安信 CA 电子认证业务规则

（CPS）

版本 V3.0

发布日期：2017 年 3 月 24 日

生效日期：2017 年 3 月 24 日



吉林省安信电子认证服务有限公司

目　　录

1　概括性描述 12

1.1　概述 12

1.2　文档名称与标识 13

1.3　电子认证活动参与者 13

1.3.1　电子认证服务机构 13

1.3.2　注册机构 13

1.3.3　证书服务受理点 13

1.3.4　垫付商 14

1.3.5　订户 14

1.3.6　依赖方 14

1.3.7　其他参与者 15

1.4　证书应用 15

1.4.1　适合的证书应用 15

1.4.2　限制的证书应用 15

1.5　策略管理 16

1.5.1　策略文档管理机构 16

1.5.2　联系方式 16

1.5.3　决定 CPS 符合策略的机构 16

1.5.4　CPS 批准程序 16

1.6　定义和缩写 17

2　信息发布与信息管理 19

2.1　认证信息的发布 19

2.2　发布时间和频率 19

2.3 信息库访问控制 19

3 身份识别与鉴别 21

3.1 命名 21

3.1.1 名称类型 21

3.1.2 需要有意义的名称 21

3.1.3 订户的匿名或伪名 21

3.1.4 不同名称形式的规则 22

3.1.5 名称的唯一性 22

3.1.6 商标的识别、鉴别和角色 22

3.2 初始身份认证 23

3.2.1 证明拥有私钥的方法 23

3.2.2 组织机构身份的鉴别 23

3.2.3 个人身份的鉴别 24

3.2.4 没有验证的申请者信息 24

3.2.5 授权确认 24

3.2.6 互操作准则 24

3.3 密钥更新请求的标识与鉴别 25

3.3.1 常规密钥更新的标识与鉴别 25

3.3.2 吊销后密钥更新的标识与鉴别 25

3.4 吊销请求的标识与鉴别 25

4 证书生命周期操作要求 27

4.1 证书申请 27

4.1.1 证书申请实体 27

4.1.2 注册过程与责任 27

4.1.2.1 注册流程 27

4.1.2.2 电子认证服务机构的责任 28

4.1.2.3 注册机构的责任 28
4.1.2.4 受理点的责任 29
4.1.2.5 垫付商责任 29
4.1.2.6 订户的责任 30
4.1.2.7 依赖方的责任 30
4.2 证书申请处理 30
4.2.1 执行识别与鉴别功能 30
4.2.2 证书申请批准和拒绝 31
4.2.3 处理证书申请的时间 31
4.3 证书的签发 31
4.3.1 证书签发中注册机构和电子认证服务机构的行为 31
4.3.2 电子认证服务机构和注册机构对用户的通告 32
4.4 证书接受 32
4.4.1 构成接受证书的行为 32
4.4.2 电子认证服务机构对证书的发布 33
4.4.3 电子认证服务机构对其他实体的通告 33
4.5 密钥对和证书的使用 33
4.5.1 订户私钥和证书的使用 33
4.5.2 依赖方公钥和证书的使用 34
4.6 证书更新 34
4.6.1 证书更新的情形 34
4.6.2 请求证书更新的实体 34
4.6.3 证书更新请求的处理 35
4.6.4 颁发新证书时对订户的通告 35
4.6.5 构成接受更新证书的行为 35
4.6.6 电子认证服务机构对更新证书的发布 35
4.6.7 电子认证服务机构对其他实体的通告 35

4.7 证书密钥更新 36
4.7.1 证书密钥更新的情形 36
4.7.2 请求证书密钥更新的实体 36
4.7.3 证书密钥更新请求的处理 36
4.7.4 颁发新证书时对订户的通告 37
4.7.5 构成接受密钥更新证书的行为 37
4.7.6 电子认证服务机构对密钥更新证书的发布 37
4.7.7 电子认证服务机构对其他实体的通告 37
4.8 证书变更 37
4.8.1 证书变更的情形 37
4.8.2 请求证书变更的实体 38
4.8.3 证书变更请求的处理 38
4.8.4 颁发新证书时对订户的通告 38
4.8.5 构成接受变更证书的行为 38
4.8.6 电子认证服务机构对变更证书的发布 38
4.8.7 电子认证服务机构对其他实体的通告 39
4.9 证书吊销和挂起 39
4.9.1 证书吊销的情形 39
4.9.2 请求证书吊销的实体 40
4.9.3 吊销请求的流程 40
4.9.4 吊销请求的宽限期 41
4.9.5 电子认证服务机构处理吊销请求的时限 41
4.9.6 依赖方检查证书吊销的要求 41
4.9.7 CRL 发布频率 41
4.9.8 CRL 发布的最大滞后时间 41
4.9.9 在线状态查询的可用性 41
4.9.10 在线状态查询要求 42
4.9.11 吊销信息的其他发布形式 42

4.9.12 密钥损害的特别要求 42
4.9.13 证书挂起的情形 42
4.9.14 请求证书挂起的实体 42
4.9.15 挂起请求的流程 43
4.9.16 挂起的期限限制 43
4.10 证书状态服务 43
4.11 订购结束 43
4.12 密钥生成、备份与恢复 43
4.12.1 密钥生成、备份与恢复的策略与行为 43
5 认证机构设施、管理和操作控制 45
5.1 物理控制 45
5.1.1 场地位置与建筑 45
5.1.2 物理访问 45
5.1.3 电力与空调 45
5.1.4 水患防治 46
5.1.5 火灾防护 46
5.1.6 介质储存 46
5.1.7 废物处理 46
5.1.8 异地备份 46
5.2 程序控制 46
5.2.1 可信角色 46
5.2.2 每项任务需要的人数 47
5.2.3 每个角色的识别与鉴别 47
5.2.4 需要职责分割的角色 48
5.3 人员控制 48
5.3.1 资格、经历和无过失的要求 48

5.3.2 背景审查程序 48
5.3.3 培训要求 49
5.3.4 再培训周期和要求 49
5.3.5 工作岗位轮换周期和顺序 50
5.3.6 未授权行为的处罚 50
5.3.7 独立合约人的要求 50
5.3.8 提供给员工的文档 50
5.4 审计日志程序 50
5.4.1 记录事件的类型 50
5.4.2 处理日志的周期 51
5.4.3 审计日志的保存期限 51
5.4.4 审计日志的保护 51
5.4.5 审计日志备份程序 51
5.4.6 审计收集系统 52
5.4.7 对导致事件实体的通告 52
5.4.8 脆弱性评估 52
5.5 记录归档 53
5.5.1 归档记录的类型 53
5.5.2 归档记录的保存期限 53
5.5.3 归档文件的保护 53
5.5.4 归档文件的备份程序 54
5.5.5 记录时间戳要求 54
5.5.6 归档收集系统 54
5.5.7 获得和检验归档信息的程序 54
5.6 电子认证服务机构密钥更替 54
5.7 损害与灾难恢复 55
5.7.1 事故和损害处理程序 55
5.7.2 计算资源、软件和/或数据的损坏 55

5.7.3 实体私钥损害处理程序 55
5.7.4 灾难后的业务连续性能力 56
5.8 电子认证服务机构或注册机构的终止 56
6 认证系统技术安全控制 57
6.1 密钥对的生成和安装 57
6.1.1 密钥对的生成 57
6.1.2 私钥传送给用户 57
6.1.3 公钥传递给证书签发机构 57
6.1.4 电子认证服务机构公钥传送给依赖方 58
6.1.5 密钥长度 58
6.1.6 公钥参数的生成和质量检查 58
6.1.7 密钥使用目的 58
6.2 私钥保护和密码模块工程控制 58
6.2.1 密码模块的标准和控制 58
6.2.2 私钥多人控制（m 选 n） 59
6.2.3 私钥托管 59
6.2.4 私钥备份 59
6.2.5 私钥归档 59
6.2.6 私钥导入、导出密码模块 59
6.2.7 私钥在密码模块中的存储 60
6.2.8 激活私钥的方法 60
6.2.9 解除私钥激活状态的方法 60
6.2.10 销毁私钥的方法 60
6.2.11 密码模块的评估 61
6.3 密钥对管理的其他方法 61
6.3.1 公钥归档 61
6.3.2 证书操作期和密钥对使用期限 61

6.4 激活数据 61
6.4.1 激活数据的产生和安装 61
6.4.2 激活数据的保护 62
6.4.3 激活数据的其他方面 62
6.5 计算机安全控制 62
6.5.1 特别的计算机安全技术要求 62
6.5.2 计算机安全评估 63
6.6 生命周期技术控制 63
6.6.1 系统开发控制 63
6.6.2 安全管理控制 63
6.6.3 生命期的安全控制 63
6.7 网络的安全控制 63
6.8 时间戳 64
7 证书、证书注销列表和在线证书状态协议 65
7.1 证书 65
7.1.1 版本号 65
7.1.2 证书扩展项 65
7.1.3 算法对象标识符 66
7.1.4 名称形式 66
7.1.5 名称限制 67
7.1.6 证书证书策略对象标识符 67
7.1.7 策略限制扩展项的用法 67
7.1.8 策略限定符的语法和语义 67
7.1.9 关键证书策略扩展项的处理规则 67
7.2 证书吊销列表 67
7.2.1 版本号 67

7.2.2 CRL 和 CRL 条目扩展项 68
7.2.3 CRL 下载 68
7.3 在线证书状态协议 68
7.3.1 OCSP 版本号 68
7.3.2 OCSP 扩展项 68
8 认证机构审计和其他评估 69
8.1 评估的频率和情形 69
8.2 评估者的资质 69
8.3 评估者与被评估者之间的关系 69
8.4 评估内容 69
8.5 对问题与不足采取的措施 70
8.6 评估结果的传达与发布 70
9 法律责任和其他业务条款 71
9.1 费用 71
9.1.1 证书签发和更新费用 71
9.1.2 证书查询费用 71
9.1.3 证书吊销或状态信息的查询费用 71
9.1.4 其他服务费用 71
9.1.5 退款策略 72
9.2 财务责任 72
9.2.1 保险范围 72
9.2.2 其他财产 72
9.2.3 对终端实体的保险或担保范围 72
9.3 业务信息保密 72
9.3.1 保密信息范围 72

9.3.2 不属于保密的信息 73
9.3.3 保护保密信息的责任 73
9.4 个人隐私保密 73
9.4.1 隐私保密方案 73
9.4.2 作为隐私处理的信息 74
9.4.3 不被视为隐私的信息 74
9.4.4 保护隐私的责任 74
9.4.5 依法律或行政程序的信息披露 74
9.4.6 其他信息披露形式 74
9.5 知识产权 74
9.6 陈述与担保 75
9.6.1 电子认证服务机构的陈述与担保 75
9.6.2 注册机构的陈述与担保 75
9.6.3 订户的陈述与担保 75
9.6.4 依赖方的陈述与担保 76
9.7 担保免责 76
9.8 有限责任 77
9.9 赔偿 77
9.9.1 赔偿范围 77
9.9.2 赔偿限制 78
9.10 有效期限与终止 78
9.10.1 有效期限 78
9.10.2 终止 78
9.11 修订 78
9.11.1 修订程序 78
9.11.2 通知机制和期限 79
9.11.3 必须修改业务规则的情形 79

9.12 争议处理 79
9.13 管辖法律 79
9.14 一般条款 79
9.14.1 完整协议 79
9.14.2 转让 80
9.14.3 分割性 80
9.14.4 强制执行 80
9.14.5 不可抗力 80

1 概括性描述

吉林省安信电子认证服务有限公司（简称安信 CA）是我国首批获得电子认证服务资质的第三方电子认证服务机构。安信 CA 依据《中华人民共和国电子签名法》、《电子认证服务管理办法》等法律规定以及工业和信息化部、国家密码管理局的要求提供安全可靠的电子认证服务。

《安信 CA 电子认证业务规则（CPS）》（以下简称本 CPS）是安信 CA 如何提供电子认证服的全面描述。其中包括安全管理机制、服务保障机制、程序要求、操作要求等，并对数字证书生命周期的服务要求及责任义务等进行了详细阐述。

1.1 概述

本 CPS 按照中华人民共和国工业和信息化部颁布的《电子认证业务规则规范（试行）》组织文章架构。参考《中华人民共和国电子签名法》、《电子认证服务管理办法》以及电子认证服务机构有关标准规范要求编制规则内容。面向所有参与安信 CA 中心认证服务的个人和实体提出了要求。安信 CA 中心将严格按照本 CPS 实施认证服务，以此满足作为第三方机构的权威性以及提供认证服务的安全性和保密性。

公司简介

吉林省安信电子认证服务有限公司（原名国投安信数字证书认证有限公司）是经国家密码管理委员会办公室批准建设，吉林省信息化领导小组办公室和吉林省国家密码管理委员会办公室联合批准成立，公司成立于 2002 年 7 月，注册资本为 3000 万元人民币，公司总部位于长春高新技术产业开发区。安信 CA 是全国首批获得工业和信息化部颁发的《电子认证服务许可证》资质的电子认证服务机构，具有国家密码管理局颁发的《电子认证服务使用密码许可证》资质和《电子政务电子认证服务机构》资质、具有国家卫计委颁发的卫生系统电子认证服务资质。安信 CA 是吉林省注册企业中唯一具有电子认证服务资质，从事跨行业提供数字证书签发管理与安全认证服务的权威第三方认证机构。

1.2 文档名称与标识

此文档名称为《安信 CA 电子认证业务规则》（下文简称 CPS）。安信 CA 申请的的对象标识符（OID）为 1.2.156.112537，目前安信 CA 为本 CPS 分配的对象标示符为：

1.2.156.112537.1.100

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

电子认证服务机构（CA）是颁发数字证书和证书吊销列表（CRL）的实体。安信 CA 及其下级 CA 机构统称安信 CA。

安信 CA 是安信 CA 信任体系的实体根。安信 CA 自己生成根密钥对，由国家根 CA 签发根证书。根据授权和协议安信 CA 可以签发下一级 CA 的证书。与安信 CA 建立起合同关系的第三方机构，可作为安信 CA 信任体系下的一个下级认证机构，拥有安信 CA 的子 CA 并开展认证业务。

1.3.2 注册机构

注册机构（RA）是 CA 的下属机构，负责对证书订户进行身份标识和鉴别、实施注册过程、发起或传递证书吊销请求，代表电子认证服务机构批准更新证书或更新密钥的申请。

安信 CA 及子 CA 的注册机构必须获得安信 CA 的授权，根据授权从事各类证书服务，并依据授权拓展相应的下级服务机构。并有责任依照《中华人民共和国电子签名法》和本 CPS 妥善保存证书用户的数据，不允许将证书用户的数据透露给与证书业务无关的任何单位或个人，不允许用作商业利益方面的用途。

1.3.3 证书服务受理点

证书服务受理点（下文简称受理点）是 RA 的下属机构，能够执行注册机构的部分职能。主要负责办理和审批数字证书的申请、吊销、查询等证书服务。

安信 CA 及其下属机构的受理点必须获得安信 CA 或其下属机构的授权，其证书服务的申请手续、办理过程和受理要求，必须与本 CPS 以及安信 CA 或其下属机构与之签署的授权协议书相一致。受理点对其提供证书服务的受理过程负有相关的法律责任，包括但不限于本 CPS 和授权协议中所规定的有关内容。

1.3.4 垫付商

垫付商是指能够为其所属或所服务的订户或潜在订户群体承担所有证书服务费用的机构或团体。垫付商根据本 CPS 的规定、安信 CA 公布的其他规定和法律、政策要求，有权取缔起支付费用的全部或部分证书服务，包括但不限于对订户证书的取消。垫付商必须根据与安信 CA 签署的协议，缴纳所有证书费用并保证订户身份的真实性。

1.3.5 订户

证书订户，即最终证书持有者。订户包括持有安信 CA 发放的证书的个人、单位、企业、组织、硬件设备、网站等参与认证服务的各种实体。然而，当最终证书持有者为设备或证书申请属于特殊情况时，订户则指替代最终证书持有者申请及领用证书的人或实体。

安信 CA 中心在订户申请证书之前会建议其参与 PKI 相关的技术培训，该培训将根据订户所使用的证书类别以及应用的不同有所差异。

当安信 CA 把数字证书发放给订户的同时，也把其相应的责任赋给证书订户，订户有责任在发现私钥丢失或有危机私钥安全的事情发生时及时通知发证机构。

1.3.6 依赖方

使用或信任安信 CA 所签发的证书进行交易的证书订户，以及依照本 CPS 在某些应用中信任证书真实性的所有实体被称为安信 CA 的依赖方。依赖方可以是证书订户也可以不是证书订户。

安信 CA 向依赖方保证安信 CA 及其下属分支机构完全按照本 CPS 的说明为订户签发证书，因此证书内所描述的信息真实可靠。

依赖方在信任某个证书前须验证该证书是否有效（如通过 CRL 判断）而且应考虑

到与信任该证书真实身份的附加条件，做出判断后才能继续操作。

1.3.7 其他参与者

安信 CA 电子认证活动的其他参与者包括以上未提及的，属于安信 CA 信任体系的，与电子认证服务相关的其他各类实体。例如安信 CA 选定的 PKI 应用技术服务提供者及第三方身份鉴别机构等。

1.4 证书应用

1.4.1 适合的证书应用

安信 CA 签发的证书，可以应用于以下应用场景：

- 身份认证：保证采用 CA 信任服务的证书持有者身份的真实性；
- 验证信息完整性：保证采用 CA 证书和数字签名时，可以验证信息在传递过程中是否被篡改，发送和接收的信息是否完整一致；
- 验证数字签名：对信任体交易不可抵赖性的依据即数字签名进行验证。必须指出，对于任何电子通信或交易，不可抵赖性应根据法律和争议解决办法裁定。

安信 CA 签发的证书可以在电子商务、电子政务、企业信息化、网上信息传递、网上公共服务等多个领域应用，为建设网络信任环境提供了基础性的信任服务。详细信息请参阅安信 CA 网站 www.anxinca.com。证书订户、依赖方等各类主体可以根据实际需要，自主判断和决定采用相应合适的证书类型，以及了解证书的应用类型、应用范围，选择自己的应用方式。

除非在本 CPS 中特别声明，安信 CA 没有义务承担因任何使用证书而产生的额外的经济赔偿责任。

1.4.2 限制的证书应用

安信 CA 签发的证书禁止在任何违反国家法律、法规或破坏国家安全的情形下使用，否则由此造成的法律后果由订户自己承担。其他限制的证书应用包括：由于证书的使用可能导致人员死亡、伤残的情形；由于证书的使用可能导致环境破坏的情形等。

1.5 策略管理

1.5.1 策略文档管理机构

安信 CA 安全策略委员会是《安信 CA 电子认证业务规则》（CPS）的最高管理机构，负责制定、维护和解释本 CPS。安信 CA 安全策略委员会由管理层、PKI 技术人员和法律顾问组成，安全策略委员会的负责人由安信 CA 的总经理担任。

1.5.2 联系方式

安信 CA 的运营部为本 CPS 的联系人，负责本 CPS 的对外沟通及其他相关事宜，任何有关本 CPS 的问题、建议和疑问都可以与运营部取得联系，具体联系方式如下：

公司地址：长春市前进大街 2266 号

邮　　编：130012

办公电话：0431-85177688

传　　真：0431-85179736

服务热线：0431-85191458

公司网址：www.anxinca.com

E-mail ：技术支持 —— surport@jlca.com.cn

认证委员会 —— chiefAuth@jlca.com.cn

1.5.3 决定 CPS 符合策略的机构

安信 CA 安全策略委员会负责审核批准 CPS，并作为 CPS 实施检查监督的最高决定机构。

1.5.4 CPS 批准程序

安信 CA 的 CPS 由安全策略委员会指定的专人或编写组起草拟定后，提交安全策略委员会审核通过后批准发布。如 CPS 需要修改，由安全策略委员会指定专人或编写组对 CPS 内容进行修订，安全策略委员会对提供的变动建议进行研究分析，并征询法律顾问有关意见后，形成最终决议。安信 CA 将在决议形成后，在网站公布变更后的《安信

CA 电子认证业务规则》正式文档。

1.6 定义和缩写

公钥基础设施（PKI）：即 Public Key Infrastructure，是利用公钥理论和技术建立的提供信息安全服务的基础设施。公钥体制是目前应用最广泛的一种加密体制，在这一体制中，加密密钥与解密密钥各不相同，发送信息的人利用接收者的公钥发送加密信息，接收者再利用自己专有的私钥进行解密。这种方式既保证了信息的机密性，又能保证信息具有不可抵赖性。目前，公钥体制广泛地用于 CA 认证、数字签名和密钥交换等领域。

电子认证服务机构（CA）：即 Certificate Authority，是指颁发用以创建数字签名和公/私密钥对的电子签名认证证书的可信第三方组织或者公司。本规则指安信 CA 认证系统。

注册机构（RA）：Registration Authority，证书的注册机构，负责证书的申请业务。本规则指安信 CA 的注册机构。

电子认证业务规则（CPS）：Certification Practice Statement，是关于电子认证服务机构在全部证书服务生命周期中的业务实践（如签发、管理、吊销、更新证书或密钥等）所遵循的规则的详细描述和声明，提供其它业务、法律和技术方面的细节。本 CPS 是安信 CA 证书相关业务和系统的运行规则。

证书吊销列表（CRL）：Certificate revocation list，认证机构的失效证书列表。证书吊销可能由于证书过期、私钥失窃或者其他原因产生。又称证书废止列表、证书黑名单。

在线证书状态协议（OCSP）：Online Certificate Status Protocal，X.509 公钥基础设施的一部分，在不请求 CRL 的情况下判断证书状态的协议。

电子签名认证证书（证书）：Certificate，是经一个权威的、可信赖的、公正的第三方电子认证服务机构签发的包含公开密钥拥有者信息以及公开密钥的电子文档。认证机构可以签发自己的证书，这种自签名的证书称为该 CA 的根证书并用来签署下级证书。

电子签名人：是指持有电子签名制作数据并以本人身份或者以其所代表的名义实施电子签名的实体。

电子签名依赖方：是指基于对电子签名认证证书或者电子签名的信赖而从事有关活动的实体。

私钥（电子签名制作数据）：是非对称算法产生的两个密钥中的一个，由最终订户唯一持有，用于制作电子签名。

公钥（电子签名验证数据）：是非对称算法产生的两个密钥中的一个，绑定在电子签名认证证书中，通过安信CA在公网上发布，用于验证电子签名信息的有效性。

2 信息发布与信息管理

2.1 认证信息的发布

安信 CA 将通过在线信息库对外公布证书业务的相关信息。安信 CA 的信息库可通过访问安信 CA 的网站 http://www.anxinca.com、目录（LDAP）服务器和 OCSP 获得。安信 CA 的信息库至少包括：所有合法的和未过期的证书信息、证书状态信息、证书吊销列表（CRL）、安信 CA 根证书、用户或依赖方使用证书有关的其它相关信息（使用说明、订户协议等等）、本 CPS 的最新版本和行业的相关法规、安信 CA 关于证书业务的公告和通知等。

2.2 发布时间和频率

安信 CA 签发证书的同时，会在目录服务器（LDAP）中发布该证书的副本。安信 CA 的证书吊销列表（CRL）至少每 24 小时更新一次。在特殊情况下，安信 CA 可立即签发 CRL 或缩短 CRL 的签发频率。

随着安信 CA 业务的发展以及行业规则的不断的完善，安信 CA 会根据公司的实际运营情况更新本 CPS，更新后的 CPS 将会发布在公司的网站上并通过公告通知用户这一变更。

其他电子认证服务相关信息，如用户支持文档、证书应用情况将会不定期更新并对外公布。

2.3 信息库访问控制

数字证书、CRL、CPS 的查询和下载是公开且没有限制的。CPS 经安信 CA 安全策略委员会审核通过后，可以发布在安信 CA 的网站上 http://www.anxinca.com 供访问者自由浏览。

安信 CA 签发的证书和 CRL 公开发布在安信 CA 的目录服务器上，任何订户或非订户均可访问。安信 CA 可以对部分对外公布的信息进行权限控制，以确保只有安信 CA

信任体系的各实体有权阅读这些信息。

安信 CA 的安全访问控制机制能够保证只有经过授权的工作人员才能编写和修改安信 CA 对外公布的任何信息。

3 身份识别与鉴别

3.1 命名

3.1.1 名称类型

安信 CA 按照证书业务办理流程及操作要求，对证书订户进行身份鉴别已确认其真实性，同时对订户证书执行命名过程以区别于其他订户。根据用户证书类型的不同这个命名信息可以是一组能够辨别订户实体的特定数据。

安信 CA 签发的证书的主要识别名称（SubjectName），采用 X.501 Distinguished Name(DN)的方式。每个证书订户按照 X.509 的规定，将对应一个可分辨的名称。

作为可信第三方的认证机构负责确认公钥与已命名实体之间的联系。命名可以由安信 CA 和申请者协商解决，也可以由申请者独立完成。

3.1.2 需要有意义的名称

安信 CA 签发的订户证书可以根据证书名称表达的含义，来确定个人、企业或设备为订户证书的主体。因此要求用户提供真实名称及详细信息，虚假的信息或用户简称在证书中出现所导致的任何后果由用户自己承担。

某些特殊应用环境中，安信 CA 可以按照一定规则为订户指定特殊的名称，并且把该特殊名称与一个真实的实体联系起来。这种特殊的命名必须经过安信 CA 安全策略委员会的批准。

3.1.3 订户的匿名或伪名

一般情况下，订户证书使用真实的名称及详细信息。在特殊情况下，如用户信息涉及党政部门信息的情形，可以按照一定规则为订户指定特殊名称。订户必须在申请证书时声明证书的使用目的和范围，安信 CA 会对其进行严格审核并建立和维护用户真实身份与特殊名称的对应关系。

3.1.4 不同名称形式的规则

安信 CA 签发的证书其甄别名 DN 的内容格式都符合 X.501 Distinguished Name（DN）的命名方式，安信 CA 的订户证书甄别名称中包含下表所列出的组成部分：

识别名称（DN）	说明	内容（示范性）
Country(C)	所在国家名称	C=CN
State(S)	所在省份	ST=吉林，可以不填写。
Locality(L)	城市	L=长春，可以不填写。
Organization(O)	单位名称	O=组织名称。可以不填写或用作其他身份标识。
Organization Unit（OU）	单位或部门名称	OU=部门名称，可以不填写。可以作为应用预留字段，具体定义结合证书应用完成。一张证书可以包含多个OU属性。
Common Name（CN）	证书持有者的一般通用名称	CN=订户名称 必须填写。

订户名称 CN 包含于每张证书的主题中，各类证书命名方式不同，但是所有证书订户名称都需要严格审查。

3.1.5 名称的唯一性

安信 CA 颁发的证书，其甄别名称在安信 CA 信任体系内是唯一的。安信 CA 能够根据该名称关联到证书订户。订户在向安信 CA 申请证书时，安信 CA 将检查该用户的甄别名称在安信 CA 信任体系内是否唯一，当出现相同甄别名称时，以先申请者优先使用。安信 CA 没有权利和义务处理因此产生的纠纷，订户可以向有关主管部门申请解决。安信 CA 将根据主管部门提供的证明文件，吊销发生命名重复的证书并重新签发证书，证书订户承担因此产生的法律责任。

3.1.6 商标的识别、鉴别和角色

安信 CA 尊重任何订户名称中的注册商标权，禁止任何证书申请者对他人知识产权的侵犯。但安信 CA 对证书申请者在其证书申请中提供的标识符是否具有知识产权不做

验证和认可，并且不保证这种权利的唯一性。对于因商标、服务标志等的归属问题造成的纠纷，安信 CA 不负有仲裁或调停等责任。

3.2 初始身份认证

3.2.1 证明拥有私钥的方法

安信 CA 需要验证证书订户拥有私钥的合法性和正确性，可以通过证书请求中所包含的数字签名来证明订户拥有私钥。私钥在用户端生成，证书请求信息中包含私钥的数字签名，安信 CA 用其对应的公钥来验证这个签名。

安信 CA 还可以为订户提供完成证书申请所需要的初始化信息。证书订户在申请证书或证书的某些操作中必须使用这些初始化信息，向安信 CA 确保其是私钥的合法所有者。

安信 CA 要求证书申请人妥善保管自己的私钥，因此，证书申请人被视作其私钥的唯一持有者。

3.2.2 组织机构身份的鉴别

在组织机构身份鉴别的流程中，组织机构应指定和授权证书申请代表，在证书的申请书上签字表示接受证书申请的有关条款，并承担相应的责任。证书申请者须向安信 CA 或其授权的服务机构提供有效的证明材料和信息，如单位营业执照、税务登记证、组织机构代码证等，以及企业联系电话、地址、邮政编码等。安信 CA 对证明材料的要求会根据证书申请者申请的证书类型的不同而有所不同。申请人在证明材料准备充分的前提下可以填写申请表并加盖企业公章以证明该申请的有效性。如果证书订户为服务器，其应向安信 CA 提供 ICP 营运证等服务器的合法身份证明。

申请者有义务保证申请材料的真实性有效，并承担与此相关的法律责任。安信 CA 在进行法律规定的有限审查后，不承担对申请者身份证明文件进行合法性甄别的义务。安信 CA 按照国家相关法律要求保存组织机构的全部申请材料。

3.2.3 个人身份的鉴别

在个人身份的鉴别流程中，证书申请者需要向安信 CA 提供有效的身份证件，如身份证、驾驶执照、军官证、警官证、士兵证等。申请者还要根据证书应用需求提供订户信息并填写申请表。证书申请表中应包含订户本人或授权代表的签字，一些特殊情况下可能需要在申请表中加盖订户所属组织的公章以证明该申请的有效性。

申请者必须承担材料的真实性的责任，安信 CA 在进行法律规定的有限审查后，不承担对申请者身份证明文件（如身份证等）进行合法性甄别的义务。安信 CA 按照国家相关法律要求保存个人的全部申请材料。

3.2.4 没有验证的申请者信息

在申请证书流程中，除安信 CA 要求必须验证的订户信息外，其余信息可不被要求必须验证（如邮件地址）。对于没有验证过的订户信息，安信 CA 不承诺这类信息的真实性 ，并且不承担由于这类信息的不真实、不完整等引起的任何责任和解决纠纷的义务。

安信 CA 向用户提供的测试证书不会验证申请者信息，此类证书 DN 中会存在类似测试或 test 的字样，有效期一般不会超过 3 个月。安信 CA 不承诺该类证书申请者身份的真实性，并且不承担由于该身份的不真实、不完整等引起的任何责任纠纷。

3.2.5 授权确认

当证书订户委托他人代理申请证书时，需出示足够的证明信息以证明代理人有权代表证书订户。安信 CA 需审核申请者的身份和资格，包括必须的身份证明和授权证明，安信 CA 可以通过合法可靠的途径，例如通过可靠第三方获取组织机构的联系方式，通过电话等途径审核申请者的授权信息，一旦审核通过，安信 CA 会将授权信息妥善保存。

3.2.6 互操作准则

涉及到交叉认证或与其他认证服务机构进行互操作的时候，对于安信 CA 之外的电子认证服务机构，安信 CA 可根据与其签署的协议信任其鉴别过的用户信息并予以受理。

对于没有与安信 CA 签署任何协议的认证机构提供的用户信息，安信 CA 有权要求对方按照本 CPS 的要求鉴别用户信息，并根据实际情况决定是否受理此申请。

3.3 密钥更新请求的标识与鉴别

在证书期满前，证书申请者需要获得新证书以保证证书可以持续使用，我们称之为证书更新。通常情况，订户证书更新同时会产生新的密钥对来代替将要期满的密钥对（技术上被定义为“密钥更新”）。订户也可以选择保留原有密钥申请新证书（技术上被定义为“证书更新”）。

通常情况下密钥更新和证书更新都被描述为“证书更新”，原因在于旧的证书已经被新的证书覆盖而不强调是否有新的密钥对产生。

如果与证书相关的信息发生变化，订户可以选择保留原有密钥对或者使用新的密钥对进行证书更新。如果保留原有密钥对，订户需要保证其密钥对的安全性没有受到威胁。

3.3.1 常规密钥更新的标识与鉴别

证书有效期一般为一年（根据应用的具体要求证书的有效期有可能不同），证书有效期满时，订户可以向安信 CA 提交更新请求并用私钥对请求签名。在处理用户常规密钥更新申请前，会鉴别用户公钥、更新申请的用户信息的真实性以及合法性。用户密钥的更新记录将会保存在用户数据库中。

3.3.2 吊销后密钥更新的标识与鉴别

安信 CA 不提供吊销后的密钥更新服务。订户必须重新进行身份鉴别和注册并生成新的密钥对和新的证书。

3.4 吊销请求的标识与鉴别

当遇到证书私钥出现泄漏、被盗等问题时，订户应该向安信 CA 申请吊销其证书。或者，证书用户一旦怀疑证书私钥泄密，必须将情况及时通知安信 CA 或相关的注册机构申请吊销其证书。在证书被吊销前，注册机构要检验证书的吊销申请是由订户提出的，

对吊销申请的鉴别过程包括：

1. 接收申请者的注销申请，验证申请者提供的信息是否与初始注册的信息相符。
2. 如用户不能及时到达现场办理注销，安信 CA 将会通过电话、传真、电子邮件或快递服务鉴别注销请求的个人或组织正是用户本人。

证书吊销的相关材料由安信 CA 或相关的注册机构妥善保存。吊销后的证书将会自动存入安信 CA 的 CRL 列表中，在 CRL 列表下次更新时对外发布。

4 证书生命周期操作要求

证书的生命周期是指证书申请、审核、签发、使用、更新、吊销和挂起等的整个维护周期。本章主要描述了这个过程中各个参与方的操作要求与责任义务。

4.1 证书申请

4.1.1 证书申请实体

在证书申请的过程中，参与整个申请过程的实体主要包括：

- 证书申请者，包含个人、企业单位、事业单位、政府机构、社会团体等各类组织机构。任何合法的组织和个人以及有明确身份归属的其他网络主体均可申请证书，以保证网络作业的安全和可靠。
- 注册机构及受理机构，包括注册机构、受理机构以及相应的系统、管理员、操作员等。
- 电子认证服务机构，本 CPS 中指安信 CA。
- 订户，从安信 CA 接受证书的实体。
- 主管部门，包括《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》等规定的各类主管部门。

4.1.2 注册过程与责任

4.1.2.1 注册流程

离线注册需要遵循以下要求：

1. 证书申请者携带相关证明到安信 CA 的注册机构或下属受理点提交证书申请表，该申请表可从安信 CA 的网站下载或从注册机构及受理点获取；

证书类型	所需材料
个人证书	身份证、学生证、军官证、护照

单位证书	单位的委托证明、单位的注册及登记文件、申请者本人的身份证复印件和安信 CA 需要的其他文件（证书的应用不同，用户所提供的材料可能有所不同）
设备证书	服务器域名所有权的声明、申请人身份证复印件。

2. 注册机构或受理点审核证书申请者和相关身份资料的真实性后，将审核通过的用户信息提交至 CA；
3. CA 中心根据注册机构或受理点的请求签发证书；
4. 注册机构或受理点使用 CA 中心提供的授权信息为用户制作证书；
5. 注册机构或受理点通过安全的方式（如，面对面提交）将证书发给用户。

4.1.2.2 电子认证服务机构的责任

电子认证服务机构必须按照本 CPS 以及国家的相关法律法规（《电子签名法》、《电子认证业务规则规范》等）提供服务，具体责任如下：

1. 安信 CA 按照上述章节的要求发布本 CPS 以及其更新版本；
2. 安信 CA 及其下属机构按照本 CPS 提供电子认证服务；
3. 保证按照国家相关法律法规建立和执行安全机制，保证电子认证服务机构本身的签名私钥得到安全的存放和保护；
4. 保证整套 CA 系统的安全及正常运转，安信 CA 不对由于客观意外或其他不可抗力事件造成的操作失败或延迟承担赔偿责任。这些事件包括罢工或其他劳动纠纷、暴动、国内骚动、供应商故意或无意的行为、不可抗力、战争、火灾、爆炸、地震、洪水或其它灾难；
5. 由于技术的进步与发展，电子认证服务机构会要求证书订户及时更换证书以保证证书的可靠性。

4.1.2.3 注册机构的责任

电子认证服务机构根据本 CPS 以及与注册机构的授权协议对注册机构实施管理。注册机构主要责任如下：

1. 保证按照本 CPS 以及上级电子认证服务机构制定的服务流程、操作规范等提供服务。
2. 按照本 CPS 以及安信 CA 制定系统运维管理规范、安全管理规范等，确保其运营的系统安全可靠，具备相应的安全管理措施。安信 CA 将不断完善这些管理规范。
3. 注册机构有责任按照本 CPS 和安信 CA 的授权协议设立和管理下级服务机构，并对下级机构进行监督管理。

4.1.2.4 受理点的责任

受理点按照安信 CA 和其上级 RA 机构的授权提供证书服务，责任包括：

1. 接受并处理证书服务申请者的证书服务请求，按照本 CPS、安信 CA 和其上级 RA 制定的服务流程、操作规范提供服务。
2. 按照本 CPS 以及安信 CA 制定系统运维管理规范、安全管理规范等，确保其运营的系统安全可靠，具备相应的安全管理措施。安信 CA 将不断完善这些管理规范。
3. 安信 CA 和其上级 RA 根据本 CPS 和授权协议对受理点实施管理，包括服务资质审核、规范执行情况检查。安信 CA 具有对所有证书服务申请者服务请求的最终处理权，并有权对申请者的资料进行复查。
4. 受理点承担对所有证书服务申请者进行身份鉴别与审核的责任，无论证书请求被允许还是拒绝，由于受理点对申请者的资格审核不严导致的损失由受理点承担。

4.1.2.5 垫付商责任

垫付商必须承担其所有垫付的证书费用，并按安信 CA 规定的方式付清。垫付商的垫付行为表明其愿意并且能够承担本 CPS 以及安信 CA 相关协议的规定，对证书服务申请者的身份真实性提供担保的责任。

4.1.2.6 订户的责任

安信 CA 在签发证书之前会建议证书申请者了解证书的作用、办理方式及相关责任义务，因此证书订户应保证：

1. 在其证书申请中提供的信息准确无误以及提供的资料的真实性。
2. 订户应了解并与 CA 中心签署用户协议。通常情况下，证书申请者提交了证书申请证明其已接受了 CA 中心的用户协议（或责任书）。
3. 订户有责任保证私钥的安全。安信 CA 只是告知，但并不要求证书申请者一定遵从安信 CA 提出的安全措施；订户可以选择任何自己认为可以保密的所有措施。安信 CA 声明，安信 CA 并不承担因订户的私钥保存出现问题而带来的所有责任，除非订户能够合法的证明这种问题产生的主要责任在安信 CA。

4.1.2.7 依赖方的责任

依赖方在信任安信 CA 及其子 CA 签发的证书时，必须保证：

1. 依赖方了解证书的使用目的和使用限制。
2. 依赖方在信任安信 CA 及其子 CA 签发的证书前，必须对其进行验证，包括但不仅限于：证书有效期限、证书吊销列表或其他基于安全考虑的条件。由于依赖方没有对证书进行充分验证或其他原因给证书订户或安信 CA 带来的损失，安信 CA 保留采取相应法律行为的权利.
3. 依赖方一旦开始信任安信 CA 及其子 CA 签发的证书就证明其了解并承认本 CPS 的有关条款。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

证书申请者向安信 CA、其下属注册机构或受理点提交证书申请后，根据证书类型检查申请者所提供的证明材料是否真实、完整和有效，同时鉴别证书申请书中的信息是否与用户提供的证明材料一致。如果证书申请者为组织机构或设备，安信 CA 还将检验申请者是否有权代表组织机构或设备申请证书。

安信 CA 及其证书服务机构将遵循本 CPS3.2 章的的身份鉴别要求，严格核对证书申请者提供的各类证件，在确认无误后处理相关业务，并将妥善保存用户提供的各类证明材料和证书申请表。

证书签发完成后，除非被通知该证书发生了本 CPS 所述的安全损害情况，安信 CA 不负责监控和调查证书中信息准确性的责任。

4.2.2 证书申请批准和拒绝

安信 CA、其下属注册机构或受理点在收到证书申请后，将按照本 CPS4.2.1 中的识别与鉴别步骤鉴别订户身份并将决定批准或拒绝证书申请，安信 CA、其下属注册机构或受理点在拒绝用户申请的同时会及时告知（通过电子邮件、电话或传真）用户。对于鉴别失败的原因，安信 CA 有权拒绝解释，法律法规对此有明确要求的除外。

如果由于第三方信息而导致身份鉴别失败，安信 CA 将向申请者提供第三方的联系方式，以便申请者查询。安信 CA 采用合理的方式来通知证书申请者其证书申请失败。安信 CA 可以根据其独立判断，拒绝为某一申请者签发证书，不需要为此做出解释，并且不对因此而导致的任何损失或费用承担责任和义务。除非证书申请者提交了欺骗性的或伪造的信息，在拒绝签发证书后，安信 CA 将归还证书申请者所付的证书购买费用，证书申请者支付的邮递费、材料费等事先发生的费用除外。

被拒绝的证书申请者可再次提出申请。

4.2.3 处理证书申请的时间

安信 CA 或下属注册机构在收到用户的证书申请到鉴别身份并决定是否为用户签发证书的时间会控制在 5 个工作日内。

4.3 证书的签发

4.3.1 证书签发中注册机构和电子认证服务机构的行为

安信 CA 或其下属电子认证服务机构的注册机构在鉴别了申请者身份、确定用户已按规定支付了证书费用并批准其申请后，会将申请信息以安全的方式传送给与其对应的

电子认证服务机构。

电子认证服务机构在收到注册机构的证书申请后为鉴别通过的证书申请签发证书并将该证书发送给注册机构，同时通过目录服务发布证书。证书的发布意味着安信 CA 最终完全正式地批准了证书申请。RA 将签发成功的数字证书在规定时间内发放给用户。

一般情况下，电子认证服务机构的认证系统建设包含了用于签发证书的签发系统和受理用户证书申请的注册系统，因此电子认证服务机构拥有注册机构的职能，可以受理用户申请以及执行用户身份鉴别和证书发放。

如果申请者申请签名证书，申请者需要将签名公钥连同证书申请材料提交给安信 CA 或下属认证服务机构的注册机构，当申请者申请审核通过后，安信 CA 或其下属电子认证服务机构将会为其签发签名证书（签发过程中电子认证服务机构和注册机构的行为同上文），安信 CA 接受符合 PKCS10 标准的证书请求。

4.3.2 电子认证服务机构和注册机构对用户的通告

安信 CA 为订户签发证书后，将会由注册机构或受理点告知用户证书已被签发或被拒绝的消息。注册机构或受理点往往通过电话、电子邮件或在用户提交申请时面对面的通知用户。

安信 CA 没有上门为用户安装证书的义务。如果申请人需要，安信 CA 可以上门安装，但需要收取相应的服务费用。安信 CA 和其授权的证书服务机构提供热线支持服务。热线支持电话和电子信箱由安信 CA 和其授权的证书服务机构公布。

4.4 证书接受

4.4.1 构成接受证书的行为

证书申请者按照安信 CA 的证书申请流程完成证书申请后，安信 CA、注册机构和受理点将证书、或者获得证书的授权数据发送给申请者，证明订户已经接受了证书的行为包括：订户接受了包含证书的介质；订户通过网络将证书下载或安装到本地存储介质；订户接受了获得证书的方式，并且没有提出反对证书或者证书中的内容。

订户接受数字证书后，应妥善保存与其证书对应的私钥。

4.4.2 电子认证服务机构对证书的发布

安信 CA 在签发用户证书的同时会将该证书的副本发布在 LDAP 中。订户、依赖方可以通过目录服务查询自己或他人的证书。

4.4.3 电子认证服务机构对其他实体的通告

安信 CA 在签发用户证书的同时会将该证书的副本发布在 LDAP 中。通常情况下不会对注册机构、受理点、主管部门等的实体进行专门的通告。这些实体可以通过访问目录服务或从信息库中获得相关信息。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户在使用私钥和证书时须遵守以下规则：

1. 订户只能在恰当的应用范围内使用私钥和证书，并且与证书内容一致，所有使用行为必须符合其与安信 CA 签署的订户协议；
2. 证书订户在使用安信 CA 签发的证书时必须遵守安信 CA 证书策略和本 CPS 的要求；
3. 订户在使用证书时，必须妥善保管证书私钥，避免遗失、泄漏、被篡改或盗用。
4. 任何人使用证书时，必须检验证书的有效性，包括该证书是否被吊销、是否在有效期内以及是否是正确的认证机构签发；
5. 安信 CA 签发的各类证书，仅用于表明订户在申请证书时所要标识的身份，以及验证证书私钥的签名。这样，通过签名和签名的验证，保证证书订户的身份真实性、信息的完整性、信息的不可抵赖性等。如果订户将该证书用于其它用途，安信 CA 将不承担任何由此产生的责任和义务。
6. 如果证书中明确了证书的使用范围和用途，那么该证书将在也只被允许在这个范围内使用。任何超出证书适用范围的行为，都将由行为人独立承担责任。安信 CA 对超出适用范围的使用行为，不承担任何的责任和义务。

4.5.2 依赖方公钥和证书的使用

依赖方信任某证书以前必须独立评估证书是否适合用于该应用，即确认证书是否应用于适当的目的。安信 CA 和注册机构不负责评估证书用途的适当性。依赖方不可以超越证书的使用限制或将证书应用于非法目的。

依赖方应检查证书是否在正确的认证机构签发。依赖方应查看证书的信任链，如果这个证书信任链中的任何一个证书过期或被吊销，依赖方不可以信赖该证书。

依赖方必须声明只有同意本 CPS 中规定的条款才可使用或信任数字证书。只有上述所有检查已完成，倘若在这种条件下对证书的信任是合理的，依赖方才有权力信赖证书。

4.6 证书更新

证书更新指在不改变证书中订户信息的情况下，为订户签发一张新证书。订户应当在证书有效期截止前办理证书更新。证书更新分为密钥更新和保留原有密钥的证书更新方式，用户可以自主选择其一。订户承担上述选择的在后续证书使用环节中的任何影响，同时保证密钥的安全。

4.6.1 证书更新的情形

通常在证书终止之前的一个月，安信 CA 会向用户发送到期提醒，用户如需继续使用证书，应在证书有效期截止前向安信 CA 或其下属分支机构提出更新申请。如用户原有注册信息未发生变化则无需提交初始注册时的身份证明资料。证书终止后不可以提出更新申请，但用户仍需使用该证书，则在证书终止后的一个月内提出申请。证书终止超过 1 个月不能进行更新。

4.6.2 请求证书更新的实体

任何证书订户在证书有效期截止前均可向安信 CA 或其下属分支机构提出证书更新申请。

4.6.3 证书更新请求的处理

安信 CA 向用户提供两种证书更新处理方法，在线更新和离线更新。

安信 CA 或其下属电子认证服务机构接收到用户的更新申请后，需要鉴别该证书是否属于该机构签发以及用户是否有权申请证书更新，同时检验该证书的有效性（是否已过期）。

如果订户选择在线更新方式，可以用原有私钥对证书更新请求签名，安信 CA 或其下属电子认证服务机构会对订户的签名和公钥、更新请求中包含的订户信息进行验证。如果订户选择离线更新方式，可以到该证书所对应的注册机构或受理点进行更新处理。

更新申请审核通过后，安信 CA 或其下属电子认证服务机构将会更新订户证书。

4.6.4 颁发新证书时对订户的通告

订户在线办理时会自动获得新证书成功颁发的提示，如为为面对面的处理方式，办理人员将会直接通知颁发成功。

4.6.5 构成接受更新证书的行为

订户按照安信 CA 的证书更新流程完成证书更新申请后，安信 CA 会对证书进行更新，或通知订户自行在线更新，一旦证书订户接受了存有新证书密钥的介质或通过在线完成证书更新后就意味着订户接受了安信 CA 的证书。

4.6.6 电子认证服务机构对更新证书的发布

安信 CA 在签发新的证书的同时会将该证书的副本发布在安信 CA 的 LDAP 服务器中。原有证书信息将会发布在证书吊销列表中，证书吊销列表发布在上述服务器中。

4.6.7 电子认证服务机构对其他实体的通告

安信 CA 在签发用户证书的同时会将该证书的副本发布在 LDAP 中。通常情况下不会对注册机构、受理点、主管部门等的实体进行专门的通告。这些实体可以通过访问目录服务获得相关信息。

4.7 证书密钥更新

证书密钥更新指在不改变证书中订户信息的情况下，为订户签发新证书并产生新的密钥对。

4.7.1 证书密钥更新的情形

通常在证书终止之前的一个月安信 CA 会向用户发送到期提醒，订户如需继续使用，或者当证书密钥对已经或怀疑被泄露、被窃取、被篡改或者其它原因导致的密钥对安全性无法得到保证，订户需要向安信 CA 或其下属分支机构提出更新申请。用户原有注册信息未发生变化则无需提交初始注册时的身份证明资料。证书终止后不可以提出更新申请，但用户仍需使用该证书，则应在证书终止后的一个月内提出申请。证书终止超过 1 个月不能进行更新。

4.7.2 请求证书密钥更新的实体

任何使用证书的订户在证书发生本 CPS4.7.1 中涉及的情形时，均可向安信 CA 或相关服务机构提出证书密钥更新申请。

4.7.3 证书密钥更新请求的处理

安信 CA 向用户提供两种证书更新处理方法，在线更新和离线更新。

安信 CA 或其下属电子认证服务机构接收到用户的更新申请后，需要鉴别该证书是否属于该机构签发以及用户是否有权申请证书更新，并检验该证书的有效性（是否已过期）。

如果订户选择在线更新方式，可以用原有私钥对证书更新请求签名，安信 CA 或其下属电子认证服务机构会对订户的签名和公钥、更新请求中包含的订户信息进行验证。如果订户选择离线更新方式，可以到该证书所对应的注册机构或受理点进行更新处理。

更新申请审核通过后，安信 CA 或其下属电子认证服务机构将会为订户更新证书。

4.7.4 颁发新证书时对订户的通告

订户在线办理时会自动获得新证书成功颁发的提示，如为为面对面的处理方式，办理人员将会直接通知颁发成功。

4.7.5 构成接受密钥更新证书的行为

订户按照安信 CA 的证书更新流程完成证书更新申请后，安信 CA 会对证书进行更新，或通知订户自行在线更新，一旦证书订户接受了存有新证书密钥的证书介质或通过在线完成证书更新后就意味着订户接受了安信 CA 的证书。

4.7.6 电子认证服务机构对密钥更新证书的发布

安信 CA 在签发新的证书的同时会将该证书的副本发布在安信 CA 的 LDAP 服务器中。原有证书信息将会发布在证书吊销列表中，证书吊销列表发布在上述服务器中。

4.7.7 电子认证服务机构对其他实体的通告

安信 CA 在签发用户证书的同时会将该证书的副本发布在 LDAP 上和信息库中。通常情况下不会对注册机构、受理点、主管部门等的实体进行专门的通告。这些实体可以通过访问目录服务或从信息库中获得相关信息。

4.8 证书变更

在证书有效期内，当订户证书中的信息需要改变时，订户应向安信 CA 提出证书变更申请。安信 CA 在对申请者递交的资料进行鉴别和审核后为其签发新的证书。

4.8.1 证书变更的情形

证书变更指改变证书中除订户公钥之外的订户信息而签发新证书的情形。证书变更原因主要为订户名称改变而造成的实体身份改变。

4.8.2 请求证书变更的实体

任何证书订户在证书发生本 CPS4.8.1 中涉及的情形时，均可向安信 CA 或相关的注册机构提出证书更新申请。

4.8.3 证书变更请求的处理

安信 CA 或其下属电子认证服务机构接收到用户的变更申请后，需要鉴别该证书的有效性以及变更后的用户身份证明材料（如变更后的企业营业执照），该过程与初始注册过程相同。

通过审核后，安信 CA 或其下属电子认证服务机构将会为用户作证书变更处理。

订户在办理证书变更时，有责任在证书申请中提供准确、有效的信息以及相应的证明文件。

4.8.4 颁发新证书时对订户的通告

订户在线办理时会自动获得新证书成功颁发的提示，如为为面对面的处理方式，办理人员将会直接通知颁发成功。

4.8.5 构成接受变更证书的行为

订户按照安信 CA 的证书变更处理流程完成证书变更申请后，安信 CA 会进行证书变更，一旦证书订户接受了存有新证书密钥的证书介质或通过在线完成证书变更后就意味着订户接受了安信 CA 的证书。

4.8.6 电子认证服务机构对变更证书的发布

安信 CA 在签发变更后的证书的同时会将该证书的副本发布在安信 CA 的 LDAP 服务器中。此外，原有证书信息将会发布在证书吊销列表中，证书吊销列表发布在上述服务器中。

4.8.7 电子认证服务机构对其他实体的通告

安信 CA 在签发订户证书的同时会将该证书的副本发布在 LDAP 上和信息库中。通常情况下不会对注册机构、受理点、主管部门等的实体进行专门的通告。这些实体可以通过访问目录服务或从信息库中获得相关信息。

4.9 证书吊销和挂起

订户、电子认证服务机构、国家法律部门或者政府公共权力部门等可以要求将证书吊销或者挂起。

4.9.1 证书吊销的情形

证书吊销分为主动吊销和被动吊销。主动吊销是指订户主动申请吊销其数字证书，受理点审核申请后吊销其证书；被动吊销是指电子认证服务机构确认用户违反 CPS 规则内容申请使用证书，或者证书主体消亡，则吊销数字证书。

证书在有效期内，如果出现下列情况，订户必须提出吊销请求：

1. 与证书中的公钥相对应的私钥被泄密、被窃取、被篡改或者其它原因产生对私钥的安全性顾虑。
2. 证书中的订户相关信息发生变更而申请证书变更时。
3. 由于证书不再需要用于原来的用途而要求终止。
4. 证书中的相关内容和申请时提交申请材料不一致。
5. 证书持有者已经不能履行或违反了本 CPS 或其它协议、法规及法律所规定的责任和义务。

证书有效期内，如果出现下列情况（包括但不限于下列情况），安信CA可以直接将证书予以吊销：

1. 由于证书订户未能履行与各参与方之间的协议（如未缴纳费用等）而被这些有权力主张吊销的实体提出。
2. 由于证书的不当使用而违反国家的法律法规及本 CPS 规定的主要和重要义务。
3. 政府公共权力部门或者国家法律部门依照正式合法的程序提出申请。

4. 订户申请证书服务时，提供不真实或者欺骗性材料的。
5. 发现并证实其证书没有根据本 CPS 要求的程序而签发的。
6. 电子认证服务机构因运营问题，导致 CA 内部重要数据或 CA 根密钥失密等原因的。
7. 证书的私钥丢失、被盗、被篡改、被未经授权泄露或被损坏。
8. 由于不可抗力、自然灾害、计算机或通信故障、法律法规的修改、政府行为（包括但不限于出口控制管理部门的限制行为）或其它超出人力合理控制的原因，拖延或阻止了订户责任的执行。

4.9.2 请求证书吊销的实体

以下实体可以申请终端实体申请者证书的吊销：

1. 安信 CA、相关注册机构或用户可根据上述吊销条件申请吊销终端实体证书。
2. 个人证书申请者可以要求吊销他们的个人证书。
3. 对于企业证书，被授权的申请者有权申请吊销组织的证书。
4. 证书垫付商有权吊销其垫付的证书。
5. 国家法律部门、政府主管部门及其他公共权力部门有权根据安全考虑申请吊销证书。

4.9.3 吊销请求的流程

订户主动提出吊销请求的处理流程：

1. 吊销申请人向安信 CA 提交吊销申请表和身份证明材料，同时说明吊销的理由。
2. 安信 CA 或其下属证书服务机构鉴别注销申请者身份的真实性。
3. 证书服务机构审核注销申请后将该申请提交至其所属的电子认证服务机构。
4. 电子认证服务机构在处理注销申请后，会在 24 小时内产生、发布 CRL 列表，并要求下属证书服务机构通知用户证书已被注销。

政府公共权力部门也可以提出吊销证书请求，必须按照规定出具书面证明材料，填写吊销申请表并签字盖章。安信CA在审核材料通过后24小时内吊销证书，在5个工作日内以电话、传真、网站公告或电子邮件等形式之一通知订户。

4.9.4 吊销请求的宽限期

用户有义务在决定注销证书后8小时内向安信CA或证书服务机构提交吊销请求。如果因用户未及时提交吊销申请而导致的任何后果，安信CA不负责承担。

4.9.5 电子认证服务机构处理吊销请求的时限

安信 CA 或相关证书服务机构会在吊销申请提交后的 24 小时之内完成吊销请求资料审核、做出吊销操作并将吊销证书发布到目录服务器中。

4.9.6 依赖方检查证书吊销的要求

依赖方必须检查他们所信任的证书信息。依赖方在信任某个证书前应主动查询安信 CA 最新发布的吊销列表确认证书的状态信息，并验证该证书是否由安信 CA 发布。安信 CA 的吊销列表定期发布且为公开信息，依赖方可以自主查询。

4.9.7 CRL 发布频率

安信 CA 每 24 小时更新 CRL 列表，订户可以访问 CRL 验证证书的当前状态。根据证书使用的相关要求，安信 CA 可以缩短 CRL 的更新周期。

4.9.8 CRL 发布的最大滞后时间

安信 CA 在生成 CRL 的同时更新原有的 CRL。特殊情况下，安信 CA 可以立即签发 CRL。安信 CA 承诺在证书吊销后，最晚也将在吊销行为发生的 24 小时内发布证书吊销列表。

4.9.9 在线状态查询的可用性

安信 CA 及其下属 CA 机构应能够向订户提供 LDAP 服务和 OCSP 在线证书状态查询服务。

4.9.10 在线状态查询要求

如果依赖方没有在最近的 CRL 中检查他所信任的证书的状态，那么依赖方必须以其他方式检查证书信息。如，依赖方可以利用安信 CA 提供 OCSP 在线状态查询服务。

4.9.11 吊销信息的其他发布形式

安信 CA 暂无除 CRL 和 OCSP 以外的证书注销信息查询服务规定。

4.9.12 密钥损害的特别要求

订户如果发现或者怀疑密钥安全被损害时，应该申请对该证书的吊销。

如果安信 CA 发现或有理由认为自身的 CA 密钥已经被损坏，安信 CA 将主动吊销 CA 证书并立即把吊销的证书发布到 CRL。证书吊销后，安信 CA 将通过合理的方式通知各电子认证服务参与方。

4.9.13 证书挂起的情形

当证书仍处于有效期范围内，为暂时停止使用证书但保留订户的证书使用权限，安信 CA 将会考虑挂起证书：

1. 用户提出暂停使用该证书；
2. 用户未能履行与安信 CA 签订的协议中应尽的责任，如用户未按期缴纳证书服务费；
3. 注册机构、受理点、政府主管部门或国家司法机关，向安信 CA 和其授权的认证服务机构提出证书挂起请求并获得批准。

4.9.14 请求证书挂起的实体

证书订户本人或其授权的代理人、证书注册机构、受理点、政府主管部门或国家司法机关有权提出证书挂起的请求。

4.9.15 挂起请求的流程

订户主动提出挂起请求的处理流程：

1. 吊销申请人向安信 CA 提交挂起申请表和身份证明材料，同时说明挂起的理由。
2. 安信 CA 或其下属证书服务机构鉴别挂起申请者身份的真实性。
3. 证书服务机构审核挂起申请后将该申请提交至其所属的电子认证服务机构。
4. 电子认证服务机构在处理挂起申请后，会在 24 小时内产生、发布 CRL 列表，并要求下属证书服务机构通知用户证书已被挂起。

政府公共权力部门也可以提出挂起证书请求，必须按照规定出具书面证明材料，填写申请表并签字盖章。安信 CA 在审核材料通过后 24 小时内挂起证书，在 5 个工作日内以电话、传真、网站公告或电子邮件等形式之一通知订户。

4.9.16 挂起的期限限制

证书挂起的最长期限不得超过证书的有效期，如超过证书有效期而用户没有提出恢复申请，则该证书将会自动失效。

证书挂起期间可以进行吊销操作，吊销操作按照 4.9.3 执行。

4.10 证书状态服务

安信 CA 通过 LDAP、OCSP 提供证书状态查询服务。

4.11 订购结束

在订户证书期满时，安信 CA 会自动终止对用户证书的认证服务。订户还可根据自身的需求申请认证服务的终止，该终止的请求流程与证书吊销流程相同。

4.12 密钥生成、备份与恢复

4.12.1 密钥生成、备份与恢复的策略与行为

用户可以选择自己生成或由安信 CA 及其授权的电子认证服务机构代理生成签名密

钥，安信 CA 及其授权的电子认证服务机构、注册机构和证书服务受理点不提供用户证书签名密钥的备份和恢复服务。

安信 CA 的用户证书加密密钥由吉林省密钥管理中心提供。该机构负责用户加密密钥的生成、管理和备份，以及在出现法律纠纷时提供司法取证的依据。其密钥的生成、备份和恢复策略由该机构制定。

5 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

安信 CA 的 CA 机房位于长春市高新技术产业开发区前进大街 2266 号，该中心建立在安全可靠的物理环境内，中心机房具有防盗、防火、防雷、防辐射的能力。机房内部配备 24 小时场地监控系统、指纹门禁系统、供电系统以及通风系统等。

5.1.2 物理访问

安信 CA 的 CA 系统分为多个物理安全级别保护，在访问高级别前必须通过低级别的要求。安信 CA 的任何敏感操作以及与认证完整生命周期相关所有行为（这些行为包括认证、鉴别、签发）都在其指定的物理安全级别中进行。任何物理访问行为自动记录并有全程监控跟踪。

安信 CA 按照安全级别划分为四个区域。 分别是：公共区域、服务区域、操作区域和安全区域。进入服务区、操作区以及安全区域进行操作时，必须通过指纹验证和权限检验。在部分关键区域还采用 m of n 机制进行访问控制。

5.1.3 电力与空调

安信 CA 为执行连续操作的所有硬件设备配备空调系统、通风系统以及照明系统等，同时还要考虑到应急环境设施。

安信 CA 的电气系统符合电子数据处理设备的防火标准。对支持 CA 系统的服务设施，如配电盘、通讯与电话间、通风以及空调系统都要采取严格的保护措施，并限制人员的随意进入。

5.1.4 水患防治

安信 CA 为 CA 系统布置了漏水检测系统来防止水灾对 CA 系统的损坏。

5.1.5 火灾防护

安信 CA 的安全防护区域采用全淹没灭火，设计成组合分配型，具有同时保护选择灭火的功能。该防火系统具有自动、手动及机械应急操作三种启动方式。

5.1.6 介质储存

安信 CA 将所有保存产品软件和数据、审计、归档文件、备份信息的介质都保存在 CA 中心的离线存贮设备或保险柜中，这些设备都配有适当的物理和逻辑访问控制来减少对授权人员的访问和对存储介质的保护（防止意外的水灾、火灾或电磁干扰）。

5.1.7 废物处理

安信 CA 的敏感文档和材料要在抛弃前粉碎。对用来收集或传输敏感信息的介质要在抛弃前做不可读取处理。加密设备在抛弃前要做物理上的毁坏或依照生产商的指导做归零处理。其他废物的处理要遵照安信 CA 的常规废物处理要求。

5.1.8 异地备份

安信 CA 定期为重要的系统数据、审计数据和其他敏感信息做备份。存储备份信息的介质在机房大厦以外的地点以安全的方式保存。

5.2 程序控制

5.2.1 可信角色

基于认证服务的安全性需求，安信 CA 及 RA 只有可信人员才能在安全性和敏感性高的岗位上工作，安信 CA 的可信角色包括影响到以下操作的所有员工：

1. 证书申请书中信息的鉴别。

2. 证书申请、吊销请求、更新请求或其他注册信息的接收、拒绝、或其他业务的受理。
3. 证书的发放、吊销和访问 CA 系统中受限制的部分。
4. 对申请者信息和请求的处理。

安信 CA 的可信人员包括但不仅限于：

1. 用户信息审核员
2. 证书业务受理员
3. CA 系统管理员
4. CA 安全管理员
5. CA 系统操作员
6. 技术服务人员

对于安信 CA 的下属证书服务机构，其人员配置及服务操作要求应遵照安信 CA 为其制定的服务管理规范执行。

5.2.2 每项任务需要的人数

安信 CA 和 RA 根据各项敏感操作的安全要求规定所需的人员数量，即确保多个员工共同完成一项敏感操作。

CA 密钥、相关加密设备以及机密文件的管理和操作应由多个可信人员共同完成且执行 m of n 机制（m≥2）。CA 及注册系统的日常维护操作应至少由 2 个信任人员完成。

5.2.3 每个角色的识别与鉴别

安信 CA 的可信人员通过认证后，根据工作性质和职位权限的情况，发放系统操作卡、门禁卡、登录密码、操作证书等安全令牌。对于使用安全令牌的员工，安信 CA 系统将独立完整地记录所有人员的操作行为。所有安信 CA 的信任人员必须确保发放的安全令牌只直接属于个人所有；发放的安全令牌不允许共享；安信 CA 的系统和程序通过识别不同的令牌对操作者进行权限控制。

5.2.4 需要职责分割的角色

当某个可信人员被分配到多个信任角色时，其所能执行的操作不能完成完整的一项业务活动，即不能使某个可信人员的操作权限过高。需要职能分割的角色包括：

- 证书申请、更新、吊销等业务处理人员
- 用户资料管理人员
- 认证和注册系统维护人员
- 密钥管理人员
- 秘密分割持有者

5.3 人员控制

5.3.1 资格、经历和无过失的要求

安信 CA 的员工要经过严格的审查才能够被录取，员工需要有 3 个月的考察期，关键岗位的人员考察期为半年，核心岗位的员工的考察期为 1 年。根据考察的结果安排相应的工作或辞退且脱离岗位。安信 CA 将会根据需要对员工进行职责、岗位、技术、政策、法律、安全等方面的培训。

安信 CA 对可信人员执行严格的背景调查，以保证其身份的真实性以及以往经历无诚信方面问题和违法乱纪的不良记录。

5.3.2 背景审查程序

安信 CA 制定了可信人员背景审查程序。背景审查必须符合法律法规的要求，审查内容、方式和从事审查的人员不得有违反法律法规的行为

可信人员的背景审查内容包括：

1. 身份证明，如个人身份证、户口本、护照等
2. 学历、学位以及其他资格证书
3. 个人简历、包括教育、培训经历，工作经历及相关的证明人
4. 无犯罪证明材料

人力资源部门和安全管理人员共同完成背景审查工作，背景审查操作包括：

1．验证先前的工作记录

2．验证身份证明的真实性

3．验证学历、学位以及其他资格证书的真实性

4．通过可靠途径确认教育、培训经历

5．验证无犯罪证明材料并确认无犯罪记录

6．通过适当途径了解是否有工作中的严重不诚实行为

背景审查中导致可信人员候选人或现有可信人员被取消资格的问题主要包括：

1. 伪造真实身份信息
2. 十分不合适或不可信的个人经历
3. 一定的犯罪行为
4. 工作中有严重不诚实行为

5.3.3 培训要求

安信 CA 向其员工和下属分支机构的人员提供与 CA 系统相关的硬件、软件及相关操作程序的岗前和在岗培训。安信 CA 还会定期的修改和加强其培训计划。

安信 CA 的培训计划主要包括：

1. PKI 基础
2. 工作职责
3. 业务培训
4. CPS、CP、安全和操作策略及程序
5. CA 系统相关的硬件和软件维护操作
6. 紧急事件和危险情况的报告和处理
7. 灾难恢复程序

5.3.4 再培训周期和要求

安信 CA 定期向员工提供再培训来确保其职业技能的熟练性。同时，当 CA 系统大环境有所改变时，培训内容也将随之更新。

5.3.5 工作岗位轮换周期和顺序

安信 CA 可以根据具体工作情况安排制定员工的工作轮换周期和顺序。

5.3.6 未授权行为的处罚

当安信 CA 的员工被怀疑或者已经进行了未授权的操作，例如未经授权滥用权力或超出权限使用安信 CA 系统或进行越权操作，安信 CA 会立即终止该员工进入安信 CA 信任体系。未授权行为的处罚包括解除或终止劳动合同、调离工作岗位、罚款、批评教育等，根据情节严重程度，实施包括提交司法机关处理等措施。

5.3.7 独立合约人的要求

在权责明确的前提下，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在职员工一样。担任可信角色的独立合约人和顾问需要通过背景审查程序，而且在进入敏感区域时应由认证机构人员陪同。

5.3.8 提供给员工的文档

安信 CA 的员工可以查看 CA 系统的相关硬件、软件以及操作程序的技术手册，同时员工也可以查看安信 CA 的业务流程介绍和本 CPS。

5.4 审计日志程序

5.4.1 记录事件的类型

安信 CA 以手动或自动记录的方式记录以下事件：

1. CA 密钥整个生命周期的管理事件：
   -密钥的产生、备份、存储、吊销、归档、销毁。
   -密码设备整个生命周期的管理事件。
2. CA 和订户证书整个生命周期的管理事件：
   -证书申请、更新、密钥替换、吊销等。

-成功或不成功的请求处理。

-签发证书和 CRL。

3. 系统操作事件，包括系统启动和关闭，系统权限创建，删除，设置或密码修改。
4. 防火墙和路由器等网络设备记录的安全事件。
5. CA 设施的访问记录，包括授权人员和非授权人员进出 CA 设施的记录。
6. 其他按规定需要记录的内容。

5.4.2 处理日志的周期

安信 CA 每天对来自网络的入侵行为进行检测和分析，巡视场地监控系统产生的各类报警事件并及时采取补救行动。

每周对 CA 系统的操作记录、访问记录、事件记录、系统数据进行审查和处理。

每月对系统产生的各类记录和日志进行审查和分析。

安信 CA 定期对系统管理、数据管理、物理环境安全管理、安全事件管理过程中产生的各类日志收集整理并加以分析和处理，这类审计每年至少执行两次。

5.4.3 审计日志的保存期限

安信 CA 会保留所有审查记录以便出现与审查相关事件时能迅速响应。审查记每个月进行归档保存，审计日志存档期至少 5 年。

5.4.4 审计日志的保护

安信 CA 通过物理或逻辑的访问控制防止电子或手写的审计日志文档被未经授权的浏览、篡改、删除和其他损坏。所有审计日志处于严格的保护状态。

5.4.5 审计日志备份程序

安信 CA 保证所有的审计日志都按照安信 CA 备份标准和程序进行备份。根据审计日志的性质和要求，有实时、每天、每周、每月、每季度等多种备份形式，采用在线和离线的各种备份工具。

5.4.6 审计收集系统

安信 CA 的审计收集系统采用自动及手动的收集方式，主要涉及以下系统：

1. 证书注册系统
2. 证书签发系统
3. 证书发布系统
4. 远程通信系统
5. 应急反应系统
6. 访问控制系统
7. 专网办公系统
8. 客户服务系统
9. 网站、数据库安全保障系统
10. 其他安信 CA 认为有必要审查的系统

在需要的时候，安信 CA 会随时应用相关检查工具来满足各项审查的要求。

5.4.7 对导致事件实体的通告

安信 CA 在进行审查中发现的攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者且保留采取相应对策实施的权力。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施，是否通知攻击者由安信 CA 决定。如果个人、系统或应用程序的行为引发一些事件且被安信 CA 的审计系统记录下来，安信 CA 有权决定是否通知对导致事件的实体。

5.4.8 脆弱性评估

审计过程中的一些事件将被记录为系统的弱点，安信 CA 安全管理要求、技术要求以及相关政策要求对这些弱点进行脆弱性评估。脆弱性评估基于实时的自动记录数据而且根据安全和审计的需求每年对系统进行评估。根据评估结果，随时调整和系统运行密切相关的安全控制措施，以便将系统运作的风险降到最低。

5.5 记录归档

5.5.1 归档记录的类型

安信 CA 会对电子认证服务的相关资料定期归档保存，归档的内容包括：

1. 安信 CA 的系统建设和升级文档 。
2. 证书申请信息、证书服务批准和拒绝的信息、与证书订户的协议、证书等。
3. 系统运行和认证服务的审计数据、认证系统密钥升级和更新信息等。
4. 电子认证服务规则、证书策略、各类服务规范和运作协议等。
5. 证书订户的签名私钥和加密私钥由订户自己保存。有关私钥的保存责任应由订户本身承担。

5.5.2 归档记录的保存期限

CA 证书生命周期内的管理事件的归档保存期限应不少于 CA 证书和密钥的生命周期；订户证书申请、查询、吊销证书的服务记录，至少保存到证书有效期结束后 5 年；CA 和 RA 系统相关操作记录的归档应至少保留 5 年以上。

在不违反法律法规和主管部门规定的前提下，安信 CA 可以自主决定信息的存档期限，并且不需要对此做出说明和解释。

5.5.3 归档文件的保护

安信 CA 根据本 CPS 的存档要求保护存档记录，只有授权的可信人员允许访问存档数据。通过实施适当的物理和逻辑的访问控制防止未授权访问、修改、删除或其他企图。安信 CA 将保护相关的档案免遭恶劣环境的威胁，例如温度、湿度和磁力的破坏。对特定资料，安信 CA 会采取异地备份的方式予以保存。

安信 CA 保存的申请者和订户基本情况资料、身份鉴别资料，除非经过国家法律部、政府主管机构门或其它公共权力部门经过合法的途径予以申请，任意无关的第三方均无法获知。

5.5.4 归档文件的备份程序

安信CA系统管理员每天对系统生成的电子归档记录备份执行服务器本地备份，每周对电子归档记录进行离线备份。书面形式的记录不需要备份，要根据上述各章节的要求汇集在一起并保存在一个安全环境中。

存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有授权的工作人员才能在监督的情况下，对档案进行读取操作。安信CA在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

5.5.5 记录时间戳要求

安信 CA 对本 CPS5.5.1 中所述的存档内容采用手动或自动方式添加时间标识，并且可以根据要求采用时间戳技术。

5.5.6 归档收集系统

安信 CA 的归档收集系统由人工和自动操作两部分组成。

5.5.7 获得和检验归档信息的程序

安信 CA 每年都会验证归档信息的完整性。

5.6 电子认证服务机构密钥更替

安信 CA 的根证书有效期不超过 30 年，任何由其签发的证书，包括子 CA 证书和订户证书，其有效期都短于根证书的有效期，任何由子 CA 签发的订户证书，其有效期都短于子 CA 证书的有效期。

CA 证书期满前要对密钥采取更新。电子认证服务机构的密钥更换程序需要：

1. 电子认证服务机构至少要在下级 CA 到期前停止签发新的下级 CA 证书。
2. 使用新密钥对签发 CA 证书。至此开始使用新的 CA 证书签发下级 CA 证书或用户证书。
3. 在使用前密钥对签发的最后一个证书期满之前， CA 会继续发布前 CA 私钥签

署的 CRL。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

在遭到攻击，发生通信网络资源破坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难时，安信 CA 将按照灾难恢复计划实施修复。安信 CA 的灾难恢复计划中包括系统故障应急方案、电力故障应急方案、网络故障应急方案、安全事件处理办法等。

5.7.2 计算资源、软件和/或数据的损坏

当认证系统的计算资源、软件和/或数据被损坏时，安信 CA 将会立即启动突发事件处理程序。对损坏情况进行调查分析后，安信 CA 将按照相应的恢复方案执行相应的恢复操作，并使认证系统能够正常运行。

5.7.3 实体私钥损害处理程序

当怀疑或发现安信 CA、、子 CA 或订户私钥被损坏，安信 CA 将会组织安全管理员、CA 运行操作人员、技术服务人员和其他安信 CA 的管理代表，对情况分析后将产生一个行动方案，经安信 CA 的安全策略委员会同意后实施此方案。

当 CA 私钥遭到损害时：

1. 立即向电子认证服务管理办公室和其他政府主管部门汇报，通过网站和其他公共媒体对依赖方和订户进行通告。
2. 吊销所有证书，更新并发布 CRL 供订户和依赖方查询。
3. 产生新的根密钥对，签发新的根证书以及下级 CA 证书。
4. 新根证书签发完毕后立即通过目录服务器、信息库以及网站等方式发布。

订户私钥遭到损害时：

1. 如订户发现其私钥遭到损坏时，应立即停止使用私钥并立即通知安信 CA 或下属分支机构注销其证书，安信 CA 按照本 CPS 要求发布证书吊销信息。

2. 当安信 CA 或其下属分支机构发现证书订户的实体私钥受到损害时，安信 CA 将主动吊销订户证书，订户必须立即停止使用私钥。

5.7.4 灾难后的业务连续性能力

安信 CA 建立了异地数据备份以及同城异地离线系统备份。除非物理场地出现了毁灭性的、无法恢复的灾难，安信 CA 有能力在灾难发生后的 48 小时内至少恢复以下操作：证书的签发、证书的撤销、发布证书撤销信息、提供密钥恢复信息。

5.8 电子认证服务机构或注册机构的终止

如果有必要终止安信 CA 及其下属电子认证服务机构或注册机构的运作，安信 CA 的安全策略委员会将在 CA 终止之前通过合理方式通知申请者、依赖方和其它受影响的实体。当安信 CA 需要终止的时候，将会采取终止方案来降低用户和信任组织的损失。这种终止方案可能会包括以下事项：

1. 通知受终止影响的组织，如申请者、依赖方和用户。
2. 安排业务承接的具体工作。
3. 按照本 CPS 的要求在一定时间范围内保存安信 CA 的归档文件和记录。
4. 过渡期内签发 CRL、保持对申请者和用户的支持服务直到 CA 根密钥停止使用。

当 RA 因故终止服务时，认证机构将按照预期签订的相关协议处理有关业务承接事宜和其他事项。

6 认证系统技术安全控制

6.1 密钥对的生成和安装

6.1.1 密钥对的生成

CA 签名密钥生成的安全性通过管理手段和技术手段两方面保证。管理上，需要制定严格的密钥管理流程对其进行控制，至少包括电磁屏蔽机房、人员监督、密钥分割、视频监控等；技术上，密钥的生成、管理、储存、备份和恢复等应遵循国家的相关技术标准，并在通过国家密码主管部门认可的加密设备中进行。

通常订户的密钥对有两对，一对用于签名和验证签名，另一对用于信息的加密和解密，其中用于加密、解密的密钥对由吉林省密钥管理中心（KMC）产生。用于签名和验证的密钥对由订户使用国家密码主管部门批准许可的密码设备（如智能 USB KEY）生成。服务器证书可以由订户利用服务器提供的密钥生成功能生成密钥对，无论何种方式产生的密钥对，相关责任方必须通过技术以及管理手段保证密钥的安全性。订户同样有责任保护密钥的安全性，并承担由此带来的法律责任。

6.1.2 私钥传送给用户

订户签名私钥是由订户自己设备生成，不需要传递。

订户加密私钥由吉林省密钥管理中心（KMC）生成，并通过安全可靠的方式传输到订户的密码设备中。

注册机构或受理点可以代替用户接收其私钥，将私钥妥善下载到证书存储设备后再将该设备以安全的方式发送给用户。

6.1.3 公钥传递给证书签发机构

证书订户以公钥向安信 CA 申请签发证书时，该请求内的公钥，得到订户私钥签名、用户身份验证和信息完整性的保护，并通过安全可靠的方式进行传输。

6.1.4 电子认证服务机构公钥传送给依赖方

依赖方可以从安信 CA 的网站 http://www.anxinca.com 上下载国家 CA 根证书和安信 CA 证书，从而获得安信 CA 的公钥。也可以通过 LDAP 获得用户公钥证书。

6.1.5 密钥长度

安信 CA 支持的密钥算法为 SM2 和 RSA，SM2 算法的密钥长度是 256 位， RSA 算法的密钥长度为 1024 位和 2048 位。

6.1.6 公钥参数的生成和质量检查

安信 CA 的公钥参数使用国家密码主管部门批准的加密设备生成，其质量符合国家密码主管部门的要求。

6.1.7 密钥使用目的

安信 CA 的签名私钥用于签发自身证书、下级 CA 证书、证书注销列表 CRL。安信 CA 的公钥用于验证安信 CA 私钥的签名。

订户的签名密钥对可以用于提供安全服务，例如身份认证、不可抵赖和信息的完整性等。订户的加密密钥对可以用于信息加密和解密。签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

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

安信 CA 采用符合国家密码管理部门要求的硬件密码模块来产生、管理、保存 CA 及下级 CA 密钥，并按照国家密码管理的相关要求执行密码模块生命周期的管理和控制，实现私钥的保护。

订户使用国家密码管理部门批准的密码模块，并有责任妥善保护、保管其密码模块，防止其失窃、丢失、损坏及非授权使用。

6.2.2 私钥多人控制（m 选 n）

安信 CA 采用多人控制实现 CA 私钥的生成、更新、吊销、备份和恢复等操作式。并保证至少其中多数人员同时在场，使用管理员卡、输入保护口令后才能实现上述操作。

6.2.3 私钥托管

安信 CA 不把根认证服务机构、下属子认证服务机构的 CA 私钥托付给任何第三方组织。

订户加密私钥由吉林省密钥管理中心（KMC）生成并负责存储、备份以及在发生法律纠纷时提供司法取证的依据。订户签名私钥由订户自行妥善保管。

6.2.4 私钥备份

为了保证业务持续开展，认证机构必须创建 CA 私钥的备份，以备进行灾难恢复操作，CA 私钥备份以加密的形式保存在硬件密码模块中。

用户加密私钥由吉林省密钥管理中心（KMC）负责备份用户签名私钥不进行备份。

6.2.5 私钥归档

安信 CA 对已过期的 CA 密钥对进行归档，归档的 CA 密钥对保存期至少为 5 年。归档的 CA 密钥不能用于其他用途，在归档期结束后安信 CA 会对密钥进行销毁处理。

用户加密密钥由吉林省密钥管理中心按照国家密钥主管部门的要求归档保存。

6.2.6 私钥导入、导出密码模块

安信 CA 严格的按照私钥保护程序和策略对私钥进行备份，私钥的备份用于密钥恢复和灾难恢复的目的，除此之外的任何导入导出操作将不被允许。CA 私钥备份到另外的硬件密码模块上时，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。

订户私钥无法从硬件导出。必须通过密码验证之后，才可以使用存储在密码模块中的私钥进行加解密操作。

6.2.7 私钥在密码模块中的存储

安信 CA 的私钥在硬件加密模块中以加密的方式存储和使用。

6.2.8 激活私钥的方法

订户私钥存储于证书载体中，只有通过口令验证后才能被激活使用。

服务器证书，如私钥由服务产生和保存，用户必须设置私钥激活口令，当服务启动软件加密模块被加载后，输入口令私钥被激活。

CA 私钥存放在硬件密码模块中，其激活数据已按照秘密分割要求进行分割，并采用 m of n 的机制对其访问加以控制，具有激活私钥权限的管理员使用管理员卡登陆并输入口令后，启动密钥管理程序，进行激活私钥的操作。

6.2.9 解除私钥激活状态的方法

对个人和机构证书，在私钥退出登录状态、移除密码设备、或关闭计算机时，私钥激活状态解除。安信 CA 建议订户在每次私钥使用结束后，将密码设备中从读取设备中移除以解除私钥激活状态。

安信 CA 签发的服务器证书在服务程序关闭、操作系统注销或关闭时解除私钥激活状态。

安信 CA 的 CA 私钥在其密码设备关闭的时候解除激活状态，或者具有激活私钥权限的管理员通过密钥管理程序，进行关闭激活私钥的操作。

6.2.10 销毁私钥的方法

在 CA 私钥不再被使用且超过归档保存期限后，CA 私钥连同其备份、与其相关的操作卡片将被销毁。 销毁过程需要多个可信人员的参与，CA 必须采用合适的方法以确保没有导致密钥重建的密钥残留，例如，采取硬件加密模块的归零、物理销毁加密设备和其他相应的方法确保 CA 私钥以及相关操作卡片被完全的销毁。一旦执行，CA 的密钥销毁动作将被记录。

订户加密私钥由吉林省密钥管理中心负责生成、保存、归档及销毁，具体执行方法

遵循国家相关法律要求。建议订户在私钥生命周期结束后的一段时间内妥善保存私钥的，以便于解开加密信息，订户承担私钥的保护责任。如果订户私钥无需继续保存可以通过私钥删除或密码设备格式化的方法销毁私钥。

6.2.11 密码模块的评估

国家密码管理部门负责对密码模块的评估。安信 CA 使用国家密码主管部门批准和许可的密码产品，接受其颁布的标准、规范、评估结果、评价证书等各类要求。安信 CA 会定期对密码模块的工作状态以及相关安全参数进行安全性检查，以确保 CA 密钥的安全性。

6.3 密钥对管理的其他方法

6.3.1 公钥归档

安信 CA 对于有效期满的根 CA、子 CA 以及订户的公钥进行归档处理，归档的操作过程以及安全管理策略遵守本 CPS。

6.3.2 证书操作期和密钥对使用期限

通常签名证书的密钥对使用期限与证书有效期一致，签名私钥只能在证书有效期内才可以用于签名。对于加密证书，加密私钥的有效期可以长于证书有效期，以保证在证书有效期内加密的信息可以被揭开。

无论是订户证书还是 CA 证书，有效期期满后，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。

6.4 激活数据

6.4.1 激活数据的产生和安装

CA 私钥的激活数据由密码模块产生，按照 m of n 机制被分割到多个 IC 卡中并分配给拥有操作权限的可信人员，其产生和分发会被记录。

订户证书私钥的激活数据是指私钥保护口令，即订户使用私钥时输入的口令，订户可根据安全需求自行修改，口令的设置应符合一定的安全规则。例如至少 6 个字节、在密码中同时具有大小写字符和数字等。

6.4.2 激活数据的保护

CA 私钥的激活数据按照 m of n 机制被分割，并由多个可信人员分别保管，这些拥有私钥激活数据的可信人员必须遵守安信 CA 的职责分割以及安全操作等要求。

订户私钥激活数据由订户自行妥善保管，不可被他人获得。为了保证私钥使用安全，应定期修改私钥的激活数据。如果发生激活数据丢失而造成私钥被盗用所进行的操作，将视同订户本人使用私钥进行的操作。

6.4.3 激活数据的其他方面

考虑到安全因素，对于订户激活数据的生命周期，规定如下：

1、订户用于申请、下载证书的口令，下载成功后失效。

2、用于保护私钥或者 IC 卡、USB Key 的口令，建议订户根据业务应用的需要随时予以变更。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

安信 CA 保证含有 CA 软件和数据文件的系统属于值得信赖的系统且不会被未经授权访问。安信 CA 采取了严格的访问控制来限制人员对系统服务器的访问，只有有效的原因才可以访问，普通的用户没有系统服务器的访问权限。安信 CA 执行双因素验证机制，拥有系统访问权限的可信人员必须同时采用用户名口令以及数字证书的登录方式。

安信 CA 的 CA 系统在网络逻辑上要与其他组件分开。这一分开能够阻止除认证全部流程以外的网络访问。CA 使用防火墙保护网络以防止内部或外部的入侵，并且限制访问系统的网络行为的来源。

6.5.2 计算机安全评估

安信 CA 的 CA 系统及运营环境通过了国家密码管理部门的安全测评和评审，并获得了相关资质。安信 CA 每年或不定期的接受国家密码管理部门和上级主管部门的检查和评估，并根据检查结果对系统进行相关的改造和完善工作。

6.6 生命周期技术控制

6.6.1 系统开发控制

安信 CA 系统的开发由满足国家相关安全和密码标准的可靠软件开发商完成，同时与该开发商建立约定以保证系统的权威性与可靠性。

6.6.2 安全管理控制

安信 CA 制定安全管理策略、制度以及程序对运营管理的各个方面实施有效的控制。

6.6.3 生命期的安全控制

安信 CA 根据安全需求的发展及行业发展动态，在不影响正常提供服务的前提下，将积极采用先进的技术和设备，及时进行技术更新以保证 CA 系统生命周期的安全性。安信 CA 对系统的任何修改和升级会记录在案并予以控制。

6.7 网络的安全控制

安信 CA 在采用多层防火墙结构，部署了入侵检测、漏洞检测、 病毒防范系统，并及时对上述安全措施进行版本更新，这些产品可以从多方面对网络系统进行监测和分析，以降低来自网络的风险。

只有经过授权的安信 CA 可信人员才能够进入签发系统、注册系统、目录服务器、证书发布系统等设备或系统。

安信 CA 只开放与申请证书、查询证书等相关的操作功能，供用户通过网络进行操作。

6.8 时间戳

安信 CA 认证系统产生的各种日志、操作记录都具有时间标识，但尚未采用时间戳技术保留上述记录的时间信息。

7 证书、证书注销列表和在线证书状态协议

7.1 证书

安信 CA 签发的证书符合 ITU-T X.509V3：信息技术-开放系统互联-目录：认证框架标准；以及 RFC5280：Internet X.509 公钥基础设施证书和 CRL 结构。

7.1.1 版本号

安信 CA 签发符合 X.509 V3 标准的数字证书，证书的版本信息存放在证书版本属性栏中。

7.1.2 证书扩展项

安信 CA 使用了标准扩展项和自定义扩展项，内容包括：

↘ 密钥用法（**Key Usage**）

此字段指示已认证的公钥有何种用途，安信 CA 签发的订户证书根据证书类别可能包含以下密钥用法：

a) digitalSignature: 用于验证数字签名。

b) nonRepudiation: 用于提供抗抵赖服务的数字签名，这种服务防止签名实体假拒绝某种动作中的证书。

c) keyEncipherment: 加密密钥或其他安全信息，例如用于密钥传输。

d) dataEncipherment: 加密用户数据，但不包括密钥或其他安全信息。

e) keyAgreement: 用作公钥协商密钥。

f) keyCertSing: 验证证书的 CA 签名。

g) CRLSign: 验证 CRL 的 CA 签名。

i) decipherOnly: 此项与 keyAgreement 一起使用时，公钥协商密钥仅用于加密数据。

↘ 基本限制（**BasicConstraints**）

用于鉴别证书持有者身份，如最终用户等。

↘ 增强型密钥用法（**Extended Key Usage**）

对于不同的证书，其增强型密钥用法可能包含以下几种：

a) 服务器验证（1.3.6.1.5.5.7.3.1）

b) 客户端验证（1.3.6.1.5.5.7.3.2）

c) 代码签名（1.3.6.1.5.5.7.3.3）

d) 安全电子邮件（1.3.6.1.5.5.7.3.4）

e) 时间戳（1.3.6.1.5.5.7.3.8）

f) 智能卡登录（1.3.6.1.4.1.311.20.2.2）

↘ CRL 分布点（CRL Distrabution Point）

CRL 分布点包含可以获取 CRL 的 URL，用于验证证书状态。

↘ 自定义扩展

根据证书应用的不同，安信 CA 签发的订户证书中可能含有以下自定义扩展项：

1.2.86.11.7.1 个人身份标识号

1.2.86.11.7.2 个人社会保险号

1.2.86.11.7.3 组织机构代码号

1.2.86.11.7.4 工商注册号

1.2.86.11.7.5 企业国税号/地税号

7.1.3 算法对象标识符

安信 CA 采用 sha1RSA 签名算法和 sm3SM2 算法，算法的标识符如下：

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

Sm3WithSM2 Encryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) cn(156) ccstc(10179) 1.501}。

7.1.4 名称形式

安信 CA 签发的证书的名称形式和内容符合 X.501 甄别名格式。证书的主体名称由：国家名（C）、省份（S）、城市（L）、组织（O）、部门（OU）、用户名称（CN）组成。

7.1.5 名称限制

订户证书的命名一定要有意义，可以通过名称确定证书主题中的个人、单位或者设备的身份，订户证书不应使用匿名或假名。在某些具有特殊要求的应用中，可以按照一定的规则为用户指定特殊名称，并且能够把该类特殊名称与一个确定的实体唯一的联系起来。

7.1.6 证书证书策略对象标识符

安信 CA 按照 X.509 标准签发的证书，其证书策略对象标识符，存放在证书内证书策略的相关栏目。

7.1.7 策略限制扩展项的用法

无规定。

7.1.8 策略限定符的语法和语义

无规定。

7.1.9 关键证书策略扩展项的处理规则

无规定。

7.2 证书吊销列表

安信 CA 定期签发 CRL 共订户和依赖方查询。

7.2.1 版本号

安信 CA 签发符合 X.509 V2 标准的 CRL。

7.2.2 CRL 和 CRL 条目扩展项

无规定。

7.2.3 CRL 下载

可以通过证书中签发的 CRL 扩展项标明的 URL 下载 CRL。

7.3 在线证书状态协议

安信 CA 提供 OCSP 服务，证书订户和依赖方均可通过此项服务及时查询证书状态信息。

7.3.1 OCSP 版本号

OCSP V1。

7.3.2 OCSP 扩展项

无规定。

8 认证机构审计和其他评估

8.1 评估的频率和情形

安信 CA 每年一次接受上级主管部门的评估和检查。

安信 CA 对内部以及下级认证服务机构和注册机构的审计工作为每年一次。

安信 CA 可以根据业务需求委托第三方机构进行审计和评估。

8.2 评估者的资质

安信 CA 接受包括国家工信部、国家及省级密码管理部门、其他具有行业监管资质的主管部门，以及这些部门认可的专家组和专业机构的评估、审核和检查。

安信 CA 的内部审计由具有相关专业技术和业务能力的安信 CA 可信人员执行。

安信 CA 委托的第三方审计机构必须是具备相关主管部门批准的资质的专业机构。

8.3 评估者与被评估者之间的关系

主管部门以及外部评估组织和机构与安信 CA 之间是相互独立的关系，评估者应以独立、公正、客观的态度对被评估者进行评估。

安信 CA 对中心内部及下属分支机构的审计工作由安信 CA 管理层指定内部人员执行。评估者与被评估者之间相互独立且没有任何利害关系足以影响评估的客观性，评估者应以独立、公正、客观的态度对被评估者进行评估。

8.4 评估内容

主管部门基于国家法律、规范制定评估内容，安信 CA 接受主管部门的任何形式及内容的评估和审计。

内部审计内容包括：本 CPS 的合规性以及执行情况；密钥及证书生命周期的管理是否符合安信 CA 的业务标准；物理环境安全、网络安全、系统运维管理、人员管理、资产管理、业务连续性管理等安全策略规范的执行情况。

8.5 对问题与不足采取的措施

对于主管部门在评估过程中提出的任何不足和整改要求，安信 CA 将制定和实施整改方案，整改过程接受主管部门的审查和评估。

对于内部评估过程中提出的不足，由安信 CA 的安全策略委员会负责收集并组织相关人员协商制定整改方案，整改过程接受安全策略委员会的监督和审查。

8.6 评估结果的传达与发布

对于主管部门的评估结果，安信 CA 按照主管部门的相关要求予以公布。内部审计结果可根据安全策略委员会的要求向安信 CA 全体工作人员公布或对部分人员公布。

9 法律责任和其他业务条款

9.1 费用

安信 CA 在公司网站上公布收费标准。订户有责任按照收费标准向安信 CA 支付费用。如安信 CA 与订户或垫付商签署的协议中规定的价格与网站公布的价格不符，以协议价格为准。

9.1.1 证书签发和更新费用

安信 CA 的证书签发和更新费用标准公布在安信 CA 网站上（www.anxinca.com）供各方查询和参考。如安信 CA 与订户或垫付商签署的协议中规定的价格与网站公布的价格不符，以协议价格为准。

9.1.2 证书查询费用

安信 CA 不向证书用户收取证书查询费用。除非用户提出的特殊需求，需要安信 CA 提供额外的服务，安信 CA 将与用户协商收取相应的费用。

9.1.3 证书吊销或状态信息的查询费用

目前，安信 CA 不收取证书吊销费用和 CRL 查询费用。

对于实时在线证书状态查询（OCSP）服务费用，在安信 CA 与相关方签订的协议中另行约定。安信 CA 保留对占用大量资源的证书吊销和状态信息查询操作进行收费的权利。

9.1.4 其他服务费用

对于上文未提到服务，服务费用在安信 CA 与相关方签署的协议中约定。

9.1.5 退款策略

安信 CA 以服务费的形式收取证书费用，安信 CA 保证在证书有效期内为订户提供符合本 CPS 的服务或其与安信 CA 约定的其他服务。证书一经订户接受，安信 CA 将不退还服务费。

9.2 财务责任

9.2.1 保险范围

安信 CA 向订户提供证书使用保障。如果由于安信 CA 造成用户使用证书过程中遭受损失，安信 CA 将按照本 CPS9.9 的所述内容提供赔偿。

9.2.2 其他财产

无规定。

9.2.3 对终端实体的保险或担保范围

安信 CA 目前没有为订户提供第三方保险服务。

9.3 业务信息保密

9.3.1 保密信息范围

安信 CA 的 CA 私钥以及订户私钥属于保密信息范围。安信 CA 将妥善保管 CA 及子 CA 的私钥且不对外公布。订户加密私钥由吉林省密钥管理中心生成并妥善保管。已发放给订户的私钥由订户自行保管不能公布给他人。订户擅自泄露私钥引发的任何后果自行承担。

安信 CA 与其授权的发证机构、证书订户，以及安信 CA 授权的发证机构与订户之间的协议、往来函和商务协定等，除非法律明确规定，一般不能在未经另一方许可擅自公开。

9.3.2 不属于保密的信息

以下为安信 CA 可对外公开的非机密信息类型：

1. 与证书有关的申请流程、所需的手续、操作指南等文档中公布的信息是可以公开的。
2. 证书（含证书中的订户信息）和吊销列表属于公开信息，安信 CA 在目录服务器中公布这些信息。
3. 安信 CA 的证书策略和本 CPS 属于公开信息。
4. 在国家法律部门的要求下可以向其公布相关保密信息，这种行为不视为违反保密要求。

9.3.3 保护保密信息的责任

安信 CA、证书订户、关联实体以及认证业务相关的参与方等，都有义务按照本 CPS 的规定，承担相应的保护保密信息的责任。

安信 CA 有责任通过安全管理策略、流程和技术手段来保护自身的商业秘密和订户信息。

当保密信息所有者因某种原因向安信 CA 提出公布其保密信息的书面请求及授权时，安信 CA 可以按照其要求公布这类信息。安信 CA 不承担因公布此类消息引发的任何赔偿责任，由保密信息所有者承担全部赔偿责任。

安信 CA 在国家法律部门的要求下可以向其公布相关保密信息，这种行为不视为违反保密责任。

9.4 个人隐私保密

9.4.1 隐私保密方案

安信 CA 尊重所有订户和他们的隐私，并按照隐私保护的相关法律对隐私执行相应的保护。

9.4.2 作为隐私处理的信息

安信 CA 在管理和使用订户提供的信息时，除了证书中已经包括的信息外，该用户的基本信息和身份认证资料将被作为隐私处理，非经用户同意或者法律法规及权力部门的合法要求，不会任意对外公开。

9.4.3 不被视为隐私的信息

不被视为隐私的信息包括证书中的信息、证书本身以及该证书的状态信息。

9.4.4 保护隐私的责任

安信 CA、证书订户、关联实体以及认证业务相关的参与方等，都有义务按照本 CPS 的规定，承担相应的隐私保护责任。

安信 CA 有责任通过安全管理策略、流程和技术手段来保护订户隐私信息。

安信 CA 在国家法律部门的要求下，可向其公布相关隐私信息，这种行为不视为违反保密责任。

9.4.5 依法律或行政程序的信息披露

安信 CA 在国家法律部门的要求下可以向其公布相关方的隐私信息，这种行为不视为违反隐私保护责任。

9.4.6 其他信息披露形式

当证书订户因某种原因向安信 CA 提出公布其隐私信息的书面请求及授权时，安信 CA 可以按照其要求公布这类信息。安信 CA 拒绝除订户本人的第三方的信息披露要求。

除国家法律机关或政府的合法请求，以及信息所有人的书面授权，或者安信 CA 的合法用途外，安信 CA 不提供任何其他的隐私信息披露。

9.5 知识产权

安信 CA 享有并保留安信 CA 提供的全部系统和软件的一切知识产权，包括所有权、

名称权和利益分享权等。安信 CA 有权决定关联机构采用的软件系统，选择的形式、方法、时间、过程和模型，以保证系统的兼容和互通。

安信 CA 签发的证书和提供的文档的一切版权、商标和其他知识产权均属于安信 CA 的产权，这些知识产权包括所有相关的文件和使用手册。授权发证机构在征得安信 CA 的同意后，可以使用相关的文件和手册。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

安信 CA 及其分支机构按照本 CPS 的要求提供认证服务。安信 CA 保证其私钥得到安全的存放和保护，所有的认证业务相关的活动都符合法律法规和主管部门的规定。

9.6.2 注册机构的陈述与担保

安信 CA 的注册机构和受理点在参与电子认证服务过程中的承诺如下：

1. 严格执行安信 CA 制定的证书管理和发放策略，服从安信 CA 整体的管理和规范要求；提供给证书订户的注册过程完全符合本 CPS 的要求。
2. 安信 CA 签发证书时，不会因为注册机构、受理点的失误而导致证书中的信息与证书申请人的信息不一致。
3. 及时响应并向安信 CA 提交订户证书申请、吊销、更新等服务请求。

9.6.3 订户的陈述与担保

安信 CA 的证书订户应该保证：

1. 就有关证书信息及其他认证信息向安信 CA 及其下属认证服务机构或注册机构作真实上报。
2. 订户提供的信息，尤其是包含在证书中需要鉴别和验证的信息是真实的、准确的。
3. 使用其私钥进行签名操作时，订户必须保证此项操作是订户本人完成，并且采取适当措施验证证书是否已过期或被吊销。以合法的目的授权使用证书，遵守

证书策略和本 CPS。

4. 订户对自己的私钥进行了有效保护，其他人无法使用订户的私钥。
5. 一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘、泄密以及其他情况，订户应立刻通知安信 CA 和注册机构，及时申请采取证书吊销等业务处理。

9.6.4 依赖方的陈述与担保

依赖方在做出任何信任行为以前必须独立评估证书是否适用于适当的目的。安信 CA 及其下属认证服务机构或注册机构不负责评估证书用途的适当性。依赖方不可以超越证书的使用限制或将证书应用于非法目的。

依赖方在信任某个证书前应检查证书的状态及其证书链。如果这个证书链中的任何一个证书被吊销，依赖方不可以信赖证书链中订户证书或其他证书。

证书依赖方对证书的信赖行为表明他们已阅读并理解本 CPS 或相关协议的所有条款，并同意承担证书依赖方有关证书使用的相关责任和义务。

9.7 担保免责

安信 CA 不对由于客观意外或其他不可抗力事件造成的操作失败或者延迟承担任何赔偿责任。这些事件包括劳动纠纷、交易一方故意或无意的行为、罢工、暴动、骚动、战争、火灾、爆炸、地震、或其他大灾难等。

安信 CA 在订户的“数字证书申请及使用责任书”的免责条款规定：安信 CA 的数字证书只能用于网络上标识身份、加密数据、电子签名、保证网络安全通讯等符合法律要求的用途，若订户将证书用于其他用途，安信 CA 不承担任何责任。如果由于安信 CA 的设备或者网络故障而导致签发的数字证书错误、延尽、中断或者无法签发，安信 CA 将重新签发证书，但不承担任何赔偿责任。

安信 CA 在签发证书之前，证书申请者已经同意遵守“数字证书申请及使用责任书”中各项规定。责任书中明确规定安信 CA 不承担任何形式的担保和义务。如果证书申请者故意或无意地提供虚假信息或未及时更新用户资料，导致安信 CA 签发证书错误，造成订户及他人损失时，由用户承担一切责任。

9.8 有限责任

由于安信 CA 自身原因，如没有严格按照业务流程进行鉴别和审核导致证书的错误签发、假冒，或管理上的疏忽造成订户、依赖方的损失，安信 CA 将承担有限赔偿责任，赔偿限制遵循本 CPS9.9。

9.9 赔偿

9.9.1 赔偿范围

安信 CA 的赔偿范围包括：

1. 由于安信 CA 的原因，用户证书的签发过程没有按照本 CPS 的要求，导致用户证书签发有误。
2. 由于安信 CA 操作人员的疏忽，导致用户证书内信息有误并造成用户损失。
3. 安信 CA 的 CA 私钥丢失或泄密。

注册机构的赔偿范围包括：

1. 由于注册机构人员的疏忽导致用户隐私信息泄露，给用户造成损失，注册机构有责任赔偿用户。
2. 注册机构没有按照业务操作流程为用户申请证书而给用户带来损失的，注册机构有责任赔偿用户。
3. 注册机构没有按照本CPS中的时间要求处理用户的证书业务给用户带来的损失，注册机构有责任赔偿用户。

订户的赔偿范围包括：

1. 订户在申请证书时提供虚假信息，给安信 CA 或证书依赖方造成的任何损失由订户赔偿。
2. 订户没有妥善保管订户私钥，导致私钥泄漏、遗失，而未及时告知安信 CA 吊销或挂起的，造成安信 CA 或第三方遭受损失的，订户应承担赔偿责任。
3. 订户证书中的信息侵犯了第三方的知识产权，所带来的后果由订户承担。

证书依赖方赔偿范围包括：

1. 在没有检查证书状态的前提下信任了某个证书。

2. 在不合理的条件下信任了某个证书。

9.9.2 赔偿限制

安信 CA 及其授权的发证机构，对所有当事人（包括但不限于订户、申请者、接受者或信赖方）的合计赔偿额度，其最高限度不超过如下金额：

（1）个人证书每张最高为 800 元；

（2）单位证书每张最高为 4000 元；

（3）设备证书每张最高为 12000 元。

本条款所称的“合计赔偿额度”，适用于所有当事人因信任安信 CA 所签发证书而造成一切形式的损害，以每张证书为计量单位，不考虑证书所造成的损害事件的数量。安信 CA 及订户或其它当事人所承担的赔偿责任，其具体额度由国家相关法律法规进行规定，或由各方协商确定。协商不成可提交安信 CA 所在地的司法机关进行解决。

9.10 有效期限与终止

9.10.1 有效期限

除安信 CA 特别声明本 CPS 提前终止，本 CPS 自对外发布之日起至新版本的正式发布前均有效，一旦新的版本发布则旧的版本自动失效。

9.10.2 终止

当新版本 CPS 正式发布时生效，旧版本 CPS 将自动终止。

9.11 修订

9.11.1 修订程序

对本 CPS 文档的修改由 CA 的安全策略委员会负责。对本 CPS 的修改要以修订版或更新版的文档形式出现。修改后的版本或更新版本将发布在安信 CA 对外发布的网站中，并将更改的消息发布在公告栏中。

9.11.2 通知机制和期限

安信 CA 在网站 www.anxinca.com 中公布修订结果，安信 CA 将视修订内容在合理的时间范围内通知相关方，新版本的 CPS 自修订之日起生效。

9.11.3 必须修改业务规则的情形

安信 CA 会视以下情况，按照相关规定更改本 CPS 的内容：

1. 当本 CPS 中描述的某些规则、流程和相关技术等内容已经不能够满足电子认证服务机构的业务要求时。
2. 当某些认证服务行业相关标准出台或更新时。
3. 当认证系统和有关管理规范发生重大升级或改变时。。

9.12 争议处理

当安信 CA 与其他各方因电子认证服务产生争议时，如双方未达成一致，应提交双方信任的权威机构进行鉴定、评估和协调。若仍为解决，可提交仲裁机构或司法部门进行裁决。

9.13 管辖法律

安信 CA 提供的电子认证服务遵守《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》等国家法律法规的规定。

9.14 一般条款

9.14.1 完整协议

安信 CA 的 CP、CPS、证书订户协议以及依赖方协议及其补充协议构成 PKI 参与者之间的完整协议。

9.14.2 转让

安信 CA 与电子认证服务业务相关的各实体之间的责任义务不能通过任何形式转让给其他方。

9.14.3 分割性

CP、CPS、订户协议和依赖方协议的任何条款在某种条件或范围内发生无效或无法执行，其余的条款仍然有效。

9.14.4 强制执行

在相应法规允许的范围内，安信 CA 与认证服务相关的各实体之间的协议可以包含一个强制执行条款来保护安信 CA 的利益。

9.14.5 不可抗力

当安信 CA 遭遇受某些超出控制力的事件发生时，将会免除或部分免除其与参与电子认证服务的相关实体之间的合同的执行责任。通常，免除执行的时间与事件所造成的延迟时间相当。构成不可抗力的事件包括：战争、恐怖袭击、罢工、自然灾害、供应商或卖方执行失败、互联网或其他基础设施的瘫痪等。