

---

# 天威诚信<sup>TM</sup>

# 电子认证业务规则

2.3 版本

生效日期: **2008 年 11 月 20 日**

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知春路 6 号锦秋国际大厦 A 座 14 层

邮政编码: 100088  
电话: (8610)-82800896  
网址: [www.itrus.com.cn](http://www.itrus.com.cn)

版本说明：

天威诚信认证业务规则版本控制表

名称及版本	主要修改说明	完成时间	修改人
天威诚信认证业务规则 1.0		2005 年 5 月	龙毅宏
天威诚信认证业务规则 2.0	1、证书类别的定义 2、电子签名法的符合校正 3、详细鉴证流程删除 4、详细密钥管理删除	2005 年 7 月	李延昭/唐志红
天威诚信认证业务规则 2.1	1、一类证书描述 2、安证通责任描述	2005 年 8 月	李延昭
天威诚信认证业务规则 2.2	1、地址及联系方式变更 2、对第五章部分描述的修改 3、按新的产品线划分修改证书类别的定义 4、修正部分前后不一致的地方	2008 年 2 月	陈韶光 许蕾
天威诚信认证业务规则 2.3	1、概述内容增加及个别修改 2、策略文档管理机构变更 3、联系人修改 4、组织机构身份的鉴证描述修改 5、天威诚信信息库更新信息栏发布地址变更	2008 年 11 月	郭志峰/曾琦

---

## 天威诚信电子认证业务规则

天威诚信电子商务服务有限公司版权所有 2004

### 商标声明

China Trusted Network (CTN, 中国可信网络) 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, 请寄往: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知春路 6 号锦秋国际大厦 A 座 14 层 1401 室, 战略发展中心。电话: (8610)-82800896, 传真: (8610)-82800636。电子邮件: [itrus\\_pma@itrus.com.cn](mailto:itrus_pma@itrus.com.cn)。

### 致谢:

在天威诚信电子认证业务规则(见: <https://www.itrus.com.cn/repository/CPS>) 的编辑及修改期间, 得到了有关人士的大力指导与帮助, 在此表示感谢。

# 目录

<b>1. 概括性描述</b>	<b>1</b>
1.1 概述.....	1
1.2 文档名称与标识.....	2
1.3 电子认证活动参与者.....	2
1.3.1 电子认证服务机构 (CA) .....	2
1.3.2 注册机构 (RA) .....	2
1.3.3 订户.....	2
1.3.4 依赖方.....	3
1.3.5 其他参与者.....	3
1.4 证书应用.....	3
1.4.1 合适的应用.....	3
1.4.1.1 颁发给个人的证书.....	3
1.4.1.2 颁发给组织机构的证书.....	3
1.4.2 受限的应用.....	3
1.4.3 受禁的使用.....	3
1.5 策略管理.....	4
1.5.1 策略文档管理机构.....	4
1.5.2 联系人.....	4
1.5.3 决定 CPS 符合策略的机构.....	4
1.5.4 CPS 批准程序.....	4
1.6 定义与缩写.....	4
1.6.1 定义.....	4
1.6.2 缩写.....	7
<b>2. 信息发布与管理</b>	<b>8</b>
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
<b>3. 身份标识与鉴证</b>	<b>9</b>
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.....	10
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.....	11
3.2 初始身份确认.....	11
3.2.1 证明拥有私钥的方法.....	11
3.2.2 组织机构身份的鉴证.....	11

3.2.3	个人身份的鉴证.....	11
3.2.3.1	1类证书的个人身份的鉴证.....	12
3.2.3.2	2类证书的个人身份的鉴证.....	12
3.2.3.3	3类证书的个人身份的鉴证.....	12
3.2.4	没有验证的订户信息.....	12
3.2.5	授权的确认.....	12
3.2.6	互操作准则.....	12
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.....	13
3.3.2	吊销之后的密钥更新的标识与鉴证.....	13
3.4	吊销请求的标识与鉴证.....	13
<b>4.</b>	<b>证书生命周期操作要求</b> .....	<b>14</b>
4.1	证书申请.....	14
4.1.1	证书申请实体.....	14
4.1.2	注册过程与责任.....	14
4.2	证书申请处理.....	15
4.2.1	执行识别与鉴别功能.....	15
4.2.2	证书申请批准和拒绝.....	15
4.2.3	处理证书申请的时间.....	15
4.3	证书签发.....	15
4.3.1	证书签发中 RA 和 CA 的行为.....	15
4.3.2	CA 和 RA 对订户的通知.....	16
4.4	证书接受.....	16
4.4.1	构成接受证书的行为.....	16
4.4.2	CA 对证书的发布.....	16
4.4.3	CA 对其他实体的通告.....	16
4.5	密钥对和证书使用.....	16
4.5.1	订户私钥和证书使用.....	16
4.5.2	依赖方公钥和证书使用.....	17
4.6	证书更新.....	17
4.6.1	证书更新的情形.....	17
4.6.2	请求证书更新的实体.....	17
4.6.3	证书更新请求的处理.....	17
4.6.4	签发新证书时对订户的通知.....	18
4.6.5	构成接受更新证书的行为.....	18
4.6.6	CA 对更新证书的发布.....	18
4.6.7	CA 对其他实体的通告.....	18
4.7	证书密钥更新.....	18
4.7.1	证书密钥更新的情形.....	18
4.7.2	请求证书密钥更新的实体.....	18
4.7.3	证书密钥更新请求的处理.....	18

4.7.4	签发新证书时对订户的通知.....	19
4.7.5	构成接受密钥更新证书的行为.....	19
4.7.6	CA 对密钥更新证书的发布 .....	19
4.7.7	CA 对其他实体的通告 .....	19
4.8	证书变更.....	19
4.8.1	证书变更的情形.....	19
4.8.2	请求证书变更的实体.....	19
4.8.3	证书变更请求的处理.....	19
4.8.4	签发新证书时对订户的通告.....	19
4.8.5	构成接受变更证书的行为.....	19
4.8.6	CA 对变更证书的发布 .....	19
4.8.7	CA 对其他实体的通告 .....	20
4.9	证书吊销和挂起.....	20
4.9.1	证书吊销的情形.....	20
4.9.2	请求证书吊销的实体.....	20
4.9.3	吊销请求的流程.....	20
4.9.4	吊销请求宽限期.....	21
4.9.5	CA 处理吊销请求的时限 .....	21
4.9.6	依赖方检查证书吊销的要求.....	21
4.9.7	CRL 发布频率 .....	21
4.9.8	CRL 发布的最大滞后时间 .....	21
4.9.9	在线状态查询的可用性.....	21
4.9.10	在线状态查询要求.....	22
4.9.11	吊销信息的其他发布形式.....	22
4.9.12	密钥损害的特别要求.....	22
4.9.13	证书挂起的情形.....	22
4.9.14	请求证书挂起的实体.....	22
4.9.15	挂起请求的流程.....	22
4.9.16	挂起的期限限制.....	22
4.10	证书状态服务.....	22
4.10.1	操作特征.....	22
4.10.2	服务可用性.....	22
4.10.3	可选特征.....	23
4.11	订购结束.....	23
4.12	密钥托管与恢复.....	23
4.12.1	密钥托管与恢复的策略与行为.....	23
4.12.2	会话密钥的封装与恢复的策略与行为.....	23
<b>5.</b>	<b>认证机构设施、管理和操作控制</b>	<b>23</b>
5.1	物理控制.....	23
5.1.1	场地位置与建筑.....	24
5.1.2	物理访问控制.....	24

5.1.3	电力与空调.....	24
5.1.4	水患防治.....	24
5.1.5	火灾防护.....	25
5.1.5.1	结构防火.....	25
5.1.5.2	火灾报警及消防设施.....	25
5.1.5.3	紧急出口.....	25
5.1.6	介质存储.....	25
5.1.7	废物处理.....	25
5.1.8	异地备份.....	25
5.1.9	注册机构物理控制.....	25
5.2	程序控制.....	26
5.2.1	可信角色.....	26
5.2.2	每项任务需要的人数.....	26
5.2.3	每个角色的识别与鉴别.....	26
5.2.4	需要职责分割的角色.....	26
5.3	人员控制.....	27
5.3.1	资格、经历和无过失要求.....	27
5.3.2	背景审查程序.....	27
5.3.3	培训要求.....	27
5.3.4	再培训周期和要求.....	28
5.3.5	工作岗位轮换周期和顺序.....	28
5.3.6	未授权行为的处罚.....	28
5.3.7	独立合约人的要求.....	28
5.3.8	提供给员工的文档.....	28
5.4	审计日志程序.....	28
5.4.1	记录事件的类型.....	28
5.4.2	处理日志的周期.....	29
5.4.3	审计日志保存期限.....	30
5.4.4	审计日志的保护.....	30
5.4.5	审计日志备份程序.....	30
5.4.6	审计收集系统.....	30
5.4.7	对导致事件主体的通知.....	30
5.4.8	脆弱性评估.....	30
5.5	记录归档.....	30
5.5.1	归档记录的类型.....	30
5.5.2	归档记录的保存期限.....	30
5.5.3	归档文件的保护.....	31
5.5.4	归档文件的备份程序.....	31
5.5.5	记录时间戳要求.....	31
5.5.6	归档收集系统.....	31
5.5.7	获得和检验归档信息的程序.....	31

5.6	CA 密钥变更 .....	31
5.7	损害与灾难恢复 .....	32
5.7.1	事故和损害处理程序 .....	32
5.7.2	计算机资源、软件和/或数据的损坏 .....	32
5.7.3	实体私钥损害处理程序 .....	32
5.7.4	灾难后的业务存续能力 .....	32
5.8	CA 或 RA 的终止 .....	33
<b>6.</b>	<b>技术安全控制 .....</b>	<b>33</b>
6.1	密钥对的产生和安装 .....	33
6.1.1	密钥对的产生 .....	33
6.1.1.1	CA 密钥对的产生 .....	33
6.1.1.2	最终订户密钥对的产生 .....	33
6.1.2	私钥传送给订户 .....	33
6.1.3	公钥传送给证书签发机关 .....	33
6.1.4	CA 公钥传送给依赖方 .....	34
6.1.5	密钥的长度 .....	34
6.1.6	公钥参数的生成和质量检查 .....	34
6.1.7	密钥使用目的 .....	34
6.2	私钥保护和密码模块工程控制 .....	35
6.2.1	密码模块的标准和控制 .....	35
6.2.2	私钥多人控制 (m 选 n) .....	35
6.2.3	私钥托管 .....	35
6.2.4	私钥备份 .....	35
6.2.5	私钥归档 .....	35
6.2.6	私钥导入、导出密码模块 .....	36
6.2.7	私钥在密码模块的存储 .....	36
6.2.8	激活私钥的方法 .....	36
6.2.8.1	用户证书私钥 .....	36
6.2.8.1.1	1 类证书 .....	36
6.2.8.1.2	2 类证书 .....	36
6.2.8.1.3	3 类证书 .....	36
6.2.8.2	服务器证书 .....	37
6.2.8.3	CA 私钥 .....	37
6.2.9	解除私钥激活状态的方法 .....	37
6.2.10	销毁私钥的方法 .....	37
6.2.11	密码模块的评估 .....	37
6.3	密钥对管理的其他方面 .....	38
6.3.1	公钥归档 .....	38
6.3.2	证书操作期和密钥对使用期限 .....	38
6.4	激活数据 .....	38
6.4.1	激活数据的产生和安装 .....	38

6.4.2	激活数据的保护.....	39
6.4.3	激活数据的其他方面.....	39
6.4.3.1	激活数据的传送.....	39
6.4.3.2	激活数据的销毁.....	39
6.5	计算机安全控制.....	39
6.5.1	特别的计算机安全技术要求.....	39
6.5.2	计算机安全评估.....	40
6.6	生命周期技术控制.....	40
6.6.1	系统开发控制.....	40
6.6.2	安全管理控制.....	40
6.6.3	生命期的安全控制.....	40
6.7	网络的安全控制.....	40
6.8	时间戳.....	40
<b>7.</b>	<b>证书、CRL 和 OCSP</b>	<b>41</b>
7.1	证书.....	41
7.1.1	版本号.....	41
7.1.2	证书扩展项.....	41
7.1.2.1	密钥用法 (Key Usage) .....	41
7.1.2.2	证书策略扩展项 (Certificate Policies) .....	42
7.1.2.3	主体备用名 (subjectAltName) .....	42
7.1.2.4	基本限制扩展项 (BasicConstraints) .....	42
7.1.2.5	扩展的密钥用法 (Extended Key Usage) .....	42
7.1.2.6	CRL 的分发点 (cRLDistributionPoints) .....	43
7.1.2.7	签发 CA 密钥标识符 .....	43
7.1.2.8	主体密钥标识符.....	43
7.1.3	密钥算法对象标识符.....	43
7.1.4	名称形式.....	43
7.1.5	名称限制.....	43
7.1.6	证书策略对象标识符.....	43
7.1.7	策略限制扩展项的用法.....	44
7.1.8	策略限定符的语法和语义.....	44
7.1.9	关键证书策略扩展项的处理规则.....	44
7.2	CRL.....	44
7.2.1	版本号.....	44
7.2.2	CRL 和 CRL 条目扩展项 .....	44
7.3	OCSP.....	44
7.3.1	版本号.....	45
7.3.2	OCSP 扩展项.....	45
<b>8.</b>	<b>认证机构审计和其他评估</b>	<b>45</b>
8.1	评估的频率和情形.....	45
8.2	评估者的资质.....	46

8.3	评估者与被评估者之间的关系.....	46
8.4	评估的内容.....	46
8.5	对问题与不足采取的措施.....	46
8.6	评估结果的传达与发布.....	46
8.7	其他评估.....	46
<b>9.</b>	<b>其他业务和法律事务</b>	<b>46</b>
9.1	费用.....	46
9.1.1	证书签发和更新费用.....	46
9.1.2	证书查取的费用.....	46
9.1.3	证书吊销或状态信息的查询费用.....	47
9.1.4	其他服务费用.....	47
9.1.5	退款策略.....	47
9.2	财务责任.....	47
9.2.1	保险范围.....	47
9.2.2	其他资产.....	47
9.2.3	对最终实体的保险或担保.....	47
9.3	业务信息保密.....	47
9.3.1	保密信息范围.....	47
9.3.2	不属于保密的信息.....	48
9.3.3	保护保密信息责任.....	48
9.4	个人隐私保密.....	48
9.4.1	隐私保密方案.....	48
9.4.2	作为隐私处理的信息.....	48
9.4.3	不被视为隐私的信息.....	48
9.4.4	保护隐私的责任.....	48
9.4.5	使用隐私信息的告知与同意.....	49
9.4.6	依法律或行政程序的信息披露.....	49
9.4.7	其他信息披露情形.....	49
9.5	知识产权.....	49
9.5.1	证书和吊销信息中的知识产权.....	49
9.5.2	CPS 中的知识产权.....	49
9.5.3	命名中的知识产权.....	49
9.5.4	密钥和密钥材料的知识产权.....	49
9.6	陈述与担保.....	50
9.6.1	CA 的陈述与担保.....	50
9.6.2	RA 的陈述与担保.....	50
9.6.3	订户的陈述与担保.....	50
9.6.4	依赖方的陈述与担保.....	51
9.6.5	其他参与者的陈述与担保.....	51
9.7	担保免责.....	51
9.8	有限责任.....	51

9.9	赔偿.....	52
9.10	有效期限与终止.....	53
9.10.1	有效期限.....	53
9.10.2	终止.....	53
9.10.3	效力的终止与保留.....	53
9.11	对参与者个别通告与沟通.....	53
9.12	修订.....	53
9.12.1	修订程序.....	53
9.12.2	通知机制与期限.....	53
9.12.3	必须修改业务规则的情形.....	54
9.13	争议解决.....	54
9.14	管辖法律.....	54
9.15	与适用法律的符合性.....	54
9.16	一般条款.....	54
9.16.1	完整协议.....	54
9.16.2	转让.....	54
9.16.3	分割性.....	54
9.16.4	强制执行.....	55
9.16.5	不可抗力.....	55
9.17	其他条款.....	55

## 1. 概括性描述

本文件是天威诚信认证业务规则（CPS），本 CPS 是按照中国信任网络证书策略（CTN CP）的相关要求制定的。CTN 是一个以中国用户为主的公钥基础设施（Public Key Infrastructure, PKI），它向用户提供各种应用的数字证书。CTN 适合于广大的、对通信和信息安全方面有各种各样需求的公众用户。

天威诚信作为 CTN 的一个子域拥有 CA，本 CPS 阐明了天威诚信作为一个证书认证机构如何根据天威诚信 CTN 证书策略（CP）开展其业务，包括批准、签发、管理、吊销和更新证书业务方式和过程，相应的服务、法律和技术上的措施和保障。

本 CPS 的总体条款结构符合信息产业主管部门所发布的《电子认证业务规则规范（试行）》，并在制定过程中参照《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务机构年度检查指引（试行）》及国家密码主管部门相关标准制定。在不改变《电子认证业务规则规范（试行）》总体框架的情况下，在制定本 CPS 时可能会该框架进行扩充，以适应天威诚信认证业务的特定需求。

本 CPS（2.2 版本）的生效日期是 2008 年 11 月 20 日。

### 1.1 概述

本 CPS 适用于天威诚信运营管理的 CA，包括主 CA（PCA）、PCA 之下的签发 CA、以及为企业客户生成的运营 CA。本 CPS 不适用于在天威诚信托管的私有体系 PKI。

按照天威诚信 CTN 证书策略，天威诚信提供三种类型的证书：1 类证书、2 类证书和 3 类证书，分别适用于不同的应用。

1 类证书只提供最基本级别的安全保证，只能用于对安全要求较低的应用场合如安全电子邮件、企业内部应用。1 类证书用于安全电子邮件时，天威诚信只对电子邮件地址的真实性进行验证，并不对证书持有人身份的真实性进行验证。1 类证书用于企业内部应用时，由企业自行对证书持有人的身份进行鉴证，且只能用于企业内部应用。

按照 CTN CP 的规定，1 类证书产生的数字签名不具备《中华人民共和国电子签名法》所规定的法律效力，除非双方当事人自行约定。

2 类证书提供中等级别的安全保证，可用于对安全要求较高的场合。2 类证书主要颁发给个人或组织机构，用于提供个人或组织机构的身份证明，能够应用于数字签名、加密和访问控制，以及中等额度交易中的身份证明，也可以颁发给组织机构所合法拥有的设备（如服务器、VPN 设备），作为设备凭证供组织机构访问控制使用。2 类个人证书可包括签名证书和加密证书。

按照 CTN CP 的规定，经过天威诚信或相关注册机构鉴证的 2 类证书，在满足《中华人民共和国电子签名法》的其他规定下，由其所产生的电子签名符合《中华人民共和国电子签名法》的要求。

3 类证书包括组织机构身份证书、组织机构代表人证书、设备证书（如服务器证书）等。在天威诚信信任域中，第 3 类证书提供最高级别的安全保证。

按照 CTN CP 的规定，经过天威诚信鉴证的 3 类证书，在满足《中华人民共和国电子签名法》的其他规定下，由其产生的电子签名符合《中华人民共和国电子签名法》的要求。

## 1.2 文档名称与标识

本文档称为《天威诚信电子认证业务规则》（简称天威诚信 CPS），该文档没有分配对象标识符。

## 1.3 电子认证活动参与者

### 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）是一个通用术语，所有得到授权能够颁发公钥证书的实体，均称为 CA。CA 中包含一个子集称为主 CA（PCA），每个 PCA 对应一类证书。天威诚信负责 PCA 的运营管理工作，PCA 的下级 CA 颁发最终用户或其他 CA 的证书。

PCA 的下级 CA 可以由天威诚信运营，也可以由与天威诚信建立合同关系的合作伙伴运营。由运营下级 CA 的合作伙伴，作为独立的运营机构，应按照 CTN CP 的相关要求制定自己的 CPS，并严格按照 CPS 执行自己的认证业务，使其所颁发的证书能够达到 CTN CP 所要求的信任等级要求。为保证 CTN 信任体系的一致性，天威诚信 PMA 将对合作伙伴每年进行一次审查。

### 1.3.2 注册机构（RA）

注册机构（Registration Authority，简称 RA）代表 CA 建立起注册过程，确认证书申请者的身份，批准或拒绝证书申请，批准订户的证书吊销请求或直接吊销证书，批准订户的证书更新请求。天威诚信及合作伙伴既是 CA，同时也是 RA。

与天威诚信或合作伙伴建立起合同关系的第三方，可运营其自己的 RA，并且在某 CTN CA 的授权下颁发证书。第三方 RA 必须遵守本 CPS 和与天威诚信签署的任何协议的规定。但 RA 可以根据其内部需求，执行更严格的流程。

### 1.3.3 订户

订户包括所有由 CTN CA 颁发证书的最终用户。订户就是一个实体，可以是个人、组织机构或基础设施的组成部件如防火墙、路由器、可信服务器或在组织中用于安全通信的其他设备。

一般情况下，证书是直接颁发给个人或实体由其自己使用。但是，总存在其他情形，需要证书的一方与申请证书的实体不同，例如一个组织可能为其雇员请求证书，或者为其 Web 服务器申请证书。当出现这种情况时，本 CPS 采用两个术语进行区分：“订户”特指与认证机构或注册机构签订合同购买证书的实体；“主体”特指证书中主体域所标识的实体。从这个角度看，订户一定是人或组织机构的授权代表，而主体则有可能是设备。

从技术的角度看，CA 也可以视为订户，不论是自签发的 PCA，还是下级 CA。但在本 CPS 中，订户特指没有签发证书权力的最终用户，不代表 CA。

#### 1.3.4 依赖方

天威诚信信任域的依赖方是为某一应用而使用、信任天威诚信签发或注册机构签发的证书的个人或组织。依赖方可以是订户，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 合适的应用

##### 1.4.1.1 颁发给个人的证书

颁发给个人的证书通常称为个人证书。个人证书常用来签署和加密电子邮件、文件以及登陆认证，也可用于其他目的，只要不违背法律、本 CPS（颁发证书所遵循的）和订户协议，使依赖方可以合理地信赖证书。

##### 1.4.1.2 颁发给组织机构的证书

颁发给组织机构的证书通常称为组织机构证书。组织机构证书通常用于加密、签名、客户端认证、服务器端认证、代码签名等，也可用于其他目的，只要不违背法律、本 CPS（颁发证书所遵循的）和订户协议，使依赖方可以合理地信赖证书。

#### 1.4.2 受限的应用

天威诚信所颁发的某些证书在功能上是受到限制的，如个人证书只能用于个人用户的应用，而不能作为服务器或组织机构证书使用。3 类组织机构身份证书只能用于代表组织机构的场合。签发给服务器的证书只能限制在 Web 服务器或 Web 流量管理设备使用。

证书的密钥用法扩展项中限制了与证书中公钥对应私钥的使用目的（6.1.7.），如最终订户证书不能作为 CA 证书使用。这种限制是基本限制扩展项缺省值确定的（7.1.2.5）。然而，基于扩展项的限制的有效性取决于软件，如果有关软件不遵守有关约定，其对证书的使用将违反本证书策略的规定，将是不受保护的。

#### 1.4.3 受禁的使用

证书不设计用于、不打算用于、也不授权用于危险环境中的控制设备，或用于要求防失败的场合，如核设备的操作、航天飞机的导航或通讯系统、空中交通控制系统 或武器控制系统中，因为它的任何故障都可能导致死亡、人员伤害或严重的环境破坏。

## 1.5 策略管理

### 1.5.1 策略文档管理机构

本 CPS 的管理机构是天威诚信策略管理委员会，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知春路 6 号锦秋国际大厦 A 座 14 层 1401 室（100088）  
电话号码：0086-010-82800896  
传真号码：0086-010-82800636  
邮箱地址：itrus\_pma@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\_pma@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知春路 6 号锦秋国际大厦 A 座 14 层 1401 室（100088）  
电话号码：0086-010-82800896  
传真号码：0086-010-82800636

### 1.5.3 决定 CPS 符合策略的机构

天威诚信策略管理委员会（PMA）。

### 1.5.4 CPS 批准程序

天威诚信有专门的策略管理机构——即 PMA，负责 CPS 的管理。认证机构的 CPS 将会被提交到 PMA，策略管理机构将负责评估 CPS 是否符合相关要求，如果符合，将批准 CPS。

## 1.6 定义与缩写

### 1.6.1 定义

表 3-定义

术语	定义
证书	是指一段信息，它至少包含了一个名字或标识特定的 CA，标识有关订户，包含了订户的公钥、证书有效期、证书序列号，及 CA 数字签名。
证书申请	来自证书申请者（或证书申请者授权代理）的、要求 CA 签发证书的请求

术语	定义
证书申请人	要求一个发证机关签发证书的个人或者组织机构。
证书链	一个有序的证书列表，包含了最终用户的证书和发证机关的证书，该列表最顶级证书为根证书，最下级证书为最终用户的证书。
证书策略	是一个有关证书业务策略的主要说明。
证书吊销列表 (CRL)	一个定期(或根据要求)发行的、并由发证机关数字签名的信息列表，用来识别在有效期内提前被吊销的证书。这个列表通常标明 CRL 发布者的名字，发布的日期，下一次 CRL 发布的日期，被吊销证书的序列号，吊销证书的时间和原因。
证书类别	CP 中定义的担保的级别。见 CPS § 1.1.1。
认证机构(CA)	一个授权签发、管理、吊销和更新证书的实体。
电子认证业务规则(CPS)	认证机构批准或拒绝证书申请、签发、管理和吊销证书时必须遵守的业务规则的描述。
挑战语	证书申请人在注册一个证书时选择的秘密短语。当一个证书被签发后，证书申请者成为了一个订户，这时如果订户要求吊销或更新这个订户证书，CA 或 RA 可以使用挑战语识别订户的身份。
中国信任网络(CTN)	天威诚信建立的基于 PKI 的安全认证体系。
一致性审计	一个认证机构或注册机构要定期经历的审计，通过该审计确定它是否满足有关的 CTN 标准。
安全损害	对安全策略的违反（或怀疑违反），包括出现敏感信息未经授权的泄漏或失去对其的控制。对于私钥，安全损害是指丢失、失窃、公开、修改、未经授权的使用或密钥受到的其它安全危害威胁。
机密/私密信息	根据 CPS § 9.3, 9.4 要求需保密的信息。
服务器证书	2 类或 3 类证书，用于支持浏览器和服务器之间的 SSL 会话。该证书用于标识组织机构的 Web 服务器的身份，将一个域名与一台服务器绑定。该服务器证书确保服务器的拥有机构有权使用证书上的域名，确保当一个用户访问一个以该域名命名的 Web 服务器时，用户访问的 Web 服务器就是他访问的服务器，而不是假冒的服务器，另外它可实现信息从客户端到服务器端的保密传送。
知识产权	在版权、专利、商业秘密、商标和其他知识产权下拥有的权利。

术语	定义
密钥生成规程参考指南	描述密钥生成规程要求和业务操作的文档。
密钥生成规程	CA 密钥对产生、其私钥被传送到密码模块、私钥备份和签发它的公钥的过程。
未经验证的订户信息	指证书申请人提交给 CA 或 RA 的、包含在证书中的信息，但该信息未经 CA 或 RA 证实，因此 CA 或 RA 除确认该信息是由证书申请人提出外，对其它信息不作确认。
抗抵赖	一种提供通信保护的属性，它可以防止通信一方否认信息的出处，否认它已经提交或传送了这些信息。否认出处包括否认某一通信与先前的一系列消息源来自同一地方，即使不知发送者是谁。（注：只有法院的判决、仲裁或其它的裁决才能够最终阻止抵赖。例如，可用证书的数字签名是裁判所作出抗抵赖裁决的支持证据，但它本身不能够抗抵赖。）
在线证书状态查询协议 (OCSP)	为依赖方提供实时查询证书状态信息的协议。
操作期限	指从证书签发日期和时间（或者证书上指定的一个较晚的日期和时间）开始，到证书过期或被吊销时的日期和时间为止的这段时间。
PKCS #10	公钥密码标准#10，由 RSA 安全公司开发。它定义了证书签名请求的结构。
PKCS #12	公钥密码标准#12，由 RSA 安全公司开发。定义了私钥安全传送的方法。
公钥基础设施(PKI)	所有支持基于证书的公开密钥系统实施和操作体系的组织机构、技术、业务和过程的总称。
注册机构(RA)	CA 批准的一个实体，它帮助证书申请者申请证书，批准或拒绝证书申请，吊销证书或更新证书。
依赖方	信赖一个证书和/或一个数字签名的个人或组织机构。
依赖方协议	协议规定了一个组织机构或个人作为依赖方的条件和要求。
信息库	认证机构提供的、可在线访问的证书和其他证书有关信息的数据库。
RSA	由 Rivest, Shamir and Adelman 发明的公钥密钥密码系统
秘密分割	根据秘密分割算法，将激活 CA 私钥需要的数据分割成多个部分，使用其中若干个分割可以恢复原激活数据。
安全套接层协议(SSL)	由网景通信公司开发的、保护 Web 通信的一个工业标准。SSL 为一个 TCP/IP 连接提供数据加密、服务器验证、信息完整性和可选的客户端验证等。

术语	定义
主体	与公钥对应的私钥的持有者。在组织机构证书中，主体指的是持有私钥的设备或装置或组织机构本身。一个主体只有唯一的、确切的命名。它和该主体证书中的公钥绑定在一起。
订户	对于个人证书，订户是指人，他是签发的证书的主体；对于组织机构身份证书，订户是指组织机构；对于组织机构代表人身份证书，订户是组织机构授权的人；对于服务器证书，它是所签发证书的主体所对应设备或装置的拥有者。一个订户可以使用或被授权使用证书所含公钥对应的私钥。
订户协议	一个 CA 或 RA 拟定的协议，规定一个人或组织机构作为证书订户需要遵循的条款和条件。
可信人员	在认证机构的雇员、合同商或顾问，他们负责保证实体基础设施的可信性，以及管理产品、服务、设施和业务的可信性。
安全可信系统	是指能够有效地避免被入侵与滥用的，提供可靠的、可用的、有正确操作保障的、能够完成预定功能的、实施了适当的安全策略的计算机硬件、软件与程序。安全可信系统不一定是政府信息系统分级中所定义的“可信系统”。

## 1.6.2 缩写

表 4-缩写

缩写	全称
CA	认证机构
CP	证书策略.
CPS	认证业务规则.
CRL	证书吊销列表.
CTN	中国可信网络
OCSP	在线证书状态查询协议
OCA	运营 CA
DN	甄别名
LDAP	轻量目录访问协议
PCA	主认证机构
PIN	个人身份识别码
PKCS	公钥密码标准
PKI	公钥基础设施
RA	注册机构

缩写	全称
<b>RFC</b>	请求评注标准(一种互联网建议标准)
<b>SSL</b>	加密套接层协议。.

## 2. 信息发布与管理

### 2.1 信息库

天威诚信的 WWW 网站、认证系统的证书服务站点、LDAP、CRL 及 OCSP 服务器构成了天威诚信认证信息发布的信息库。另外，注册机构的证书服务站点也是认证信息发布的信息库。

### 2.2 认证信息的发布

天威诚信的认证业务规则可从天威诚信的 WWW 网站获取；用户证书可从天威诚信的 LDAP、证书服务站点获取；已被吊销了的证书的信息可从 CRL 站点、LDAP 查获，而证书的状态（有效、吊销、挂起）可通过 OCSP 获得。

### 2.3 发布的时间或频率

天威诚信的认证业务规则可通过信息库 7X24 获得。天威诚信签发的订户证书一经签发即发布到 LDAP 服务器供用户下载，同时订户可通过证书服务站点获得已签发的证书。通过 OCSP 对证书状态的查询是及时的。天威诚信对每个证书签发 CA 发布一个证书吊销列表，发布该 CA 签发的证书中的已吊销了的证书。证书吊销列表一般是每 24 小时、在午夜 0 点整更新。对于特殊的客户，天威诚信可为其专门定制吊销列表的更新频率。

### 2.4 信息库访问控制

对于 2.2 中所说的认证信息的查询、获取是公开的、没有限制的。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。

### 3. 身份标识与鉴证

#### 3.1 命名

##### 3.1.1 名称类型

根据证书对应实体的类型不同，天威诚信签发的证书的实体名字可以是人员姓名、组织机构名、部门名、域名等，命名符合 X.501 甄别名规定。

天威诚信 CA 证书的签发者和主体域中包含 X.501 甄别名。天威诚信 CA 证书的主体甄别名由表 5 中的内容组成。

表 5- 天威诚信 CA 证书主体甄别名属性

属性	值
国家 (C) =	CN 或者不用
机构(O) =	iTruschina Co., Ltd
机构部门(OU) =	天威诚信证书中可以包含多个 OU 属性。这些属性可以包含一个或多个下面的内容： <ul style="list-style-type: none"> <li>• CA 名</li> <li>• CA 服务名，如 Individual Comsumer Service Center</li> <li>• China Trust Network</li> <li>• 一个依赖方协议声明的引用，该依赖方协议明确了使用证书的条款。</li> <li>• 版权通告</li> </ul>
省 (S) =	没有使用
地区 (L) =	没有使用
通用名(CN) =	这个属性包括 CA 名（如果 CA 名没有在 OU 属性中指明）或不用。

最终订户证书的主体域中包含一个 X.501 甄别名，它由表 6 中的内容组成。

表 6-最终订户证书主体甄别名属性

属性	值
国家 (C) =	CN 或不用.
机构(O) =	组织机构属性使用如下： <ul style="list-style-type: none"> <li>• 对于没有确定组织的个人证书，是 iTruschina Co., Ltd。</li> <li>• 对于其他类型证书，是证书订户所在机构的机构名。</li> </ul>
机构部门(OU) =	天威诚信最终订户证书主体名可以包含多个 OU 属性。这些属性可以包含一个或多个下面的内容： <ul style="list-style-type: none"> <li>• 订户组织机构部门</li> <li>• China Trust Network</li> </ul>

属性	值
	<ul style="list-style-type: none"> <li>• 一个引用依赖方协议的声明，该依赖方协议明确了使用证书的条款。</li> <li>• 版权通告</li> <li>• 第 1 类个人证书包含“Personal Not Validated”。</li> <li>• 描述证书类型的文字。</li> </ul>
省(州) (S) =	指出订户所在的省或不用
位置(L) =	订户所在地区或不用
通用名(CN) =	这个属性包括 <ul style="list-style-type: none"> <li>• 域名（服务器证书），或</li> <li>• 组织机构名（组织机构身份证书），或</li> <li>• 个人姓名（个人证书、组织机构代表人证书），或</li> <li>• 假名（1 类邮件证书）。</li> </ul>
E-Mail 地址 (E) =	个人证书包含的 e-mail 地址

在第 2~3 类证书的情况下，最终订户证书主体的甄别名中的通用名（CN=）部分被鉴别和确认：

- 包含在组织机构身份证书主体甄别名中的的通用名是一个机构的法定名称或法定机构中部门的名称。
- 包含在服务器证书主体甄别名中的的通用名是一个该组织机构拥有或授权使用的域名。
- 个人证书的通用名是这个人的通常被接受的名字。

### 3.1.2 对名称有意义的要求

天威诚信签发的最终订户证书所包含的名称具有通常理解的语义，用它可以确定证书主体中的个人、组织机构或设备的身份。

### 3.1.3 订户的匿名或伪名

订户不宜使用匿名或伪名申请证书。

### 3.1.4 理解不同名称形式的规则

依 X.501 甄别名命名规则解释。

### 3.1.5 名称的唯一性

天威诚信签发给某个实体的证书，其主体甄别名，在该 CA 信任域内是唯一的，其中的例外是签发双证书时（一个签名证书、一个加密证书），属于同一实体的两个证书具有同样的主体甄别名，但证书的密钥用法扩展项不同。

### 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，但天威诚信并不决定证书申请者是否具有相关知识产权，也无需判断、裁决或解决任何关于域名、名称、商标、服务标的争端问题。当出现此类争端时，天威诚信有权拒绝或挂起证书申请，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，或其它相当的密码格式，或其他天威诚信批准的方法，验证证书申请者拥有私钥。

如果天威诚信代表订户产生一个密钥对（如，将产生的密钥对放置到智能卡上），那么，这个要求不适用。

### 3.2.2 组织机构身份的鉴证

对于组织机构证书，包括组织机构身份证书、组织机构代表人证书、服务器证书，是签发给一个组织机构，或一个组织机构代表人，或一个组织机构拥有的服务器，对这类证书的签发，无论是天威诚信审批，还是通过注册机构审批，天威诚信或注册机构必须按照《天威诚信鉴证计划》的要求对订户所在组织机构进行身份鉴证，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文件，如营业执照、组织机构代码证等，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。确认的方式可以通过可靠的第三方途径，获得组织机构有关申请及授权事宜的确认。当证书中包含某个人（作为该组织的授权代表）的名字时，则此人的雇佣关系和他/她代表组织的权威性也应得到确认。

### 3.2.3 个人身份的鉴证

对于所有类型的个人证书，天威诚信或注册机构确认：

- 证书申请者确实存在（1类证书除外）。
- 证书申请者是证书申请中所说的那个人（1类证书除外）。
- 按照§ 3.2.1，确认证书申请者拥有与证书中所列公钥相对应的私钥。
- 除了未经验证的订户信息，包含在证书中的信息是准确的。

具体鉴证过程按照《天威诚信鉴证计划》执行。

### 3.2.3.1 1类证书的个人身份的鉴证

对于1类个人证书，证书申请订户的身份鉴证包括：保证在天威诚信1类证书信任域中，主体甄别名是一个唯一的、明确的主体名，这类订户的通用名是未经验证的订户信息。针对电子邮件的1类证书鉴证包括对证书申请者E-mail地址的确认。

### 3.2.3.2 2类证书的个人身份的鉴证

2类证书的个人身份的鉴证，将通过信息匹配的方式对订户身份进行人工确认，可采用两种方式进行匹配确认：

- 采用天威诚信认可的、提供身份证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、主流的信用机构或其他可靠的信息源；
- 对于RA向与其相关的合作人员颁发证书的情形，可采用包含在RA业务交易记录或数据库中的信息。

### 3.2.3.3 3类证书的个人身份的鉴证

3类个人证书的鉴证是在2类证书鉴证的基础上增加对有效证件的验证，如身份证、护照或其他身份凭证。

3类管理员证书也应包括对组织机构的鉴证和组织机构对于作为管理员的人的雇佣关系和授权的确认。

## 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：

- 组织单元（OU）
- 1类证书的订户名称
- 证书中指明不验证的其他信息

## 3.2.5 授权的确认

对于组织机构证书，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，如通过可信第三方获得申请者所在组织机构电话号码，然后联系组织机构的有关人员，确认申请者获得了所在组织机构的授权。

## 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相应的服务网页，但用户无需填写申请信息，系统会自动获取有关的订户信息。

对于天威诚信的证书认证业务，在证书有效期到期前只能通过密钥更新或证书更新签发有相同签发者、主体名和证书用途的证书。除非先将证书吊销，否则在证书有效期到期前，不能通过申请新证书的方法获得有相同签发者、主体名和证书用途的证书。

#### 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注册机构管理员吊销，天威诚信和注册机构在认为必须的时候，有权发起吊销订户证书。

在订户自己吊销时，可接受的鉴别过程如下：

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，可接受的鉴别过程如下：

订户通过一定的方式，如邮件、传真、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。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、传真、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

任何希望保证电子邮件安全的用户都可以申请 1 类电子邮件安全证书。

任何自然人需要在应用中进行基于数字证书的身份鉴别、需要采用数字签名及实现信息加密时，可以申请 1 类个人证书（包括签名证书、加密证书）。

当一个企业、组织提供的应用需要对最终用户进行基于数字证书的身份鉴别、需要采用数字签名及实现信息加密时，该企业、组织可申请获得天威诚信的 RA 账户服务而成为天威诚信认证机构的注册机构，该企业、组织的雇员、合作伙伴、供应商和客户作为该企业、组织应用的最终用户可以申请 2 类个人证书（包括签名、加密证书）。

组织机构身份证书、组织机构代表人证书由企业、组织授权的人员申请；服务器证书（SSL 证书）由域名拥有机构或获得域名使用授权的机构中的授权人申请。

#### 4.1.2 注册过程与责任

1 类证书申请者可到天威诚信 1 类证书注册服务站点和天威诚信 1 类注册机构的证书注册服务站点注册申请证书。注册时申请者须填写正确的个人信息，申请 1 类个人邮件证书的必须填写正确的电子邮件地址。

2 类证书申请者可到天威诚信 2 类注册机构的证书注册服务站点注册申请证书。注册时申请者须填写注册机构要求的信息。

各类 3 类证书申请者可到天威诚信相应的证书注册服务站点和天威诚信 3 类注册机构的证书注册服务站点注册申请证书。注册时申请者须填写正确信息，包括，

- 1) 组织机构联系人信息，即所在组织机构名，组织机构部门名、联系人姓名、邮件地址、联系电话；
- 2) 技术联系人信息，即所在组织机构名、组织机构部门名、联系人姓名、邮件地址、联系电话；
- 3) 域名（对于服务器证书）。

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，给电子签名依赖方、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 1 类证书申请，天威诚信及其注册机构完成证书申请者的鉴别，并确保证书申请者申请信息的正确性和证书签发给正确的申请人。对于 1 类证书中对应虚拟实体的证书，如电子邮件证书，天威诚信及其注册机构只鉴别用户是否拥有电子邮箱地址。

对于 2 类证书申请，天威诚信可以自行完成对证书申请者的鉴别，也可以委托作为注册机构的注册机构完成证书申请者的鉴别，天威诚信或注册机构确保证书申请信息的正确性和证书签发给正确的申请人。

对于 3 类证书申请，天威诚信或其注册机构对申请者提供的信息进行真伪鉴别，在必要的时候通过第三方数据库验证组织机构信息，然后按 CPS§ 3.2.2 所描述的过程进行个人及组织机构身份鉴别。

### 4.2.2 证书申请批准和拒绝

在天威诚信或注册机构完成对证书申请的鉴证，有关鉴证获得通过并且证书申请者履行了其他应尽的责任（如付款）后，天威诚信或注册机构批准申请。如果鉴证未获通过或证书申请者拒绝履行了其他应尽的责任（如付款），天威诚信或注册机构将会拒绝申请。

### 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不超过 5 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行者，天威诚信是一个 CA，同时天威诚信建设了 RA 系统提供证书零售服务。天威诚信的注册机构在接受、处理证书请求时担当 RA 的角色。

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。为了批准证书申请，RA 管理员将使用证书登录到 RA 系统，查询系统记录的有关请求并批准请求。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，RA 系统会通过邮件自动通知订户。如果证书申请获得批准，邮件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：

- 通过面对面的提交，订户从注册机构（天威诚信或注册机构）接受载有证书和私钥的介质。在这种情况下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。
- 订户根据电子邮件中获取证书的的指示，访问专门的证书下载服务站点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。认证系统会记录订户已下载证书。

对于第一种方式，当订户接受了载有证书的介质即表明订户接受了证书。对于第二种方式，系统记录订户下载了证书即表明订户接受了证书。

### 4.4.2 CA 对证书的发布

天威诚信有基于 LDAP 协议的目录服务，天威诚信可根据用户的意愿将其签发的证书发布到目录系统上，或不发布。

### 4.4.3 CA 对其他实体的通告

对于其签发的证书，天威诚信及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

对于签名证书，其私钥可用于对信息的签名。在可能的情况下，签名证书及信任链上的证书（根证书除外）应同被签名信息一起提交给依赖方。证书持有人使用私钥对信息签名时，应该知晓并确认签名的内容。对于具有身份鉴别用途的证书，其私钥可用于对鉴别方提交的挑战信息签名；在可能的情况下，具有身份鉴别用途的证书及信任链上的证书（根证书除外）应提交给验证方。对于加密证书，其私钥可用于对采用对应公钥加密的信息解密。证书持有人应按 6.1, 6.2, 6.4 妥善保管其证书私钥。

## 4.5.2 依赖方公钥和证书使用

当依赖方接受到经数字签名的信息后，应该，

- (1) 获得数字签名对应的证书及信任链；
- (2) 确认该签名对应的证书是依赖方信任的证书；
- (3) 证书的用途适用于对应的签名。
- (4) 使用证书上的公钥验证签名。

以上任何一个环节失败，依赖方应该拒绝接受签名信息。

当依赖方需要发送加密信息给接受方时，须先通过适当的途径获得接受方的加密证书，然后使用证书上的公钥对信息加密。依赖方应将加密证书连同加密信息一起发送给接受方。

## 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订户证书，证书到期前 30 天系统将会自动发邮件给订户提醒用户证书将到期，如继续使用可进行证书更新。到期前 30 天内或已到期后 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更新站点申请证书更新。申请证书更新时用户无需象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。

### 4.6.2 请求证书更新的实体

证书订户（1、2、3 类个人证书）、证书订户的授权代表（组织机构证书）或证书对应实体的拥有者（比如服务器证书的拥有者）可以要求更新证书。

### 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，天威诚信认证系统会自动完成如下验证操作：

- 申请对应的原证书存在并且由认证机构签发。
- 证书更新请求在允许的期限。
- 用原证书上的订户公钥对更新申请的签名进行验证。

在此基础上，天威诚信或注册机构按与初次证书申请一样的鉴证过程完成证书更新请求的鉴证，然后批准、签发证书。

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订户证书，证书到期前 30 天系统将会自动发邮件给订户提醒用户证书将到期。如果用户希望继续使用证书并且原注册信息继续有效，订户可以申请证书密钥更新（通常作为证书更新），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。在证书到期前 30 天内或已到期后 30 天内，订户可访问天威诚信或注册机构的证书密钥更新站点申请证书密钥更新。申请证书密钥更新时用户无需象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**

证书订户（1、2、3 类个人证书）、证书订户的授权代表（组织机构的授权代表）或证书对应实体的拥有者（如服务器证书的拥有者）可以要求对新公钥的认证。

#### **4.7.3 证书密钥更新请求的处理**

对于证书密钥的更新，订户须提交能够识别原证书的足够信息，如订户甄别名、证书序列号等，使用更新前的私钥对包含新公钥的申请信息签名。天威诚信将执行下述操作：

- 申请对应的原证书存在并且由认证机构签发。
- 用原证书上的订户公钥对申请的签名进行验证。
- 基于原注册信息进行身份鉴别。

#### **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**

无规定。

#### **4.8.3 证书变更请求的处理**

无规定。

#### **4.8.4 签发新证书时对订户的通告**

无规定。

#### **4.8.5 构成接受变更证书的行为**

无规定。

#### **4.8.6 CA 对变更证书的发布**

无规定。

#### 4.8.7 CA 对其他实体的通告

无规定。

### 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，最终订户证书必须吊销：

- 天威诚信、注册机构或最终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。
- 天威诚信或注册机构和订户达成的订户协议已经终止。
- 天威诚信或注册机构有理由相信证书签发时没有依据 CP、CPS 规定的有关程序，证书签发给非证书主体的人员（1 类证书中对应虚拟实体的证书除外）或没有鉴证该人员在证书主体中的命名就签发了证书（1 类证书中对应虚拟实体的证书除外）。
- 天威诚信或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。
- 对于 3 类证书，订户的组织机构名改变了。
- 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订户证书：

- 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订户证书。
- 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个人证书。
- 对于组织机构身份证书，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。
- 对于服务器证书，拥有该服务器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

当天威诚信或注册机构有充分的理由相信需要吊销最终订户的证书时，天威诚信或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，天威诚信或注

册机构将通过适当的方式，包括邮件、传真等，通知最终订户证书已被吊销及被吊销的理由。

订户可以通过各种方式要求吊销自己的证书，这些方式可以包括：

- 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 1、2、3 类证书。
- 通过电子邮件、传真、特快专递等可靠的方式告知天威诚信或注册机构。

#### **4.9.4 吊销请求宽限期**

当最终订户发现出现 4.9.1 中的情况时，应该尽快提出吊销请求，从发现需要吊销证书到向天威诚信或注册机构提出吊销请求的时间间隔，

- 对于 1 类证书不能超过 24 小时。
- 对于 2 类证书不能超过 8 小时。
- 对于 3 类证书不能超过 4 小时。

#### **4.9.5 CA 处理吊销请求的时限**

天威诚信或注册机构从接到吊销请求到完成处理请求的时间，

- 对于 1 类证书不能超过 24 小时。
- 对于 2 类证书不能超过 16 小时。
- 对于 3 类证书不能超过 8 小时。

#### **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零时为证书签发 CA 产生证书吊销列表。对于特别的证书签发 CA，天威诚信可定制证书吊销列表产生的频率。

#### **4.9.8 CRL 发布的最大滞后时间**

一个证书从它被吊销到它被发布到 CRL 上的滞后时间不超过 24 小时。

#### **4.9.9 在线状态查询的可用性**

天威诚信提供证书状态的在线查询服务（OCSP），该服务 7X24 小时可获得。

#### **4.9.10 在线状态查询要求**

依赖方应检查证书的吊销状态。如果依赖方未通过 CRL 方式查询，则应通过 OCSP 在线方式查询。

#### **4.9.11 吊销信息的其他发布形式**

除了 LDAP 目录服务发布 CRL、OCSP 服务器外，天威诚信所发布的 CRL 也可通过天威诚信网站上的相关 URL 获得。

#### **4.9.12 密钥损害的特别要求**

无论是最终订户还是天威诚信、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**

无规定。

#### **4.9.14 请求证书挂起的实体**

无规定。

#### **4.9.15 挂起请求的流程**

无规定。

#### **4.9.16 挂起的期限限制**

无规定。

### **4.10 证书状态服务**

天威诚信通过网站 URL、OCSP、LDAP 提供证书状态服务。

#### **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 RFC2560，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 证书状态服务须保证 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部门的相关规定，提供加密证书密钥的集中管理和恢复。

#### 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可以由天威诚信的密钥管理中心系统集中安全产生和保存，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) 证书持有人提出申请；
- 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

天威诚信认证机构的物理场地满足以下安全要求并最有效地控制风险：

- 防止物理非法进入  
7层物理结构及完善的安全管理体系保护天威诚信的运营设施和信息安全。
- 防止未经授权的物理访问  
确保未经过授权的人或仅被授权访问有限物理区域的人员不得访问天威诚信认证机构内的受到限制区域。
- 维护 CA 服务的完整性、可用性  
保障提供 CA 服务的系统、设施不受到破坏，保证认证服务不被中断。

### 5.1.1 场地位置与建筑

天威诚信认证业务的运营场地是按照《天威诚信物理场地建设规范》进行构建的，整体建筑由能够阻止物理穿透的材料建成。建筑物的外墙、地板和天花板都属于永久性建造，并互相联结，可以阻止未经授权进入、穿透。敏感区域及以上区域的墙壁，在其双层干饰面内墙之间，采用镀钢夹层。敏感区域只设置一个门作为的常规入口。根据消防要求置了消防紧急出口。敏感区域及以上区域没有窗口。通风孔、管道口或任何类似的通向敏感区域的孔口都采用了硬金属条进行加固。

物理安全是基于物理层级的保护，每一物理层就是一个屏障，需要设置可以控制进出的带锁的门来控制每个人进出每一个区域。每一层区域必须有非常严格的控制方法防止未经授权的物理访问。而且要求每一个物理安全层在物理上必须能完全包含下一个物理安全层，而且要求内部的安全层不能与外部的安全层使用一样外部墙体，最外层的安全层应该是整个建筑物的外墙。

### 5.1.2 物理访问控制

天威诚信的物理设施的访问控制系统是与控制各层门进出的门禁系统相结合的，并实现了以下安全功能：

- 进出每一道门都有记录作为审计依据；
- 系统采用身份识别卡和生物识别鉴定的控制方法，控制每道门的进出；
- 授权人员进出每一道门都会有时间记录和相关信息提示；
- 所有的门都设有强行开门报警。
- 四层以上的区域安装移动报警器，防止有任何未经允许的人员滞留在房间内；
- 整套访问控制系统配有断电保护装置，还配有发电机、UPS 提供紧急用电；

与门禁系统配合使用的还有录像监控系统，所有的录像资料根据安全审计要求保留一段时间。

### 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 7X24 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，天威诚信认证机构还具有加热/通风/空调系统控制运营设施中的温度和湿度。

### 5.1.4 水患防治

天威诚信数据中心有专门的技术措施，防止、检测漏水的出现，并能够在出现漏水时最大程度地减小漏水对认证系统的影响。

## 5.1.5 火灾防护

### 5.1.5.1 结构防火

天威诚信认证机构的运营中心耐火等级符合GBJ45《高层民用建筑设计防火规范》中规定的二级耐火等级，防护方法应符合当地管理部门或机构的安全要求。

### 5.1.5.2 火灾报警及消防设施

- 天威诚信认证机构设施内设置火灾报警装置。在机房内、各物理区域内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位设置烟、温感探测器。
- 敏感区及高敏区配置了独立的气体灭火装置。

### 5.1.5.3 紧急出口

根据国家的有关消防要求、规定和标准，在非敏感区及敏感区的办公区域内，设置了紧急出口，紧急出口设有消防门。紧急出口有监控设备进行实时监控，并保证紧急出口门随时可用。紧急出口门外部没有门开启的装置，且紧急出口门与门禁报警设备联动外。非紧急避险状态下，紧急出口门不能被内部人员任意打开。

## 5.1.6 介质存储

天威诚信认证机构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

天威诚信对敏感的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的指南将其物理销毁或初始化。其他废物处理按天威诚信正常废物处理的要求进行。

## 5.1.8 异地备份

天威诚信认证机构对关键系统数据、审计日志数据和其他敏感信息进行日常备份，这些备份信息保存在天威诚信建筑物以外的安全的地方。

## 5.1.9 注册机构物理控制

天威诚信注册机构的物理场地也需要有足够的安全措施，保证只有授权的人员才能进入，只有授权的人员才能接触系统进行证书管理。

## 5.2 程序控制

### 5.2.1 可信角色

天威诚信的可信人员包括：

- 鉴证和客户服务人员
- 安全管理人员
- 密钥与密码设备管理人员
- 加密设备操作人员
- 系统管理员
- 人力资源管理人员
- 掌握 CA 秘密共享的人员。
- 能够进入三层以上工作区域的人员。

### 5.2.2 每项任务需要的人数

天威诚信有严格策略和控制程序，以保障基于工作性质的职责分离。最敏感的操作要求多名可信人员共同参与完成。

- 鉴证和签发 3 类证书，要求 2 个可信人员的参与。
- 访问 CA 密钥离线生成室和 CA 密钥离线存放室，至少两名有访问权限的人员。
- 掌管秘密共享，至少 5 人。
- 操作存放有 CA 密钥的密码设备，包括密钥生成、分配、备份、销毁等，至少需要 3 个秘密共享持有人，一个密钥管理员，一个见证人。

### 5.2.3 每个角色的识别与鉴别

对于物理访问控制，天威诚信通过门禁磁卡、指纹识别鉴别不同人员，并确定相应的权限。

对于进行证书生命周期管理的天威诚信、注册机构证书管理员，他们使用相应的数字证书访问认证系统、注册机构系统，完成证书管理工作。

对于系统维护人员，他们使用安全的身份鉴别机制进入认证系统进行维护工作。

### 5.2.4 需要职责分割的角色

所谓职责分割，是指如果一个人担任了完成某一职能的角色，就不能再担任完成另一特定职能的角色。天威诚信对如下人员进行了职责分割：

- 密钥管理员
- 安全管理员
- 证书申请鉴证人员
- 系统维护人员

- 秘密分割持有者

### 5.3 人员控制

#### 5.3.1 资格、经历和无过失要求

在天威诚信中担任一定角色、执行一定功能、完成一定工作的人员，其所受教育、培训及工作经历应足够胜任其工作。

天威诚信客户服务人员必须受过专门的客户服务技能培训，通过 PKI 及相关应用基本知识培训，熟悉有关证书业务，考试通过后方能进行有关工作。这些培训和考试由天威诚信负责。

天威诚信安全管理人员必须熟悉、掌握有关的安全知识和安全管理，熟悉天威诚信安全要求，熟悉天威诚信安全与审计指南，有很强的责任感。为了达到此要求，天威诚信将对安全管理人员进行培训。

天威诚信密钥与密码设备管理人员必须熟悉 PKI 基本知识，熟悉 CA 证书和密钥相关的证书，如 CA 证书的产生、签发、更新、密钥更新等，熟悉有关密码设备操作使用。

天威诚信所有的可信人员必须符合清白要求：没有伪造教育、工作经历，没有违法犯罪记录，工作中没有严重的不诚实行为。

#### 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。在成为天威诚信的可信人员前，有关人员必须提交相关材料，以证明他们能够胜任预期的工作。

天威诚信依据有关材料进行背景调查，在调查过程中，天威诚信将为有关人员保密，保护其隐私。

背景调查时如果出现提交材料与事实不符或证明提交材料为捏造时，天威诚信将拒绝可信职位候选人获得有关职位或取消其可信人员的资格。

#### 5.3.3 培训要求

为了使有关人员能胜任其承担的工作，天威诚信对所有入职员工制定有专门的培训计划，培训内容包括：

- 本人工作职责。
- 安全管理要求及制度。
- 事故和安全威胁的报告和处理。

对于销售、服务和支持还包括

- PKI 及应用。
- 天威诚信的产品与服务。
- 客户服务流程与要求（客户服务）。

- 安全操作流程（系统、密钥）。

#### 5.3.4 再培训周期和要求

天威诚信根据业务需要安排。

#### 5.3.5 工作岗位轮换周期和顺序

内部安排。

#### 5.3.6 未授权行为的处罚

天威诚信对于未授权行为或其他违反公司安全策略和程序的行为制定有相应的处罚措施，包括警告、罚款直至辞退，情节严重的将依法追究刑事责任。

#### 5.3.7 独立合约人的要求

在有限制的情况下，独立合约人或顾问可以担任可信职位。任何合约人或顾问在某一职务的职能和安全标准应与相应职位的内部雇员一样。

担任可信角色的独立合约人和顾问需要通过 5.3.2 中所述的背景调查程序，否则，他们不能担任可信角色，当进入敏感区时，只能在认证机构人员的陪同和直接监督下访问认证机构的安全设施，完成有关的工作。

#### 5.3.8 提供给员工的文档

提供给员工的文档通常包括员工培训资料及员工工作手册，这些资料通常是不公开的。

### 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 密钥生命周期内的管理事件，包括：
  - 密钥生成，备份，存储，恢复，归档和销毁。
  - 密码设备生命周期的管理事件，例如接收、使用、卸载和弃用。这些记录都是密钥管理员完成的纸质记录。
- CA 和订户证书生命周期内的管理事件，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自动记录，保存在数据库。

- 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。
- 对于系统文件的非授权的访问及访问企图。
- 安全、敏感的文件或记录的读、写或删除。
- 系统崩溃，硬件故障和其他异常。
- 防火墙和路由器记录的安全事件。

这些记录由操作系统自动完成，天威诚信的系统维护人员会定期检查系统日志。

- 系统操作事件

- 系统启动和关闭。
- 系统权限的创建、删除、设置或修改密码。

这些记录由操作系统自动完成，天威诚信的系统维护人员会定期检查系统日志。

- 天威诚信物理设施的访问

- 授权人员进出。
- 非授权人员进出及陪同人。
- 安全存储设施（离线密钥）的访问。

授权人员进出物理设施由天威诚信物理场地的访问控制系统自动记录。非授权人员进出由陪同人员作纸质记录。

- 可信人员管理记录，包括且不限于：

- 网络权限的帐号申请记录
- 系统权限的申请、变更、创建申请记录
- 人员情况变化

日志记录包括如下信息：

- 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。
- 日志记录的种类。

#### 5.4.2 处理日志的周期

对于 CA 和订户证书生命周期内的管理事件日志，天威诚信将一个季度进行一次内部检查、审计。

系统安全事件和系统操作事件日志天威诚信将每周进行一次检查、处理。

天威诚信物理设施的访问日志天威诚信将每月进行一次检查、处理。

### 5.4.3 审计日志保存期限

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

天威诚信采取了物理和逻辑的访问控制方法，防止未经授权而浏览、修改、删除或以其他方式篡改电子或纸质审计日志文件。

### 5.4.5 审计日志备份程序

对于认证系统的日志，天威诚信定期进行备份。

### 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，则有专门的文件管理柜来实现审计信息的收集。

### 5.4.7 对导致事件主体的通知

当审计记录报告一个事件时，天威诚信会立即通知引起该事件的个人、组织机构。

### 5.4.8 脆弱性评估

根据审计记录，天威诚信定期进行系统、物理场地、运营管理、人事管理等方面的安全脆弱性评估，并根据评估报告采取措施。

## 5.5 记录归档

### 5.5.1 归档记录的类型

天威诚信归档下列信息：

- 审计记录的归档依据§ 5.4.1 要求
- 证书申请信息
- 证书签发过程中的支持文档
- 证书生命周期的相关信息

### 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。

- 对订户证书生命周期内的管理事件的归档，保留一年以上。
- 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。

### 5.5.3 归档文件的保护

天威诚信对各种电子、磁带、纸资形式的归档文件，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

天威诚信对归档文件定期进行备份，分为增量备份和全备份。增量备份每天进行，全备份每周进行。备份文件将被放在异地进行保存。

### 5.5.5 记录时间戳要求

天威诚信对每项目志有时间记录。对于纸质记录，有操作人员手工记录；对于电子记录，由系统自动增加时间，但 these 时间未采用时间戳技术。

### 5.5.6 归档收集系统

天威诚信有专门的电子归档文档的存放系统。

### 5.5.7 获得和检验归档信息的程序

只有可信人员才可以查看和获得归档信息，这些信息被归还时必须得到验证。

## 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（或最终订户）的证书请求，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，这些应急处理方案有，

- 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
- 安全事故应急处理方案等。

### **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，当出现计算机资源、软件和/或数据的损坏时在最短的时间内恢复被损害的资源、软件和/或数据。

### **5.7.3 实体私钥损害处理程序**

对于实体私钥的损害，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) 当天威诚信或注册机构的 CA 证书出现私钥损害时，天威诚信将立即吊销 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其业务。

## 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中止业务的规定要求进行有关工作。

## 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

对于天威诚信 CA 密钥对，天威诚信专门的密钥管理员及若干名接受过相关培训的可靠雇员在天威诚信安全设施中的密钥生成室（CPS § 5.1.1.2）按照天威诚信的密钥管理策略中规定的密钥生成规程进行产生。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。天威诚信 CA 的密钥对采用硬件实现，所使用的生成及保存的密码模块（含密钥生成算法芯片）符合国家密码主管部门的要求，并通过国家密码主管部门的鉴定。

##### 6.1.1.2 最终订户密钥对的产生

对于 1 类证书，订户可以使用浏览器自带的密码模块生成密钥对，也可以使用硬件密码模块（如 USB Key，智能卡）产生密钥对；对于 2 类证书，订户最好使用硬件密码模块生成密钥对；对于第 3 类证书组织机构身份证书、组织机构代表人证书，建议在密钥对产生后，使用 USB Key、智能卡等硬件密码设备存放私钥；对于服务器证书，订户利用 Web 服务程序软件提供的密钥生成功能生成密钥对或采用专门的硬件加速模块产生密钥对。

#### 6.1.2 私钥传送给订户

私钥传送给订户过程按照 CP § 6.1.2 进行。

#### 6.1.3 公钥传送给证书签发机关

需要天威诚信认证的证书公钥，最终订户通过 PKCS#10 格式的证书签名请求信息文件包格式，以电子的方式将公钥提交给认证机构（或通过注册机构），这些请求通过网络传送时使用安全套接层协议（SSL）和其他安全协议。

### 6.1.4 CA 公钥传送给依赖方

对于天威诚信的主 CA 公钥，通过如下方式传输给依赖方：

- 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，或
- 2) 依赖方访问天威诚信的目录系统，或
- 3) 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，或
- 4) 天威诚信、注册机构或其合作伙伴通过签名电子邮件将 CA 证书传输给依赖方，或
- 5) 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最终订户。

### 6.1.5 密钥的长度

天威诚信 CA 和最终订户密钥对至少是 1024 位 RSA。

### 6.1.6 公钥参数的生成和质量检查

符合国家密码管理部门的要求。

### 6.1.7 密钥使用目的

主 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。订户证书的使用目的需满足证书策略的要求，证书中的密钥用法扩展项按表 6 所示设定：

表 8 - 密钥用法扩展项的设置

	CA 证书	1 类证书	2 类个人 签名证书	2 类个人 加密证书	3 类组织机 构身份证 书、组织机 构代表人证 书	3 类服务器 证书
criticality	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
0 digitalSignature	Clear	Set	Set	Clear	Set	Set
1 nonRepudiation	Clear	Clear	Clear	Clear	Set	Clear
2 keyEncipherment	Clear	Set	Clear	Set	Clear	Set
3 dataEncipherment	Clear	Clear	Clear	Clear	Clear	Clear
4 keyAgreement	Clear	Clear	Clear	Clear	Clear	Clear
5 KeyCertSign	Set	Clear	Clear	Clear	Clear	Clear
6 CRLSign	Set	Clear	Clear	Clear	Clear	Clear
7 EncipherOnly	Clear	Clear	Clear	Clear	Clear	Clear

		CA 证书	1 类证书	2 类个人 签名证书	2 类个人 加密证书	3 类组织机 构身份证 书、组织机 构代表人证 书	3 类服务器 证书
8	DecipherOnly	Clear	Clear	Clear	Clear	Clear	Clear

## 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

天威诚信使用国家密码管理部门认可、批准的硬件密码模块生成主 CA、证书签发 CA 和其他 CA 密钥对，存储 CA 私钥。

天威诚信制定有专门密码管理策略，在从运送、验收、初始化、离线存放、在线使用到销毁的整个密码设备生命周期内，对密码模块进行管理和控制。CA 密码模块离线存放在 CA 密钥离线存放区中（见 5.1.1.2），CA 密码模块在线放置在屏蔽机房或机柜中（见 5.1.1.2）。CA 密码设备的操作遵从多人在场、多人控制的原则。

### 6.2.2 私钥多人控制（m 选 n）

天威诚信的各类 CA 私钥存放在硬件加密卡中，该加密卡启动的秘密被分割保存在 5 张 IC 卡中（称为秘密共享），这 5 张 IC 卡由天威诚信 5 名可信雇员持有（称为秘密分管者），保存天威诚信内部保险盒中。当要操作使用 CA 私钥时（离线），需要 3 名秘密分管者持有秘密共享 IC 卡才能启动加密卡。

### 6.2.3 私钥托管

天威诚信所有 CA（包括主 CA 和运营 CA）的私钥均未托管。

### 6.2.4 私钥备份

天威诚信对 CA 私钥通过专门的备份加密卡进行备份，这些备份分别作为本地常规备份和异地灾难恢复备份。对备份加密卡的保护符合 CP § 6.2.4 的要求。

对于最终订户证书，如 1 类、2 类证书和服务器证书，天威诚信会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 CPS § 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 CPS § 6.2.10 销毁。

## 6.2.6 私钥导入、导出密码模块

天威诚信的 CA 密钥对在硬件密码模块上生成，保存和使用。此外，为了常规恢复和灾难恢复，天威诚信对 CA 密钥进行复制。当 CA 密钥对从一个硬件密码模块复制到另一个硬件密码模块上时，被复制的密钥对以加密的形式在模块之间传送，并且在传递前要进行模块间的相互身份鉴别。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、被窃、修改、非授权的泄露、非授权的使用。

## 6.2.7 私钥在密码模块的存储

天威诚信 CA 私钥以加密的形式存放在硬件密码模块中，在密码模块中使用。

## 6.2.8 激活私钥的方法

### 6.2.8.1 用户证书私钥

#### 6.2.8.1.1 1类证书

天威诚信签发的 1 类证书的私钥可以存放在订户计算机的软件密码模块中，这时订户应该采用合理的措施从物理上保护计算机以防止在没有得到订户授权的情况下其他人员使用订户的计算机。如果存放在软件密码模块中的私钥没有口令保护，那么，软件密码模块的加载意味着私钥的激活。如果该私钥有口令保护，软件密码模块加载后，还需要输入口令才能激活私钥。

天威诚信签发的 1 类证书的私钥还可存放在诸如 USB Key 和智能卡等硬件密码模块中，这时私钥可以通过 PIN 码（口令）或指纹鉴别等安全机制保护。如果私钥没有 PIN 码（口令）或指纹鉴别保护，那么，当用户计算机上安装了相应的硬件密码模块驱动程序后，将 USB Key 或智能卡插入到相应的读卡设备中，私钥将会被激活可以使用。如果私钥有 PIN 码（口令）或指纹鉴别保护，那么，当用户计算机上安装了相应的驱动程序并将 USB Key 或智能卡插入到相应的读卡设备中后，只有输入 PIN 码（口令）或指纹信息，私钥才被激活可以使用。

#### 6.2.8.1.2 2类证书

天威诚信签发的 2 类证书的私钥激活类似于 1 类证书，只是对于 2 类证书，天威诚信建议将私钥存放在诸如 USB Key、智能卡等硬件密码模块中，并且私钥通过 PIN 码（口令）或指纹鉴别等机制保护。

#### 6.2.8.1.3 3类证书

对于天威诚信签发的组织机构身份证书、组织机构代表人证书，建议订户使用 USB Key、智能卡等硬件密码设备存放私钥，私钥不能出卡，并且订户要使用 PIN 码（口令）

或指纹鉴别等机制保护私钥。要激活私钥，用户计算机上需安装相应的驱动程序并将 USB Key 或智能卡插入相应的读卡设备，输入相应的 PIN 码（口令）或指纹鉴别信息，私钥才激活可以使用。

#### 6.2.8.2 服务器证书

对于天威诚信签发的服务器证书，如果没有使用硬件密码模块产生、保存私钥，则私钥是存放在服务程序的软件密码模块中，这时订户应该使用口令对私钥进行保护。当服务程序启动，软件加密模块被加载，并输入相应的私钥保护口令后，证书私钥被激活。

如果使用硬件密码模块，则私钥需要被口令保护。当硬件密码模块被安装到订户服务器上，服务程序启动，并输入相应私钥保护口令后，证书私钥被激活。

#### 6.2.8.3 CA 私钥

天威诚信的 CA 私钥存放在硬件密码模块中，并且其激活数据按 CPS § 6.2.2 进行分割。当需要使用 CA 私钥时，将硬件密码模块加载并按 5 选 3 的原则输入激活数据的秘密共享。

#### 6.2.9 解除私钥激活状态的方法

对于存放在软件密码模块中的 1 类、2 类证书的私钥，当软件密码模块被下载、用户退出登录状态、操作关闭或计算机断电时，私钥被解除激活状态。对于存放在硬件密码模块中的 1 类、2 类、3 类证书的私钥，当每次操作后注销计算机，或者把硬件密码模块从读卡器中取出时，私钥成为非激活状态。对于服务器证书，当服务程序下载、系统注销或系统断电后私钥即进入非激活状态。

对于天威诚信 CA 私钥，当存放私钥的硬件密码模块断电，私钥进入非激活状态。

#### 6.2.10 销毁私钥的方法

私钥不再使用、不需要保存时，应该将私钥销毁，从而避免丢失、偷窃、泄露或非授权使用。

对于天威诚信签发的最终订户加密证书私钥，在其生命周期结束后，订户应该妥善保存一定期限，以便于解开加密信息。对于天威诚信签发的最终订户签名私钥，在其生命周期结束后，无需再保存，可以通过私钥的删除、系统或密码模块的初始化来销毁。

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。

#### 6.2.11 密码模块的评估

由国家密码管理部门负责。

## 6.3 密钥对管理的其他方面

### 6.3.1 公钥归档

对于生命周期外的 CA 和最终订户证书，天威诚信将进行归档，归档的证书存放在归档数据库中。

### 6.3.2 证书操作期和密钥对使用期限

公钥和私钥的使用期限与证书的有效期限相关但却有所不同。

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，直到私钥受到损害或密钥对存在被破解的风险，如加密算法被破解。当私钥受到损害或密钥对存在被破解的风险后，签名证书的公钥在技术上仍然可以用于验证数字签名，但这种验证在法律上不一定是有效的。

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。

另外无论是订户证书还是 CA 证书，有效期到了后，在保证安全的情况下，允许证书进行更新而密钥对不变。但是密钥对不能无限期使用。对于不同的证书，密钥对通过证书更新允许的最长使用期限如下：

- 对于 2048 位根证书，其密钥对的最长允许使用年限是 50 年。
- 对于 1024 位主 CA 证书，其密钥对的最长允许使用年限是 30 年。
- 对于 1024 位其他 CA 证书，其密钥对的最长允许使用年限是 15 年。
- 对于 1024 位最终订户证书，其密钥对的最长允许使用年限是 2 年。

## 6.4 激活数据

### 6.4.1 激活数据的产生和安装

存放有天威诚信 CA 私钥的加密卡的激活信息（秘密共享），其产生按天威诚信密钥生成规程参考指南中的规定进行。所有秘密共享的创建和分发有相应的记录，包括产生时间、持有人等信息。

天威诚信 CA 私钥的激活数据由硬件加密卡内部产生，并分割保存在 5 个 IC 卡中，需通过专门的读卡设备和软件读取。

如果订户证书、管理员证书、或 RA 证书的私钥的激活数据是口令，这些口令必须：

- 由用户产生；
- 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；
- 不能和操作员的姓名相同；
- 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+密码，生物识别设备+密码等）来控制私钥的激活。

## 6.4.2 激活数据的保护

保存有天威诚信 CA 私钥的激活数据的 5 个 IC 卡，由天威诚信 5 个不同的可信人员持有，而且持有人员必须符合职责分割的要求，签署协议确认他们知悉秘密分管者责任。秘密共享必须存放在保险盒中。

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

## 6.4.3 激活数据的其他方面

### 6.4.3.1 激活数据的传送

存有天威诚信 CA 私钥的激活数据的 IC 卡，通常保存在天威诚信的安全设施中，不能携带外出或传送。如因某种特殊情况确实需要传送时，其传送过程需在天威诚信安全管理人员和密钥管理人员的监督下进行。

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

### 6.4.3.2 激活数据的销毁

存有天威诚信 CA 私钥的激活数据的 IC 卡，其销毁所采取的方法包括将 IC 卡初始化，或者彻底销毁 IC 卡，无论采取何种方式，都将保证不会残留有任何秘密信息。CA 私钥激活数据的销毁是在天威诚信安全管理人员和密钥管理人员的监督下进行。

当订户证书私钥的激活数据不需要时应该销毁，订户应该确保无法通过残余信息、介质直接或间接恢复激活数据的部分或全部，比如记录有口令的纸页必须粉碎。

## 6.5 计算机安全控制

### 6.5.1 特别的计算机安全技术要求

天威诚信的证书认证系统主机实现了自主访问控制（DAC），进行了安全漏洞扫描和安全优化，安装了防病毒系统，确保了包含 CA 软件和数据文件的系统是安全可信的系

统，不会受到未经授权的访问。此外，认证机构只允许有工作需求的必要人员访问产品服务器，一般的应用用户在产品服务器上没有账户。

认证机构的生产系统网络与其它部分逻辑分离，并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，只有认证机构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直接访问认证系统数据库。

## **6.5.2 计算机安全评估**

天威诚信的 CA 系统及其运营环境通过了中国国家信息安全测评认证中心的运营系统安全测评。

## **6.6 生命周期技术控制**

### **6.6.1 系统开发控制**

天威诚信通过内部流程来控制证书认证系统的研发工作，并确保该系统安装的可靠性。

### **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**

天威诚信的证书认证系统在系统设计过程中充分进行了安全性考虑，在开发过程中有严格的流程进行代码安全管理，在开发完成后进行了严格的安全测试，在正式使用前通过了国家有关部门的系统安全性审查。

## **6.7 网络的安全控制**

天威诚信证书认证系统网络进行安全漏洞扫描和安全优化，部署了防火墙、入侵检测系统，并在系统通信过程中使用加密和数字签名进行保护。

## **6.8 时间戳**

天威诚信暂不提供时间戳服务。

## 7. 证书、CRL 和 OCSP

### 7.1 证书

天威诚信签发的证书符合(a)ITU-T X.509v3 4-edition (2001)：信息技术-开放系统互连-目录：认证框架(1997年6月)标准；(b)RFC 3280：Internet X.509 公钥基础设施证书和 CRL 结构(1999年1月)。

证书至少包含基本的 X.509v1 域，其规定值或值的限制如表 7 所描述。

表 9 – 证书结构的基本域

域	值或值的限制
版本	V3
序列号	每个证书唯一的值
签名算法	用于签证书的算法的名称(见 CPS § 7.1.3)
签发者 DN	签发者的甄别名。
有效期从	基于国际通用时间(UTC)，和北京时间同步，按 RFC 3280 要求编码
有效期到	基于国际通用时间(UTC)，和北京时间同步，按 RFC 3280 要求编码。有效期限的设置符合 CPS § 6.3.2 规定的限制
主体 DN	证书持有者或实体的甄别名。
公钥	根据 RFC 3280 编码，使用 CPS § 7.1.3 中指定的算法，密钥长度满足 CPS § 6.1.5 指定的要求。
签名	生成和编码满足 RFC 3280 的要求。

#### 7.1.1 版本号

X.509v3 证书。

#### 7.1.2 证书扩展项

针对特别的用户，天威诚信签发的证书有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，不同证书该扩展项的设置见 CPS § 6.1.7。这个扩展项的 criticality 域通常设置为 FALSE。

### 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**。最终订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 **FALSE**。

CA 证书的基本限制扩展项中的路径长度设定为在证书路径中该证书之后的 **CA** 级数。对于最终订户证书签发 CA，其 CA 证书“**pathLenConstraint**”域的值设为 **0**，表示证书路径中仅有一个最终订户证书可以跟在这个 CA 证书后面。

### 7.1.2.5 扩展的密钥用法 (Extended Key Usage)

对天威诚信不同的证书，扩展的密钥用法扩展项设定如下。

**表 10 - 可扩展的密钥用法扩展项的设置**

		3 类服务器 CA 证书	3 类服务器证书	3 类组织机构身份证书	3 类组织机构代表人证书	1 类和 2 类个人证书
<b>Criticality</b>		FALSE	FALSE	FALSE	FALSE	FALSE
<b>0</b>	ServerAuth	Set	Set	Clear	Clear	Clear
<b>1</b>	ClientAuth	Set	Set	Set	Set	Set
<b>2</b>	CodeSigning	Clear	Clear	Clear	Clear	Clear
<b>3</b>	EmailProtection	Clear	Clear	Clear	Set	Set
<b>4</b>	IpssecEndSystem	Clear	Clear	Clear	Clear	Clear
<b>5</b>	IpssecTunnel	Clear	Clear	Clear	Clear	Clear
<b>6</b>	IpssecUser	Clear	Clear	Clear	Clear	Clear
<b>7</b>	TimeStamping	Clear	Clear	Clear	Clear	Clear
<b>8</b>	OCSP Signing	Clear	Clear	Clear	Clear	Clear
-	Microsoft Server Gated Crypto (SGC) - OID: 1.3.6.1.4.1.311.10.3.3	Clear	Set	Clear	Clear	Clear
-	Netscape SGC - OID: 2.16.840.1.113730.4.1	Set	Set	Clear	Clear	Clear
-	TBD - OID: 2.16.840.1.113733.1.8.1	Set	Set	Clear	Clear	Clear

#### 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 项应设为 FALSE。

#### 7.1.2.7 签发 CA 密钥标识符

天威诚信最终订户证书及中级 CA 证书中有签发 CA 密钥标识符扩展项，当证书签发者包含主体密钥标识扩展项时，签发 CA 密钥标识符由 160 位的签发证书的 CA 的公钥进行 SHA-1 散列运算后的值构成；否则，它将包含签发 CA 的主体 DN 和序列号。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

天威诚信签发的证书按照 RFC 3280 标准，用 sha1RSA 算法签名：

sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}。

### 7.1.4 名称形式

天威诚信签发证书的甄别名符合 X500 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 签发机构中的部门或服务类（如 CN Individual Consumer Service Center）。甄别名可以包含不止一个的 OU 用于存放其他信息，如可将一个附加的组织部门(OU)域包含在最终订户证书中，该域指出证书对应的依赖方协议所在的 URL。

### 7.1.5 名称限制

除一类证书外，天威诚信签发的其他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

天威诚信的每类证书（1 类、2 类、3 类）对应一个证书策略对象标识符。当使用证书策略扩展项时，天威诚信签发证书中包含证书策略对象标识符，该对象标识符与相应的证书类别对应。

### 7.1.7 策略限制扩展项的用法

没使用。

### 7.1.8 策略限定符的语法和语义

没有规定。

### 7.1.9 关键证书策略扩展项的处理规则

与 ITU X.509 和 RFC3280 规定一致。

## 7.2 CRL

天威诚信认证系统签发的 CRL 符合 RFC3280 标准。CRL 至少包含如表 9 所述基本域和内容。

表 11 – CRL 结构的基本域

域	值或值的限制
版本	V2
签名算法	签发 CRL 的算法。使用 sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) 算法签名。
颁发者	签发 CRL 的实体。颁发者甄别名。
有效期	CRL 的签发日期。
下次更新	CRL 下次签发的日期。对于主 CA, 隔 3 个月; 对于其他 CA、隔 10 天。最终订户证书 24 小时。
吊销的证书	列出吊销的证书, 包括吊销证书的序列号和吊销日期。

### 7.2.1 版本号

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

天威诚信认证系统签发的 OCSP 响应符合 RFC2560 标准。OCSP 响应至少包含如表 10 所述基本域和内容。

表 12 – OCSP 结构的基本域

域	值或值的限制
状态	响应状态，包括成功、请求格式错误、内部错误、稍候重试、请求没有签名和请求签名证书无授权，当状态为成功时必须包括以下各项。
版本	V1
签名算法	签发 OCSP 的算法。使用 sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)算法签名。
颁发者	签发 OCSP 的实体。签发者公钥的 SHA1 数据摘要值和证书甄别名。
产生时间	OCSP 响应的产生时间。
证书状态列表	包括请求中所查询的证书状态列表。每个证书状态包括证书标识、证书状态以及证书吊销信息。
证书标识	包括数据摘要算法(SHA1, OID: 1.3.14.3.2.26)、证书甄别名数据摘要值、证书公钥数据摘要值和证书序列号。
证书状态	证书的最新状态，包括有效、吊销和未知。
证书吊销信息	当返回证书状态为吊销时包含吊销时间和吊销原因。

### 7.3.1 版本号

V1。

### 7.3.2 OCSP 扩展项

与 RFC2560 一致。

## 8. 认证机构审计和其他评估

天威诚信定期对物理控制、密钥管理、操作控制、鉴证执行等情况进行审查，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

天威诚信每年进行一次一致性审计，即信息产业主管部门的年度审查。

## **8.2 评估者的资质**

天威诚信将选择熟悉 IT 运营管理、具有多年审计经验的审计机构对天威诚信的运营管理进行一致性审计。在进行审计前，审计机构必须熟悉公钥基础设施技术。

## **8.3 评估者与被评估者之间的关系**

评估者为独立的第三方审计机构，与天威诚信不存在任何商业利益关系。

## **8.4 评估的内容**

评估的内容包括：CA 环境控制、密钥管理操作和 CPS 的执行情况等。

## **8.5 对问题与不足采取的措施**

天威诚信管理层将对审计报告进行评估，对在一致性审计中发现的重大意外或不作为积极采取补救措施，直到问题解决。从完成审计到采取行动纠正问题的时间不超过 30 天。

## **8.6 评估结果的传达与发布**

信息产业部门年度审查结果将其相关网站上公开，任何人均可查询。

## **8.7 其他评估**

除了信息产业主管部门的年度审计外，天威诚信将定期进行内部审计评估，审计评估的内容与外部审计一致。

# **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**

根据市场和管理部门的规定自行决定。

### **9.1.2 证书查取的费用**

天威诚信目前不对证书查取收取专门的费用。

### 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）的获取不应收取任何费用。天威诚信有可能根据需要 will 将 OCSP 服务作为增值服务收取费用。

### 9.1.4 其他服务费用

无规定。

### 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

天威诚信客户保障计划提供的服务保障针对的最终实体主要是证书订户和证书依赖方。

## 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

天威诚信保密的信息包括但不限于：

- 系统方面
  - 认证系统结构、配置，包括系统、网络、数据库等；
  - 认证系统安全策略和方案；
  - 系统操作、维护记录；
  - 各类系统操作口令。

- 运营管理方面
  - 物理安全策略与实施方案，包括场地、访问控制、入侵检测等实施方案；
  - 密钥管理策略与操作记录；
  - CA 或 RA 批准或拒绝的申请纪录；
  - 可信人员名单；
  - 内部安全管理策略与制度。
  
- 客户信息
  - 客户的注册信息；
  - 客户系统、应用访问 CRL、OCSP 的记录（时间、频度）；
  - 客户与认证机构、注册机构签订的协议；

### 9.3.2 不属于保密的信息

证书、证书状态信息及信息库中的信息，都不是不需保密的信息。

### 9.3.3 保护保密信息

天威诚信不但有各种严格的管理制定、流程和技术手段保护自身的商业秘密，并且把保护客户信息作为自己应尽的义务。天威诚信的每个员工都要接受信息保密方面的培训。

## 9.4 个人隐私保密

### 9.4.1 隐私保密方案

天威诚信有客户隐私计划保护证书订户的个人

### 9.4.2 作为隐私处理的信息

作为隐私处理的信息包括，最终订户注册申请证书中提交的、但不在证书中显示的信息，包括联系电话、地址等；个人与天威诚信、注册机构签订的协议。

### 9.4.3 不被视为隐私的信息

不被认为是隐私信息包括，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**

天威诚信或其注册机构如果需要将客户隐私信息用于双方约定的用途以外的目的，则需要事先告知客户并获得客户同意和授权，用户同意和授权信息以下列方式之一传送给天威诚信或其注册机构：

- 1) 有手写签名的同意和授权文件，并将文件邮寄、快递到天威诚信或其注册机构，  
或者
- 2) 将手写签名的同意和授权文件传真到天威诚信，或者
- 3) 以签名电子邮件的形式同意并授权。

#### **9.4.6 依法律或行政程序的信息披露**

由于法律执行、法律授权的行政执行的需要，天威诚信及其注册机构有可能需要将有关信息在客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**

#### **9.5.1 证书和吊销信息中的知识产权**

天威诚信对它签发的证书、证书吊销列表及其中信息的拥有知识产权，证书公钥是订户的知识产权。

#### **9.5.2 CPS 中的知识产权**

天威诚信对本 CPS 拥有知识产权。

#### **9.5.3 命名中的知识产权**

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。

#### **9.5.4 密钥和密钥材料的知识产权**

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

订户同意天威诚信订户协议是订户注册申请天威诚信证书的一个条件，在订户成功完全证书申请注册前，订户必须以下列两种方式之一接受订户协议：

- 1) 对订户协议文件签名并提交给天威诚信或其注册机构，或者
- 2) 阅读注册页面上订户协议，并点击同意订户协议。

依赖方决定信赖天威诚信签发的证书前需阅读天威诚信依赖方协议，用户接收证书及状态信息即表明其接受了依赖方协议。

天威诚信不负责评估证书是否被恰当使用。订户和依赖方必须依订户协议和依赖方协议确保证书用于允许使的目的。

天威诚信、注册机构和订户之间的担保、免责和有限责任由他们之间的协议规定约束。

天威诚信对证书订户做出如下担保：

- 证书中不存在批准证书申请或签发证书时天威诚信已知的对事实的实质性错误描述；
- 批准证书申请或签发证书时，不会因为工作疏忽将错误信息包含到了证书中；
- 证书满足天威诚信 CTN 证书策略所有实质性的要求；
- 吊销服务和信息库的使用在所有方面符合天威诚信 CTN 证书策略的要求。

天威诚信对证书依赖方做出如下担保：

- 除了未经鉴证的订户信息外，包含在证书中的所有信息都是准确的。
- 在天威诚信信息库中发布的证书已经签发给了个人或组织机构（它们的名字包含在证书中），订户已经根据 CPS § 4.4 接收了该证书。
- 批准证书申请或签发证书的实体签发证书时完全遵守了 CP、CPS 的规定。
- 天威诚信所采纳的与证书服务有关的技术，基于目前的技术发展与评估是安全的、可靠的。
- 天威诚信已通过技术的、物理的防护及流程控制，确保服务系统、设备和设施的安全、可靠。

### 9.6.2 RA 的陈述与担保

天威诚信认证机构的注册机构必须做出如下担保：

RA 在批准证书前，完成了所有必要的确认工作，并且确认了信息是正确的、准确的。

### 9.6.3 订户的陈述与担保

作为获得证书的一个条件，证书申请人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；

- 订户提供的，特别是包含在证书中的信息是真实的、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，订户已经接收了证书，且该证书没有过期或吊销。
- 订户对自己的私钥进行了有效的保护，其他人员无法使用订户的私钥。

#### 9.6.4 依赖方的陈述与担保

依赖方确认，在任何信赖行为发生之前，阅读了依赖方协议，并评估了在特定应用中信赖证书的适当性，不在证书适用目的以外的应用中信任证书。

#### 9.6.5 其他参与者的陈述与担保

为天威诚信提供客户身份验证服务的第三方已向天威诚信做出如下承诺，

- 是合法的、获得授权的组织机构信息服务提供商；
- 提供的信息权威性的，覆盖全国；
- 在其能够管理与控制范围了，其提供的数据是真实的、准确的；
- 其保存的组织机构信息在最短的时间内获得了更新。

#### 9.7 担保免责

天威诚信不对其签发的证书适用于其规定的目的以外的任何应用承担任何担保，对证书在其规定的目的以外的应用不承担任何责任。对由不可抗力，如战争、地震、洪灾、爆炸、恐怖活动等，造成的服务中断并由此造成的客户损失，天威诚信及注册机构不承担责任。

#### 9.8 有限责任

对于由于天威诚信自身原因，如没有严格按业务流程进行证书审批导致证书的错误签发、假冒，或管理上的疏忽导致 CA 私钥泄漏、盗用等，造成了证书订户、依赖方的损失，天威诚信将承担相应的赔偿责任，但这种责任是有限的。根据证书的类别，天威诚信所承担的有限责任的赔偿见表 10。

表 13 – 责任赔偿

证书类别	责任赔偿
2类	最高人民币 10,000 元
3类	最高人民币 24,000 元

天威诚信只对由于自身原因造成的用户直接损失承担责任，对间接的损失不承担责任。

## 9.9 赔偿

有下列情形之一的，天威诚信承担有限的赔偿责任：

- 天威诚信将证书错误的签发给订户以外的第三方，导致订户或者依赖方遭受损失的；
- 订户提交的注册信息或者资料真实、完整、准确，但天威诚信签发了有错误信息的证书，导致订户或者依赖方遭受损失的；
- 订户提供了虚假的注册信息或者资料，天威诚信仍然签发了证书，导致依赖方遭受损失的；
- 由于天威诚信的原因导致证书私钥被破译、窃取，致使订户或者依赖方遭受损失的；

订户有下列情形之一的，给天威诚信、依赖方造成损失的，应当承担赔偿责任：

- 提供的资料或者信息不真实、不完整或者不准确的；
- 证书中的信息有变更，未终止使用该证书并通知各方的；
- 订户没有使用可信系统保护私钥，或者没有采取必要的注意防止订户私钥的安全损害、丢失、泄漏、修改或非授权的使用；
- 知悉证书私钥已经丢失或者可能已经丢失时，未终止使用该证书并通知各方的；
- 订户使用的名字（包括但不限于通用名、域名和 e-mail 地址）破坏了第三方的知识产权的；
- 超过证书的有效期限使用证书的；
- 使用证书用于违法、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，

- 依赖方没有执行依赖方职责义务；
- 依赖方在不合理的环境下信赖一个证书；
- 而依赖方没有检查证书状态确定证书是否过期或吊销。

有下列情形之一的，天威诚信不承担赔付责任：

- 因订户原因致使依赖方遭受损失的；
- 依赖方未经检验证书的状态即决定信赖证书的；
- 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；
- 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**

除非天威诚信特别声明 CPS 提前终止，在天威诚信颁布新版本 CPS 之前，本 CPS 一直有效。

### **9.10.2 终止**

当天威诚信终止业务时，天威诚信 CPS 终止。在终止服务六十日前向信息产业主管部门报告，并作出妥善安排。

### **9.10.3 效力的终止与保留**

天威诚信 CPS 的终止（而非更新），意味着天威诚信认证业务的终止。天威诚信终止认证业务的过程将按国家有关主管部门的规定进行，并根据规定对受影响的客户进行安排，保证客户的利益不受影响或将受影响的程度减少到最小。

当由于某种原因，如内容修改、与适用法律相冲突，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。

## **9.12 修订**

### **9.12.1 修订程序**

本认证业务规则将尽量避免不必要的修改。但不定期地，天威诚信将对本 CPS 进行检查、评估，当天威诚信认为应该对本 CPS 做出修改时，天威诚信战略发展中心将对本 CPS 及其他相关文档、协议提出修改建议，获得天威诚信管理层批准后，由天威诚信战略发展中心负责组织有关文档、文件的修改。修改后的 CPS 及其他相关文档、协议经天威诚信策略管理委员会（PMA）及管理层批准后正式发布。

### **9.12.2 通知机制与期限**

天威诚信将修改了的 CPS 通过天威诚信信息库更新通告栏发布，其地址为：[https://www.itrus.com.cn/read.php?go=read\\_Knowledge\\_83](https://www.itrus.com.cn/read.php?go=read_Knowledge_83)。在认为有必要时，天威诚信将通过电子邮件、信件、媒体等方式通知有关各方。

修改后的 CPS 经批准后将立即在天威诚信信息库更新通告栏发布。对于需要通过电子邮件、信件、媒体等方式通知的修改，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面受到的影响最小。

### **9.12.3 必须修改业务规则的情形**

由天威诚信策略管理委员会（PMA）根据公司业务情况决定。

### **9.13 争议解决**

当天威诚信、订户和依赖方之间出现争议时，有关方面可依据协议通过协商解决，协商解决不了的，可通过法律解决。天威诚信订户协议、依赖方协议和其他订户协议已包括该项内容。

### **9.14 管辖法律**

中华人民共和国法律、规则、规章、法令和政令将管辖天威诚信的业务活动。天威诚信的任何业务活动受有关法律、法规的制约，任何业务和法律文件、合同的解释、执行不能同有关法律、法规相冲突。

### **9.15 与适用法律的符合性**

天威诚信的所有业务、活动、合同、协议符合中华人民共和国法律、法规，包括但不限于，公司法、合同法、消费者权益保护法等。

### **9.16 一般条款**

#### **9.16.1 完整协议**

CP、CPS、订户协议及依赖方协议及其补充协议将构成天威诚信 CTN 信任域参与者之间的完整协议。

#### **9.16.2 转让**

天威诚信、注册机构、订户及依赖方之间的责任、义务不能通过任何形式转让给其他方。

#### **9.16.3 分割性**

法律允许的范围内，在天威诚信订户协议、依赖方协议和其他订户协议内出现可以同其他条款分割的条款时，协议中的可分割条款的无效不应该影响协议中其他条款效力。

#### **9.16.4 强制执行**

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。

#### **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**

无规定。