天威诚信™

CTN 证书策略

2.1版本

生效日期**: 2006** 年 **5**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 1401（100088）

邮政编码：100088

电话：(8610)-82800896

网址：www.itrus.com.cn

天威诚信证书策略

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（100088）
电话：(8610)- 82800896，
传真：(8610)- 82800636。
电子邮件：practices@itrus.com.cn 。

致谢：

在天威诚信的证书策略（见：https://www.itrus.com.cn/repository/CP）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

1. 简介 1

1.1 概述 1

1.1.1 第 1 类证书 1

1.1.2 第 2 类证书 2

1.1.3 第 3 类证书 2

1.2 文档名称与标识 2

1.3 PKI参入者 3

1.3.1 认证机构（CA） 3

1.3.2 注册机构（RA） 3

1.3.3 证书种类和订户 3

1.3.4 信赖方 4

1.3.5 其他参入者 4

1.4 证书使用 4

1.4.1 合适的应用 4

1.4.1.1 1 类个人证书的应用 4

1.4.1.2 2 类证书的应用 5

1.4.1.3 3 类证书的应用 5

1.4.1.3.1 3 类组织机构代表人证书的应用 5

1.4.1.3.2 3 类组织机构身份证书的应用 5

1.4.1.3.3 3 类服务器证书的应用 5

1.4.2 受限的应用 5

1.4.3 受禁的使用 6

1.5 策略管理 6

1.5.1 策略文档管理机构 6

1.5.2 联系人 6

1.5.3 决定CPS符合策略的人员 6

1.5.4 CPS批准程序 6

1.6 定义与缩写 7

1.6.1 定义 7

1.6.2 缩写表 9

2. 发布与信息库责任 10

2.1 信息库 10

2.2 认证信息的发布 10

2.3 发布的时间或频率 10

2.4 信息库访问控制 10

3. 识别与鉴别 10

3.1 命名 10

3.1.1 命名类型 10

3.1.2 对命名有意义的要求 11

3.1.3 订户的匿名或伪名 11
3.1.4 解释不同命名的规则 11
3.1.5 命名的唯一性 11
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 组织机构身份的鉴别 11
3.2.3 个人身份的鉴别 12
3.2.3.1 1类证书的个人身份的鉴别 12
3.2.3.2 2类证书的个人身份的鉴别 12
3.2.3.3 3类组织机构代表人证书的个人身份的鉴别 12
3.2.4 没有验证的订户信息 12
3.2.5 授权、权限的确认 12
3.2.6 互操作准则 12
3.3 密钥再造请求的识别与鉴别 13
3.3.1 常规的密钥再造的识别与鉴别 13
3.3.2 吊销之后的密钥再造的识别与鉴别 13
3.4 吊销请求的识别与鉴别 13
4. 证书生命周期操作要求 13
4.1 证书申请 13
4.1.1 谁能提交证书请求 13
4.1.2 注册过程与责任 14
4.2 证书申请处理 14
4.2.1 执行识别与鉴别功能 14
4.2.2 证书申请批准和拒绝 14
4.2.3 处理证书申请的时间 14
4.3 证书签发 14
4.3.1 证书签发中RA和CA的行为 14
4.3.2 CA和RA通知订户证书的签发 14
4.4 证书接受 15
4.4.1 构成接受证书的行为 15
4.4.2 CA对证书的发布 15
4.4.3 CA通知其他实体证书的签发 15
4.5 密钥对和证书使用 15
4.5.1 订户私钥和证书使用 15
4.5.2 信赖方公钥和证书使用 15
4.6 证书更新 16
4.6.1 证书更新的情形 16
4.6.2 谁能要求更新 16
4.6.3 处理证书更新请求 16
4.6.4 通知订户新证书的签发 16

4.6.5 构成接受更新证书的行为 16
4.6.6 CA对更新证书的发布 17
4.6.7 CA通知其他实体证书的签发 17
4.7 证书密钥再造 17
4.7.1 证书密钥再造的情形 17
4.7.2 谁能要求新公钥的认证 17
4.7.3 处理证书密钥再造请求 17
4.7.4 通知订户新证书的签发 17
4.7.5 构成接受密钥再造证书的行为 17
4.7.6 CA对密钥再造证书的发布 17
4.7.7 CA通知其他实体证书的签发 17
4.8 证书修改 18
4.8.1 证书修改的情形 18
4.8.2 谁能要求证书修改 18
4.8.3 处理证书证书请求 18
4.8.4 通知订户修改证书的签发 18
4.8.5 构成接受修改的证书的行为 18
4.8.6 CA对修改的证书的发布 18
4.8.7 CA通知其他实体证书的签发 18
4.9 证书吊销和挂起 18
4.9.1 证书吊销的情形 18
4.9.2 谁能请求吊销 19
4.9.3 提出吊销请求的程序 19
4.9.4 吊销请求的宽限期 19
4.9.5 CA必须处理吊销请求的时间 19
4.9.6 信赖方检查证书吊销的要求 20
4.9.7 CRL发布频率 20
4.9.8 CRL发布的最大滞后时间 20
4.9.9 在线状态查询的可用性 20
4.9.10 在线状态查询要求 20
4.9.11 吊销信息发布的其他形式 20
4.9.12 密钥损害的特别要求 20
4.9.13 证书挂起的情形 20
4.9.14 谁能请求挂起 20
4.9.15 挂起请求的程序 21
4.9.16 挂起的期限限制 21
4.10 证书状态服务 21
4.10.1 操作特征 21
4.10.2 服务可用性 21
4.10.3 可选特征 21
4.11 订购的结束 21

4.12 密钥托管与恢复 21
4.12.1 密钥托管与恢复的策略与行为 21
4.12.2 会话密钥的封装与恢复的策略与行为 21
5. 设施、管理和操作控制 22
5.1 物理控制 22
5.1.1 场地位置与建筑 22
5.1.2 物理访问控制 22
5.1.3 电力与空调 22
5.1.4 漏水 23
5.1.5 火灾防护 23
5.1.6 介质存放 23
5.1.7 废物处理 23
5.1.8 异地备份 23
5.2 程序控制 23
5.2.1 可信角色 23
5.2.2 每项任务需要的人数 24
5.2.3 每个角色的识别与鉴别 24
5.2.4 需要职责分割的角色 24
5.3 人员控制 25
5.3.1 资格、经历和清白要求 25
5.3.2 背景调查程序 25
5.3.3 培训要求 26
5.3.4 再培训的频度和要求 26
5.3.5 工作岗位轮换的频度和次序 26
5.3.6 未授权行为的制裁 26
5.3.7 独立合约人的要求 26
5.3.8 提供给人员的文件 26
5.4 审计记录程序 27
5.4.1 记录事件的类型 27
5.4.2 处理日志的频度 28
5.4.3 审计日志保留的期限 28
5.4.4 审计日志的保护 28
5.4.5 审计日志备份程序 28
5.4.6 审计收集系统 28
5.4.7 对导致事件主体的通知 28
5.4.8 脆弱性评估 28
5.5 记录归档 28
5.5.1 归档记录的类型 28
5.5.2 归档记录的保留期限 29
5.5.3 归档文件的保护 29
5.5.4 归档文件的备份过程 29

5.5.5 记录时间戳要求 29
5.5.6 归档收集系统 29
5.5.7 获得和检验归档信息的程序 29
5.6 密钥变更 29
5.7 损害与灾难恢复 30
5.7.1 事故和损害处理程序 30
5.7.2 计算机资源、软件和/或数据的损坏 30
5.7.3 实体私钥损害处理程序 30
5.7.4 灾难后的业务存续能力 30
5.8 CA或RA的中止 31
6. 技术安全控制 31
6.1 密钥对的产生和安装 31
6.1.1 密钥对的产生 31
6.1.1.1 CA密钥对的产生 31
6.1.1.2 最终订户密钥对的产生 32
6.1.2 私钥传输给订户 32
6.1.3 公钥传输给证书签发机关 32
6.1.4 CA公钥传输给信赖方 32
6.1.5 密钥的长度 32
6.1.6 公钥参数的生成和质量检查 32
6.1.7 密钥使用目的 32
6.2 私钥保护和密码模块工程控制 33
6.2.1 密码模块的标准和控制 33
6.2.2 私钥多人控制（m选n） 33
6.2.3 私钥托管 33
6.2.4 私钥备份 34
6.2.5 私钥归档 34
6.2.6 私钥导入、导出密码模块 34
6.2.7 私钥在密码模块的存储 34
6.2.8 激活私钥的方法 34
6.2.8.1 最终订户私钥 34
6.2.8.1.1 1类证书 34
6.2.8.1.2 2类证书 35
6.2.8.1.3 3类证书 35
6.2.8.2 服务器证书 35
6.2.8.3 CA私钥 35
6.2.9 解除私钥激活状态的方法 35
6.2.10 销毁私钥的方法 36
6.2.11 密码模块的评估 36
6.3 密钥对管理的其他方面 36
6.3.1 公钥归档 36

6.3.2 证书操作期和密钥对使用期限 36
6.4 激活数据 37
6.4.1 激活数据的产生和安装 37
6.4.2 激活数据的保护 37
6.4.3 激活数据的其他方面 37
6.4.3.1 激活数据的传送 37
6.4.3.2 激活数据的销毁 37
6.5 计算机安全控制 38
6.5.1 特别的计算机安全技术要求 38
6.5.2 计算机安全评估 38
6.6 生命周期技术控制 38
6.6.1 系统开发控制 38
6.6.2 安全管理控制 38
6.6.3 生命期的安全控制 38
6.7 网络的安全控制 38
6.8 时间戳 38
7. 证书、CRL和OCSP轮廓 39
7.1 证书轮廓 39
7.1.1 版本号 39
7.1.2 证书的扩展项 39
7.1.2.1 密钥用法（Key Usage） 39
7.1.2.2 证书策略扩展项（Certificate Policies） 40
7.1.2.3 主题备用名（subjectAltName） 40
7.1.2.4 基本限制扩展项（BasicConstraints） 40
7.1.2.5 扩展的密钥用法（Extended Key Usage） 40
7.1.2.6 CRL的分发点（cRLDistributionPoints） 41
7.1.2.7 签发CA密钥标识符 41
7.1.2.8 主题密钥标识符 41
7.1.3 密钥算法对象标识符 41
7.1.4 命名形式 41
7.1.5 命名限制 42
7.1.6 证书策略对象标识符 42
7.1.7 策略限制扩展项的用法 42
7.1.8 策略限定符的语法和语义 42
7.1.9 关键证书策略扩展项的处理语义 42
7.2 CRL 轮廓 42
7.2.1 版本号 42
7.2.2 CRL 和CRL条目扩展项 43
7.3 OCSP轮廓 43
7.3.1 版本号 43
7.3.2 OCSP扩展项 43

8. 一致性审计和其他评估 43
8.1 评估的频度和情形 43
8.2 评估者的身份/资格 43
8.3 评估者与被评估者之间的关系 43
8.4 评估的内容 43
8.5 对问题与不足采取的行动 43
8.6 评估结果的传达与发布 44
8.7 其他评估 44
9. 其他业务和法律事务 44
9.1 费用 44
9.1.1 证书签发和更新费用 44
9.1.2 证书查取的费用 44
9.1.3 证书吊销或状态信息的访问费用 44
9.1.4 其他服务费用 44
9.1.5 退款政策 44
9.2 财务责任 45
9.2.1 保险覆盖 45
9.2.2 其他财产 45
9.2.3 保险或担保对最终实体的覆盖 45
9.3 商业信息保密 45
9.3.1 保密信息范围 45
9.3.2 不属于保密的信息 46
9.3.3 保护保密信息的责任 46
9.4 个人隐私保密 46
9.4.1 隐私保密计划 46
9.4.2 作为隐私处理的信息 46
9.4.3 不被认为隐私的信息 46
9.4.4 保护隐私的责任 46
9.4.5 使用隐私信息的告知与同意 46
9.4.6 依法律或行政程序的信息披露 46
9.4.7 其他信息披露情形 47
9.5 知识产权 47
9.5.1 证书和吊销信息中的知识产权 47
9.5.2 CP中的知识产权 47
9.5.3 命名中的知识产权 47
9.5.4 密钥和密钥材料的知识产权 47
9.6 表述与担保 47
9.6.1 CA 的表述与担保 47
9.6.2 RA 的表述与担保 48
9.6.3 订户的表述与担保 48

9.6.4 信赖方的表述与担保 48
9.6.5 其他参入者的表述与担保 48
9.7 担保免责 48
9.8 有限责任 49
9.9 赔偿 49
9.10 期限与终止 49
9.10.1 期限 49
9.10.2 终止 50
9.10.3 终止的效果与存续 50
9.11 对参入者个别通告及信息交互 50
9.12 修改 50
9.12.1 修改程序 50
9.12.2 通知机制与期限 50
9.12.3 OID必须修改的情形 51
9.13 争议解决条款 51
9.14 管辖法律 51
9.15 符合适用法律 51
9.16 一般条款 51
9.16.1 完整协议 51
9.16.2 让渡 51
9.16.3 分割性 51
9.16.4 强制执行 52
9.16.5 不可抗拒力 52
9.17 其他条款 52

1. 简介

本文件是中国可信网络（CTN）证书策略（CP）。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的需求的公众用户。

证书策略是管辖 CTN 的主要策略说明。在 CTN 中，它为批准、签发、管理、使用、吊销和更新证书和相关的可信服务制定商务、法律和技术上的规范。这些规范是 CTN 标准，它应用于所有 CTN 的参与者，保护 CTN 的安全性和完整性，因此，在 CTN 中，它提供了一致性。遵循本 CP 的认证机构应根据本 CP 制定认证业务声明（Certification Practices Statement），及其他的管理规范和辅助协议。

天威诚信策略管理中心（Policy Management Authority，PMA）负责 CP 的修改、更新、及评述整理工作。PMA 还负责检查 CP 要求的遵守情况。

本 CP 的结构符合“互联网 X.509 公开密钥基础设施证书策略和证书业务框架”（*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*），即由互联网标准组织“互联网工程工作组”（Internet Engineering Task Force）制定的 RFC3647 标准。RFC3647 框架已经成为 PKI 行业中的一个标准。本 CP 服从 RFC3647 标准，这样使得使用或考虑使用天威诚信服务的用户很容易实现证书策略的映射、比较、评估和互操作。

天威诚信尽可能地使 CP 符合 RFC3647 标准，但它保留在需要的时候采用不同于 RFC3647 结构的权利，如，为了提高 CP 的质量或其对天威诚信信任域参与者的适用性。而且天威诚信 CP 的结构不一定会与 RFC3647 以后的版本保持一致。

1.1 概述

本证书策略为整个 CTN 制定了要求，它管辖 VTN 内的所有个人和实体（称为 VTN 参与者）。在 CTN 中，天威诚信和它的每个合作伙伴都在其信任域内具有权威性。天威诚信信任域包括下级实体，如客户、订户和信赖方。而且，证书策略扮演着保护伞的角色，它为整个 CTN 制定了一整套 CTN 标准。

在很多情况下，在很多情况下，对于直接在 CP 中包括某些业务的特别说明有可能损害天威诚信子信任域的安全情形，本证书策略将引用这些辅助文件。

本证书策略假设读者是熟悉数字证书和PKI的。如果不熟悉，天威诚信建议读者接受一些CTN中用到的公开密码技术和公钥基础设施方面的培训。一般性的知识和培训可以在天威诚信的网站上获得，其地址：**http://www.itrus.com.cn**。

CTN 包含 1-3 三类证书，对应不同的安全保障级别，信任级别。天威诚信证书策略描述了这三类证书如何符合三类应用的一般安全要求。除非特别说明，本证书策略的内容、要求、规定适应于所有三类证书。

1.1.1 第 1 类证书

在天威诚信 CTN 信任域中，1 类证书提供最低级的安全保证，它们是个人安全电子邮件证书。第 1 类证书申请的验证过程是基于在天威诚信信任域中订户甄别名的唯一性和

确定性，一个电子邮件地址与一个公钥相关联。它们主要用于电子邮件的数字签名、加密、非商业性的访问控制或无需提供身份证明的低额交易。

1.1.2 第 2 类证书

第 2 类是个人证书。同其他两类证书相比，2 类证书提供了中间级别的安全保证。第 2 类证书申请的验证过程除了 1 类证书的验证过程外，还必须将证书申请者提交的信息与商业记录或数据库中的信息、或天威诚信批准的第三方身份验证服务数据库中的信息进行比较。它们主要用于提供个人的身份证明，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。2 类个人证书可包括签名证书和加密证书。

1.1.3 第 3 类证书

第 3 类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（SSL 证书）。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。3 类证书提供的订户身份保证是基于必须确认：订户组织机构确实存在，该组织机构授权证书申请，并且代表订户提交证书申请的人获得授权这么做。

组织机构身份证书可用于信息活动中的组织机构的身份证明，用于签订合同、完成交易等。组织机构代表人证书是签发给组织机构授权的代表人，除提供组织机构身份证书的的保证外，还保证证书持有人获得组织机构授权。证书用途与组织机构身份证书类似。服务器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，用户访问的 Web 服务器就是他要访问的服务器，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。

1.2 文档名称与标识

本文档称为中国可信网络证书策略，是一个覆盖了三类数字证书的证书策略。在本 CP 中为每类证书的证书策略项分配了一个对象标示符。用于三类证书的对象标示符值为：

- 1 类证书策略: itrus/pki/policies/ctn-cp/class1 (1.2.156.112535.1.1.1.1).
- 2 类证书策略: itrus /pki/policies/ctn-cp/class2 (1.2.156.112535.1.1.1.2).
- 3 类证书策略: itrus /pki/policies/ctn-cp/class3 (1.2.156.112535.1.1.1.3).

这些对象标示符与相应的本 CP 中的版本号相对应。CA 证书包含的对象标示符可能会略掉 CP 版本号，表明它们不受限于本 CP 的版本。

1.3 PKI 参入者

1.3.1 认证机构（CA）

认证机构（Certification Authority，简称 CA）作为可信第三方，对个人、实体及设备进行主题信息及其它属性与公钥绑定的确认。CA 是向最终用户或其下 CA 签发证书的实体的术语。它的一个特例是根 CA。一个根 CA 是一类证书体系的最高层。在 CTN 系统中有三类证书，对应于三类证书有三个根 CA。

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者。在用户获得证书前，它必须以申请者的身份来注册证书。证书申请者必须从 CA 或 RA 建立的注册过程来完成注册，并将注册信息提交给 CA 或 RA。CA 或 RA 将对申请者的身份及其它属性进行确认，然后决定是签发还是拒绝该请求。如果签发证书，则证书将被发送给申请者。RA 还可以根据用户需要吊销证书，尽管是 CA 的系统完成最终的吊销工作，并将证书加入到证书吊销列表(“CRL”)中去，或是在 CA 信息库中显示证书已吊销。

1.3.3 证书种类和订户

如 CP § 1.1.1-1.1.3 所描述的那样， CTN 中有三类证书。个人或组织因其应用需要而申请证书。1 类证书是仅签发给个人最终订户的个人证书。3 类证书有些可以签发给个人，有些可以签发给组织机构，还有些可以签发给组织机构的服务器。2 类个人证书只可以签发给一个组织机构的相关个人，相关个人是指与组织机构相关的自然人，如主管、经理、职员、合伙者、合同契约者、实习者或有共同利益的成员。因此，2 类证书所对应的组织机构将作为注册机构。CTN 信任域中每类和每种证书的订户类型如下所示。

表 1 – 证书与订户的类型

证书种类	签发对象	订户类型
1 类	个人	任何个人，包括一般公众成员。
2 类	个人	就其与注册机构的关系而言是关联人员，如雇员、合作伙伴等。
3 类	组织机构	进行电子商务、电子政务的组织机构
	服务器	拥有服务器的组织机构。
	个人	组织机构授权的代表人员。

就技术而言，CA 本身也是证书的订户，或者作为一个根 CA 给自己签发一个自签名证书，或者作为被上级 CA 签发了一个证书的 CA。可是，在 CP 中提到的“订户”是指最终订户。

1.3.4 信赖方

信赖方指为某一应用而使用、信任其他方证书的个人或组织。例如，接收到发送者发送的签名邮件，接收者作为信赖方可以用发送方数字证书的公钥对签名进行验证。另外，发送者作为信赖方可以使用接收者的证书发送加密邮件，只有接收者的私钥可以解开此加密邮件。

1.3.5 其他参入者

在证书申请审批过程中，提供个人与组织身份确认服务的权威第三方，可以提供订户身份确认。

1.4 证书使用

1.4.1 合适的应用

本 CP 描述了在 CTN 信任域中规范使用 1~3 类证书的行为，每一类证书通常适用的应用。通过合同或在特殊环境下（例如内部公司环境），允许 CTN 参与者将证书用于比本 CP 描述的应用安全高的应用。但是任何这种用法，必须仅限于这些实体，并且这些实体须为这种用法带来的任何伤害和赔偿承担唯一的责任。

个人证书和组织机构身份证书允许信赖方验证数字签名。CTN 信任域的参与者必须确认和同意在法律允许的范围内，当一个交易需要书写时，如果一个消息或记录有数字签名，而这个数字签名可用一 CTN 证书来验证，那么该消息或记录是合法的、有效的，而且其效力不得低于书面签名的同样消息或记录。受限于适用法律，一个相对于 CTN 证书的数字签名或交易，无论证书签发、数字签名产生或使用的地理位置在哪，无论 CA 开展业务或订户地理位置在哪，都是有效的。

1.4.1.1 1 类个人证书的应用

1 类个人证书又称为安全电子邮件证书，用于电子邮件的签名、加密。与其他类应用相比，该类证书适用的应用所要求的担保级别低。它们不提供用户身份的担保。因此，使用 1 类证书所对应的私钥进行的数字签名不提供身份鉴别目的或抗抵赖的证据。电子邮件的数字签名提供了切实的方法保证邮件是证书持有人发出。但是证书无法提供证据，证明发送者所使用的电邮地址的真实性，这需要签发机构在签发证书前确认证书订户拥有证书上所列邮箱。加密应用使信赖方使用接受者的证书来加密消息，尽管信赖方不能确认接收者确实是证书所对应的人员。

1 类证书还可以用于在线会话中的客户端鉴别。网站或其它设备可以使用证书来确认一系列会话的发起者为拥有某一电邮地址的订户，但证书无法提供订户的真实身份的证据。

1.4.1.2 2 类证书的应用

2 类证书适用于电子邮件的安全，比如，个人间的、公司内部或外部的电子邮件，基于 Web 的访问控制、中等额度的交易等。与其他类应用相比，该类应用所要求的保证级别中等。通过数字签名的使用提供了电子邮件的身份鉴别、消息完整性、抗抵赖的安全保障。2 类证书还适用于客户端的鉴别，可以向网站或设备提供中等担保级别的保证。客户端鉴别可以提供诸如数据库或网站的访问控制。

1.4.1.3 3 类证书的应用

1.4.1.3.1 3 类组织机构代表人证书的应用

3 类组织机构代表人证书适用于各类应用，包括但不限于代表组织机构签订文件、合同、协议、网上交易等，提供高等担保级别的保证。3 类组织机构代表人证书还适用于客户端的鉴别，可以提供诸如数据库或网站的访问控制，以及提供电子邮件的签名加密。

1.4.1.3.2 3 类组织机构身份证书的应用

与类组织机构代表人证书类似，3 类组织机构身份证书适用于各类应用，如用于组织机构签订文件、合同、协议、网上交易等，提供高等担保级别的保证。3 类组织机构身份证书还适用于客户端的鉴别，可以提供诸如数据库或网站的访问控制。

1.4.1.3.3 3 类服务器证书的应用

服务器证书使浏览器可以鉴别网站服务器的身份，并创建 SSL 加密通道以使双方进行加密会话。服务器证书是一种加强了的服务器证书，提供 128 位 SSL 会话加密强度。

1.4.2 受限的应用

一般而言，CTN 证书是一般性目的的证书。CTN 证书可以在全球范围内使用，并且可以和不同的信赖方之间相互操作。CTN 证书的使用通常不只限于特定的商业环境，如导航、金融服务系统、行业市场环境或虚拟商场。尽管如此，证书的受限使用是允许的，在他们自己环境中使用证书的客户可以对证书在这些环境中的使用增加更加严格的限制。但是认证机构不对注意和实施这些环境中的这种限制负责。

尽管如此，某些 CTN 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在 CTN 中的使用目的（见 CP § 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（见 CP § 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 类证书不能用于身份证明，不能用于具有身份证明的抗抵赖。

1.5 策略管理

1.5.1 策略文档管理机构

管理本CP 的机构是天威诚信法律部，其联系地址如下：

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（100088）

部门：市场商务管理中心

电话：(8610)- 82800896

传真：(8610)- 82800636

邮箱地址：practices@itrus.com.cn

1.5.2 联系人

如果需要CP请发邮件到信箱：practices@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（100088）

部门：市场商务管理中心

电话：(8610)- 82800896

传真：(8610)- 82800636

1.5.3 决定CPS 符合策略的人员

天威诚信法律部。

1.5.4 CPS 批准程序

天威诚信有专门的策略管理机构，负责CP 和CPS 的管理。认证机构的CPS 将会被提交到天策略管理机构，策略管理机构将负责评估CPS 是否符合本证书策略，如果符合，将批准 CPS。

1.6 定义与缩写

1.6.1 定义

表 2 定义

术语	*定义*
关联个人	与给定实体有一定合作关系的自然人。他可以是（1）政府的一名官员、该组织机构的主管、雇员、合伙人、合约人、实习人员或者其他人员；（3）也可以是和某实体保持一定关系的人员，该实体提供这个人身份担保的商业或其他记录。
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。
证书申请人	要求一个发证机关签发证书的个人或者组织机构。
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
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，该列表最终证书为根证书。
证书策略	是指本证书策略文档，是一个有关 CTN 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。
证书签名请求	包含希望签发的证书请求的信息。
认证机构 (CA)	一个授权签发、管理、吊销和更新证书的实体。
认证业务声明(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。
类	CP 中定义的担保的级别。见 CP § 1.1。
一致性审计	一个处理中心、服务中心或安征通客户要定期经历的审计，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 CP § 9.3，9.4 要求需保密的信息。

术语	*定义*
服务器证书	3 类证书，用于支持浏览器和服务器之间的 SSL 会话。
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。
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。
在线证书状态协议 (OCSP)	为信赖方提供实时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的体系的组织机构、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。
信赖方	信赖一个证书和/或一个数字签名的个人或组织机构。.
信赖方协议	一个 CA 使用的协议，这个协议规定了一个组织机构或个人成为信赖方的条款和条件。
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 私钥需要的数据的分割成多个部分，使用多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。
主题	与公钥对应的私钥的持有者。在组织机构证书中，主题指的是

术语	*定义*
	持有私钥的设备或装置。一个主题只有唯一的、确切的命名。它和该主题证书中的公钥绑定在一起。
订户	在个人证书的情况下，订户是指人，它是签发的证书的主题；在组织机构证书的情况下，订户是指组织机构，它是所签发证书的主题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，及管理产品、服务、设施和业务的可信性。
安全可信系统	是指这样的计算机硬件、软件与程序，它能相当有效地避免入侵与滥用，提供合理程度的可用性、可靠性与正确操作保障，能恰当地完成预定功能，并实施适当的安全策略。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”。
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。
中国信任网络 (CTN)	天威诚信建立、基于 PKI 的安全信息体系。

1.6.2 缩写表

表 3-缩写

缩写	*全称*
B2B	企业对企业(的电子商务)
CA	认证机构
CP	证书策略.
CPS	认证业务声明.
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
OID	对象标识符
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
RFC	请求评注标准(一种互联网建议标准)
SSL	加密套接层协议。.

2. 发布与信息库责任

2.1 信息库

认证机构应有信息库用于各类信息的发布，如证书策略、认证业务声明、协议、证书、证书吊销列表。认证机构应在其认证业务声明、信赖方协议等中指明有关信息发布、获取的位置。

2.2 认证信息的发布

认证机构需发布的认证信息包括，证书策略、认证业务声明、订户协议、信赖方协议、证书及证书状态。

2.3 发布的时间或频率

证书策略、认证业务声明、订户协议、信赖方协议，通过信息库 7X24 可获得，另外在订户进行证书申请注册时，阅读并同意订户协议是成功注册的一个条件。订户证书一经签发即发布到证书信息库，而证书状态发布的时间和频率见 CP § 4.9.7。

2.4 信息库访问控制

发布在认证机构信息库中的信息是对外公开的，任何人都能够查阅，对这些信息的只读访问应该是不受任何限制的，这里的一个例外是 OCSP，允许 OCSP 作为一种付费服务。

认证机构也应该实现了物理和逻辑上的安全以阻止未经授权的增加、删除或修改信息库的内容。

3. 识别与鉴别

3.1 命名

3.1.1 命名类型

根据实体的类型不同，实体名字可以是姓名、组织机构名、部门名、域名、商标名、IP 地址等，命名必须是符合 X500 规定。

3.1.2 对命名有意义的要求

2 类和 3 类最终订户证书包含的命名应具有通常理解的语义，用它可以确定证书主题中的个人、机构或设备的身份。对于这类证书，使用假名（命名不是订户真实的姓名或组织机构名）是不允许的。但 1 类最终订户证书中可以使用假名。

3.1.3 订户的匿名或伪名

除了 1 类证书外，订户不能使用匿名或伪名申请证书，证书中也不能使用匿名或伪名。

3.1.4 解释不同命名的规则

依 X501 命名规则解释。

3.1.5 命名的唯一性

认证机构应保证签发给某个实体的证书，其主题甄别名，在 CA 信任域内是唯一的。

3.1.6 商标的识别、鉴证和角色

在订户的证书中允许包含商标信息。在证书签发前，认证机构必须对商标信息进行鉴证。对商标的鉴别主要基于：(1) 众所周知的商标；或(2) 提交的商标注册文件。商标不能用于组织机构名的命名，但可用于部门和通用名的命名，也可以放在证书中其他合适的地方已实现特定的目的。但是，商标在证书中使用所实现的功能不能超过本证书策略的约定。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

订户必须使用经数字签名的 PKCS#10 格式的证书请求，或其它相当的密码格式，申请证书，认证机构依此验证证书申请者拥有私钥。

3.2.2 组织机构身份的鉴别

在把证书签发给一个组织机构、组织机构拥有的设备或组织机构的代表人时，认证机构须对订户所在组织机构进行身份鉴证。对组织机构身份鉴证应该包括如下两个内容：

- 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，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，代表组织机构提交证书申请的人是经过授权的。确认的方式可以是通过可靠的第三方，如电话黄页、话费单，获得组织机构的电话，通过电话确认有关申请及授权。

3.2.3 个人身份的鉴别

除了 1 类证书申请，对于所有类型的个人证书，在批准证书前应确认：

- 证书申请者是证书申请中所说的那个人。
- 除了未经验证的订户信息，包含在证书中的信息是准确的。
- 按 CP § 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。

针对每类证书，具体的个人身份的鉴证过程如下。

3.2.3.1 1 类证书的个人身份的鉴别

对于 1 类个人证书，需确认主题甄别名在 CA 域内是一个唯一的、明确的主题名，但订户的通用名是未经验证的订户信息，确认订户拥有证书申请中的 E-mail 地址。确认订户拥有证书申请中的 E-mail 地址可以采用将证书获取的有关信息发送到有关邮箱实现，或通过其他可靠的方式。

3.2.3.2 2 类证书的个人身份的鉴别

2 类证书的个人身份的鉴证，除了完成 1 类证书所需的鉴证外，还必须通过可靠的方式确保证书申请人所在的组织、部门与证书中所列的组织、部门一致，证书中通用名就是用户的真实姓名。

3.2.3.3 3 类组织机构代表人证书的个人身份的鉴别

对 3 类组织机构代表人证书的个人身份的鉴证，包括按 CP §3.2.1 确认组织机构身份和申请人提供的其他注册信息，同时确认证书订户属于该组织机构，证书订户确实被雇佣并被授权作为组织机构代表人。

3.2.4 没有验证的订户信息

1 类证书中通用名可以是未经验证的信息。

3.2.5 授权、权限的确认

确认三类证书申请时，必须通过可靠的途径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

无规定。

3.3 密钥再造请求的识别与鉴别

在进行 CP § 4.7 所述的证书密钥再造签发新证书前，需对再造的密钥进行鉴别以确保密钥再造请求来自原证书密钥拥有者。

3.3.1 常规的密钥再造的识别与鉴别

对于一般正常情况下的密钥再造申请，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，使用再造前的私钥对包含新公钥的申请信息签名。对申请的鉴别须基于以下几个方面：

- 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。

3.3.2 吊销之后的密钥再造的识别与鉴别

证书吊销后不能进行密钥再造。

3.4 吊销请求的识别与鉴别

证书吊销请求可以来自订户，也可以来自认证机构、注册机构。证书吊销的方式可以是订户自己吊销，也可以订户要求认证机构、注册机构吊销。批准证书申请的实体，即认证机构、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 谁能提交证书请求

证书申请可由证书拥有实体或相应的授权人提交。

4.1.2 注册过程与责任

认证机构必须设定安全可靠的证书申请方式和程序，注册过程必须做到：

- 提供必需的信息。
- 保证订户信息不被篡改、私密信息不被泄漏。
- 注册过程必须保证所有订户必须明确同意相关的订户协议，才能完成注册过程。
- 按 CP § 3.2.1 规定的产生一个密钥对，并将公钥传给认证机构、注册机构。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

当认证机构、注册机构接受到订户的证书申请后，应按§ 3.2 的要求，对订户进行身份识别与鉴别。

4.2.2 证书申请批准和拒绝

认证机构、注册机构应在鉴证的基础上，批准或拒绝申请。如果拒绝申请，则应该通过适当的方式、在合理的时间内通知证书申请者。

4.2.3 处理证书申请的时间

认证机构的认证业务声明和其他业务规范应规定合理的证书请求处理时间。

4.3 证书签发

4.3.1 证书签发中 RA 和 CA 的行为

在证书的签发过程中 RA 的管理员负责证书申请的审批，并通过操作 RA 系统将签发证书的请求发往 CA 的证书签发系统。RA 发往 CA 的证书签发请求信息须有 RA 的身份鉴别与信息保密措施，并确保请求发到正确的 CA 证书签发系统。

认证机构的证书签发系统在获得 RA 的证书签发请求后，对来自 RA 的信息进行鉴别与解密，对于有效的证书签发请求，证书签发系统签发证书。

4.3.2 CA 和 RA 通知订户证书的签发

无论是拒绝还是批准订户的证书申请，RA 须通过适当的方式通知订户。如果证书申请获得批准并签发，RA 应通过适当的方式告诉订户如何获取证书。

认证机构的证书签发系统签发证书后，将证书签发的信息通过适当的方式通知证书订户或 RA。

4.4 证书接受

4.4.1 构成接受证书的行为

订户接受证书的方式可以有如下几种：

- 通过面对面的提交，订户接受载有证书和私钥的介质。
- 按 CA 或 RA 的指示，通过网络将证书下载到本地存放介质，如本地计算机、USB Key、智能卡。

完成以上行为表明订户接受证书。另外，在订户接受到证书后，应立即对证书进行检查和测试。

4.4.2 CA 对证书的发布

对于订户证书，CA 根据用户的意愿将证书发布到目录系统上，或者不进行发布。

4.4.3 CA 通知其他实体证书的签发

除证书订户和 RA 外，CA 不需要通知其他实体证书的签发。

4.5 密钥对和证书使用

订户密钥对和证书须用于其规定的、批准的用途。签名密钥对用于签名与签名验证，加密密钥对用户加密解密。如果密钥对允许用于身份鉴别，则可以用于身份鉴别。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信赖方。证书持有人对信息签名时，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）应提交给鉴别方。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 CP § 6.1, 6.2, 6.4 妥善保管其证书私钥。

4.5.2 信赖方公钥和证书使用

当信赖方接受到签名的信息后，应该，

1. 获得对应的证书及信任链；
2. 确认该签名对应的证书是信赖方信任的证书；
3. 证书的用途适用于相应的签名。
4. 使用证书上的公钥验证签名。

以上任何一个环节失败，信赖方应该拒绝接受签名信息。

当信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。信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

每个证书都有其有效期，在一个订户的证书到期前 30 天内或已到期后 30 天内，如果订户的注册信息没有改变，订户可以申请证书更新，证书更新将不改变证书公钥。证书更新与重新申请一个同样主题甄别名的新证书区别在于：

- 证书更新用户无需再提交注册信息，重新申请证书需要用户提交注册信息。
- 对于证书更新，不更新密钥对，而对于重新申请证书，必须使用新的密钥对。

在进行证书更新时，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，使用原证书的私钥对包含公钥的更新申请信息签名。

证书吊销后将不能更新。

4.6.2 谁能要求更新

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（服务器证书）可以要求更新证书。

4.6.3 处理证书更新请求

处理证书更新请求的过程，包括申请验证、鉴别、签发证书。对申请的验证和鉴别须基于以下几个方面：

- 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。

在以上验证和鉴别通过后才可签发证书。

4.6.4 通知订户新证书的签发

同 CP § 4.3.2。

4.6.5 构成接受更新证书的行为

同 CP § 4.4.1。

4.6.6 CA 对更新证书的发布

同 CP § 4.4.2。

4.6.7 CA 通知其他实体证书的签发

同 CP § 4.4.3。

4.7 证书密钥再造

证书密钥再造即产生新的密钥对，使用与原证书一样的主题甄别名签发新证书。

4.7.1 证书密钥再造的情形

每个证书都有其有效期，在一个订户的证书到期前 30 天内或已到期后 30 天内，如果订户的注册信息没有改变，订户可以申请证书密钥再生，证书密钥再造将使用新的公钥。

证书吊销后不允许证书密钥再造。

4.7.2 谁能要求新公钥的认证

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（服务器证书）可以要求对新公钥的认证。

4.7.3 处理证书密钥再造请求

见 CP § 3.3.1。

4.7.4 通知订户新证书的签发

同 CP § 4.3.2

4.7.5 构成接受密钥再造证书的行为

同 CP § 4.4.1。

4.7.6 CA 对密钥再造证书的发布

同 CP § 4.4.2。

4.7.7 CA 通知其他实体证书的签发

同 CP § 4.4.3。

4.8 证书修改

4.8.1 证书修改的情形

无规定。

4.8.2 谁能要求证书修改

无规定。

4.8.3 处理证书证书请求

无规定。

4.8.4 通知订户修改证书的签发

无规定。

4.8.5 构成接受修改的证书的行为

无规定。

4.8.6 CA 对修改的证书的发布

无规定。

4.8.7 CA 通知其他实体证书的签发

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：

- 认证机构、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。
- 认证机构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。
- 和订户达成的订户协议已经终止。
- 认证机构或注册机构有理由相信证书签发时没有依据 CP 规定的有关程序，证书签发给了非证书主题的人员（1 类证书除外）或没有鉴证该人员在证书主题中的命名就签发了证书（1 类证书除外）。
- 认证机构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。

- 认证机构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 谁能请求吊销

以下实体可以请求吊销一个最终订户证书：

- 批准订户证书申请的认证机构或注册机构可以依 CP § 4.9.1 要求吊销一个最终订户证书。
- 对于个人证书，证书订户可以请求吊销他们自己的个人证书。
- 对于组织机构身份证书，只有组织机构授权的代表有资格请求吊销已经签发给组织机构的证书。
- 对于服务器证书，只有拥有服务器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 提出吊销请求的程序

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：

- 直接通过认证机构、注册机构提供的证书服务网页，并提供证书申请时提供的挑战语作为身份鉴别的信息。
- 通过电子邮件、传真、特快专递等可靠的方式告知认证机构、注册机构。

认证机构、注册机构在接到最终订户的吊销请求后，需通过可靠的方式确认请求确实来自最终订户。

认证机构、注册机构在确信出现 CP § 4.9.1 中的情况而需要立即吊销证书时，可以立即吊销证书。

4.9.4 吊销请求的宽限期

当最终订户发现出现 CP § 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认证机构、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 必须处理吊销请求的时间

认证机构、注册机构从接到吊销请求到完成处理请求需要一定的时间，但从接到请求到完成吊销的时间，如果认证机构在业务时间内接到请求，

- 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 信赖方检查证书吊销的要求

对于安全保障要求比较高并且完全依赖证书进行身份鉴别与授权的应用，信赖方在信赖一个证书前必须查询证书吊销列表确认该证书的状态。

4.9.7 CRL 发布频率

认证机构须定时发布最新的证书吊销列表。证书吊销列表更新的时间间隔不能超过 24 小时。

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 上的滞后时间不能超过 24 小时。

4.9.9 在线状态查询的可用性

认证机构须提供供证书状态的在线查询服务（OCSP），以供安全保障要求高的应用使用。

4.9.10 在线状态查询要求

对于安全保障要求高并且完全依赖证书进行身份鉴别与授权的应用，信赖方在信赖一个证书前必须通过证书状态在线查询检查该证书的状态。

4.9.11 吊销信息发布的其他形式

除了 CRL、OCSP 外，认证机构可以提供其他形式的吊销信息发布，但这不是必须的。

4.9.12 密钥损害的特别要求

无论是最终订户还是认证机构、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 谁能请求挂起

无规定。

4.9.15 挂起请求的程序

无规定。

4.9.16 挂起的期限限制

无规定。

4.10 证书状态服务

认证机构应该通过 CRL、OCSP 提供证书状态服务。

4.10.1 操作特征

认证机构提供的证书状态查询必须以网络服务的形式，让信赖方能够随时查询、下载。CRL 的发布频率和延迟必须符合 CP § 4.9.7、4.9.8。OCSP 应能立即反映证书的当前状态。证书状态服务的提供应该使标准、通用的方式。对服务请求应该有合理的响应时间和并发处理能力。

4.10.2 服务可用性

CRL、OCSP 证书状态服务须保证 7X24 可用，应该有很高的可靠性和可用性。

4.10.3 可选特征

无规定。

4.11 订购的结束

当证书到期或证书被吊销则认证机构与订户关系结束。

4.12 密钥托管与恢复

无规定。

4.12.1 密钥托管与恢复的策略与行为

无规定。

4.12.2 会话密钥的封装与恢复的策略与行为

无规定。

5. 设施、管理和操作控制

5.1 物理控制

CTN 有详细的文件，描述 CA 和 RA 需遵守的物理控制和安全策略。对这些策略的符合性要求，在第 8 章中的 CTN 独立审计要求中规定。这些文件包含敏感信息，需要与天威诚信签署保密协议后才浏览。下面只简单描述一下相关要求。

5.1.1 场地位置与建筑

CTN 中的所有 CA 和 RA 都将在物理上受保护的环境中运营，该环境能够防止、检测并阻止非授权的访问、使用或披露敏感信息和系统。对于天威诚信和与其相关的执行 CA 和 RA 相应功能的机构，其环境需要满足《天威诚信安全和审计要求指南》。

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。

证书的认证等级决定了 CA 或 RA 的物理安全最小安全级别，例如：CTN 签发了 1、2、3 类证书，因此他们运营在很高安全级别的 CTN 系统环境下，CA 或 RA 机构的证书管理签发程序被要求在相应的证书安全策略指导下，CA 或 RA 机构需要在他们的 CPS 中详细描述物理和环境的一些细节。

5.1.2 物理访问控制

进出每一个物理安全层的行为都需要被记录、审计和控制，这样才可以保证进出每一个物理安全层的人都是经过授权的。

5.1.3 电力与空调

认证机构和注册机构须有安全、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。认证机构应该有加热/通风/空调系统控制温度和湿度。

5.1.4 漏水

认证机构和注册机构应采取预防措施以最大程度地减小水灾或其他水泄漏对认证系统的影响和破坏。

5.1.5 火灾防护

认证机构和注册机构应采取预防措施,并制定相应的程序来消除和防止火灾的发生，这些防护方法应符合当地管理部门或机构的安全要求。

5.1.6 介质存放

储存产品软件和数据、归档、审计或备份信息的介质要保存在安全设施中，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

认证机构和注册机构应执行废物处理程序（如纸、电子介质或其他敏感信息）来控制未经授权的使用和访问，防止通过废物泄漏重要的公司商业信息和客户隐私信息。

5.1.8 异地备份

认证机构和注册机构应对关键系统数据、审计日志数据和其他敏感信息要进行日常备份和维护，这些备份信息要保存在安全的地方。

5.2 程序控制

5.2.1 可信角色

出于可靠性人员管理的需求，雇员、合约人、顾问等需要被认定为可信人员才可在可信岗位进行工作，可信人员的条件在本节中进行描述。

可信人员包括所有可以接触或控制鉴证或密钥操作的人员，他们可能对以下几个方面具有重要影响：

- 证书应用中的信息确认
- 对证书申请、吊销请求、更新请求或注册信息的接收、鉴证、批准、拒绝或其他操作；
- 证书的签发或吊销，包括能够访问受限资料档案的人员以及处理证书用户相关信息或请求的人员。

可信人员包括、但不限于：

- 接触客户信息并进行证书生命周期管理的客户服务人员；
- 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 密钥口令分割的人员；

5.2.2 每项任务需要的人数

认证机构和注册机构应建立、维护相应的策略和严格的控制程序，以保障敏感的操作进行了职责分工，确保多名可信人员共同参与完成一些敏感的任务：

职责分割的策略和控制程序是基于实际工作职责的要求。对于认证业务来讲，最敏感的任务是访问和管理 CA 密码设备（如根密钥和加密卡）和涉及密码的相关材料，这些工作要求多名可信人员参与。

一些敏感的内部控制流程要求至少有两名可信人员参与，要求他们有各自独立的物理或逻辑控制设施，关于 CA 的密钥设备的生命周期过程被严格的要求多名可信人员共同参加。关键的控制要进行物理和逻辑上的分割，如掌握关键设备的物理权限的人员不能再持有逻辑权限分割权力，反之易然。

其他的一些主要操作，如 3 类证书的鉴证和签发不能自动签发，要求至少 2 个可信人员的参与。

5.2.3 每个角色的识别与鉴别

认证机构和注册机构必须通过适当的方式，对有关人员的角色进行鉴别，并确认其可信，并且：

根据这些可信员工不同的权限功能要求定义不同鉴别方式

给与这些可信员工 CA 和 RA 系统相应的管理权限

确认可信员工需要通过人力资源政策和安全政策，如对身份证、驾驶执照的确认，可信人员的背景调查将在 CP 中进行描述。

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。

需要职责分割的角色包括且不限于：

- 密钥管理员
- 接触证书客户资料的人员
- 安全管理员
- 证书申请鉴证人员
- 认证系统操作人员

- 秘密分割持有者

5.3 人员控制

5.3.1 资格、经历和清白要求

认证机构和注册机构要求确认可信人员的程序需要有必备的背景调查。包括资格审查、工作经历调查、违法犯罪记录调查，确保这些人员能够胜任其工作。

5.3.2 背景调查程序

认证机构和注册机构应制定可信人员调查程序，并确定最多 5 年需要对可信人员重复一次调查。调查程序必须符合我国的法律法规要求，关于人员的背景调查还要服从人员所在地域的政府或管理机构的要求。

背景调查的主要因素包括却不限于以下内容：

- 身份证明，如个人身份证、护照、户口本等。
- 学历、学位及其他资格证书。
- 个人简历，包括教育、培训经历，工作经历及相关的证明人。
- 无犯罪证明材料。
- 是否有金融信贷不良记录

为了防止信息有假造情形发生，背景调查中认证机构应通过合法手段，尽可能地通过相关组织、部门进行人员背景信息的核实。并由认证机构的人力资源部门和安全管理人员共同完成人员评估工作。

背景调查材料包括以下内容：

- 验证先前的工作记录
- 验证身份证明的真实性。
- 验证学历、学位及其他资格证书的真实性。
- 通过可靠途径确认教育、培训经历。
- 检验无犯罪证明材料并确认无犯罪记录。
- 通过适当途径了解是否有工作中的严重不诚实行为。

背景调查时出现下列情况可以作为拒绝其获得可信职位候选人的资格或取消其可信人员的资格：

- 候选人或可信人员捏造事实；
- 不可靠人员的证明；
- 某些的犯罪事实；
- 非法的个人身份证明；
- 工作中有严重不诚实行为。

5.3.3 培训要求

为了使认证机构和注册机构的人员能胜任其承担的工作，认证机构应该提供岗前培训和必要的工作培训，和周期性的再培训。建议的培训包括以下内容：

- CTN 系统安全策略与安全机制
- 基本的 PKI 概念；
- 工作职责；
- 安全操作策略程序；
- 硬件和软件的使用和操作；
- 事故和安全威胁的报告和处理。

5.3.4 再培训的频度和要求

认证机构和注册机构应根据需要安排周期性的培训，以保证关键岗位的职员保持熟练的工作水平，顺利的完成其工作职责。

5.3.5 工作岗位轮换的频度和次序

没有约定。

5.3.6 未授权行为的制裁

认证机构和注册机构应建立并维护一套管理办法来保障对于未授权行为或其他对认证机构及注册机构策略和程序的破坏行为应采取适当的纪律处罚。这些纪律处罚包含的措施包括中止员工相应工作并解除相应员工的劳动合同，纪律处罚程度与未经授权行为的频度和严重性相关。

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认证机构雇员一样。

担任可信角色的独立合约人和顾问需要通过 CP § 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 提供给人员的文件

提供给认证机构和注册机构内部员工的文件应包括培训材料和与员工工作相关文档。

5.4 审计记录程序

5.4.1 记录事件的类型

认证机构和注册机构的审计日志和事件记录不管采用是电子的还是手动生成的,都应该包含如下信息：

- 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

认证机构应在 CPS 中说明记录事件及日志的类型。

.

认证机构应手工或自动记录如下几类事件：

- 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。

- 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。

- 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。

- 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。

- 认证机构设施的访问
  - 授权人员进出认证机构设施。
  - 非授权人员进出认证机构设施及陪同人。
  - 安全存储设施的访问。

- 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

5.4.2 处理日志的频度

认证机构应定期检查一次审计日志以便发现重要的安全和操作事件，并对发现的安全事件采取相应的措施。对于审计结果形成文档。

5.4.3 审计日志保留的期限

审计日志处理和归档之后，具体应根据 5.5.2 内容要求。

5.4.4 审计日志的保护

应通过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

认证机构对审计日志应定期进行备份。增量备份应该每天进行，全备份应该每周进行。

5.4.6 审计收集系统

无规定。

5.4.7 对导致事件主体的通知

审计记录报告一个事件时，应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，认证机构应定期进行安全脆弱性评估，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

需要归档记录的类型如 CP § 5.4.1，除此之外，对订户证书、CA 证书也要进行归档。

认证机构和注册机构需要归档下列信息：

- 审计记录的归档依据 CP § 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 归档记录的保留期限

对于 CP § 5.5.1 中的不同的归档记录，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。

- 对认证机构和注册机构管理事件的归档，应保留一年以上。
- 对 CA 证书和密钥生命周期内的管理事件的归档，其保留期限应不少于 CA 证书和密钥生命周期。
- 订户证书的归档保留期限不少于 5 年。
- CA 证书和密钥的归档在 CA 证书和密钥生命周期之外，需额外保留 5 年。

5.5.3 归档文件的保护

应通过适当的物理和逻辑的访问控制方法保护归档数据，只有授权的可信人员允许访问归档数据，防止未经授权的浏览、修改、删除或其它的篡改行为。

5.5.4 归档文件的备份过程

认证机构对归档文件应定期进行备份。增量备份应该每天进行，全备份应该每周进行。备份文件将被放在异地进行保存。

5.5.5 记录时间戳要求

如 CP § 5.4.1 所规定，每项记录必须有时间，但这个证书时间戳不需要是基于密码技术的。

5.5.6 归档收集系统

各自实体应在内部建设归档收集系统，包括认证机构和外部独立实体的注册机构。

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 密钥变更

只要 CA 密钥对的累计寿命没有超过 CP § 6.3.2 中规定的、最大生命期，那么， CA 证书可以使用原密钥进行更新。否则，它将不再用于服务，这时需要产生新的密钥对，替换已经过期的 CA 密钥对。在一个上级 CA 证书过期之前，密钥变更过程被启动，以保障

这个上级 CA 体系中的实体从 CA 旧密钥对到新密钥对的平稳过渡。认证机构 CA 密钥变更应遵从如下要求：

- 一个上级 CA 应不迟于其私钥到期之前 60 天停止签发新的下级 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，对于确认、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

认证机构必须通过实施物理、逻辑和过程控制等有效的综合方案将密钥损害或其他灾难造成的风险和潜在影响降到最小。此外，认证机构必须建立灾难恢复方案和程序，并且在合理的期限内恢复业务运作。

5.7.1 事故和损害处理程序

认证机构应建立事故和损害处理程序，进行事故调查和事故响应。

备份信息应该被妥善保存，在一旦发生损害和灾难的时候应可以被有效使用，这些信息包括：

- 证书认证系统的主要数据、审计数据、证书签发记录
- CP6.2.4 中规定的私钥归档信息
- 备份的证书认证系统
- 注册中心和客户的应用系统应由其妥善备份

5.7.2 计算机资源、软件和/或数据的损坏

如果出现计算机资源、软件和/或数据的损坏的事件，必须将事件报告给认证机构的安全管理部门，并立即启动事故处理程序，如有必要，可启动灾难恢复程序。

5.7.3 实体私钥损害处理程序

当证书订户发现其私钥损害时，订户应立即通知认证机构吊销其证书，并尽可能地通知信赖方；认证机构应及时吊销订户证书并按 CP § 4.9 发布证书吊销信息。

当 CA 证书出现私钥损害时，认证机构应立即吊销 CA 证书并及时通过广达的途径通知信赖方，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

认证机构和注册机构在发生灾难后，应有如下几个方面的业务存续能力：

- 在尽可能短的时间内恢复业务系统，最多不超过 24 小时。
- 能够恢复客户信息。
- 能够保证恢复后的运营场地符合安全要求。
- 能够恢复对老客户、新客户的服务。
- 有足够的人有继续业务并且不违反职责分割的要求。

5.8 CA 或 RA 的中止

认证机构或注册机构需要停止运行时，在停止运作之前，有关实体要在合理的时间内尽快通知订户、信赖方和其他受到影响的实体。如果认证机构要终止运行，认证机构应制定终止 CA 运行计划，以使订户和信赖方的损失降到最低。这种终止计划包括下列适用内容：

- 通知政府主管机构
- 通告由于 CA 运行停止而受到影响的各方，如订户和信赖方，通知他们该 CA 的状态。
- 处理通知费用问题。
- 吊销认证机构签发的 CA 证书。
- 保存 CA 归档文件和记录到规定的期限。
- 订户和用户服务的继续。
- 证书吊销服务的继续，如 CRL 的签发或在线证书状态检查服务的维护。
- 如果必要，吊销最终订户和下级 CA 的未过期和未被吊销的证书。
- 如果需要，对证书未到期、未吊销而根据 CA 中止计划被吊销订户的赔偿支付，或者由继任 CA 签发替换证书给订户。
- CA 私钥和保存这个私钥的硬件模块的处理。
- 将终止的 CA 服务传给继任 CA 的条款。

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

CA 密钥对的产生，必须由若干名接受过相关培训的可信雇员在密钥生成室（CP §5.1.1.2.6）按照严格的安全过程，在能够生成有足够安全强度密钥的可信系统上操作完成。用于此类密钥生成的密码模块需通过国家密码主管部门鉴定、认证。对于 CA 密钥对的产生，认证机构应该有严格的密钥生成流程。

6.1.1.2 最终订户密钥对的产生

对于第 1 类证书可以使用浏览器自带的密码模块生成密钥，也可以使用硬件密码模块（如 USB Key，智能卡），对于第 2 类证书最好使用硬件密码模块生成密钥，对于第 3 类证书（除服务器证书外）必须使用硬件密码模块生成密钥。对于服务器证书，订户利用 Web 服务器软件提供的密钥生成功能生成密钥或用专门的硬件加速模块。

6.1.2 私钥传输给订户

在最终订户生成自己的密钥对的情况下，不需要将私钥传给订户。如果认证机构或注册机构在硬件加密卡或智能卡中为最终订户生成密钥对，那么，它应该通过安全的、采用了防篡改封装的方式将这些装置分发给最终订户。用于激活设备的数据通过其他途径发给最终订户。认证机构或注册机构应记录这种设备的分发。

6.1.3 公钥传输给证书签发机关

为了获得数字证书，最终订户和 RA 通过 PKCS#10 格式的证书签名请求信息或其它数字签名的文件包格式，以电子的方式将公钥提交给认证机构签发，这些请求或文件包的传送需要使用安全协议保护，比如安全套接层协议（SSL）。

6.1.4 CA 公钥传输给信赖方

认证机构应该通过安全可靠的途径将 CA 公钥传给信赖方，包括从安全站点下载、面对面的提交、软件及操作系统预埋等方式。

在订户证书签发时，认证机构可通过 PKCS#7 格式将除根证书外的证书链传递给最终订户。认证机构也需要通过目录发布其 CA 证书。

6.1.5 密钥的长度

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

无规定。

6.1.7 密钥使用目的

认证机构签发的 X.509v3 证书包含了密钥用法扩展项，其用法与 RFC 3280 标准 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002) 相符。证书中的密钥用法扩展项按表 5 所示设定：

表 5 –密钥用法扩展项的设置

		CA	*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	Set	Set	Set
1	nonRepudiation	Clear	Clear	Clear	Clear	Set	Clear
2	keyEncipherment	Clear	Set	Clear	Clear	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
8	decipherOnly	Clear	Clear	Clear	Clear	Clear	Clear

抗抵赖位不是必须设置的，是因为 PKI 还未就此位的真正意义达成共识。除非达成共识，否则此位对于信赖方没有什么意义。而且，很多应用不能识别此位。因此，设置此项不能帮助信赖方达到信任的目的。

6.2 私钥保护和密码模块工程控制

认证机构必须通过物理、逻辑和过程控制的综合实现来确保天 CA 私钥的安全。订户合同会要求证书订户采取必要的预防措施防止私钥的丢失、泄露、更改或未经授权的使用。

6.2.1 密码模块的标准和控制

认证机构必须使用国家密码管理部门认可、批准的硬件密码模块生成根 CA、签发证书的 CA 和其他 CA 密钥对，并存储相关 CA 私钥。

6.2.2 私钥多人控制（m 选 n）

认证机构必须通过技术及过程上的控制机制来实现多名可信人员共同参与 CA 加密设备的操作。技术上的控制可使用“秘密分割”技术，即将使用一个 CA 私钥时所需的激活数据分成若干个部分，称为秘密分割，分别由受过训练的可信人员持有，这些人员称为“秘密分管者”。如果为一个硬件密码模块的秘密分割总数为 m，那么必须有超过 n 个的秘密分割才能激活储存在密码模块中的 CA 私钥。在这里 m 不小于 3，n 不小于 2。

6.2.3 私钥托管

无规定。

6.2.4 私钥备份

为了常规恢复和灾难恢复目的，认证机构必须创建 CA 私钥的备份。这种私钥备份以加密的形式保存在硬件密码模块中。存储 CA 私钥的密码模块应符合 CP § 6.2.1 的要求。CA 私钥复制到备份硬件密码模块中要符合 CP § 6.2.6 的要求。备份的私钥要避免通过物理或加密方式进行的非授权的修改或泄露，例如存放在保险箱。

对于最终订户证书，如 1 类、2 类证书和服务器证书，如果其私钥存放在软件密码模块中，建议订户对私钥进行备份，备份的私钥需要采用口令保护等授权访问控制，防止非授权的修改或泄露。

6.2.5 私钥归档

当认证机构的 CA 密钥对到期后，这些 CA 密钥对必须归档保存至少 5 年。归档 CA 密钥对要使用满足 CP § 6.2.1 要求的硬件密码模块安全存储，并且要有过程控制阻止归档 CA 密钥对返回到产品系统中。在归档期限末期，对 CA 私钥的销毁应符合 CP § 6.2.10 所述。

6.2.6 私钥导入、导出密码模块

认证机构必须在硬件密码模块上生成 CA 密钥对，该密钥对将在这个模块中使用。此外，为了常规恢复和灾难恢复，认证机构需要创建 CA 密钥对的副本。当 CA 密钥对备份到另外的硬件密码模块上时，这种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身份鉴别，以防止 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

CA 私钥必须存放在硬件密码模块中，并且在密码模块中使用。3 类证书除服务器证书外，私钥必须存放硬件密码模块中，并且在密码模块中使用。1 类、2 类个人证书私钥最好在硬件密码模块（如 USB Key、SmartCard）中存储和使用，当然也可以使用有安全保护措施的软件密码模块。服务器证书私钥可以存放在服务器程序特定的软件密码模块中，但最好使用带有硬件密码模块的加速卡。

6.2.8 激活私钥的方法

6.2.8.1 最终订户私钥

6.2.8.1.1 1 类证书

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订户的订户计算机以防止在没有得到用户授权的情况下，其他人员使用订户的订户计算机和相关的私钥。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。如果使用口令保护私钥，软件密码模块加载后，还需要输入口令才能激活私钥。

1 类证书可以将私钥存放在诸如 USB Key 和智能卡硬件密码模块中，并且私钥可以通过 PIN 码（口令）、指纹鉴别进一步保护。如果私钥没有 PIN 码（口令）、指纹鉴别保护，那么，当用户计算机上安装了相应的驱动后，将 USB Key 和智能卡插入相应的读卡设备中，则私钥被激活可以使用。如果私钥有 PIN 码（口令）、指纹鉴别保护，那么，当用户计算机上安装了相应的驱动后并将 USB Key 和智能卡插入相应的读卡设备后，只有输入通过相应的 PIN 码（口令）、指纹鉴别，私钥才激活可以使用。

6.2.8.1.2　2 类证书

2 类证书的私钥激活类似于 1 类证书，只是 2 类证书建议将私钥存放在诸如 USB Key 和智能卡硬件密码模块中，并且私钥通过 PIN 码（口令）、指纹鉴别保护。

6.2.8.1.3　3 类证书

对于组织机构身份证书、组织机构代表人证书、必须使用 USB Key、智能卡等硬件密码设备存放私钥，私钥不能出卡，并且使用 PIN 码（口令）、指纹鉴别保护私钥。要激活私钥，用户计算机上需安装相应的驱动后并将 USB Key 和智能卡插入相应的读卡设备，通过相应的 PIN 码（口令）、指纹鉴别，私钥才激活可以使用。

6.2.8.2 服务器证书

对于服务器证书，如果没有使用硬件密码模块，则私钥是存放在服务程序的软件密码模块中，这时应该使用口令对私钥进行保护。但服务程序启动，软件加密模块被加载，输入相应私钥保护口令后，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计算机上，服务程序启动，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

认证机构的私钥存放在硬件密码模块中，并且其激活数据按 CP § 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 CP § 6.2.2 规定的 m 选 n 的原则输入激活数据的分割。

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 CA 私钥，当存放私钥的加密卡断电,，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。

对于最终订户加密证书私钥，在其生命周期结束后，应该妥善保存一定期限，以便于解开加密信息。对于最终订户私钥，在其生命周期结束后，如果无需再保存，可以通过私钥的删除、系统或密码模块的初始化来销毁。

认证机构 CA 私钥，在生命周期结束后，需将 CA 私钥的一个或多个备份进行归档，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时需在多名可信人员参与的情况下安全销毁。CA 私钥存放在硬件加密卡中，CA 私钥的销毁必须通过将 CA 私钥从加密卡中彻底删除或将加密卡初始化的方式销毁。

6.2.11 密码模块的评估

无规定。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

认证机构必须归档 CA 和最终订户证书，归档的证书可存放在方数据库中。

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。

另外需注意的是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，允许使用原密钥对对证书进行更新。但是密钥对不能无限期使用。对于不同的证书，其密钥对允许通过证书更新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 位根 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

用于保护存放有认证机构 CA 私钥的加密卡激活信息（秘密分割）的产生过程必须安全可靠，符合天威诚信密钥生成规程参考指南中的要求。秘密分割的创建和分发记录有相应的日志。

CA 私钥和订户证书私钥的激活数据一般是口令，这些口令必须：

- 由用户产生；
- 至少 8 位字符；
- 至少包含一个字符和一个数字；
- 至少包含一个小写字母；
- 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。

6.4.2 激活数据的保护

对于 CA 私钥的激活数据，认证机构必须通过秘密分割将分割后的激活数据由不同的可信人员掌管，而且掌管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割掌管者责任。秘密分割必须存放在 CP § 5.1.1.2.6 所描述的第 7 层保险盒中。

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

当私钥的激活数据进行传送时，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。还有，Windows 或网络的登录用户的用户名/密码（用于最终订户激活数据），经过网络传送时注意非法用户的窃取。

6.4.3.2 激活数据的销毁

当私钥的激活数据不需要时应该销毁，并保护它们在此过程中免于丢偷窃、泄露或非授权使用，销毁的结果是无法通过残余信息、介质直接或间接获得激活数据的部分或全部，比如记录有口令的在纸页必须粉碎。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

认证机构应确保包含 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，认证机构应只允许有工作需求的必要人访问产品服务器，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。这种分离可以阻止除指定的应用程序外对网络访问的访问。认证机构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。

系统口令口令必须符合。

6.5.2 计算机安全评估

CA 和 RA 作用的特别敏感的安全区域应符合 EAL 3 安全保障要求(信息技术安全评估 v 2.1, Aug. 1999)。

6.6 生命周期技术控制

6.6.1 系统开发控制

无规定。

6.6.2 安全管理控制

认证机构应制定策略、管理制度与流程对 CA 运营的各方面进行安全管理。

6.6.3 生命期的安全控制

无规定。

6.7 网络的安全控制

认证机构应通过防火墙、入侵检测、防病毒、安全身份认证等安全技术，确保认证系统的安全运营。对于认证系统的网络安全，认证机构应制定专门的网络安全策略与实施方案，有关方案应符合天威诚信安全和审计要求指南。

6.8 时间戳

认证系统的各种系统日志、操作日志应该有对应的记录时间。

7. 证书、CRL 和 OCSP 轮廓

7.1 证书轮廓

依本证书策略签发的证书符合(a)ITU-T X.509v3（1997）：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 6 所描述。

表 6 – 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 CP § 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
主题 DN	证书持有者或实体的甄别名。
公钥	根据 RFC 3280 编码，使用 CP § 7.1.3 中指定的算法，密钥长度满足 CP § 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 证书的扩展项

依本证书策略签发的 X.509v3 证书的扩展项满足 CP §§ 7.1.2.1-7.1.2.8 的要求。私有扩展项的使用是允许的，但是除非由于特别应用而包含该项，不保证私有扩展项的使用。

7.1.2.1 密钥用法（Key Usage）

指定证书密钥对的用法。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本 CP 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 主题备用名（subjectAltName）

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

7.1.2.4 基本限制扩展项（BasicConstraints）

CA 证书的基本限制扩展项中的主题类型被设为 CA。最终订户证书的基本限制扩展项的主题类型设为最终实体 (End-Entity)。这个扩展项的 criticality 域设置为 FALSE。将来，对于其它的证书，这个扩展项的 criticality 域可以设置为 TRUE。

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）

对不同的证书，22 设定扩展的密钥用法扩展项。

表 7 – 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*
Criticality		FALSE	FALSE	FALSE	FALSE	FALSE
0	ServerAuth	Set	Set	Clear	Clear	Clear
1	ClientAuth	Set	Set	Set	Set	Set
2	CodeSigning	Clear	Clear	Clear	Clear	Clear
3	EmailProtection	Clear	Clear	Clear	Set	Set
4	IpsecEndSystem	Clear	Clear	Clear	Clear	Clear
5	IpsecTunnel	Clear	Clear	Clear	Clear	Clear
6	IpsecUser	Clear	Clear	Clear	Clear	Clear
7	TimeStamping	Clear	Clear	Clear	Clear	Clear
8	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）

证书中的 CRL 的分发点扩展项，它包含本地的一个链接，可以向信赖方提供 CRL 的信息以便其查询证书状态。此扩展项的 criticality 项应设为 FALSE。

7.1.2.7 签发 CA 密钥标识符

最终订户证书及中级 CA 证书加入签发 CA 密钥标识符扩展项，当证书签发者包含主题密钥标识扩展项时，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 的主题 DN 和序列号。这个扩展项的 criticality 域设置为 FALSE。

7.1.2.8 主题密钥标识符

证书的主题密钥标识符扩展项赋值时，证书主题的公钥的密钥标识符被产生？？。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

依本 CP 签发的证书按照 RFC 3280 标准，用 sha1RSA (OID: 1.2.840.113549.1.1.5) 或 md5RSA (OID: 1.2.840.113549.1.1.4)算法签名。

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

md5WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}

md2WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 2}

id-dsa-with-sha1 ID ::= { iso(1) member-body(2) us(840) x9-57 (10040) x9cm(4) 3}

7.1.4 命名形式

依本 CP 签发的证书的甄别名符合 X500 关于目录名的规定。对于证书主题甄别名，O 代表证书持有者所在的组织机构，第一个 OU 代表所在的部门。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。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信赖方协议所在的 URL。

7.1.5 命名限制

除一类证书外，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

当使用证书策略扩展项时，证书中包含证书策略的对象标识符，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

无规定。

7.1.8 策略限定符的语法和语义

该策略限定符可存放指向 CP 的 URL。

7.1.9 关键证书策略扩展项的处理语义

与 X509 和 PKIX 规定一致。

7.2 CRL 轮廓

依本 CP 签发的 CRL 符合 RFC3280 标准。CRL 至少包含如表 8 所述基本域和内容。

表 8 – 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) 或 md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) 或 md2RSA (OID: 1.2.840.113549.1.1.2)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。天威诚信 CRL 自发布之日起有效。
下次更新	CRL 下次签发的日期。对于根 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 X509 和 PKIX 规定一致。

7.3 OCSP 轮廓

7.3.1 版本号

无规定。

7.3.2 OCSP 扩展项

无规定。

8. 一致性审计和其他评估

认证机构应定期对物理控制、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、要求一直，并根据审查结果采取行动。

8.1 评估的频度和情形

一致性审计应该每年执行一次。

8.2 评估者的身份/资格

进行审计的评估者必须是：

- 熟悉公钥基础设施技术、信息安全工具和技术、安全审计和具有第三方的证明能力。
- 具有中华人民共和国注册会计师资格或类似资格，接受过专项培训，每年都接受了资格评估、测试、供职于权威机构和接受过持续的专业教育。

8.3 评估者与被评估者之间的关系

评估者必须是独立于认证机构的会计事务所（或等同组织）。

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行动

对在一致性审计中发现的重大意外或不作为应该采取行动。采取行动的决定由认证机构管理层根据审计报告作出。认证机构的管理层负责根据审计结果制定和实施改正计划，

如果认证机构确认审计中发现的意外或不作为对证书体系的安全或完整性会造成立即威胁，则认证机构必须在 30 天内制定改正行动计划，并在合理的期限内执行它。

8.6 评估结果的传达与发布

审计结果传达和发布给一般的公众是不需要。

8.7 其他评估

除了一致性审计外，认证机构也可以执行其他的评估和调查以保证其信任域的可信赖性，这些内容包括但不限于：

- 认证机构的安全和业务评估。内容可包含认证机构的安全设施、安全文档、CPS、相关协议、隐私策略和鉴证计划的执行情况。
- 在进行一致性的审计或风险管理过程中，如果发现不完全符合或出现例外情况，认证机构或它授权的代表有资格可进行“补充的风险管理评估”。

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

无规定。

9.1.2 证书查取的费用

无规定。

9.1.3 证书吊销或状态信息的访问费用

证书吊销和吊销列表（CRL）的获取不应收取任何费用。OCSP 服务可以作为增值的吊销和状态信息服务收费。

9.1.4 其他服务费用

无规定。

9.1.5 退款政策

无规定。

9.2 财务责任

9.2.1 保险覆盖

认证机构、订户和信赖方应该通过第三方保险，对于自身原因造成的其他方的损失进行赔偿。保险覆盖的范围主要针对 CP § 9.9 中所规定的赔偿。
订户协议、信赖方协议可以要求订户和信赖方购买有关保险。

9.2.2 其他财产

无规定。

9.2.3 保险或担保对最终实体的覆盖

保险对最终实体的覆盖见 CP § 9.9，CP § 9.2.1。

9.3 商业信息保密

认证机构、注册机构应有专门的保密方案、计划，在符合法律的前提下，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

认证机构、注册机构需要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

证书策略、认证业务声明、信赖方协议、订户协议等。

9.3.3 保护保密信息的责任

认证机构、注册机构须通过有效的技术手段和管理程序，保护商业的和客户的保密信息。

9.4 个人隐私保密

9.4.1 隐私保密计划

认证机构应制定隐私保密计划对证书订户的个人信息保密。

9.4.2 作为隐私处理的信息

作为隐私处理的信息包括，最终订户注册申请证书中提交的信息，包括联系电话、地址等；个人与认证机构、注册机构签订的协议。

9.4.3 不被认为隐私的信息

如下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。

9.4.4 保护隐私的责任

认证机构、注册机构在没有获得客户授权的情况下，不得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

认证机构、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，而且这种同意和授权是要用可归档的方式（如传真、信函、电子邮件等）。

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，认证机构、注册机构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、行政执行机关是允许的，即使这样，认证机构、注册机构也应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

认证机构对它签发的证书、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 CP 中的知识产权

认证机构对本 CP 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题对应实体或实体拥有者的知识产权。

9.6 表述与担保

9.6.1 CA 的表述与担保

订户同意订户协议是作为订户注册申请的一个条件，信赖方同意信赖方协议作为接收证书及状态信息的一个条件。同样地，认证机构必须按要求使用订户协议和信赖方协议。

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

认证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和约束。

认证机构对证书订户必须做出如下担保：

- 证书中不存在批准证书申请或签发证书的实体已知的对事实的实质性错误描述，或来自于这些实体的错误信息。
- 在管理证书申请或制造证书时，批准证书申请或签发证书的实体不会因为工作疏忽将错误信息包含到了证书中。
- 他们的证书满足 CP 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本 CP 的要求。

认证机构对证书信赖方必须做出如下担保：

- 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。
- 在认证机构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 CP § 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 的规定。

除此之外，认证机构还可以提供其他的担保。

9.6.2 RA 的表述与担保

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，并且需确认的信息是正确的、准确的。

9.6.3 订户的表述与担保

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：

- 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。
- 保护好自己的私钥，没有经过授权的人员不得访问订户的私钥。
- 在证书申请时，订户的所有陈述都是对的。
- 订户提供的和包含在证书中的所有信息都是对的。
- 证书只能按照本 CP 用于经过授权的或其它合法的使用目的。
- 不将证书用于与证书使用目的以外的场合。

9.6.4 信赖方的表述与担保

在任何信赖行为发生之前，信赖方阅读必须信赖方协议，独立评估证书使用于任何目的适当性，并确定证书将会被恰当使用于一目的。

9.6.5 其他参入者的表述与担保

无规定。

9.7 担保免责

在法律允许的范围内，认证机构认证业务声明、订户协议、信赖方协议和其他订户协议应包含条款免除认证机构的某些可能担保，这包括为了某个特定目的的任何适销性和合适性担保。

9.8 有限责任

在法律允许的范围内，认证机构订户协议、信赖方协议和其他订户协议限制认证机构承担的责任。责任限制包括排除间接的、特殊意外造成的、偶然的和后续性的损失。

9.9 赔偿

在如下情况，认证机构对自身原因造成的订户损失对订户进行赔偿，或信赖方在履行了信赖方协议的情况下，由于认证机构或订户的原因造成的信赖方损失，认证机构对信赖方的赔偿。认证机构可通过购买第三方保险对赔偿进行覆盖。

- 认证机构在批准证书前没有执行程序确认证书申请，造成证书的错误签发。
- 由于认证机构的原因，使得证书中出现了错误信息
- 由于认证机构 CA 私钥的泄漏。

在如下情况，订户对自身原因造成的认证机构、信赖方损失对认证机构进行赔偿。订户可通过购买第三方保险对赔偿进行覆盖。

- 订户在证书申请中对事实的虚假或错误时描述。
- 在证书申请中订户没有披露重要的事实，如果这种错误表述或遗漏是因为粗心或故意欺骗任何一方。
- 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。
- 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法。

在如下情况，信赖方对自身原因造成的认证机构损失对认证机构进行赔偿。信赖方可通过购买第三方保险对赔偿进行覆盖。

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

9.10 期限与终止

9.10.1 期限

作为认证机构的核心业务文件，CP 和 CPS 在认证机构中止业务前一直有效，在发布新的 CP 和 CPS 版本后，新的 CP 和 CPS 版本将取代原 CP 和 CPS 版本。对于证书订户而言，证书签发时的 CP、CPS 和订户协议将起作用直到证书到期或吊销，除非法律相冲突的内容、与事实不符的错误描述。对某一特定证书而言，在公钥的有效使用期限内，信赖方协议有效。公钥的有效使用期限可以比证书有效期长，比如签名证书到期后，公钥可以

继续对证书有效期内私钥签名的信息进行验证。其他合同、协议的有效期限，由相应的合同、协议约定。

9.10.2 终止

当认证机构中止业务时，CP 和 CPS 及终止。当证书到期或吊销后，订户协议即终止。公钥到了的有效使用期，对应的信赖方协议终止。

9.10.3 终止的效果与存续

CP 和 CPS 的中止，而非更新，意味着认证机构认证业务的终止，但认证业务的终止不意味着认证机构责任的终止。认证机构在业务终止后应采取合理的措施，保证订户的利益，如证书可继续使用，对客户进行赔偿，或将认证服务转到其他认证机构。订户证书到期、证书吊销意味着订户协议的终此，认证机构不再对证书私钥（签名）或公钥（加密）的使用承担任何责任，信赖方不应再信赖证书对应的签名私钥或加密公钥和。
当由于某种原因，如内容修改、与适用法律相冲突，CP、CPS、订户协议、信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 对参入者个别通告及信息交互

认证机构在必要的情况下，如主动吊销订户证书、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，可通过适当方式，如电话、电邮、信函、传真等，个别通知订户、信赖方。

9.12 修改

9.12.1 修改程序

本证书策略将尽量避免不必要的修改。不定期地，天威诚信将对本 CP 进行检查、评估，当天威诚信认为应该对本 CP 做出修改时，天威诚信法律部门将对本 CP 及其他相关文档、协议的修改提出建议，获得天威诚信 PMA 及天威诚信管理层批准后，由天威诚信法律部门负责组织修改。修改后的 CP 及其他相关文档、协议经 PMA 及天威诚信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CP通过天威诚信信息库的业务更新和通告栏发布，其地址为：**https://www.itrus.com.cn/repository/updates**.。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 CP 经批准后将立即在天威诚信信息库的业务更新和通告栏发布。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 OID 必须修改的情形

如果天威诚信 PMA 认为需要对证书策略的对象标识符进行修改，则此项修改应包含每类证书的证书策略的新对象标识符。

9.13 争议解决条款

当认证机构、订户和信赖方之间出现争议时，有关方面应依据协议通过协商解决，协商解决不了的，可通过法律解决。订户协议、信赖方协议和其他订户协议都应该包含解决争执的相应条款。

9.14 管辖法律

中华人民共和国法律、规则、规章、法令和政令将管辖认证机构的业务活动。认证机构的任何业务活动必须受有关法律、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 符合适用法律

认证机构的所有业务、活动、合同、协议必须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、隐私法、消费者权益保证法等。

9.16 一般条款

9.16.1 完整协议

CP、CPS、订户协议及信赖方协议及其补充协议将构成 PKI 参入者之间的完整协议。

9.16.2 让渡

认证机构、订户及信赖方之间的责任、义务不能通过任何形式让渡给其他方。

9.16.3 分割性

在法律允许的范围内，认证机构的订户协议、信赖方协议和其他订户协议可以包含可分割性条款。一个协议中的可分割性条款防止协议中一个条款的无效影响协议中其他条款效力。

9.16.4 强制执行

在认证机构、订户和信赖方之间出现纠纷、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 不可抗拒力

在法律允许的范围内，认证机构的订户协议、信赖方协议和其他订户协议应该包括保护不可抗力条款，明确在出些哪些不可抗拒力情况下，认证机构可以免除或部分免除责任。一般地，自然灾害、战争属于不可抗拒力。

9.17 其他条款

无规定。