

天津市中环认证服务有限公司

手机证书策略

V1.0

天津市中环认证服务有限公司

2020 年 11 月

手机证书策略

天津市中环认证服务有限公司版权声明

天津市中环认证服务有限公司所颁布的《天津市中环认证服务有限公司手机证书策略》受到完全的版权保护。本文件中所涉及的“中环CA手机证书策略”由天津市中环认证服务有限公司独立享有版权。

未经天津市中环认证服务有限公司的书面同意，本文件的任何部分不得以任何方式、任何途径（电子的、机械的、影印、录制等）进行复制、存储、调入网络系统检索或传播。

在满足下述条件下，本文件可以被书面授权以在非独占性的、免收版权许可使用费的基础上进行复制及传播：前文的版权说明和上段主要内容应标于每个副本开始的显著位置。副本应按照天津市中环认证服务有限公司提供的文件准确、完整地复制。

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：022-23522103/400-0655-110，传真：022-23522103。

版本信息

当前版本号	最近更新日期
V1.0	2020.11.22

修订时间	修订说明	修订版本	修订人	审核人
2020.11.22	创建本 CP	V1.0	李维	安全策略 委员会

目 录

第一章 概括性描述	10
1.1 概述	10
1.1.1 公司简介	10
1.1.2 电子认证证书策略	10
1.2 文档名称与标识	11
1.2.1 名称	11
1.2.2 标识	11
1.2.3 版本	11
1.2.4 发布	11
1.3 电子认证活动参与者	11
1.3.1 电子认证服务机构	11
1.3.2 注册机构 (Registration Authority)	11
1.3.3 注册分支机构 (Registration Authority Branch)	12
1.3.4 受理点 (Business Terminal)	12
1.3.5 证书垫付商 (sponsor)	12
1.3.6 订户 (Certificates Applicant)	13
1.3.7 依赖方 (Relying Party)	13
1.3.8 其他参与者 (Other Participants)	13
1.4 证书应用	13
1.4.1 适合的证书应用	13
1.4.2 限制的证书应用	13
1.5 策略管理	13
1.5.1 策略文档管理机构	13
1.5.2 联系人	14
1.5.3 决定 CP 符合策略的机构	14
1.5.4 CP 批准程序	14
1.5.5 CP 修订	14
1.6 定义与缩写	14
第二章 信息发布与信息管理	16
2.1 中环 CA 信息库	16
2.2 认证信息的发布	16
2.3 发布的时间和频率	17
2.4 信息库访问控制	17

2.4.1 信息的发布与处理	17
2.4.2 信息访问控制和安全审计	17
第三章 身份标识与鉴别	18
3.1 命名	18
3.1.1 名称类型	18
3.1.2 对名称意义化的要求	18
3.1.3 订户的匿名或假名	18
3.1.4 理解不同名称形式的规则	18
3.1.5 名称的唯一性	19
3.1.6 商标的识别、鉴别和角色	19
3.2 初始身份确认	19
3.2.1 证明拥有私钥的方法	19
3.2.2 组织机构身份的鉴别	19
3.2.3 个人身份的鉴别	20
3.2.4 没有验证的订户信息	20
3.2.5 授权确认	20
3.2.6 互操作准则	20
3.3 密钥更新请求的标识与鉴别	20
3.3.1 常规密钥更新的标识与鉴别	21
3.3.2 撤销后密钥更新的标识与鉴别	21
3.4 撤销请求的标识与鉴别	21
第四章 证书生命周期操作要求	22
4.1 证书申请	22
4.1.1 证书申请实体	22
4.1.2 申请过程与责任	22
4.2 证书申请处理	22
4.2.1 执行识别与鉴别功能	22
4.2.2 证书申请批准和拒绝	23
4.2.3 处理证书申请的时间	23
4.3 证书签发	23
4.3.1 证书签发中注册机构和电子认证服务机构的行为	23
4.3.2 订户证书签发的通知	23
4.4 证书接受	24
4.4.1 构成接受证书的行为	24

4.4.2 电子认证服务机构对证书的发布	24
4.4.3 电子认证服务机构对其他实体的通告	24
4.5 密钥对和证书的使用	24
4.5.1 订户私钥和证书的使用	24
4.5.2 依赖方公钥和证书的使用	24
4.6 证书更新	25
4.7 证书密钥更新	25
4.7.1 证书密钥更新的情形	25
4.7.2 请求证书更新的实体	25
4.7.3 证书更新请求的处理	25
4.7.4 颁发新证书时对订户的通告	25
4.7.5 构成接受更新证书的行为	25
4.7.6 电子认证服务机构对更新证书的发布	26
4.7.7 电子认证服务机构对其他实体的通告	26
4.8 证书变更	26
4.8.1 证书变更的情形	26
4.8.2 请求证书密钥更新的实体	26
4.8.3 证书密钥更新请求的处理	26
4.8.4 订户新证书签发的通知	26
4.8.5 构成接受密钥更新证书的行为	26
4.8.6 电子认证服务机构对密钥更新证书的发布	26
4.8.7 电子认证服务机构对其他实体的通告	26
4.9 证书撤销和冻结	26
4.9.1 证书撤销的情形	26
4.9.2 请求证书撤销的实体	27
4.9.3 撤销请求的流程	27
4.9.4 撤销请求宽限期	27
4.9.5 电子认证服务机构处理撤销请求的时限	27
4.9.6 依赖方检查证书撤销的要求	27
4.10 证书状态服务	28
4.10.1 操作特征	28
4.10.2 服务可用性	28
4.10.3 可选特征	28
4.11 订购结束	28

4.12 密钥生成、备份与恢复	28
4.12.1 密钥备份与恢复的策略与行为	28
4.12.2 会话密钥的封装与恢复的策略与行为	29
第五章 认证机构设施、管理和操作控制	30
第六章 认证系统技术安全控制	31
6.1 密钥对的生成和安装	31
6.1.1 密钥对的生成	31
6.1.2 加密私钥传送给订户	31
6.1.3 公钥传送给证书签发机构	31
6.1.4 电子认证服务机构公钥传送给依赖方	31
6.1.5 密钥的长度	31
6.1.6 公钥参数的生成和质量检查	31
6.1.7 密钥使用用途	31
6.1.8 密钥使用目的	32
6.2 私钥保护和密码模块工程控制	32
6.2.1 密码模块的标准和控制	32
6.2.2 私钥多人控制（5选3）	32
6.2.3 私钥托管	32
6.2.4 私钥备份	32
6.2.5 私钥归档	32
6.2.6 私钥导入、导出密码模块	32
6.2.7 私钥在密码模块的存储	32
6.2.8 激活私钥的方法	32
6.2.9 解除私钥激活状态的方法	33
6.2.10 销毁私钥的方法	33
6.2.11 密码模块的评估	33
6.3 密钥对管理的其他方面	33
6.3.1 公钥归档	33
6.3.2 证书操作期和密钥对使用期限	33
6.4 激活数据	33
6.4.1 激活数据的产生和安装	33
6.4.2 激活数据的保护	33
6.4.3 激活数据的其他方面	34
6.5 计算机安全控制	34

6.5.1 特别的计算机安全技术要求	34
6.5.2 计算机安全评估	34
6.6 生命周期技术控制	34
6.6.1 系统开发控制	34
6.6.2 安全管理控制	35
6.6.3 生命周期的安全控制	35
6.7 网络的安全控制	35
6.8 时间戳	35
第七章 证书、证书撤销列表和在线证书状态协议	35
7.1 证书	35
7.1.1 版本号	35
7.1.2 证书标准项及扩展项	36
7.1.3 算法对象标识符	37
7.1.4 名称形式	37
7.1.5 名称限制	37
7.1.6 证书策略对象标识符	37
7.1.7 策略限制扩展项的用法	37
7.1.8 策略限定符的语法和语义	37
7.1.9 关键证书策略扩展项的处理规则	37
7.2 证书撤销列表	37
7.2.1 版本号	37
7.2.2 CRL 和 CRL 条目扩展项	37
7.3 在线证书状态协议	37
7.3.1 版本号	38
7.3.2 OCSP 扩展项	38
第八章 认证机构审计和其他评估	39
8.1 评估的频率或情形	39
8.2 评估者的资质	39
8.3 评估者与被评估者之间的关系	39
8.4 评估内容	39
8.5 对问题与不足采取的措施	40
8.6 评估结果的传达与发布	40
第九章 法律责任和其他业务条款	41

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《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8月开始建设天津市中环认证服务有限公司（以下简称“中环CA”），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。

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，在2018年5月通过了国家密码管理局组织的天津市中环认证服务有限公司电子认证服务系统技术测试、技术文档鉴定和安全性审查，并于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》。

1.1.2 电子认证证书策略

中环CA电子认证服务系统是由天津市中环认证服务有限公司建设、运营的一个公开密钥基础设施，提供基于数字证书的电子认证服务。中环CA是依照《电子认证服务密码管理办法》和《电子认证服务管理办法》设立的第三方电子认证服务机构，致力于构建和谐的网络信任环境，向互联网订户提供安全、可靠、可信的电子认证服务。

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。

证书策略（Certification Policy，以下简称 CP）是关于电子认证服务机构制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。

《天津市中环认证服务有限公司手机证书策略》（以下简称《手机证书策略》）满足互联网标准组织制定的 RFC3647《互联网X.509公钥基础设施-证书策略和证书业务声明框架》，以及国内标准GB/T 26855-2011《信息安全技术公钥基础设施证书策略与认证业务声明框架》的框架和内容要求。本《事件证书策略》适用范围为数字认证公司发

放的事件证书。具体设定了证书策略、生命周期、使用、依赖和管理的角色、责任与要求，以及各相关主体的职责。为批准、签发、管理和使用证书和相关的可信服务制定业务，提供技术、策略和法律上的要求和规范。

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手机证书策略》（简称《中环CA手机证书策略》）。

1.2.2 标识

本CP没有向相关管理机构注册对象标识符（OID）。

1.2.3 版本

本策略为中环CA发布的第一个版本，即《天津市中环认证服务有限公司手机证书策略》V1.0。

1.2.4 发布

本CP的发布在中环CA网站发布，网站地址：<https://www.tjzhca.com>

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式（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订户，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

本CA机构签发的手机证书适合应用在移动互联网、云服务和传统业务等各领域，用于证明订户在移动化和云服务环境中所进行的身份认证与电子签名。

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CP，并作为CP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、更新本电子认证服务系统证书策略。中环CA安全策略委员会由来自于公司管理层、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组成。

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将对本证书策略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115室（300060）

电子邮件：tjzhca@126.com

网站地址：<https://www.tjzhca.com>

1.5.3 决定 CP 符合策略的机构

中环CA安全策略委员会作为最高策略管理机构，负责决定本CP的符合性和可用性。

1.5.4 CP 批准程序

按照信息产业部公布的《电子认证业务规则规范》的要求，在本电子认证服务系统证书策略做出任何变动之前，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。

1.5.5 CP 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电子认证服务系统证书策略，CP编写小组根据相关的情况拟定CP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。

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

电子认证服务机构（CA）

电子认证服务机构（Certification Authority，简称CA）是受订户信任的，负责签发数字证书的权威机构，又称为数字证书认证中心。作为电子交易中受信任的第三方，负责为电子认证业务中各个实体颁发数字证书，以证明各实体身份的真实性，并负责在交易中检验和管理证书。

注册机构 (RA)

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

数字证书 (Digital Certificate)

数字证书是指经CA数字签名的包含数字证书使用者身份公开信息和公开密钥的电子文件。数字证书提供了一种在Internet上验证身份的方式, 其作用类似于日常生活中的身份证。

证书撤销列表 (CRL)

证书撤销列表 (Certificate Revocation List, 简称CRL), 是一种包含撤销的证书列表的签名数据结构。CRL是证书撤销状态的公布形式, 就像信用卡的黑名单, 它通知其他证书订户某些电子证书不再有效。

在线证书状态协议 (OCSP)

在线证书状态协议是用于检查数字证书在某一交易时间是否有效的标准。

证书策略 (CP, Certificate Policy)

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.509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

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撤销证书列表; 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工作人员才能登陆、访问和控制。

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，对证书申请人的身份和其他属性进行鉴别，并以不同的标识记录其信息。证书持有者的标识命名，以甄别名（Distinguished Name）形式包含在证书主体内，是证书持有者的唯一识别名。

中环CA的证书符合X.509标准，分配给证书持有者实体的甄别名，采用X.509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

手机证书的甄别名(DN)通常包含业务场景的相关数据信息。

3.1.3 订户的匿名或假名

订户在CA证书服务体系中不能使用假名或匿名，并在中环CA的数据库中记录订户的相关信息。

3.1.4 理解不同名称形式的规则

中环CA签发的数字证书符合X.509标准，甄别名格式遵守X.509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

通过证书请求中所包含的数字签名来证明证书申请人持有与注册公钥对应的私钥。

在手机证书服务体系中，私钥在订户移动终端和签名服务云端共同计算生成，证书请求信息中包含用私钥进行的数字签名，CA用订户移动终端和签名服务云端共同计算生成的公钥来验证这个签名，视作申请人为其私钥的拥有者。

3.2.2 组织机构身份的鉴别

对于组织身份的鉴别，CA机构或授权的注册机构需要验证组织的合法证件。证书申请人需持营业执照等证件，以及组织给经办人的授权和经办人身份证件，向CA机构提出申请。CA机构或授权的注册机构按照CA审核流程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。

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。CA机构或授权的注册机构可通过权威第三方数据库查询系统来进行身份鉴别审核。

CA机构或授权的注册机构依法采集并妥善保存订户身份信息，包括订户的电子影像数据或证明订户有效身份的其他电子数据等。

3.2.3 个人身份的鉴别

个人订户在申领证书前应持个人有效身份证件，包括：身份证、港澳台居民身份证、户口簿、护照、军官证等。提出证书申请，并接受证书申请的有关条款，承担相应的责任。CA 机构或授权的注册机构将复核并验证申请文件的真实性，并进行批准申请或拒绝申请的操作。

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。CA 机构或授权的注册机构可通过公安部身份核实接口或银行用户查询系统来进行身份鉴别审核。

CA机构或授权的注册机构依法采集并妥善保存订户身份信息，包括订户的电子影像数据或证明订户有效身份的其他电子数据等。

3.2.4 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。

3.2.5 授权确认

当申请人代表个人或组织机构申请证书时，需要出示足够的证明信息以证明个人或组织机构是否真实存在，申请人是否已获得个人或组织机构的授权。CA机构或授权的注册机构有责任确认该授权信息，并将授权信息妥善保存。

3.2.6 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的证书策略的要求，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

3.3.1 常规密钥更新的标识与鉴别

手机证书常规密钥更新中，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，中环CA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。

此过程订户可以通过移动终端自助完成。

3.3.2 撤销后密钥更新的标识与鉴别

手机证书撤销后的密钥更新等同于订户重新申请证书，其要求与3.2相同。

3.3.3 证书变更的标识与鉴别

手机证书的证书变更是指订户的证书信息发生变更，申请重新签发一张证书，对原证书进行撤销处理。

证书变更的标示与鉴别使用原始身份验证相同的流程，其要求与 3.2 相同。

3.4 撤销请求的标识与鉴别

手机证书撤销请求的标示与鉴别使用原始身份验证相同的流程，其要求与3.2相同。

如果是因为订户没有履行本《中环CA手机证书策略》和《中环CA电子认证业务规则》所规定的义务，由CA机构或授权的注册机构申请撤销订户的证书时，不需要对订户身份进行标识和鉴别。

第四章 证书生命周期操作要求

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、事业单位、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

订户按照《中环CA云证书策略》和《中环CA电子认证业务规则》规定的要求，将申请人身份证明材料递交给中环CA或其授权的注册机构，中环CA或授权的注册机构将对用户提交的身份证明材料进行身份鉴别，并决定是否受理申请。

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。

中环CA或授权的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审核工作，通过鉴证后，CA机构向订户签发证书。如果用户身份信息的鉴别由授权的注册机构完成，CA机构应对授权的注册机构进行监督管理和审计。

根据《中华人民共和国电子签名法》的规定，订户未向CA机构提供真实、完整和准确的信息，或者有其他过错，给CA机构或依赖方造成损失的，应承担相应的法律责任和经济赔偿。

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CP3.2.2、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或授权的注册机构有权决定接受或拒绝订户的申請。

- 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或授权的注册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;

- 1) 订户不能提供所需要的补充文件;
- 2) 订户不接受或者反对订户协议的内容和要求;
- 3) 没有或者不能够按照规定支付相应的费用;
- 4) 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或授权的注册机构将尽快确认证书申请信息, 一旦中环CA或授权的注册机构收到了所有必须的相关信息, 将在24小时内处理证书申请。

中环CA或授权的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中环CA或授权的注册机构的管理要求。

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

中环CA在批准证书申请之后, 将签发证书。证书的签发意味着电子认证服务机构最终完全正式地批准了证书申请。

4.3.2 订户证书签发的通知

中环CA签发手机证书, 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

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

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。

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。

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

订户在提交了证书申请并接受了中环CA所签发的证书后，均视为已经同意遵守与中环CA、依赖方有关的权利和义务的条款。

手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) 证书是否由可信任的CA所签发；
- 2) 证书被适当的使用，判断该证书没有被用于电子认证业务规则或者法律法规禁止或限制的使用范围；
- 3) 证书的使用与证书密钥用途包含内容是否一致；
- 4) 查询证书及其证书信任链中的证书状态，如果订户证书或其信任链内的任何证书已经被撤销，依赖方必须独立去了解该订户证书对应的私钥所做的签名是否是在撤销之前做的，是否可以依赖，并独立承担相应的风险。

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

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

4.6 证书更新

证书更新指在不改变证书中订户的公钥或其他任何信息的情况下，为订户签发一张新证书。

手机证书更新，必须同时进行密钥更新。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

证书密钥更新是指订户生成新密钥并申请为新公钥签发新证书，中环CA提供证书更新时，密钥必须同时更新。

在手机证书到期之前，订户可通过移动终端自助完成证书密钥更新。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。

4.7.2 请求证书更新的实体

订户可以请求证书密钥更新。订户包括持有中环CA签发的手机证书的证书持有人。

4.7.3 证书更新请求的处理

同3.3密钥更新请求的标识与鉴别。

4.7.4 颁发新证书时对订户的通告

同4.3.2电子认证服务机构对证书的发布。

4.7.5 构成接受更新证书的行为

同4.4.1构成接受证书的行为。

4.7.6 电子认证服务机构对更新证书的发布

同4.4.2电子认证服务机构对证书的发布。

4.7.7 电子认证服务机构对其他实体的通告

同第4.4.3节“电子认证服务机构对其他实体的通告”。

4.8 证书变更

4.8.1 证书变更的情形

证书变更是指订户的证书信息发生变更，申请重新签发一张证书，对原证书进行撤销处理。

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。

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或其授权机构的授权代表；
- 3) 司法机关等公共权力部门的授权代表。

4.9.3 撤销请求的流程

订户到中环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。

订户证书在24小时内进入CRL或被直接签发CRL，向外界公布。

4.9.4 撤销请求宽限期

当最终订户发现出现第4.9.1章节中的情况时，应该尽快提出证书撤销请求，撤销请求必须在密钥泄密或有泄密嫌疑8小时以内发现提出，其它撤销原因从发现需要撤销证书到向中环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24小时内完成请求的处理。

4.9.6 依赖方检查证书撤销的要求

依赖方在信任证书前，必须对证书的状态进行检查，包括：

- 1) 在使用证书前根据中环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。

4.10 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。除上述方式外, 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。

4.10.2 服务可用性

中环CA的CRL发布周期不超过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

订购结束是指当证书有效期满或证书撤销后, 该证书的服务时间结束。订购结束包含以下两种情况:

1) 证书有效期满, 订户不再延长证书使用期或者不再重新申请证书时, 订户可以终止订购;

2) 在证书有效期内, 证书被撤销后, 即订购结束。

4.12 密钥生成、备份与恢复

4.12.1 密钥备份与恢复的策略与行为

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 会话密钥的封装与恢复的策略与行为

非对称算法组织数字信封的方式来封装会话密钥。数字信封使用信息接受者的公钥对会话密钥加密, 接受者用自己的私钥解开并恢复会话密钥。

第五章 认证机构设施、管理和操作控制

本章规定参见CPS。

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

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码）、随机数等部分计算得到。

6.1.2 加密私钥传送给订户

手机证书的签名密钥对，由订户移动终端和签名服务云端共同计算协同产生，通过安全通道协商传输。

6.1.3 公钥传送给证书签发机构

手机证书公钥通过安全通道，经RA传递到CA。

从RA到CA以及从密钥管理中心到CA的传递过程中，采用国家密码主管部门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

依赖方可以从数字认证公司的网站<https://www.tjzhca.com>下载根证书和CA证书，从而得到CA的公钥。

6.1.5 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。

6.1.6 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、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管理局具体实施。

6.1.7 密钥使用用途

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。

6.1.8 密钥使用目的

订户的签名密钥可以用于提供安全服务，实现身份认证、不可抵赖性和信息的完整性等，用于签署具备法律效力的电子文档和电子交易数据。

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的签名密钥，采取5个管理人员中至少3个在场才可进行操作的原则。

6.2.3 私钥托管

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

订户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

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

通过CA软件把私钥安全导入到密码模块中，服务云端私钥无法从硬件密码模块中导出。

6.2.7 私钥在密码模块的存储

签名服务云端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的身份的加密IC卡登录，启动密钥管理程序，进行激活私钥的操作，需要半数以上的管理员同时在场。

6.2.9 解除私钥激活状态的方法

具有解除私钥激活状态权限的管理员使用含有自己的身份的加密 IC卡登录，启动密钥管理程序，进行解除私钥的操作，需要半数以上的管理员同时在场。

6.2.10 销毁私钥的方法

订户签名私钥，在其生命周期结束后，无需再保存，可以通过私钥的删除、系统或密码模块的初始化来销毁。

6.2.11 密码模块的评估

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

订户证书中的公钥，由签名服务端归档。

6.3.2 证书操作期和密钥对使用期限

所有订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

存放有中环CA根密钥备份分量的密码机管理员卡，其产生按中环CA密钥生成规程参考指南中的规定进行。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根密钥由密码机产生，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根密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根密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根密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根密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 and 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。

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

- 微缩图算法。
- 证书内容的签名算法。
- 微缩图证书内容的签名值。

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服务系统证书策略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，每年一次接受上级主管部门的合规性审计。

根据审计结果，需要整改后复审的，应接受复审。

8.2 评估者的资质

对中环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；

是否严格按照本电子认证服务系统证书策略、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服务系统证书策略表达一致，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

本章规定参见 CPS。