天威诚信电子签名认证证书

证书策略和认证业务规则

1.0 版本

生效日期:2026 年 10 月 31 日

北京天威诚信电子商务服务有限公司

中华人民共和国北京市海淀区上地八街 7 号院 4 号楼 401

邮政编码：100085

电话：(8610)-50947500

网址：www.itrus.com.cn

版本说明：

版本控制表

名称及版本	主要修改说明	发布和生效时间	审批人
电子签名认证证书证书策略和认证业务规则 1.0	编写	2026 年 10 月 31 日	天威诚信安全策略委员会

商标声明

CTN（China Trust Network，中国信任网络）由天威诚信注册拥有，是天威诚信的服务标识。文档中的其他商标、服务标识是相应拥有者的财产。

对版权的保留不限于以上声明，除了下文中明确许可的外，未经天威诚信公司的书面同意，本文件的任何部分不得复制、存储或引入到查询系统，或以任何方式、任何途径（电子的、机械的、影印、录制等）传播。

然而，在满足下述条件下，本文件可以在非排他性的、免收版权使用许可费的基础上被授权进行复制及传播：I．前面的版权说明和上段主要文字内容标于每个复制副本开始的显著位置；II．复制副本应按照天威诚信提供的文件准确、完整地复制。

对任何复制本文件的其他请求，请联系北京天威诚信电子商务服务有限公司。

地址：中华人民共和国北京市海淀区上地八街 7 号院 4 号楼 401，CPS 编制组。

电话：(8610)-50947500。

电子邮件：itrus_cps@itrus.com.cn。

目　　录

1. 概括性描述 1
1.1 承诺 1
1.2 基本信息 1
1.3 文档名称与标识 2
1.4 电子认证活动参与者 3
1.4.1 电子认证服务机构（CA） 3
1.4.2 注册机构（RA） 3
1.4.3 订户 3
1.4.4 电子签名依赖方 4
1.5 证书应用 4
1.5.1 证书应用分类 4
1.5.2 受限的应用 5
1.5.3 受禁的使用 5
1.6 策略管理 6
1.6.1 策略文档管理机构 6
1.6.2 策略文档批准程序 7
1.7 定义和缩写 7
1.7.1 定义 7
1.7.2 缩写 8
2. 信息发布与信息管理 10
2.1 信息库 10
2.2 认证信息的发布 10
2.3 发布的时间或频率 10
2.4 信息库访问控制 11
3. 身份标识与查验 12
3.1 身份查验通用要求 12
3.1.1 通用要求 12
3.1.2 订户告知 12
3.2 初始身份确认 14
3.2.1 证明拥有私钥的方法 14
3.2.2 个人身份的查验 14
3.2.3 组织机构身份的查验 16
3.3 订户意愿记录 17
3.3.1 订户意愿记录内容 17
3.3.2 个人高等级证书的意愿记录 17
3.3.3 个人基础级证书的意愿记录 17
3.3.4 机构高等级证书的意愿记录 18
3.3.5 机构基础级证书的意愿记录 18
3.4 订户协议 18

3.5 未验证的订户信息 18
3.6 互操作准则 19
3.7 命名与主体标识 19
3.7.1 命名规范 19
3.7.2 DN 项结构规则 19
3.7.3 扩展与约束 20
4. 证书生存周期操作要求 21
4.1 通用要求 21
4.2 证书申请 21
4.2.1 证书申请主体 21
4.2.2 注册过程与责任 21
4.2.3 证书申请处理 22
4.3 证书签发 22
4.3.1 签发过程 22
4.3.2 结果通知 23
4.4 证书接受 23
4.4.1 证书的交付 23
4.4.2 证书的接受 24
4.4.3 证书接受记录的保存 25
4.4.4 CA 对证书的发布 26
4.4.5 CA 对其他实体的通告 26
4.5 密钥对和证书使用 26
4.5.1 密钥对和证书管理 26
4.5.2 订户私钥和证书使用 27
4.5.3 依赖方公钥和证书使用 27
4.6 证书续期 27
4.6.1 证书续期的情形 27
4.6.2 请求证书续期的实体 28
4.6.3 证书续期请求的处理 28
4.6.4 签发续期证书时对订户的通知 29
4.6.5 构成接受续期证书的行为 29
4.6.6 CA 对续期证书的发布 29
4.6.7 CA 对其他实体的通告 30
4.7 证书密钥更新 30
4.7.1 证书密钥更新的情形 30
4.7.2 请求证书密钥更新的实体 30
4.7.3 证书密钥更新请求的处理 30
4.7.4 签发新证书时对订户的通知 31
4.7.5 构成接受密钥更新证书的行为 31
4.7.6 CA 对密钥更新证书的发布 31
4.7.7 CA 对其他实体的通告 31

4.8 证书变更 31
4.8.1 证书变更的情形 31
4.8.2 请求证书变更的实体 32
4.8.3 证书变更请求的处理 32
4.8.4 签发新证书时对订户的通告 32
4.8.5 构成接受变更证书的行为 32
4.8.6 CA 对变更证书的发布 32
4.8.7 CA 对其他实体的通告 32
4.9 证书撤销和冻结 32
4.9.1 证书撤销的情形 32
4.9.2 请求证书撤销的实体 33
4.9.3 撤销请求的流程 33
4.9.4 撤销请求宽限期 34
4.9.5 CA 处理撤销请求的时限 34
4.9.6 依赖方检查证书撤销的要求 34
4.9.7 CRL 发布频率 34
4.9.8 CRL 发布的最大滞后时间 35
4.9.9 在线状态查询的可用性 35
4.9.10 在线状态查询要求 35
4.9.11 撤销信息的其他发布形式 35
4.9.12 密钥损害的特别要求 35
4.9.13 证书冻结的情形 35
4.9.14 请求证书冻结的实体 35
4.9.15 冻结请求的流程 35
4.9.16 冻结的期限限制 36
4.10 证书状态信息服务 36
4.10.1 操作特征 36
4.10.2 服务可用性 36
4.11 停止使用认证服务 36
4.11.1 停止订户服务的情形 36
4.11.2 停止服务请求的处理时限、执行方式 37
4.11.3 服务终止后的责任延续条款 37
4.12 密钥托管与恢复 37
5. 认证机构设施、管理和操作控制 38
5.1 物理控制 38
5.1.1 物理访问控制 38
5.1.2 电力与空调 39
5.1.3 水患防治 39
5.1.4 火灾防护 39
5.1.5 介质存储 39
5.1.6 废物处理 40

5.1.7 异地备份 40
5.2 操作过程控制 40
5.2.1 可信角色 40
5.2.2 职责分离 41
5.2.3 每个角色的识别与鉴别 42
5.3 人员控制 42
5.3.1 资格、经历和无过失要求 42
5.3.2 背景审查程序 42
5.3.3 可信人员培训要求 43
5.3.4 再培训周期和要求 44
5.3.5 工作岗位轮换周期和顺序 44
5.3.6 未授权行为的处罚 44
5.3.7 独立合约人的要求 44
5.3.8 提供给员工的文档 44
5.4 审计日志程序 44
5.4.1 记录事件的类型 44
5.4.2 处理日志的周期 45
5.4.3 审计日志保存期限 45
5.4.4 审计日志的保护 45
5.4.5 审计日志备份程序 46
5.4.6 审计收集系统 46
5.4.7 对导致事件主体的通知 46
5.4.8 脆弱性评估 46
5.5 记录归档 46
5.5.1 归档记录的类型 46
5.5.2 归档记录的保存期限 47
5.5.3 归档文件的保护 48
5.5.4 归档文件的备份程序 48
5.5.5 记录时间戳要求 48
5.5.6 归档收集系统 48
5.5.7 获得和检验归档信息的程序 49
5.6 电子认证服务机构密钥更替 49
5.7 损害与灾难恢复 49
5.7.1 事故和损害处理程序 49
5.7.2 计算机资源、软件和/或数据的损坏 50
5.7.3 实体私钥损害处理程序 50
5.7.4 灾难后的业务存续能力 50
5.8 电子认证服务机构的终止 51
5.9 重大事项报告 51
6. 认证系统技术安全控制 53
6.1 技术安全管理制度要求 53

6.2 密钥对的生成和安装 53
6.2.1 CA 密钥对的生成和安装 53
6.2.2 订户密钥对的生成和交付 53
6.2.3 公钥传送给证书签发机关 54
6.2.4 CA 公钥传送给依赖方 54
6.2.5 密钥的长度 54
6.2.6 公钥参数的生成和质量检查 54
6.2.7 密钥使用目的 55
6.3 私钥保护和密码模块工程控制 55
6.3.1 CA 私钥保护和密码模块工程控制 55
6.3.2 订户私钥保护和密码模块工程控制 55
6.3.3 私钥备份 56
6.3.4 私钥归档 56
6.3.5 私钥导入、导出密码模块 56
6.3.6 销毁私钥的方法 57
6.4 密钥对管理的其他方面 57
6.4.1 公钥归档 57
6.4.2 证书操作期和密钥对使用期限 57
6.5 激活数据 58
6.5.1 激活数据的产生和安装 58
6.5.2 激活数据的保护 58
6.6 计算机安全控制 58
6.6.1 特别的计算机安全技术要求 58
6.6.2 计算机安全评估 59
6.7 生存周期安全控制 59
6.7.1 系统开发控制 59
6.7.2 安全管理控制 59
6.7.3 生命期的安全控制 60
6.8 网络的安全控制 60
6.9 时间戳 60
7. 证书、CRL 和 OCSP 61
7.1 证书 61
7.2 CRL 61
7.3 OCSP 61
8. 认证机构审计和其他评估 62
8.1 审计评估制度 62
8.2 认证业务审计 62
8.3 全面符合性评估 62
9. 法律责任和其他业务条款 64
9.1 费用 64
9.1.1 证书签发或更新费用 64

9.1.2 证书访问费用 64
9.1.3 证书撤销的费用 64
9.1.4 状态信息访问费用 64
9.1.5 其他服务费用 65
9.1.6 退款策略 65
9.2 财务责任 65
9.2.1 保险范围 65
9.2.2 资金保障 65
9.2.3 对最终实体的保险或担保 65
9.3 业务信息保密 66
9.3.1 保密信息范围 66
9.3.2 不属于保密的信息 66
9.3.3 保护保密信息的责任 66
9.4 个人隐私保护 67
9.4.1 个人隐私保护方案 67
9.4.2 作为隐私处理的信息 67
9.4.3 不被视为隐私的信息 67
9.4.4 保护隐私的责任 67
9.4.5 隐私信息的处理 68
9.4.6 依法律或行政程序的信息披露 68
9.4.7 其他信息披露情形 68
9.5 知识产权 68
9.6 陈述与担保 69
9.6.1 CA 的陈述与担保 69
9.6.2 订户的陈述与担保 70
9.6.3 依赖方的陈述与担保 71
9.6.4 其他参与者的陈述与担保 71
9.7 担保免责 71
9.7.1 订户违约、违规、未履行义务导致的免责 71
9.7.2 不可抗力导致的免责 72
9.7.3 技术故障导致的免责 72
9.8 偿付责任规则 73
9.8.1 财务赔偿范围 73
9.8.2 赔付计算方式 73
9.8.3 赔付监督机制 75
9.8.4 天威诚信的赔偿责任 75
9.8.5 订户的赔偿责任 75
9.8.6 依赖方的赔偿责任 76
9.8.7 天威诚信免责情形 76
9.9 赔偿 77
9.9.1 索赔申请 77

9.9.2 材料提交 77
9.9.3 审核处理 77
9.9.4 赔付执行 78
9.9.5 争议解决 78
9.10 有效期限与终止 78
9.10.1 有效期限 78
9.10.2 终止 78
9.10.3 效力的终止与保留 78
9.11 对参与者的个别通告与沟通 79
9.12 修订和发布 79
9.12.1 修订程序 79
9.12.2 通知机制与期限 79
9.12.3 必须修改业务规则的情形 79
9.13 争议处理 80
9.13.1 争议解决机制 80
9.13.2 举证制度与能力体系 81
9.14 管辖法律 83
9.15 与适用法律的符合性 83
9.16 一般条款 84
9.16.1 完整协议 84
9.16.2 转让 84
9.16.3 分割性 84
9.16.4 强制执行 84
9.16.5 不可抗力 85
9.17 其他条款 85
附录：电子签名认证证书内容 86

1. 概括性描述

本文档《证书策略和电子认证业务规则》（Certificate Policy, CP ； Certification Practice Statement, CPS），阐明了天威诚信在遵守《中华人民共和国电子签名法》、《电子认证服务管理办法》相关要求的前提下，签发用于民事活动中电子签名用途的数字证书的业务方式和过程，以及相应的服务、法律和技术上的措施和保障，以供电子认证活动参与方了解和遵循。

本 CP 和 CPS 的总体条款结构符合信息产业主管部门相关规范要求，在制定本 CP 和 CPS 时可能会对该框架进行扩充，以适应天威诚信认证业务的特定需求。

1.1 承诺

天威诚信开展经营和服务活动时，遵守法律、行政法规，树立以人民为中心的服务理念，承担社会责任；与客户建立业务关系前，天威诚信开展应用业务调研，建立应用接入业务风险评估及内部定责机制，严禁为存在违法违规风险的业务提供电子认证服务；天威诚信使用经过国家密码管理局审查的电子认证服务系统开展电子认证服务，并接受政府和社会监督，对主管部门检查发现的问题及时整改，建立问题纠治长效机制，持续符合整改要求。

1.2 基本信息

北京天威诚信电子商务服务有限公司（下称“天威诚信数字认证中心”，或简称“天威诚信”），是首批获得《电子认证服务许可证》的电子认证服务机构。作为国内专注于电子认证服务的运营商，天威诚信依靠先进而实用的技术和优质的服务，为广大的、对通信和信息安全方面有各种各样需求的公众提供数字证书认证服务。

天威诚信法定代表人为倪天宏，总部位于北京海淀区上地八街七号院 4 号楼 401 室，联系电话：010-50947500。天威诚信在长沙建有备份机房，地址为：湖南省长沙市望城区雷锋大道 1389 号 14 栋 2 层 207 号。天威诚信还在全国多个省市设有分部，详情参见：https://www.itrus.com.cn/contact.html。

天威诚信《电子认证服务许可证》许可证号为 ECP11010820003，工信部于 2020 年 8 月 19 日批准，有效期起止时间为 2020 年 8 月 19 日至 2025 年 8 月 18 日，目前正在办理续期。

天威诚信签发电子签名认证证书的信任体系包含两套，一套称为中国信任网络（China Trust Network, CTN）体系，该体系的主 CA（Primary CA, PCA）为天威诚信自签名根 CA；另一套称为国密信任体系，其主 CA 由国家密码管理局根 CA 签发。天威诚信在主 CA 之下创建证书签发 CA、以及为机构客户创建并运营的客户子 CA。两套体系均由天威诚信拥有、并负责运营和维护，具体信息如下：

iTrusChina Class 1 Root CA - G3，60C67B8A650DF705E2BDF34A3A7F6E774E760A2C，颁发机构天威诚信，RSA2048，有效期 20 年，计划服务到 2033 年；

iTrusChina Class 2 Root CA - G3，3C70317D8BA754676BCE78A6046D372B395A30C1，颁发机构天威诚信，RSA2048，有效期 30 年，计划服务到 2043 年；

iTrusChina Class 3 Root CA - G3，7BD98BF8DE388518E4123173CD8596564009EE80，颁发机构天威诚信，RSA2048，有效期 30 年，计划服务到 2033 年；

天威诚信数字认证中心根 CA，381EE63A885487A325B89969D4914D4A，SM2，有效期 20 年，计划服务到 2033 年；

天威诚信 SM2 算法证书链，其密钥长度为 256 位；更多证书链信息参见：https://www.itrus.com.cn/certificate1.html。

本 CP 和 CPS 仅适用于民事活动场景下天威诚信上述体系签发的电子签名认证证书。

1.3 文档名称与标识

本文档称为《天威诚信电子签名认证证书证书策略和认证业务规则》（简称天威诚信签名证书 CP 和 CPS），版本号、发布和生效日期、历史版本信息等见前述“版本控制表”。

天威诚信注册的 OID 为 1.2.156.112535。天威诚信民事活动场景下签发的电子签名认证证书使用 T/CQAE 11034-2025《电子认证业务规则规范》中规定的证书策略 OID，如下表所示：

证书类型	证书策略 OID	含义
个人高等级电子签名认证证书	2.16.156.339.2.1.1.2	适用于高风险业务、符合《电子签名法》的个人电子签名认证证书
个人基础级电子签名认证证书	2.16.156.339.2.1.1.1	适用于低风险业务、符合《电子签名法》的个人电子签名认证证书
机构高等级电子签名认证证书	2.16.156.339.2.1.2.2	适用于高风险业务、符合《电子签名法》的机构电子签名认证证书
机构基础级电子签名认证证书	2.16.156.339.2.1.2.1	适用于低风险业务、符合《电子签名法》的机构电子签名认证证书

1.4 电子认证活动参与者

1.4.1 电子认证服务机构（CA）

电子认证服务机构（Certification Authority，简称 CA）指获得授权能够颁发证书的实体。天威诚信作为根据《中华人民共和国电子签名法》、《电子认证服务管理办法》有关规定、依法设立的第三方电子认证服务机构，运营并维护天威诚信证书信任体系，向订户颁发电子签名认证证书等不同类型的数字证书。

1.4.2 注册机构（RA）

注册机构（Registration Authority，简称 RA）指具有受理、审核、批准或拒绝数字证书的申请、更新、恢复和撤销等的实体。

天威诚信除了承担 CA 的角色外，同时也承担 RA 的角色，且天威诚信民事活动场景下签发电子签名认证证书时，其 RA 机构仅由天威诚信承担。

1.4.3 订户

“订户”指向天威诚信申请证书的个人或组织机构，也称为用户（user）、或最终用户（end-user）。订户通常需要与天威诚信签订合同明确约定与证书有关的权利义务，并承担作为证书订户的责任。

1.4.4 电子签名依赖方

依赖方是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的实体。依赖方可以是证书订户，也可以不是订户。

1.5 证书应用

1.5.1 证书应用分类

天威诚信签发的数字证书分为电子签名认证证书和其他数字证书两大类。电子签名认证证书适用于《中华人民共和国电子签名法》规定的民事场景下的电子签名用途，其他数字证书不适用于电子签名用途。

1.5.1.1 电子签名认证证书

按照证书主体对象的类型，天威诚信签发的电子签名认证证书分为：

a) 个人证书

包含个人订户证书和机构雇员证书，适用于需精准区分、唯一标识、可靠鉴别自然人身份、进行个人电子签名的场景。个人证书细分为高等级和基础级两个级别，其证书策略OID 等信息参见 1.3 文档名称与标识。

个人基础级证书禁止用于涉及生命健康、财产权益等高风险活动。

b) 机构证书

包含机构单位证书和机构代表人证书，适用于需区分、标识、鉴别法人/非法人组织身份、进行机构电子签名的场景。机构证书细分为高等级和基础级两个级别，其证书策略OID 等信息参见 1.3 文档名称与标识。

机构基础级证书禁止用于涉及生命健康、财产权益等高风险活动。

天威诚信同时签发电子政务电子签名认证证书，适用于政务场景下的电子签名，其管理遵循《电子政务电子认证服务管理办法》等相关规定，详细信息参见电子政务证书相关CP/CPS。

1.5.1.2其他证书

天威诚信签发的其他数字证书均不适用于电子签名用途，具体包括：

a) 身份证书

身份证书安全等级为基础级，根据身份查验深度的不同可提供差异化认证强度，主要用于个人或机构身份识别、访问控制及数据完整性校验等场景，不适用于《中华人民共和国电子签名法》规定的民事场景下的电子签名用途。

b) 设备证书

设备证书安全等级为基础级至高等级，支持多级别身份验证，可满足不同安全等级的设备认证需求；主要用于域名认证、服务器等设备身份标识以及通信链路加密与数据完整性保护，以提供信息源发性证明、实现信息保密和完整性保障。典型应用包括 SSL/TLS 服务器证书、物联网设备证书等，不适用于《中华人民共和国电子签名法》规定的民事场景下的电子签名用途。

c) 时间戳证书

时间戳证书安全等级为高等级，基于可信时间源提供权威时间标记服务，主要用于固化电子数据的存在性与行为时序，遵循相关行业技术规范，不适用于《中华人民共和国电子签名法》规定的民事场景下的电子签名用途。

上述其他证书的详细信息参见相关 CP/CPS。

1.5.2 受限的应用

本 CP 和 CPS 所定义的天威诚信电子签名认证证书，主要适用于电子商务、互联网金融、企业信息化等合法的民事活动数字业务场景。

超出本 CP 和 CPS 及对应证书策略限定的应用范围、超出相关协议约定的应用范围、或未按规范使用证书的，相关电子签名行为不受天威诚信服务保障，由此产生的风险与法律责任由证书使用者自行承担。

1.5.3 受禁的使用

天威诚信签发的电子签名认证证书，不适用于以下活动中的文书：

a) 涉及婚姻、收养、继承等人身关系的；

b) 涉及停止供水、供热、供气等公共事业服务的；

c) 法律、行政法规明确规定的不适用电子文书的应用场景或类型；

d) 国家法律法规禁止的活动。

涉及生命健康、财产权益等高风险活动禁止使用基础级电子签名认证证书。

1.6 策略管理

1.6.1 策略文档管理机构

天威诚信设立了安全策略委员会，负责本 CP 和 CPS 的管理；其职责包括但不限于：

a) 确定维护 CPS 和 CP 等策略文档的职能分工，建立合理有效的修订和批准流程，形成 CP 和 CPS 管理制度并定期维护；

b) 对涉及信息安全策略、根证书密钥、证书签发自动审核等重要操作和流程进行审批；

c) 每年至少进行一次 CPS 和 CP 全面评审，根据实际需要及时修订策略文档；

d) 每年组织运营风险评估并形成报告。

天威诚信安全策略委员会成员名单获得公司批准后，在公司内部对委员会成员名单及委员会工作职责进行公示。安全策略委员会各次例会的重大决议的相关文件和会议记录均由专门人员进行整理、保存和归档。

天威诚信安全策略委员会联系地址和方式如下：

北京天威诚信电子商务服务有限公司

中华人民共和国北京市海淀区上地八街 7 号院 4 号楼 4 层（100085）

电话号码：0086-010-50947500

邮箱地址：itrus_pma@itrus.com.cn

1.6.2 策略文档批准程序

a) 天威诚信 CP 和 CPS 的具体编制、修订工作，由天威诚信安全策略委会授权合规部门协调相关业务部门骨干组成编写小组进行编制；该小组成员包括但不限于产品、认证、运维、审计、法务、合规等岗位人员。

b) 编写小组将 CP 和 CPS 草案提交天威诚信安全策略委员会进行审批；当安委会审批成员超过半数批准，且当安委会主任审批“同意”后，此版 CP 和 CPS 视为审批通过。

c) 通过审批的 CP 和 CPS 由编制小组提交公司网站管理部门发布到官网。

d) 编制小组根据国家法律法规和主管部门的要求，将通过审批的 CP 和 CPS 向主管部门报备。

e) 编写小组至少每年检查一次 CP 和 CPS，确保其符合国家法律法规和主管部门的要求及相关标准规范，以及 CP 和 CPS 是否需要根据认证业务开展的实际情况进行调整；当出现需要修订 CP 和 CPS 的情形时，由编写小组提出修订意见，经天威诚信安全策略委员会批准后，由编写小组负责完成修订，并执行审批流程。

1.7 定义和缩写

1.7.1 定义

术语	定义
安全策略委员会	认证服务体系内的最高策略管理监督机构和CP&CPS一致性决定机构
电子认证服务机构	Certificate Authority，也就是证书认证机构，是颁发证书的实体。
注册机构（RA）	负责处理证书申请人和证书订户的服务请求，并将之提交给认证服务机构，为证书申请人建立注册过程的实体。
证书策略（CP）	一套命名的规则集，用以指明证书对一个特定团体或者具有相同安全需求的应用类型的适用性。例如，一个特定的CP可以指明某类证书适用于鉴别从事企业到企业交易活动的参与

	方，针对给定价格范围内的产品和服务。
认证业务规则（CPS）	构成对证书的创建、颁发、管理和使用的治理框架的若干文档之一。
数字证书	也称公钥证书，由电子认证服务机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期及扩展信息的一种数据结构。
电子签名认证证书	由电子认证服务机构签发的，可证实电子签名人与电子签名制作数据有联系的数字证书。
电子签名	具有识别签名人身份和表明签名人认可签名数据的功能的技术手段。
数字签名	通过使用非对称密码加密系统对电子记录进行加密、解密变换来实现的一种电子签名。
电子签名人	是指持有电子签名制作数据并以本人身份或者以其所代表的名义实施电子签名的人。
电子签名依赖方	是指基于对电子签名认证证书或者电子签名的信赖而从事有关活动的实体。
私钥（电子签名制作数据）	非对称密码算法中由拥有者在电子签名过程中使用的不公开密钥，可将电子签名与电子签名人可靠地联系起来。
公钥（电子签名验证数据）	非对称密码算法中可公开的密钥，可用于验证电子签名。
订户	从电子认证服务机构接收证书的实体，也被称为证书持有人、证书所有者。
依赖方	依赖于证书真实性的实体。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。

1.7.2 缩写

缩写	全称	中文翻译

CA	Certificate Authority	电子认证服务机构，证书颁发机构
CP	Certificate Policy	证书策略
CPS	Certification Practice Statement	电子认证业务规则
DN	Distinguished Name	甄别名称，甄别名
SSL	Secure Sockets Layer	加密套接层协议
CRL	Certificate Revocation List	证书撤销列表
LDAP	Lightweight Directory Access Protocol	轻型目录访问协议
OCSP	Online Certificate Status Protocol	在线证书状态协议
PIN	Personal Identification Number	个人身份识别码
PKCS	Public KEY Cryptography Standards	公共密钥密码标准
PKI	Public Key Infrastructure	公共密钥基础设施
RA	Registration Authority	注册审核服务机构
OID	Object Identifier	对象标识符

2. 信息发布与信息管理

2.1 信息库

天威诚信通过 WWW 官方网站公布本 CP 和 CPS，以及相关的技术支持等信息。官网网址为：www.itrus.com.cn。本 CP 和 CPS 已按照国家电子认证服务管理平台的要求进行了备案。

2.2 认证信息的发布

天威诚信 CPS、CP 的所有版本可从天威诚信的官网获取；订户证书及证书链可从天威诚信的 LDAP 目录服务（ldap://ica-directory.itrus.com.cn:389）、或用户证书服务站点等方式获取；证书的状态（有效、撤销）可通过用户证书服务站点等方式查询；订户也可根据自身需要，向天威诚信申请使用 OCSP 服务向依赖方提供证书状态实时查询。

天威诚信将完成与国家电子认证服务管理平台的技术对接，实现根据证书唯一编码、订户身份信息等维度查询已签发证书列表的功能，并完成备案。

另外，天威诚信还通过官网或项目渠道公布如下信息：

a）详细的业务办理指南，包括但不限于服务网点地址、营业时间、联系电话等；

b）依赖方协议；

c）查询天威诚信的电子认证业务规则、证书策略的指引；

d）投诉处理政策及投诉方式，包括但不限于：投诉处理部门的地址、联系电话、电子邮件地址，以及内部监督部门名称。

2.3 发布的时间或频率

天威诚信发布的信息发生变化的，最迟不晚于变化生效后 1 个工作日内完成相关信息的更新。

2.4 信息库访问控制

对于天威诚信官网公布的信息，公众均可查询，没有限制。天威诚信通过网络安全防护、系统安全设计、安全管理制度确保这些信息只有授权人员才能修改。

只有经过审批的 RA/CA 管理员可以查询 CA 和 RA 数据库中的其他数据。

3. 身份标识与查验

3.1 身份查验通用要求

3.1.1 通用要求

天威诚信依据《中华人民共和国电子签名法》《电子认证服务管理办法》及相关标准规范，在本 CP 和 CPS 中完整明确证书签发前证书申请人身份信息、主体属性的全流程查验程序，同步规范密钥更新申请人、证书撤销申请人的身份查验实施规则，保障申请人身份真实、申请意愿合法有效。

总体查验原则如下：

a) 受理证书申请时，天威诚信将对订户和/或受托人进行告知、身份确认、意愿记录和协议签署。

订户和/或受托人阅读《电子认证服务协议》后，可通过手抄、录入或口述专属提示语、主动确认、线上勾选等方式完成意愿确认与协议签署。

b) 身份查验义务未委托外部机构、外部个人实施（与天威诚信非同一法人主体的机构均界定为外部机构），全部核验流程由天威诚信独立完成，实现查验全流程可控、操作全程可追溯。

3.1.2 订户告知

3.1.2.1告知内容

受理证书申请时，天威诚信向订户完整告知以下事项：

a) 订户权利义务：订户享有证书申请、续期、撤销等权利，同时承担如实提交材料、及时报备信息变更、妥善保管私钥、合规用证、私钥异常立即申请撤销或冻结等义务。

b) 服务收费项目和标准：收费标准以业务页面公示内容、双方协商约定内容为准。天威诚信有权变更收费标准并通过官方平台、业务系统、公示页面等合理方式进行告知。

c) 证书及电子签名使用条件：订户应按照约定的合法用途使用证书及电子签名，不得将其用于法定禁止使用电子签名的场景。

d) 信息安全保障措施：天威诚信遵循合法必要原则处理订户信息；资料留存不少于证书失效后 5 年，并依法承担保密责任。

e) CA 与订户责任划分

CA 责任：依法完成身份查验、保障证书内容在有效期内完整准确；因天威诚信过错造成订户直接损失的，按规则承担赔偿责任；因不可抗力、外部故障等非天威诚信原因导致的损失，不承担赔偿责任。

订户责任：保证申请资料及信息真实、完整、有效，信息变更的应在两个工作日内书面告知；因违规用证、提交虚假材料引发的全部损失由订户自行承担。

f) 签名私钥存储及安全要求

订户自行保管签名私钥的，订户负责妥善保管签名私钥、存储介质、相关密码口令等安全要素信息；因订户原因导致私钥泄露、损毁或丢失的，损失由订户自行承担；发现异常应立即告知天威诚信并进行处置。

订户委托天威诚信保管签名私钥的，天威诚信采用安全技术手段及必要措施存储私钥，未经授权天威诚信不得使用订户签名私钥。

g) 证书使用禁止条款：严禁将证书用于违法违规、违背公序良俗，或损害国家、公共及第三方合法权益的活动。

3.1.2.2 告知方式

天威诚信按照证书安全保障等级，采取差异化告知方式，所有告知操作均留存可追溯记录：

a) 高等级证书：采用面对面现场告知、电话语音告知、视频远程告知，或行业主管部门认可的其他合规方式完成告知，完整留存沟通记录、确认凭证。

b) 基础级证书：可选用高等级证书全部告知方式；也可采用业务页面强制阅读弹窗、短信告知、邮件书面告知等形式，同步留存用户已阅读、已确认的电子存证记录。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

天威诚信为订户提供符合国家密码标准的技术手段和管理措施，保障私钥生成安全，确保订户对私钥专有专控：

a) 按照 6.2.2 规定的方式生成订户密钥对；

b) 通过使用经数字签名的 PKCS#10 格式的证书请求，验证证书申请人拥有私钥。

3.2.2 个人身份的查验

3.2.2.1个人身份信息有效性的确认

天威诚信受理个人证书申请时，按以下要求完成个人身份信息查验工作：

a) 证件材料要求：要求订户出示法律法规、国家规范认可的有效身份证件原件或提交合规证件信息，仅采信法定有效身份证件作为核验依据；

b) 真实性核验方式：采用证件机读设备、公安部门等官方权威身份数据库，或主管部门认可的其他渠道，核验身份证件真实、有效，确认申请人提交身份信息客观属实；

c) 委托代办核验规则：若订户委托受托人代办证书业务，须核验由订户本人签署、权责清晰且在有效期内的书面授权文件，同时要求受托人出示自身有效身份证件或有效身份证件信息，并依据本条 b 项规则，同步核验订户本人、受托人双方身份资料；

d) 境外人员身份查验：境外人员身份核验，执行专属专项查验流程。

3.2.2.2个人高等级证书的实人查验

天威诚信对个人高等级证书订户开展实人查验，选用以下任一方式实施：

a) 面对面现场查验：工作人员现场核验身份证件原件，比对申请人现场样貌，完成线下人证合一校验并留存现场核验记录；

b) 远程人工面对面视频查验：通过实时视频连线，由天威诚信授权人员线上核验证件、比对申请人实时人脸，全过程留痕存证；

c) 生物特征验证：采用活体人脸、指纹、声纹、掌纹等合规生物识别技术，完成人证一致性校验；

d) 行业主管部门认可的其他等效身份核验方式;

e) 境外人员专属查验：境外自然人订户实人核验，执行专属专项查验流程。

天威诚信以可追溯形式完整记录、留存全部身份查验过程与核验结果，为单张证书分别建立独立身份验证档案；天威诚信有权依据国家最新法律法规、监管政策，动态更新个人高等级证书实人鉴别方法与查验流程。

3.2.2.3个人基础级证书的实人查验

天威诚信对个人基础级证书订户开展实人查验，选用以下任一方式实施：

a) 采用 3.2.2.2 条款规定的全部个人高等级证书实人查验方式；

b) 电信运营商三要素核验：比对姓名、身份证件号码、预留手机号在电信运营商系统信息一致性，向该手机号下发随机短信验证码完成二次校验；

c) 银行卡四要素核验：比对姓名、身份证件号码、银行卡号、银行预留手机号在银行系统信息一致性，通过预留手机号随机短信验证码完成二次校验；

d) 存量有效证书签名核验：依托申请人本人持有、状态合法有效的电子签名认证证书完成身份签名校验；

e) 主管部门认可的其他可信核验途径：包括居民身份网络可信凭证、公民网络电子身份标识、国家网络身份认证系统、内地银行或支付机构对外提供的个人账户与身份关联信息校验等方式。

天威诚信完整记录并归档全部身份查验过程与核验结果，为每张基础级证书单独建立独立身份验证记录；天威诚信有权依据国家最新法律法规、监管政策，动态更新个人基础级证书实人鉴别方法与查验流程。

3.2.3 组织机构身份的查验

3.2.3.1机构身份信息有效性的确认

天威诚信受理机构证书申请时，按以下要求完成身份信息查验：

a) 机构有效证件查验：核验机构法定主体证明文件，有效证件仅限法律法规、国家文件规定类型，包含但不限于营业执照、事业单位法人证书、统一社会信用代码证书、社会团体法人登记证书、律师事务所执业许可证、行业主管部门核发的批文或登记证书及其他法定机构资质证件；

b) 法定代表人、受托人身份查验规则：

法定代表人、受托自然人的身份证件真实性、有效性查验流程，参照本规范3.2.2.1 个人身份信息有效性的确认条款执行；

受托人办理时，额外核验加盖机构公章、权责完整且在有效期内的书面授权文件。

c) 境外机构和特殊机构，按国家相关规定执行专属查验流程。

3.2.3.2机构高等级证书的实人查验

天威诚信对机构高等级证书订户开展实人查验，选用以下任一方式实施：

a) 法定代表人实人查验，查验方式参照 3.2.2.2 个人高等级证书实人查验全部方法执行；

b) 受托人实人查验，先按 3.2.2 条款完成受托人实人核验，再叠加机构对公账户随机金额打款验证，或采用主管部门认可的其他等效核验方式。

天威诚信以可追溯形式完整记录、留存全部身份查验过程与核验结果，为每张机构高等级证书单独建立独立身份验证记录；天威诚信有权依据国家最新法律法规、监管政策，动态更新机构高等级证书实人鉴别方法与查验流程。

3.2.3.3机构基础级证书的实人查验

天威诚信对机构基础级证书订户开展实人查验，选用以下任一方式实施：

a) 法定代表人实人查验，查验方法参见 3.2.2.3 条款；

b) 受托人实人查验，查验方法参见 3.2.2.3 条款；

c) 采用订户自身持有的、同等级或更高安全等级的有效机构证书完成签名核验。

天威诚信完整记录并归档全部身份查验过程与核验结果，为每张机构基础级证书单独建立独立身份验证记录；天威诚信有权依据国家最新法律法规、监管政策，动态更新机构基础级证书实人鉴别方法与查验流程。

3.3 订户意愿记录

3.3.1 订户意愿记录内容

天威诚信留存的订户意愿记录，包含但不限于以下信息：

a) 订户身份信息：个人订户身份信息、机构订户身份信息及其法定代表人或受托自然人身份信息；

b) CA 机构信息：对订户身份进行查验的 CA 机构信息，即天威诚信信息；

c) 签名私钥保存方及其保存义务：区分订户自行保管、委托天威诚信保管的情形，详见订户与天威诚信签订的协议；

d) 订户对电子签名的法律责任：详见订户与天威诚信签订的协议；

e) 订户明确知晓并同意的意思表示记录：即可证明订户已知晓本条 a 至 d 全部条款内容并自愿办理证书业务、同意与天威诚信签署协议的，可追溯的完整记录。

3.3.2 个人高等级证书的意愿记录

天威诚信对个人高等级证书订户开展申请意愿确认，选用以下任一方式实施：

a) 现场办理场景：采用面对面确认或手抄专属提示语完成意愿核验，并采用录音录像或主管部门认可的其他合规手段留存订户意愿记录；

b) 远程办理场景：通过实时音视频连线或主管部门认可的其他等效方式完成意愿确认，并完整留存对应意愿记录。

3.3.3 个人基础级证书的意愿记录

天威诚信对个人基础级证书订户开展申请意愿确认，选用以下任一方式实施：

a) 采用 3.2.2.2 条款规定的个人高等级证书全部意愿确认方式；

b) 采用强制阅读弹窗、短信核验、邮件确认等电子化渠道完成意愿确认。

天威诚信完整留存完整、可追溯的订户意愿确认记录，为每张个人基础级证书单独建立独立意愿留存档案；天威诚信有权依据国家最新法律法规、监管政策，动态更新证书意愿确认与存证流程。

3.3.4 机构高等级证书的意愿记录

天威诚信对机构高等级证书订户开展申请意愿确认，选用以下任一方式实施：

a) 法定代表人自行申请的，依照 3.3.2 条款规定方式完成法定代表人意愿确认；

b) 受托人代办申请的，先核验加盖机构公章的有效授权文件，再依照 3.3.2 条款规定方式完成受托人意愿确认。

3.3.5 机构基础级证书的意愿记录

天威诚信对机构基础级证书订户开展申请意愿确认，选用以下任一方式实施：

a) 法定代表人自行申请的，依照 3.3.3 条款规定方式完成法定代表人意愿确认；

b) 受托人代办申请的，查验验加盖机构公章的有效授权文件，并依照 3.3.3 条款规定方式完成受托人意愿确认。

天威诚信完整留存完整、可追溯的订户意愿确认记录，为每张机构基础级证书单独建立独立意愿留存档案；天威诚信有权依据国家最新法律法规、监管政策，动态更新机构证书意愿确认与存证流程。

3.4 订户协议

天威诚信订立的订户协议包含 3.1.2.1 列明的全部告知事项内容，明确约定 CA 与订户双方各项权责。

3.5 未验证的订户信息

天威诚信对证书中载明的全部信息（证件号、地址、联系方式等）按照3.2.2、3.2.3实施合理、必要的查验与核验，确保信息真实、准确、有效。

电子签名认证证书中不包含未经验证的订户信息。

3.6 互操作准则

天威诚信能根据业务情况，与其他经过国家主管部门批准的电子认证服务机构签订互操作协议，遵循国家统一规范开展跨机构证书互认与互操作业务。

3.7 命名与主体标识

3.7.1 命名规范

天威诚信签发的个人证书和机构证书，命名规则具备实际语义且唯一对应实体主体、支持全生命周期追溯。证书主体 DN 项或扩展项中，须包含申请人个人有效身份证件类型及其编号（或其映射值，如包括但不限于编号的散列值、掩码等）、或组织机构的有效证件类型及其编号。

3.7.2 DN 项结构规则

证书主体 DN 项结构严格遵循 GB/T 16264.8 国家标准要求。编码规则见下表。

代码	说明	可选性
C	国家（固定为 CN）	必选
ST	省份 / 自治区 / 直辖市	可选
L	城市 / 区县	可选
O	订户所属机构全称	可选（机构代表人证书和机构雇员证书必选）
OU	订户所属机构部门	可选（对于机构代表人证书本项标明为“机构代表人”）
CN	订户名称（个人姓名 / 机构法定全称）	必选

3.7.3 扩展与约束

天威诚信在不影响证书通用性的前提下，可按业务需求增加合规自定义扩展项的其他内容。

证书禁止使用匿名、伪名或非法定义名称申请与签发。

天威诚信为同一个主体可按不同证书策略、用途，以相同的甄别名签发多个合法有效证书。

证书申请人不得使用侵害他人知识产权、商标权的名称申请证书；天威诚信受理证书申请时，不主动核查商标权属与纠纷状态，若出现相关争端，天威诚信有权拒绝新申请或撤销/冻结已签发证书，直到争端依法解决。

4. 证书生存周期操作要求

4.1 通用要求

天威诚信（即 CA）与订户分别承担以下责任：

a) CA 负责搭建、运营及维护证书注册办理通道；

b) CA 负责与证书订户签署订户协议（即电子认证服务协议）；

c) 订户负有向 CA 提交真实、准确、完整身份信息及资料的责任；

d) CA 负责妥善记录并保存证书业务办理流程的相关信息及资料。

4.2 证书申请

4.2.1 证书申请主体

符合国家法律法规规定，在民事活动应用场景中需使用电子签名认证证书的个人、法人、非法人组织，均可向天威诚信申请证书。

组织机构申请机构证书时，须由法定代表人/经营者/负责人或书面授权的经办人提交申请。

4.2.2 注册过程与责任

证书申请人可通过天威诚信官方证书服务站点，或通过上述证书服务站点对接的证书申请平台注册并提交申请，须本人或受托人明确表示证书申请的真实意愿。在受理证书申请时，天威诚信将与申请人签订电子认证服务协议（或订户协议），明确双方的权利义务。

a) 对于机构证书，注册时申请人须正确填写以下信息：

   1) 身份信息：机构的真实身份标识信息，如机构法定名称、统一社会信用代码、注册地址、法定代表人信息等；

   2) 授权材料：机构授权的申请人姓名、身份证号码、授权委托书、联系电话与邮箱、对公账户信息（如需）等。

b) 对于个人证书，注册时申请人须正确填写以下信息：

1) 身份信息：个人的真实身份标识信息，如个人真实姓名、身份证号码、实名登记的电话号码、人脸核验信息等；

2) 辅助信息：所属单位（如需）、邮件地址、用途说明等。

天威诚信将妥善记录并保存上述注册过程中的相关材料和信息。

申请人提供虚假、残缺、错误信息，或冒用他人身份申请，或者有其他过错，给电子签名依赖方、天威诚信造成损失的，依法承担相应的民事赔偿甚至刑事责任。

4.2.3 证书申请处理

4.2.3.1执行标识和查验功能

天威诚信按照本 CP 和 CPS 第 3 章所述方式执行对证书申请人的标识和查验，完成对申请人的告知、身份确认、意愿记录及协议签署，并对处理过程进行全程留痕、确保可追溯。

4.2.3.2证书申请的批准和拒绝

在天威诚信完成对证书申请的查验、且证书申请人履行了其他应尽的责任（如付款）后，天威诚信将批准证书申请。如果查验未获通过或证书申请人未履行其他应尽的责任（如付款），天威诚信将拒绝该证书申请。

4.2.3.3处理证书申请的时限

天威诚信将在合理时间内完成证书请求处理。在申请人提交资料齐全、准确的情况下，处理证书申请的时间一般不超过两个工作日。高敏感与复杂场景等特殊情形，天威诚信将及时告知，并与订户协商申请处理的时间期限。

4.3 证书签发

4.3.1 签发过程

在证书签发前，天威诚信负责对证书申请材料及信息进行查验；查验通过后，天威诚信将批准证书申请，验证通过的信息由天威诚信认证系统执行证书生成及签发操作。

4.3.2 结果通知

无论是拒绝还是批准订户的证书申请，天威诚信在证书申请处理完毕后将向订户通知处理结果，通知方式包括但不限于：

a) 通过认证应用工具进行系统提示；

b) 通过信函、站内信或电子邮件发送；

c) 通过短信通知；

d) 通过电话通知；

e) 当面通知或通过实时视频等相当于面对面的方式通知；

通过主管部门认可的其他方式通知。

4.4 证书接受

4.4.1 证书的交付

天威诚信根据证书类型、安全等级与应用场景采用差异化交付方案，在线交付通道启用加密传输机制，确保证书交付过程的机密性、完整性与可追溯性。

4.4.1.1硬件交付

a) 现场交付：订户或其受托人持有效身份证明文件，到天威诚信自有服务网点完成身份核验后，现场领取存储证书的介质（如智能密码钥匙等）；

b) 物流交付：通过具备全程物流追踪能力的渠道，将硬件证书寄送至订户预留的收件地址，并要求收件人本人签收。

4.4.1.2非硬件交付

a) 在线自助下载交付：订户通过身份二次核验后，登录天威诚信官方服务平台或指定认证服务工具，主动在线下载公钥证书文件。订户成功下载公钥证书文件之时即为交付完成时间。

b) 接口方式交付：天威诚信系统通过加密通道将公钥证书文件返回至预先约定的应用系统或设备终端，推送结果实时回执留痕。系统收到成功接收的回执之时即为交付完成时间。

c) 邮件通知交付：天威诚信将证书下载链接与安装指引通过电子邮件发送至订户预留的授权电子邮箱，订户需主动登录电子邮箱下载公钥证书文件。订户成功下载公钥证书文件之时即为交付完成时间。

d) 主管部门认可的安全交付方式。

4.4.2 证书的接受

4.4.2.1构成接受证书的行为

符合以下任一情形的，视为订户有效接受证书：

a) 明示接受

1) 订户在天威诚信官方服务平台、指定认证服务工具中通过点击、勾选等操作主动完成接受证书的；

2) 现场领取硬件证书时，订户或受托人签署证书接受凭证；

3) 订户使用有效数字签名签署证书接受凭证并反馈至天威诚信。

b) 默示接受

1) 订户首次使用证书完成电子签名、身份认证、数据加密等密码运算行为；

2) 订户成功下载/接收证书后，未在 2 个工作日内提出书面拒绝申请；

3) 通过物流渠道收取介质的，自渠道反馈本人签收状态之日起未在 2 个工作日内未提出书面异议。

4) 非硬件证书推送至指定终端后，订户未在 2 个工作日内提出书面异议。

5) 证书签发完成满 7 个自然日，订户未提交书面拒绝材料的，视作接受证书。

证书接受即代表订户确认证书所载信息无误，充分知晓并认可全部证书使用义务与法律责任。

4.4.2.2拒绝接受证书的行为

a) 拒绝接受证书的适用情形

订户有正当理由的，可在异议期内申请拒绝接受证书，适用情形包括：

1) 证书所载信息与申请内容不符，存在信息录入错误、主体信息偏差等问题；
2) 证书文件损坏无法正常安装使用，或介质证书硬件故障、无法正常识别；
3) 订户确认非本人/本机构提交证书申请，存在冒领、误发情形。

b) 拒绝接受证书的办理流程

1) 申请提交：订户需在证书交付后的 2 个工作日内，通过天威诚信官方服务渠道提交书面拒绝申请，说明拒绝理由并附上对应证明材料；
2) 核验处理：天威诚信收到申请后 2 个工作日内完成材料核验与事实核查。拒绝理由成立的，立即对该证书执行注销操作，同步告知订户后续方案（如免费重新签发或按协议退费）；拒绝理由不成立的，向订户出具书面说明并告知依据，证书维持正常状态；
3) 结果生效：订户逾期未提出异议的，视为默认接受证书；已生效的拒绝申请，订户无需承担该证书对应的使用责任。

4.4.3 证书接受记录的保存

天威诚信对证书的交付、接受与拒绝全流程留存完整可追溯记录，以满足监管审计与司法举证要求。

4.4.3.1记录内容

a) 证书标识信息：如证书序列号；
b) 交付与接受信息：交付方式、交付时间、接受时间、操作人信息；
c) 异常处理信息：如存在拒绝、异议流程，同步留存申请材料、核验结果、处理节点与最终结论。

4.4.3.2记录管理要求

a) 电子记录存储方式：应采取安全技术手段保障记录不可篡改、可追溯；
b) 记录保存期限：不少于证书有效期届满后5年，法律法规、行业规范对保存期限有更长要求的，从其规定；
c) 记录查阅与调取：严格执行权限管控与审批流程，仅授权合规、审计与法务人员可按规定访问，保障订户信息安全与隐私。

4.4.4 CA对证书的发布

天威诚信提供基于LDAP协议的目录服务，天威诚信根据订户需求决定是否将其证书发布到目录系统或者数据库中。

4.4.5 CA对其他实体的通告

对于天威诚信签发的证书，天威诚信不通知其他实体。

4.5 密钥对和证书使用

4.5.1 密钥对和证书管理

密钥对和证书不应用于其规定的、批准的用途之外的目的，否则其应用是不受相关法律和天威诚信策略保障的。

天威诚信在将密钥对交给订户保管前，保护电子认证服务活动中密钥对和证书使用的安全性，具体包括：

a) 保障私钥生成和传输过程的安全性，在私钥交付前实施有效的安全控制措施；
b) 审核订户密钥的安全性，拒绝为不符合国家或行业相关安全标准要求的密钥颁发证书；
c) 对于使用天威诚信签名私钥委托保管服务的订户，天威诚信确保：
    1) 未经订户书面授权，不保存或委托他人保存订户签名私钥；

2) 订户签名私钥仅在获得订户明确授权的情况下使用； 对于机构证书签名私钥的使用，仅应设置法定代表人或受托人作为授权主体进行使用；
3) 签名私钥以加密形式存储，保存条件符合相关安全标准；
4) 签名私钥所有操作均有完整记录并可追溯。

天威诚信建有便捷的外部安全事件反馈渠道，及时受理和处理证书信息错误、私钥失密或证书被盗用等异常情况。

4.5.2 订户私钥和证书使用

订户在提交了证书申请并接受了天威诚信签发的证书后，视为已同意遵守与天威诚信和依赖方有关的权利和义务条款。

订户只能在指定的应用范围内使用私钥和证书，并在证书到期或撤销后，停止使用该证书及对应的私钥。

4.5.3 依赖方公钥和证书使用

当依赖方接收到数字签名的信息后，应该，

a) 获得数字签名对应的证书及信任链；
b) 验证证书有效性；
c) 确认该签名对应的证书是依赖方信任的证书；
d) 确认证书的用途适用于对应的签名；
e) 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。

4.6 证书续期

4.6.1 证书续期的情形

证书续期指在不改变订户主体信息的情况下，在原证书到期前，为订户签发新证书的行为。通常情况下，天威诚信会在证书到期前 30 天内通过电子邮件、短信或站内信等方式向订户发送证书到期提醒。

符合以下条件的，订户可以申请证书续期：

a) 原证书由天威诚信签发且当前状态有效；

b) 续期申请在原证书到期前 30 天内提出；

c) 订户注册信息无实质变更（包括但不限于主体名称、统一社会信用代码、法定代表人等核心信息）；

d) 续期后证书用户与原证书一致。

有下列情形之一的，不予办理续期，需按照初始申请流程重新申请证书：

a) 订户主体信息发生实质性变更的；

b) 原证书已过期、已撤销或已冻结的；

c) 订户申请更换密钥对的（按证书密钥更新流程办理）；

d) 其他不符合续期条件的情况。

4.6.2 请求证书续期的实体

证书续期申请人为订户本人或其授权受托人。申请主体要求同 4.2.1。

4.6.3 证书续期请求的处理

4.6.3.1 身份查验方式

接收到证书续期请求后，天威诚信按照以下规则进行身份查验：

a) 自申请人上次完成身份查验之日起至本次续期申请日未满三年的，可使用有效的原证书进行电子签名验证的方式进行身份确认；

b) 自申请人上次完成身份查验之日起至本次续期申请日已满三年的，按照本规则 3.2 的规定重新进行身份查验。

4.6.3.2 续期请求验证

对于不更新密钥的续期请求，订户提交的证书签名请求（PKCS#10）包含原证书的公钥，并由原证书私钥签名。

接收到证书续期请求后，天威诚信认证系统自动以下验证：

a) 确认原证书存在并且由天威诚签发；

b) 确认续期申请在允许的期限内；

c) 原证书电子签名验证通过。

4.6.3.3续期审核与新证书签发

续期请求验证通过的，天威诚信根据证书类型完成续期审核与新证书的签发：

a) 个人证书

针对个人订户证书，按照新证书申请同等流程完成身份审核查验后，批准续期申请并签发新证书；证书中包含所属组织机构信息的，还需确认订户仍与相关组织机构存在所属关系。

针对机构雇员证书，按照新证书申请同等流程完成身份审核查验、并确认订户仍为对应机构雇员后，批准续期申请并签发新证书。

b) 机构证书

对于机构证书（包括机构单位证书和机构代表人证书），按照新证书申请同等流程完成机构身份查验、授权确认等审核后，批准续期请求并签发新证书。

以上审核过程可采取自动或手动方式完成；签发新证书的流程同 4.3.1。

对于更换密钥的证书密钥更新请求处理，参见 4.7.3。

4.6.4 签发续期证书时对订户的通知

同 4.3.2。

4.6.5 构成接受续期证书的行为

同 4.4.2.1。

4.6.6 CA 对续期证书的发布

同 4.4.4。

4.6.7 CA 对其他实体的通告

同 4.4.5。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

对于天威诚信签发的任何最终用户证书，除与订户有特殊约定外，证书到期前 30 天系统将通过电子邮件、短信或站内信等方式向订户提醒订户证书将到期。如果订户希望继续使用证书、保持原有注册信息继续有效但要变更证书密钥对，则订户可以申请证书密钥更新。证书密钥更新将使用新的公钥但证书的签发者和主体名不变，因此，证书密钥更新是改变证书密钥对的证书更新。在证书到期前 30 天内，订户可访问天威诚信的证书服务站点或对接的证书申请平台申请证书密钥更新。

若订户希望保持证书密钥对不变，则应采用证书续期（参见 4.6）。

若订户需要改变注册信息，则不能更新证书，需按新证书申请流程进行。

证书过期或撤销后不允许证书密钥更新。

4.7.2 请求证书密钥更新的实体

同 4.2.1。

4.7.3 证书密钥更新请求的处理

对于证书密钥更新请求，订户提交的证书签名请求（PKCS#10）包含有新的公钥，并由新私钥签名；同时，证书签名请求中还包含有用原证书私钥签名的更新请求信息。

接收到订户的证书密钥更新请求后，天威诚信认证系统会自动完成如下验证操作：

a) 确认、验证申请对应的原证书存在并且由天威诚信认证机构签发；

b) 证书更新请求在允许的期限内；

c) 用订户新的公钥对证书签名请求进行签名验证；

d) 用原证书的公钥对证书签名请求中的、使用原证书私钥签名的有关更新请求信息进行签名验证。

以上自动验证通过后，天威诚信按与证书续期相同的方式和流程（参见 4.6.3）完成证书密钥更新请求的鉴证、批准，签发新的证书。

注：关于身份查验，按照 4.6.3 的处理方式，自申请人上次完成身份查验之日起至本次更新申请日未满三年的，可使用有效的原证书进行电子签名验证的方式进行身份确认；自申请人上次完成身份查验之日起至本次更新申请日已满三年的，按照本规则 3.2 的规定重新进行身份查验。

4.7.4 签发新证书时对订户的通知

同 4.3.2

4.7.5 构成接受密钥更新证书的行为

同 4.4.2.1。

4.7.6 CA 对密钥更新证书的发布

同 4.4.4。

4.7.7 CA 对其他实体的通告

同 4.4.5。

4.8 证书变更

4.8.1 证书变更的情形

证书变更指改变证书中除订户公钥之外的信息而签发新证书的情形，例如：订户名称改变等。天威诚信的认证业务不直接支持证书变更。订户要变更证书中的内容时，视为申请一张新证书，需要先将原有证书撤销，才能申请新证书，且证书的申请及处理流程与申请新证书一致。

4.8.2 请求证书变更的实体

原证书订户。

4.8.3 证书变更请求的处理

同 4.2.3。

4.8.4 签发新证书时对订户的通告

同 4.3.2。

4.8.5 构成接受变更证书的行为

同 4.4.2.1。

4.8.6 CA 对变更证书的发布

同 4.4.4。

4.8.7 CA 对其他实体的通告

同 4.4.5。

4.9 证书撤销和冻结

证书撤销是使证书永远失效的操作，证书冻结是证书在有效期内暂时中止其使用效力的操作。天威诚信不提供证书冻结服务。

4.9.1 证书撤销的情形

出现以下情况，最终用户证书必须撤销：

a) 天威诚信或订户有理由相信或强烈的怀疑一个订户的私钥安全已经受到损害。
b) 天威诚信有理由相信订户违背了订户协议下的义务、陈述或担保、或者违反了法律法规。

c) 天威诚信和订户达成的订户协议已经终止。

d) 天威诚信有理由相信证书签发时没有遵循本 CP 和 CPS 规定的有关程序，如：证书签发给了非证书主体的人员或机构或没有鉴证该人员或机构在证书中的主体信息就签发了证书等情况。

e) 除了未经鉴证的订户信息外，包含在证书中的信息不正确或已经改变。

f) 天威诚信有理由认为证书申请信息存在与事实不符的错误、或证书信息虚假、伪造、失效。

g) 天威诚信确认证书签发的某项必要前提条件未满足且未获得豁免。

h) 订户在证书使用过程中存在重大安全风险、纠纷或涉及司法/监管要求；

i) 订户请求撤销证书。

4.9.2 请求证书撤销的实体

有权申请撤销最终用户证书的实体包括证书订户、订户授权受托人、证书依赖方及CA机构（即天威诚信），具体规则如：

a) 天威诚信、证书订户、订户授权受托人、证书依赖方，可依据 4.9.1 所列情形发起证书撤销请求。

b) 个人证书的订户，可随时自主申请撤销本人持有的证书。

c) 机构证书仅可由该组织机构授权代表（订户授权受托人）发起撤销申请。

4.9.3 撤销请求的流程

天威诚信仅支持对有效状态的证书办理撤销，具体流程如下：

a) 订户自助撤销：订户在申请证书阶段预留专属挑战语。发起自助撤销时，提交对应挑战语，经系统校验一致后，自动完成证书撤销。

b) 线下/人工渠道撤销申请：订户可通过电话、邮件等方式咨询撤销办理流程并提交正式撤销申请。本机构根据证书安全等级，采用电话回访、邮件核验、纸质函件、线下寄递等方式组合核验申请人身份与权限，核实申请人为证书订户本人或其合法授权受托人，核验无误后办理证书撤销。

c) 机构主动撤销：当查实证书存在安全隐患、违规使用等问题时，本机构有权启动审批流程，主动实施证书撤销。证书撤销办结后，将以电子邮件等形式通知订户，同步告知撤销状态及具体缘由。

天威诚信设立客服热线等便捷受理渠道，完整记录密钥丢失、私钥泄露、主体信息变更、违规用证等各类影响证书与私钥安全的事件。

所有撤销申请均须核验申请人真实身份及对应操作权限，核验完成后作出受理或驳回决定。

天威诚信完整留存全部证书撤销业务的申请材料、核验记录、审批流程及处置结果，所有操作记录全程可追溯。

4.9.4 撤销请求宽限期

当订户发现出现 4.9.1 中的情况时，应该及时向天威诚信提出撤销请求。

4.9.5 CA 处理撤销请求的时限

一般情况下，天威诚信从接到撤销请求及撤销申请材料并完成审核后，24 小时内撤销证书。

4.9.6 依赖方检查证书撤销的要求

依赖方应当检查他们所信任的证书是否被撤销。检查方式是通过用户证书服务站点查询或查询天威诚信发布的 CRL 完成。

4.9.7 CRL 发布频率

天威诚信的认证系统每天为证书签发 CA 产生证书撤销列表，也可根据订户需要定制证书撤销列表产生的其他频率。

天威诚信的 CA 证书的 CRL（ARL）定期进行更新。如果撤销 CA 证书，天威诚信在撤销后 24 小时之内更新 ARL。

4.9.8 CRL 发布的最大滞后时间

天威诚信的 CRL 发布最大滞后时间为 CRL 签发之后的 24 小时内。

4.9.9 在线状态查询的可用性

订户可根据自身需要，向天威诚信申请使用 OCSP 服务向依赖方提供证书状态实时查询。天威诚信提供的证书状态在线查询服务（OCSP）7X24 小时可用。

4.9.10 在线状态查询要求

订户可通过用户证书服务站点查询，或根据自身需要，向天威诚信申请使用 OCSP 服务向依赖方提供证书状态实时查询。天威诚信 OCSP 响应时间不超过 200ms。

4.9.11 撤销信息的其他发布形式

订户可通过用户证书服务站点下载天威诚信所发布的 CRL 来查询证书撤销信息。

4.9.12 密钥损害的特别要求

无论是订户还是天威诚信，发现证书密钥受到安全损害时应立即撤销证书。

4.9.13 证书冻结的情形

天威诚信不提供证书冻结。

4.9.14 请求证书冻结的实体

不适用。

4.9.15 冻结请求的流程

不适用。

4.9.16 冻结的期限限制

不适用。

4.10 证书状态信息服务

证书的状态（有效、撤销）可通过用户证书服务站点查询；订户也可根据自身需要，向天威诚信申请使用 OCSP 服务向依赖方提供证书状态实时查询。

4.10.1 操作特征

天威诚信提供的证书状态查询以网络服务的形式：

a) CRL 通过 80 端口采用 HTTP 协议提供；

b) OCSP 符合国家相关标准，反映证书的当前状态；

c) 证书目录 LDAP 符合 LDAP V3（RFC3377，2251-2256，2829-2830）。

4.10.2 服务可用性

天威诚信的 CRL、OCSP 证书状态服务均保证 7X24 可用，并且采用了冗余技术，服务可用率不低于 99%。

天威诚信提供上述查询服务不可用时的备用查询机制，包括电话查询、邮件查询等，并在官网公布服务故障情况及预计恢复时间。

4.11 停止使用认证服务

4.11.1 停止订户服务的情形

a) 订户主动申请终止电子认证服务；

b) 证书到期后订户放弃续期、密钥更新；

c) 订户存在虚假申报信息、违规超范围使用证书、拒不履行协议义务等违约行为；

d) 法律法规、监管要求需终止服务的其他情形。

4.11.2 停止服务请求的处理时限、执行方式

a) 处理时限：订户主动申请停止服务，资料齐全核验无误后 2 个工作日内办结；
b) 证书与私钥处置：服务终止后，对订户名下全部有效证书执行撤销操作；由本机构托管的签名私钥按安全规范彻底销毁，不再留存可用私钥；
c) 用户数据管理政策：业务档案、身份核验、意愿留存等法定凭证资料按要求持续留存至证书失效满 5 年。

4.11.3 服务终止后的责任延续条款

a) 证书撤销前已发生的电子签名行为效力不受服务终止影响，双方对应权责持续有效；
b) 天威诚信对留存档案承担法定保密、举证义务；订户对服务终止前违规用证、虚假信息造成的损失仍承担全部责任；
c) 数据留存期内，天威诚信配合司法、监管机关调阅相关业务记录。

服务终止的申请材料、身份核验记录、证书撤销审批单等相关记录将被完整保存。

4.12 密钥托管与恢复

天威诚信未将 CA 私钥托管给任何第三方机构或个人，CA 私钥在天威诚信控制的安全环境中保管。天威诚信建立了 CA 密钥备份与恢复策略，对 CA 密钥进行安全备份，参见 6.3.3。

5. 认证机构设施、管理和操作控制

5.1 物理控制

天威诚信的运营场地位于北京市海淀区上地八街 7 号院 4 号楼 401，天威诚信的机房场地建设符合 GB/T 25056-2018《证书认证系统密码及其相关安全技术规范》中关于物理环境建设的要求。

天威诚信机房场地根据业务功能分为公共区、管理区、服务区和核心区，安全等级和相应的防护要求逐级提高，区域功能和防护控制措施遵循 GB/T 25056-2018《证书认证系统密码及其相关安全技术规范》相关要求。

5.1.1 物理访问控制

天威诚信的管理区、服务区和核心区的门禁系统可实现对各层门进出的控制，具备以下功能：

a) 采用身份识别卡和指纹鉴别的控制方式控制每道门的进入；
b) 进出每一道门都有日志记录，门禁日志保存 12 个月以上；
c) 服务区、管理区、和核心区的门都设有强开报警和超时报警；
d) 整套门禁系统连接 UPS，在市电中断时由 UPS 提供紧急供电。
e) 管理区和核心区采取身份识别卡和指纹鉴别的“双因素认证”的访问控制策略；并且核心区屏蔽机房采取两名可信人员同时使用身份识别卡和指纹鉴别“双人共管”访问控制策略。

整个区域还有视频监控系统，对场地内外的重要通道实行 7*24 小时不间断录像。所有录像资料至少保留 12 个月，以备查询。天威诚信定期对相关记录进行检查，形成的检查记录存档备查。

5.1.2 电力与空调

天威诚信有安全、可靠的电力供电系统及电力备用系统以确保系统 7*24 小时正常供电，防止供电中断时影响服务。另外，天威诚信还具有加热/通风/空调系统控制运营设施中的温度和湿度。

天威诚信机房采用不间断供电系统 UPS，可提供至少 8 小时的电力供应。机房区域内采用了防静电措施，实现机柜、服务器、网络设备等电位连接和接地。

机房的空调采用风冷式冷凝器机组，室外风冷式冷凝器机组放置在顶楼。机房室内设计温度 23±2℃，并保持相对湿度在 40%-60%。

5.1.3 水患防治

天威诚信机房部署有漏水报警系统，一旦发生水患系统将立即报警，通知有关人员采取应急措施。

5.1.4 火灾防护

天威诚信机房内各区域均采用了烟感和温感火灾探测器，并安装了火灾自动报警系统及气体自动灭火系统，该系统具有自动和手动操作两种启动方式，并在机房内配备有专用呼吸器。天威诚信定期进行消防安全检测。

另外，根据国家的有关消防要求，天威诚信在管理区内设置了紧急出口，紧急出口设有消防门，门外部没有开启装置，仅能从内部打开。紧急出口有视频监控设备进行实时监控。当消防门被打开时，监控系统将报警通知值班人员。

5.1.5 介质存储

天威诚信建立有设备台账，设备台账包含每台设备的责任人、使用状态等信息，并定期进行设备盘点和核对，确保设备实际情况与设备台账相符。天威诚信制定了详细的介质管理制度和报废管理规定，规定包含使用权限、报废标准、销毁方法和审批流程，完整记录相关信息。天威诚信对储存产品软件和数据、归档、审计或备份信息的介质保存在安全

设施中，这些设施受到适当的物理和逻辑访问控制的保护，只允许授权人员的访问，并防止这些介质受到意外损坏（如水、火灾和电磁）。

5.1.6 废物处理

天威诚信对不再使用的敏感文件和材料在处理之前将其切成碎片，使信息无法恢复。密码设备在作废处置前根据制造商提供的方法先将其初始化再进行物理销毁。

5.1.7 异地备份

天威诚信对关键数据、审计日志数据进行异地备份，该备份地点的位置与主机房的距离不小于 10 公里，其安全级别不低于实际生产环境。

天威诚信的关键业务恢复的时间目标(RTO)为业务中断后 4 小时内恢复，恢复的数据点目标(RPO)为 15 分钟以内。天威诚信每年至少进行一 次灾难恢复演练。

5.2 操作过程控制

5.2.1 可信角色

天威诚信在提供电子认证服务过程中，将能从本质上影响证书的颁发、使用、管理和撤销等涉及密钥操作的关键岗位都应为可信角色。这些角色包括但不限于：

a) 认证系统管理员：负责对天威诚信电子认证服务系统进行系统策略配置、业务管理、系统用户管理、角色权限设置、业务授权等；
b) 系统运维员：负责对天威诚信物理环境、网络、服务器、平台软件、电子认证服务系统等基础设施进行日常监控、维护与保障；
c) 数据库管理员：负责对天威诚信的各类数据库进行日常运维、性能优化，并严格按制度执行数据备份、归档策略；
d) 系统审计员：负责对系统和网络进行审计，包括上述系统的日志记录管理与审计、审计报告的生成和审核，并对审计结果进行汇报等；

e) 密钥管理员：负责根密钥材料的安全保管，组织及参与 CA 密钥生成仪式，负责参与 CA 密钥对的创建与生存周期维护。其人员数量需符合密钥控制策略的具体要求；

f) 业务操作员：负责证书申请的受理、审核和证书制作，对证书订户的身份真实性、申请意愿及过程的真实性进行鉴证，核实证书主体与订户的一致性；

g) 客户档案管理员：负责客户证书申请及相关档案资料的归档和维护，保障客户信息资料的完整性与保密性；

h) 运营审计员：负责对客户身份查验、证书签发、客户服务等核心业务的业务流程进行独立审计，依据 CPS、CP 及相关法律法规标准，评估运营的合规性、安全性与服务能力。

i) 其他人员：对公司运营有重要影响的其他管理人员。

5.2.2 职责分离

天威诚信按职责分离原则和岗位备份原则设定各角色人数：所有涉及关键操作（密钥管理、审计、鉴证、系统管理）的角色应实现双人操作或复核机制；涉及业务连续性相关操作（运维、鉴证、审计等）的角色按工作量设置人员冗余，在任何一人缺岗时仍能实现双人操作；禁止同一人员掌握可独立完成“发起、审批、执行、审计”全流程的任何组合。

各角色禁止兼任的规则包括但不限于：

a) 认证系统管理员、系统运维员、数据库管理员、系统审计员的角色不能相互兼任；

b) 业务操作员在人工受理审核过程中，对同一个证书业务，证书信息录入和审核环节应由不同人员完成；

c) 业务操作员、客户档案管理员、运营审计员不能相互兼任；

d) 密钥管理员与认证系统管理员、系统运维员不能兼任；

e) 密钥管理员（包括密码设备操作员和持有 mofn 分割密钥的分管者）与除策略管理机构成员以外的其他可信角色均不宜兼任。

5.2.3 每个角色的识别与鉴别

所有可信角色在访问系统时应使用多因素认证机制进行身份鉴别，以验证身份的真实性：

a) 对于可信人员的物理访问，天威诚信通过门禁卡和指纹识别进行鉴别，并确定相应的权限。

b) 对于进行订户证书生命周期管理的天威诚信的可信人员，他们使用相应的数字证书访问系统，完成证书管理工作。

c) 对于系统维护人员，他们使用各自的账户和密码通过堡垒机登录系统进行维护工作。

天威诚信定期对可信角色身份鉴别过程的有效性和安全性进行审计。

5.3 人员控制

5.3.1 资格、经历和无过失要求

天威诚信对承担可信角色的工作人员的资格要求如下：

a) 具备良好的社会和工作背景；

b) 遵守国家法律、法规，无违法犯罪记录；

c) 遵守天威诚信有关安全管理的规范、规定和制度；

d) 具备所属岗位所需背景知识及专业技能；

e) 具有认真负责的工作态度和良好的从业经历；

f) 具备良好的团队合作精神。

5.3.2 背景审查程序

为了确保担任可信角色的人员能够胜任有关工作，天威诚信将按照《天威诚信可信雇员政策》对雇佣的人员先进行背景调查。背景调查符合法律法规的要求，尽可能地通过相关组织、部门进行人员背景信息的核实，并保护个人隐私。

所有的可信员工和申请调入的可信员工都必须书面同意对其进行背景调查。背景调查分为：基础调查和高级调查。

基础调查包括对工作经历、教育方面的调查。

高级调查除包含基础调查项目外，还包括对犯罪记录的调查。

调查程序包括：

a) 人力部门负责对应聘人员的个人资料予以确认。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。

b) 人力部门通过电话、网络等形式对其提供的材料的真实性进行鉴定。

c) 在背景调查中，对发现以下情形的人员，可直接拒绝其成为可信人员的资格：

1) 存在捏造事实或资料的行为；

2) 借助不可靠人员的证明；

3) 使用非法的身份证明或者学历、任职资格证明；

4) 工作中有严重不诚实的行为。

d) 人力部门完成调查后，将结果上报主管相关工作的领导进行批准。

e) 通过批准后，天威诚信与员工签订劳动合同和保密协议，以约束员工不许泄露 CA 证书服务的所有保密和敏感信息。

5.3.3 可信人员培训要求

天威诚信建有覆盖所有可信角色的分级、分岗、持续性培训体系，所有可信人员在正式上岗前完成不少于 20h 岗前培训并通过考核。天威诚信培训内容总体应包括但不限于：

a) 国家关于电子认证服务的法律法规与技术标准；

b) 岗位通用职责要求及各角色特定的工作要求；

c) 内部管理政策、制度及流程等；

d) PKI 和密码技术基础知识；

e) CP、CPS 及相关标准和程序；

f) 安全管理策略和机制；

g) 订户身份查验和审核策略和流程；

h) 运营体系构成；

i) 技术体系构成；

j) 灾难恢复和业务连续性管理。

5.3.4 再培训周期和要求

所有可信角色每年应至少进行一次培训，每人每年培训时长不少于 20h，培训内容应包括最新的法律法规、技术进展、安全威胁等。天威诚信对所有可信角色进行持续培训和考核，培训和考核内容包括理论知识、操作技能、安全意识等，要求所有可信角色需通过考核。

5.3.5 工作岗位轮换周期和顺序

天威诚信在职人员的工作岗位轮换周期和顺序将依据内部工作安排决定。

5.3.6 未授权行为的处罚

天威诚信建立并维护一套管理办法，对未授权行为进行适当的处罚，包括解除或终止劳动合同、调离工作岗位、罚款、批评教育等方式。这些处罚行为符合法律法规的要求。

5.3.7 独立合约人的要求

天威诚信目前未聘用外部独立合约人从事认证相关的工作。

5.3.8 提供给员工的文档

提供给员工的文档通常包括证书策略、电子认证业务规则、员工手册、岗位职责说明书、工作流程和规范等。

5.4 审计日志程序

5.4.1 记录事件的类型

天威诚信持续、完整地记录关键操作与事件，包括但不限于：

a) 根证书密钥操作：包括密钥生成、备份、存储、恢复、归档、销毁，以及密码设备的启用、停用、转移和销毁等；

b) 系统访问行为：包括所有对系统的访问企图，包括成功的和失败的登录、退出、权限使用行为等；

c) 系统操作与变更：包括对系统的各种关键查询、修改、删除等操作，系统组件的安装、升级、维修，人员，以及敏感信息的获取与取阅等；

d) 网络安全事件：包括防火墙、路由器、入侵检测安全设备记录的告警信息，以及针对被攻击事件识别与相应处理过程、结果等；

e) 证书生存周期关键过程：包括记录证书申请、审核、签发、更新、变更、撤销、冻结、恢复等操作，CRL 的签发与发布等，所有操作的通过或拒绝结果均应明确记录；

f) 机房门禁控制等物理环境事件：包括业务人员、运维人员、外部人员等在不同安全区域的进出记录等。

日志记录一般包括每个事件记录的时间、类型、内容、操作人、作用对象及结果。对系统的关键操作由操作人员进行电子签名。

5.4.2 处理日志的周期

天威诚信至少每月对上述记录进行一次审计，核实系统和操作人员的合规性，识别潜在的违规或可疑行为，记录审查的结果，并基于结果采取改进措施。

5.4.3 审计日志保存期限

天威诚信妥善保存电子认证服务的审计日志，与证书相关的审计日志，在证书失效后至少保留 5 年。

5.4.4 审计日志的保护

天威诚信的系统日志备份到日志服务器，手工电子记录备份到 SVN，手工纸质记录归档保存到管理区内。

天威诚信采取了物理和逻辑的访问控制方法，以确保只有授权人员才能接近这些审查记录，严禁未授权的访问、阅读、修改和删除等操作。

天威诚信对电子认证系统内部的操作，由操作人员对事件进行电子签名。

5.4.5 审计日志备份程序

天威诚信的系统日志实时同步到日志服务器，并且每天备份到异地。

天威诚信保存在 SVN 的手工电子记录，实行工作时间内每 15 分钟增量备份、每天夜间全量备份的备份策略。

5.4.6 审计收集系统

对于电子审计信息，天威诚信设置了专门的审计信息存储系统，自动或人工完成审计信息的收集。对于纸质的审计信息，则有专门的文件柜来实现审计信息的收集。

5.4.7 对导致事件主体的通知

当天威诚信发现被攻击时，将记录攻击者的行为，在法律许可的范围内追溯攻击者，保留采取相应对策措施的权利。天威诚信有权决定是否对事件相关实体进行通知。

5.4.8 脆弱性评估

天威诚信定期指定专人定期评估审计报告，基于审计结果每年对系统、物理场地、运营管理等方面进行安全脆弱性评估，并根据评估报告采取措施，以降低运营风险。审计报告及相关记录保存期限至少到相关证书失效五年后。天威诚信建立了对审计过程中发现的异常操作的响应处理程序，内容包括对未授权操作的撤销与纠正，对责任人的处理措施，以及向主管部门报告的安全事件通报机制。

5.5 记录归档

5.5.1 归档记录的类型

天威诚信日志记录归档范围包括所有审计日志、证书申请信息、支持证书申请的文档、订户意愿表达的证明等。归档记录的类型，包括但不限于：

a) 证书申请材料和订户意愿记录；

b) 所有审计日志；

c) 密码设备全生存周期管理记录；

d) 密码设备的日常操作与使用记录；

e) 根证书或密钥生存周期管理相关的全部记录；

f) 证书认证系统运行日志；

g) 已识别的安全事件及处置记录；

h) 证书认证系统关键操作日志；

i) 电子认证服务过程中其他操作记录。

此外，还对以下资料进行归档：

j) 与证书系统安全性相关的文档；

k) 与证书申请和证书的鉴别和验证、颁发和撤销相关的文档；

l) CP 和 CPS；

m) 员工资料，包括但不限于背景调查、录用、培训等资料；

n) 各类外部、内部审计评估报告。

5.5.2 归档记录的保存期限

对于不同的归档记录，其保留期限是不同的。对于系统操作事件和系统安全事件记录，其归档应保留到完成安全脆弱性评估或一致性审计。

a) 对 CA 证书和密钥生命周期内的管理事件的归档，其保留期限不少于 CA 证书和密钥生命周期。

b) 订户相关档案、系统日志和审计记录的归档保留期限不少于证书失效后 5 年，以符合审计和法律追溯要求。

c) CA 证书和密钥的归档在 CA 证书和密钥生命周期之外，额外保留 5 年。

d) 其它记录保留 1 年。

已超过法定及政策要求规定保存期限档案，天威诚信在完成内部审批程序后，按相关规定进行销毁。

5.5.3 归档文件的保护

天威诚信对各种电子、纸质形式的归档文件，都有安全的物理和逻辑保护措施和严格的管理程序，确保归档了的文件不会被损坏，防止非授权的访问、修改、删除或其它的篡改行为：

a) 对于所有的电子归档记录，采取技术手段保证数据的完整性，防止被非法修改或替换；
b) 归档记录（包括电子或物理媒体）存放在安全的物理环境中，保护其不受未经授权的访问、篡改或破坏；
c) 建立电子归档记录的备份措施，防止数据丢失；
d) 安全管理人员定期检查归档记录的管理情况；
e) 在确认内容真实、完整、正确的前提下，天威诚信将纸质档案扫描为电子格式，并采用技术手段进行完整性保护后，按电子档案的要求进行归档管理。

5.5.4 归档文件的备份程序

对于系统生成的电子归档记录，每天备份到异地存放；对于手工生成的电子记录，归档到 SVN，SVN 数据实行工作时间内每 15 分钟增量备份、每天夜间全量备份的备份策略。

对于书面的归档资料，不需要进行备份，但需要采取严格的措施保证其安全性，防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

天威诚信的日志未采用时间戳技术。

5.5.6 归档收集系统

对于系统生成的电子记录，实时同步到日志服务器，并且每天备份到异地。

对于手工生成的电子记录，由 SVN 服务器完成收集备份工作。

对于书面的归档资料，收集归档到管理区内。

5.5.7 获得和检验归档信息的程序

天威诚信采取了物理和逻辑的访问控制方法，以确保只有授权人员才能接近这些归档信息，严禁未授权的访问、阅读、修改和删除等操作。

5.6 电子认证服务机构密钥更替

当 CA 密钥对的累计寿命超过 6.3.2 中规定的最大生命期，天威诚信将启动密钥更新流程，替换已经过期的 CA 密钥对。天威诚信密钥变更按如下方式进行：

a) 一个上级 CA 将在其私钥到期时间小于下级 CA 的生命期之前停止签发新的下级 CA 证书（“停止签发日期”）；如发现密钥泄露或存在安全隐患，天威诚信将立即启动密钥更替程序，并同步执行旧密钥的撤销及事件通告。

b) 产生新的密钥对，签发新的上级 CA 证书；在颁发或更换根证书时，天威诚信在安全可靠的环境中生成新密钥对，见 6.1。除证书续期外，不同证书不得使用相同的密钥对。

c) 在“停止签发证书的日期”之后，对于批准的下级 CA 或最终用户证书请求，将采用新的 CA 密钥签发证书，天威诚信将新的 CA 公钥证书发布给证书订户和依赖方。

d) 上级 CA 继续利用原来的 CA 私钥签发 CRL 直到利用原私钥签发的最后的证书过期为止。

e) 在完成签名密钥更替后，天威诚信按 GB/T 25056 中 8.2.4.3 规定的方式，销毁旧私钥及其备份，并保留相关操作记录。

f) 发现密钥泄露或存在安全隐患，天威诚信将立即启动密钥更替程序，按 5.7.3 处理。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

天威诚信已制定完整的电子认证服务的连续性计划与灾难恢复应急预案，规定了相应的事故和损害处理程序，这些应急处理方案包括：

a) 认证系统应急方案：包括重建安全运行环境的流程，生成受影响并被撤销的证书列表，对订户密钥的处理方式，以及重新向订户提供实体公钥证书的要求和流程；

b) 密钥应急处理方案：根密钥损害的恢复过程：包括重建安全环境的流程，为订户重新签发公钥证书，向订户提供新的公钥证书的流程。

c) 其他关键资产恢复方案：物理设施、计算资源、网络环境、软件或数据，以及其他密钥数据的恢复方案。

d) 每年进行一次根私钥应急处理流程应急演练。

e) 天威诚信定期验证备份的设备、数据可用性，包括备份恢复测试和功能验证，每年至少进行一次灾难恢复演练。

5.7.2 计算机资源、软件和/或数据的损坏

天威诚信对业务系统及其他重要系统的资源、软件和/或数据进行了备份，并制定了相应的应急处理流程，当发生网络故障、系统、软件被破坏、数据库故障等现象或因不可抗力造成灾难时，天威诚信将按照灾难恢复计划实施恢复。

5.7.3 实体私钥损害处理程序

对于实体证书私钥的损害，天威诚信有如下处理要求和程序：

a) 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，并立即访问天威诚信的证书服务网站撤销其证书，或者立即通过电话、电子邮件的方式通知天威诚信撤销其证书。天威诚信按 4.9 发布证书撤销信息。

b) 当天威诚信发现证书订户的实体证书私钥受到损害时，天威诚信将立即撤销证书，并通知证书订户，订户必须立即停止使用其私钥。天威诚信按 4.9 发布证书撤销信息。

c) 当天威诚信的 CA 证书（含根证书）出现私钥损害时，天威诚信将立即撤销该 CA 证书并及时通过广达的途径通知依赖方，然后生成新的 CA 密钥对、签发新的 CA 证书。

5.7.4 灾难后的业务存续能力

天威诚信在异地建立了容灾系统，一旦物理场地出现了重大灾难，天威诚信能够根据业务连续性计划在最短时间内恢复业务。

5.8 电子认证服务机构的终止

当天威诚信因为技术性原因或商业原因需要终止服务时，将严格按照《中华人民共和国电子签名法》及相关法规中对认证机构终止业务的规定要求实施处理流程和相关通告。

天威诚信承诺至少完成以下步骤：

a) 起草并发布终止声明，至少提前九十日通知与证书订户、依赖方等相关实体，至少提前六十日向主管部门报告；
b) 确定具体资质的电子认证服务业务承接单位，并签署承接协议，明确约定承接机构的工作范围与责任；
c) 向承接方移交密钥及相关关键数据，协调承接单位启动相关运营工作；
d) 停止证书状态服务并归档相关数据；
e) 停止认证中心的服务并归档相关数据；
f) 停止密码设备并归档相关密钥数据；
g) 及时撤销业务管理员和业务操作员的操作权限；
h) 对所有存档文件记录进行整理和封存；
i) 对所有敏感文档和数据进行安全处理和封存；
j) 清除主机和密码硬件设备中的敏感数据；
k) 其他涉及 CA 运营的数据、密钥安全的操作。

5.9 重大事项报告

天威诚信建立了处理重大事件的管理与报告机制，包括事件发生后 24 小时内上报公司管理层、完成内部审批后立即上报主管部门等规定。

重大事件包括但不限于：

a) 证书认证系统迁移或改造：包括系统软件、网络、部署的重大改变。符合以下任意之一：
    1) 机房迁移，或机房内服务区、管理区或核心区划设范围改变；
    2) 变更电子签名认证证书签发逻辑；
    3) 新增远程证书注册子系统；

4) 新增、更改或者删除用于签发电子签名认证证书的证书链；

5) 其他对电子认证服务安全、用户资料安全有影响的改变。

b) 重大安全事故：包括电子认证服务系统遭受黑客攻击、病毒入侵、数据泄露等，导致系统无法正常运行或数据安全性受到严重威胁的情形。符合以下任意之一：

1) 证书签发及验证服务连续停机时间超过 24h；

2) 发生根证书密钥等关键数据泄露；

3) 持续或较大范围未经授权的私钥访问记录或其他异常活动；

4) 系统日志持续或较大范围显示异常操作（如非授权时间或网络地址访问敏感功能）。

c) 订户信息泄露事件：包括订户身份信息、证书申请资料等敏感数据被泄露等。符合以下任意之一：

1) 个人信息泄露事件影响范围较广，造成一定的经济损失或客户投诉；

2) 数据丢失导致无法恢复证书状态信息。

d) 合规性事件：包括不符合相关法律法规、标准或监管要求的情形。符合以下任意之一：

1) 涉及电子认证服务的司法判定；

2) 收到行政部门违规通知或处罚决定。

e) 人力资源类事件：包括一个月内核心管理层集体离职、大规模劳动纠纷、重大职场安全事件等。符合以下任意之一：

1) 涉及 2 名及以上管理层人员或 10%以上可信人员的离职；

2) 劳动纠纷参与人数超过员工总数 10%，且经法院或仲裁机构生效裁决确认由 CA 承担法律责任。

6. 认证系统技术安全控制

6.1 技术安全管理制度要求

天威诚信建立并实施了覆盖密钥管理、系统开发、网络防护等领域的技术安全管理制度，并定期接受安全策略委员会的评审，频率不低于每年一次。

6.2 密钥对的生成和安装

6.2.1 CA 密钥对的生成和安装

a) 天威诚信在物理隔离的安全环境中采用通过国家密码主管部门检测认证的硬件密码设备生成 CA 签名密钥对、及认证系统相关管理密钥；
b) 生成、备份、恢复、销毁过程实施 5 选 3 多人控制机制，操作将在安全策略委员会授权下进行，操作人员均接受过相关培训，根密钥操作过程通过录音录像方式全程记录，保存期限不少于操作完成后十年。

6.2.2 订户密钥对的生成和交付

订户签名密钥对的生成、交付及控制方式符合以下要求之一：

a) 由订户持有的符合国家安全标准的密码模块产生和存储，具体包含两种情形：
   1）订户在本地安全环境中使用通过商用密码检测认证的密码模块自行生成并保存签名密钥对，不存在密钥对交付的情况；
   2）天威诚信使用通过商用密码检测认证的密码模块代订户生成密钥对后，将载有私钥的密码模块通过安全可靠的方式（如面对面）交付订户自行保管。
   天威诚信向订户充分告知签名密钥保存、使用的要求与安全风险。
b) 由天威诚信产生、保存订户签名密钥对，并通过技术措施确保订户对签名私钥的独占控制权，具体表现在：天威诚信使用通过商用密码检测认证的密码模块生成订户签名密钥并保存在天威诚信，并通过身份校验、操作审计等技术措施确保订户私钥的安全以及订户对签名私钥的独占控制权。
c) 采用通过主管部门认可的其他创新性保护方案（如适用）。

天威诚信完整记录所有与订户签名私钥相关的操作日志，包括时间、方式、操作人员等信息，操作日志保存期限不少于证书失效后五年。

6.2.3 公钥传送给证书签发机关

订户或订户通过第三方，将 PKCS#10 格式的证书签名请求信息或其它数字签名的文件包，以电子文本的方式将公钥提交给天威诚信签发证书。当需要通过网络传送时将使用安全协议或其他安全加密方式。

6.2.4 CA 公钥传送给依赖方

天威诚信的主 CA 公钥，通过如下方式之一传输给依赖方：

a) 依赖方访问天威诚信的证书服务站点下载 CA 证书，该站点受到服务器证书的保护；

b) 天威诚信或其合作伙伴到依赖方业务系统现场将 CA 证书安装到业务系统中；

c) 天威诚信或其合作伙伴分发给依赖方的软件中绑定、包含有 CA 证书。

对于天威诚信的其他 CA 公钥，除了上面所述的方式传输给依赖方外，当证书订户获取证书时天威诚信通过 PKCS#7 格式将除根证书外的证书链传递给订户。

6.2.5 密钥的长度

天威诚信 CA 和订户密钥对包含两种：2048 位 RSA 密钥和 256 位 SM2 密钥。

6.2.6 公钥参数的生成和质量检查

公钥参数使用通过商用密码检测认证的密码模块生成，并遵从这些设备的生成规范和标准。

对于参数质量的检查，由于使用通过商用密码检测认证的密码模块生成和存储密钥，已经具备足够的安全等级要求。

6.2.7 密钥使用目的

根 CA 的密钥用于签发运营 CA 的证书及 CRL，运营 CA 的密钥用于签发订户证书和 CRL。订户的签名密钥用于提供电子签名、抗抵赖、以及信息完整性检查等目的。

6.3 私钥保护和密码模块工程控制

6.3.1 CA 私钥保护和密码模块工程控制

天威诚信 CA 私钥保护使用通过商用密码检测认证的密码产品，应符合 GB/T 37092-2018《信息安全技术 密码模块安全要求》第 5 章的要求。

天威诚信 CA 私钥实施严格的分割保护机制，实现单人无法获取完整私钥。

天威诚信 CA 证书私钥备份由密钥管理员分别保存在有防盗措施的安全场所。

天威诚信 CA 操作私钥记录保存期限不少于操作完成后十年。

6.3.2 订户私钥保护和密码模块工程控制

6.3.2.1 订户自主持有签名私钥

订户证书的密钥应使用通过商用密码检测认证的密码模块生成和存储。

天威诚信在订户协议中要求订户采取预防措施防止私钥及其激活数据的丢失、泄露、更改或未经授权的使用。

6.3.2.2 CA 受托保管订户签名私钥

天威诚信可接受订户委托，提供签名私钥托管保管服务。天威诚信受托保管订户签名私钥的：

a) 采用基于云计算的电子签名模式，满足如下要求：

订户签名私钥使用通过商用密码检测认证的密码模块生成，私钥明文永不脱离密码模块环境，签名运算在密码模块内部完成；

订户通过身份认证发起签名授权，天威诚信接收并验证确认授权的有效性后，调用对应私钥完成签名运算。

b) 天威诚信通过技术与管理双重措施保障托管私钥安全，并建立常态化安全评估机制；

c) 每次签名私钥调用必须获得订户的明确授权，授权记录完整保存；

d) 电子签名模式和控制措施符合相关标准或采用经主管部门认可的其他方式。

此外，天威诚信向订户提供关于私钥及激活数据安全使用的指导与建议，并定期对私钥保护措施进行安全评估。

6.3.3 私钥备份

天威诚信对根私钥和 CA 私钥进行备份，可分为两种，一是按照密码设备制造商提供的操作规范生成备份密文文件和备份恢复权限介质并保存到屏蔽机房的保险柜；一是按照密码设备制造商提供的操作规范生成克隆设备和分管密钥介质并存放在屏蔽机房。

对于订户证书，如果存放证书私钥的密码模块允许私钥备份，天威诚信建议订户对私钥进行备份，并对备份的私钥采用口令或其他访问控制机制保护，防止非授权的修改或泄露。

6.3.4 私钥归档

当天威诚信的 CA 密钥对超过使用期后，这些 CA 密钥对将归档保存至少 5 年。归档 CA 密钥对保存在 6.2.1 所述的硬件密码模块中，并且天威诚信的密钥管理策略和流程阻止归档 CA 密钥对返回到产品系统中。对归档私钥到了归档保存期，天威诚信将按 6.2.6 销毁。

天威诚信不对订户用于签名的证书私钥进行归档。

6.3.5 私钥导入、导出密码模块

天威诚信 CA 密钥对在硬件密码模块上生成，保存和使用。此外，为了实现恢复，天威诚信按照密码设备制造商提供的操作规范对 CA 密钥进行备份。另外天威诚信还有严格的密钥管理流程对 CA 密钥对复制进行控制。所有这些有效防止了 CA 私钥的丢失、失窃、修改、非授权的泄露、非授权的使用等。

对于订户证书，若使用的密码模块支持私钥的导出、导入，则天威诚信要求订户对导出、导入的私钥必须使用足够安全的口令进行保护，且订户需要确保导出的私钥不被丢失、失窃、修改、非授权的泄露、非授权的使用等。

6.3.6 销毁私钥的方法

在天威诚信私钥生命周期结束后，天威诚信将 CA 私钥继续保存在一个备份硬件密码模块中，并进行归档，其他的 CA 私钥备份被安全销毁。归档的 CA 私钥在其归档期限结束后，需在多名可信人员参与的情况下安全销毁。CA 私钥的销毁将确保 CA 私钥从硬件密码模块中彻底删除，不留有任何残余信息。

对于订户证书私钥，若不再使用，应该将私钥销毁，从而避免丢失、偷窃、泄露或非授权使用。若私钥对应的公钥证书被撤销、到期作废后，还需要用于信息解密的，最终用户应该妥善保存一定期限，以便于解开加密信息。

6.4 密钥对管理的其他方面

6.4.1 公钥归档

天威诚信对所签发的订户证书在其过期 3 个月后对证书公钥进行归档，证书存放在数据库中并进行异地备份。

6.4.2 证书操作期和密钥对使用期限

天威诚信根 CA 证书的最长有效期不超过 30 年，其他 CA 证书的最长有效期不超过 25 年，订户证书的最长有效期不超过 5 年 3 个月。

公钥和私钥的使用期限与证书的有效期相关但却有所不同。无论是订户证书还是 CA 证书，证书到期后，其私钥不可用于电子签名。

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。但是，为了保证在证书有效期内签名的信息可以验证，公钥的使用期限可以在证书的有效期限以外。

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。但是，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。

6.5 激活数据

6.5.1 激活数据的产生和安装

天威诚信 CA 私钥的激活数据按照密码设备制造商提供的操作规范，由密码设备产生。

如果订户证书私钥的激活数据是口令，建议这些口令：

a) 至少 8 位字符或数字；

b) 至少包含一个字符和一个数字；

c) 不能包含很多相同的字符；

d) 不能和操作员的名字相同；

e) 不能包含订户名信息中的较长的子字符串。

天威诚信还建议订户使用双因素机制（如硬件设备结合密码，生物识别设备结合密码等）来控制私钥的激活。

6.5.2 激活数据的保护

对于 CA 私钥的激活数据，天威诚信按照可靠的方式由可信人员掌管，存储在天威诚信屏蔽机房保险柜中。

订户应妥善保管好其激活数据，防止泄露或窃取。

6.6 计算机安全控制

6.6.1 特别的计算机安全技术要求

证书认证系统的信息安全管理，按照 GB/T 25056-2018《证书认证系统密码及其相关安全技术规范》、工业和信息化部公布的《电子认证服务管理办法》，参照 ISO27001 信

息安全管理体系要求，以及其他相关的信息安全标准，制定出全面、完善的安全管理策略和制度，在运营中予以实施、审查和记录。

天威诚信至少每半年检查一次系统升级补丁，记录系统升级审批及实施过程；对无官方补丁支持的系统，制定网络隔离、功能限制等加强防护措施和系统更替计划。

天威诚信对所有服务器和操作终端安装杀毒软件，杀毒软件可自动更新病毒库；天威诚信每周对服务器进行病毒扫描。

6.6.2 计算机安全评估

天威诚信的证书认证系统及其运营环境通过了国家密码管理局和工信部的审查，获得了相应资质。

6.7 生存周期安全控制

6.7.1 系统开发控制

天威诚信建立并实施符合 GB/T 25056-2018《证书认证系统密码及其相关安全技术规范》相关要求的生存周期安全控制体系。

天威诚信采用的 CA 软件是通过商用密码检测认证的产品。天威诚信通过内部变更控制流程来控制证书认证系统的上线工作，并要求运维人员严格按照审批和上线流程执行，以保证系统的安全性和可用性：

a) 系统软件必须在测试环境测试成功后，再申请部署于生产环境；
b) 申请部署时需要提供变更说明、测试报告、部署说明等文档；
c) 部署上线前根据规范要求进行审批；
d) 变更部署前进行有效的在线备份；
e) 变更部署后应立即进行测试，通过测试后方可对外服务。

6.7.2 安全管理控制

天威诚信已制定了各种安全策略、管理制度与流程对 CA 运营系统进行安全管理。

6.7.3 生命期的安全控制

天威诚信通过内部变更控制流程来控制证书认证系统的研发和上线工作，确保该系统安全可靠。

6.8 网络的安全控制

天威诚信的网络安全控制体系符合 GB/T 25056-2018《证书认证系统密码及其相关安全技术规范》相关要求，包括但不限于：

a) 网络结构满足 GB/T 25056—2018 附录 A 中规定形式的一种；
b) 对所有 Web 服务配置防火墙、Web 应用防火墙、入侵检测系统和内容过滤等网络安全防护措施；
c) 建立并维护网络拓扑图，包含所有网络设备、连接关系和安全边界，定期更新，与机房实际情况保持一致；
d) 网络访问控制：
   1) 建立针对证书签发子系统及数据库的访问白名单机制，仅授权证书注册子系统的必要功能模块及必要的管理设备进行访问；
   2) 建立针对证书注册子系统和数据库的访问白名单机制。
e) 网络监控：
   1) 定期对系统日志进行分析；
   2) 分析内容包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件。

6.9 时间戳

天威诚信部署了时间戳服务该服务适用于电子合同、数据存证等需要证明电子数据在某一时间点前已存在且未被篡改的场景。天威诚信通过标准接口方式为用户提供服务。

天威诚信时间戳服务符合 RFC 3161 等国内外标准，并且使用国家可信标准时间；天威诚信对该服务实施严格的访问控制和操作审计，保障服务的机密性、完整性和不可否认性。

7. 证书、CRL 和 OCSP

7.1 证书

天威诚信签发的电子签名认证证书符合 GB/T 20518-2018《信息安全技术公钥基础设施 数字证书格式》中的要求（详见附录“电子签名认证证书内容”），至少包括以下内容：

a) 支持的数字证书格式版本号；
b) 密码算法对象标识符；
c) 电子认证服务机构和订户的名称；
d) 证书策略对象标识符；
e) 证书序列号；
f) 证书有效期；
g) 证书持有人的电子签名验证数据；
h) 电子认证服务机构的电子签名。

7.2 CRL

天威诚信认证系统签发的 CRL 符合 GB/T 20518-2018《信息安全技术公钥基础设施 数字证书格式》中的要求。

7.3 OCSP

天威诚信认证系统可根据订户需要提供该项服务。天威诚信在线证书状态服务符合 GB/T 19713-2005《信息技术 安全技术 公钥基础设施 在线证书状态协议》第 7 章的要求。

8. 认证机构审计和其他评估

8.1 审计评估制度

天威诚信已制定《电子认证服务审计评估管理制度》，建立常态化监督与持续改进机制，确保电子认证服务合规运行。根据相关制度开展如下认证业务审计和全面符合性评估工作。

除了内部审计和评估外，天威诚信还可委托第三方审计机构实施质量管理体系和信息安全管理体系审计。

内部审计和评估，由天威诚信内部审计评估小组执行；外部审计，由天威诚信委托具备资质的第三方机构。

内部审计人员与天威诚信的系统管理员、业务管理员、业务操作员的工作岗位不能重叠；外部审计机构和天威诚信之间是相互独立的关系，双方无任何足以影响评估客观性的利害关系。

8.2 认证业务审计

天威诚信采用风险导向抽样审计法开展认证业务审计，重点关注高风险业务领域和高价值客户项目；认证业务审计每半年至少开展一次。

审计内容包括但不限于证书申请、续期、密钥变更、更新、撤销、冻结等业务中订户告知、身份查验、意愿记录、协议签署、资料保存的合规性。

天威诚信采用抽样审计方式，按照审计周期内证书签发量从高到低排序，审计覆盖的项目累计业务量不低于总签发量的 80%。

对于天威诚信内部审计结果中发现的问题，由审计评估小组负责监督相关责任部门的改进情况；对于由外部审计机构评估发现的问题，天威诚信按照其审计报告进行整改。

8.3 全面符合性评估

天威诚信每年至少开展一次全面符合性评估，对电子认证服务的整体合规性进行全面审查，并在 1 月底前将上一年度符合性评估报告报送主管部门。

全面符合性评估内容包括但不限于年度电子认证服务开展情况、电子认证服务许可条件符合性情况以及认证规则和证书策略符合性情况等。

全面符合性评估采用抽样方式的，抽样率不低于 8.2 规定的认证业务审计的抽样率。

对于天威诚信内部审计结果中发现的问题，由审计评估小组负责监督相关责任部门的改进情况；对于由外部审计机构评估发现的问题，天威诚信按照其审计报告进行整改。

9. 法律责任和其他业务条款

9.1 费用

天威诚信已开展服务成本核算并指定价格策略。

天威诚信可通过公司官网、证书管理门户、与订户或依赖方或合作伙伴等签署的合同或协议、电子邮箱、客服电话、现场告示等方式公布与证书相关服务的收费标准。

9.1.1 证书签发或更新费用

天威诚信可就电子签名认证证书的签发及更新收取费用，具体收费标准根据市场和管理部门的规定自行决定。在收费标准范围内，即不超过收费标准的情况下，天威诚信有权根据市场状况，针对不同订户群体推出不同的收费策略或优惠措施。

如果天威诚信签署的协议中指明的价格和天威诚信公布的价格不一致，以协议中的价格为准。

9.1.2 证书访问费用

天威诚信可就访问其证书数据库收取合理费用。

9.1.3 证书撤销的费用

天威诚信就证书撤销不收取任何费用。

天威诚信有可能就其他增值撤销服务收取费用。

9.1.4 状态信息访问费用

天威诚信就通过证书撤销列表（CRL）查询已签发证书的有效状态不收取任何费用。天威诚信有可能根据需要将 OCSP 服务作为增值服务收取费用。

天威诚信有可能就提供定制证书撤销列表、在线证书状态协议（OCSP）服务或其他增值状态信息服务收取费用。

9.1.5 其他服务费用

天威诚信可能向订户提供证书存储介质及其他如下相关服务，天威诚信将在与订户或者其他实体签署的协议中指明该项价格、或在受理证书申请前向订户告知有关服务费用。

a) 电子签名的费用；

b) 签名验证的费用；

c) 签名验证报告的费用；

d) 其他服务的费用。

9.1.6 退款策略

如果因天威诚信违反本 CP 和 CPS 规定的责任及重大义务，导致订户合同无法履行、订户证书无法使用的，天威诚信可根据申请将已支付但未使用服务的相关费用返还给订户、并撤销相应的证书。

9.2 财务责任

9.2.1 保险范围

天威诚信根据业务发展情况及国内保险种类自行决定证书投保策略。

9.2.2 资金保障

天威诚信预留与业务规模相适配的现金资产以确保具备维持业务运作、履行相关责任及/或承担财务赔偿责任的能力。保障资金额度不低于上一年度电子认证服务营业收入的 1.5%。

保障资金来自于天威诚信自有资金；天威诚信开立保障资金专户，专门用来存储及管理备用资金。

9.2.3 对最终实体的保险或担保

天威诚信提供的电子认证服务保障的最终实体是指证书订户及证书依赖方。

最终实体可依据生效的法律文书（如判决书、裁决书等）要求天威诚信承担相应的赔偿责任（法定或约定免责的除外）。

最终实体欲就在证书有效期内产生的损失向天威诚信提出索赔的，应在知道或应当知道损失发生之日起三年内书面提出索赔申请；超出三年的，该索赔无效。

天威诚信按照本 CP 和 CPS 第 9.9 节规定对最终实体承担有限赔偿责任。

9.3 业务信息保密

9.3.1 保密信息范围

天威诚信将以下信息视为保密信息：

a) 订户的签名私钥。

b) 用于访问私钥或接入证书认证系统的激活数据。

c) 审计记录和档案记录，包括本地日志、服务器日志、归档日志信息等，这些信息只有安全审计员和业务管理员可以查看；除法律要求，不可在公司外部发布。

d) 其他由天威诚信保存的个人和公司信息应视为保密，除法律要求，不可公布。

9.3.2 不属于保密的信息

天威诚信将以下信息视为不保密信息：

a) 由天威诚信签发的证书和 CRL 中载明的信息。

b) 由天威诚信支持、CPS 识别的证书策略中的信息。

c) 天威诚信许可的证书订户及依赖方可使用的、在天威诚信网站公开发布的信息。

d) 信息主体同意公开的信息。

e) 依据法律、行政法规规定可以公开的信息。

f) 可以通过公共、公开渠道获取的信息。

9.3.3 保护保密信息的责任

天威诚信有妥善保管与保护本 CP 和 CPS 第 9.3.1 节中规定的保密信息的责任与义务。

天威诚信、订户以及与认证业务相关的参与方，均应按照本 CP 和 CPS 的规定，承担保护保密信息的责任，采取有效技术措施和管理程序对保密 信息进行保护。

保密信息的所有者要求天威诚信公开或披露其专属保密信息的，天威诚信可依其申请予以办理；同时，天威诚信有权要求该保密信息的所有者就签署披露事项出具书面授权文件，以确认其公开或者披露的真实意思表示。因该等披露行为引发的全部损失及赔偿责任，由保密信息的所有者自行承担，天威诚信不就相关损失承担任何赔偿或补偿责任。

天威诚信因法律、法规强制性规定，或者人民法院以及其他有权国家机关依照法定程序要求，提供本 CP 和 CPS 中规定的保密信息的，该等提供行为不构成违反保密义务，天威诚信就此不承担任何法律责任。

9.4 个人隐私保护

9.4.1 个人隐私保护方案

天威诚信在开展个人信息处理活动时，严格依照官网（https://www.itrus.com.cn）发布的《隐私政策》执行，并遵守中华人民共和国个人信息保护及隐私保护相关法律法规。同时，天威诚信将督促全体从业人员严格遵从内部管理制度和业务操作规范。

本 CP 和 CPS 未尽事宜以天威诚信官网公布的《隐私政策》为准。

9.4.2 作为隐私处理的信息

作为隐私处理的信息包括订户提交的、但不在证书中显示的符合法律法规有关隐私信息定义的个人信息。

9.4.3 不被视为隐私的信息

不被视为隐私的信息包括，证书、证书撤销列表（CRL）以及其中包含的个人信息。

9.4.4 保护隐私的责任

天威诚信、订户以及与认证业务相关的参与方，均应按照本 CP 和 CPS 的规定履行隐私保护义务并承担相应责任。如遇法律法规强制性规定，或主管部门、人民法院或其他有

权国家机关依照法定程序要求提供隐私信息的情形，天威诚信依法配合提供的，无需就此承担任何法律责任。

9.4.5 隐私信息的处理

订户在向天威诚信申请证书的过程中，已同意天威诚信为提供证书服务之必要，对其提供的个人信息及隐私信息依法开展处理活动。

天威诚信将采取合理、适当的技术措施于管理手段保障证书订户个人隐私及已存储隐私信息的安全。

天威诚信确需超出约定范围及用途使用证书订户隐私信息的，应事先告知证书订户并取得其明确同意与授权；未取得前述同意及授权的，不得向任何第三方披露订户隐私信息。

9.4.6 依法律或行政程序的信息披露

依据法律、行政法规、规章及其他具有法律效力的规范性文件规定，因司法执行、法律授权的行政执行等法定事由，天威诚信可能需要向执法机关、行政执法机关提供订户有关隐私信息，该等披露行为可依法在不另行通知订户的情况下实施。即使出现前述情形，天威诚信仍将在法定范围内最大限度保护订户的隐私信息。

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

天威诚信对其签发的证书，以及通过官方网站及其他各类渠道对外发布、提供的全部软件、文档、数据与信息等，享有并保留完整知识产权，包括但不限于所有权、署名权、著作权、专利权、利益分享权及其他合法权利。

天威诚信在提供服务过程中使用的证书、商标、专有标识及其他知识产权，均归天威诚信所有；天威诚信对其签发的证书、证书撤销列表（CRL）及其中体现的信息，以及本CP和CPS与相关的运营管理工作文件，均享有完整知识产权。

证书订户和/或申请人保留其在天威诚信为其签发的证书中所含的商标、服务标志、商品名或甄别名中所享有的知识产权。

9.6 陈述与担保

9.6.1 CA的陈述与担保

天威诚信作为电子认证服务机构（CA），就其向订户、依赖方提供证书签发及管理服务，做出如下陈述与保证：

a) 遵守《中华人民共和国电子签名法》及相关法律法规，接受行业主管部门的监督与指导，并依据本CP和CPS对签发的证书承担相应的法律责任；

b) 已建立并有效运行证书服务所必需的业务规范与管理制度体系；

c) 向订户签发的证书符合本CP和CPS的各项实质性要求；

d) 将向证书订户通报已知的且足以实质影响订户证书的有效性、可靠性的事件；

e) 按照本CP和CPS的规定及时实施撤销证书操作；

f) 对订户提出的证书申请、证书及密钥更新、证书撤销等服务请求，无论批准或驳回，均及时向订户进行告知。

天威诚信保证已采取合理必要的核验措施，确保证书所载订户信息在证书签发时真实、准确。

天威诚信不就证书的具体使用范围及适当性做出评估与保证，订户、依赖方应分别依照订户协议和依赖方协议的约定在许可范围内使用证书。天威诚信不介入订户、依赖方使用证书的具体行为，对因订户、依赖方自身过错使用证书所造成的全部损失不承担损害赔偿责任。

9.6.2 订户的陈述与担保

作为订户协议的有效组成部分，订户就申请、接收、使用证书事宜，向天威诚信作出如下陈述与保证，该等承诺与保证为订户获取证书的前提条件。

a) 证书申请时

1) 订户已充分阅读、理解并同意订户协议全部内容，申请证书系订户的真实意思表示，或为开展已获得合法授权的相关事务；
2) 订户在证书申请过程中做出的全部陈述、提交的信息与资料均真实、完整、准确、有效，其中证书所载须经验证的信息符合真实性要求；前述陈述或信息发生变化的，订户应立即通知天威诚信；
3) 订户可自行申请证书，也可委托他人代为申请；委托他人申请的，订户与受托人承担连带责任，订户有责任就受托人的不实陈述、信息遗漏等情况及时通知天威诚信。

b) 证书接受、保存与使用过程中：

1) 订户在接受或使用证书前，已核验确认证书所载信息的准确性；
2) 订户按照本 CP 和 CPS 之规定，在合法且获授权的范围内使用证书，不得超出证书使用目的以外的场合使用；
3) 用于电子签名的证书私钥由订户自行产生的，订户应采取必要且有效的措施保障证书私钥、密码、口令等身份认证要素的安全性；委托他人代为产生签名私钥、使用证书的，订户应明确授权范围并定期核查授权事项履行情况；
4) 使用证书中公钥对应的私钥产生的数字签名，均视为订户做出的有效数字签名；订户知晓待签名的内容，且实施签名行为时，订户已经接受了证书，且该证书未过期、未被撤销；
5) 订户对使用私钥的行为负责，并应采取有效措施保护，确保未经授权的主体无法使用订户的私钥；
6) 发生私钥遗失、泄露、口令遗忘等任何可能危机证书安全的情形时，订户应立即通知天威诚信，申请证书撤销等处理措施，并立即停止使用该证书；

7) 订户按照本 CP 和 CPS 的要求，及时向天威诚信提出证书续期、密钥更新、证书变更、证书撤销等服务请求。

订户协议可另行约定其他陈述与保证内容。

9.6.3 依赖方的陈述与担保

依赖方确认并承诺，在基于天威诚信签发的证书实施任何信赖行为前，履行以下义务：

a) 已熟知本 CP 和 CPS 的相关规定，清晰知晓证书的许可使用目的；

b) 已核验确认证书所载信息与待证事项内容一致；

c) 已采取合理必要措施核查订户证书及电子签名的有效性，包括但不限于：查询最新证书撤销列表（CRL）或在线证书状态协议（OCSP）以确认证书未被撤销、核验证书链的可信性、检查证书有效期及其他影响证书有效性的信息；

d) 自行评估在特定应用场景中信赖证书的适当性，不得在证书许可使用目的以外的应用场景中信赖证书。

9.6.4 其他参与者的陈述与担保

从事电子认证活动的其他参与者应遵守本 CP 和 CPS 的所有规定。

9.7 担保免责

天威诚信仅就本 CP 和 CPS 及相关服务协议中明确载明的事项承担明示担保责任，不提供任何形式的默示担保，包括但不限于对证书的适销性、特定用途适用性、安全性、可靠性、无权利瑕疵等模式保证。

存在下列任意情形的，应免除天威诚信的全部担保责任，天威诚信不向任何主体承担赔偿、补偿及其他任何法律责任。

9.7.1 订户违约、违规、未履行义务导致的免责

订户在证书申请、持有、使用过程中，存在下列违反法定义务、约定义务或本 CP 和 CPS 规定行为之一的：

a) 未履行真实信息提交义务，提供虚假、无效、不完整或不准确的申请材料及信息；
b) 未妥善保管证书载体及与私钥有关的保护 PIN 码、口令等，泄漏保护 PIN 码、口令或将证书载体随意交付他人使用；
c) 使用非安全、不可信赖的系统操作密钥或使用数字证书；
d) 知悉电子签名制作数据已经失密或者可能失密时，未及时通知天威诚信及相关方，且未立即终止使用该电子签名；
e) 违反国家法律、法规和行政规章的规定使用证书，或超出许可使用范围使用证书；
f) 超出证书有效期使用证书，或使用已失密或可能失密、已过期、已被撤销的证书；
g) 未按约定及本 CP 和 CPS 规定按时足额向天威诚信支付服务费用。

9.7.2 不可抗力导致的免责

因不可抗力导致数字证书签发延迟、中断、无法签发，或证书服务全部或部分暂停、终止的。本项所称不可抗力，是指不能预见、不能避免且不能克服的客观情况，包括但不限于：

a) 自然灾害，包括地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等；
b) 社会异常事件及政府行为，包括新法律法规与政策颁发、战争、罢工、暴动、骚乱等。

9.7.3 技术故障导致的免责

因技术故障而导致证书签发延迟、中断、无法签发，或书服务全部或部分暂停、终止的。本项所规定技术故障，包括但不限于：

a) 不可抗力引发的系统故障；
b) 电力、电信、通讯等关联单位服务中断或故障；
c) 网络黑客攻击、恶意入侵等网络安全事件；
d) 天威诚信自有设备、网络系统出现故障。

证书订户、依赖方因天威诚信提供的电子认证服务从事民事活动遭受损失的，天威诚信将承担不超过本 CP 和 CPS 第 9.9 节规定的有限赔偿责任。

天威诚信已谨慎遵循国家法律、法规及本 CP 和 CPS 开展服务，仍发生相关损失的。

9.8 偿付责任规则

证书订户、依赖方因天威诚信提供的电子认证服务从事民事活动遭受损失的，天威诚信按照以下规则承担有限赔偿责任。

9.8.1 财务赔偿范围

依据《中华人民共和国电子签名法》规定，天威诚信适用过错推定责任原则承担赔付责任。赔偿范围覆盖天威诚信在履行电子认证服务职责过程中，因自身过错引发各类风险所造成的订户、证书依赖方直接经济损失，风险情形包括但不限于技术故障、人为操作失误、安全漏洞等。

针对索赔事项，天威诚信赔付审核工作组将对事件原因、过错归属、损失事实及因果关系开展核查评估，并根据评估结果与受损方协商确定最终赔偿范围。

本条款所述直接经济损失，指因天威诚信过错直接导致的财产利益实际减损，不包括间接损失、预期利益损失、商誉损失、间接商业机会损失及精神损害赔偿等非直接损失。

9.8.2 赔付计算方式

天威诚信根据损失类型、CA 过错程度，实行限额赔付制度，赔付计算遵循实际损失为基础、限额为上限、过错程度相匹配的原则。

9.8.2.1赔付限额标准

天威诚信就单张证书所致直接损失的赔偿责任上限为该证书购买价格的 10 倍。

若经司法生效判决或仲裁裁决确认的赔付金额超出上述限额，天威诚信将按生效法律文书履行赔付义务。

天威诚信的全部赔偿义务以本条款规定的责任上限为限；天威诚信可根据监管要求及业务实际调整赔偿上限，调整后将及时书面通知相关主体。

9.8.2.2分情形赔付计算规则

a) 证书签发错误、信息失真类赔付

经核实确属天威诚信审核疏漏或系统缺陷导致证书主体身份、权限范围、有效期等核心信息错误的：

1) 未造成实际经济损失的，免费为用户办理证书信息更正、重新签发或全额注销退费；
2) 造成直接经济损失的，按索赔方举证实际直接损失金额赔付；实际损失低于对应证书限额的按实际金额赔付，超出限额的按对应证书最高赔偿限额赔付。

b) 安全事件、操作过失类赔付

因安全漏洞、操作过失导致私钥泄露、数据被盗用、证书被冒用的，根据过错程度划分责任比例后计算赔付金额：

1) 天威诚信承担全部责任的，按实际直接损失100%计算，最高不超过对应证书赔偿限额；
2) 天威诚信承担主要责任的，按实际直接损失的70%计算，最高不超过对应证书赔偿限额；
3) 双方承担同等责任的，按实际直接损失的50%计算；
4) 天威诚信承担次要责任的，按实际直接损失的30%计算。

9.8.2.3损失认定依据

索赔方需提供合法有效的损失证明材料，包括但不限于财产损失支付凭证、司法机关生效裁判文书、具备资质的第三方机构审计/评估报告、合规的损失明细凭证等。损失金额无法举证或举证无效的，天威诚信有权按对应证书购买价格或服务费倍数进行赔付。

索赔方未在损失发生之日起3年内书面提出索赔的，索赔权利自动消灭，天威诚信不再承担赔偿责任。

9.8.3 赔付监督机制

天威诚信设立由合规管理部门、法务部门、风险管理部门、业务部门共同组成的赔付审核工作组，负责赔付申请的核查、责任认定与金额核算。

按照国家监管要求与行业规范计提电子认证服务风险保障金，实行专款专用、专户管理，仅用于偿付责任赔付与相关风险处置。财务部定期核算准备金计提与使用情况，内部审计部门每年开展专项审计，确保准备金足额、合规使用，不得挪作他用。

发生单次赔付金额超 100 万元的重大赔付事件，或因重大安全事故引发的批量赔付，在处置完成后 10 个工作日内主动向工业和信息化部、国家密码管理局等主管部门报备，接受监管部门监督检查。

9.8.4 天威诚信的赔偿责任

天威诚信按照本 CP 和 CPS 第 9.8.1 节及 9.8.2 节承担赔偿责任。

9.8.5 订户的赔偿责任

订户存在下列情形之一，造成天威诚信、依赖方或第三方损失的，应承担全部赔偿责任：

a) 申请证书时，因故意、过失或恶意提供不真实、不完整、不准确的资料，造成天威诚信或第三方损害的；
b) 因故意或过失导致私钥泄露、遗失，明知私钥泄露、遗失未及时告知天威诚信，或擅自交付他人使用，造成天威诚信、第三方损害的；
c) 违反本 CP 和 CPS 及相关操作规范使用证书，或超出证书许可范围使用的；
d) 自有权主体提出证书撤销请求至天威诚信发布撤销信息期间，证书被用于非法交易或引发交易纠纷，且天威诚信已按本 CP 和 CPS 规范操作的，订户承担该期间内的全部损害赔偿责任；
e) 证书信息变更后未停止使用证书，且未及时通知天威诚信及依赖方的；
f) 未对私钥采取有效保护措施，导致私钥丢失、损毁、窃取、泄露的；

g) 得知私钥丢失或存在安全风险时，未停止使用证书且未及时通知天威诚信及依赖方的；

h) 订户在使用私钥或证书时，未使用可信赖、安全的系统的；

i) 超出证书有效期使用证书的；

j) 证书信息侵犯第三方知识产权的；

k) 超出证书许可范围及目的使用证书，或利用证书从事违法犯罪活动的。

9.8.6 依赖方的赔偿责任

依赖方因自身过错造成天威诚信或第三方损失的，应承担全部赔偿责任，具体情形包括：

a) 未履行与天威诚信的协议或本 CP 和 CPS 规定的义务，造成天威诚信或第三方损害的；

b) 未按本 CP 和 CPS 规定对证书进行合理审核，造成天威诚信或第三方损害的；

c) 未验证证书信任链，造成天威诚信或第三方损害的；

d) 未检查证书状态即信赖使用，造成天威诚信或第三方损害的；

e) 在不合理情形或环境下信赖证书，包括证书存在超范围使用、超期限使用、被盗用等风险仍予以信赖的。

9.8.7 天威诚信免责情形

无论本 CP 和 CPS 是否有相反或不同规定，存在下列情形之一的，天威诚信不承担任何赔付责任：

a) 非因天威诚信的原因导致损失的，如因订户自身过错（如私钥保管不当、身份信息提供不实、违规使用证书、未及时撤销/冻结证书等）导致的损失、因依赖方未尽合理审查义务（如未核验证书有效性、证书用途等）而产生的损失等；

b) 订户和/或依赖方的任何预期损失或间接损失、直接或间接的利润或收入损失、信誉或商誉损害、任何商机或契机损失；

c) 因不可抗力（地震、火灾、战争、政府管制或政策变化、大规模超防护能力网络攻击等）导致的服务中断或损失；

d) 因第三方系统、设备、软件故障导致的损失，且天威诚信已按规范履行自身服务职责的。

9.9 赔偿

天威诚信按照本 CP 和 CPS 第 9.8 节承担有限赔偿责任。发生需天威诚信承担赔偿责任情形的，天威诚信按照以下流程处置相关索赔事项。

9.9.1 索赔申请

索赔主体仅限符合本 CP 和 CPS 规定的证书订户、依赖方等合法权益受损方。

索赔方应在知道或应当知道损失发生之日起 3 年内，以书面形式向天威诚信提出索赔申请。

书面索赔申请应载明：索赔方身份信息、涉案证书信息、索赔事由、损失明细、赔偿金额主张、索赔依据及联系方式。

9.9.2 材料提交

索赔方提交书面索赔申请时，应同步附完整证明材料，包括但不限于：

a) 索赔方有效身份证明文件（个人身份证件、企业营业执照等）；

b) 涉案电子签名认证证书的完整信息及权属证明；

c) 损失发生的凭证、损失金额计算依据；

d) 损失与天威诚信过错存在因果关系的证明材料；

e) 其他与索赔相关的证据材料。

9.9.3 审核处理

天威诚信在收到完整索赔申请及证明材料后，15 个工作日内完成合规性、真实性、关联性审核，并出具书面审核意见；索赔情形复杂、无法在 15 个工作日内完成审核的，天威诚信可延长审核时限至 30 个工作日，并书面告知索赔方延期理由。

9.9.4 赔付执行

经审核认定属于天威诚信赔偿责任的，天威诚信在书面审核意见出具并与索赔方达成一致后 15 个工作日内，按照本 CP 和 CPS 约定的赔偿限额及赔付标准完成赔付；赔付方式以双方约定为准，包括但不限于银行转账、现金赔付等。

索赔方应在收到赔付后，向天威诚信出具收款确认文件。

9.9.5 争议解决

索赔方对天威诚信的审核结果、赔付标准有异议的，可与天威诚信协商解决；协商不成的，可按照本 CP 和 CPS 约定的争议解决方式，通过诉讼、仲裁等法定途径处理。

争议解决期间，不影响天威诚信对已认定赔付事项的执行。

9.10 有效期限与终止

9.10.1 有效期限

本 CP 和 CPS 在生效日期零时正式生效，上一版本的 CP 和 CPS 同时失效；本 CP 和 CPS 在下一版本 CP 和 CPS 生效之日或在天威诚信终止电子认证服务时失效。

9.10.2 终止

当新版本 CP 和 CPS 正式发布生效后，旧版本 CP 和 CPS 自动终止。

9.10.3 效力的终止与保留

本 CP 和 CPS 终止后，其效力将同时终止，但对终止之日前发生的法律事实，本 CP 和 CPS 中对各方责任的规定及责任免除仍然适用，包括但不限于 CP 和 CPS 中涉及审计、保密信息、隐私保护、知识产权等内容，以及涉及赔偿的有限责任条款，在本 CP 和 CPS 终止后继续有效。

当由于某种原因，如内容修改、与适用法律相冲突，CP 和 CPS、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

天威诚信在本 CP 和 CPS 第 1.5 节指定的地址接收与本 CP 和 CPS 相关的通知，相关通知自发件人收到天威诚信出具的有效书面确认文件之日起生效。

天威诚信可根据服务开展的必要需要，通过电话、电子邮件、系统站内信、信函、传真等适当方式，就本 CP 和 CPS 项下相关服务事项进行个别通知。

9.12 修订和发布

9.12.1 修订程序

本证书策略和认证业务规则（CP 和 CPS）将依据国家法律法规、行业主管部门监管要求、相关标准规范及认证业务实际运营需求，实施不定期修订与完善，确保持续符合合规要求与业务实践。

本 CP 和 CPS 的修订与更新工作由 CP 和 CPS 编写小组负责完成，修订后的 CP 和 CPS 经过天威诚信安全策略委员会批准后正式对外发布并生效。

9.12.2 通知机制与期限

修订后的 CP 和 CPS 经批准后，将在天威诚信官网予以公示发布。

对于需通过电子邮件、信函、官方媒体等渠道专项通知的修订事项，天威诚信将在合理期限内通知相关参与方，该合理期限以最大限度降低修订事项对相关方的影响为确定原则。

9.12.3 必须修改业务规则的情形

出现下列情况之一的，天威诚信必须对本 CP 和 CPS 进行修订：

a) 本 CP 和 CPS 所载内容与现行有效的管辖法律、行政法规、规章及监管规定存在冲突的；
b) 国家行业主管部门对天威诚信认证业务提出明确变更、调整或整改要求的；
c) 相关国家标准、行业标准发生实质性更新，需同步调整 CP 和 CPS 内容的；

d) 其他依法应当对本 CP 和 CPS 予以修订的情形。

9.13 争议处理

9.13.1 争议解决机制

天威诚信建立协商优先、调解补充、司法终局的多层级争议解决机制，覆盖与电子认证服务相关的全类型争议。

9.13.1.1 争议受理范围

天威诚信受理与电子认证服务、本 CP 和 CPS 履行相关的民事争议，具体包括：

a) 订户与天威诚信之间因证书申请、身份审核、证书签发、交付、变更、注销、服务收费、偿付责任等产生的争议；

b) 合法证书依赖方与天威诚信之间因证书信赖、证书状态查询、签名验证服务等产生的争议；

c) 其他因天威诚信提供电子认证服务所引发的、与本 CP 和 CPS 条款相关的争议。

下列情形不属于天威诚信争议受理范围：

a) 争议事项已进入诉讼、仲裁、行政复议等法定程序的；

b) 争议内容与天威诚信电子认证服务无直接关联的；

c) 同一争议已经处理完毕且无新事实、新证据重复提出的。

9.13.1.2 协商解决

a) 受理渠道：争议方可通过天威诚信官方客服热线、专项邮箱、线下服务网点等渠道提交争议申请，申请应当载明争议双方信息、争议事项、事实理由、相关证据及诉求。

b) 响应与处理时限：天威诚信收到符合要求的争议申请后，于 5 个工作日内予以受理并告知处理对接人；双方应在受理之日起 15 个工作日内开展友好协商；案情复杂的，经双方同意可延长协商期限，最长不超过 45 个工作日。

c) 协商结果：协商达成一致的，双方签署书面和解协议并按协议履行；协商不成的，告知争议方可通过调解或司法途径解决。

9.13.1.3 调解解决

协商不成的争议，双方可自愿选择调解途径解决：

a) 行业调解：可向全国性或地方电子认证行业自律组织申请行业调解，按照行业调解规则开展调解工作。
b) 第三方调解：可向争议发生地或天威诚信住所地的人民调解委员会、商事调解机构申请第三方调解。
c) 调解规则：调解遵循自愿、公平、保密原则，调解结果不具有强制执行力；经调解达成协议的，双方可依法申请司法确认；调解不成的，任何一方均有权通过诉讼或仲裁方式解决争议，调解过程中的意见与让步不得作为后续司法程序中的不利证据。

9.13.1.4 诉讼与仲裁

a) 适用条件：争议双方经协商、调解仍无法达成一致的，可通过诉讼或仲裁方式解决；双方事先达成有效仲裁协议的，优先适用仲裁。
b) 管辖规则：若无专门仲裁约定，因天威诚信电子认证服务及本 CP 和 CPS 引发的争议，任何一方均有权向天威诚信住所地有管辖权的人民法院提起诉讼。
c) 法律适用：本争议解决机制适用中华人民共和国法律（不含香港特别行政区、澳门特别行政区及台湾地区法律）。

9.13.2 举证制度与能力体系

天威诚信建立覆盖证书全生命周期的举证能力体系，通过技术与管理双重措施保障证据的真实性、完整性、可追溯性，满足争议处理、司法举证与监管检查的要求。

9.13.2.1 证书签发环节举证材料

证书签发全流程留存完整审核与确认记录，可作为身份真实性、意愿真实性与签发合规性的举证依据，包括但不限于身份验证记录、材料审查记录、告知记录、意愿确认记录等。

9.13.2.2 签名环节举证材料

针对天威诚信提供的签名服务与私钥托管服务的，完整留存签名操作记录，可作为签名行为真实性、授权有效性的举证依据，包括但不限于签名请求验证记录、签名操作日志、时间戳记录等。

9.13.2.3 验证签名环节举证材料

证书状态查询、签名验证服务全流程留痕，可作为验证行为与验证结果的举证依据，包括但不限于验证请求记录、验证结果记录、异常情况处理记录等。

9.13.2.4 提供举证材料的时间承诺

天威诚信对举证材料调取提供明确时限保障：

a) 订户/依赖方举证申请：订户或依赖方申请调取自身相关的证书服务证明材料，完成身份核验后，天威诚信于 10 个工作日内提供对应证明文件；涉及复杂日志调取的，最长不超过 20 个工作日。

b) 司法/行政机关调取：对司法机关、行政监管部门依法定程序调取的证据材料，天威诚信在收到符合要求的调取文书后，于 10 个工作日内完成证据提供；紧急案件可根据办案需求开通绿色通道加急处理。

c) 争议处理举证：在争议协商、调解过程中，天威诚信应对方要求或争议处理机构要求提供举证材料的，于 10 个工作日内提交对应证据材料。

9.13.2.5　举证责任分配

a) 天威诚信对自身已按照法律法规、本 CP 和 CPS 要求履行身份审核、安全保障、规范操作等义务承担举证责任；若天威诚信无法证明自身无过错，依法承担相应责任。
b) 主张损失存在、主张天威诚信存在过错的一方，对损失事实、损害结果、因果关系承担举证责任。
c) 订户对自身私钥保管不当、违规使用证书等自身过错情形，自行承担举证责任。

9.13.2.6　证据留存管理

证据留存期限不少于对应证书有效期届满后 5 年；法律法规、监管规定对留存期限有更长要求的，从其规定。

证据查阅、调取严格执行权限审批与留痕管理，保障用户信息安全与商业秘密。

9.14 管辖法律

本 CP 和 CPS 及对应的 CP 受《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务使用密码管理办法》的管辖和解释。

9.15 与适用法律的符合性

电子认证服务的相关参与者均应遵守中华人民共和国现行有效的法律法规。在中华人民共和国境内适用的法律法规包括但不限于《中华人民共和国电子签名法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《商用密码管理条例》《电子认证服务管理办法》《电子认证服务使用密码管理办法》。

无论证书订户、依赖方等主体的住所地、经常居住地或证书实际使用地位于何处，本 CP 和 CPS 的执行、解释和程序有效性均适用上述中华人民共和国法律；因本 CP 和 CPS 引发的任何争议，均适用上述中华人民共和国法律予以解决。

9.16 一般条款

9.16.1 完整协议

本 CP 和 CPS 完整的文档结构包含标题、目录及主体内容三部分。经修订后的目录及主体内容替代文本，将完全替代所有先前或同时期相关的解释对应内容，并通过天威诚信官方网站公示，供相关方查阅和浏览。

天威诚信将在订户协议中明确载明对应的 CP 和 CPS 版本。

本 CP 和 CPS 对应依赖方协议的版本以天威诚信官方网站公示的内容为准。

CP、CPS、订户协议、依赖方协议以及订户协议和依赖方协议的补充协议构成各参与者之间的完整协议。

9.16.2 转让

本 CP 和 CPS 项下各方主体的权利和义务，未经天威诚信事先书面同意，任何一方不得通过任何方式进行转让。

9.16.3 分割性

如果本 CP 和 CPS 的任何条款或其适用因与天威诚信所在地管辖法律相冲突，被有权机关认定为无效或不可执行的，天威诚信可以在最低必要的限度下修订该条款，使其符合法律规定并继续有效，其余部分不受影响，天威诚信将在本章项下批露该等修订内容。

9.16.4 强制执行

天威诚信、订户、依赖方之间因本 CP 和 CPS 发生纠纷或诉讼的，胜讼方有权要求败诉方支付合理的诉讼费用作为损失补偿的一部分。

乙方对单次合同违约行为的赔偿责任免除，不构成对其他合同违约行为赔偿责任的免除。

天威诚信声明，若证书订户、依赖方等主体未履行本 CP 和 CPS 中某项规定的，不视为其放弃将来履行该项规定或其他规定的义务。

9.16.5 不可抗力

因不可抗力导致天威诚信无法正常提供本 CP 和 CPS 项下的服务的，天威诚信不承担由此给相关方造成的损失。

本条款所称不可抗力，是指不能预见、不能避免且不能克服的客观情况，包括但不限于地震、洪灾、雷电等自然灾害及新规政策颁布、战争、罢工、骚乱等政府行为和社会异常事件。

9.17其他条款

天威诚信对本 CP 和 CPS 具有最终解释权。

附录：电子签名认证证书内容

下表描述了天威诚信电子签名认证证书的内容要求。未在下表中说明的证书内容项，遵循 GM/T 0015 的规定。

电子签名认证证书内容

项	值
支持的数字证书格式版本号	整数 2 用于版本 3 证书
证书序列号	唯一正整数
密码算法对象标识符	1.2.840.113549.1.1.11 （SHA256WithRSAEncryption） 1.2.156.10197.1.501 （SM3WithSM2Encryption）
颁发者名称	国家；机构名称；通用名等
有效期	起始有效期；终止有效期
订户名称	国家；省份；地市；用户名称等
证书策略扩展项	1.主管部门分配的电子签名认证证书策略对象标识符（OID），其值为 个人高级 OID：2.16.156.339.2.1.1.2 个人基础 OID：2.16.156.339.2.1.1.1 机构高级 OID：2.16.156.339.2.1.2.2 机构基础 OID：2.16.156.339.2.1.2.1 2.CA 注册的电子签名认证证书策略对象标识符（OID）