# 天津市中环认证服务有限公司

# 电子认证业务规则

# V1.4

天津市中环认证服务有限公司

2023 年 1 月

# 版本信息

| 当前版本号 | 最近更新日期 |
| --- | --- |
| V1.4 | 2023/1 |

修订记录：

| 日期 | 修订说明 | 修订版本 | 修订人 | 审核人 |
| --- | --- | --- | --- | --- |
| 2018.8 | 创建本 CPS | V1.0 | 李维 | 安全策略委员会 |
| 2020.8.3 | 修订官方网址、邮箱；增加提供设备证书身份鉴别方式；增加了企业、个人身份在线审核的方式； | V1.1 | 李维 | 安全策略委员会 |
| 2020.11.22 | 增加云证书、事件证书、手机证书身份标识与鉴别；云证书、事件证书、手机证书生命周期操作要求；云证书、事件证书、手机证书密钥的安全控制 | V1.2 | 李维 | 安全策略委员会 |
| 2022.1.21 | 修订 1.5.2 联系人地址；5.1.3 机房等级、相对湿度数值 | V1.3 | 李维 | 安全策略委员会 |
| 2023.1.5 | 修订版权声明中联系电话；<br>修订 3.2.2 组织机构身份的鉴别，增加法定代表人身份鉴别的方式。 | V1.4 | 李维 | 安全策略委员会 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# 电子认证业务规则

## 天津市中环认证服务有限公司版权声明



对任何复制及传播本文件的请求，请寄往：天津市中环认证服务有限公司。地址：天津市河西区体院北环湖中道9号。邮编：300060。电话：022-23522103/400-0566-110，传真：022-23522103。

目录

# 第一章 概括性描述

## 1.1 概述

### 1.1.1 公司简介

天津市中环认证服务有限公司（以下简称“中环CA”）成立于2018年，注册资金5千万元，是天津市中环系统工程有限责任公司的国有控股子公司，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。

天津市中环认证服务有限公司依照《中华人民共和国电子签名法》、《电子认证服务密码管理办法》和《电子认证服务管理办法》的要求，于2017年10月完成系统建设。中环CA机房位于天津市河西区体院北环湖中道9号科研楼一层，占地面积98平方米，整体设施设备齐全、系统建设符合国家相关标准要求。

中环CA自成立以来，严格按照国家规定的各项要求进行系统建设和管理，于2018年5月获得了国家密码管理局颁发的《电子认证服务使用密码许可证》，2018年11月获得了工业和信息化部颁发的《电子认证服务许可证》，2019年1月，中环CA取得了国家密码管理局电子政务电子认证服务资质。

### 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,详细阐述了中环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。

本规范适用于中环CA及其分支机构，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，以确保中环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。对于中环CA所提供的认证服务过程的责任范围，本业务规则也给予了明确的规定。

## 1.2 文档名称与标识

### 1.2.1 名称

本文档称为《天津市中环认证服务有限公司电子认证业务规则》（简称《中环CA CPS》），是中环CA对所提供的认证及相关业务的全面描述，对象标识符CPS为“Certificate Practice Statement”的缩写。本文档中，CPS等同于本节中定义的文档名称和适用名称。

### 1.2.2 标识

本CPS没有向相关管理机构注册对象标识符（OID）。

### 1.2.3 版本

本规则为中环CA发布的第三个版本，即《天津市中环电子认证服有限公司电子认证业务规则》V1.2。

### 1.2.4 发布

本电子认证业务规则文档的发布以电子的方式，在中环CA网站发布。

网站地址：https://www.tjzhca.com

LDAP查询地址:61.181.121.102:389

## 1.3 电子认证活动参与者

### 1.3.1 电子认证服务机构

中环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。中环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。

中环CA建设和运营的认证系统是多层次的CA结构模式，中环CA及其下层CA系统统称电子认证服务机构，这些签发实体均可发放证书，中环CA的认证系统是所有中环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，中环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。中环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。中环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机构或个人，不允许用作商业利益方面的用途。

注册机构可以由中环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，中环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。注册分支机构由中环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）

经过中环CA审查，中环CA授权特定机构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，必须与中环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。受理点负责向中环CA授权的注册机构或中环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）

在电子签名应用中，订户即是电子签名人、证书持有人，是中环CA颁发证书的所有最终用户，可以是个人、机构或基础设施的组成部件如路由器、防火墙、服务器或用于安全通信的其他设备。

### 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）

指为中环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

证书应用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。

根据证书的功能以及使用证书的实际应用，目前中环CA签发的主要证书类型分为通用型证书（个人、机构和设备等证书）、云证书、事件证书、手机证书具体如下：

个人证书：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；

机构证书：机构包括企事业机构、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；

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。

云证书：面向移动互联网和云服务等新技术领域业务场景的签名需要，中环CA签发基于云服务的数字证书。该证书是在业务过程中订户通过应用系统实名认证后，向中环CA申请签发的证书。订户将证书私钥托管到中环CA的专用的密码设备中保存，中环CA确保订户私钥的安全性。订户自己保存调用私钥的方法（包括但不限于PIN码、短信验证码等）

事件证书：中环CA面向签名行为业务场景签发出的数字证书。在业务过程中，根据订户提交的业务场景中相关信息（电子文档、签名行为特征信息、手写笔迹或其他签名行为证据信息等）自动固化至数字证书的扩展域，签发出事件证书。事件证书所对应的私钥为一次性使用，对业务场景的信息数据进行电子签名，在使用后即被销毁。

手机证书：中环CA面向移动互联网等新技术领域所签发出的手机证书，该类型证书支持在使用移动端设备的环境中应用数字签名、身份认证等证书服务功能。通过手机证书与服务，在移动互联网领域可以实现各参与主体身份的真实性、信息的完整性以及签名行为的不可抵赖性。

### 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。

中环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）中环CA与订户约定的证书禁止应用的范围。

## 1.5 策略管理

中环CA安全策略委员会是中环CA电子认证服务所有策略的最高管理机构，负责审核批准CPS，并作为CPS实施检查监督的最高决定机构。

### 1.5.1 策略文档管理机构

策略文档管理机构为中环CA安全策略委员会，作为策略管理机构负责制订、发布、更新本CPS。中环CA安全策略委员会来自于公司管理层、运营管理部、安全管理部、客户服务部、行政管理部等拥有决策权的合适代表。

中环CA安全策略委员会的所有成员在就证书策略进行管理和批准时，均享有一票决定权，如果选票相同，委员会主任可拥有双票决定权。

本策略文档的对外咨询服务等日常工作由安全管理部负责。

### 1.5.2 联系人

中环CA将对电子认证业务规则进行严格的版本控制，并由中环CA指定专人负责。

联系人：李维

电话：022-23522103/400-0655-110

传真：022-23522103

地址：天津市河西区体院北环湖中道9号科研楼210室（300060）

电子邮件：tjzhca@126.com

网站地址：https://www.tjzhca.com

### 1.5.3 决定 CPS 符合策略的机构

中环CA安全策略委员会是公司CPS策略制定的最高权威机构，审定批准CPS，决定CPS是否符合策略。

### 1.5.4 CPS 批准程序

按照工业和信息化部公布的《电子认证业务规则规范》的要求，在中环CA电子认证业务规则做出任何变动之前，中环CA安全部门将对提供的变动建议进行研究，在征询中环CA法律顾问有关方面的意见后，提交中环CA安全策略委员会审批。中环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30日内向工业和信息化部备案。

### 1.5.5 CPS 修订

中环CA根据国家的政策法规、技术要求、标准的变化及业务发展情况及时修订本CPS，CPS编写小组根据相关的情况拟定CPS修订建议，提交中环CA安全策略委员会审核，经该委员会批准后，正式在中环CA官方网站上发布。

修订后的CPS，从对外发布之日起30日之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冻结证书。处理订户撤销或冻结其证书的请求，同意或拒绝订户更新其证书或密钥的请求。但是，RA并不签发证书（即RA代表CA承担某些任务）。

**数字证书（Digital Certificate）**

数字证书是电子认证服务机构签发的用以证明证书持有人的电子签名、身份、资格及其他有关信息的电子文件。证书包含有公开密钥拥有者的信息、公开密钥、签名算法和CA的数字签名。

**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）**

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

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

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

**私钥（Private key）**

私钥（Private key）是在公钥基础设施（PKI）中为一个密码串，由特定算法与公钥一起生成，用于解密信息或进行数字签名。在数字签名中又称为电子签名制作数据，是在电子签名过程中使用的、将电子签名与电子签名人可靠地联系起来的字符、编码等数据。

**公钥(Public key)**

公钥(Public key)是在公钥基础设施（PKI）中为一个密码串，由特定算法与私钥一起生成，用于加密信息或验证数字签名。在数字签名中又称为电子签名验证数据，是用于验证电子签名的数据，包括代码、口令等。

**甄别名(DN , Distinguished Name)**

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

# 第二章 信息发布与信息管理

## 2.1 中环 CA 信息库

中环CA信息库是一个对外公开的信息库，它能够保存、取回证书及与证书有关的信息。中环CA信息库内容包括但不限于以下内容：CPS现行和历史版本、证书、CRL、订户协议，以及其它由中环CA不定期发布的信息。中环CA将及时发布包括证书、CPS修订和其它资料等内容，这些内容必须保持与CPS及有关法律法规一致。

中环CA信息库可以通过网址：https://www.tjzhca.com查询，或由中环CA随时指定的其它通讯方法获得。

## 2.2 认证信息的发布

中环CA在官方网站https://www.tjzhca.com发布信息库，该网站是中环CA发布所有信息最主要、最及时、最权威的渠道。

中环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中环CA的目录服务器获取证书的信息和吊销证书列表；中环CA也提供在线证书状态查询服务，订户或依赖方可实时查询证书的状态信息。同时，中环CA也将会根据需要采取其他可能的形式进行信息发布。

## 2.3 发布的时间和频率

中环CA在订户证书签发或者撤销时，通过目录服务器或官方网站自动将证书和CRL发布，发布周期为不大于24小时，即在24小时内发布最新CRL；在紧急的情况下，中环CA可以自行决定证书和CRL的发布时间。信息库其他内容的发布时间和频率，由中环CA独立做出决定，这种发布应该是即时的、高效的，并且是符合国家法律的要求的。

## 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，中环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。但只有中环CA有权对公布的各类信息进行处理。

### 2.4.2 信息访问控制和安全审计

中环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中环CA工作人员才能控制和修改。

# 第三章 身份标识与鉴别

## 3.1 命名

### 3.1.1 名称类型

中环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。订户的标识命名，以甄别名（Distinguished Name）形式包含在证书主体内，是订户的唯一识别名。

中环CA的证书符合X.509标准，分配给订户实体的甄别名，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 | 中环 |
| Organizational Unit（OU） = | 组织机构 | 认证服务有限公司 |
| State or Province （S） = | 省 | 天津 |
| Locality（L） = | 区 | 河西区 |
| Common Name（CN） = | 通用名 | ZHCA |
| Email= | 邮件地址 | tjzhca@126.com |

中环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 |
| Organization（O） = | 组织 | ZHCA |
| Common Name（CN） = | 通用名 | ZHCA |

### 3.1.2 对名称意义化的要求

中环CA签发的个人证书、机构证书、设备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，中环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、机构或设备）唯一联系起来。

### 3.1.3 订户的匿名或假名

中环CA的订户在证书中的名称不可以是假名或匿名，仅接受可追溯的名称作为唯一标识符。使用假名或伪造材料者申请的证书无效，一经证实立即予以撤销。

### 3.1.4 理解不同名称形式的规则

中环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中环CA定义与解释。

### 3.1.5 名称的唯一性

在中环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。中环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。中环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

中环CA证明拥有私钥的方法是根据证书申请信息进行验证。在中环CA证书服务体系中，用户证书请求信息中包含用私钥进行的数字签名，中环CA用其对应的公钥来验证这个签名，验证成功后，证书申请人被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

对组织机构的身份或组织机构中个人身份的鉴别按照以下方式进行：

1. 组织机构证明材料的提交方式分为以下几种：

1）组织机构经办人携带机构有效证件原件或复印件（加盖公章）、法定代表人身份证原件或复印件（加盖公章）、经办人身份证原件或复印件（加盖公章），到数字证书业务受理机构，填写数字证书申请表，经过机构盖章，表示接受证书业务申请的有关条款，并承担相应的责任。

2）组织机构经办人通过中环CA提供的自助服务平台办理，提交经过机构盖章的申请表、机构有效证件原件或复印件（加盖公章）、法定代表人身份证原件或复印件（加盖公章）、经办人身份证原件或复印件（加盖公章）的扫描件或照片，上传到中环CA自助服务系统中进行在线申请。

或通过权威第三方数据库查询系统来进行机构身份鉴别审核。

3）对于证书应用于甲方内部环境中，可由甲方单位出具证明的形式进行身份确认，由甲方委托的经办人进行证书申请。

2.中环CA发证机构的审核人员对订户申请资料的真实性进行审查并进行批准或拒绝的操作。

### 3.2.3 个人身份的鉴别

中环CA的个人证书签发给合法的个人申请者，中环CA需要严格审核个人申请者的身份。

通过鉴别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。

中环CA对个人身份鉴别的模式有以下几种：

1. 面对面方式

个人可持上述有效身份证件亲自到中环CA授权的注册机构提交书面证书申请表和身份证件的复印件等申请材料到现场办理。

2. 在线方式

个人可通过中环CA自助服务平台提交经本人签字确认的证书申请表、有效的个人身份证件原件的电子版照片，通过平台上传到中环CA自助服务系统中进行在线申请，中环CA发证机构的审核人员对订户申请资料的真实性进行审查并进行批准或拒绝的操作。

或使用具有人体生物特征识别、活体检测、身份信息权威数据源比对、金融验证、手机验证等认证技术进行身份鉴别。

### 3.2.4 设备身份的鉴别

如果证书的名称为域名（或IP地址），除了在对申请者递交的书面材料进行审核外，中环CA需要申请者提供额外的域名（IP地址）使用权证明材料，以确定申请者是否有权使用相应的域名（IP 地址）。中环CA在进行了法律规定的有限审查后，不承担对申请者申请资料进行合法的鉴别，申请者自行负责申请材料的真实性。

### 3.2.5 云证书订户身份的鉴别

云证书订户身份的鉴别参照个人身份和机构身份鉴别方法进行鉴别。

### 3.2.6 事件证书订户身份的鉴别

事件证书订户身份的鉴别参照个人身份和机构身份鉴别方法进行鉴别，也可以采取包括录音、录像等有效的身份核验方式进行自动鉴别。

### 3.2.7 手机证书订户身份的鉴别

手机证书身份鉴别除采用传统线下方式提交材料进行鉴别，也可以通过移动化、在线化的方式来进行鉴别。订户可通过手机拍照、证件照上传等方式来提交材料。

### 3.2.8 没有验证的订户信息

除该类型证书所必须要求的身份信息需要得到明确、可靠的验证以外，中环CA不对申请时的其他信息予以验证。

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

### 3.2.9 授权确认

证书申请者申请某一类型的证书时，中环CA和其授权的证书服务机构还需审核申请经办人的身份和资格，包括必需的身份资料和授权证明文件。机构或个人在中环CA数字证书申请文件上签字或加盖公章后，则证明其对办理人员的授权确认。

### 3.2.10 互操作准则

对于中环CA外的其他证书服务机构颁发的证书，可以与中环CA进行互操作，但是必须符合中环CA的电子认证业务规则，并且与中环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。同时产生一个新的密钥对，称作“密钥更新”,对于中环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签发有相同签发者、主体名和证书用途的证书。我们在表述证书更新时包含密钥更新。

### 3.3.1 常规密钥更新的标识与鉴别

对于常规通用型证书密钥更新，订户可以用原有的私钥对更新请求进行签名。中环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。

中环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，中环CA会告知订户使用原密钥对加密的文件或数据进行解密，如订户未按照中环CA所告知的内容进行文件或数据解密，由此造成的损失，中环CA将不承担责任。

云证书密钥更新中，通过订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，CA 机构使用订户原有公钥验证确认签名来进行订户身份标识和鉴别。

事件证书没有密钥更新。

手机证书的密钥更新，和通用型证书的密钥更新的标识与鉴别要求一致。

### 3.3.2 撤销后密钥更新的标识与鉴别

中环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中环CA申请重新签发证书。

## 3.4 撤销请求的标识与鉴别

在中环CA的证书业务中，证书撤销请求可以来自订户，也可以来自中环CA。当中环CA授权的发证机构发现订户有如本CPS4.9.1中描述的证书撤销的情况时，有权撤销证书，这种情况无须进行鉴证。如果订户主动要求撤销证书，则需要递交初始身份验证时的申请材料。如果是司法机关依法提出撤销，中环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

中环CA授权的发证机构提供完整的数字证书周期，包括申请、审核、制证、发布、更新、变更、冻结/解冻、证书恢复、撤销、归档等过程，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，中环CA签发的通用型证书、云证书、手机证书默认有效期为1年；中环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

证书申请实体包括个人和具有独立法人资格的组织机构（包括行政机关、事业机构、社会团体和人民团体等）。

### 4.1.2 申请过程与责任

1. 证书的注册过程

中环CA的数字证书申请有线下申请和在线申请两种方式，订户将填写完整的申请表及其它证明材料递交给中环CA的注册机构进行证书申请，注册机构审核通过后，录入申请资料。其中审核员和业务办理员分别为两个不同的系统操作人员。

注册机构向中环CA提交证书请求，通过应用安全协议发送至中环CA。

中环CA根据注册机构的请求签发证书。

2. 责任

订户有责任向中环CA提供真实、完整和准确的证书申请信息和资料。

注册机构承担对订户提供的证书申请信息与身份证明资料的一致性检查工作，同时承担相应审核责任。

## 4.2 证书申请处理

### 4.2.1 执行识别与鉴别功能

当中环CA及其注册机构接受到订户的证书申请后，应按本CPS3.2.2、3.2.3、3.2.4及3.2.5的要求，对订户进行身份识别与鉴别。

中环CA在处理证书申请过程中，将通过有效手段确保证书信息与正确的申请信息相符，并将证书签发给正确的申请者。

### 4.2.2 证书申请批准和拒绝

依据识别与鉴别的信息，中环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，中环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，中环CA授权的发证机构有权拒绝订户的证书申请：

订户不提供鉴别所需材料或在鉴别过程中不予配合；

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）中环CA授权的发证机构认为批准该申请将会对中环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

中环CA授权的发证机构必须在一个工作日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。

事件证书申请为即时处理。

## 4.3 证书签发

### 4.3.1 证书签发中注册机构和电子认证服务机构的行为

在证书的签发过程中RA的管理员负责证书申请的审批，并通过操作RA系统将签发证书的请求发往CA的证书签发系统。RA发往CA的证书签发请求信息有RA的身份鉴别的电子签名与信息加密措施，并确保请求发至正确的CA证书签发系统。

CA的证书签发系统在获得RA的证书签发请求后，对来自RA的信息进行鉴别与解密，对于有效的证书签发请求，证书签发系统签发订户证书。

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

通常中环CA签发的证书在24小时内生效。

### 4.3.2 订户证书签发的通知

对于通用型证书，中环CA会采取以下几种通告方式告知订户：

1、通知订户到注册机构或受理点面对面的方式领取证书；

2、电子邮件（Email）或短信；

3、其他中环CA认为安全可行的方式。

对于云证书，通过证书申请程序或系统对订户进行通告。

对于事件证书，订户成功完成数字签名，即视为CA机构证书签发成功，CA机构不再就证书签发向订户进行其他方式的通告。

对于手机证书，订户所使用移动终端应用程序会有数字证书已签发或下载成功的展示，中环CA不再就证书签发向订户进行其他方式的通告。

## 4.4 证书接受

### 4.4.1 构成接受证书的行为

在中环CA通用型证书签发完成后，中环CA将把数字证书当面给订户，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。

云证书签发完成后，并将证书应用于对应的电子签名时起，就被视为同意接受证书。

中环CA签发事件证书给订户，证书应用于对应的电子签名时起，就被视为同意接受证书。

中环CA为订户签发手机证书，订户所使用移动终端设备或 APP 应用程序接收到数字证书起，就被视为同意接受证书。

### 4.4.2 电子认证服务机构对证书的发布

通用型证书的订户接受证书后，中环CA在24小时内将该订户证书发布到中环CA的目录服务系统。

中环CA采用主、从目录服务器结构来发布所签发证书。签发完成的数据直接发布到主目录服务器中，然后通过主从映射，将主目录服务器的数据自动同步到从目录服务器中，供订户和依赖方查询和下载。

中环CA签发的云证书，会将证书信息记录在指定的数据库中，订户终端会对证书状态实时检测。根据依赖方约定，可向依赖方提供状态查询服务。

中环CA签发事件证书，会将证书信息进行保存。根据依赖方约定，可向依赖方提供状态查询服务。

中环CA不提供手机证书的发布。根据依赖方约定，可向依赖方提供证书查询服务。

### 4.4.3 电子认证服务机构对其他实体的通告

中环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中环CA查询服务获得所需证书信息。

## 4.5 密钥对和证书的使用

中环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，否则中环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

通用型证书的订户接受到数字证书后，应妥善保存其证书对应的私钥。订户可以从中环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。

云证书由订户通过PIN码或短信验证码等方式调用云端托管私钥完成数字签名。订户只能在指定的应用范围内使用私钥和证书，订户只有在接受了相关证书之后才能使用对应的私钥，并且在证书到期或被撤销之后，订户必须停止使用该证书对应的私钥。

事件证书仅应用于订户对应的电子签名行为，订户只能在该次电子签名中使用私钥和证书，订户只有在接受了相关证书之后，才能使用对应的私钥执行电子签名运算。私钥将在完成本次电子签名运算后进行销毁，之后订户须停止使用该证书对应的私钥。

手机证书必须由订户和签名服务云端协同配合才能完成一次数字签名。订户只能在指定的应用范围内使用私钥和证书，订户只有在接受了相关证书之后才能使用对应的私钥，并且在证书到期或被撤销之后，订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

依赖方只能在接受中环CA协议要求的前提下，才能依赖中环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）获得对应的证书及信任链；

2）验证证书的有效性；

3）确认该签名对应的证书是依赖方信任的证书；

4）证书的用途适用于相应的签名；

5）使用证书上的公钥验证签名。

以上任何一个环节失败，依赖方应该拒绝接受签名信息。

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

### 4.6.1 证书更新的情形

为保证通用型证书、云证书、手机证书及其密钥对的安全有效和订户的权利，中环CA会为签发的通用型证书证书设置有效期。订户必须在证书有效期到期前90日内，到中环CA授权的发证机构申请证书更新。证书到期后将失效，用户无法使用证书。证书到期前90日内没有更新证书，订户如需继续使用，必须重新申请新证书。

证书更新的具体情形如下：

1）证书的有效期在中环CA规定的更新有效期内；

2）密钥对的使用期将要到期；

3）因加密密钥的丢失、损坏或泄漏导致原证书被撤销且还有证书使用需求；

4）其他。

以上情况主要体现为证书的补发和换发。

A.证书的补发：

补发是指在证书有效期内，订户出现证书载体丢失和证书载体损坏并进行更

新证书（密钥）的操作。补发操作成功时，旧证书将被撤销，新证书有效期从补发成功之日起到旧证书失效日止。

B.证书的换发：

每个证书都有其有效期，在认证机构规定的期限内，如果订户的注册信息没有改变，订户可以申请证书更新。换发操作成功时，旧证书将被撤销，新证书有效期将在原证书有效期的基础上增加一个有效周期（已经过期的证书换证，其有效期仅为证书有效期）。

事件证书仅用于业务场景的一次性的电子签名，不提供证书更新服务。

### 4.6.2 请求证书更新的实体

请求更新的实体为证书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，在中环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；或在中环CA授权的发证机构书面填写《中环CA数字证书申请表》。中环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）。中环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。

订户也可以选择一般的初始证书申请流程进行证书更新，按照本CPS3.2的要求提交相应的证书申请和身份证明资料。中环CA在任何情况下都可将这种初始证书申请的鉴别方式作为证书更新时的鉴别处理手段。

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，中环CA不承担任何责任。

### 4.6.4 颁发新证书时对订户的通告

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”。

新证书签发后，旧证书将被撤销。中环CA在目录服务器上发布新证书，用户旧证书通过CRL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 证书变更

### 4.7.1 证书变更的情形

证书变更指改变证书中除有效期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。

事件证书仅用于业务场景的一次性的电子签名，不提供证书变更服务。

### 4.7.2 请求证书变更的实体

请求证书变更实体为证书订户本人或其授权代表。

### 4.7.3 证书变更请求的处理

证书变更按照初次申请证书的注册过程进行处理。

### 4.7.4 颁发新证书时对订户的通告

同第4.6.4节“颁发新证书时对订户的通告”。

### 4.7.5 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”。

### 4.7.6 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”。

新证书签发后，旧证书将被撤销。中环CA在目录服务器上发布新证书，用户就证书通过CRL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 证书密钥更新

证书密钥更新是指不改变证书中包含的信息的情况下，产生新的密钥对，并由中环CA签发新证书。除必须更新密钥的情形外，中环CA不采取证书密钥更新。

### 4.8.1 证书密钥更新的情形

通用型证书订户申请更新密钥的情形主要有：

（1）证书的密钥泄露。对此，订户负有立即告知中环CA的责任；

（2）证书到期时，要求更新证书密钥；

（3）证书丢失，其他。

在云证书到期之前，订户可通过终端应用程序完成证书密钥更新。中环CA会按照之前注册的用户身份签发新的证书，同时必须产生新的密钥。证书到期后更新按照证书新办流程处理。

事件证书私钥在使用过一次后即销毁，不提供证书密钥更新服务。

手机证书的证书变更，按照证书新办流程处理。

### 4.8.2 请求证书密钥更新的实体

请求密钥更新的实体为证书订户本人或其授权代表。

### 4.8.3 证书密钥更新请求的处理

同第4.6.3节“证书更新请求的处理”。

### 4.8.4 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”。

### 4.8.5 构成接受密钥更新证书的行为

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密钥更新证书的发布

同第4.4.2节“电子认证服务机构对证书的发布”。

### 4.8.7 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 证书撤销和冻结

### 4.9.1 证书撤销的情形

当发现以下的情况，证书必须被撤销：

1) 私钥失窃、篡改、未经授权的泄露和其它安全威胁；

2) 证书主体(无论是CA还是订户）违反了CPS规定的重要职责；

3) CPS中职责的履行被延迟或受不可抗力的阻碍；自然灾害；计算机或通信失败；法律、规章或其它法律的改变；政府行为；或其它超过个人控制的原因并且对他人信息构成威胁的；

4) 订户主动提出撤销请求；

5) 中环CA发现订户在申请时提供的证明材料不真实；

6) 中环CA已经履行催缴义务后，订户仍未缴纳服务费。

事件证书仅用于业务场景的一次性的电子签名，证书私钥在使用过一次后即销毁，不提供证书撤销服务。

### 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）中环CA或其授权机构；

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

订户到中环CA授权的发证机构书面填写《中环CA数字证书申请表》，并注明撤销的原因。中环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。中环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，中环CA授权的发证机关管理员可以对订户证书进行强制撤销，撤销后立即通知该证书订户。强制撤销的命令来自于：中环CA、中环CA授权的发证机构或司法机关等公共权力部门。

事件证书没有证书撤销。

订户证书的撤销状态在24小时内通过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中环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

中环CA从收到证书撤销请求起一个工作日内完成请求的处理。

### 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）在使用证书前根据中环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，确保它是经中环CA发行并电子签名的。

依赖方应根据中环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

中环CA的CRL发布周期为24小时，特殊紧急情况下可以立即签发CRL。

### 4.9.8 CRL 发布的最大滞后时间

中环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

中环CA向证书订户提供7×24在线证书状态查询服务（OCSP）。

事件证书仅用于业务场景的一次性的电子签名，证书私钥在使用过一次后即销毁，不提供证书状态服务。

### 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

中环CA网站（https;//www.tjzhca.com）提供CRL文件下载。

### 4.9.12 密钥损害的特别要求

中环CA所有订户在发现证书密钥受到损害时，应立即通知中环CA撤销证书。

### 4.9.13 证书冻结的情形

证书冻结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，可以申请证书冻结。

事件证书仅用于业务场景的一次性的电子签名，不提供证书冻结服务。

### 4.9.14 请求证书冻结的实体

请求证书冻结的人包括：

1）订户本人或其授权代表；

2）中环CA或其授权机构；

3）司法机关等公共权力部门的授权代表。

### 4.9.15 冻结请求的流程

申请者到中环CA授权的发证机构书面填写《中环CA数字证书申请表》，并注明冻结的原因。中环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冻结申请进

行审核。如是强制冻结，中环CA授权的发证机关管理员可以依法对订户证书进行强制冻结，冻结后必须立即通知该证书订户。强制冻结的命令来源于：司法机关、中环CA或其授权机构。中环CA冻结订户证书后，发证机构将当面通知或通过发送Email邮件或邮寄等方式通知订户证书被冻结。

### 4.9.16 冻结的期限限制

订户证书被冻结后，订户必须在证书有效期到期前恢复证书，否则中环CA或中环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，中环CA不负责任。

### 4.9.17 电子认证服务机构处理冻结请求的时限

中环CA从收到证书冻结请求起一个工作日内完成请求的处理。

### 4.9.18 证书解冻

证书冻结订户或其授权者，在需要解冻时到中环CA授权的发证机构书面填写《中环CA数字证书申请表》，并注明解冻的原因。中环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解冻申请进行审核。审核通过之后，为订户解冻证书，并通知订户证书已解冻。

### 4.9.19 证书恢复

证书恢复是指加密密钥的恢复，订户加密密钥对由天津市密钥管理中心产生、保存，密钥恢复是一种严格受控的过程，只有在例如证书的密钥损坏或丢失，需要恢复密钥解除之前加密信息等情况下才允许进行证书恢复：

订户提出申请：当订户的加密密钥损坏或者丢失后，某些加密数据无法解密，订户可向中环CA提交申请，经过审核后，通过中环CA向天津市密钥管理中心发送请求，天津市密钥管理中心同意订户的恢复请求，中环CA恢复订户的密钥并下载于订户证书载体中。

## 4.10 证书状态服务

中环CA通过CRL、OCSP、LDAP提供证书状态服务。

### 4.10.1 操作特征

中环CA提供以下三种方式为证书订户提供证书状态查询。

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

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

3）提供LDAP目录查询证书状态服务，符合LDAP V3标准。

### 4.10.2 服务可用性

中环CA的CRL发布周期为24小时。

中环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

证书状态的其他可选服务方式为订户利用中环CA指定的CRL地址，通过目录服务器提供的查询系统，查询并下载CRL到本地，进行证书状态的查询。

## 4.11 订购结束

订购结束即服务终止，是指证书订户终止与中环CA的服务，它包含以下两种情况：

1.证书到期时终止与中环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，中环CA或其发证机构与订户的服务终止;

2.证书未到期时中止与中环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。

中环CA将根据证书订户的要求撤销证书，证书订户与中环CA的服务终止。

## 4.12 密钥生成、备份与恢复

### 4.12.1 密钥的生成与备份策略与行为

通用型证书的订户的加密密钥由天津市密钥管理中心（KMC）生成、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，由中环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。

订户签名密钥对由订户的密码设备生成，由订户自行保管。

云证书的密钥对，由签名服务云端经过国家密码局主管部门许可的服务器密码机产生。签名服务云端进行密钥备份与恢复。

事件证书的签名密钥对由签名设备生成密钥并执行签名后，即时销毁，签名密钥的私钥不进行保管。

手机证书的密钥对，由订户移动终端和签名服务云端协同计算产生。由订户移动终端和签名服务云端分别各自进行密钥备份与恢复。

### 4.12.2 密钥恢复的策略与行为

通用型证书订户加密密钥恢复：当订户的加密密钥损坏或丢失后，某些密文数据将无法还原，此时订户可向中环CA提交申请，经过审核后，通过中环CA向天津市密钥管理中心发送请求，天津市密钥管理中心同意订户的恢复请求，中环CA恢复订户的密钥并下载于订户证书载体中。

问责取证密钥恢复：问责取证人员向中环CA提交申请，经过审核后，通过中环CA向天津市密钥管理中心发送恢复请求，经天津市密钥管理中心同意后，由密钥恢复模块恢复所需的密钥并记录。

通用型证书订户签名密钥由订户保存，中环CA无法对签名密钥进行恢复。

云证书签名密钥对，由服务云端经过国家密码局主管部门许可的服务器密码机产生。服务云端进行密钥备份与恢复。

事件证书订户的签名密钥对由签名设备生成密钥并执行签名后，即时销毁，签名密钥不进行保管。

手机证书的密钥对，由订户移动终端和签名服务云端协同计算产生。由订户移动终端和签名服务云端分别各自进行密钥备份与恢复。

# 第五章 认证机构设施、管理和操作控制

## 5.1 物理控制

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

防止未授权访问中环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

中环CA电子认证服务业务的运行场地位于天津市河西区体院北环湖中道9号科研楼一楼。

根据GM/T 0034-2014《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》要求，机房分为以下各区域：

接待区（控制区，面积18㎡）：

接待区是CA机房的支持区域，为工作人员及访客提供防护措施及访客登记区域，采用访客控制措施，使用门禁控制出入。

管理区（限制区，面积20㎡）：

管理区是提供证书录入、审批、签发以及证书管理的电子认证服务区域，配备了RA管理终端、RA审计终端和安全管理终端，以及保险箱和文件柜，采用门禁控制出入。

服务区（敏感区，面积20㎡）：

该区域是电子认证RA、OCSP系统管理区域，主要用于放置RA系统、OCSP系统的软硬件设备，区域内安装有精密空调和柜式七氟丙烷气体灭火系统，门禁采用双人控制出入。

缓冲区（面积2.5㎡） ：

缓冲区是管理区进入核心区之前的中间地带，由两扇AB互锁屏蔽门组成。进入缓冲区需要一人指纹一人密码方可开启，进入后关闭A门才可以开启B门，同时要更换门禁验证方式，保证了核心区的安全。

核心区（屏蔽区，面积16㎡）：

核心区是CA系统、根私钥密码设备、数据库系统软硬件存放的区域。配备有CA管理终端、CA审计终端和保险柜，CA操作人员可在此区域执行操作。配备有精密空调、

新风系统和柜式七氟丙烷气体灭火系统。核心区还专门配备了氧气呼吸机防止突发情况的发生。

配电间（面积11㎡）

配电间装有外部市电双回路，由两路独立变电所提供，内部配备ATS自动电源切换系统，配置了两台深圳科士达UPS20千瓦时的UPS主机，可持续供电八小时的4组电池。保障计算机设备供电可靠性。

### 5.1.2 物理访问

中环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口令和指纹验证的结合方式控制，服务区采用身份鉴别卡和口令结合方式控制进出；

其他功能区域只采用身份鉴别卡或口令控制门的进出；

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

根据《电子计算机机房设计规范》（国标GB50174-2008）的有关规定，中心机房的温湿度控制执行C级标准，即温度为23℃±5℃，相对湿度为35%—75%，所采购的空调设备满足上述要求。

为保证系统设备的正常运转，避免服务器在过热的条件下工作，在屏蔽机房内安装了STULZ精密空调。

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。供配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。

使用不间断电源（UPS）来保证供电的稳定性和可靠性。采用双电源，在单路电源损坏时，可以自动切换，维持系统正常运转。

### 5.1.4 水患防治

中环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

中环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

中环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

中环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管理部审批通过后，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，其他废物处理按照中环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

中环CA对业务系统中的程序、数据等关键信息按照数据备份策略和流程进行安全备份。备份介质按照备份策略和流程保存在本地机房和异地。在异地备份时按照策略和流程由专人送交到银行保险柜保管。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

在中环CA提供的电子认证服务过程中，能从本质上影响证书的签发、使用、管理和撤销等涉及密钥操作的职位都被中环CA视为可信角色。这些角色包括但不限于：密钥管理员、系统管理员、网络安全管理员、审计员、业务管理人员及业务操作人员等，具体岗位名称和要求以中环CA的岗位说明书为准。

### 5.2.2 每项任务需要的人数

中环CA确保单个角色不能接触、导出、恢复、更新、废止中环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。至少三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密钥恢复的操作。

中环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

所有中环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、密码或者指纹识别；进入系统需要使用数字证书进行身份鉴别。中环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

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。中环CA人员职责分割的角色包括（但不限于）以下几种：

审计员；

网络安全管理员；

密钥管理员；

系统维护员；

物理环境管理员；

数据库管理员。

## 5.3 人员控制

### 5.3.1 资格、经历和无过失要求

中环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，核心和关键岗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。中环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。

中环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，可以参照中环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，但不得违背中环CA电子认证业务规则。

中环CA确立流程管理规则，所有的员工与中环CA签订保密协议，据此中环CA员工受到合同和章程的约束，不得泄露中环CA证书服务体系的敏感信息。

### 5.3.2 背景审查程序

中环CA制定了严格的员工背景审查程序，完成对中环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

中环CA对中环CA员工进行以下内容的综合性培训：

员工手册；

电子认证业务（CPS）；

岗位职责及说明书 ；

公司各项管理制度；

PKI基础知识；

中环CA应急预案管理；

国家关于电子认证服务的法律、法规及标准、程序；

其他需要进行的培训等。

### 5.3.4 再培训周期和要求

根据中环CA策略调整、系统更新等情况，中环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

当中环CA员工进行了未授权或越权操作，中环CA在确认后将立即中止该员工进入中环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，中环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

中环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，中环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

中环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。

中环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）运营环境和环境管理事件，包括：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员和安全存储设施的访问；

4）密钥和证书生命周期管理的日志和事件。

### 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，中环CA将每月进行一次内部检查、审计。

对系统安全事件和系统操作事件日志，中环CA将每月进行一次检查、处理。

对运营环境和环境管理事件日志，中环CA将每月进行一次检查、处理。

### 5.4.3 审计日志的保存期限

中环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，离线存档为五年。

### 5.4.4 审计日志的保护

中环CA执行严格的保护和管理，确保只有中环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

中环CA保证所有的审查记录和审查总结都按照中环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，系统日志随数据备份一并进行备份保存，每周备份一次，保存在机房保险柜中。每月进行异地备份保存。

### 5.4.6 审计收集系统

中环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）；

门禁管理系统；

视频监控系统；

网站、数据库安全保障系统；

其他中环CA认为有必要审查的系统。

### 5.4.7 对导致事件实体的通告

中环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，并且中环CA保留进一步追究责任的权利。

### 5.4.8 脆弱性评估

CA安全程序根据政策、技术和管理的变化及时进行薄弱环节分析，属于可以弥补的薄弱环节，及时弥补，属于不可弥补的薄弱环节，中环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

中环CA按照制度和流程定期对电子生成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

中环CA归档存档期限一般规定为五年。订户资料保存期限为订户证书失效后五年。

### 5.5.3 归档文件的保护

中环CA的归档文件存放在档案室和机房保险柜中，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。中环CA可以保护相关的档案免遭恶劣环境（如温度、湿度和磁力等的破坏）的威胁。

### 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，备份介质在中环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中环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。中环CA的所有硬件设备采用NTP服务器，保证各种操作的时间同步。

### 5.5.6 归档收集系统

中环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，中环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

在中环CA的密钥对遭受攻击或因为密钥生命期而需要更新根私钥的情况下，采用与根私钥初始化生成相同的流程和方法，由安全策略委员会授权，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私钥。新旧根证书过渡期，采用新私钥为旧公钥签名证书、旧私钥为新公钥签名证书、新私钥为新公钥签名的证书方式，确保用户和依赖方能够可靠地验证中环CA根证书以及证书信任链的有效性。

## 5.7 损害与灾难恢复

### 5.7.1 事故和损害处理程序

中环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：

根私钥泄露应急制度；

消防系统应急处理预案；

电力系统应急处理预案；

水灾应急处理预案；

通信系统应急处理预案；

网络系统瘫痪应急处理预案；

黑客攻击应急处理预案；

病毒应急处理预案；

系统数据应急处理预案；

人员应急处理预案。

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、软件或数据的损坏

中环CA对业务系统及其他重要系统的资源、软件或数据进行了备份，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，中环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，并立即通知中环CA或注册机构撤销其证书。中环CA按CPS第4.9节发布证书撤销信息；

2）当中环CA或注册机构发现证书订户的实体私钥受到损害时，中环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。中环CA按CPS第4.9节发布证书撤销信息；

3）当中环CA的证书出现私钥损害时，中环CA将立即撤销CA证书并及时通过途径通知依赖方，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，中环CA的灾难恢复时间目标RTO小于7天，恢复点目标RPO小于24小时。中环CA计划建立异地灾难恢复中心，灾难恢复中心的建立，将进一步增强中环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

当中环CA打算终止经营时，会在终止经营前三个月给中环CA授权的注册机构和订户书面通知，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。

中环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；

处理中环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。根据中环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中环CA，要完成相似的操作，唯一不同在发送中环CA终止通知的时间限制上：由于密钥受损原因终止中环CA，要求中环CA通知订户的过程尽快完成；由于非密钥受损的原因终止中环CA，在通知所有订户后，采取适当的步骤减轻中环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、中环CA证书签发系统申请的、天津市密钥管理中心的加密机设备生成的。

通用型证书签名密钥对是由国家密码主管部门许可的、中环CA数字证书签发系统支持的密码设备生成签名密钥对。签名密钥存储在密码设备中不可导出，保证中环CA无法复制签名密钥对。中环CA支持多种密码设备，如智能密码钥匙、智能IC卡、服务器密码机、签名验签服务器等。中环CA可根据证书申请者要求或自身选择签名密钥对生成的密码设备。

云证书签名密钥对，由服务云端经过国家密码局主管部门许可的服务器密码机产生。

事件证书的签名密钥由签名设备生成。

手机证书签名密钥对，由订户移动终端和签名服务云端共同计算协同产生。服务端密钥因子应在国家密码主管部门许可的服务器密码机中产生，客户端密钥因子应包含终端设备信息、用户知晓的（例如用户设置的 PIN）、随机数等部分计算得到。

### 6.1.2 加密私钥传送给订户

证书订户的加密私钥是在天津市密钥管理中心产生的，该私钥只保存在天津市密钥管理中心。在加密私钥从天津市密钥管理中心到订户的传递时，采用国家密码主管部门许可的对称密钥算法加密，中环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

中环CA从天津市密钥管理中心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主管部门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中环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。

电子认证服务机构公钥传送给依赖方中环CA的根公钥包含在中环CA自签发的根证书中。

证书订户可以从中环CA的网站（https://www.tjzhca.com）上下载中环CA根证书，也可以由中环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。

### 6.1.4 密钥的长度

为了保证加密/解密的安全性，中环CA所使用的加密和签名的非对称密钥对的模长是256比特，对称密钥的长度是128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，中环CA将会完全遵从。

### 6.1.5 公钥参数的生成和质量检查

公钥参数由国家密码主管部门许可、中环CA数字证书签发系统支持的硬件生成；质量检查由国家密码主管部门具体实施。

### 6.1.6 密钥使用用途

在中环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。

中环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

中环CA使用国家密码主管部门许可的产品，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（5 选 3）

中环CA采用多人控制策略激活、使用、备份、停止和恢复中环CA的根私钥，采取5个密钥分管者中至少3个在场才可进行操作的原则。

### 6.2.3 私钥托管

天津市密钥管理中心可以根据客户和法律的需要，对加密密钥进行托管。通用型证书签名私钥由订户自己保管，以保证其不可否认性。

云证书的签名密钥对，由服务器密码机生成，在服务云端经过密码机主密钥加密后保存。

事件证书无密钥托管。

手机证书的密钥对，由订户移动终端和签名服务云端协同计算产生并分别保管。

### 6.2.4 私钥备份

通用型证书的订户的签名密钥中环CA都不备份。加密私钥由天津市密钥管理中心备份，备份数据以密文形式存在。

中环CA根私钥的备份必须经安全策略委员会的批准，并填写《根私钥操作审批记录表》，将结果汇报给安全策略委员会。在生成密钥后，应立即做好根私钥的备份。备份过程中密钥分管者不得离场。根私钥应该备份到5张管理员卡上，5张备份卡分别由5名密钥分管者保存，备份的管理员卡的保存在核心机房的保险柜中。

云证书的证书私钥由服务云端备份，备份数据以密文形式存在。

手机证书由订户移动终端和签名服务云端各自备份各自的私钥因子。

### 6.2.5 私钥归档

天津市密钥管理中心提供过期的托管加密私钥的存档服务；保存期为五年。当加密私钥过了保存期，将依据相关规定对其进行销毁。

中环CA根私钥过期后，应在5个工作日内完成归档。根私钥的归档必须经安全策略委员会的批准，并填写《根私钥操作审批记录表》，将结果汇报给安全策略委员会。根私钥归档期限为5年在归档期内，根私钥不得重新投入生产环境使用。每年应检查归档的根私钥是否仍在归档期限内，归档期满5年后应立即启动销毁流程。

云证书的私钥通过数据库备份进行归档保存。

### 6.2.6 私钥导入、导出密码模块

私钥在硬件密码模块上生成或可以通过CA软件导入到密码模块中，私钥无法从密码模块中导出。

### 6.2.7 私钥在密码模块的存储

私钥以加密的形式存放在硬件密码设备中。

### 6.2.8 激活私钥的方法

中环CA将订户私钥保存在USBKEY或密码机等密码设备中，只有用户通过PIN码，私钥才能被激活使用。

中环CA根私钥存在核心区密码设备中，只有具有激活权限的3位以上密钥分管者使用管理员卡登陆，启动密钥管理程序，才能进行激活私钥的操作。

### 6.2.9 解除私钥激活状态的方法

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。

对于中环CA根私钥，只有具有激活权限的3位以上密钥分管者使用管理员卡登陆，启动密钥管理程序，才能进行解除私钥的操作。

### 6.2.10 销毁私钥的方法

对于中环CA签发的订户加密证书私钥，在其生命周期结束后，天津市密钥管理中心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。对于中环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。

对于中环CA根私钥，只有具有激活权限的3位以上密钥分管者使用管理员卡登陆，启动密钥管理程序，才能进行摧毁私钥的操作。

事件证书的订户私钥仅用于业务场景的一次性的电子签名，证书私钥在使用过一次后即销毁。

### 6.2.11 密码模块的评估

中环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

对于生命周期外的订户证书，中环CA将进行归档。归档的证书存放在归档数据库中。

云证书中的公钥，由服务云端归档。

### 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。中环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

存放有中环CA根私钥备份分量的密码机管理员卡，其产生按中环CA《根私钥生命周期管理制度》中的规定进行。所有密钥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。

中环CA根私钥由密码机产生，并分割保存在5个管理员卡中，需通过对应的密码机读取。

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。

### 6.4.2 激活数据的保护

保存有中环CA根私钥备份分量的密码机管理员卡，由中环CA5个不同的密钥分管者掌管，密钥分管者必须由安全策略委员会任命，需知悉密钥分管者相关职责。

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

### 6.4.3 激活数据的其他方面

1.激活数据的传送

存有中环CA根私钥备份分量的密码机管理员卡，通常保存在中环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，其传送过程需在中环CA安全管理人员的监督下进行。

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

2.激活数据的销毁

存有中环CA根私钥备份分量的密码机管理员卡，其销毁所采取的方法包括将管理员卡初始化，或者彻底销毁管理员卡，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中环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

中环CA的数字证书签发系统的数据文件和设备由中环CA系统维护员维护，未经中环CA安全部门授权，其它人员不能操作和控制中环CA系统；其它普通人员无系统账号和密码。中环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。中环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，中环CA系统维护员定期更改系统密码。

### 6.5.2 计算机安全评估

中环CA证书系统设计、建设实施严格遵守《GM/T0034-2014基于SM2密码算法的证书认证系统密码及其相关安全技术规范》的相关要求。

## 6.6 生命周期技术控制

### 6.6.1 系统开发控制

按照中环CA内部系统开发流程进行控制。

### 6.6.2 安全管理控制

中环CA的配置以及任何修改和升级都会记录在案并进行控制，并且中环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，只有中环CA授权的员工能够进入中环CA的系统或设备。

### 6.6.3 生命周期的安全控制

中环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

中环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。只有经过授权的中环CA员工才能够进入中环CA签发系

统、注册系统、目录服务器、证书发布系统等设备或系统。所有授权人员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

中环CA认证系统的各种系统日志、操作日志有对应的记录时间。中环CA的所有硬件设备采用NTP服务器，保证各种操作的时间同步。

# 第七章 证书、证书撤销列表和在线证书状态协议

## 7.1 证书

中环CA签发的证书均符合X.509 V3证书格式，遵循RFC 5280标准。

### 7.1.1 版本号

X.509 V3

### 7.1.2 证书标准项及扩展项

1. 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 = network trust CA，为通用名。
- C = CN，表示中国。
- 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）订户公开密钥信息域包含两个重要信息：订户的公开密钥的值；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。

2.证书扩展项：

中环CA证书扩展项除使用RFC 5280中定义的证书扩展项，还支持私有扩展项。

中环CA采用的IETF RFC 5280中定义的扩展项有：

- 颁发机构密钥标识符Authority Key Identifier
- 主题密钥标识符Subject Key Identifier
- 密钥用法Key Usage

- 扩展密钥用途Extended Key Usage
- 基本限制Basic Constraints
- CRL分发点CRL Distribution Points

私有扩展项可支持以下类型：

- 个人身份标识码
- 个人社会保险号
- 企业组织机构代码
- 企业工商注册号
- 企业税号

### 7.1.3 算法对象标识符

中环CA签发的证书按照RFC 5280标准，用SM2算法签名。

### 7.1.4 名称形式

中环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，并在中环CA的数据库中记录订户的相关信息。中环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、机构或设备）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

中环CA定期签发证书撤销列表（CRL），其所签发的CRL遵循RFC 3280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

CRL扩展项：颁发机构密钥标识符。

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

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版本：V1。

### 7.3.2 OCSP 扩展项

与RFC 2560一致。

# 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。

中环CA本身也需要对中环CA的关联机构（包含中环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，其频率可由中环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》的要求，按照上级主管部门的要求接受合规性审计。

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

对中环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

对中环CA进行审计的第三方，必须是一个独立于中环CA的合法审计实体。中环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；

电子认证业务规则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；

是否存在其它可能的安全风险；

中环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，包括中环CA的技术、手续、员工的相关管理制度和电子认证业务规则；

中环CA是否实施了相关技术、管理、相关制度和电子认证业务规则；

审计者或中环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，发生问题的职能部门对业务进行改进和完善，由安全策略委员会进行监督，完成对评估结果的改进后，各职能部门必须向安全策略委员会提交业务改进工作总结报告。

如果在外部评估过程中发现执行有不足之处，中环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，中环CA一般不公开审计结果。在必要的情况下，中环CA可依照与关联机构（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，向关联机构通知审计结果。

# 第九章 法律责任和其他业务条款

## 9.1 费用

证书相关费用在中环CA的网站上公布（https://www.tjzhca.com）。价目表按中环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。中环CA也可以通过其他方法通知订户或其他各方费用变化。

### 9.1.1 证书签发和更新费用

根据中环CA的价目确定。

### 9.1.2 证书查询费用

中环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。中环CA有可能根据需要OCSP服务作为增值服务收取费用。

### 9.1.4 其他服务费用

根据中环CA的价目确定。

### 9.1.5 退款策略

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

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

## 9.2 财务责任

中环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）中环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）中环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）由于中环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）中环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

中环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

中环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，则中环CA将按照发布的赔偿办法予以赔偿。

## 9.3 业务信息保密

中环CA对业务过程中所接收的属于私有信息的业务信息负有保密责任。中环CA有专门的保密管理制度，保护自身和订户的敏感信息及商业秘密。

### 9.3.1 保密信息范围

中环CA保密的信息包括（但不限于）：

1.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。

2.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。

3.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

中环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

中环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

中环CA制定有隐私保护制度并签订保密协议，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；订户与中环CA、注册机构签订的协议。

### 9.4.3 不被视为隐私的信息

不被认为是隐私的信息包括：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，中环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

中环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中环CA或其注册机构：

1）将手写签名的同意和授权文件邮寄、快递到中环CA或其注册机构；

2）将手写签名的同意和授权文件传真到中环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

当中环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，中环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

中环CA保留对本CPS的所有知识产权。中环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。

## 9.6 陈述与担保

### 9.6.1 电子认证服务机构的陈述与担保

除非中环CA做出特别约定，若本电子认证业务规则的规定与其他中环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。在中环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。

中环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；保证中环CA的签名私钥在中环CA内部得到安全的存放和保护；中环CA建立和执行的安全机制符合国家政策的规定。中环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、洪灾或其他大灾难等。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，中环CA的服务机构、中环CA授权的发证机构、中环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中环CA必须承担其它的义务或中环CA必须对其行为做出其它的承诺。

第二：在上述内容中所罗列不可抗力的任何情况下，中环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，中环CA会要求订户及时更换证书以保证中环CA能更好地履行本节所述的责任。

### 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。这些程序和保障由中环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，以后中环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9.6.1节。

### 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写的所有声明和信息必须是完整、精确、真实和正确的，可供中环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或者由中环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，订户应立刻通知中环CA或中环CA授权的发证机构，申请采取冻结、撤销等处理措施。

### 9.6.4 依赖方的陈述与担保

依赖方确认，在任何信赖行为发生之前，阅读了依赖方协议，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，应当免除中环CA的责任：

1）订户在申请和使用中环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；
- 订户应当妥善保管中环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，应当及时告知中环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，不得将数字证书在中环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、被冻结、被撤销的数字证书；订户应当根据规定按时向中环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、洪灾、火山爆发、滑坡、泥石流、雪崩、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）中环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

中环CA根据与订户签订的合同承担相应的有限责任，且责任仅限于涉及由中环CA颁发的数字证书方面，但对于因订户或依赖方的原因造成的损害中环CA不承担任何责任。

中环CA承诺在现有的电子认证服务业务下，中环CA签发的数字证书不会被伪造、篡改；如果由于中环CA的私钥管理问题造成数字证书被伪造、篡改，中环CA将承担相应有限责任。

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。

对于由如下原因造成的订户或依赖方损失，中环 CA 对订户或依赖方进行赔偿：

1. 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. 由于中环 CA 的原因，使得证书中出现了错误信息；

3. 因中环 CA 的原因，导致订户无法正常验证证书状态，使订户或依赖方利益受损。中环 CA 对于每份证书产生的所有数字签名和交易处理，对所有当事实体（包括但不限于用户、申请人或信赖方）有关该特定证书的合计责任应不超过赔付责任上限，这种赔付上限可以由中环 CA 视情况重新制定，中环 CA 会将重新制定后的情况立刻通知相关当事人。

中环 CA 所颁发数字证书的赔付责任上限如下：

A. 个人证书 500 元；

B. 机构证书 500 元；

C. 设备证书 2000 元。

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，每份证书的责任均有封顶而不考虑数字签名和交易处理等有关的其他索赔的数量。当超过责任封顶时，可用的责任封顶将首先分配给最早得到索赔解决的一方，中环CA没有责任为每个证书支付高出责任封顶的赔付，而不管责任封顶的总量在索赔提出者之间如何分配。

## 9.9 赔偿

1）对于由如下原因造成的订户或依赖方损失，中环CA对订户或依赖方进行赔偿：

（1）中环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）由于中环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中环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措施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Email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中环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）依赖方没有检查证书状态确定证书是否过期或撤销。

4）中环CA承担赔偿责任（法定或约定免责除外）的赔偿限制如下：

（1）中环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赔偿上限可以由中环CA根据情况重新制定，中环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，中环CA不承担责任，由订户或依赖方自行承担；

（3）中环CA只有在其证书有效期限内承担损失赔偿。

## 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生效时或中环CA终止业务时，旧版本CPS自动终止；当中环CA中止业务时，中环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

中环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，通知订户、依赖方。

## 9.12 修订

中环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。

中环CA有权在中环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，中环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，由安全管理部门讨论，提出修订报告，经中环CA安全策略委员会批准后，由安全管理部门负责组织修订，修订后的CPS经过中环CA安全策略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经批准后将立即在中环CA网站更新通告栏发布。对于需要通过电子邮件、信件、媒体等方式通知的修改，中环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。

中环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

由中环CA安全管理部门根据公司业务情况提出，中环CA安全策略委员会审批。

## 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。中环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中环CA信任域参与者间的完整协议。

### 9.16.2 转让

中环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，在中环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 强制执行力

在中环CA、注册机构、订户和依赖方之间出现法律诉讼时，胜诉方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，如战争和地震、洪灾、火山爆发等自然灾害等，造成中环CA、注册机构无法提供正常的服务时，中环CA、注册机构不承担由此给客户造成的损失。

## 9.17 其他条款

中环CA对本CPS具有最终解释权。