吉林省安信电子认证服务有限公司
电子认证业务规则
（CPS）

版本 V4.3



吉林省安信电子认证服务有限公司

2023 年 3 月

版本控制

版本	生效日期	发布者
V3.0	**2017.3.24**	**安信CA安全策略委员会**
V4.0	**2020.04.24**	**安信CA安全策略委员会**
V4.1	**2020.08.07**	**安信CA安全策略委员会**
V4.2	**2021.06.10**	**安信CA安全策略委员会**
V4.3	**2023.03.05**	**安信CA安全策略委员会**
V3.0变更记录		
变更位置	变更描述	
公司名称	公司名称由安信数字证书认证有限公司变更为吉林省安信电子认证服务有限公司	
V4.0变更记录		
变更位置	变更描述	
第1章	增加了场景型证书和云应用证书的相关描述	
第2章	对信息发布的相关内容进行了修改	
V4.1变更记录		
第三章	根据实际业务流程，补充修改了鉴别流程的相关内容	
其他部分	根据上述修改内容以及现有业务情况进行了相应的修改	
V4.2变更记录		
第二章	信息发布加入LDAP端口	
第五章	修改背景审查程序	
V4.3变更记录		
第三章	**3.2.4 增加域名和IP鉴定内容**	
第七章	增加7.4 根证书认证体系内容	

目 录

1 概括性描述 12

1.1 安信 CA 12

1.2 CPS 概述 12

1.3 标识 12

1.4 电子认证活动参与者 13

1.4.1 电子认证服务机构 13

1.4.2 注册机构 13

1.4.3 订户 13

1.4.4 依赖方 13

1.5 证书应用 13

1.5.1 适合的证书应用 13

1.5.2 限制的证书应用 14

1.6 策略管理 15

1.6.1 策略文档管理机构 15

1.6.2 联系方式 15

1.6.3 决定 CPS 符合策略的机构 15

1.6.4 CPS 批准程序 15

1.7 定义和缩写 16

2 信息发布与信息管理 17

2.1 信息的发布 17

2.2 发布时间和频率 17

2.3 信息访问控制 17

3 身份识别与鉴别 18

3.1 命名 18
3.1.1 名称类型 18
3.1.2 名称包含的内容 18
3.1.3 订户的匿名或伪名 18
3.1.4 名称的唯一性 18
3.1.5 商标的承认、鉴别和角色 19
3.2 初始身份认证 19
3.2.1 证明拥有私钥的方法 19
3.2.2 组织机构身份的鉴别 19
3.2.3 个人身份的鉴别 20
3.2.4 其他类型证书订户身份鉴别 20
3.2.5 没有验证的申请者信息 21
3.2.6 授权确认 21
3.2.7 互操作准则 21
3.3 密钥更新请求的标识与鉴别 21
3.3.1 常规密钥更新的标识与鉴别 21
3.3.2 吊销后密钥更新的标识与鉴别 21
3.4 注销请求的标识与鉴别 22
4 证书生命周期操作要求 22
4.1 证书申请 22
4.1.1 证书申请实体 22
4.1.2 注册过程与责任 22
4.2 证书申请处理 23
4.2.1 执行识别与鉴别功能 23
4.2.2 证书申请批准和拒绝 24
4.2.3 处理证书申请的时间 24
4.3 证书的签发 24

4.3.1 证书签发中注册机构和电子认证服务机构的行为 24
4.3.2 电子认证服务机构和注册机构对订户的通告 24
4.4 证书接受 25
4.4.1 构成接受证书的行为 25
4.4.2 电子认证服务机构对证书的发布 25
4.4.3 电子认证服务机构对其他实体的通告 25
4.5 密钥对和证书的使用 25
4.5.1 订户私钥和证书的使用 25
4.5.2 依赖方对证书的使用 26
4.6 证书更新 26
4.6.1 证书更新的情形 26
4.6.2 请求证书更新的实体 26
4.6.3 证书更新请求的处理 26
4.6.4 颁发新证书时对订户的通告 27
4.6.5 构成接受更新证书的行为 27
4.6.6 电子认证服务机构对更新证书的发布 27
4.6.7 电子认证服务机构对其他实体的通告 27
4.7 证书密钥更新 27
4.7.1 证书密钥更新的情形 27
4.7.2 请求证书密钥更新的实体 28
4.7.3 证书密钥更新请求的处理 28
4.7.4 颁发新证书时对订户的通告 28
4.7.5 构成接受密钥更新证书的行为 28
4.7.6 电子认证服务机构对密钥更新证书的发布 28
4.7.7 电子认证服务机构对其他实体的通告 28
4.8 证书变更 29
4.8.1 证书变更的情形 29
4.8.2 请求证书变更的实体 29

4.8.3 证书变更请求的处理 29
4.8.4 颁发新证书时对订户的通告 29
4.8.5 构成接受变更证书的行为 29
4.8.6 电子认证服务机构对变更证书的发布 29
4.8.7 电子认证服务机构对其他实体的通告 29
4.9 证书注销和挂起 30
4.9.1 证书注销的情形 30
4.9.2 请求证书注销的实体 30
4.9.3 注销请求的流程 30
4.9.4 注销请求的宽限期 31
4.9.5 电子认证服务机构处理注销请求的时限 31
4.9.6 依赖方检查证书注销的要求 31
4.9.7CRL 发布频率 31
4.9.8CRL 发布的最大滞后时间 31
4.9.9 在线状态查询的可用性 31
4.9.10 在线状态查询要求 31
4.9.11 密钥损害的特别要求 32
4.9.12 证书冻结的情形 32
4.9.13 请求证书冻结的实体 32
4.9.14 冻结请求的流程 32
4.9.15 证书冻结的期限限制 32
4.10 证书状态服务 33
4.11 订购结束 33
4.12 密钥生成、备份与恢复 33
5 认证机构设施、管理和操作控制 34
5.1 物理控制 34
5.1.1 场地位置与建筑 34

5.1.2 物理访问 34
5.1.3 电力与空调 35
5.1.4 水患防治 35
5.1.5 火灾防护 35
5.1.6 介质储存 35
5.1.7 废物处理 36
5.1.8 异地备份 36
5.2 程序控制 36
5.2.1 可信角色 36
5.2.2 每项任务需要的人员 37
5.2.3 每个角色的识别与鉴别 37
5.2.4 需要职责分割的角色 37
5.3 人员控制 37
5.3.1 资格、经历和无过失的要求 37
5.3.2 背景审查程序 38
5.3.3 培训要求 38
5.3.4 再培训周期和要求 39
5.3.5 工作岗位轮换周期和顺序 39
5.3.6 未授权行为的处罚 39
5.3.7 独立合约人的要求 39
5.3.8 提供给员工的文档 39
5.4 审计日志程序 39
5.4.1 记录事件的类型 39
5.4.2 处理日志的周期 41
5.4.3 审计日志的保存期限 41
5.4.4 审计日志的保护 41
5.4.5 审计日志备份程序 41
5.4.6 审计收集系统 41
5.4.7 对导致事件实体的通告 42

5.4.8 脆弱性评估 42
5.5 记录归档 42
5.5.1 归档记录的类型 42
5.5.2 归档记录的保存期限 43
5.5.3 归档文件的保护 43
5.5.4 归档文件的备份程序 43
5.5.5 记录时间戳要求 43
5.5.6 归档收集系统 44
5.5.7 获得和检验归档信息的程序 44
5.6 电子认证服务机构密钥更替 44
5.7 损害与灾难恢复 44
5.7.1 事故和损害处理程序 44
5.7.2 计算资源、软件和/或数据的损坏 44
5.7.3 实体私钥损害处理程序 45
5.7.4 灾难后的业务连续性能力 45
5.8 电子认证服务机构或注册机构的终止 45
6 认证系统技术安全控制 47
6.1 密钥对的生成和安装 47
6.1.1 密钥对的生成 47
6.1.2 私钥传送给订户 47
6.1.3 公钥传送给证书签发机构 48
6.1.4 电子认证服务机构公钥传送给依赖方 48
6.1.5 密钥长度 48
6.1.6 公钥参数的生成和质量检查 48
6.1.7 密钥使用目的 48
6.2 私钥保护和密码模块工程控制 49
6.2.1 密码模块的标准和控制 49

6.2.2 私钥多人控制（m 选 n） 49
6.2.3 私钥托管 49
6.2.4 私钥备份 49
6.2.5 私钥归档 49
6.2.6 私钥导入、导出密码模块 50
6.2.7 私钥在密码模块中的存储 50
6.2.8 激活私钥的方法 50
6.2.9 解除私钥激活状态的方法 50
6.2.10 销毁私钥的方法 51
6.2.11 密码模块的评估 51
6.3 密钥对管理的其他方面 51
6.3.1 公钥归档 51
6.3.2 证书操作期和密钥对使用期限 51
6.4 激活数据 52
6.4.1 激活数据的产生和安装 52
6.4.2 激活数据的保护 52
6.4.3 激活数据的其他方面 52
6.5 计算机安全控制 52
6.5.1 特别的计算机安全技术要求 52
6.5.2 计算机安全评估 53
6.6 生命周期技术控制 53
6.6.1 系统开发控制 53
6.6.2 安全管理控制 53
6.6.3 生命期的安全控制 53
6.7 网络的安全控制 53
6.8 时间戳 54
7 证书、证书注销列表和在线证书状态协议 54

7.1 证书 54
7.1.1 版本号 54
7.1.2 证书扩展项 54
7.1.3 名称形式 55
7.1.4 名称限制 55
7.2 证书吊销列表 56
7.2.1 版本号 56
7.2.2CRL 和 CRL 条目扩展项 56
7.3 在线证书状态协议 56
7.4 根证书体系要求 56
8 认证机构审计和其他评估 57
8.1 评估的频率和情形 57
8.2 评估者的资质 57
8.3 评估者与被评估者之间的关系 57
8.4 评估内容 57
8.5 对问题与不足采取的措施 58
8.6 评估结果的传达与发布 58
9 法律责任和其他业务条款 59
9.1 费用 59
9.1.1 证书签发和更新费用 59
9.1.2 证书查询费用 59
9.1.3 证书注销或状态信息的查询费用 59
9.1.4 其他服务费用 59
9.1.5 退款策略 60
9.2 财务责任 60

9.2.1 保险范围 60
9.2.2 其他财产 60
9.2.3 对终端实体的保险或担保范围 60
9.3 业务信息保密 60
9.3.1 保密信息范围 60
9.3.2 不属于保密的信息 61
9.2.3 保护保密信息的责任 61
9.4 个人隐私保密 62
9.4.1 隐私保密方案 62
9.4.2 作为隐私处理的信息 62
9.4.3 不被视为隐私的信息 62
9.4.4 保护隐私的责任 62
9.4.5 依法律或行政程序的信息披露 62
9.4.6 其他信息披露形式 63
9.5 知识产权 63
9.6 陈述与担保 63
9.6.1 电子认证服务机构的陈述与担保 63
9.6.2 注册机构的陈述与担保 63
9.6.3 订户的陈述与担保 64
9.6.4 依赖方的陈述与担保 64
9.7 担保免责 65
9.8 有限责任 65
9.9 赔偿 65
9.9.1 赔偿范围 65
9.9.2 赔偿限制 66
9.10 有效期限与终止 67
9.10.1 有效期限 67

9.10.2 终止 67
9.11 修订 67
9.11.1 修订程序 67
9.11.2 通知机制和期限 67
9.11.3 必须修改业务规则的情形 67
9.12 争议处理 68
9.13 管辖法律 68
9.14 一般条款 68
9.14.1 完整协议 68
9.14.2 转让 68
9.14.3 分割性 68
9.14.4 强制执行 68
9.14.5 不可抗力 69

1 概括性描述

1.1 安信 CA

吉林省安信电子认证服务有限公司（原国投安信数字证书认证有限公司，简称：安信 CA）是经国家密码办公室批准建设，吉林省信息化工作领导小组办公室和吉林省国家密码管理委员会联合批准成立，首批获得了国家工信部颁发的《电子认证服务许可证》和国家密码管理局颁发的《电子政务电子认证服务机构》资质证书，专业从事跨行业、跨地区数字证书签发与管理等安全认证服务的权威第三方电子认证服务机构。公司成立于 2002 年 7 月，注册资本为捌仟万元人民币，主要股东包括长春万盈投资有限公司、吉林省伟威孚科技有限公司以及吉大正元信息技术股份有限公司。

安信 CA 的主营业务是电子认证服务和电子认证安全产品。安信 CA 采用先进的 PKI 技术为身份认证、信息传输的安全性、信息传输的完整性、交易的不可抵赖性提供安全服务。安信 CA 签发的数字证书符合国家相关的各项标准，数字证书广泛应用于电子商务和电子政务活动中需要身份认证及数据安全的各类业务，从而积极的推动电子商务和电子政务的发展。已建立起覆盖全国的电子认证服务网络和较完善的电子认证产品体系。

1.2 CPS 概述

本规则是由安信 CA 根据《中华人民共和国电子签名法》、《电子认证服务管理办法》以及《电子认证业务规则规范（试行）》编写，阐述在证书签发、管理、注销以及更新等认证服务过程中的业务规则以及各参与方的责任。本规则适用于参与安信 CA 认证服务的本公司的工作人员、注册机构、证书订户以及依赖方。

1.3 标识

本规则名称是《吉林省安信电子认证服务有限公司电子认证业务规则》（简称 CPS）。

1.4 电子认证活动参与者

1.4.1 电子认证服务机构

电子认证服务机构（简称 CA）是根据《中华人民共和国电子签名法》、《电子认证服务管理办法》的规定，依法设立的可信的第三方电子认证服务机构。CA 负责签发、更新、吊销、查询数字证书以及发布证书黑名单等工作。

1.4.2 注册机构

注册机构（下文简称 RA）是经过 CA 正式授权管理的业务分支机构，包括证书注册审核（RA）中心，证书服务受理点（LRA）等。RA 负责受理数字证书的申请、更新、恢复、吊销等业务。

1.4.3 订户

证书订户，即最终证书持有者。订户包括持有电子认证服务机构发放的证书的个人、单位、企业、组织、硬件设备、网站等参与认证服务的各种实体。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。

1.4.4 依赖方

使用或信任电子认证服务机构所签发的证书进行交易的证书订户以及依照本业务规则在某些应用中信任证书真实性的所有实体被称为电子认证服务机构的依赖方。依赖方可以是证书订户也可以不是证书订户。

1.5 证书应用

1.5.1 适合的证书应用

安信 CA 签发的订户证书适用于电子政务、电子商务、医疗、教育、企业信息化等领域，以实现以下安全需求：

1. 身份认证：为证书订户身份的确认提供安全保证。
2. 保密传输：为信息的传输和交换提供安全保障。
3. 数字签名及验证：为依赖方进行网上交易的不可抵赖性提供依据。
4. 验证信息完整性：可以验证信息在传递过程中是否被篡改，发送方和接收方的信息是否完整一致。

目前安信 CA 发放的证书包括：个人证书、机构证书、设备证书、场景型证书以及云应用证书。具体证书类型及用途参见安信 CA 网站（http://www.anxinca.com），证书申请人根据实际需求决定使用哪类证书。

- 个人证书：用于标识鉴别个人身份，适用于个人身份认证，电子签名，数据加解密等服务。
- 机构证书：主要应用标识鉴别机构的身份，适用于电子政务、机构信息服务平台以及电子商务平台等用于机构身份认证、电子签名和数据加解密等服务。
- 设备证书：包括各种服务器证书、设备证书和域名证书。用于标识鉴别各种设备身份，实现设备身份认证、数据加解密，保证传输数据完整性和安全性。
- 场景型证书：面向即时业务或特定业务场景的签名需要，在业务需要时自动申请，将业务场景信息整合成数字证书扩展域信息。使用场景证书对业务或场景证据签名后可以证明证据在取证结束后无篡改。场景型证书对应的私钥为一次性使用，在脱离场景后不能被再次使用。
- 云应用证书：面向互联网、手机、云服务等信息技术领域签发的数字证书。适用于在移动互联网、物联网以及云服务等环境中证明订户的身份和电子签名服务。由订户终端和服务器端协同配合完成可靠数字签名。

1.5.2 限制的证书应用

各类证书的订户都只能应用于证书订户主题身份合适的应用。如果参与方不遵守相关约定超出本 CPS 限定应用范围，将不受安信 CA 的保护。

证书密钥的应用范围在订户证书的扩展项中进行了限制。基于证书扩展项限制判断证书有效性取决于应用软件。任何未经安信 CA 认可的证书应用都将不受安信 CA 的保护。

安信 CA 发放的数字证书禁止在违反国家法律，法规或破坏国家安全情况下使用，由此造成的法律后果由订户负责。

1.6 策略管理

1.6.1 策略文档管理机构

安信 CA 安全策略委员会是《安信 CA 中心电子认证业务规则》（CPS）的最高管理机构，负责制定、维护和解释本 CPS。当需要编写或修订本 CPS 时，由安信 CA 策略委会组织相关人员编写，并制定编写负责人。

1.6.2 联系方式

安信 CA 的安全策略委员会为本 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安全策略委员会取得联系，具体联系方式如下：

公司地址：吉林省长春市高新区栖乐荟双创中心 A 座 16 层

邮　　编：130012

办公电话：0431-85177688

公司网址：www.anxinca.com

电子邮箱地址：anxin@anxinca.com

1.6.3 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。

1.6.4 CPS 批准程序

安信 CA 的 CPS 由安信 CA 安全策略委员会组织人员，按照信息产业部的相关规定编写的。所有安信 CA 的 CPS 的更新版本必须经过以下审批程序：

安信 CA 安全策略委员向公司全体员工广泛征集 CPS 的修改建议，并将这些建议汇集到各部门的负责人；安信 CA 安全策略委员会组织专人修改 CPS；安信 CA 安全策略委员会对修改后的 CPS 进行审议；安信 CA 安全策略委员对 CPS 审议通过后，安信 CA 将会根据《电子签名法》、《电子认证服务管理办法》和《电子认证业务规则规范》等行业法规的要求发布 CPS 的最新版本并向信息产业部备案。

1.7 定义和缩写

缩写表

字母缩写	术　　语
CA	电子认证服务机构
CP	认证策略
CPS	认证业务规则
CRL	证书注销列表
DN	证书甄别名
LDAP	轻量级目录访问协议
OCSP	在线证书状态协议
PIN	个人身份号码
PKCS	公钥加密标准
PKI	公钥基础设施
PMA	政策管理机构
RA	注册机构
RFC	意见申请
S/MIME	安全多用途互联网邮件扩展
SSL	安全套接层
WAP	无线应用协议
WTLS	无线传输层安全

术语表

名称	术　　语
安全策略委员会	安信 CA 认证服务体系内的最高策略管理监督机构和 CPS 一致性决定机构
电子认证服务机构	受用户信任，负责创建和分配公钥证书的权威机构
注册机构	面向订户证书，负责订户证书申请审批和管理工作
数字证书	经 CA 数字证书签名包含数字证书使用者身份公开信息和公开密钥的电子文件
证书吊销列表	一个经电子认证服务机构数字签名的列表，标记了已经被注销的公钥证书列表，表示这些证书无效
订户	被签发证书的自然人或者法律实体，且受订户协议或使用条款约束的自然人或法律实体
订户协议	认证服务机构与证书订户之间的协议，规定了各方的权力与责任
公钥	非对称密码算法中可以公开的密钥
私钥	非对称密码算法中只能由拥有者使用不公开的密钥
依赖方	依赖于证书所证明的基础信任关系并依此进行业务活动的个人或机构

2 信息发布与信息管理

2.1 信息的发布

安信 CA 将通过在线方式向订户及证书应用的依赖方提供信息服务。安信 CA 信息服务包含但不限于以下内容： CPS 现行和历史版本，证书 CRL、订户协议、以及其他由安信 CA 在必要时发布的信息，这些信息将严格遵守本 CPS，并符合国家和主管部门颁布的有关法律法规。这些信息将通过安信 CA 网站、安信 CA 的目录（LDAP）服务器和安信 CA 的 OCSP 服务对外发布。

2.2 发布时间和频率

安信 CA 将在成功签发证书的同时在目录服务器上发布证书相关信息（不包含任何交易数据，数据信息以数据库方式存放），在证书挂起或吊销后 24 小时内发布证书注销列表（CRL）。

除非另有规定，安信 CA 将至少每 24 小时一次发布各类证书的吊销列表（CRL）。在紧急情况下，安信 CA 可自行决定缩短公布证书吊销列表的时间。

网站的公告、安信 CA 的 CPS、证书应用情况、协议流程等信息不定期进行更新，无固定的发布时间或频率。

2.3 信息访问控制

安信 CA 的 CPS 以及相关的技术支持、订户协议等在安信 CA 官网（http://www.anxinca.com）上发布。已被吊销了的证书可以在目录（LDAP）服务器 ldap://sm2ldap.anxinca.com:390 上查询，证书状态可以通过 OCSP 服务获得。

数字证书查询、CRL、CPS 的查询和下载是公开的。CPS 经安信 CA 安全策略委员审核通过后发布，提供给访问者自由浏览。

安信 CA 在必要时可自主选择是否实行信息的权限管理，以确保只有经过授权的人员或机构才有权阅读受安信 CA 控制的信息资料，确保安信 CA 相关实体的实际权益。

安信 CA 设置了信息访问控制和安全审计措施，保证只有经过授权的安信 CA 工作人员才能编写和修改安信 CA 网站的公告或发布信息。

3 身份识别与鉴别

3.1 命名

3.1.1 名称类型

安信 CA 签发的证书，含有颁发机构和订户证书主体的名称，对证书订户和其他属性进行的鉴别和记录采用甄别名（Distinguished Name，简称 DN），甄别名包含在证书主体内，是证书持有者的唯一标识。安信 CA 的证书符合 X.509 标准，甄别名采用 X.500 的命名方式。

3.1.2 名称包含的内容

安信 CA 签发的证书可以根据证书甄别名确定订户证书的主体。证书甄别名所采用的用户识别信息一般具有明确的、可追溯的、肯定的代表意义，应该使用反映证书主体真实身份的、具有实际意义的、与法律不冲突的内容。

个人证书通常包含个人真实姓名或证件号码，作为标识订户的关键信息被认证。

机构证书通常使用包括《营业执照》《事业单位法人证书》等证书中标识的统一社会信用代码和单位名称，作为标识订户的关键信息被认证。

设备证书应使用能标识该设备的名称、域名、IP 等结合订户的其他信息一起被认证。

场景型证书应使用申办场景的申请人真实姓名或场景的特征等，结合作为标识订户的关键信息被认证。

云应用证书应使用注册机构标识，订户名称，唯一标识等特征，作为标识订户的关键信息被认证。

3.1.3 订户的匿名或伪名

安信 CA 的订户在进行数字证书申请时不能使用匿名或伪名。

3.1.4 名称的唯一性

在安信 CA 服务体系中，不同订户证书的甄别名是唯一的，对于同一订户，安信

CA 可以用其甄别名为其签发多张证书。

3.1.5 商标的承认、鉴别和角色

安信 CA 签发的证书不包含任何商标或者可能对其他机构构成侵权的信息。安信 CA 签发证书时不验证申请人是否使用商标。发生纠纷时安信 CA 有权拒绝申请或者吊销已签发的证书。

3.2 初始身份认证

3.2.1 证明拥有私钥的方法

除场景型证书和云应用证书外，证书私钥由介质生成并直接保存在介质中，证书持有者通过证书申请书中包含的数字签名证明申请者持有与所要申请证书中的公钥相对应的私钥。安信 CA 签发证书时，系统将自动使用订户申请书中的公钥验证签名的有效性和申请数据的完整性，来确认使用者拥有私钥。

3.2.2 组织机构身份的鉴别

对于组织机构身份的鉴别，安信 CA 或授权的注册机构需要验证组织的合法证件。组织机构应指定和授权证书的申请代表，在证书的申请书上签字表示接受证书申请的有关条款，经办人应持身份证件供鉴别身份，并承担相应的责任。

经办人经组织机构授权，到安信 CA 受理机构提交书面材料办理或在线提交电子化材料办理。CA 受理机构对组织机构身份的鉴别包括现场核验、通过可信任的第三方数据库等辅助手段进行身份鉴别。

组织机构身份鉴别证明材料包括不限于如下：

- 数字证书申请表（签字加盖公章）
- 授权委托书（签字加盖公章）
- 经办人有效身份证原件及复印件
- 证明组织机构身份的证件，如营业执照副本及复印件等。（复印件需要加盖公章）
- 如果申请服务器证书还需提交域名使用权证明、ICP 运营证明、设备所有权使用权书面承诺等合法身份证明（加盖公章）

安信 CA 按照鉴别流程对申请资料的原件、复印件或电子材料进行鉴别后批准或拒绝申请。安信 CA 保存组织机构申请材料的期限为证书失效后 5 年，这个规定期限随法律、政策、主管部门的要求修改。

3.2.3 个人身份的鉴别

对于个人身份的鉴别，证书申请者需要向 CA 中心的审核人员提供有效的身份证明（身份证、驾驶执照、军官证等等）和充足的证书申请者信息。申请者信息根据不同的应用采取不同的要求。对于机构中的个人证书申请者，其申请材料需要加盖公章或者授权证明材料或者由机构对该个人信息进行有效确认后，安信 CA 将对该组织机构进行鉴别鉴别并进行评定审核。

个人或授权代表人，到安信 CA 受理机构提交书面材料办理或在线提交电子化材料办理。CA 受理机构对个人身份的鉴别包括现场核验、在线生物识别以及可信任的第三方数据库等手段进行身份核验。

个人身份鉴别证明材料包括不限于如下：

- 数字证书申请表（签字加盖公章）
- 有效身份证原件及复印件
- 如果委托他人办理需要授权委托书（签字）委托人身份证原件和复印件
- 如需授权机构确认，提供机构授权证明材料或经安信 CA 认可的方式传递的机构确认信息。

安信 CA 按照鉴别流程对申请资料的原件、复印件或电子材料真实性进行鉴别后进行批准申请或拒绝申请的操作。批准后，安信 CA 保存个人申请材料的期限为证书失效后 5 年，这个规定期限随法律、政策、主管部门的要求修改。

3.2.4 其他类型证书订户身份鉴别

场景型证书订户身份鉴别参照个人身份和机构身份的鉴别方法进行，也可以采取录音、录像等有效的电子场景核验方式进行自动鉴别。

云应用证书订户身份鉴别参照个人身份和机构身份的鉴别方法进行。

订户申请域名或 IP 的鉴别参照个人身份和机构身份的鉴别方法进行。鉴别无法通过的订户将拒绝申请。

3.2.5 没有验证的申请者信息

订户在申请证书时，除安信 CA 要求必须验证的申请者信息外，其余的信息可不被要求必须验证。

3.2.6 授权确认

当申请者代表组织机构申请证书时，需出示足够的证明信息以证明其是否有权代表那个实体。组织在证明文件上加盖公章后，则证明本组织对办理人授权确认，一旦审核通过，安信 CA 会将授权信息妥善保存。

个人如果需要代办人代办，需要对代办人证明信息签字授权确认。

3.2.7 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 根据业务需要，决定是否接受这些被其他机构鉴别审核过的资料进行受理。

3.3 密钥更新请求的标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

在证书期满前，证书订户有必要获得新证书以保证证书可以持续使用。通常 CA 要求订户产生新的密钥对来代替将要期满的密钥对，称为“密钥更新”。证书的密钥更新时，通过订户使用原有私钥对更新请求进行签名，安信 CA 使用订户原有公钥验证确认签名来进行常规密钥更新的标识与鉴别。

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。

3.4 注销请求的标识与鉴别

当安信 CA 根据本 CPS4.9.1 所述理由撤销的订户证书时，无需进行鉴别。如果订户主动要求撤销证书，则按照本 CPS3.2 进行身份鉴别。

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

证书申请实体包括个人和具有独立法人资格的组织机构（包括事业单位、企业单位、社会团体和人们团体等）。

4.1.2 注册过程与责任

4.1.2.1 申请及注册流程

安信 CA 的证书申请人可以通过现场面对面方式或在线方式提交证书申请请求，但证书申请人需要遵循以下要求：

1. 订户需提供本 CPS 3.2 中所述的有效身份证明材料及相关申请文件，并保证所提供的证明材料真实有效；
2. 安信 CA 的注册机构在审核订户申请后，将审核通过的订户信息提交至安信 CA；
3. 安信 CA 根据注册机构的请求签发证书；
4. 注册机构使用安信 CA 提供的授权信息为订户制作证书；
5. 注册机构通过安全的方式（如：面对面提交）将证书发给订户。

4.1.2.2 电子认证服务机构的责任

安信 CA 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）进行实施，具体责任如下：

1. 参照本 CPS 3.2 中的要求对订户提供身份信息进行采集、记录、鉴别和审核，通过审核后向订户签发证书。
2. 如身份鉴别过程由授权注册机构完成，安信 CA 对所授权的注册机构有监督、管理和审计职责。
3. 安信 CA 及授权的注册机构有妥善保管订户信息资料的责任。

4.1.2.3 注册机构的责任

注册机构主要负责对证书申请者身份的鉴别和订户信息的录入，具体责任如下：

1. 注册机构参照本 CPS 3.2 的要求对订户所提交的申请材料进行采集、记录和审核，通过审核后，向安信 CA 提交证书申请。
2. 注册机构需要接受安信 CA 的监督、管理和审计。
3. 应当按照 CA 机构的要求，向安信 CA 提交订户身份审核资料或自行妥善保存。
4. 有义务告知证书订户使用数字证书时享有的权利和责任。

4.1.2.4 订户的责任

订户的责任如下：

1. 订户必须保证提供资料的真实性，有效。
2. 订户须配合安信 CA 或授权的注册机构完成对其身份信息及相关资料的采集、记录与审核工作。
3. 订户须了解并与安信 CA 签署订户协议。

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 或相关注册机构提交证书申请后，安信 CA 或授权的注册机构按照本 CPS 3.2 所规定对申请人的身份进行识别与鉴别，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订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为合法被授权者。

4.2.2 证书申请批准和拒绝

安信CA按照本CPS所规定的身份鉴别流程对订户提交的申请材料及其身份信息进行识别与鉴别，并根据鉴别结果决定批准或拒绝证书申请。

如果证书申请人通过本CPS所规定的身份鉴别流程且鉴别结果为合格，安信CA或授权的注册机构等将批准证书申请，为证书申请人制作颁发数字证书。

如证书申请人未能通过身份鉴别，安信CA或注册机构将拒绝证书申请人的申请，并将拒绝理由告知给对方。

被拒绝的申请人可准备符合本CPS所规定的相关材料后，再次提出申请。

4.2.3 处理证书申请的时间

安信CA或注册机构在收到订户的所有必须的证书申请信息后，将在2个工作日内处理证书申请。

安信CA或授权的注册机构能否在上述时间期限处理证书申请取决于证书申请人是否真实、完整、准确地提交了相关信息和是否及时响应了安信CA的管理要求。

针对场景型证书和云应用证书等对实时性要求较高的申请为即时处理。

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

在证书订户申请通过身份鉴别后，安信CA和注册机构的系统操作员负责录入订户的申请信息，并将申请提交给系统审核员审核；审核通过后，向CA签发系统提交证书申请。

CA签发系统向注册系统返回证书下载凭证或证书。证书的最终签发意味着安信CA最终完全正式批准了证书申请。

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或授权的注册机构，当申请者申请审核通过后，安信CA将会为其签发签名证书。

4.3.2 电子认证服务机构和注册机构对订户的通告

安信CA会采用以下几种方式告知订户：

1. 电子或纸质的受理回执。
2. 电子邮件（e-mail）。
3. 采用现场方式面对面通知订户。
4. 其他的安全可行的方式。

4.4 证书接受

4.4.1 构成接受证书的行为

证书申请人按照安信 CA 的证书申请流程完成证书申请后，安信 CA 将为其签发数字证书，并通过面对面、邮寄或电子等方式发给证书申请人，证书申请人从获得数字证书起，就被视为同意接受证书。

4.4.2 电子认证服务机构对证书的发布

安信 CA 在签发完通用型证书后 24 小时内，将该订户证书发布到安信 CA 的目录服务系统中，供订户和依赖方查询和下载。

安信 CA 不提供场景型证书的发布。

4.4.3 电子认证服务机构对其他实体的通告

安信 CA 不对其他实体进行通告，其他实体可以通过安信信息服务自行查询。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户在提交了证书申请并接受了安信 CA 所签发的证书后，均视为同意遵守与安信 CA、依赖方有关的权利和义务条款。

证书订户接受到数字证书，应妥善保管其所持有证书对应的私钥。订户只能在指定的应用范围内使用私钥和证书，订户只有在接受了相关证书后才能使用对应的私钥，并在证书使用到期或吊销后，订户须停止使用该证书对应的私钥。

场景型证书仅应用于订户对应的电子签名行为，订户只能在该次电子签名中使用私

钥和证书，订户只有在接受了相关证书之后，才能使用对应的私钥，私钥将在完成本次电子签名数学运算后进行销毁，之后订户须停止使用该证书对应的私钥。

云应用证书必须由订户和签名服务云端协同配合才能完成一次数字签名，订户只能在指定的应用范围内使用私钥和证书，订户只有在接受了相关证书之后才能使用对应的私钥，并在证书到期或吊销之后，订户须停止使用该证书对应的私钥。

4.5.2 依赖方对证书的使用

依赖方只能在恰当的应用范围内依赖于证书，并且与证书适用范围相一致，依赖方获得对方证书后，依赖方有义务进行如下确认操作：

1. 确认证书是依赖方信任的认证服务机构签发；
2. 确认该证书在有效期之内；
3. 确认该证书是否被注销；
4. 确认密钥用法是否符合证书标识的密钥用途。

4.6 证书更新

证书更新指在不改变证书中订户的公钥或其他信息的情况下，为订户签发一张新证书。

4.6.1 证书更新的情形

当订户的证书即将到期时，可向安信 CA 或其授权的注册机构提出证书更新申请。

4.6.2 请求证书更新的实体

请求证书更新的实体为证书订户。

4.6.3 证书更新请求的处理

安信 CA 向订户提供两种证书更新处理方法，分别为在线更新和离线更新。

当安信 CA 或其授权注册机构接收到订户的更新申请后，需要鉴别该证书是否属于安信 CA 签发的证书以及订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），如果订户采用在线的方式申请更新，安信 CA 或其授权注册机构还应检查该申请所附签名的真实性。

通过审核后，安信 CA 或其授权注册机构将会为订户作证书更新处理。

如果订户选择离线的方式进行更新，可以到安信 CA 或其授权注册机构进行更新处理。

如果订户选择在线方式进行更新，安信 CA 或其授权注册机构将会把证书更新所需的授权信息以安全的方式（该方式在订户申请之初已被定义）发送给订户。

4.6.4 颁发新证书时对订户的通告

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 电子认证服务机构对更新证书的发布

同 4.4.2

4.6.7 电子认证服务机构对其他实体的通告

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

证书密钥更新的情形包括：

1. 当订户的证书即将到期。
2. 当订户证书密钥遭到损坏时。
3. 当订户证实或怀疑其证书密钥不安全时。

4. 其他可能导致更新的情形。

4.7.2 请求证书密钥更新的实体

已经申请过安信 CA 证书的订户可以申请证书密钥更新。

4.7.3 证书密钥更新请求的处理

安信 CA 向订户提供两种密钥更新处理方法，分别为在线更新和离线更新。

当安信 CA 或其授权注册机构接收到订户的更新申请后，需要鉴别该证书是否属于该机构签发的证书以及订户是否有权申请证书密钥更新，并且检验该证书的有效性（是否已过期），如果订户采用在线的方式申请更新，安信 CA 或其授权注册机构还应检查该申请所附签名的真实性。

通过审核后，安信 CA 或其授权注册机构将会为订户作证书密钥更新处理。

如果订户选择离线的方式进行更新，可以到安信 CA 或其授权注册机构进行更新处理。

如果订户选择在线方式进行更新，安信 CA 或其授权注册机构将会把证书更新所需的授权信息以安全的方式（该方式在订户申请之初已被定义）发送给订户。

4.7.4 颁发新证书时对订户的通告

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 电子认证服务机构对密钥更新证书的发布

同 4.4.2

4.7.7 电子认证服务机构对其他实体的通告

同 4.4.3

4.8 证书变更

4.8.1 证书变更的情形

证书变更指订户的证书信息发生变更，申请重新签发一张证书，对原证书进行吊销处理。

场景型证书没有变更服务。

云应用证书按照新办证书业务流程处理。

4.8.2 请求证书变更的实体

任何使用证书的订户在证书发生本 CPS4.8.1 中涉及的情形时，均可向安信 CA 或其授权注册机构提出证书变更申请。

4.8.3 证书变更请求的处理

当安信 CA 或其授权注册机构接收到订户的变更申请后，需要鉴别该证书是否属于安信 CA 签发的证书以及订户是否有权申请证书变更，并且检查证书的有效性以及变更后的订户身份证明材料，该过程与初始注册过程相同。

4.8.4 颁发新证书时对订户的通告

同 4.3.2

4.8.5 构成接受变更证书的行为

同 4.4.1

4.8.6 电子认证服务机构对变更证书的发布

同 4.4.2

4.8.7 电子认证服务机构对其他实体的通告

同 4.4.3

4.9 证书注销和挂起

4.9.1 证书注销的情形

如果有以下情况，证书将被注销：

1. 安信 CA、授权注册机构或订户认为或十分怀疑有威胁订户私钥安全的不利因素存在；
2. 安信 CA、授权注册机构或订户认为申请者违背了订户责任条款中的义务、要求或保证；
3. 证书订户与组织从属关系已被终止；
4. 安信 CA、授权注册机构或订户认为证书的签发没有遵循本 CPS（或业务规则）所要求的过程执行，证书没有签发给证书的主体，或证书的签发未通过证书主体的人的许可；
5. 证书中的信息不准确或被更改；
6. 订户根据证书注销流程要求自愿撤销证书；
7. 由于法律或政策的要求安信 CA 采取的作废措施。

4.9.2 请求证书注销的实体

已申请安信 CA 证书的订户可以请求证书注销。

同时，安信 CA 也可在 4.9.1 所述的情形下主动吊销订户的证书。

4.9.3 注销请求的流程

证书注销请求的处理采用与初始证书签发相同的流程

1. 证书注销的申请人到安信 CA 或其授权的注册机构提交书面资料，并注明注销理由。
2. 安信 CA 或授权的注册机构根据本 CPS 的相关要求对订户提交的注销请求进行审核。
3. 安信 CA 或授权的注册机构注销订户证书后，应通知证书订户结果，订户证书在 24 小时内进入 CRL 列表，并对外发布。
4. 场景型证书没有证书注销。

4.9.4 注销请求的宽限期

如果出现私钥泄露等事件，注销请求必须在发现泄露嫌疑 8 小时内提出。其他注销原因的请求必须在 48 小时内提出。

4.9.5 电子认证服务机构处理注销请求的时限

安信 CA 或其授权的注册机构会在注销申请提交后的立即注销证书并在 24 小时之内生效。

4.9.6 依赖方检查证书注销的要求

依赖方必须在信任某个证书前查询注销列表确认证书的状态信息，这一列表由安信 CA 定期和实时发布。

4.9.7CRL 发布频率

安信 CA 可采用实时或定期的方式发布 CRL，发布 CRL 的频率根据证书策略确定，一般为 24 小时定期发布。

4.9.8CRL 发布的最大滞后时间

CRL 发布的最长滞后时间为 24 小时。

4.9.9 在线状态查询的可用性

安信 CA 能够向安全保障要求高的订户提供 OCSP 在线证书状态查询服务。

4.9.10 在线状态查询要求

安信 CA 能够订户提供 OCSP 在线证书状态查询服务，

依赖方可以申请使用安信 CA 提供 OCSP 服务在线状态查询服务。

4.9.11 密钥损害的特别要求

当订户发现或有充足的理由发现其密钥被损害时，应当及时提出证书注销请求。

4.9.12 证书冻结的情形

如果有以下情况，安信 CA 将会考虑冻结证书：

1. 订户提出暂停使用该证书；
2. 订户未能履行与安信 CA 签订的协议中应尽的责任，如订户未按期缴纳证书服务费；
3. 注册机构、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冻结请求并获得批准。

4.9.13 请求证书冻结的实体

证书订户本人或其授权的代理人、证书注册机构、政府主管部门或国家司法机关。

4.9.14 冻结请求的流程

1. 证书冻结申请人向安信 CA 或其授权注册机构提交证书冻结申请表和身份证明材料，同时说明证书冻结的理由，如果为证书持有者以外的人（如证书注册机构或国家司法机关）提交冻结申请，同样需要填写申请表并加盖公章；
2. 安信 CA 或其授权注册机构鉴别冻结申请者身份的真实性，并确认申请者是否有权提出该申请；
3. 注册机构审核冻结申请后，将该申请提交至安信 CA，等待安信 CA 对该申请的处理；
4. 安信 CA 在处理冻结申请后，会定期或实时产生 CRL 列表，并通知订户证书已被冻结。

4.9.15 证书冻结的期限限制

证书冻结的最长期限不得超过证书的有效期，如超过证书有效期而订户没有提出解冻申请，则该证书将会自动失效。

4.10 证书状态服务

安信 CA 通过 LDAP、OCSP、以及 CRL 提供证书状态查询服务，如订户想了解证书状态可使用此类服务。安信 CA 提供 7×24 小时的证书状态查询服务。

4.11 订购结束

在订户证书期满时，安信 CA 会自动终止对订户证书的认证服务。此外，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注销流程相同。

4.12 密钥生成、备份与恢复

订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 及其授权的注册机构不提供订户证书签名密钥的备份和恢复服务。

安信 CA 的订户证书加密密钥对由吉林省密钥管理中心提供。该机构负责订户加密密钥对的生成、管理和备份，并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。

场景型证书的签名密钥对由签名设备生成密钥并执行签名后，签名私钥不进行保管，即时销毁。

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

为了保证 CA 系统在运行中的稳定、安全和可靠，安信 CA 在硬件设备、操作系统、数据库系统和目录服务系统的选用及物理环境的建设等各方面紧密结合 CA 系统的设计，原 CA 系统于 2004 年通过国家密码管理部门的安全性审查和技术鉴定，升级后的 CA 系统于 2013 年通过国家密码管理部门的安全性审查和技术鉴定。

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。

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。

安信 CA 的环境共分为四个区域：公共区、服务区、管理区、核心区，每个区域具有不同区域访问控制措施；

任何物理访问行为必须自动记录并有全程监控跟踪。安信 CA 设置了以下安全访问级别：

普通级：不涉及对 CA 系统核心组件操作的区域，该级别主要包括日常的办公场所和公司内部的公共区域，这些区域的门均安装了门禁系统。

敏感级：主要是中心网络的控制区域。这个区域的走廊里安装了红外报警系统防止无人进入时的非法入侵。在此区域中的机房设计为六面钢板的屏蔽式结构，在机房的门口配有指纹门禁系统。

高度敏感级：CA 系统核心组件所在的位置。

5.1.3 电力与空调

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

机房空调采用高效能、高灵敏度的空调系统，配合通风、温湿度调节等手段，控制机房内设备运行温湿度，保证系统正常运行。

安信 CA 的电气系统符合电子数据处理设备的防火标准。机房电力供应按照机房设备负载要求设计，采取三向方式供电，机房采用两台 UPS 供电设备并行双路向机房内设备供电，并在每个区域机房内设置了 ATS 不间断电源切换装置，保障了单电路出现故障后，另外一条线路可随时供应电力。

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，当出现漏水、水灾时，监控系统可以进行警示。

5.1.5 火灾防护

安信 CA 的火灾自动报警系统设计依据 GB50116-98《火灾自动报警系统设计规范》进行设计，七氟丙烷自动灭火系统设计依据 GB50370-2005《气体灭火系统设计规范》进行设计。火灾自动报警系统通过设置在机房的温感、烟感探头采集消防数据，提供系统实时处理火灾自动报警终端的报警数据和系统运行状态数据。机房关键区域均安装了七氟丙烷自动灭火系统，当火灾报警信号确认后，报警控制装置自动联动相关设备，并启动七氟丙烷自动灭火系统。。该防火系统具有自动、手动及机械应急操作共三种启动方式。

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。所有的处理需至少两人同时在场监督，并对销毁资料进行记录确认，相关记录需存档保存。

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第三方以安全的方式保存。

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，CA 及 RA 必须保证只有被认定为可信的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、注销请求、更新请求或其他注册信息的接收、拒绝、或其它业务的受理
3. 证书的发放、注销和访问 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. 订户信息审核员
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 的授权证书服务机构，其人员配置及服务操作要求应执行安信 CA 为其制定的服务管理规范。

5.2.2 每项任务需要的人员

安信 CA 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和数据的管理和操作应有多个可信人员共同完成。认证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

所有安信 CA 的可信人员，必须通过相关审核后，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能本人使用；发放的安全令牌不允许共享；安信 CA 的系统和应用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、注销等业务处理人员
- 订户资料管理人员
- 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。

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

在开始一个可信人员的雇佣关系前安信 CA 将会至少执行以下背景检查：

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

组织人力资源部门和安全管理人员共同完成背景审查工作，背景审查具体操作内容至少包括以下内容：

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．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. 备选人或可信人员伪造真实身份信息
2. 十分不合适或不可信的个人经历
3. 工作中有严重不诚实行为

5.3.3 培训要求

安信 CA 向其员工和授权注册机构的人员提供与 CA 系统相关的硬件、软件及其 CA 应用程序的岗前和在岗培训，目的是为了让员工能够胜任其工作。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. CA 中心的安全和操作策略及程序
4. 使用和操作相关的硬件和软件
5. 紧急事件和危险情况的报告和处理

6. 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 在得到信息后立即终止该员工进入安信 CA 认证服务体系，未授权行为的处罚包括接触或终止劳动合同、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、软件以及应用程序的技术手册，同时员工也可以查看安信 CA 的业务流程介绍和证书策略，还可以浏览本 CPS。

5.4 审计日志程序

5.4.1 记录事件的类型

审计日志和时间记录应包括每个日志记录的日期和时间、日志记录的序号、生成日

志记录的实体身份、日志记录的种类。安信 CA 会以手动或自动记录的方法记录以下重大事件：

1. CA 密钥整个生命周期的管理事件：

   -密钥的产生、备份、存储、注销、归档、销毁。

   -加密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、注销。

   -成功或不成功的请求处理。

   -签发证书和 CRL。

与安全相关的事件：

1. 成功或失败的系统访问
2. 系统人员对安全系统的操作
3. 对于安全有关的敏感文件或记录的读、写或删除操作
4. 系统崩溃、硬件错误、其他异常现象
5. 防火墙和路由器的工作
6. CA 系统设备访问者的进入/退出

日志访问包括以下元素：

1. 访问的日期和时间
2. 日志访问序号
3. 日志访问实体的身份
4. 何种访问

注册机构记录以下证书申请信息：

1. 证书申请者提交的是何种身份证明文件
2. 记录证明文档的证明数据、数字或相关信息（如：证书申请者的身份证号码）
3. 申请书和证明文档复印件的存储位置
4. 接受申请书的实体的身份
5. 验证证明文档的方法
6. 负责接受的申请的认证服务机构和负责提交申请的注册机构名称

5.4.2 处理日志的周期

安信 CA 每日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。

每月对证书生命周期内的管理事件进行审查。

每个季度对系统管理、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。

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。审查记录每日渐增备份并且在每个月送到另外一个安全的环境中进行长期归档保存，与证书相关的审计日志存档期至少为证书失效后 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来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 的审计收集系统结合了 CA 系统的自动及手动的审计收集方式，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

安信 CA 随时准备上述系统的检查管理和审查工具。在需要的时候，安信 CA 会随时应用这些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，安信 CA 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、系统或应用程序对本 CPS5.4.6 中涉及的系统引发事件，又被安信 CA 的审计系统记录下来，安信 CA 没有义务通知他们。

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 对这种事件进行检查后将会执行逻辑安全脆弱性评估。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。

5.5 记录归档

5.5.1 归档记录的类型

除了审计日志，安信 CA 会对 CA 的数据库定期存档。存档内容包括安信 CA 处理的每个证书的申请、使用、注销、过期、密钥替换、密钥更新的实质性的动作和信息。

安信 CA 记录证书生命周期的以下事件：

1. 证书申请者的身份

2. 证书申请审批材料
3. 订户证书
4. 证书注销列表（CRL）
5. 完整性审计相关的信息。

签名私钥和加密私钥原则上由实体本身保存，有关私钥的责任由实体本身承担。

如果上述记录是正确的且完整的编入索引、储存、保护和复制，那么他们将会存入安全的电子档或硬件存储设备中。

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；CA 证书、密钥和订户证书的归档应在其过期后额外保留 5 年；CA 和 RA 与系统相关操作记录的归档应保留一年以上。

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，只有授权的信任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对电子归档记录的未授权访问、修改、删除或其他企图。存储归档数据的介质和处理归档数据的应用软件要保证归档数据在其归档期限内能够成功被访问。

5.5.4 归档文件的备份程序

安信 CA 系统管理员每天对签发的证书信息做电子档备份，每日备份包括服务器本机、移动存储、备用服务器共计三份，每月对全部信息进行离线备份并保存在安全环境中。

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，如有必要，安信 CA 可以为相关记录添加时间戳服务。

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，并由具有相关权限的管理人员进行管理和分类。

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 的密钥对在生命周期结束时其服务也将终止。只有在密钥的累计使用时间未超过密钥最大生命周期的前提下安信 CA 的密钥才可以被更新。新的密钥对替换旧密钥对并且支持新的服务。

在上级电子认证服务机构的 CA 证书期满前，要对密钥采取更新以加快上级电子认证服务机构密钥对顺利过渡为新的电子认证服务机构密钥对。电子认证服务机构的密钥更换程序需要：

1. 上级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. 使用新密钥对签发上级 CA 证书。至此开始使用新的上级 CA 证书签发下级 CA 证书或订户证书。
3. 在使用前密钥对签发的最后一个证书期满之前，上级 CA 还会继续发布前上级 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

当发生故障时，安信 CA 将按照灾难恢复计划实施恢复。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。

5.7.2 计算资源、软件和/或数据的损坏

当计算资源、软件和/或数据被损坏时将会立即报告安信 CA 的安全事件负责人，突

发事件处理程序将被启动。这种程序需要相应的自动调整、事件调查和事件响应。必要时安信 CA 的密钥损坏或灾难恢复程序将会启动。

5.7.3 实体私钥损害处理程序

当怀疑或发现安信 CA、安信 CA 的授权注册机构或订户私钥被损坏，安信 CA 将会组织安全管理员、CA 运营操作人员、技术服务人员和其他安信 CA 的管理代表，他们对情况分析后将产生一个行动方案，经安信 CA 安全策略委员会同意后将实施此方案。当 CA 证书有必要注销时，将会执行以下程序：

1. 立即向行业主管部门汇报，通过公司网站或公共媒体对订户进行通告。
2. 注销所有证书并将证书的注销状态传达给订户及依赖方。
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。

订户证书私钥遭到损坏时：

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 或授权的注册机构注销其证书，安信 CA 按照本 CPS 要求发布证书注销信息。
2. 当安信 CA 或其授权注册机构发现证书订户的实体私钥受到损害时，安信 CA 将注销证书并通知证书订户，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

当主运营场所发生灾难或不可抗力事故而不能正常运营时，安信 CA 将利用备份数据和设备恢复各项业务的正常运行并应能够满足以下业务连续性要求：

- 在尽可能短的时间内恢复业务系统
- 能够恢复客户信息
- 能够恢复对客户的服务
- 有足够的人员继续业务并且不违反职责分割的要求

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 的运作，安信 CA 将按照相关的法律法规所制定的步骤终

止运营，并按照相关法律法规要求进行档案和证书的存档。

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订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. 起草安信 CA 终止声明。
2. 通知受终止影响的组织，如申请者、依赖方和订户。
3. 支付这种通知的开销。
4. 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。
5. 保持对申请者和订户的支持服务。
6. 保持注销服务，如 CRL 的发布。
7. 如必要的话，注销未过期、未注销的终端实体申请者和下级 CA 的证书。
8. 对未期满、未注销的证书将被注销或后续电子认证服务机构签发替换证书。
9. 对电子认证服务机构私钥和包含该私钥的硬件的部署。
10. 将该电子认证服务机构的服务过渡到后续电子认证服务机构。

当注册机构因故终止服务时，电子认证服务机构将按照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 签名密钥的生成，其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。加密机采用密钥分割机制进行备份，按照《安信 CA 密码设备及密钥策略》授权 3 个密钥管理员，凭借智能 IC 卡对密钥进行控制管理。

个人和机构订户的密钥对：签名密钥对应使用国密局认可的、安信 CA 证书签发系统支持的介质生成签名密钥对。安信 CA 并不承诺接受所有类型的密码产生设备。加密密钥对由吉林省密钥管理中心（以下简称 KMC）对密钥生成进行生成控制保存管理。并通过安全方式传输给订户。

场景型证书密钥对：订户的签名密钥由签名设备生成。

云应用证书密钥对：由订户终端和云端的国家密码主管部门许可的密码服务器共同计算协同产生。

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。证书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 私钥传送给订户

订户签名私钥是由订户证书存储设备产生不需要传递。订户加密私钥由吉林省密钥管理中心生成并保存。在制作证书时，加密私钥采用国家密码主管部门许可的算法加密，并在安全通道中传送到订户证书存储介质。

云应用证书由用户终端和云端共同产生和保存。

6.1.3 公钥传送给证书签发机构

订户通过安信 CA 的注册管理系统生成的数字证书申请书将公钥提交给安信 CA 签发。在传递过程中采用国家密码主管部门许可的密钥算法，保证传输中数据安全。

6.1.4 电子认证服务机构公钥传送给依赖方

安信 CA 为订户提供公钥证书的在线下载功能，订户可以通过访问安信 CA 的对外发布网站 www.anxinca.com 即可获取安信 CA 的公钥证书，安信 CA 还提供面对面提交或软件预置的方式向订户提供 CA 公钥证书。

6.1.5 密钥长度

安信 CA 按照国家法律法规，政府主管机构等对密钥长度的明确规定和要求。

安信 CA 支持 RSA 国际算法证书和 SM2 国产算法证书，支持签发 RSA-1024 和 RSA-2048 支持签发 SM2-256，安信 CA 根据订户需求提供相应密钥类型证书。

6.1.6 公钥参数的生成和质量检查

安信 CA 的公钥参数在国家密码主管部门批准的加密设备中生成，并遵从这些设备的生成规范和标准。这些设备内置的协议、算法等已经具备了足够的安全等级要求。参数的质量检查同样由通过国家密码主管部门批准许可的加密设备和硬件介质进行。

6.1.7 密钥使用目的

安信 CA 认证服务体系中的密钥用途与证书的类型相关。

安信 CA 的私钥用于签发自身证书、下级证书和证书注销列表 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身份认证、责任认定、授权管理等安全服务过程中的签名和验签，加密密钥对可以用于信息的加密解密服务。

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 密钥对采用了符合国家密码主管部门要求的硬件密码模块来产生、管理、保存、备份和恢复。安信 CA 制定了规范化管理办法，会通过物理、逻辑等控制方式实现私钥的保护，订户应按照与安信 CA 签署的协议内容妥善保管订户私钥。

6.2.2 私钥多人控制（m 选 n）

安信 CA 密钥的生成、更新、撤销、备份、恢复等操作采用多人控制机制。管理密钥分割保存在三张 IC 卡中由三位经过授权的安全员管理，三人中至少二人同时控制激活、使用、停止私钥。

6.2.3 私钥托管

安信 CA 不会把根 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。

安信 CA 和密钥管理中心均不对订户签名私钥进行托管。

6.2.4 私钥备份

安信 CA 私钥由加密机产生，有备份加密机，对加密机的备份操作 3 人以上才可完成。

订户加密私钥由吉林省密钥管理中心（KMC）负责备份至数据库供以后恢复及查询使用。订户的签名私钥安信 CA 和 KMC 都不进行保存和备份

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 密钥对保存期为 10 年。归档后的 CA 密钥形成历史信息链。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。

订户密钥由 KMC 按照国家密钥主管部门的要求归档保存，归档保存期限不小于 5 年。

6.2.6 私钥导入、导出密码模块

安信 CA 的 CA 密钥对在硬件加密模块中生成并在其中使用。安信 CA 有备份加密设备。CA 私钥从一个密码设备份到另外的设备的全过程必须由安信 CA 授权的多位可信人员同时操作，并且采取相应的技术手段确保密钥传输中的安全。

安信 CA 不提供订户私钥从硬件密码模块中导出的方法，也不允许此操作。

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

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 2 of3 的机制对其访问加以控制，因此需要使用 CA 私钥时，持有 CA 私钥激活数据分割的人员必须按照要求共同完成。

订户使用 USBKey、智能卡等密码设备存放私钥。使用私钥前，订户须安装私钥存储设备的驱动程序，将密码设备插入相应的读取设备中并输入口令，才能激活私钥进行使用。

安信 CA 签发的服务器证书，私钥由服务程序产生和保存，私钥存放在服务程序的软件密码模块中，订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。

6.2.9 解除私钥激活状态的方法

密钥管理员多半数以上密钥管理员同时使用管理员卡登录密码机，可以进行密钥解除激活操作。

安信 CA 签发的订户证书私钥，在订户退出登录状态、驱动程序关闭、或关闭计算机时，私钥激活状态解除。

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接触私钥激活

状态。

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，安信 CA 将会把 CA 私钥连同其备份、与其相关的操作卡片销毁。 销毁过程需要多个信任人员的参与。

订户加密私钥经授权后由吉林省密钥管理中心负责归档及销毁，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。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 密钥存储所用的密码模块均经过国家密码管理部门的许可，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面

6.3.1 公钥归档

安信 CA 对于有效期满的 CA 以及订户的公钥进行定期归档处理。

公钥归档的保存期限，保存机制，安全措施等与证书保持一致。

6.3.2 证书操作期和密钥对使用期限

证书的操作期在证书期满或被撤销时结束，除特殊声明的情况，CA 和订户可以在使用期限内使用原有密钥更新证书，最长使用期限如下：

1. RSA2048 位根证书和 SM2-256 位根证书，其密钥对的最长使用年限是 30 年
2. RSA1024 位根证书，其密钥对的最长允许使用年限是 25 年
3. 其他 CA 证书，其密钥对的最长允许使用年限是 15 年
4. RSA1024 位订户证书，其密钥对的最长允许使用年限是 6 年
5. RSA2048 位订户证书，其密钥对的最长允许使用年限是 10 年

6. SM2-256 位订户证书，其密钥对的最长允许使用年限是 10 年

所有订户证书的有效期和其对应的密钥对的有效期都是一致的

6.4 激活数据

6.4.1 激活数据的产生和安装

安信 CA 用来保护含有 CA 私钥的激活数据要根据本 CPS 和密钥产生规则的要求产生。安信 CA 的私钥激活数据被分割成多个秘密共享分别存放在多个 USBKey 中，其产生和分发会被记录。

订户使用口令来激活他们用于存储私钥的介质（如 USB key），初始下载安信 CA 提供初始口令，随后口令由订户自己设置，安信 CA 不负责管理这些口令。

云应用证书使用订户终端授权的方式来激活证书私钥。

6.4.2 激活数据的保护

CA 私钥激活数据，安信 CA 按照可靠方式分割后由不同可信人员掌管。

订户应妥善管理好自己的口令，防止泄露和窃取。应该经常对激活数据进行修改。

云应用证书需要妥善管理好订户终端的授权数据。

6.4.3 激活数据的其他方面

只有在拥有证书介质并知道口令时才能激活证书存储介质使用私钥

只有在拥有订户终端设备并知道授权数据时才能激活云端证书使用私钥

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 按照工信部《电子认证服务管理办法》等法律法规制定出全面、完善的安全管理策略和制度，在运营进行实施、审查和记录，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控制。

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。安信 CA 部署在多级网络且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。

安信 CA 系统使用至少有一定字符长度并结合字母和特殊字符的口令并且口令要定期更换。

6.5.2 计算机安全评估

安信 CA 的核心操作软件满足相关的国际标准，相关技术满足信息技术以及安全技术评估标准，系统的安全策略要符合安全保障需求。通过了国家密码管理局等部门的有关评估、审查。

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安全保密约定以保证系统的权威性与可靠性。其开发过程符合国家密码主管部门的相关要求。

6.6.2 安全管理控制

安信 CA 认证系统安全管理遵循国家密码局有关运行管理规范进行操作，安信 CA 制定安全管理策略、制度以及流程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 根据国际安全标准和行业发展动态，将及时进行软硬件升级以保证 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。安信 CA 建立了有效的定期检查软件完整性的验证机制。

6.7 网络的安全控制

安信 CA 在采用多层防火墙、入侵防护、安全检测、 病毒防范系统，并及时对上述安全措施进行版本更新，保障网络基础设施安全。

6.8 时间戳

安信 CA 系统使用可信时间源保证系统时间的准确性。

安信 CA 可以提供时间戳服务。根据对系统安全管理和控制的需要，安信 CA 会决定是否使用时间戳。根据不同数据对时间的敏感性、严密性和逻辑关系的要求，安信 CA 将确定时间戳服务的有关规范和策略。

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 签发的证书均符合 X.509 证书格式，遵循 RFC5280 标准。

7.1.1 版本号

安信 CA 所签发证书的版本号 X.509 V3、X.509 V4,信息存放在证书版本属性栏内。

7.1.2 证书扩展项

- 证书版本号（Version）

X.509　V3、X.509　V4

- 证书序列号（**SerialNumber**）

安信 CA 分配给证书的唯一的数字表示符。

- 签名算法标识符(Signature)

符合国家密码主管部门批准的算法对象表示符。

- 颁发机构密钥标识符（**Authority Key Identifier**）

此字段标识用于识别与安信 CA 证书签名私钥相对应的公钥，用来辨别安信 CA 使用的不同密钥。

- 主题密钥标识符（**Subject Key Identifier**）

此字段标识了订户证书被认证的公钥，它能够区分同一主体使用的不同密钥（如证书密钥更新时）。

- 签名算法标识符（**Signature algorithm identifier**）

安信 CA 签发的的 RSA 算法数字证书采用 sha1RSA sha256RSA 签名算法，国产 SM2 算法数字证书采用 SM3_SM2 签名算法。

- 密钥用法（**Key Usage**）

此字段指示已认证的公钥有何种用途如电子签名、密钥加密、数据加密、不可抵赖等等。

- 基本限制（**BasicConstraints**）

用于鉴别证书持有者身份，如 CA 证书等。

- 增强型密钥用法（**Extended Key Usage**）

指明公钥的多种用途，对密钥用法中指明的基本用途的补充或替代，如：服务器验证、客户端验证、代码签名、安全电子邮件、时间戳、智能卡登录

- CRL 分布点（CRL Distrabution Point）

CRL 分布点包含可以获取 CRL 的地址和协议，用于依赖方验证证书状态。

- 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国标扩展项：

1.2.86.11.7.1　（旧国标）1.2.156.10260.4.1.1（新国标）个人身份标识号

1.2.86.11.7.2　（旧国标）1.2.156.10260.4.1.2（新国标）个人社会保险号

1.2.86.11.7.3　（旧国标）1.2.156.10260.4.1.4（新国标）组织机构代码号

1.2.86.11.7.4　（旧国标）1.2.156.10260.4.1.3（新国标）工商注册号

1.2.86.11.7.5　（旧国标）1.2.156.10260.4.1.1（新国标）企业国税号/地税号

针对特别的订户，安信 CA 签发的证书有可能包含私有扩展项，根据不同项目私有扩展项不同。

7.1.3 名称形式

安信 CA 发放的所有证书都包含唯一的符合 X.509 标准证书签发者名称，同时也包含唯一的证书主体订户名称。

7.1.4 名称限制

订户证书的命名一定要有意义，可以通过名称明确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

照一定的规则为订户指定特殊名称，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。

7.2 证书吊销列表

7.2.1 版本号

安信 CA 定期签发 CRL（证书吊销列表），其所签发的 CRL 遵循 RFC5280 标准。采用 X.509 V2 格式。

7.2.2CRL 和 CRL 条目扩展项

version： CRL 版本号

signature：用于签发 CRL 的数字签名

issuer：签发者名称

this Update：这次签发时间

next Update：下次签发时间

revoked Certificates：被注销的证书信息包括序列号和吊销日期

7.3 在线证书状态协议

安信 CA 为证书订户提供 OCSP（在线证书状态查询服务），OCSP 为 CRL 的有效补充，方便证书订户及时查询证书状态信息。安信 CA OCSP 服务遵循 RFC2560 标准。

7.4 根证书体系要求

安信 CA 根证书体系分成三级结构，第一级根为国家根（CN = ROOTCA,O = NRCAC,C = CN），第二级根为安信 CA 根（CN = AnXin SM2 CA,O = AnXin CA,C = CN），第三级根为下级子 CA 根（CN = NMG SM2 CA,O = NMG CA,C = CN）。

8 认证机构审计和其他评估

8.1 评估的频率和情形

按照《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》等规定，安信 CA 定期进行内审和外审。

内部审计是安信 CA 对中心内部和注册机构的审计工作，结果供安信 CA 机构改进、完善业务。每年进行一次。

安信 CA 还按照规定接受行业主管部门的定期评估和检查。

8.2 评估者的资质

安信 CA 的内部审计工作是由具备以下条件的专业人士完成。包括精通 PKI 技术、信息安全工具和技术、拥有参与 CA 应用的经历、了解安全审计的责任等。

内部审计人员选择一般包括：

1. CA 的安全负责人及安全管理人员
2. CA 业务负责人
3. 人事负责人
4. 其他需要的人员

8.3 评估者与被评估者之间的关系

安信 CA 对中心内部及下属分支机构的审计工作由安信 CA 管理层指定的内部人员或第三方机构执行。评估者与被评估者之间应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

评估内容包括不限于以下方面：

1. 人事审查
2. 技术风险审查

3. 安全运营管理检查
4. 信息安全管理制度审查
5. 物理环境风险评估检查
6. 客户服务及证书处理流程审查

8.5 对问题与不足采取的措施

安信 CA 在审计过程中发现的任何错误和不足将会及时提交到安全策略委员会，根据审计报告内容准备一份解决方案，并明确对此采取的行动。安信 CA 将根据法律、法规迅速解决问题。

8.6 评估结果的传达与发布

当安信 CA 接受行业主管部门审查评估后，评估结果由行业主管部门向公众发布。

安信 CA 内部审计后，审计结果在公司内部进行传达。

9 法律责任和其他业务条款

9.1 费用

安信 CA 在公司网站上公布数字证书的服务与收费的标准和相关信息，数字证书的服务与收费将坚持订户自愿的原则，即“按需选择，按项收费”；在证书有效期内，订户有义务向安信 CA 接续交纳证书的使用服务费。

9.1.1 证书签发和更新费用

安信 CA 根据市场需求情况和相关管理部门的规定向机构内的证书订户收取费用，安信 CA 可在不高于收费标准的前提下针对不同订户群体推出不同的收费策略或优惠措施。

如果安信 CA 签署的协议中指明的价格和安信 CA 公布的价格不一致，以协议中的价格为准。

9.1.2 证书查询费用

在证书有效期内，对安信 CA 证书订户的证书信息查询，安信 CA 不收取查询费用，但保留对此项服务收取费用的权利。

9.1.3 证书注销或状态信息的查询费用

查询证书是否注销，安信 CA 不收取查询费用。但保留对此项服务收取费用的权利。

对于使用在线证书状态查询（OCSP）的费用，由安信 CA 与依赖方或订户在协议中约定。

9.1.4 其他服务费用

安信 CA 可根据请求者的要求，定制各类服务，具体服务费用，在与订户签订的协议中约定。

9.1.5 退款策略

安信 CA 在证书操作和签发过程中坚持并且严格遵守相关的实施规范。如果由于某种原因导致订户对证书不满意，订户可以在证书签发后 30 天内要求安信 CA 注销证书并返回相应的退款。

如订户使用证书超过 30 天，订户可以因停止证书的使用提出注销证书和索取退款。安信 CA 将会根据订户使用证书的时间段来收取证书的服务费用，其余的服务费退还给订户。

9.2 财务责任

9.2.1 保险范围

安信 CA 保证其具有维持其运作和履行其责任的财务能力，能够承担对订户、依赖方等造成的责任风险，并依据 CPS 规定，进行赔偿担保。

9.2.2 其他财产

暂无规定。

9.2.3 对终端实体的保险或担保范围

如果安信 CA 根据司法判定须承担赔偿和（或）补偿责任的，安信 CA 将按照相关仲裁机构的裁定或法院的判决承担相应的赔偿责任。

9.3 业务信息保密

9.3.1 保密信息范围

保密信息包括但不限于以下内容：

1. 安信 CA 与订户之间的协议、资料中未公开的内容等属于保密信息。除法律明文规定或政府、执法机关等要求，安信 CA 承诺不对外公布或透露订户证书信息以外的任何其他隐私信息。

2. 订户私钥属于机密信息，订户应当根据本 CPS 的规定妥善保管，如因订户自己泄露私钥造成的损失，由此引起的后果订户应当自行承担。

9.3.2 不属于保密的信息

以下为安信 CA 对外发布的非机密信息类型：

1. 安信 CA 签发的证书和 CRL 中的信息不保密。
2. 安信 CA 证书策略中信息不保密。
3. 本 CPS 的信息不保密，根据 CA 证书策略要求，只有订户方可使用，包括交叉认证的 CA 域内的订户。
4. 其他可以通过公共、公开渠道获取的信息。

9.2.3 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，也都有义务按照本 CPS 的规定，承担相应的保护保密信息的责任。

1、安信 CA： 安信 CA 制定了各种严格的安全管理策略、流程和技术手段来保护自身的商业秘密和订户信息。负责接收和保存保密信息的人员均为安信 CA 授权的可信人员，这些可信人员有责任在接收到保密信息后保护保密信息的安全，防止其泄露、避免使用和发布给第三方。

2、订户：当证书信息的所有者出于某种原因，要求安信 CA 公开或披露其所拥有的保密信息时，安信 CA 可以满足其要求；同时，安信 CA 将要求该保密信息的所有者对这种申请进行书面授权，以表示其自身的公开或者披露的意愿。如果这种披露保密信息的行为涉及任何其他方的赔偿义务，安信 CA 不应承担任何与此相关的或由于公开保密信息所造成的损失。保密信息的所有者应承担与此相关的或由于公开保密信息引起的所有赔偿责任。

3、例外原则：当安信 CA 在任何法律、法规或者法院以及其他权力部门通过合法程序的要求下，必须披露本 CPS 中规定的保密信息时，安信 CA 可以按照法律、法规或法规条令以及法院判决的要求，向执法部门公布相关的保密信息。安信 CA 无须承担任何责任。这种披露不能被视为违反了保密要求和义务。

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权，个人隐私信息保护遵循现行法律和政策规定，任何订户选择使用安信 CA 的证书服务时，就表明已经接受安信 CA 的隐私保护制度。

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相关信息时，除了证书中已经包括的信息外，该订户的基本信息和身份认证资料将被作为隐私处理，非经订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：证书订户持有的证书中的信息，以及该证书的状态信息等。

9.4.4 保护隐私的责任

安信 CA、注册机构、订户、依赖方等机构或个人有义务遵照本 CPS 规定，承担相应的隐私保护责任。在法律法规或公共权力部门通过合法程序要求下，安信 CA 可以向特定的对象公布隐私信息，安信 CA 无需承担责任。

9.4.5 依法律或行政程序的信息披露

当安信 CA 在法律、规章或法规条款的要求下，或在法院的要求下必须披露本 CPS 中具有保密性质的信息时，安信 CA 可以按照法律、法规、或法规条令以及法院判决的要求，向执法部门公布相关的保密信息。安信 CA 无需承担任何责任。这种披露不能视为违反了保密的要求和义务。

9.4.6 其他信息披露形式

安信 CA、订户、注册机构、依赖方等机构或个人都有义务遵循本 CPS 的规定，承担相应的隐私保护责任。当保密信息所有者出于某种原因要求安信 CA 公开或披露其所拥有的保密信息或法律法规、相关权利部门通过合法程序的要求下，安信 CA 可以向特定对象公布隐私信息，安信 CA 无需承担由此造成的任何责任。

9.5 知识产权

安信 CA 享有并保留对证书以及安信 CA 提供的全部软件的一切知识产权，包括（所有权、名称权、利益分享权等）。安信 CA 网站上公布的一切信息均为安信 CA 所有，他人不能转载用于商业行为。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

电子认证服务机构在提供电子认证服务活动中遵循如下承诺：

1. 电子认证服务机构遵守《中华人民共和国电子签名法》及相关法律规定，接受行业主管部门的领导，安信 CA 对所签发的数字证书承担相应的法律责任。
2. 电子认证服务机构保证所使用的系统及密码符合国家政策与标准，保证 CA 本身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策和标准的规定。
3. 安信 CA 的运营遵守本 CPS 规定并随着业务的调整对 CPS 进行修订。
4. 电子认证服务机构签发给订户的证书符合本机构的 CPS 的所有实质性要求。

9.6.2 注册机构的陈述与担保

注册机构在参与电子认证服务活动中遵循如下承诺：

1. 提供给证书订户的注册过程符合电子认证服务机构的 CPS 的所有实质性要求。
2. 注册机构在批准证书前，完成了所有必要的鉴别与确认工作，并且需确认的信息是正确的、准确的。

3. 注册机构将按照本 CPS 的规定，及时向电子认证服务机构提交证书申请、吊销、更新等服务请求。
4. 注册机构应当对订户的信息及与认证相关的信息妥善保存，并于适当的时间转交给安信 CA 归档保存。
5. 注册机构应当根据相关协议内容配合安信 CA 进行必要的电子认证业务合规性审计。

9.6.3 订户的陈述与担保

安信 CA 的证书订户应该保证：

1. 订户确认已经阅读和了解了 CPS 及有关规定的全部内容，并愿意接受本 CPS 文件规定的约束。
2. 订户在申请数字证书时，应当提供真实、完整、有效和准确的信息与资料，并在这些信息资料发生变化时及时通知安信 CA 或其授权的注册机构。
3. 订户应当妥善保管私钥，采取安全的措施防止证书私钥的遗失、泄露和被篡改的事件发生，订户对使用私钥的行为负责。
4. 一旦发生任何可能导致安全性危害的事件，如遗失私钥、遗忘、泄露等情况，订户应立即通知安信 CA 及其授权注册机构，申请采取吊销等保护措施。
5. 若要求更改证书或证书申请的信息，则应及时通知安信 CA 及其授权注册机构；并且应通过证书策略允许的安全传递方式亲自发送通知。
6. 使用证书的行为应符合全部使用的法律法规及相关规定。

9.6.4 依赖方的陈述与担保

1. 依赖方必须熟悉本 CPS 的条款和订户数字证书相关的证书策略，并遵守本 CPS 中的所有规定。
2. 确定证书在规定的范围和期限内使用证书。
3. 获取并安装该证书对应的证书链。
4. 在信赖证书所证明的信任关系前确认该证书记载的内容与所要证明的内容一致。

9.7 担保免责

如有以下情况，应当免除 CA 机构之责任。

1. 证书申请人或订户故意或过失提供或未按要求提供不准确、不真实或不完整信息而获得签发的证书，订户在使用该证书时产生的任何纠纷，证书申请人或订户自行承担全部法律责任，安信 CA 对此不承担任何责任。
2. 由于非安信 CA 原因造成的设备故障、网络中的导致的事故所造成的损失，损失方可以追究侵权方责任，安信 CA 应当予以配合，但安信 CA 不向任何方承担赔偿或补偿责任。
3. 数字证书超出使用范围或以非预期的方式使用，安信 CA 不向任何方承担赔偿或补偿责任。
4. 由于不可抗力，如战争、自然灾害等造成的服务中断并由此造成的客户损失，安信 CA 不承担相应的责任。

9.8 有限责任

安信 CA 应承担的责任和业务包括：

1. 保证其使用和发放的公钥算法在现有技术条件下不会被攻破；
2. 保证安信 CA 及其授权的注册机构的私钥被安全的存放和保护；
3. 安信 CA 建立和执行的安全机制符合国家政策的规定。

除上述责任外，安信 CA 及其授权的注册机构和相关的信任人员不承担其他任何义务。

9.9 赔偿

9.9.1 赔偿范围

安信 CA 的赔偿范围：

1. 由于安信 CA 的原因，订户证书的签发过程没有按照本 CPS 的要求，导致订户证书签发有误；
2. 由于安信 CA 操作人员的疏忽，导致订户证书内信息有误并造成订户损失；

3. 安信 CA 的 CA 私钥丢失或泄密。

注册机构的赔偿范围：

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

订户的赔偿范围：

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，导致的一切后果由订户承担；
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：

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

当安信 CA 违反了本 CPS9.8 中的责任要求时，安信 CA 承担赔偿责任（法律免责除外）。安信 CA 所有的赔偿义务不得高于证书的赔偿上限，这种上限由安信 CA 依据国家相关法律要求进行调整，并对外公布。

依赖方和证书订户在使用或信赖证书时，若有任何行为或疏漏而致使安信 CA 及其授权注册机构产生损失，依赖方和证书订户应承担赔偿的责任、相应的损失及诉讼等费用。安信 CA 及其授权的注册机构有权要求赔偿。

当一个证书应证书订户的代理人要求被签发后，代理人和证书订户两者负有联带责任。如出现 9.9.1 中所述的责任，他们共同承担赔偿责任。证书持有者有责任就代理人所作任何不实陈述与遗漏通知安信 CA 及其授权注册机构。

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

自新版本的 CPS 正式对外发布生效时，上一版本的 CPS 效力将自动终止。

当安信 CA 中止电子认证服务时，本 CPS 自动终止。

9.11 修订

9.11.1 修订程序

本 CPS 的修改和更新，由安信 CA 安全策略委员会负责，并组织 CPS 编写小组进行修改更新。修改完成之后，经安全策略委员会审核、批准，通过后方可对外发布。

9.11.2 通知机制和期限

安信 CA 将在公司官方网站（http://www.anxinca.com）中公布最新版本的 CPS，安信 CA 有权修订本 CPS 中的任何术语、条款。事前无需通知任何一方。新版本的 CPS 自发布之日起生效。

9.11.3 必须修改业务规则的情形

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；当某些认证服务行业相关标准出台或更新时；当认证系统和有关管理规范发生重大升级或改变时；安信 CA 会视具体情况按照相关规定更改本 CPS 的部分内容。

9.12 争议处理

安信 CA 与订户或授权注册机构产生争议时，首先应遵循相应的协议进行协调，如需要诉诸法律，则处理办法依照国家的相关法律。

9.13 管辖法律

本 CPS 的编写依照《中华人民共和国电子签名法》和《电子认证服务管理办法》之规定，并受其管辖。

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。