者有被第三者窃用的疑虑时，东方新诚信 CA 采用如下措施处理：

1. 立即向电子认证服务主管部门和其他政府主管部门汇报，通过网站和其他公共媒体对订户进行通告，采取措施保证用户利益不受损失；
2. 立即吊销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询。同时，立即生成新的密钥对，并自签发新的根证书；
3. 新的根证书签发以后，按照本 CPS 关于证书签发的规定，重新签发下级证书和用户证书；
4. 新的根证书签发以后，将立即通过东方新诚信 CA 的信息库、目录服务器、门户网站等方式进行发布。

订户的私钥出现损毁、遗失、泄露、破解、被篡改、或者有被第三者窃用的疑虑时，订户应按照本 CPS 的规定，首先申请吊销证书，然后按照规定重新申请新的证书。

5.7.4 灾难后的业务连续性能力

针对证书系统的核心业务系统，证书签发系统和证书接口系统采用备份方式；对核心数据库，证书管理系统数据库采用磁盘阵列方式来确保证书系统的高可靠性和可用性。

发生自然或其它不可抗力性灾难后，东方新诚信 CA 可采用备份恢复方式对运营进行恢复。具体的安全措施按照东方新诚信 CA 灾难恢复计划实施。

5.8 电子认证服务机构或注册机构的终止

因各种情况，东方新诚信 CA 需要终止运营时，将按照相关法律规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。

在东方新诚信 CA 终止前必须：

1. 在暂停或者终止服务九十日前，就业务承接及其他有关事项向主管机构、证书持有者以及其他所有相关实体进行通告；
2. 安排业务承接；
3. 保存所有的认证服务相关运营资料，包括（但不限于）证书、用户信息、系统文件、CPS、规范与协议等；
4. 停止有关运营服务；
5. 清除系统根密钥；
6. 清除东方新诚信 CA 主机硬件。

当东方新诚信 CA 授权的证书服务机构因故终止服务时，东方新诚信 CA 将按照与其签订的相关协议处理有关业务承接事宜与其他事项。因注册机构故终止服务时，东方新诚信 CA 将按照与注册机构签订的相关协议处理有关业务承接事宜与其他事项。

6 认证系统技术安全控制

6.1 密钥对的生成和安装

6.1.1 密钥对的生成

用户的签名密钥对由用户的密码设备生成，加密密钥对由密钥管理中心生成。

6.1.2 私钥传送给订户

用户的签名密钥对由用户的密码设备生成并保管。

加密密钥对由密钥管理中心产生，通过安全通道传到用户的密码设备。

6.1.3 公钥传送给证书签发机构

用户的签名公钥通过安全通道，经证书注册管理系统传递到证书管理系统。

用户的加密公钥，由密钥管理中心通过安全通道传递到证书管理系统。

从证书注册管理系统到证书管理系统以及从密钥管理中心到证书管理系统的传递过程中，采用国家密码管理局许可的通讯协议及密钥算法，保证了传输中数据的安全。

6.1.4 电子认证服务机构公钥传送给依赖方

依赖方可以从东方新诚信 CA 的网站或目录服务器下载认证机构证书，从而得到东方新诚信 CA 的公钥。

6.1.5 密钥的长度

东方新诚信 CA 支持 RSA 算法与 SM2 算法。RSA 非对称密钥对的模长是 1024 比特，SM2 非对称密钥对的长度是 256 比特。

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，东方新诚信 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的密码设备产生。

公钥参数质量的检查同样通过国家密码管理局许可的密码设备进行。

6.1.7 密钥使用目的

用户的签名密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等，加密密钥可以用于信息加密和解密。

签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

所有密钥的使用，均必须遵循本 CPS 的规范。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块标准和控制

东方新诚信 CA 所用的密码设备都是经国家相关部门认可的产品，其安全性达到以下要求：

1. 接口安全：不执行规定命令以外的任何命令和操作；
2. 协议安全：所有命令的任意组合，不能得到私钥的明文；
3. 密钥安全：密钥的生成和使用必须在硬件密码设备中完成；
4. 多因素认证：密钥管理员进行密钥操作过程时，需通过数字证书、密钥管理 IC 卡、PIN 码等多因素认证；
5. 物理安全：密码设备具有物理防护措施，任何情况下的拆卸均立即销毁在设备内保存的密钥。

6.2.2 私钥的多人控制

认证系统的私钥的生成、更新、注销、备份和恢复等操作采用多人控制机制，即采取三

选二方式，将私钥的管理权限分散到 3 张密钥卡中，只有其中二至三人在场并许可的情况下，才能对私钥进行上述操作。

用户的私钥由用户自己通过密码设备控制。

6.2.3 私钥托管

用户加密证书对应的私钥由密钥管理中心托管，用户的签名证书对应的私钥由自己保管，密钥管理中心不负责托管。

密钥管理中心严格保证用户加密密钥对的安全，密钥以密文形式保存，密钥库具有最高安全级别，禁止外界非法访问。

6.2.4 私钥备份

用户的签名密钥东方新诚信 CA 不予备份。加密密钥由东方新诚信 CA 的密钥管理中心备份，备份数据以密文形式保存。

6.2.5 私钥归档

用户密钥对的归档是将已过生命周期或决定暂不使用的加密密钥以密文形式保存在数据库中，并通过数据库备份出来进行归档保存。归档后的密钥形成历史信息链，供查询或恢复。

东方新诚信 CA 提供过期的托管加密密钥的归档服务。

6.2.6 私钥导入、导出密码模块

使用东方新诚信 CA 软件可以把私钥安全导入到密码模块中，私钥无法从硬件密码模块中导出。

6.2.7 私钥在密码模块中的存储

私钥在硬件密码模块中加密保存。

6.2.8 激活私钥的方法

具有激活私钥权限的管理员使用含有自己身份的密码设备登录，启动密钥管理程序，进行激活私钥的操作，需要三名管理员同时在场。

6.2.9 解除私钥激活状态的方法

具有解除私钥激活状态权限的管理员使用含有自己身份的密码设备登录，启动密钥管理程序，进行解除私钥的操作，需要三名管理员同时在场。

6.2.10 销毁密钥的方法

具有销毁密钥权限的管理员使用含有自己身份的密码设备登录，启动密钥管理程序，进行销毁密钥的操作，需要三名管理员同时在场。

6.2.11 密码模块的评估

东方新诚信 CA 使用国家密码主管部门批准和许可的密码设备。根据东方新诚信 CA 对密码设备的性能、工作效率、供应厂商的资质等方面的评估，选择需要的密码模块。

6.2.12 智能密码钥匙的生命周期管理

东方新诚信 CA 提供符合国家密码管理相关的规定的智能密码钥匙作为订户签名密钥的生成与存储设备。东方新诚信 CA 保证证书申请者获得的智能密码钥匙能够满足证书和私钥的管理与应用需求。

1. 智能密码钥匙在提供给订户前得到了妥善的保管、包括采购、库存、发放等管理均有严格的规范予以执行；
2. 智能密码钥匙在使用时必须通过密码认证后才可以进行；
3. 智能密码钥匙的存储的私钥不可明文导出，并以密文形式存储；
4. 智能密码钥匙一旦发放给订户，将为订户持有，由订户完全控制与拥有；
5. 东方新诚信 CA 为订户提供一年的质保服务；

6. 订户证书注销或更新后，订户自行处置其持有的智能密码钥匙，东方新诚信 CA 不负责销毁或收回智能密码钥匙。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

用户证书中的公钥包括签名公钥和加密公钥。公钥的归档，其操作过程、安全措施、保存期限以及保存策略和证书保持一致，由东方新诚信 CA 定期归档。

6.3.2 证书操作期和密钥对使用期限

所有用户证书的有效期和其对应的密钥对的有效期都是一致的。

6.4 激活数据

6.4.1 激活数据的产生和安装

激活数据是私钥保护密码，智能密码钥匙（证书存储介质）出厂时设置了缺省的 PIN 值，证书制作时，将该 PIN 值修改为私钥保护密码，从而激活了智能密码钥匙的 PIN。

6.4.2 激活数据的保护

智能密码钥匙的 PIN 值使用密码信封中的密码进行保护。订户应该经常对激活数据进行修改。

6.4.3 激活数据的其他方面

只有在拥有智能密码钥匙并知道 PIN 值时才能激活证书存储介质，进而使用私钥。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

为了保证系统的正常运行，对所需要的计算机设备进行正确的选型、验收，制定操作规范。另外，本系统采用增加冗余资源的方法，使系统在有故障时仍能正常工作。

对于设备有一套完整的保管和维护制度：

1. 专人负责设备的领取和保管，做好设备的领用、进出库和报废登记；
2. 对设备定期进行检查、清洁和保养维护；
3. 制定设备维修计划，建立满足正常运转最低要求的易损坏备件库；
4. 对设备进行维修时，必须记录维修的对象、故障原因、排除方法、主要维修过程及与维修有关的情况等。

6.5.2 计算机安全评估

东方新诚信 CA 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

系统开发采用先进的安全控制理念，同时应兼顾开发环境的安全、开发人员的安全、产品维护期的配置管理安全。系统设计和开发运用软件工程的方法，做到系统的模块化和层次化，系统的容错设计采用多路并发容错方式，确保系统在出错的时候尽可能不停止服务。

6.6.2 安全管理控制

东方新诚信 CA 的信息安全管理，严格遵循国家密码管理局等主管部门的有关运行规范和东方新诚信 CA 的安全管理策略进行操作。

东方新诚信 CA 的使用具有严格的控制措施，所有和系统都经过严格的测试验证后才进

行使用。任何修改和升级均记录在案并进行版本控制、功能测试和记录。东方新诚信 CA 还对认证系统进行定期和不定期的检查与测试。

东方新诚信 CA 采取严格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。

所有设备从采购到上线前，均进行安全性检查。密码设备的采购与安装，在更加严格的安全控制机构下，进行检验、安装与验收。

对废旧设备进行处理时，必须确认其是否有影响认证业务安全性的信息存在。

6.6.3 生命期的安全控制

整个系统从设计到实现，系统的安全性始终是重点保证的。完全依据国家有关标准进行严格设计，使用的算法和密码设备均通过了国家密码管理局的鉴定与安全性审查，使用基于标准的强化安全通信协议以确保通信数据的安全；在系统安全运行方面，充分考虑了人员权限、系统备份、密钥恢复等安全运行措施，整个系统安全可靠。

6.7 网络的安全控制

系统网络安全的主要目标是保障网络基础设施运行的安全。东方新诚信 CA 采用多级防火墙、病毒防治、入侵检测、漏洞扫描等网络安全防护措施，并及时更新各网络安全设备的版本，以尽可能降低来自网络的风险。

6.8 时间戳

东方新诚信 CA 暂不采用时间戳。

7 证书、证书注销列表和在线证书状态协议

7.1 证书

东方新诚信 CA 签发的证书符合国家相关标准的要求，符合 X.509 V3 格式。

7.1.1 版本号

X.509 V3。

7.1.2 证书扩展项

东方新诚信 CA 支持使用证书标准项和标准扩展项。

1. 密钥用途。主要包括：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、只签名等；
2. 证书策略。东方新诚信 CA 签发的证书策略，符合 X.509 证书格式，这一策略信息存放在证书策略属性栏；
3. 基本限制。用于鉴别证书持有者身份；
4. CRL 发布点。东方新诚信认证系统定义的 CRL 发布点。

7.1.3 算法对象标识符

1. RSA 证书使用 SHA1WithRSAEncryption 算法，算法 OID 1.2.840.113549.1.1.5；

2. SM2 证书使用 SM3withSM2 算法，算法标识 OID 为 1.2.156.10197.1.501。

7.1.4 名称形式

东方新诚信 CA 签发的数字证书中的主体 Subject 的 X.500 DN 是 C=CN 命名空间下

的 X.500 目录唯一名字，各属性的编码一律使用 UTF8String。

主体 Subject 的 X.500 DN 支持多级 OU，其格式如下：

C=CN;

OU=XX；

OU=××；

OU=××;

OU=××;

CN=××;

C（Country）应为 CN，表示中国。

OU（Organization Unit）应为证书主体或者证书主体所属单位的名称全称；

CN（Common Name）中的内容分为 4 种：

1. 个人证书中应为证书主体的姓名；

2. 法人证书中应为证书主体单位的名称或企业税务登记号；

3. 设备证书应为证书主体设备的域名或者 IP 地址；

4. 专网证书中应为证书主体单位的内部名称。

7.1.5 名称限制

证书名称的使用采用实名制，要求证书名称与证书持有者所提交的各种证件原件、复印件、证明材料、印鉴等必须相符。

7.1.6 证书策略对象标识符

证书基本对象标识符可包含证书序列号、证书主题、证书状态、证书有效期等内容。

证书附加对象标识符可包含对证书所相对应的订户信息如订户名、电子邮件地址等内容。

每个证书模版均可根据证书对象按文件字节限定的范围内，按照管理策略的要求自定义

的扩展项进行标识符的内容加载。

7.1.7 策略限制扩展项的用法

在系统策略中可以设定扩展项结果的分页返回条数，查询结果可进行分页显示。这样，可以支持海量数据的查询，减轻系统的负担。

7.1.8 策略限定符的语法和语义

遵照国家规范的语法和语义进行编写录入。

7.1.9 关键证书策略扩展项的处理规则

根据应用场合的要求，需要对关键证书扩展项的添加、删除、修改操作进行评估和审查，以判断这些操作的必要性、正确性、规范性和合法性。

7.2 证书注销列表

东方新诚信 CA 签发的证书注销列表符合 X.509 V2 格式。

7.2.1 版本号

X.509 V2。

7.2.2 CRL 和 CRL 条目扩展项

1. CRL 扩展项：颁发机构密钥标识符 Authority Key Identifier。
2. CRL 条目扩展项：不使用 CRL 条目扩展项。

7.3 在线证书状态协议

东方新诚信 CA 为用户提供在线证书状态查询服务（OCSP 服务）。

7.3.1 版本号

使用 OCSP 版本 1（OCSP v1）。

7.3.2 OCSP 扩展项

目前未使用 OCSP 扩展项。

8 认证机构审计和其他评估

8.1 评估的频率或情形

审计是为了检查、确认东方新诚信 CA 是否按照 DFCA-CPS 及其业务规范、管理制度和安全策略开展业务，发现存在的可能风险。审计分内部审计和外部审计。

内部审计是由东方新诚信 CA 自己组织内部人员进行的审计，审计的结果可供东方新诚信 CA 改进、完善业务，内部审计结果不需要公开。

外部审计由委托第三方审计机构来承担，审计的依据包括东方新诚信 CA 所有与业务有关的安全策略、DFCA-CPS、业务规范、管理制度，以及国家或行业的相关标准。

8.2 评估者的资质

内部审计人员的选择一般包括：

1. 东方新诚信 CA 的安全负责人及安全管理人员；
2. 东方新诚信 CA 业务负责人；
3. 认证系统及信息系统负责人；
4. 人事负责人；
5. 其他需要的人员。

外部审计的审计人员的资质由第三方确定。

8.3 评估者与被评估者之间的关系

评估者与被评估者应无任何业务、财务往来或其它利害关系，足以影响评估的客观性。

8.4 评估内容

审计所涵盖的主题包括：

1. 人事审查；

2. 物理环境建设及安全运营管理规范审查；

3. 系统结构及其运行审查；

4. 密钥管理审查；

5. 客户服务及证书处理流程审查。

8.5 对问题与不足采取的措施

在内部评估完成后，评估人员需列出所有问题项目的清单，由评估人员与被评估者共同讨论有关问题，并将结果书面通知东方新诚信 CA 安全策略委员会与被评估者，进行后续处理。被评估者必须根据评估结果检查缺失与不足，提交修改与预防措施以及整改计划书，并接受评估者对整改情况的检查，以及对整改情况的再次评估。

在外部评估完成后，东方新诚信 CA 根据评估的结果检查缺失与不足，根据其提出的整改要求，提交修改与预防措施以及整改计划书，并接受外部评估机构的对整改情况的检查，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，一般不公开评估结果。

对关联方，将依据签署的协议来公布评估结果。

9 法律责任和其他业务条款

9.1 费用

9.1.1 证书签发和更新费用

数字证书的收费标准按照国家主管部门批准的收费标准执行。根据证书实际应用的需要，东方新诚信 CA 在不高于收费标准的前提下可以对证书价格进行适当调整。

证书订户有义务根据东方新诚信 CA 公布的价格或者双方签署的协议中指明的价格向东方新诚信 CA 支付费用。

9.1.2 证书查询费用

在证书有效期内，对证书信息进行查询，东方新诚信 CA 不收取查询费用。

9.1.3 证书注销或状态信息的查询费用

对于查询证书是否注销，目前，东方新诚信 CA 不收取信息访问费用。如果该项查询服务的收费政策有任何变化，东方新诚信 CA 会及时予以公布。

对于在线证书状态查询，由东方新诚信 CA 与订制者在协议中约定。

9.1.4 其他服务的费用

可根据请求者的要求，订制各类通知服务。具体服务费用，在东方新诚信 CA 与订制者签订的协议中约定。

9.1.5 退款策略

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

如果用户在证书服务期内退出数字证书服务体系，东方新诚信 CA 将不退还剩余时间的

服务费用。

9.2 财务责任

东方新诚信 CA 保证其具有维持其运作和履行其责任的财务能力。它应该有能力承担对用户、依赖方等造成的责任风险，并依据 CPS 规定，进行赔偿担保。

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. 东方新诚信 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. 东方新诚信 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. 由于东方新诚信 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. 东方新诚信 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

东方新诚信 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

东方新诚信 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

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。

对于东方新诚信 CA 来说，保密信息包括但不限于以下方面：

1. 最终用户的私人签名密钥都是保密的；
2. 保存在审计记录中的信息；
3. 年度审计结果也同样视为保密；
4. 除非有法律要求，由东方新诚信 CA 掌握的，除作为证书、CRL、认证策略被清楚发布之外的个人和单位的信息需要保密。

东方新诚信 CA 不保存任何证书应用系统的交易信息。

除非法律明文规定，东方新诚信 CA 没有义务公布或透露用户数字证书以外的信息。

9.3.2 不属于保密的信息

与证书有关的申请流程、申请需要的手续、申请操作指南等信息是公开的。东方新诚信 CA 在处理申请业务时可以利用这些信息，包括发布上述信息给第三方。

用户数字证书的相关信息可以通过东方新诚信 CA 目录服务等方式向外公布。

东方新诚信 CA 在其目录服务器中公布证书的注销信息，供网上查询。

9.3.3 保护保密信息的责任

各方有保护自己和其他人员或单位的机密信息并保证不泄露给第三方的责任。不将机密数据和信息（也不会促使或允许他人将机密数据和信息）用于协议项下活动目的之外的其他用途，包括但不限于：将此保密信息的全部或部分进行仿造、反向工程、反汇编、逆向推导；在披露当时，如果已明确表示机密数据和信息不得复印、复制或储存于任何数据存储或检索系统，接受方不得复印、复制或储存机密数据和信息。

当东方新诚信 CA 在任何法律、法规或规章的要求下，或在法院的要求下必须提供本 DFCA-CPS 中具有保密性质的信息时，东方新诚信 CA 应按照要求，向执法部门公布相关的保密信息，东方新诚信 CA 无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

9.4 个人隐私保密

9.4.1 隐私保密方案

除非证书申请人主动提供，东方新诚信 CA 保证不会截取任何证书申请人的资料。

东方新诚信 CA 应保护证书申请人所提供的，证明其身份的资料。东方新诚信 CA 应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。

9.4.2 作为隐私处理的信息

证书申请人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

证书申请人提供的用来构成数字证书内容的资料不认为是隐私信息。

数字证书是公开的，通过东方新诚信 CA 目录服务等方式向外公布。

9.4.4 保护隐私的责任

接收到隐私信息的参与者有责任保护隐私信息不被泄漏、使用或发布给第三方。

9.4.5 使用隐私信息的告知与同意

使用隐私信息，须获得本人同意。

9.4.6 依法律或行政程序的信息披露

当东方新诚信 CA 在任何法律、法规或规章的要求下，或在法院的要求下必须提供证书申请人的特定资料或隐私信息时，东方新诚信 CA 按照法律、法规或规章的要求或法院的要求，向执法部门公布相关信息，东方新诚信 CA 无须承担任何责任。这种提供不能被视为违反了隐私保护的责任和义务。

9.4.7 其他信息披露情形

其他信息的披露遵循国家的相关规定处理。

9.5 知识产权

除非额外声明，东方新诚信 CA 享有并保留对证书以及东方新诚信 CA 提供的全部软件的一切知识产权，包括所有权、名称权和利益分享权等。东方新诚信 CA 有权决定关联机构采用的软件系统，选择采取的形式、方法、时间、过程和模型，以保证系统的兼容和互通。

按本 DFCA-CPS 的规定，所有由东方新诚信 CA 签发的证书和提供的软件中使用、体现和相关的一切版权、商标和其他知识产权均属于东方新诚信 CA 所有，这些知识产权包括所有相关的文件和使用手册。注册机构应征得东方新诚信 CA 的同意使用相关的文件和手册，并有责任和义务提出修改意见。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

东方新诚信 CA 在提供电子认证服务活动过程中的承诺如下：

1. 东方新诚信 CA 遵守《中华人民共和国电子签名法》及相关法律的规定，接受信息产业部的领导，对签发的数字证书承担相应的法律责任；
2. 东方新诚信 CA 保证使用的系统及密码符合国家政策与标准，保证自身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定；
3. 除非已通过东方新诚信 CA 证书库发出了东方新诚信 CA 的私钥被破坏或被盗的通知，东方新诚信 CA 保证其私钥是安全的；
4. 东方新诚信 CA 签发给用户的证书符合东方新诚信 CA 的 CPS 的所有实质性要求；
5. 东方新诚信 CA 将向证书用户通报任何已知的、将在本质上影响用户的证书的有效性和可靠性事件；
6. 东方新诚信 CA 将及时注销证书；
7. 证书公开发布后，东方新诚信 CA 向证书依赖方证明，除未经验证的用户信息外，证书中的其他用户信息都是准确的。

9.6.2 注册机构的陈述与担保

东方新诚信 CA 的注册机构在参与电子认证服务过程中的承诺如下：

1. 提供给证书用户的注册过程完全符合东方新诚信 CA 的 CPS 的所有实质性要求；
2. 在东方新诚信 CA 生成证书时，不会因为注册机构的失误而导致证书中的信息与证书申请人的信息不一致；
3. 注册机构将按 CPS 的规定，及时向东方新诚信 CA 提交证书申请、注销、更新等服务请求。

9.6.3 订户的陈述与担保

订户一旦接受东方新诚信 CA 签发的证书，就被视为向东方新诚信 CA、注册机构及信赖证书的有关当事人作出以下承诺：

1. 订户需熟悉本 DFCA-CPS 的条款和与其证书相关的证书政策，还需遵守证书持有人证书使用方面的有关限制；
2. 订户在证书申请表上填列的所有声明和信息必须是完整、真实和正确的，可供东方新诚信 CA 或注册机构检查和核实；
3. 订户应当妥善保管私钥，采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件的发生；
4. 私钥为订户本身访问和使用，订户对使用私钥的行为负责；
5. 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、泄密以及其他情况，订户应立刻通知东方新诚信 CA 和注册机构，申请采取注销等处理措施；
6. 订户已知其证书被冒用、破解或被他人非法使用时，应及时通知东方新诚信 CA 注销其证书。

9.6.4 依赖方的陈述与担保

依赖方必须熟悉本 DFCA-CPS 的条款以及和用户数字证书相关的证书政策，并确保本身的证书用于申请时预定的目的。

依赖方在信赖用户的数字证书前，必须采取合理步骤，查证用户数字证书及数字签名的有效性。

所有依赖方必须承认，他们对证书的信赖行为就表明他们承认了解本 DFCA-CPS 的有关条款。

9.6.5 其他参与者的陈述与担保

其他参与者的陈述与担保同“ 9.6.4 依赖方的陈述与担保 ”。

9.7 担保免责

东方新诚信 CA 在下列情况下免于承担责任：

1. 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赔偿责任。这些事件包括但不限于劳动纠纷、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；
2. 如果由于非东方新诚 CA 的原因而造成的设备故障、线路中断，导致签发数字证书错误、延误、中断或无法签发，东方新诚信 CA 不负任何赔偿责任；
3. 本 CPS 的内容，没有任何信息可以暗示或解释成，东方新诚信 CA 必须承担其他的义务或东方新诚信 CA 必须对其行为作出其他承诺。包括不承担其他任何形式的任何保证和义务，任何对特殊目的适用性的保证；
4. 如果申请者故意或无意地提供不完整、不可靠或已过期的，包括但不限于伪造、篡改、虚假的信息，而其又根据正常的流程提供了必须的审核文件，由此得到了东方新诚信 CA 签发的数字证书。由此引起的法律问题、经济纠纷应由申请人全部承担，东方新诚信 CA 不承担与该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和举证帮助；
5. 东方新诚信 CA 不承担任何其他未经授权的人或组织以东方新诚信 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；
6. 对于由于证书、签名或根据本 CPS 而提供或设计的任何其他交易或服务的使用、签发、授权、执行或拒绝执行而导致的或与之有关的任何间接性的、特别性的、附带性的、或结果性的损失，或任何利益损失、数据丢失，或其他间接性的、结果性的或惩罚性损失，无论是否可以合理预见，东方新诚信 CA 将不会对此负责，即使东方新诚信 CA 曾经警告过这种损害的可能性；
7. 东方新诚信 CA 对签发的各类证书的适用范围有明确的规定，若证书订户将其证书用于其他不被允许的用途，东方新诚信 CA 不承担任何责任，无论这种使用是滞造成损失；
8. 东方新诚信 CA 在法律许可的法律内，根据法律、政策等以及受害者的要求，如实提供不可抵赖的电子签名依据，但并不对此承担法律或政策规定之外的责任。

9.8 有限责任

根据《中华人民共和国公司法》、《中华人民共和国电子签名法》和其他法律法规的规定，作为依法设立的有限责任公司，东方新诚信 CA 在承担任何责任和义务时，只承担法律范围内的有限责任。

东方新诚信 CA 在与订户和依赖方签订的协议中，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

9.9.1 赔偿范围

在认证活动中产生的赔偿，都以本 CPS 的规定为处理依据，法律法规另有要求的除外。

1. 东方新诚信 CA 的赔偿责任

(1) 在签发证书时，如果未按照本 CPS 的规定进行处理，或者违反法律法规的要求而造成的证书订户损失的，东方新诚信 CA 应承担赔偿责任；

(2) 因为操作人员恶意、故意或疏忽，未按照本 CPS 的规定办理证书的签发、注销等请求，布造成证书订户损失的，东方新诚信 CA 应赔偿订户的损失；

(3) 因东方新诚信 CA 的根密钥出现问题，造成订户证书出现问题，东方新诚信 CA 应赔偿相关损失；

(4) 证书订户或其他有权提出注销证书的人提出注销请求后，到东方新诚信 CA 将该证书注销信息予以发布的期间，如果该证书被用以进行非法交易，或进行交易时产生纠纷的，如果东方新诚信 CA 按照本 CPS 的规范进行了有关操作，东方新诚信 CA 不承担任何损害赔偿责任；

(5) 证书订户赔偿的追溯有效期限，按照法律法规的要求进行操作。

2. 注册机构的赔偿责任

(1) 注册机构及其操作人员没有妥善保管订户的注册和身份验证的相关隐私信息，而造成订户信息泄漏、被冒用、自发或者任意使用导致产生损失的，注册机构应承担损

害赔偿责任；

(2) 如果因为操作人员故意、恶意或者疏忽，没有按照本 CPS 的规定办理证书服务注册，或者违反法律法规而造成订户损失的，注册机构应赔偿用户的直接损失，以及其他随之产生的附带损失和相关补偿；

(3) 因为注册机构的原因造成系统或软件错误，未能在本 CPS 规定的时间内，将订户的证书申请、注销、更新等请求信息发给东方新诚信 CA，而导致订户或依赖方损失的，注册机构应承担所有的损害赔偿责任；

(4) 该类赔偿的追溯有效期限，按照有关法律法规的要求进行操作。

3. 订户的赔偿责任

(1) 订户申请注册证书时，因故意、过失或者恶意提供不真实资料，导致造成东方新诚信 CA 及其授权的证书服务机构或者第三方遭受损害的，订户应赔偿一切损害责任；

(2) 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知东方新诚信 CA 及其授权的证书服务机构，以及不当交付他人使用造成东方新诚信 CA 及其授权的证书服务机构、第三方遭受损害的，订户应承担一切损害赔偿责任；

(3) 订户使用证书或者依赖方信任证书的行为，有违反本 CPS 及相关操作规范，或者将证书用于非本 CPS 规定的业务范围的，订户或者依赖方应自行承担一切损害赔偿责任；

(4) 用户使用或信赖证书时，未能按照本 CPS 等规范进行合理审核，导致东方新诚信 CA 及其授权的证书服务机构或者第三方遭受损害的，应由该用户承担一切损害赔偿责任；

(5) 证书订户或者其他有权提出注销证书的实体提出注销请求后，到东方新诚信 CA 将该证书注销信息予以发布期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果东方新诚信 CA 按照本 CPS 的规范进行了有关操作，那么该证书订户必须承担所有损害赔偿责任；

(6) 东方新诚信 CA 与之签署的协议另有赔偿规定的，参照其规定。

9.9.2 赔偿限额

东方新诚信 CA 及其授权的注册机构，对所有当事人（包括但不限于订户、申请者、接受者或信赖方）的合计赔偿责任，不可能超过发下所述对这些证书的封顶赔偿金额：

对于有关一张特定证书的所有签名和交易处理的总计，东方新诚信 CA 及其授权的证书服务机构对于任何人（或者其他实体）有关该特定证书的合计赔偿责任应该限制在一个不超出下述数额的范围内（单位：人民币元）

1. 个人类证书，不超过 2,000 元

2. 单位类证书，不超过 50,000 元

3. 设备类证书，不超过 80,000 元

本条款限制用于一定形式的损害，包括但不限于任何人或实体（包括但不限于订户、证书申请者、接收方或者信赖方）由于信任或者使用东方新诚信 CA 签发、管理、使用或注销的证书或已过期证书而导致的直接的、补偿性的、间接的、特别的、结果的、惩戒性的或意外的损害。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任。每份证书的赔偿均有限额而不考虑签名、交易处理或其他有关的索赔数量。当超过赔偿限额时，除非得到依法判决或仲裁，可用的赔偿限额将首先分配给最早得到索赔解决的一方。东方新诚信 CA 没有责任为每张证书支付高出赔偿限额总和的赔偿，而不管高出赔偿限额总和在索赔提出之间是如何分配的。

9.10 有效期限与终止

9.10.1 有效期限

本 DFCA-CPS 自发布之日起正式生效。

更新版本 DFCA-CPS 自发布之日起三十日正式生效。

本 DFCA-CPS 中将详细注明版本号及发布日期。

9.10.2 终止

当新版本的 DFCA-CPS 正式发布生效时，旧版本的 DFCA-CPS 自动终止。

9.10.3 效力的终止与保留

DFCA-CPS 的某些条款在终止后继续有效，如知识产权承认和保密条款。另外，各参与方应返还保密信息到其拥有者。

9.11 对参与者的个别通告与沟通

认证活动的某一参与方与另一参与方进行通信时必须使用安全通道，以使其通信过程在法律上有效。

9.12 修订

9.12.1 修订程序

当本 DFCA-CPS 不适用时，由东方新诚信 CA 的 CPS 策略委员会组织 CPS 编写小组进行修订。

修订完成后，东方新诚信 CACPS 策略委员会进行审批，审批通过后将在东方新诚信 CA 的网站上发布新的 DFCA-CPS。

DFCA-CPS 将进行严格的版本控制。

9.12.2 通知机制和期限

本 DFCA-CPS 在在东方新诚信 CA 的网站上发布。

版本更新时，最新版本的 DFCA-CPS 在在东方新诚信 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

当管辖法律、适用标准及操作规范等有重大改变时，必须修改 DFCA-CPS。

9.13 争议处理

证书用户、依赖方等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 DFCA-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. 任何因与东方新诚信 CA 或授权机构就本 DFCA-CPS 所产生的任何争议而提起诉讼的，受东方新诚信 CA 所在地的人民法院管辖。

9.14 管辖法律

本 DFCA-CPS 在各方面服从中国法律和法规的管制和解释，包括但不限于《中华人民共和国电子签名法》及《电子认证服务管理办法》等。

9.15 与适用法律的符合性

无论在任何情况下，本 DFCA-CPS 的执行、解释、翻译和有效性均适用中华人民共和国的法律。

9.16 一般条款

9.16.1 完整协议

本 DFCA-CPS 将替代先前的、与主题相关的书面或口头解释。

9.16.2 转让

东方新诚信 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

当法庭或其他仲裁机构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

免除一方对合同某一项的违反应该承担的责任，不意味着继续免除或未来免除这一方对合同其他项的违反应该承担的责任。

9.16.5 不可抗力

不可抗力是指不能预见、不能避免并不能克服的客观情况。不可抗力既可以是自然现象或者自然灾害，如地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；也可以是社会现象、社会异常事件或者政府行为，如合同订立后政府颁发新的政策、法律和行政法规，致使合同无法履行，再如战争、罢工、骚乱等社会异常事件。

在数字证书认证活动中，东方新诚信 CA 由于不可抗力因素而暂停或终止全部或部分证书服务的，可根据不可抗力的影响而部分或者全部免除违约责任。其他认证各方（如用户）不得提出异议或者申请任何补偿。

9.17 其他条款

东方新诚信 CA 对本 DFCA-CPS 拥有最终解释权。