天威诚信通用安全认证证书

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
通过安全认证证书 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公司提供的文件准确、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，CP 和 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 概述 1
1.2 文档名称与标识 2
1.3 通用安全认证证书认证活动参与者 3
1.3.1 电子认证服务机构（CA） 3
1.3.2 注册机构（RA） 3
1.3.3 订户 3
1.3.4 依赖方 4
1.3.5 其他参与者 4
1.4 证书应用 4
1.4.1 适合的应用 4
1.4.1.1 身份证书 4
1.4.1.2 设备证书 4
1.4.1.3 时间戳证书 4
1.4.2 受限的应用 5
1.4.3 受禁的使用 5
1.5 策略管理 5
1.5.1 策略文档管理机构 5
1.5.2 联系人 5
1.5.3 决定 CPS 符合策略的机构 6
1.5.4 CPS 批准程序 6
1.6 定义与缩写 6
1.6.1 定义 6
1.6.2 缩写 7
2. 信息发布与管理 8
2.1 信息库 8
2.2 认证信息的发布 8
2.3 发布的时间或频率 8
2.4 信息库访问控制 8
3. 身份标识与鉴证 9
3.1 命名 9
3.1.1 名称类型 9
3.1.2 对名称有意义的要求 9
3.1.3 订户的匿名或伪名 10
3.1.4 理解不同名称形式的规则 10
3.1.5 名称的唯一性 10
3.1.6 商标的识别、鉴证和角色 10
3.2 初始身份确认 10
3.2.1 证明拥有私钥的方法 10

3.2.2 机构身份的鉴证 11
3.2.3 个人身份的鉴证 12
3.2.4 没有验证的订户信息 13
3.2.5 授权的确认 13
3.2.6 互操作准则 13
3.3 密钥更新请求的标识与鉴证 13
3.3.1 常规的密钥更新的标识与鉴证 14
3.3.2 吊销之后的密钥更新的标识与鉴证 14
3.4 吊销请求的标识与鉴证 14
4. 证书生命周期操作要求 15
4.1 证书申请 15
4.1.1 证书申请实体 15
4.1.2 注册过程与责任 15
4.2 证书申请处理 16
4.2.1 执行识别与鉴别功能 16
4.2.2 证书申请批准和拒绝 16
4.2.3 处理证书申请的时间 17
4.3 证书签发 17
4.3.1 证书签发中 RA 和 CA 的行为 17
4.3.2 CA 和 RA 对订户的通知 17
4.4 证书接受 17
4.4.1 构成接受证书的行为 17
4.4.2 CA 对证书的发布 18
4.4.3 CA 对其他实体的通告 18
4.5 密钥对和证书使用 18
4.5.1 订户私钥和证书使用 19
4.5.2 依赖方公钥和证书使用 19
4.6 证书更新 19
4.6.1 证书更新的情形 19
4.6.2 请求证书更新的实体 20
4.6.3 证书更新请求的处理 20
4.6.4 签发新证书时对订户的通知 21
4.6.5 构成接受更新证书的行为 21
4.6.6 CA 对更新证书的发布 21
4.6.7 CA 对其他实体的通告 21
4.7 证书密钥更新 21
4.7.1 证书密钥更新的情形 22
4.7.2 请求证书密钥更新的实体 22
4.7.3 证书密钥更新请求的处理 22
4.7.4 签发新证书时对订户的通知 23
4.7.5 构成接受密钥更新证书的行为 23

4.7.6 CA 对密钥更新证书的发布 23
4.7.7 CA 对其他实体的通告 23
4.8 证书变更 23
4.8.1 证书变更的情形 23
4.8.2 请求证书变更的实体 23
4.8.3 证书变更请求的处理 23
4.8.4 签发新证书时对订户的通告 24
4.8.5 构成接受变更证书的行为 24
4.8.6 CA 对变更证书的发布 24
4.8.7 CA 对其他实体的通告 24
4.9 证书吊销和挂起 24
4.9.1 证书吊销的情形 24
4.9.2 请求证书吊销的实体 25
4.9.3 吊销请求的流程 25
4.9.4 吊销请求宽限期 26
4.9.5 CA 处理吊销请求的时限 26
4.9.6 依赖方检查证书吊销的要求 26
4.9.7 CRL 发布频率 26
4.9.8 CRL 发布的最大滞后时间 26
4.9.9 在线状态查询的可用性 26
4.9.10 在线状态查询要求 27
4.9.11 吊销信息的其他发布形式 27
4.9.12 密钥损害的特别要求 27
4.9.13 证书挂起的情形 27
4.9.14 请求证书挂起的实体 27
4.9.15 挂起请求的流程 27
4.9.16 挂起的期限限制 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 密钥托管与恢复 28
4.12.1 密钥托管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
5. 认证机构设施、管理和操作控制 30
5.1 物理控制 30
5.1.1 场地位置与建筑 30
5.1.2 物理访问控制 30
5.1.3 电力与空调 30
5.1.4 水患防治 31

5.1.5 火灾防护 31
5.1.6 介质存储 31
5.1.7 废物处理 32
5.1.8 异地备份 32
5.2 程序控制 32
5.2.1 可信角色 32
5.2.2 每项任务需要的人数 32
5.2.3 每个角色的识别与鉴别 33
5.2.4 需要职责分割的角色 33
5.3 人员控制 33
5.3.1 资格、经历和无过失要求 33
5.3.2 背景审查程序 34
5.3.3 培训要求 34
5.3.4 再培训周期和要求 35
5.3.5 工作岗位轮换周期和顺序 35
5.3.6 未授权行为的处罚 35
5.3.7 独立合约人的要求 35
5.3.8 提供给员工的文档 35
5.4 审计日志程序 35
5.4.1 记录事件的类型 35
5.4.2 处理日志的周期 37
5.4.3 审计日志保存期限 37
5.4.4 审计日志的保护 37
5.4.5 审计日志备份程序 37
5.4.6 审计收集系统 37
5.4.7 对导致事件主体的通知 37
5.4.8 脆弱性评估 38
5.5 记录归档 38
5.5.1 归档记录的类型 38
5.5.2 归档记录的保存期限 38
5.5.3 归档文件的保护 38
5.5.4 归档文件的备份程序 39
5.5.5 记录时间戳要求 39
5.5.6 归档收集系统 39
5.5.7 获得和检验归档信息的程序 39
5.6 CA 密钥变更 39
5.7 损害与灾难恢复 40
5.7.1 事故和损害处理程序 40
5.7.2 计算机资源、软件和/或数据的损坏 40
5.7.3 实体私钥损害处理程序 40
5.7.4 灾难后的业务存续能力 41

5.8 CA 或 RA 的终止 41
6. 技术安全控制 42
6.1 密钥对的产生和安装 42
6.1.1 密钥对的产生 42
6.1.1.1 CA 密钥对的产生 42
6.1.1.2 订户密钥对的产生 42
6.1.2 私钥传送给订户 42
6.1.3 公钥传送给证书签发机关 43
6.1.4 CA 公钥传送给依赖方 43
6.1.5 密钥的长度 43
6.1.6 公钥参数的生成和质量检查 43
6.1.7 密钥使用目的 44
6.2 私钥保护和密码模块工程控制 44
6.2.1 密码模块的标准和控制 44
6.2.2 私钥多人控制（m 选 n） 44
6.2.3 私钥托管 45
6.2.4 私钥备份 45
6.2.5 私钥归档 45
6.2.6 私钥导入、导出密码模块 45
6.2.7 私钥在密码模块的存储 46
6.2.8 激活私钥的方法 46
6.2.9 解除私钥激活状态的方法 46
6.2.10 销毁私钥的方法 47
6.2.11 密码模块的评估 47
6.3 密钥对管理的其他方面 47
6.3.1 公钥归档 47
6.3.2 证书操作期和密钥对使用期限 47
6.4 激活数据 48
6.4.1 激活数据的产生和安装 48
6.4.2 激活数据的保护 48
6.4.3 激活数据的其他方面 49
6.5 计算机安全控制 49
6.5.1 特别的计算机安全技术要求 49
6.5.2 计算机安全评估 50
6.6 生命周期技术控制 50
6.6.1 系统开发控制 50
6.6.2 安全管理控制 50
6.6.3 生命期的安全控制 50
6.7 网络的安全控制 51
6.8 时间戳 51
7. 证书、CRL 和 OCSP 52

7.1 证书 52
7.1.1 版本号 52
7.1.2 证书扩展项 52
7.1.2.1 密钥用法（Key Usage） 52
7.1.2.2 证书策略扩展项（Certificate Policies） 52
7.1.2.3 主体备用名（subjectAltName） 52
7.1.2.4 基本限制扩展项（BasicConstraints） 53
7.1.2.5 扩展的密钥用法（Extended Key Usage） 53
7.1.2.6 CRL 的分发点（cRLDistributionPoints） 53
7.1.2.7 签发 CA 密钥标识符 53
7.1.2.8 主体密钥标识符 53
7.1.3 密钥算法对象标识符 53
7.1.4 名称形式 53
7.1.5 名称限制 54
7.1.6 证书策略对象标识符 54
7.1.7 策略限制扩展项的用法 54
7.1.8 策略限定符的语法和语义 54
7.1.9 关键证书策略扩展项的处理规则 54
7.2 CRL 54
7.2.1 版本号 54
7.2.2 CRL 和 CRL 条目扩展项 55
7.3 OCSP 55
7.3.1 版本号 55
7.3.2 OCSP 扩展项 55
8. 认证机构审计和其他评估 56
8.1 评估的频率和情形 56
8.2 评估者的资质 56
8.3 评估者与被评估者之间的关系 56
8.4 评估的内容 56
8.5 对问题与不足采取的措施 57
8.6 评估结果的传达与发布 57
8.7 其他评估 57
9. 其他业务和法律事务 58
9.1 费用 58
9.1.1 证书签发和更新费用 58
9.1.2 证书查取的费用 58
9.1.3 证书吊销或状态信息的查询费用 58
9.1.4 其他服务费用 58
9.1.5 退款策略 58
9.2 财务责任 59
9.2.1 保险范围 59

9.2.2 其他资产 59
9.2.3 对最终实体的保险或担保 59
9.3 业务信息保密 59
9.3.1 保密信息范围 59
9.3.2 不属于保密的信息 60
9.3.3 保护保密信息的责任 60
9.4 个人隐私保密 61
9.4.1 隐私保密方案 61
9.4.2 作为隐私处理的信息 61
9.4.3 不被视为隐私的信息 61
9.4.4 保护隐私的责任 61
9.4.5 使用隐私信息的告知与同意 61
9.4.6 依法律或行政程序的信息披露 62
9.4.7 其他信息披露情形 62
9.5 知识产权 62
9.6 陈述与担保 62
9.6.1 CA 的陈述与担保 62
9.6.2 RA 的陈述与担保 63
9.6.3 订户的陈述与担保 63
9.6.4 依赖方的陈述与担保 64
9.6.5 其他参与者的陈述与担保 64
9.7 担保免责 65
9.8 有限责任 66
9.9 赔偿 66
9.10 有效期限与终止 68
9.10.1 有效期限 68
9.10.2 终止 68
9.10.3 效力的终止与保留 69
9.11 对参与者个别通告与沟通 69
9.12 修订 69
9.12.1 修订程序 69
9.12.2 通知机制与期限 69
9.12.3 必须修改业务规则的情形 70
9.13 争议解决 70
9.14 管辖法律 70
9.15 与适用法律的符合性 70
9.16 一般条款 70
9.16.1 完整协议 70
9.16.2 转让 71
9.16.3 分割性 71
9.16.4 强制执行 71

9.16.5 不可抗力..... 71
9.17 其他条款..... 71

1. 概括性描述

1.1 概述

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“天威诚信”），是 2005 年首批获得信息产业主管部门颁发《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用户提供电子认证服务。

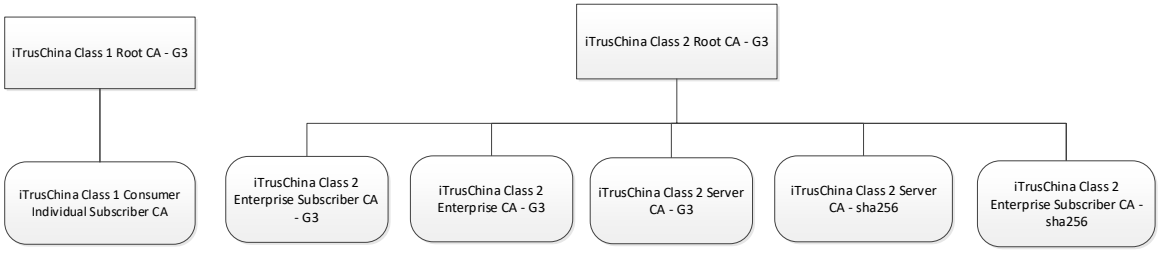
天威诚信通用安全认证证书证书策略和认证业务规则是关于天威诚信提供的而一类数字证书生命周期管理的策略和业务实践声明。该类数字证书主要面向电子签名认证之外的其他 PKI 应用场景，实现身份识别、数字签名、加解密、时间戳等安全服务。

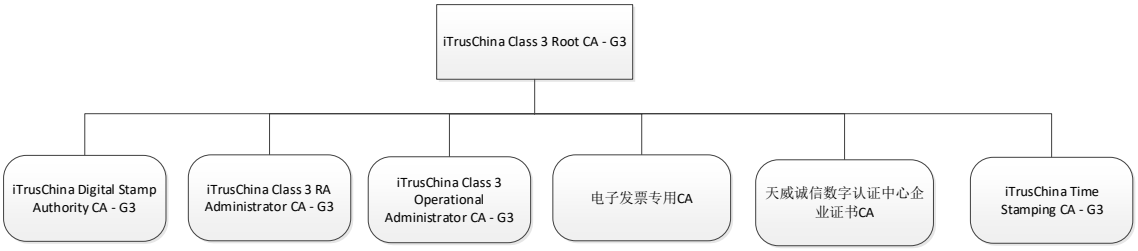
本文档依据天威诚信证书策略和相关要求制定，旨在阐明天威诚信如何开展天威诚信 CTN（China Trust Network）根体系和国密根体系下除电子签名认证证书之外的其他认证业务，包括批准、签发、管理、吊销和更新证书的业务方式和过程，以及相应的服务、技术、和法律上的措施和保障，以供电子认证活动参与方了解和遵循。

天威诚信 CTN 根体系涉及以下 3 个根证书：

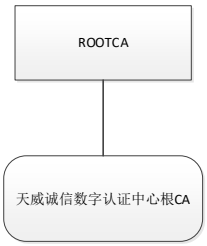
1) iTrusChina Class 1 Root CA - G3
2) iTrusChina Class 2 Root CA - G3
3) iTrusChina Class 3 Root CA - G3

根据业务场景不同，根 CA 之下包含中级 CA/客户子 CA。客户子 CA 是天威诚信为客户创建的项目子 CA，由天威诚信持有、管理和运营。





国密根体系的根证书“ROOTCA”由国家密码管理局持有、管理和运营，它签发的“天威诚信数字认证中心根 CA”及其下整个 CA 体系由天威诚信持有、管理和运营。



订户和依赖方可访问天威诚信官网 https://www.itrus.com.cn/certificate1.html 下载上述根体系证书。

本 CP 和 CPS 的总体条款结构符合相关标准；在制定本 CP 和 CPS 时可能会对该框架进行微调，以适应天威诚信认证业务的特定需求。

1.2 文档名称与标识

本文档称为《天威诚信通用安全认证证书证书策略和认证业务规则 v1.0》（简称“天威诚信通用安全证书 CP 和 CPS”）。

天威诚信注册的 OID 为 1.2.156.112535。天威诚信签发的通用安全认证证书的证书策略 OID，如下表所示：

证书类型	证书策略 OID
身份证书-个人证书	1.2.156.112535.1.1.1.4

身份证书-机构证书	1.2.156.112535.1.1.1.5
设备证书	1.2.156.112535.1.1.1.6

1.3 通用安全认证证书认证活动参与者

1.3.1 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公钥证书的实体。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公共认证体系，向订户颁发包括个人证书、机构证书、设备证书在内的各类公钥证书。

1.3.2 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、恢复和吊销等的实体。

天威诚信除了承担 CA 的角色外，同时也承担部分 RA 的角色。

天威诚信下属独立法人机构、或与天威诚信签署相关书面文件的外部机构，可作为天威诚信外部 RA 负责 RA 相关证书业务。在不违反本 CP 和 CPS 及与天威诚信签署的相关书面文件的前提下，外部 RA 可以根据其内部需求，自行制定管理流程。

1.3.3 订户

“订户”指向天威诚信申请证书的个人或组织机构，也称为最终用户（end-user）。订户通常需要与天威诚信数字认证中心或 RA 签订合约获得证书，并承担作为证书订户的责任。

1.3.4 依赖方

依赖方是指信赖于证书所证明的基础信任关系并依此进行业务活动的实体。依赖方可以是证书订户，也可以不是订户。

1.3.5 其他参与者

无规定。

1.4 证书应用

1.4.1 适合的应用

天威诚信签发的通用安全认证证书适合应用于电子商务、企业信息化等领域需要进行身份识别、访问控制、数据完整性校验等场景。根据业务应用场景的不同，分为身份证书、设备证书和时间戳证书。具体如下：

1.4.1.1 身份证书

身份证书包含个人证书与机构证书。

个人证书，包括个人用户证书和机构雇员证书，可用于需要区分、标识、鉴别个人身份的场合，适用于个人身份识别、数字签名以及数据加密等服务。

机构证书，包括机构单位证书和机构代表人证书，可用于需要区分、标识、鉴别机构身份的场合，适用于机构身份识别、数字签名以及数据加密等服务。

1.4.1.2 设备证书

设备证书用于标识域名（如服务器证书）、或服务器等设备身份，实现个人或企业的域名认证、或设备身份认证、以及数据加解密和信息签名，以提供信息源发性证明、及实现信息保密和完整性保障。

1.4.1.3 时间戳证书

时间戳证书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。

1.4.2 受限的应用

天威诚信所颁发的各类证书，其密钥用法在订户证书扩展项中进行了限制。但是，基于证书扩展项的限制有效性取决于应用软件，如果有关方不遵守约定，对证书的使用超出本 CP 和 CPS 限定的应用范围，将是不受保护的。

1.4.3 受禁的使用

天威诚信签发的证书不能在任何与国家或地方法律法规相违背的领域中使用，也不能在任何未经安全检测的环境及应用中使用。

天威诚信签发的通用安全认证证书不适用于合同、协议等影响实体权利义务文件的电子签名认证活动。

1.5 策略管理

1.5.1 策略文档管理机构

本 CP 和 CPS 的管理机构是天威诚信安全策略委员会，其联系地址如下：

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 401（100085）

电话号码：0086-010-50947500

邮箱地址：itrus_spc@itrus.com.cn

1.5.2 联系人

如果需要天威诚信策略文档请发邮件到信箱：itrus_spc@itrus.com.cn，或来信请寄：

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（100085）

电话号码：0086-010-50947500

其他联系信息可访问 https://www.itrus.com.cn/contact.html 获取。

1.5.3 决定 CPS 符合策略的机构

天威诚信安全策略委员会。

1.5.4 CPS 批准程序

天威诚信 CP 和 CPS 的最高管理机构是天威诚信安全策略委员会，该委员会负责制定、批准、发布、实施、更新、废止 CP 和 CPS。

CP 和 CPS 的具体编制、修订工作，由天威诚信安全策略委会指定相关业务部门组成编写小组负责，并由编制人负责检查 CP 和 CPS 与实际情况的符合性；该小组完成编制后，提交安全策略委员会审核和批准。

1.6 定义与缩写

1.6.1 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。
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。

1.6.2 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。

2.2 认证信息的发布

天威诚信的证书策略和认证业务规则可从天威诚信的官网获取；用户证书可从天威诚信的 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、吊销）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。

2.3 发布的时间或频率

天威诚信的证书策略和认证业务规则按照 1.5.4 的批准程序完成审批后，10 个工作日内发布到官网，并且 7*24 小时可供查询。

2.4 信息库访问控制

对于天威诚信官网公布的信息，公众查询没有限制。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. 身份标识与鉴证

3.1 命名

3.1.1 名称类型

天威诚信签发的证书主体 DN 项结构遵循相关标准要求。编码规则见下表。

DN 项	说明
C	国家（固定为 CN）
ST	省份 / 自治区 / 直辖市
L	城市 / 区县
O	机构名称
OU	机构部门
CN	订户名称

证书 DN 中根据客户要求，可能包含上述各项中的部分或全部，以及电子邮件地址等其他子项。

3.1.2 对名称有意义的要求

个人证书主体甄别名中的通用名通常是个人的真实姓名，或者其他能唯一标识用户身份的其他信息，如个人身份证号码等，它作为标识订户的关键信息被鉴别和认证。

机构单位证书主体甄别名的通用名通常是组织机构的名称，或者其他能唯一标识该机构的其他信息，如组织机构代码等，它作为标识订户的主要信息同其他信息一起被鉴别和认证。

机构代表人证书主体甄别名中的通用名通常是个人的真实姓名，或者其他能唯一标识用户身份的其他信息，如个人身份证号码等，它作为标识订户的主要信息同其他信息（如组织机构名称）一起被鉴别和认证。

设备证书主体甄别名中的通用名通常是该组织机构的设备名，如域名，它作为标识订户的主要信息同其他信息（如组织机构名称）一起被鉴别和认证。

3.1.3 订户的匿名或伪名

通用安全认证证书体系中，根据具体业务场景的需求，在证书中可不记录订户的真实名称，可使用匿名或伪名。

3.1.4 理解不同名称形式的规则

依 X.500 甄别名命名规则解释。

3.1.5 名称的唯一性

天威诚信不强制要求通用名唯一。证书之间的唯一性通过分配唯一的证书序列号来维持。

3.1.6 商标的识别、鉴证和角色

证书申请者不应在其证书申请中使用侵害他人知识产权的名称，天威诚信签发证书时并不验证申请者是否使用商标或处于商标纠纷中。当出现此类争端时，天威诚信有权拒绝证书申请或吊销已发放的证书，直到争端得到有效解决。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

天威诚信通过使用经数字签名的 PKCS#10 格式的证书请求，验证证书申请者拥有私钥。

3.2.2 机构身份的鉴证

签发机构证书时，天威诚信或其注册机构需对组织机构进行身份鉴证，鉴证包括如下两方面内容：

- 确认组织机构是确实存在的、合法的实体。确认的方式可以是，政府签发的组织机构成立的有效证件或证件的具体信息，如营业执照、事业单位法人证书等，或通过权威的第三方数据库确认。
- 确认该组织机构知晓并授权证书申请，即代表组织机构提交证书申请的人是经过授权的。确认的方式可以是，由该机构提供加盖公章的信函或其电子版扫描件确认，通过第三方数据库等辅助手段验证进行授权事宜的确认。

签发服务器证书时，天威诚信或其注册机构需对组织机构进行身份鉴证，鉴证包括如下内容：

- 确认组织机构是确实存在的、合法的实体。确认的方式可以是，政府签发的组织机构成立的有效证件或证件的具体信息，如营业执照、事业单位法人证书等，或通过权威的第三方数据库确认。
- 确认组织机构对域名有所有权或使用权。确认的方式可以是，通过域名注册商确认域名所有者信息。
- 确认该组织机构知晓并授权证书申请，即代表组织机构提交证书申请的人是经过授权的。确认的方式可以是，由该机构提供加盖公章的信函或其电子版扫描件确认，通过第三方数据库等辅助手段验证进行授权事宜的确认。

鉴证审核批准后，天威诚信或注册机构按照相关法律法规的要求妥善保管订户申请材料，订户申请材料可以是纸质或电子数据形式。

当天威诚信对外向有关机构（如注册机构或其他申请机构）签发与运营有关的设备证书时，将通过书面形式（包括加盖公章的信函或其电子扫描件），向该机构的有关责任人确认设备证书申请者来自该机构，且有关申请获得了授权。

天威诚信保留根据国家最新的法律法规和政策的要求更新机构身份的鉴别方法与流程的权利。

3.2.3 个人身份的鉴证

签发个人证书时，天威诚信或注册机构需对个人进行身份鉴证，鉴证包括如下内容：

- 确认证书申请者提交的身份信息确实存在且正确，具体方法包括：
  - 采用天威诚信认可的、提供身份核实服务的数据库中的信息，如公安部门提供的个人身份数据库或其他可靠的信息源。
  - 对于承担注册机构职能的机构向与其相关的人员（如其员工、客户、合作伙伴）颁发证书的情形，可通过采用包含在该机构业务记录或有效电子信息来完成鉴别。
- 验证证书申请者是证书申请中所说的那个人，验证的方式包括：
  - 验证申请者知晓或拥有通常只有真正的申请者才知晓或拥有的秘密，如通过订户银行帐户进行转帐验证；向订户注册的手机号码发送短信进行验证、设置密码口令进行验证、指纹识别、人脸识别等。
  - 通过承担注册机构职能的机构中的管理员验证、确认与该机构相关的证书申请者（如其员工、客户、合作伙伴）的身份及其证书申请行为。
  - 对于订户在注册时填写的电子邮箱信息，将通过发送邮箱验证邮件的方式完成验证；
  - 其他安全可靠的方式验证确认。

若个人证书的身份信息中包含有组织机构信息，则天威诚信认证机构或其注册机构还需要对该组织机构信息进行鉴证，其情形分为如下两种：

若申请者个人直接向天威诚信或其注册机构提交申请，则天威诚信或其注册机构，首先按“3.2.2 机构身份的鉴证”所述方法，确认组织机构信息的真实性；然后按“3.2.2 机构身份的鉴证”所述方法，确认申请者属于该组织机构的员工。

若证书申请通过天威诚信批准的承担注册机构职能的组织机构提交，在这种情形下，由组织机构负责确保有关信息的正确性。鉴证审核批准后，天威诚信或注册机构按照相关法律法规的要求妥善保管订户申请材料，订户申请材料可以是纸质或电子数据形式。

天威诚信向承担注册机构角色的机构签发与运营管理有关的管理员证书时，将通过信函、电子版扫描件等形式，向该机构的有关责任人确认该申请人来自该机构，且获得了有关申请的授权。

天威诚信保留根据国家最新的法律法规和政策的要求更新个人身份的鉴别方法与流程的权利。

3.2.4 没有验证的订户信息

天威诚信不对下列订户信息进行验证：

- 机构部门（OU）；
- 证书中指明不验证的其他信息。

3.2.5 授权的确认

对于机构证书和设备证书，天威诚信在签发前，将确认证书申请获得正当授权。确认的方式有多种，如§ 3.2.2 中对机构授权证书申请者的确认方式。

3.2.6 互操作准则

不在此规定。

3.3 密钥更新请求的标识与鉴证

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。天威诚信一般要求订户产生一个新的密钥对代替过期的密钥对，称作“密钥更新”。然而，在某些情况下，天威诚信允许订户为一个现存的密钥对申请一个新证书，称作“证书更新”。对于密钥更新而言，订户证书除公钥、有效期和序列号改变外，其他信息都没改变；对于证书更新而言，和密钥更新相比，订户证书公钥也不改变。

密钥更新和证书更新与申请一个新证书在技术上是不同的。在申请一个新证书时，证书订户需到天威诚信或其注册机构的证书服务站点申请注册，填写必要的申请信息；而对于密钥更新和证书更新，订户虽然同样需要访问天威诚信或其注册机构的证书服务站点的相应服务网页，但用户无需填写申请信息，系统会自动获取订户的有关信息。

3.3.1 常规的密钥更新的标识与鉴证

对于一般正常情况下的密钥更新，订户访问天威诚信或其注册机构的证书服务站点相应的服务网页进行密钥更新申请，系统自动获取订户原证书的相关信息，如订户甄别名、证书序列号等，形成证书密钥更新申请信息，申请信息包含新公钥并由更新前的私钥签名（对于加密证书密钥更新而言，申请信息不包含新公钥）。

天威诚信的证书认证系统将对密钥更新申请进行验证，包括验证申请签名，然后进行与新证书申请一样的鉴证。

3.3.2 吊销之后的密钥更新的标识与鉴证

天威诚信对吊销后证书不进行密钥更新。

3.4 吊销请求的标识与鉴证

在天威诚信的证书业务中，证书吊销请求可以来自订户，也可以来自天威诚信或其注册机构。证书吊销的方式可以是订户自己吊销，也可以由订户要求天威诚信或其注册机构管理员吊销，天威诚信和其注册机构在认为必要的时候，有权发起吊销订户证书。

在订户自己吊销时，吊销请求的鉴别过程如下：

订户在申请证书需提交一挑战语，在订户吊销证书时提交挑战语，如果挑战语匹配，证书吊销自动完成。

订户通过认证机构、注册机构吊销时，吊销请求的鉴别过程如下：

订户通过一定的方式，如邮件、电话等，向认证机构、注册机构提交请求，认证机构、注册机构通过与证书保障级别相应的通讯方式与订户联系，确认要吊销证书的人或组织确实是订户本人，或者其授权者。依据不同的环境，通讯方式可以采用下面的一种或几种：电话、e-mail、邮寄或快递服务。

4. 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

任何需要在各类应用中采用数字证书的个人或机构，都可以向天威诚信申请证书。

组织机构申请机构证书时，由机构被授权人员申请。

服务器证书等设备证书由个人或所属机构授权的机构中的被授权人申请。

天威诚信数字认证中心或其注册机构中进行证书审批和系统管理操作的被授权人员，可以申请管理员证书。

4.1.2 注册过程与责任

证书申请者可向天威诚信或其批准的注册机构的证书服务站点，或通过上述证书服务站点对接的证书申请平台注册并申请各类证书。天威诚信或其注册机构的证书服务站点以及对接的证书申请平台，在受理证书申请之前，应以合理的方式向申请人告知与电子认证服务有关的事项。

对于机构证书，注册时申请者须正确填写以下信息：

1）机构的真实身份标识信息，如机构法定名称、统一社会信用代码等；

2）机构授权的申请人信息，如真实姓名、身份证号码、电话、邮件地址等。

对于个人证书，注册时申请者须正确填写以下信息：

1）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、所属机构（若需要）等；

2）其他信息，如邮件地址等。

对于服务器证书等运营设备证书，注册时申请者须正确填写以下信息：

1）服务器主机名、域名、IP 地址、或设备名称、及所有者信息等；

2）申请人信息，如姓名、身份证号码、电话、邮件地址等。

对于管理员证书，注册时申请者须正确填写以下信息：

1）个人的真实身份标识信息，如个人真实姓名、所属机构、实名登记的电话号码等；

2）其他信息，如邮件地址等。

根据《中华人民共和国电子签名法》的规定，申请者未向天威诚信提供真实、完整和准确的信息，或者有其他过错，给证书依赖方、天威诚信造成损失的，承担相应的法律及赔偿责任。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

对于个人证书的申请，天威诚信及其注册机构按本 CP 和 CPS 3.2.3 所述的方式对订户进行识别和鉴别。

对于机构证书和设备证书，天威诚信及其注册机构按本 CP 和 CPS 3.2.2 所述的方式对组织机构及其授权申请人进行识别和鉴别。特别地，对组织机构代表人证书，除了按 CP 和 CPS 3.2.2 所述的方式完成对组织机构被授权的申请人的识别和鉴别外，还需按 CP 和 CPS 3.2.3 所述的方式确认包含在证书中的代表人个人信息是真实而准确的。

4.2.2 证书申请批准和拒绝

在天威诚信或其注册机构完成对证书申请的鉴证、有关鉴证获得通过且证书申请者履行了其他应尽的责任（如付款）后，天威诚信或其注册机构将批准证书申请。如果鉴证未获通过或证书申请者未履行其他应尽的责任（如付款），天威诚信或其注册机构将会拒绝该证书申请。

4.2.3 处理证书申请的时间

天威诚信及注册机构将在合理时间内完成证书请求处理。在申请者提交资料齐全且符合要求的情况下，处理证书申请的时间一般不超过两个工作日。

4.3 证书签发

4.3.1 证书签发中 RA 和 CA 的行为

作为证书认证系统的运营者，天威诚信既是一个 CA，同时也承担了部分 RA 的职能。另外，天威诚信批准的机构也承担相应的 RA 职能，处理证书服务请求。

在证书签发前 RA 管理员负责证书申请的鉴证，在证书申请通过鉴证后，RA 管理员将批准证书请求。在批准证书申请时，RA 管理员使用证书登录到 RA 系统，查询系统记录的有关请求并批准该请求。批准的信息将会发送到天威诚信的 CA 系统，CA 系统签发证书并返回给 RA 系统供证书申请者下载。

4.3.2 CA 和 RA 对订户的通知

无论是拒绝还是批准订户的证书申请，天威诚信及注册机构应将申请结果告知订户。通常情况下，RA 系统会通过电子邮件、短信或站内信等方式将申请结果通知订户；如果证书申请获得批准，通知内容中包含有获取证书的信息。

4.4 证书接受

4.4.1 构成接受证书的行为

天威诚信订户接受证书的方式可以有如下几种：

- 对于由注册机构替证书订户产生证书请求、证书密钥对、下载证书的情形，则订户通过面对面的方式从注册机构（天威诚信或其注册机构）接受载有证书和私钥的介质的行为，即表明了用户接受了证书；或者，当订户通过其他方式，如邮件快递，接收载有证书和私钥的介质后，在约定的时间内未表示异议，即表明用户接受了证书。
- 订户根据电子邮件、短信或站内信等告知的获取证书的指示信息，通过访问专门的证书下载服务站点可将证书下载到本地存放介质，如本地计算机硬盘、USB Key、智能卡。系统记录订户下载了证书即表明订户接受了证书。
- 如订户通过应用程序、应用系统、不同的终端等设备设施，包括但不限于网站、客户端、小程序等（统称“证书申请平台”）向天威诚信或天威诚信批准的注册机构申请证书的，天威诚信将证书发送至证书申请平台后，两个工作日内订户未提出异议或者订户使用了该证书的，则视为订户接受了该证书。
- 将证书用于对应的数字签名或其他密码运算时起，即视为订户接受了该证书。
- 天威诚信也可以通过其他安全的方式向订户交付证书。

4.4.2 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。

4.4.3 CA 对其他实体的通告

对于天威诚信签发的证书，天威诚信及其注册机构不通知其他实体。

4.5 密钥对和证书使用

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。

4.5.1 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，并在证书到期或吊销后，停止使用该证书及对应的私钥。

4.5.2 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，

(1) 获得数字签名对应的证书及信任链；

(2) 验证证书有效性；

(3) 确认该签名对应的证书是依赖方信任的证书；

(4) 确认证书的用途适用于对应的签名；

(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收方时，须先通过适当的途径获得接收方的加密证书，然后使用证书上的公钥对信息加密。

4.6 证书更新

4.6.1 证书更新的情形

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 天系统将会通过电子邮件、短信或站内信等方式向订户提醒用户证书将到期，如需继续使用可进行证书更新。到期前 30 天内，如果订户原来的注册信息继续有效，订户可访问天威诚信或注册机构的证书服务站点以及对接的证书申请平台申请证书更新。申请证书更新时用户无需像初次申请那样填写注册信息，系统会自动获取所需的信息。证书更新可以更换

密钥对，也可以使用原有密钥对，视更新的具体情形而定，关于证书更新与重新申请一个同样主体甄别名的新证书区别见§ 3.3。

若用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。除与订户有特殊约定或根据招投标业务场景需要外，证书到期或吊销后，将无法进行更新，只能按照初始流程重新申请证书。

4.6.2 请求证书更新的实体

同 CP 和 CPS§ 4.1.1。

4.6.3 证书更新请求的处理

对于不更换密钥的证书更新请求，用户提交的证书签名请求（PKCS#10）包含有原有证书的公钥，并由原证书私钥签名。

接收到用户的证书更新请求后，天威诚信认证系统会自动完成如下验证操作：

- 确认、验证申请对应的原证书存在并且由天威诚信认证系统签发；
- 证书更新请求在允许的期限内；
- 用原证书上的订户公钥对更新申请的签名进行验证。

若以上自动验证通过，则天威诚信或其注册机构根据证书种类的不同，分别按如下方式和过程完成证书更新请求的鉴证、批准，及新证书的签发。

对于机构证书（包括机构单位证书和机构代表人证书）和设备证书（包括服务器证书等设备证书）根据用户以前提交的注册信息，按与新证书申请一样的流程完成证书申请的鉴证，包括机构身份信息正确性、有效性的验证和确认，证书申请者及证书申请授权的确认等。在进行鉴证时，若机构用户以前提交的机构身份证明文件（如组织机构代码、营业执照）仍在其有效期内，则更新申请人可无需重新提交有关的机构身份证明文件，但天威诚信或其注册机构仍会通过第三方数据库确认有关材料是否继续有效。完成以上鉴证后，批准更新请求，签发新证书。

以上过程可以是自动或手动的。

对于个人用户证书的更新，若包含在证书中的需鉴别的信息不包含该证书用户所属组织机构，则只要该证书用户履行了应尽的责任（如支付了有关费用），则证书更新请求将获得批准，新证书将获得签发。以上过程可以是自动或手动的。若包含在证书中的需鉴别的信息包含该证书用户所属组织机构，则在批准更新请求、签发新证书前，需要确认该证书用户仍然是所属机构的人员。

对于机构雇员证书的更新，则在完成如下确认后，批准证书更新请求，签发新证书：

1）该证书用户仍然是对应机构的雇员；

2）该用户的证书更新获得了该机构的许可。

以上过程可以是自动或手动的。

对于更换密钥的证书更新，参见 4.7.3。

4.6.4 签发新证书时对订户的通知

同 4.3.2。

4.6.5 构成接受更新证书的行为

同 4.4.1。

4.6.6 CA 对更新证书的发布

同 4.4.2。

4.6.7 CA 对其他实体的通告

同 4.4.3。

4.7 证书密钥更新

证书密钥更新即产生新的密钥对，使用与原证书一样的主体甄别名并由同一签发者签发新证书。

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 天系统将会通过电子邮件、短信或站内信等方式向订户提醒用户证书将到期。如果用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或注册机构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。申请证书密钥更新时用户无需像初次申请那样填写注册信息，系统会自动获取所需的信息。

若用户希望保持证书密钥对不变，则应采用证书更新（参见 CP 和 CPS§ 4.6）。

若用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。

除与订户有特殊约定外，证书过期或吊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 CP 和 CPS§ 4.1.1。

4.7.3 证书密钥更新请求的处理

对于证书密钥更新请求，用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。

接收到用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：

- 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；
- 证书更新请求在允许的期限内；
- 用订户新的公钥对证书签名请求进行签名验证；
- 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，天威诚信或其注册机构按与证书更新相同的方式和流程（参见 CP 和 CPS§ 4.6.3）完成证书密钥更新请求的鉴证、批准，签发新的证书。

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 4.4.1。

4.7.6 CA 对密钥更新证书的发布

同 4.4.2。

4.7.7 CA 对其他实体的通告

同 4.4.3。

4.8 证书变更

4.8.1 证书变更的情形

证书变更是指在证书未到期之前，更改除公钥及有效期之外的其他信息。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，需要先将原有证书吊销，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。

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 4.4.1。

4.8.6 CA 对变更证书的发布

同 4.4.2。

4.8.7 CA 对其他实体的通告

同 4.4.3。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

出现以下情况，最终用户证书必须吊销：

- 天威诚信、注册机构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。
- 天威诚信或其注册机构有理由相信订户违背了订户协议下的义务、陈述或担保。
- 天威诚信或其注册机构和订户达成的订户协议已经终止。
- 天威诚信或其注册机构有理由相信证书签发时没有遵循 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。
- 天威诚信或其注册机构有理由相信证书申请中的信息有违背事实的错误。
- 天威诚信或其注册机构确定证书签发的一个必要前提条件既没有满足又没有豁免。
- 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。

- 订户请求吊销证书。

4.9.2 请求证书吊销的实体

以下实体可以请求吊销一个最终用户证书：

- 天威诚信、注册机构或证书订户可以在 4.9.1 所述情形下要求吊销一个最终用户证书。
- 对于个人证书，证书订户可以随时根据自己的意愿请求吊销自己的证书。
- 对于机构证书，组织机构授权的代表有资格请求吊销签发给组织机构的证书。
- 对于设备证书，拥有该设备证书的组织机构授权的代表有资格请求吊销已经签发的证书。

4.9.3 吊销请求的流程

当天威诚信或其注册机构有充分的理由相信需要吊销订户的证书时，天威诚信或其注册机构的有关人员可以通过内部确定的流程提请吊销证书。在证书吊销后，天威诚信或其注册机构将通过适当的方式，包括但不限于电子邮件等，通知订户证书已被吊销及被吊销的理由。

订户可以通过以下方式要求吊销自己的证书：

- 直接访问天威诚信或注册机构提供的证书服务网页。在订户提交吊销请求时，需同时提供证书申请时提供的挑战语作为身份鉴别的信息。这种方式适用于所有类别的证书。
- 通过电子邮件、特快专递等可靠的方式告知天威诚信或其注册机构。

天威诚信收到订户的吊销申请资料后，将查询订户需吊销的证书是否为天威诚信签发，证书是否在有效期内，审核通过后则对证书进行吊销。

4.9.4 吊销请求宽限期

当订户发现出现 4.9.1 中的情况时，应该及时向天威诚信或其注册机构提出吊销请求。

4.9.5 CA 处理吊销请求的时限

一般情况下，天威诚信或注册机构从接到吊销请求及吊销申请材料并完成审核后，24 小时内吊销证书。

4.9.6 依赖方检查证书吊销的要求

依赖方应当检查他们所信任的证书是否被吊销。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 产生证书吊销列表，也可根据订户需要定制证书吊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。如果吊销 CA 证书，天威诚信在吊销后 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。

4.9.11 吊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 来查询证书吊销信息。

4.9.12 密钥损害的特别要求

无论是订户还是天威诚信、注册机构，发现证书密钥受到安全损害时应立即吊销证书。

4.9.13 证书挂起的情形

天威诚信不提供证书挂起。

4.9.14 请求证书挂起的实体

不适用。

4.9.15 挂起请求的流程

不适用。

4.9.16 挂起的期限限制

不适用。

4.10 证书状态服务

证书的状态（有效、吊销）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：

- CRL 通过 80 端口采用 HTTP 协议提供；
- OCSP 符合 RFC6960，反映证书的当前状态；
- 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。

4.10.3 可选特征

无。

4.11 订购结束

当证书到期或证书被吊销则认证机构、注册机构与订户关系结束。

4.12 密钥托管与恢复

天威诚信依国家密码管理局的相关规定，提供加密证书密钥的集中产生、保存和恢复。

4.12.1 密钥托管与恢复的策略与行为

订户加密证书密钥对由天威诚信的密钥管理中心系统集中产生和保存，密钥恢复是一种严格受控的过程，只有在如下情况下才允许进行密钥恢复：

1）证书持有者提出申请；

2）注册机构提出申请，并有充分的理由；

3）国家执法、司法机构因执法、司法的需要；

4）国家其他管理部门管理需要。

密钥恢复只有在必须的情况下才进行，并且申请要提出充分的理由和提供有关文件、材料。

4.12.2 会话密钥的封装与恢复的策略与行为

会话密钥是指用户在使用证书建立加密通道时临时生成的加密密钥，该密钥由应用环境来决定使用，天威诚信不对其进行保存和恢复。

5. 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

天威诚信的 CA 机房运营场地位于北京市和长沙市，天威诚信的 CA 机房和系统建设按照 GB/T 25056-2010《信息安全技术证书认证系统密码及其相关安全技术规范》规定实施。

天威诚信 CA 机房按功能分为四个区域，由外到里分别是：公共区、管理区、服务区和核心区。

5.1.2 物理访问控制

天威诚信的服务区、管理区、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：

- 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；
- 进出每一道门都有日志记录；
- 服务区、管理区、和核心区的门都设有强开报警和超时报警；
- 整套门禁系统连接 UPS，在市电中断时由 UPS 提供紧急供电。

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。

5.1.3 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 小时正常供电及在出现供电系统出现供电中断是能够提供正常的服务。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℃。

5.1.4 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。

5.1.5 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。

在自动状态下，当防护区发生火警时，火灾报警控制器接到防护区两独立火灾报警信号后立即发出联动信号。经过 30 秒时间延时，火灾报警控制输出信号，启动灭火系统，同时，报警控制器接收压力讯号器反馈信号，防护区内门灯显亮，避免人员误入。

当防护区经常有人工作时，可以通过防护区门外的手动/自动转换开关，使系统自动状态转换到手状态，当防护区发生火警时，报警控制器只发出报警信号，不输出动作信号。由值班人员确认火警，按下控制面板或击碎防护区外紧急启动按钮，即可立即启动系统，喷发气体灭火剂。

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。

5.1.6 介质存储

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）。

5.1.7 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。

5.1.8 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，该备份地点的安全级别不低于实际生产环境。

5.2 程序控制

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、管理和吊销等涉及密钥操作的职位都视为可信角色。这些角色包括但不限于：

1)密钥与密码设备管理人员，负责维护 CA 密钥和证书生命周期，负责管理密码设备；

2) 鉴证人员，负责订户信息录入、审核数字证书申请信息并完成鉴证和审批工作；

3) 系统维护人员，负责对 CA 系统的硬件和软件实施日常维护，并监控和排查故障；

4) 安全管理人员，负责场地安全、日常安全管理工作；

5) 安全审计人员，负责对业务操作行为进行审计；

6) 人力资源管理人员，负责对关键岗位人员实施可信度背景调查、安全管理等工作。

5.2.2 每项任务需要的人数

天威诚信对业务操作流程有严格的控制程序，按照本 CP 和 CPS 第 5.2.4 节的职责分割策略，确保个人不能同时承担多项重要角色，且敏感操作需要多个可信人员共同完成，这包括：

1) 屏蔽区场地访问设置为双人进出模式；

2) 保存根密钥激活数据的保险柜设置为双人开启模式；

3) 密码设备的管理权限按照 5 选 3 方式进行分割，并由不同可信人员持有；

4) 鉴证过程至少两名可信人员参与。

5.2.3 每个角色的识别与鉴别

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。

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

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。

5.2.4 需要职责分割的角色

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。

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：

1) 具备良好的社会和工作背景；

2) 遵守国家法律、法规，无违法犯罪记录；

3) 遵守天威诚信有关安全管理的规范、规定和制度；

4) 具有认真负责的工作态度和良好的从业经历；

5) 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：

1) 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。
2) 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。
3) 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：
   - 存在捏造事实或资料的行为；
   - 借助不可靠人员的证明；
   - 使用非法的身份证明或者学历、任职资格证明；
   - 工作中有严重不诚实的行为。
4) 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。
5) 天威诚信与员工签订保密协议，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 培训要求

为了使有关人员能胜任其承担的工作，天威诚信对所有可信角色岗位的员工制定有专门的培训计划，培训内容包括：

1) 天威诚信颁布的证书策略和电子认证业务规则；
2) PKI 基本知识；
3) 天威诚信运营体系、技术体系和安全管理制度；

4) 工作职责和岗位说明。

5.3.4 再培训周期和要求

对于充当可信角色或其他重要角色的人员，每年至少接受天威诚信组织的培训一次。对于认证系统运营相关的人员，每年至少进行一次相关技能和知识培训。此外，天威诚信将根据机构系统升级、策略调整等要求，不定期的要求人员进行继续培训。

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

天威诚信对如下几类事件进行记录：

- CA 密钥生命周期的管理事件，包括，
  - 密钥生命周期的管理事件，例如生成、备份、存储、恢复和归档。

- 密码设备生命周期的管理事件，例如接收、使用和销毁。

这些记录都是密钥管理员完成的手工记录。

- CA 和订户证书生命周期的管理事件，包括，
  - 证书的申请、批准、更新、吊销等。
  - 成功或失败的证书操作。

这些记录由认证系统的系统日志和操作人员的手工记录组成。

- 系统操作事件，包括，
  - 系统启动和关闭。
  - 系统权限的创建、删除、变更、和密码修改。

这些记录由认证系统的系统日志和操作人员的手工记录组成。

- 系统安全事件，包括，
  - 成功或不成功访问 CA 系统的活动。
  - 对于 CA 系统网络的非授权访问及访问企图。
  - 系统崩溃，硬件故障和其他异常。
  - 防火墙记录的安全事件。

这些记录由系统的自动日志和操作人员的手工记录组成。

- 天威诚信场地的工作记录，如，
  - 授权人员进出。
  - 非授权人员进出及陪同人。
  - 场地设施的维护操作。

这些记录由系统的自动日志和操作人员的手工记录组成。

日志记录一般包括如下信息：

- 每个日志记录的日期和时间。
- 对于自动日志记录，登记的序列号或序号。
- 做日志记录的实体的身份。
- 日志记录的内容。

5.4.2 处理日志的周期

对于系统的自动日志和操作人员的手工记录，天威诚信每月进行一次检查和汇总。

对系统安全日志，每月进行一次跟踪处理，检查违反策略和规范的重大事件。

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。

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

根据审计发现的安全事件，天威诚信将每年对系统、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。

5.5 记录归档

5.5.1 归档记录的类型

天威诚信归档所有审计日志（如第 5.4.1 节所述）。 此外，还对以下资料进行归档：

1) 与证书系统安全性相关的文档；
2) 与证书申请和证书的鉴别和验证、颁发和吊销相关的文档；
3) CP 和 CPS；
4) 员工资料，包括但不限于背景调查、录用、培训等资料；
5) 各类外部、内部评估文档。

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。

- 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。
- 订户证书的归档保留期限不少于证书失效后 5 年。
- 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。
- 其它记录保留 1 年。

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。

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 CA 密钥变更

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：

- 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”）。
- 产生新的密钥对，签发新的上级 CA 证书。
- 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。

- 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。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

天威诚信已制定各种应急处理方案，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：

- 认证系统应急方案；
- 电力系统应急方案；
- 消防应急方案；
- 网络与信息系统应急方案；
- 密钥应急处理方案等。

相关岗位的工作人员将按照相关制度和应急方案，定期进行应急演练。

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：

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，并立即访问天威诚信或相应的注册机构的证书服务网站吊销其证书，或者立即通过电话、电子邮件的方式通知天威诚信或注册机构吊销其证书。天威诚信按 § 4.9 发布证书吊销信息。

2）当天威诚信或注册机构发现证书订户的实体证书私钥受到损害时，天威诚信或注册机构将立即吊销证书，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 发布证书吊销信息。

3）当天威诚信的 CA 证书或其受委托的 CA 证书出现私钥损害时，天威诚信将立即吊销该 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 CA 或 RA 的终止

当天威诚信及其注册机构需要停止其业务时，将会严格按照《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进行有关工作。

在天威诚信终止前，必须：

1) 确定业务承接单位；
2) 起草终止声明；
3) 通知相关实体；
4) 处理存档文件记录；
5) 停止 CA 系统服务；
6) 存档相关系统日志；
7) 处理和存储敏感文档。

6. 技术安全控制

6.1 密钥对的产生和安装

6.1.1 密钥对的产生

6.1.1.1 CA 密钥对的产生

天威诚信 CTN 根体系和国密根体系所有 CA 证书密钥对均在天威诚信 CA 机房产生，密钥使用通过商密检测认证的密码设备生成，私钥由天威诚信自身持有和保存。

CA 密钥对的生成过程，由天威诚信专门的密钥管理员和若干名可信雇员，在天威诚信屏蔽机房按照天威诚信密钥生成规程完成。天威诚信密钥生成规程规定了 CA 密钥产生的流程控制及参加人员。

6.1.1.2 订户密钥对的产生

对于个人证书和机构证书，订户根据不同业务场景，选择不同生成方式，并确保密钥生成的可靠性和私钥存储的安全性。订户密钥对的产生方式，可能根据最新国家政策法规的要求进行调整。

对于设备证书，天威诚信或其注册机构将使用专门的程序软件在通过商密检测认证的密码模块（如加密卡或加密机）中生成密钥对。

6.1.2 私钥传送给订户

对于天威诚信签发的订户证书，私钥在客户端生成的，不存在传送私钥给订户的情形；其他如涉及订户私钥传送，应确保传送过程的安全性。

天威诚信各种运营设备证书的密钥对由天威诚信或其注册机构在设备所在地产生，并在本地保存，不存在传送私钥的情形。

6.1.3 公钥传送给证书签发机关

订户或订户通过注册机构，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套接层协议（SSL）或其他安全加密方式。

6.1.4 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：

1）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；

2）天威诚信、注册机构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；

3）天威诚信、注册机构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。

6.1.5 密钥的长度

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

6.1.6 公钥参数的生成和质量检查

公钥参数使用通过商密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，由于使用通过商密检测认证的密码模块生成和存储密钥，相关算法和协议参数符合国家密码管理局相关要求。

6.1.7 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。订户的签名密钥可用于提供身份认证、以及信息完整性等目的，加密密钥可用于信息加密和解密。

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

天威诚信的密钥使用通过商密检测认证的密码设备生成，该设备对密钥的生成、管理、存储、备份和恢复遵循国家密码管理局相关规范要求。

CA 密钥对的生成过程，由天威诚信专门的密钥管理员和若干名可信雇员，在天威诚信屏蔽机房按照天威诚信密钥生成规程完成。天威诚信密钥生成规程规定了 CA 密钥产生的流程控制及参加人员。

订户证书的密钥使用通过商密检测认证的密码模块生成和存储，订户应妥善保护、保管其密码模块、激活数据等，防止其失窃、丢失、损坏及被非授权的使用。

6.2.2 私钥多人控制（m 选 n）

天威诚信的各类 CA 私钥的生成、备份和恢复等操作采用多人控制机制，此机制通过密码设备的 5 选 3 分割管理权限实现，即将私钥的管理权限分割保存在 5 个介质中（称为秘密分割份额，或简称秘密分割），这 5 个介质由天威诚信 5 名可信雇员持有（称为秘密分管者），保存在天威诚信内部保险盒中。当需要使用管理员权限时，至少在其中 3 名秘密分管者在场并许可的情况下，插入管理员介质并输入 PIN 码，才能对私钥进行备份恢复等操作。当不使用时，这个被称为秘密分割份额存储在屏蔽机房的保险盒中。

天威诚信的 CA 私钥的激活需要由密钥管理者持有的操作员管理介质。介质保存在天威诚信屏蔽机房的保险盒中，在需要激活 CA 私钥时才使用。

6.2.3 私钥托管

天威诚信所有 CA（包括根 CA 和运营 CA）的私钥均未在其他地方托管。

根据国家密码管理局的要求，天威诚信的用户的加密证书私钥托管在天威诚信密钥管理系统中。

6.2.4 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管理员操作员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。

6.2.5 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 CP 和 CPS § 6.2.1 所述的密码设备中，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 CP 和 CPS§ 6.2.10 销毁。

天威诚信根据国家密码管理局要求，对订户加密证书的私钥进行归档；天威诚信不对订户用于签名的证书私钥进行归档；如果订户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归档，并对归档的私钥采用口令或其他访问控制机制保护，防止非授权的泄露。

6.2.6 私钥导入、导出密码模块

天威诚信 CA 密钥对在密码设备上生成，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（软件或硬件）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。

6.2.7 私钥在密码模块的存储

天威诚信 CA 私钥使用通过商密检测认证的密码设备生成和存储，且私钥的使用也在密码设备中进行。

对于订户证书，订户应将私钥保存在通过商密检测认证的密码模块中，且存放私钥的密码模块必须在订户其可控制的范围内，订户需要采取相应的安全手段防止对私钥的非授权访问、获取和使用，使用的手段包括私钥的使用受口令保护，服务器及密码模块位于安全可控的物理环境等。

6.2.8 激活私钥的方法

天威诚信 CA 私钥存放在密码设备中，激活需要按本 CP 和 CPS 第 6.2.2 节使用密码设备的操作员权限实现，即需要密钥管理员提供操作员介质进行激活。

订户证书私钥需在订户提供 PIN 码等激活数据，或通过短信验证等方式授权后才能被激活和使用。订户密钥对的激活方法，可能根据最新国家政策法规的要求进行调整。

6.2.9 解除私钥激活状态的方法

对于天威诚信 CA 私钥，当 CA 系统向密码设备发出退出登录或密码管理软件向密码设备发出关闭指令，或存放私钥的密码设备断电，私钥进入非激活状态。

订户解除私钥激活状态由其自行决定，当服务程序关闭、系统注销或系统断电后私钥即进入非激活状态。

6.2.10 销毁私钥的方法

在天威诚信 CA 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密码设备中，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 私钥从密码设备中彻底删除，不留有任何残余信息。

订户应在其证书私钥不再使用后将私钥销毁，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吊销、到期作废后，还需要用于信息解密的，订户应妥善保存一定期限，以便于解开加密信息。

6.2.11 密码模块的评估

天威诚信使用通过商密检测认证的密码产品，符合国家相关标准。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

天威诚信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。

6.3.2 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。

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。

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。

当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

6.4 激活数据

6.4.1 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：

- 至少 8 位字符或数字；
- 至少包含一个字符和一个数字；
- 不能包含很多相同的字符；
- 不能和操作员的名字相同；
- 不能包含用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。

6.4.2 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管理，存储在天威诚信屏蔽机房保险盒中。

订户的激活数据必须在安全可靠的环境下产生，必须进行妥善保管，或者记住以后进行销毁，不可被他人所获悉。如果证书订户使用口令或 PIN 码保护私钥匙，订户应妥善保管好其口令或 PIN 码，防止泄露或窃取。如果证书订户使用生物特征保护私钥，订户也应注意防止其生物特征被人非法窃取。

6.4.3 激活数据的其他方面

存有天威诚信数字认证中心 CA 私钥的激活数据的介质，通常保存在天威诚信的屏蔽机房内，不能携带外出或传送。如因某种特殊情况确实需要传送时，其传送过程需在天威诚信两名可信人员的监督下进行。

通常情况下订户证书私钥的激活数据由订户自己产生、保管，不应传送给其他人员，若私钥激活数据因特别的原因需要进行传送时，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。

对于申请证书的订户激活数据的生命周期，建议如下：

1、订户用于申请证书的口令，申请成功后失效。

2、用于保护私钥或者介质、USB Key 的口令，建议订户根据业务应用的需要随时予以变更，使用期限超过 3 个月后应进行修改。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

CA 系统的信息安全管理，按照国标《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。主要的安全技术和控制措施包括：身份识别和验证、逻辑访问控制、网络访问控制等。

对每位拥有系统（包括 CA 系统、RA 系统）业务操作权限的可信人员实行严格的双因素验证机制，即访问时同时采用用户名、口令以及数字证书双因素登录方式。

对系统运维人员，通过堡垒机登录系统实施操作，确保 CA 软件和数据文件安全可信，不会受到未经授权的访问。

核心系统必须与其他系统物理分离，生产系统与其他系统逻辑隔离。这种分离可以阻止除指定的应用程序外对网络的访问。使用防火墙阻止从内网和外网入侵生产系统网络，

限制访问生产系统的活动。只有 CA 系统操作与管理组中的、有必要工作需要、访问系统的可信人员可以通过口令访问 CA 数据库。

6.5.2 计算机安全评估

天威诚信的 CA 系统及其运行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。

CA 系统使用的网络设备、安全设备等具备国家相关安全标准资质。

6.6 生命周期技术控制

6.6.1 系统开发控制

天威诚信 CA 系统部署了通过商密检测认证的 CA 软件，并通过严格的内部变更控制流程、规范的运维审批与上线流程等措施，确保系统安全与可用：

1) 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；
2) 申请部署时需要提供 changelog、测试报告、部署说明等文档；
3) 部署上线前根据规范要求进行审批；
4) 变更部署前进行有效的在线备份；
5) 变更部署后应立即进行测试，通过测试后方可对外服务。

6.6.2 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。

6.6.3 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。

6.7 网络的安全控制

天威诚信的认证系统采用防火墙进行系统的访问控制，采用 IDS\IPS 进行网络的攻击防御，使用堡垒机对远程登录进行权限管理，使用路由器进行网络分层控制。

认证系统应仅对指定的服务或人员开放，且只开放最小的访问权限。

6.8 时间戳

天威诚信认证系统签发的数字证书、CRL 包含有日期信息，且这些日期信息是经过数字签名的。

认证系统日志、操作日志都有相应的时间标识。这些时间标识不需要采用基于密码的数字时间戳技术。

认证系统所取的时间源是国家可信标准时间。

7. 证书、CRL 和 OCSP

7.1 证书

天威诚信签发的证书符合 ITU-T X.509v3 和 RFC 5280：Internet X.509 公钥基础设施证书和 CRL 结构。

7.1.1 版本号

证书符合 X.509 V3 版证书格式，版本信息存放在证书版本格式栏内。

7.1.2 证书扩展项

证书扩展项是一个或多个证书扩展的序列。针对某些证书，天威诚信签发的证书可能包含私有扩展项，不能识别私有扩展项的应用、依赖方可以忽略该扩展项。

7.1.2.1 密钥用法（Key Usage）

该扩展项指定证书密钥对的用法。这个扩展项的 criticality 域通常设置为 TRUE。

7.1.2.2 证书策略扩展项（Certificate Policies）

证书策略扩展项中有天威诚信证书策略中对应证书类的 CP 对象标识符及策略限定符。这个扩展项的 criticality 域设置为 FALSE。

7.1.2.3 主体备用名（subjectAltName）

扩展项的使用符合 RFC 3280。此扩展项的 criticality 设为 FALSE。

7.1.2.4 基本限制扩展项（BasicConstraints）

天威诚信 CA 证书的基本限制扩展项中的主体类型被设为 CA。最终用户证书的基本限制扩展项的主体类型设为最终实体 (End-Entity)。这个扩展项的 criticality 域设置为 TRUE。

7.1.2.5 扩展的密钥用法（Extended Key Usage）

扩展密钥用法指公钥可用于一种或多种用途，作为对密钥用法扩展项中指明的基本用途的补充或替代。此扩展项的 criticality 设为 FALSE。

7.1.2.6 CRL 的分发点（cRLDistributionPoints）

天威诚信签发的证书中包含 CRL 的分发点扩展项，依赖方可根据该扩展项提供地址和协议下载 CRL。此扩展项的 criticality 项设为 FALSE。

7.1.2.7 签发 CA 密钥标识符

天威诚信最终用户证书及中级 CA 证书中有签发 CA 密钥标识符扩展项，该值由证书签发者的公钥产生。这个扩展项的 criticality 域设置为 FALSE。

7.1.2.8 主体密钥标识符

当证书包含主体密钥标识符扩展项时，该值由证书主体的公钥产生。使用该扩展项时，其扩展项的 criticality 域设为 FALSE。

7.1.3 密钥算法对象标识符

符合国家密码管理局批准的算法对象标识符。

7.1.4 名称形式

天威诚信签发证书的甄别名符合 X.500 关于甄别名的规定。对于证书主体甄别名，O 代表证书持有者所在的组织机构，第一个 OU 代表证书持有者所在的部门。

对于证书签发者甄别名，O 代表证书签发机构，第一个 OU 签发机构体系名称或密钥算法名称。

甄别名可能包含不止一个的 OU 用于存放自定义信息。

7.1.5 名称限制

除特定场景下的个别证书外，天威诚信签发的证书中的通用名不能使用假名、伪名。

7.1.6 证书策略对象标识符

天威诚信证书策略对象标识符存放在证书内证书策略相关项内，详见证书模版。

7.1.7 策略限制扩展项的用法

无规定。

7.1.8 策略限定符的语法和语义

无规定。

7.1.9 关键证书策略扩展项的处理规则

无规定。

7.2 CRL

天威诚信认证系统签发的 CRL 符合 RFC3280 标准。

7.2.1 版本号

X.509 V2。

7.2.2 CRL 和 CRL 条目扩展项

与 ITU X.509 和 RFC3280 规定一致。

7.3 OCSP

天威诚信认证系统可根据订户需要提供该项服务。

7.3.1 版本号

V1。

7.3.2 OCSP 扩展项

与 RFC6960 一致。

8. 认证机构审计和其他评估

天威诚信数字认证中心在物理控制、密钥管理、操作控制、证书生命周期管理等方面的执行等情况将被审查、评估，以确定实际发生情况是否与预定的标准、要求一致，称为一致性审计，并根据审查结果采取行动。

8.1 评估的频率和情形

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。

8.2 评估者的资质

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。

8.3 评估者与被评估者之间的关系

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。

8.4 评估的内容

内部审计工作涉及以下内容：

1) 运营工作流程和制度是否得到严格遵守；
2) 是否严格按 CP 和 CPS、业务规范和安全要求开展认证业务；
3) 各种日志、记录是否完整，是否存在问题；
4) 是否存在其他可能存在的安全风险。

外部审计由第三方机构按照 GB／T 19001-2016 (ISO 9001-2015)质量管理体系要求和 GB／T 22080-2016 (ISO ／ IEC27001-2013)信息技术安全技术信息安全管理体系要求对天威诚信进行独立审计。

8.5 对问题与不足采取的措施

对于本机构内部审计结果中的问题，由审计评估小组负责监督相关责任部门的改进情况。

外部审计评估完成后，天威诚信按照其审计报告进行整改。

8.6 评估结果的传达与发布

内部审计结果向本机构各责任部门进行正式通报，对可能造成的订户安全隐患，天威诚信将及时向订户通报。

外部审计评估完成后，由第三方机构向天威诚信提供审计报告，天威诚信按照报告完成整改工作和再评估后，天威诚信将在官网公布最终审计结果（认证证书）。

8.7 其他评估

根据《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》等要求，天威诚信还将接受主管部门的检查。

9. 其他业务和法律事务

9.1 费用

9.1.1 证书签发和更新费用

天威诚信可根据提供的证书相关服务向本机构的证书订户收取费用，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 证书查取的费用

在证书有效期内，天威诚信不对证书查询收取专门的费用。如果用户提出特殊需求，可能需要支付额外的费用，将由天威诚信营销部门与用户协商收取。

9.1.3 证书吊销或状态信息的查询费用

证书吊销和吊销列表（CRL）的获取不收取任何费用。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。

9.1.4 其他服务费用

如果天威诚信向订户提供证书存储介质及相关服务，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。

9.1.5 退款策略

如果由于天威诚信的原因，造成订户合同无法履行、订户证书无法使用，天威诚信会将有关费用返还给订户。

9.2 财务责任

9.2.1 保险范围

天威诚信向证书订户提供证书使用保障。如果由于天威诚信原因造成用户使用证书过程中遭受损失，天威诚信公司将向证书订户、依赖方提供赔偿（具体情形参见 9.9）。

9.2.2 其他资产

天威诚信具备国家信息产业主管部门所规定的资金实力，具备承担赔偿责任的条件。

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）。

最终实体欲向天威诚信提出索赔，在证书有效期内产生的损失，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。

天威诚信对按照本 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

天威诚信有专门的信息保密制度，保护自身和客户的敏感信息、商业秘密。

9.3.1 保密信息范围

在天威诚信提供的电子认证服务中，以下信息视为保密信息：

1） 天威诚信订户的私钥及解密密钥。

2） 审计记录包括：本地日志、服务器日志、归档日志的信息，这些信息被天威诚信视为保密信息，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。

3） 其他由天威诚信和注册机构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：

1） 由天威诚信发行的证书和 CRL 中的信息。

2） 由天威诚信支持、CPS 识别的证书策略中的信息。

3） 天威诚信许可的只有天威诚信订户方可使用的、在天威诚信网站公开发布的信息。

4） 其它天威诚信信息的保密性取决于特殊的数据项和申请。

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。

CA、注册机构、订户以及与认证业务相关的参与方等，都有义务按照本 CP 和 CPS 的规定，承担相应的保护保密信息的责任，必须通过有效的技术手段和管理程序对其进行保护。

当保密信息的所有者出于某种原因，要求天威诚信公开或披露他所拥有的保密信息时，天威诚信应满足其要求；同时，天威诚信将要求该保密信息的所有者对这种申请进行书面授权，以表示其自身的公开或者披露的意愿。如果这种披露保密信息的行为涉及任何其他方的赔偿义务，天威诚信不应承担任何与此相关的或由于公开保密信息所造成的损失。保密信息的所有者应承担与此相关的或由于公开保密信息引起的所有赔偿责任。

当天威诚信在任何法律、法规、法院以及其他公权力部门通过合法程序的要求下，必须提供本 CP 和 CPS 中规定的保密信息时，天威诚信应按照法律、法规以及法院判决的要求，向执法部门公布相关的保密信息，天威诚信无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

9.4 个人隐私保密

9.4.1 隐私保密方案

天威诚信尊重证书订户的资料的隐私权，保证完全遵照国家对隐私保护的相关规定及法律。同时，天威诚信将确保全体职员严格遵从内部工作相关制度和规定。

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注册证书中提交的、但不在证书中显示的信息，如联系电话、地址、个人与天威诚信、天威诚信注册机构签订的协议等。

9.4.3 不被视为隐私的信息

不被认为是隐私信息包括，要出现在证书中的信息、证书及证书状态信息。

9.4.4 保护隐私的责任

除非执法、司法方面的强制需要，天威诚信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

天威诚信将采取适当的步骤保护证书订户的个人隐私，并将采取可靠的安全手段保护已存储的个人隐私信息。

天威诚信及其注册机构如需超出约定范围及用途使用证书订户的隐私信息，应事先告知证书订户并获得同意及授权；如未获得同意及授权，天威诚信不会将订户隐私信息透露给任意第三方。

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、决定、命令等，由于司法执行或法律授权的行政执行需要，天威诚信及其注册机构有可能需要将有关信息在订户知晓或不知晓的情况下提供有关执法机关、行政执行机关。即使出现这种情形，天威诚信及其注册机构也将尽可能地保护客户隐私信息。

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

天威诚信享有并保留对天威诚信签发的数字证书以及天威诚信通过网站等各种渠道对外公布并提供的所有软件、资料、数据、信息等的著作权、专利权等知识产权。

天威诚信对数字证书系统软件享受所有权、名称权、利益分享权；对所签发的证书、证书吊销列表及其中的信息享有拥有知识产权。

天威诚信对本 CP 和 CPS 及相关的运营管理工作文件拥有知识产权。

证书订户对证书注册信息及签发给他的证书中包含的商标、服务标志或商品名和甄别名拥有知识产权。

证书中的密钥对是证书中主体对应实体或实体拥有者的知识产权。

9.6 陈述与担保

9.6.1 CA 的陈述与担保

天威诚信在提供电子认证服务活动过程中对订户的承诺如下：

1) 签发给订户的证书符合本 CP 和 CPS 的所有实质性要求。

2) 将向证书订户通报任何已知的，将在本质上影响订户的证书的有效性和可靠性事

件。

3) 将根据 CP 和 CPS 的要求及时吊销证书。

证书公开发布后，天威诚信保证除未经验证的订户信息外，证书中的其他订户信息都是准确的。

天威诚信不负责评估证书是否在适当的范围内使用，订户和依赖方依照订户协议和依赖方协议确保证书用于允许使用的目的。

9.6.2 RA 的陈述与担保

天威诚信认证机构的注册机构做出如下担保：

1) 提供给订户的注册过程符合天威诚信制定的 CP 和 CPS 的所有实质性要求。

2） 注册机构应按照天威诚信的 CP 和 CPS 要求，及时向天威诚信提交证书申请、更新、恢复和吊销等服务请求。

3）注册机构对于无论是拒绝还是批准订户的证书申请、证书及密钥更新以及证书吊销等，有向订户进行告知的义务。

4）注册机构在批准证书前，完成了所有必要的鉴证工作，并且确认了信息是正确的、准确的。对于订户的信息以及认证相关的信息，注册机构应按照相关法律法规的要求进行妥善保存，并适时提交天威诚信进行归档。

5）注册机构应当向订户就证书的相关事项进行告知，并且在订户完全知晓、同意天威诚信 CP 和 CPS、订户协议的前提下，为订户办理证书。

6）在天威诚信需要的任何情况（包括但不限于：监管要求、客户投诉、诉讼案件及其他情况）下，注册机构都应积极配合天威诚信提供订户的相关授权文件以及鉴证资料。

9.6.3 订户的陈述与担保

作为获得证书的一个条件，证书申请者在证书申请时已阅读了订户协议并且同意订户协议，并且：

- 在证书申请时，订户的所有陈述都是对的，订户的陈述内容发生变化时应及时通知天威诚信和天威诚信的注册机构；

- 订户申请、使用证书的行为是符合订户真实意愿或者为了处理已获取授权的事务；
- 订户提供的，特别是包含在证书中的需要鉴别、验证的信息是真实的、准确的。

在证书的保存和使用过程中，订户同意做到：

- 按照天威诚信 CP、CPS 将证书用于规定的使用目的，不将证书用于证书使用目的以外的场合；
- 利用与证书中的公钥相对应的私钥产生的数字签名是订户的数字签名，订户知晓要签名的内容，产生数字签名时，订户已经接受了证书，且该证书没有过期或吊销。
- 订户对使用私钥的行为负责，并对自己的私钥进行了有效的保护，其他人员未经授权无法使用订户的私钥。
- 一旦发生任何可能导致安全性事件的危机情况时，如：私钥遗失、遗忘、泄露以及其他类似情况，订户应立刻通知天威诚信机构和注册机构，申请采取吊销等处理措施。

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，在信赖证书所证明的信任关系前确认该证书记载的内容与所要证明的内容一致，采取合理措施，查证了订户数字证书及数字签名的有效性，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

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

有下列情形之一的，应免除天威诚信之担保责任，天威诚信不向任何方承担任何法律责任，包括但不限于赔偿责任及补偿责任。

1) 订户在申请和使用天威诚信数字证书时，有违反如下义务之一的：
   - 订户有义务提供真实、完整、准确的材料和信息，不得提供虚假、无效的材料和信息；
   - 订户应当妥善保管天威诚信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、安全的系统；
   - 订户知悉私钥已经失密或者可能已经失密时，应当及时告知天威诚信及相关各方，并终止使用该证书；
   - 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。不得将数字证书用于天威诚信规定使用范围外的其他任何用途使用；
   - 订户必须在证书有效期内使用该证书；不得使用已失密或可能失密、已过有效期、被冻结、被吊销的数字证书；
   - 订户有义务根据规定按时向天威诚信交纳服务费用。
2) 由于不可抗力原因而导致数字证书签发延迟、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：
   - 自然现象或者自然灾害，包括地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；
   - 社会现象、社会异常事件或者政府行为，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) 因天威诚信的设备或网络故障等技术故障而导致数字证书签发延迟、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“技术故障”引起原因包括但不限于：
   - 不可抗力；

- 关联单位如电力、电信、通讯部门而致；
- 黑客攻击；
- 天威诚信的设备或网络故障。

4) 天威诚信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

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，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。

9.9 赔偿

天威诚信只对由于自身原因造成证书订户、依赖方的直接损失承担责任，对间接损失不承担责任。

天威诚信对于直接损失所负法律责任的上限为：在任何情况下每张证书赔偿额不得超过证书购买价格的 3 倍。

如天威诚信违反了本 CP 和 CPS 第 9.6.1 节中的陈述，证书订户、依赖方等最终实体可以申请赔偿（法定或约定免责除外）。如出现下述情形，天威诚信承担有限赔偿责任：

1） 天威诚信将证书错误的签发给订户、证书申请平台或天威诚信批准的注册机构之外不相关的第三方，导致订户或依赖方遭受损失的；

2） 在订户提交信息或资料真实、完整、准确的情况下，天威诚信签发的证书出现了错误信息，导致订户或依赖方遭受损失的；

3） 在天威诚信明知订户提交信息或资料存在虚假谎报的情况，但仍然向订户签发证书，导致依赖方遭受损失的；

4） 由于天威诚信的原因导致证书私钥被破译、窃取、泄露，导致订户或依赖方遭受损失的；

5） 天威诚信未能及时吊销证书，导致依赖方遭受损失的。

另外，天威诚信赔偿限制如下：

1） 天威诚信所有的赔偿义务不得高于天威诚信所承担的上限额度，这种赔偿上限可以由天威诚信根据情况重新制定，天威诚信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，天威诚信不承担任何赔偿责任，由订户或依赖方自行承担。

3） 在证书有效期内产生的损失，订户或依赖方应在知道或应当知道损失发生之日起三年内向天威诚信书面提出索赔；超出三年的，该索赔无效。

订户有下列情形之一，给天威诚信、依赖方造成损失的，应当承担赔偿责任：

1） 订户申请注册证书时，因故意、过失或者恶意提供不真实、不完整、不准确资料，造成天威诚信及其授权的注册机构或者第三方遭受损害；

2） 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有及时告知天威诚信及其注册机构以及不当交付他人使用造成天威诚信及其注册机构、第三方遭受损害；

3） 订户使用证书的行为，有违反本 CP 和 CPS 及相关操作规范，或者将证书用于非本 CP 和 CPS 规定的业务范围；

4） 自证书订户或者其他有权提出吊销证书的实体提出吊销请求，至天威诚信将该证书吊销信息予以发布期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果天威诚信按照本 CP 和 CPS 的规范进行了有关操作，那么该证书订户必须承担吊销信息发布之前的所有损害赔偿责任；

5） 证书中的信息发生变更但未停止使用证书并及时通知天威诚信和依赖方；

6） 没有对私钥采取有效的保护措施，导致私钥丢失或被损害、窃取、泄露等；

7） 在得知私钥丢失或存在危险时，未停止使用证书并及时通知天威诚信和依赖方；

8） 超出证书有效期限使用证书的；

9） 订户的证书信息侵犯了第三方的知识产权；

10） 在规定的范围及目的外使用证书，如从事违法犯罪活动的。

在如下情况，依赖方对自身原因造成的天威诚信损失承担责任：

1） 依赖方没有执行天威诚信与依赖方的协议或本 CP 和 CPS 规定的义务，导致天威诚信及注册机构或第三方遭受损害；
2） 未能依照本 CP 和 CPS 规定对证书进行合理审核，导致天威诚信及注册机构或第三方遭受损害；
3） 依赖方没有对证书的信任链进行验证，导致天威诚信及注册机构或第三方遭受损害；
4） 依赖方没有确认证书是否被吊销，导致天威诚信及注册机构或第三方遭受损害。
5） 在不合理的情形或环境下信赖证书，如依赖方明知证书存在超范围、超期限使用的情形或证书已经或有可能被人窃取的情形，但仍然信赖证书。

有下列情形之一的，天威诚信不承担赔付责任：
1） 因订户原因致使依赖方遭受损失的；
2） 依赖方未经检验证书的状态即决定信赖证书的；
3） 依赖方明知或者应当知道证书存在超范围使用、超期限使用、被人窃取或者信息错误等情况，仍然信赖该证书并从事有关活动的；
4） 因不可抗力原因导致订户或者依赖方遭受损失的。

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

当天威诚信终止业务时，天威诚信 CP 和 CPS 终止。在终止服务六十日前向电子认证服务主管部门报告，并做出妥善安排。

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 对参与者个别通告与沟通

天威诚信及其注册机构在必要的情况下，如在主动吊销订户证书、发现订户将证书用于规定外用途及订户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，个别通知订户、依赖方。

本 CP 和 CPS 终止后，天威诚信将就文档失效的有关事项通知有关当事人。

9.12 修订

9.12.1 修订程序

本证书策略和认证业务规则将不定期的进行修改，确保其符合国家法律法规和主管部门的要求及相关国际标准，并符合认证业务开展的实际需要。

本 CP 和 CPS 的修改和更新，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。

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发布。对于需要通过电子邮件、信件、媒体等方式通知的修改，天威诚信将在合理的时间内通知有关各方，合理的时间应保证有关方受到的影响最小。

9.12.3 必须修改业务规则的情形

天威诚信必须对本 CP 和 CPS 进行修改的情形包括：CP 和 CPS 中相关内容与管辖法律的不一致、国家监管部门对本机构认证业务有明确的更改或调整要求等。

9.13 争议解决

天威诚信、证书订户、依赖方等最终实体在电子认证活动中产生争议的，首先应根据协议友好协商解决；协商未果的，可通过法律途径解决。

任何与天威诚信或注册机构就本 CP 和 CPS 所涉及的任何争议提起诉讼的，各方同意提交天威诚信工商注册所在地人民法院管辖处理。

9.14 管辖法律

天威诚信的 CP 和 CPS 受国家已颁布的《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》等法律法规管辖。

9.15 与适用法律的符合性

无论天威诚信的证书订户、依赖方等实体在何地居住以及在何处使用天威诚信的证书，本 CP 和 CPS 的执行、解释和程序有效性均适用中华人民共和国的法律。任何与天威诚信或注册机构就本 CP 和 CPS 所涉及的任何争议，均适用中华人民共和国法律。

9.16 一般条款

9.16.1 完整协议

本 CP 和 CPS 完整的文档结构包括 3 部分：标题、目录、主体内容。关于对目录和主体内容修改后的替代内容，将完全代替所有先前部分、并被放置在天威诚信的网站中以供查阅和浏览。

9.16.2 转让

天威诚信声明，根据本 CP 和 CPS 中详述的认证实体各方的权利和义务，各方当事人在未经过天威诚信事先书面同意的情况下，不能通过任何方式进行转让。

9.16.3 分割性

如果本 CP 和 CPS 的任何条款或其应用由于与天威诚信所在管辖区的法律产生冲突而被判定为无效或不具执行力时，天威诚信可以在最低必要的限度下修订该条款，使其继续有效，其余部分不受影响，天威诚信将在此章节批露修订的内容。

9.16.4 强制执行

在天威诚信、注册机构、订户和依赖方之间出现纠纷、诉讼时，胜讼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。

天威诚信声明，若证书订户、依赖方等实体未执行本 CP 和 CPS 中某项规定，不被认为该实体将来继续不执行该项或其他规定。

9.16.5 不可抗力

当由于不可抗力，如地震、洪灾、雷电等自然灾害和战争等，造成天威诚信、注册机构无法提供正常的服务时，天威诚信、注册机构不承担由此给客户造成的损失。

9.17 其他条款

天威诚信对本 CP 和 CPS 具有最终解释权。