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 V5.0





吉林省安信电子认证服务有限公司

2026 年 06 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
V4.4	2024.04.07	安信CA安全策略委员会
V4.5	2024.11.21	安信CA安全策略委员会
V4.6	2025.12.30	安信CA安全策略委员会
V5.0	2025.06.30	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		
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	
V4.4变更记录		

第二章	2.4增加信息告知
V4.5变更记录	
全文	修订云应用证书相关的管理规则
V4.6变更记录	
第五章	5.2.4修改了需要职责分割的角色 5.7.4增加了灾难发生后的系统恢复时间
V5.0变更记录	
全文	按照《T/CQAE 11034-2025 电子认证业务规则规范》进行全文修改

目 录

1. 概括性描述 1

1.1. 承诺 1

1.2. 基本信息 1

1.2.1. 机构资质 2

1.2.2. 证书链 3

1.3. 文档名称与标识 4

1.3.1. 名称 4

1.3.2. 版本 5

1.3.3. 历史版本 5

1.3.4. 证书策略 OID 6

1.4. 电子认证活动参与者 7

1.4.1. 电子认证服务机构 7

1.4.2. 注册机构 7

1.4.3. 订户 7

1.4.4. 依赖方 7

1.4.5. 其他参与者 7

1.5. 证书应用 8

1.5.1. 证书应用分类 8

1.5.2. 证书应用限制 9

1.6. 策略管理 10

1.6.1. 策略管理机构 10

1.6.2. 策略文档的批准程序 10

1.7. 定义和缩写 12

1.7.1. 定义 12

1.7.2. 缩写 15

2. 信息发布与信息管理 16

2.1. 信息发布 16

2.2. 信息更新 16

2.3. 监管备案 16

2.4. 证书信息对接 16

3. 身份标识与查验 17

3.1. 身份查验通用要求 17
3.1.1. 通用要求 17
3.1.2. 订户告知 17
3.2. 初始身份确认 18
3.2.1. 证明拥有私钥的方法 18
3.2.2. 个人身份的查验 18
3.2.3. 机构身份的查验 19
3.3. 订户意愿记录 20
3.3.1. 订户意愿记录内容 20
3.3.2. 个人高等级证书的意愿记录 20
3.3.3. 个人基础级证书的意愿记录 20
3.3.4. 机构高等级证书的意愿记录 21
3.3.5. 机构基础级证书的意愿记录 21
3.4. 订户协议 21
3.5. 未验证的订户信息 22
3.6. 互操作要求 22
3.7. 命名 22

4. 证书生存周期操作要求 23

4.1. 通用要求 23
4.2. 证书申请 23
4.2.1. 处理流程 23
4.2.2. 处理期限 24
4.3. 证书签发 24
4.3.1. 签发过程 24
4.3.2. 结果通告 24
4.4. 证书接受 25
4.5. 密钥对和证书的使用 25
4.5.1. 交付前的安全保护 25
4.5.2. 私钥管理服务要求 25
4.5.3. 安全事件反馈 26
4.6. 证书续期 26

4.6.1. 证书续期的情形 26
4.6.2. 申请主体 26
4.6.3. 身份查验方式 26
4.6.4. 证书签发与接受 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. 申请主体 27
4.7.3. 身份查验方式 27
4.7.4. 证书签发与接受 27
4.8. 证书变更 28
4.8.1. 证书变更的情形 28
4.8.2. 申请主体 28
4.8.3. 身份查验方式 28
4.8.4. 证书签发与接受 28
4.9. 证书撤销或冻结 28
4.9.1. 证书撤销 28
4.9.2. 证书冻结 29
4.9.3. 申请主体 30
4.9.4. 申请渠道与事件记录 30
4.10. 证书状态信息服务 30
4.11. 停止使用认证服务 31
4.11.1. 停止订户服务的情形 31
4.11.2. 处理停止服务请求的时限和方式 31
4.11.3. 停止服务后的责任条款 32
4.11.4. 记录操作过程 32
4.12. 密钥托管与恢复 32

5. 认证机构设施、管理和操作控制 32

5.1. 物理控制 32
5.1.1. 基础设施 32
5.1.2. 分区管理与访问控制 34
5.1.3. 电力保障 34
5.1.4. 门禁与监控 35
5.1.5. 灾备 35

5.1.6. 环境保障措施 35
5.1.7. 消防措施 36
5.1.8. 设备管理 36
5.1.9. 存储媒体管理 36
5.2. 操作过程控制 37
5.2.1. 可信角色 37
5.2.2. 职责分离 37
5.3. 人员控制 38
5.3.1. 可信人员资格要求 38
5.3.2. 可信人员培训要求 38
5.4. 审计日志程序 39
5.4.1. 记录范围 39
5.4.2. 记录内容 39
5.4.3. 保存期限 39
5.4.4. 日志审计内容 40
5.4.5. 审计周期 40
5.5. 记录归档 40
5.5.1. 归档范围 40
5.5.2. 保存期限 40
5.5.3. 保护措施 40
5.5.4. 归档管理 41
5.6. 电子认证服务机构根密钥更替 41
5.6.1. 密钥更替程序 41
5.6.2. 密钥更替的时间 41
5.7. 损害与灾难恢复 41
5.7.1. 业务连续性目标 42
5.7.2. 恢复流程 42
5.7.3. 根私钥应急处理 44
5.7.4. 事件报告 44
5.7.5. 定期验证 45
5.8. 电子认证服务机构终止 45
5.9. 重大事项报告 45
5.9.1. 重大事件范围 45
5.9.2. 重大事件报告流程 46

5.9.3. 报告时限与内容 47

6. 认证系统技术安全控制 47

6.1. 技术安全管理制度要求 47
6.2. 密钥对的生成和安装 48
6.2.1. 根证书密钥对的生成和安装 48
6.2.2. 订户密钥对的生成和交付 48
6.3. 私钥保护和密码模块工程控制 48
6.3.1. CA 私钥保护和密码模块工程控制 48
6.3.2. 订户私钥保护和密码模块工程控制 49
6.4. 密钥对管理的其他方面 49
6.4.1. 公钥归档 49
6.4.2. 证书操作期和密钥对使用期限 49
6.5. 激活数据 49
6.5.1. 激活数据的产生和安装 49
6.5.2. 激活数据的保护 50
6.5.3. 激活数据的其他方面 50
6.6. 计算机安全控制 50
6.7. 生存周期安全控制 50
6.8. 网络安全控制 51
6.9. 时间戳 51

7. 证书、证书撤销列表和在线证书状态协议 51

7.1. 证书 51
7.2. 证书撤销列表 52
7.3. 在线证书状态协议 52

8. 认证机构审计及相关评估 52

8.1. 审计评估制度 52
8.2. 认证业务审计 52
8.3. 全面符合性评估 53

9. 法律责任和其他业务条款 53

9.1. 费用 53
9.2. 财务责任 53
9.3. 业务信息保密 54
9.3.1. 保密信息范围 54
9.3.2. 不属于保密的信息 54
9.4. 个人隐私保护 54
9.4.1. 隐私保密方案 55
9.4.2. 作为隐私处理的信息 55
9.4.3. 不被视为隐私的信息 55
9.4.4. 用户个人信息的收集 55
9.4.5. 个人信息的存储 56
9.4.6. 用户个人信息的使用 56
9.4.7. 用户个人信息的共享 56
9.4.8. 个人信息的管理 56
9.4.9. 个人信息的查阅 57
9.4.10. 个人信息的删除和更改 57
9.5. 知识产权 57
9.6. 陈述和担保 57
9.6.1. 电子认证服务机构的陈述与担保 57
9.6.2. 注册机构的陈述与担保 58
9.6.3. 订户的陈述与担保 58
9.6.4. 依赖方的陈述与担保 59
9.6.5. 其他参与者的陈述与担保 59
9.7. 担保免责 59
9.8. 偿付责任规则 60
9.9. 赔偿 60
9.10. 有效期和终止 60
9.10.1. 有效期限 60
9.10.2. 终止 61
9.11. 对参与者的个别通告与沟通 61
9.12. 修订和发布 61
9.12.1. 修订程序 61
9.12.2. 通知机制和期限 61
9.12.3. 必须修改业务规则的情形 61

9.13. 争议处理与举证 62
9.13.1. 争议解决程序 62
9.13.2. 举证制度与能力体系 62
9.14. 管辖法律 62
9.15. 与适用法律的符合性 63
9.16. 一般条款 63
9.17. 其他条款 63

1. 概括性描述

1.1. 承诺

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）郑重承诺：在电子认证经营与服务的全过程中，严格遵守国家相关法律及行政法规，牢固树立以人民为中心的服务理念，主动履行企业社会责任。在与客户建立业务关系前，全面开展应用业务调研，健全完善应用接入业务的风险评估及内部定责管理机制，严禁为存在违法违规风险的业务提供任何电子认证服务；严格选用经国家密码管理局审查通过的电子认证服务系统，依规开展电子认证服务；自觉接受政府及社会公众监督，对主管部门检查督导发现的问题第一时间落实整改，建立健全问题纠治长效管理机制，常态化规范运营，持续保持合规经营与服务标准。

1.2. 基本信息

安信 CA 成立于 2002 年 7 月，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，是专业从事跨行业、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。

安信 CA 严格遵循《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》等法律法规，按照中华人民共和国工业和信息化部、国家密码管理局等主管部门的各项要求，向包括政府机构、企事业单位和个人在内的公众提供电子认证服务。

安信 CA 的基本信息如下：

机构全称：吉林省安信电子认证服务有限公司；

法定代表人：张智勇

机构住所：吉林省长春市高新区光谷大街 1300 号正元大厦 18 楼；

联系方式：0431-85177688；

邮箱：anxinca@anxinca.com。

1.2.1.机构资质

1. 《电子认证服务许可证》

证书编号：ECP22010420005

发证机关：中华人民共和国工业和信息化部

批准日期：2005 年 8 月 19 日

有效期：2020 年 8 月 19 日至 2025 年 8 月 18 日

2. 《电子认证服务使用密码许可证》

证书编号：0007

发证机关：国家密码管理局

批准日期：2005 年 5 月 20 日

有效期：2025 年 3 月 1 日至 2030 年 2 月 28 日；

3. 《电子政务电子认证服务机构资质证书》

证书编号：ZWRZ-2220100010

发证机关：国家密码管理局

批准日期：2010 年 10 月 28 日

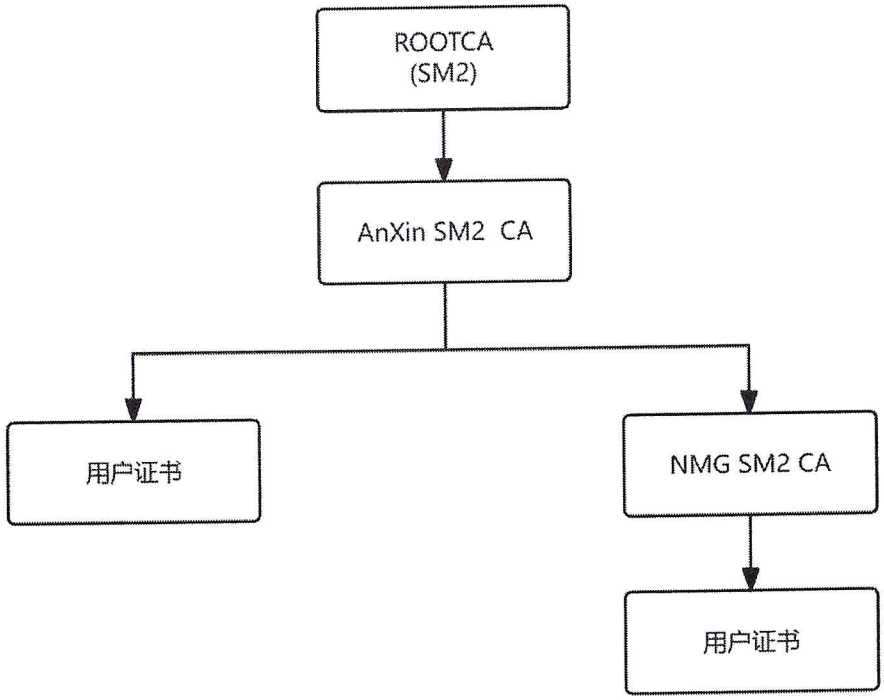
有效期：2025 年 06 月 03 日至 2030 年 06 月 02 日；

1.2.2.证书链

安信 CA 当前运行两套并行的数字证书体系，各体系证书链结构如下：

1. 国密算法根证书体系（主用体系）

采用三级证书链架构：顶层为 ROOTCA，由其签发 AnXin SM2 CA；该 CA 承担双签发职能，一是直接向终端用户签发 SM2 算法用户证书，二是签发 NMG SM2 CA，再由 NMG SM2 CA 向其覆盖范围内的终端用户签发 SM2 算法用户证书。



ROOTCA 根证书 DN 主题为 CN=ROOTCA,O=NRCAC,C=CN，证书编号为 69e2fec0170ac67b，颁发机构为国家密码管理局（CN=ROOTCA,O=NRCAC,C=CN），密码算法为 SM2，密钥长度为 256bit，该证书将于 2042 年 7 月 7 日到期。

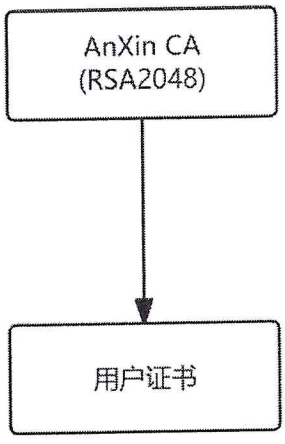
AnXin SM2 CA 根证书 DN 主题为 CN=AnXin SM2 CA,O=AnXin CA,C=CN，证书编号 76756e291181250671eac079853625dc，颁发者 CN=ROOTCA,O=NRCAC,C=CN，密钥算法 SM2，密钥长度 256bit，有效期 2013 年 08 月 09 日至 2033 年 08 月 04 日，计划服务时间 18 年。

NMG SM2 CA 根证书 DN 主题为 CN = NMG SM2 CA,O = NMG CA,C = CN，证书

编号 73e70a73831702bb84af24a9b007b1fe，颁发者 CN = AnXin SM2 CA，O = AnXin CA，C = CN，密钥算法 SM2，密钥长度 256bit，有效期 2016 年 03 月 25 日至 2033 年 06 月 24 日，计划服务时间 15 年。

2. RSA2048 算法根证书体系

采用两级证书链架构：顶层为 AnXin CA（RSA2048 根证书），由其直接向终端用户签发 RSA2048 算法用户证书。



AnXin CA 根证书 DN 主题为 CN=AnXin CA,O=AnXin CA,C=CN，证书编号 72ed0343717e1ed36071486c51a9030f，颁发者 CN=AnXin CA,O=AnXin CA,C=CN，密钥算法 RSA，密钥长度 2048bit，有效期 2016 年 10 月 27 日至 2046 年 10 月 20 日，计划服务时间 20 年。

1.3. 文档名称与标识

1.3.1. 名称

本文档的名称为《吉林省安信电子认证服务有限公司电子认证业务规则》，是吉林省安信电子认证服务有限公司对所提供的第三方认证服务及相关业务的全面描述。

1.3.2.版本

本电子认证业务规则（CPS）版本号为5.0，发布日期为2026年06月30日。

本CPS将会根据安信CA第三方认证业务的发展更新。电子认证业务规则（CPS）后应注明版本信息（如 “1.0 版本”或 “CPS1.0”）。

1.3.3.历史版本

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
V4.4	2024.04.07	安信CA安全策略委员会
V4.5	2024.11.21	安信CA安全策略委员会
V4.6	2025.12.30	安信CA安全策略委员会
V5.0	2025.06.30	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	
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
V4.4变更记录	
第二章	2.4增加信息告知
V4.5变更记录	
全文	修订云应用证书相关的管理规则
V4.6变更记录	
第五章	5.2.4修改了需要职责分割的角色 5.7.4增加了灾难发生后的系统恢复时间
V5.0变更记录	
全文	按照《T/CQAE 11034-2025 电子认证业务规则规范》进行全文修改

1.3.4.证书策略 OID

安信 CA 证书策略 OID 是指安信 CA 在 http://www.china-oid.org.cn 官方网站注册的 OID 号。

OID	说明
1.2.156.112537.1.1	《吉林省安信电子认证服务有限公司电子认证服务证书策略（安信 CA CP）文档标识》
1.2.156.112537.1.2	《吉林省安信电子认证服务有限公司电子认证服务业务规则（安信 CA CPS）文档标识》

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》和《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

安信 CA 的数字证书注册机构是经安信 CA 的业务分支机构，包括证书注册审核（RA）中心、证书本地受理点（LRA）等，是为安信 CA 的证书申请者办理注册流程的实体。注册机构和受理点有责任妥善保存客户的信息，不允许将客户信息透露给与证书申请无关的任何单位或个人，不允许用作商业利益方面的用途。

注册机构必须获得安信 CA 的授权。注册机构不得进行证书用户信息身份核验工作。

1.4.3.订户

安信 CA 颁发的证书的证书主体，在不同的阶段，也称为证书申请人、证书持有人。属于《中华人民共和国电子签名法》中电子签名人的一种类型。

1.4.4.依赖方

是指基于对电子签名认证证书或电子签名的信赖，从事相关活动的实体。

1.4.5.其他参与者

是指为安信 CA 的电子认证服务活动提供相关服务的其他实体。

1.5. 证书应用

1.5.1. 证书应用分类

1.5.1.1. 电子签名证书

按证书主体对象的类型和风险等级，电子签名认证证书可分为个人高等级电子签名认证证书、个人基础级电子签名认证证书、机构高等级电子签名认证证书、机构基础级电子签名认证证书四种类型。

1. 个人高等级电子签名认证证书

证书类型：个人高等级电子签名认证证书；

主管部门证书策略 OID：2.16.156.339.2.1.1.2；

证书特点：适用于高风险业务、符合《电子签名法》的个人电子签名认证证书；

应用场景：涉及生命健康、财产权益等高风险活动，且非证书应用限制场景的个人电子签名业务。

2. 个人基础级电子签名认证证书

证书类型：个人基础级电子签名认证证书；

主管部门证书策略 OID：2.16.156.339.2.1.1.1；

证书特点：适用于低风险业务、符合《电子签名法》的个人电子签名认证证书；

应用场景：涉及生命健康、财产权益等高风险活动之外的，且非证书应用限制场景的个人电子签名业务。

3. 机构高等级电子签名认证证书

证书类型：机构高等级电子签名认证证书；

主管部门证书策略 OID：2.16.156.339.2.1.2.2；

证书特点：适用于高风险业务、符合《电子签名法》的机构电子签名认证证书；

应用场景：涉及生命健康、财产权益等高风险活动，且非证书应用限制场景的机构电子签名业务。

4. 机构基础级电子签名认证证书

证书类型：机构基础级电子签名认证证书；

主管部门证书策略 OID：2.16.156.339.2.1.2.1；

证书特点：适用于低风险业务、符合《电子签名法》的个人电子签名认证证书；

应用场景：涉及生命健康、财产权益等高风险活动之外的，且非证书应用限制场景的机构电子签名业务。

1.5.1.2. 其他类型证书

安信 CA 发放的其他类型证书包括：为服务器或设备颁发的数字证书，用以代表服务器或设备身份的真实性，如：服务器身份证书、SSL 服务器证书、IPSec VPN 设备证书等；代码签名证书，用于代码防篡改；加密证书用于文件加密、邮件加密、传输加密。以上类型证书不属于电子签名认证证书，不适用于电子签名，安全级别为基础级。

1.5.2.证书应用限制

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。

安信 CA 签发的证书，禁止在下列场景中使用，包括但不限于：

1. 涉及人身关系的，如婚姻、收养、继承等；
2. 涉及公共事业服务停止的，如停止供水、供热、供气等；
3. 法律、行政法规规定的其他不适用电子签名的应用场景或类型；
4. 国家法律法规禁止的活动；
5. 涉及金融、医疗等有关人民生命、财产安全关系的活动中使用基础级电子签名认证证书的。

1.6. 策略管理

1.6.1. 策略管理机构

1.6.1.1. 组成

安信 CA 安全策略委员会（以下简称“安策委”）是《吉林省安信电子认证服务有限公司电子认证业务规则》（CPS）的最高管理机构。安策委由以下成员构成：

主任委员：由总经理担任；

副主任委员：由副总经理担任；

委员：由各部门负责人组成；

1.6.1.2. 职责

安全策略委员会负责 CPS 和 CP 以及配套制度的维护，包括但不限于以下职责：

1. 确定维护 CPS 和 CP 等策略文档的职能分工，建立合理有效的修订和批准流程；
2. 对涉及信息安全策略、根证书密钥、证书签发自动审核等重要操作和流程进行审批；
3. 每年至少进行一次 CPS 和 CP 全面评审，根据实际需要及时修订策略文档；
4. 每年组织运营风险评估并形成报告；
5. 妥善保存安全策略委员会重大决议的相关文件和会议记录。

1.6.2. 策略文档的批准程序

安信 CA 的 CPS 由安信 CA 安全策略委员会指定的专人或编写组起草拟定后，提交安信 CA 安全管理委员会审核。如需变更，由指定的专人或编写组提交变更报告并完成修改，安信 CA 安全策略委员会将对变更建议进行研究分析，征询法律顾问意见后形成最终决议。决议形成后，安信 CA 将在网站公布变更后的《吉林省安信电子认证服务有限公司电子认证业务规则》正式文档。

1.6.2.1. 起草小组的成立流程

安信 CA 信息策略管理体系规范文档由安全策略委员会负责起草或组织起草。

负责起草的部门应当确定一名熟悉相关内容员工为项目负责人，如涉及多个部门时，可由有关部门共同派人组成联合起草小组，由主要起草部门负责牵头组织。

1.6.2.2. 安全策略委员会的审批流程

报送审查的管理制度送审稿应当由起草部门负责人签署后报安全策略委员会审查。几个部门共同起草的规范送审稿，应当由起草部门负责人共同签署后报安全策略委员会审查。

下列材料应当与规范送审稿一并报送安全策略委员会审查：

1. 起草说明。
2. 与此规范内容有关的规范性文件。
3. 汇总的各方意见。
4. 如需制定实施细则，应当提交实施细则的主要内容和实施细则拟出台的时间。
5. 其他需要报送的材料。

安全策略委员会主要从以下方面对送审稿进行审查：

1. 是否符合权限和程序。
2. 是否符合原则。
3. 是否与其他规范相协调、衔接。
4. 是否已对有关不同意见进行协调。
5. 是否具有可行性。
6. 是否符合相关技术要求。
7. 需要审查的其他内容。

由安全策略委员会对送审稿提出审查结论，对草案涉及的有关争议问题以及修改情况作重点说明。由安全策略委员会负责人签署的书面审查报告应当反馈起草部门。

评审工作每年至少举行一次，发生以下情况时，也需要启动管理评审工作：

1. 系统业务发生重大变更。
2. 系统信息安全策略的重大变更。
3. 目前安全管理制度体系的执行不力。
4. 系统安全管理制度体系的范围发生变更。
5. 相关标准法规发布修订版本或有变更。
6. 评审工作的会议记录均需归档，以保存正式的记录。

1.6.2.3. 向主管机关的备案流程

本 CPS 原则上每年至少修订一次。若内容无变更，仅递增版本编号，并同步更新发布时间、生效时间及修订记录。修订完成的 CPS，须在对外发布之日起 30 日内，向工业和信息化部完成备案。

1.6.2.4. 发布流程

规范草案经安全策略委员会审议并原则通过后，由起草部门根据审议提出的修改意见对草案进行修订完善。修订后的草案经安全策略委员会负责人签发后，以安信 CA 管理制度规范正式文本的形式对外发布。

1.7. 定义和缩写

1.7.1.定义

下列术语和定义适用于本文件。

1. 加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。

2. 密码模块 cryptographic module

实现密码运算功能的，相对独立的软件、硬件、固件或这三者组合。

3. 密码算法 cryptographic algorithm

描述密码处理过程的算法。

4. 密钥 key

控制密码变换操作的符号序列。

5. 私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。

6. 公钥 public key

非对称密码算法中可公开的密钥。

7. RSA 算法 RSA algorithm

一种基于大整数因子分解问题的公钥密码算法。

8. SM2 算法 SM2 algorithm

由 GB/T 32918 定义的一种椭圆曲线公钥密码算法。

9. SM3 算法 SM3 algorithm

由 GB/T 32905 定义的一种密码杂凑算法。

10. 公钥基础设施 public key infrastructure (PKI)

基于公钥密码技术，具有普适性，可用于提供机密性，完整性、真实性及抗抵赖性等安全服务的基础设施。

11. 数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

12. 电子认证服务机构 certification service provider

取得电子认证服务许可证，为需要第三方认证的电子签名，签发电子签名认证证书并为有关各方提供真实性、可靠性验证的实体。

13. 数字证书 digital certificate

也称公钥证书，是由证书认证机构签名的包含公开密钥拥有者信息、公开密钥、签

发者信息、有效期以及扩展信息的一种数据结构。

14. 电子签名认证证书 electronic signature certificate

由依据《中华人民共和国电子签名法》设立的电子认证服务机构签发的，可证实电子签名人与电子签名制作数据有联系的数字证书。

15. 电子签名依赖方 electronic signature relying party

是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人。

16. 订户 subscriber

被颁发给一张证书的证书主体。[来源：GB/T 26855-2011, 3.15]

17. 对象标识符 object identifier (OID)

用于无歧义地标识对象的全局唯一值。

18. 证书策略 certificate policy

指明证书对于具有普通安全需求的特定团体和/或应用类的适用性的规则集合。

19. 证书策略对象标识符 CP OID

对某个证书策略文档进行唯一标识的 OID。

20. 证书链 certificate chain

证书链是一个用于证书验证的证书序列。

21. 身份查验 entity authentication

证实某个实体就是所声称身份的过程。

22. 激活数据 activation data

用于使密码模块进入可操作状态的数据。可为口令、生物特征等。

23. 时间戳 time stamp (TS)

对时间和其他待签名数据进行签名得到的数据，用于表明数据时间属性的数据。

24. 证书续期 certificate renewal

指在不改变订户信息的情况下，用一个新证书来代替旧证书的过程。

25. 密钥更新 key re-key

用一个新密钥来代替旧密钥的过程。

26. 密钥恢复 key recovery

将归档或备份的密钥恢复到可用状态的过程。

27. 证书撤销列表 certificate revocation list (CRL)

由电子认证服务机构签发并发布的被撤销证书的列表。

28. 证书认证系统 CA system

对数字证书的申请、签发、发布、更新、撤销、验证等数字证书全生命周期进行管理和服务的系统。

29. 高等级电子签名认证证书 enhanced electronic signature certificate

适用于金融、医疗等涉及公民生命、财产安全领域的电子签名认证证书。

30. 基础级电子签名认证证书 qualified electronic signature certificate

适用于除高等级证书规定场景外的其他电子签名场景的证书。

1.7.2.缩写

下列缩略语适用于本文件。

1. CA：电子认证服务机构（Certification Authority）
2. CPS：电子认证业务规则（Certification Practice Statement）
3. CP：证书策略（Certificate Policy）
4. CRL：证书撤销列表（Certificate Revocation List）
5. DN：甄别名称（Distinguished Name）
6. LDAP：轻量级目录访问协议（Lightweight Directory Access Protocol）
7. OCSP：在线证书状态协议（Online Certificate Status Protocol）
8. OID：对象标识符（Object Identifier）
9. RTO：恢复时间目标（Recovery Time Objective）
10. RPO：恢复点目标（Recovery Point Objective）

2. 信息发布与信息管理

2.1. 信息发布

安信 CA 通过官方网站（www.anxinca.com）公布以下信息：CP、CPS 的最新版本及历史版本、《吉林省安信电子认证服务有限公司电子认证服务协议》；证书链，在线证书状态服务或证书撤销列表等证书状态信息；详细的业务办理指南，服务网点地址、营业时间、联系电话；依赖方协议；投诉处理部门的地址、联系电话、电子邮件地址，以及内部监督部门名称。

2.2. 信息更新

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。

网站公告、安信 CA 的 CPS、证书应用情况、协议流程等信息若发生变化，应在变化生效后一个工作日内完成更新。

2.3. 监管备案

安信 CA 按照国家电子认证服务管理平台的要求进行相关备案工作。

2.4. 证书信息对接

安信 CA 按照国家电子认证服务管理平台的要求进行技术对接，实现根据证书唯一编码、订户身份信息等维度查询本机构已签发证书列表的功能。

3. 身份标识与查验

3.1. 身份查验通用要求

3.1.1. 通用要求

安信 CA 在受理订户证书申请前，对订户本人和/或受托人履行告知义务、完成身份信息核验、留存其真实申请意愿相关记录和电子认证服务协议签署记录。

身份查验相关义务由安信 CA 自行履行，不委托给外部机构或个人。

3.1.2. 订户告知

3.1.2.1. 告知内容

安信 CA 订户申请证书时需告知以下内容：

1. 订户的权利与义务；
2. 服务收费的项目及标准；
3. 电子签名认证证书与电子签名的使用条件；
4. 信息安全保障措施；
5. CA 与订户的责任划分；
6. 订户签名私钥的存储方式及安全要求；
7. 订户不得将所获证书用于任何违法违规、违背公序良俗的用途，不得利用证书从事侵害国家利益、社会公共利益及第三方合法权益的活动。

3.1.2.2. 告知方式

安信 CA 对不同类型的证书采用不同的告知方式：

1. 高等级证书采用面对面、电话、视频或主管部门认可的其他方式之一进行告知，并保留告知记录。
2. 基础级证书采用高等级证书的告知方式，或采用强制阅读、短信、邮件等方式

之一进行告知；并保留告知的记录。

3.2. 初始身份确认

3.2.1. 证明拥有私钥的方法

安信 CA 按照本 CPS 6.2.2 规定的方式生成订户密钥对。证书订户通过数字签名的方式来确认其拥有公钥对应的签名私钥。

3.2.2. 个人身份的查验

3.2.2.1. 个人身份信息有效性的确认

安信 CA 在受理个人证书申请时，对个人身份信息查验方式及核心要求如下：

1. 安信 CA 在受理个人数字证书申请时，要求订户出示本人有效身份证件，或提供真实完整的有效身份证件信息；证件类型须为国家法律法规及相关政策文件规定的合法有效身份证件，不符合规定的证件类型不予接受；
2. 为确保订户身份信息的真实性与有效性，安信 CA 将通过专用证件机读设备核验订户出示的身份证件有效性，或通过国家权威身份信息数据库查验订户提交的身份资料；
3. 当订户委托他人代办时，安信 CA 将查验订户本人签署的有效书面授权证明，要求受托人出示其有效身份证件或提供有效身份证件信息，并按照 2 款规定的方式核验订户与受托人的身份证件或身份资料。

3.2.2.2. 个人高等级证书的实人查验

安信 CA 对申请个人高等级证书的订户开展实人查验时，可采用以下方式之一：面对面查验、远程人工面对面查验、生物特征验证，或主管部门认可的其他方式。

安信 CA 通过可追溯的方式完整记录并保存身份查验过程和结果，为每张证书建立独立的身份验证记录。

3.2.2.3. 个人基础级证书的实人查验

安信 CA 对申请个人基础级证书的订户开展实人查验时，可采用以下方式之一：本 CPS 3.2.2.2 规定的方式、电信运营商三要素验证、银行卡四要素验证、申请人持有的有效电子签名认证证书签名验证，或主管部门认可的其他方式。

安信 CA 通过可追溯的方式完整记录并保存身份查验过程和结果，为每张证书建立独立的身份验证记录。

3.2.3.机构身份的查验

3.2.3.1. 机构身份信息有效性的确认

安信 CA 在受理机构证书申请时，对机构身份信息查验方式及内容：

1. 安信 CA 在受理机构数字证书申请时，要求订户出示本机构及办理人的有效证件，或提供真实、完整的有效证件信息；证件类型须为国家法律法规及相关政策文件规定的合法有效证件，不符合规定的证件类型不予接受；
2. 法定代表人或受托人的身份查验方式参见本 CPS 3.2.2.1；若由受托人办理，安信 CA 将查验机构加盖公章的有效书面授权证明。

3.2.3.2. 机构高等级证书的实人查验

安信 CA 在对申请机构高等级证书的订户办理人进行实人查验时，将采用以下方式之一：

1. 法定代表人实人查验，具体方法参见本 CPS 3.2.2.2；
2. 受托人实人查验，具体方法参见本 CPS 3.2.2.2，且需通过机构对公账户随机金额打款验证或主管部门认可的其他方式。

安信 CA 通过可追溯的方式完整记录并保存身份查验过程和结果，为每张证书建立独立的身份验证记录。

3.2.3.3. 机构基础级证书的实人查验

安信 CA 对申请机构基础级证书的订户办理人开展实人查验时，将采用以下方式之一：

1. 法定代表人实人查验，方法见本 CPS 3.2.2.3；
2. 受托人实人查验，方法见本 CPS 3.2.2.3；
3. 通过订户持有的同等级或更高级有效机构证书进行签名验证。

安信 CA 通过可追溯的方式完整记录并保存身份查验过程和结果，为每张证书建立独立的身份验证记录。

3.3. 订户意愿记录

3.3.1.订户意愿记录内容

订户在申请和使用安信 CA 数字证书及电子签名服务前，须完成意愿确认。意愿记录内容包括但不限于：订户身份信息、CA 机构信息、签名私钥保存方及其保存义务、订户对电子签名的法律责任，以及订户对上述内容已充分知晓并同意的明确意愿表示。

3.3.2.个人高等级证书的意愿记录

安信 CA 对申请个人高等级证书的订户意愿确认，采用以下方式之一：

1. 现场办理时，通过面对面确认或手抄提示语的方式确认订户意愿，并通过录音录像或经主管部门安全性评估的其他方式记录；
2. 远程办理时，通过音视频或经主管部门安全性评估的其他方式确认并记录订户意愿。

安信 CA 将保留完整、可追溯的订户意愿记录。

3.3.3.个人基础级证书的意愿记录

安信 CA 对申请个人基础级证书的订户意愿确认，采用以下方式之一：与高等级证书相同的方式，具体方法见本 CPS 3.2.2.3；采用强制阅读、短信或邮件确认等电子方式。

安信 CA 将保留完整、可追溯的订户意愿记录。

3.3.4.机构高等级证书的意愿记录

安信 CA 对申请机构高等级证书的订户意愿的确认采用下列方式之一：

1. 法定代表人申请：安信 CA 将按照本 CPS 3.3.2 规定的方式确认机构法定代表人的意愿。
2. 受托人申请：安信 CA 将查验加盖机构公章的授权文件，并按照本 CPS 3.3.2 规定的方式确认受托人的意愿。

安信 CA 会对订户意愿确认进行全程录音录像，完整记录并保存订户的意愿确认方式、意愿确认时间及意愿确认结果等信息。统一归档留存，全程可查询、可追溯。

3.3.5.机构基础级证书的意愿记录

安信 CA 对申请机构基础级证书的订户意愿的确认采用下列方式之一：

1. 法定代表人申请：安信 CA 将按照本 CPS 3.3.3 规定的方式确认机构法定代表人的意愿。
2. 受托人申请：安信 CA 将查验加盖机构公章的授权文件，并按照本 CPS 3.3.3 规定的方式确认受托人的意愿。

安信 CA 会完整记录并保存订户的意愿确认方式、意愿确认时间及意愿确认结果等信息。统一归档留存，全程可查询、可追溯。

3.4. 订户协议

安信 CA 应与用户签订电子认证服务协议，协议包括以下内容：

1. 订户的权利与义务；
2. 服务收费的项目及标准；
3. 电子签名认证证书与电子签名的使用条件；
4. 信息安全保障措施；
5. CA 与订户的责任划分；

6. 订户签名私钥的存储方式及安全要求；
7. 订户不得将所获证书用于任何违法违规、违背公序良俗的用途，不得利用证书从事侵害国家利益、社会公共利益及第三方合法权益的活动。

3.5. 未验证的订户信息

安信 CA 执行统一的证书信息查验方法与标准化查验流程，针对订户提交的各类资料信息开展核验工作，查验范围包括但不限于订户证件号码、地址、电子邮箱等附加信息。

安信 CA 签发的证书不能包含任何未核查、未验证的订户信息。

3.6. 互操作要求

涉及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。如果国家法律法规对此有规定，安信 CA 将严格予以执行。

3.7. 命名

安信 CA 证书主体甄别名称（DN）的命名规则，包括但不限于：

1. 针对个人和机构等不同类型的证书，分别约定其命名规则；
2. 确保命名具有实际意义，且能追溯到唯一实体的方法：

- 个人证书：主体 DN 项中包含订户姓名，在 DN 项或扩展项中包含有效证件类型及其编号（或这些信息的某种映射，包括但不限于编号的散列值、掩码等）；
- 机构证书：主体 DN 项中包含机构名称，在 DN 项或扩展项中包含组织机构的有效证件类型及其编号。

3. 对证书名称中商标权的处理策略和方式，妥善处理商标名及其风险；
4. 不影响证书通用性的前提下，可在证书中增加自定义的其他内容；
5. DN 项结构定义符合 GB/T 16264.8 的要求，证书主体 DN 项编码规则见下表。

代码	说明	示例
C	国家	CN
S	省份（可选）	北京
L	城市（可选）	北京
O	订户所在机构信息（可选）	xx 公司
OU	订户所在机构部门信息（可选）	xx 部门
CN	订户名称（个人姓名或机构法定名称）	张三 /xx 公司

4. 证书生存周期操作要求

4.1. 通用要求

安信 CA 负责证书注册通道的建设、运营及维护，覆盖线上平台与线下网点。通过常态化运维、安全加固、权限管控及日志审计等措施，保障注册通道安全、稳定、合规运行。

安信 CA 依据《中华人民共和国电子签名法》《商用密码管理条例》《电子认证服务使用密码管理办法》等法规，制定安信 CA 电子认证服务协议。在证书签发前，安信 CA 需向订户告知协议内容，明确双方权利义务与责任范围，同时查验订户身份并确认其申请证书的真实意愿。安信 CA 应妥善保存相关记录。

订户应对其提交的注册资料、身份信息、主体信息等材料的真实性、准确性和完整性负责，不得伪造、篡改或隐瞒相关信息。因信息虚假、失效或未及时更新导致证书异常、使用风险及相关法律损失的，由订户自行承担全部责任。

4.2. 证书申请

4.2.1. 处理流程

1. 订户可以通过现场面对面方式或在线方式提交证书申请请求。
2. 安信 CA 在接受订户申请前，需按照本 CPS 3.1.2 所描述的内容对订户进行告知，且要求订户提供本 CPS 3.2 中所述的有效身份证明材料及相关申请文件，

并根据本 CPS 3.3 中所描述的方法确认申请意愿，且与安信 CA 签订电子认证服务协议。

3. 安信 CA 审核订户的申请；若审核通过为订户签发证书，若审核失败拒绝订户证书申请，并告知失败原因。

4.2.2.处理期限

安信 CA 在收到证书请求后的合理时间内启动证书申请处理流程。若订户提交的申请资料齐全，安信 CA 将在两个工作日内完成证书申请处理；若遇特殊情况，可适当延长处理时间。

4.3. 证书签发

4.3.1.签发过程

在证书签发过程中，RA 管理员负责证书申请的审批，并通过操作 RA 系统向 CA 证书签发系统发送证书签发请求。RA 向 CA 发送的证书签发请求信息须采取 RA 身份鉴别与信息保密措施，确保请求准确发送至指定的 CA 证书签发系统。

CA 证书签发系统在收到 RA 的证书签发请求后，将对来自 RA 的信息进行鉴别与解密；对于有效请求，系统将签发订户证书。

安信 CA 在批准证书申请后，将签发证书。证书签发即表示电子认证服务机构最终正式批准该证书申请。

4.3.2.结果通告

证书申请处理完毕后，安信 CA 将通过以下方式之一向订户通告处理结果：

1. 通过认证应用工具进行信息提示；
2. 通过信函、站内信或电子邮件发送；
3. 通过短信通知；
4. 通过电话通知；

5. 当面通知或通过实时视频等相当于面对面的方式通知；
6. 通过主管部门认可的其他方式。

4.4. 证书接受

安信 CA 证书交付、接受与拒绝的规则如下：

1. 安信 CA 及注册机构通过面对面、邮寄或电子方式向订户交付数字证书，自订户获得证书并完成签收确认时起，即视为其已接受证书；若订户拒绝签收，则视为拒绝接受证书。
2. 通过网络下载证书的，证书下载的系统记录表明用户已经接受证书，三十天内未下载证书，则视为拒绝接受证书。
3. 对于云端协同证书，安信 CA 将证书发送到终端模块或云平台后，即视为已经接受证书，用户在两个工作日内提出拒绝，则视为拒绝接受证书。
4. 安信 CA 也可以通过其他安全的方式交付数字证书。
5. 安信 CA 完整保存订户接受证书的所有记录，包括接受时间、方式、操作人等。

4.5. 密钥对和证书的使用

安信 CA 建立了严格的密钥对和证书使用安全管理体系，确保密钥生成、传输、存储及使用全过程的安全可控，保护订户合法权益。

4.5.1. 交付前的安全保护

安信 CA 将密钥对交付订户保管前，采取以下安全措施：

1. 签名私钥采用经国家密码管理部门核准的商用密码产品及算法生成，生成过程在安全可控的环境中进行，且通过安全加密方式保障私钥传输安全。
2. 安信 CA 将拒绝为不符合国家或行业安全标准要求的情况颁发证书。

4.5.2. 私钥管理服务要求

安信 CA 为订户提供的签名私钥管理服务，遵循以下管理与技术要求：

1. 未经订户书面授权，不保存且不委托第三方保存其签名私钥；

2. 机构签名私钥的使用，必须由法定代表人或受托人作为唯一授权主体；
3. 仅在获得订户明确授权情况下使用其签名私钥；
4. 签名私钥以加密形成存储，且存储条件符合安全标准；
5. 对所有涉及签名私钥的操作，均保留完整且可追溯的记录。

4.5.3.安全事件反馈

安信 CA 建立了便捷的外部安全事件反馈渠道，通过官方网站、客服热线、电子邮件及线下服务网点等方式，及时受理和处理证书信息错误、私钥失密、证书被盗用或冒用等异常情况，并按照应急响应预案进行处置。

4.6. 证书续期

4.6.1.证书续期的情形

证书续期指在不改变证书中订户信息的情况下，在原证书到期前，为订户签发新证书。证书续期的情形包括：

1. 原证书有效期即将届满；
2. 订户主体身份信息未发生任何变更；
3. 原证书未被吊销、冻结或撤销；
4. 订户未违反本认证业务声明及相关服务协议约定。

4.6.2.申请主体

证书续期的申请人须为证书订户本人或其合法受托人。受托人提出申请时，需同时提交本人有效身份证明文件及订户出具的授权委托书。

4.6.3.身份查验方式

安信 CA 处理续期请求时，按以下规则进行身份查验：

1. 自申请人上次完成身份查验之日起至本次续期申请日未满三年的，可通过原证书进行电子签名验证的方式确认身份；

2. 上述期限已满三年的，应按照本 CPS 3.2 的规定重新进行完整身份查验。

4.6.4.证书签发与接受

证书续期的签发流程遵循本 CPS 4.3 规定，证书接受流程遵循本 CPS 4.4 规定。

4.7.证书密钥更新

4.7.1.证书密钥更新的情形

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。证书密钥更新的情形包括：

1. 当订户证书即将到期或已经到期时；
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. 其他可能导致密钥更新的情形。

4.7.2.申请主体

证书密钥更新的申请人须为证书订户本人或其合法受托人。受托人提出申请时，需同时提交本人有效身份证明文件及订户出具的授权委托书。

4.7.3.身份查验方式

安信 CA 处理密钥更新请求时，按以下规则进行身份查验：

1. 自申请人上次完成身份查验之日起至本次密钥更新申请日未满三年的，可通过原证书进行电子签名验证的方式确认身份；
2. 上述期限已满三年的，应按照本 CPS 3.2 的规定重新进行完整身份查验。

4.7.4.证书签发与接受

证书的签发流程遵循本 CPS 4.3 规定，证书接受流程遵循本 CPS 4.4 规定。

4.8. 证书变更

4.8.1. 证书变更的情形

证书变更是指改变证书中除订户公钥之外的信息而签发新证书。

4.8.2. 申请主体

证书变更的申请人须为证书订户本人或其合法受托人。受托人提出申请时，需同时提交本人有效身份证明文件及订户出具的授权委托书。

4.8.3. 身份查验方式

安信 CA 处理变更请求时，按以下规则进行身份查验：

1. 按照本 CPS 3.2 的规定，对申请人的身份进行严格查验；
2. 发起方不是证书订户，安信 CA 需取得订户同意。

4.8.4. 证书签发与接受

证书的签发流程遵循本 CPS 4.3 规定，证书接受流程遵循本 CPS 4.4 规定。

4.9. 证书撤销或冻结

4.9.1. 证书撤销

4.9.1.1. 证书撤销的情形

发生以下情形时，可执行证书撤销操作：

1. 与证书公钥对应的私钥泄密，或订户怀疑自身密钥泄密；
2. 证书不再用于原用途，且密钥未失密，订户要求中止使用证书；
3. 未收到证书更新费用；
4. 订户未能履行本电子认证业务规则，或其他协议、法律法规规定的责任义务；

5. 订户申请初始注册时提供不实材料；
6. 有证据证明证书被盗用、冒用、伪造或者篡改；
7. 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；
8. 其他因法律或政策要求，安信 CA 需采取的临时撤销措施；
9. 订户申请撤销证书时注明的其他原因。

4.9.1.2. 证书撤销的流程

1. 证书订户（或者其授权的委托代理人）填写书面申请表并签字盖章，向安信 CA 提交撤销申请，同时提供合法证明材料。
2. 安信 CA 收到撤销申请后，验证申请者的身份、权限以及撤销理由的正当性，对审核资料进行书面归档，验证无误后作出撤销决定并及时处理。若因条件限制无法完成现场审核，安信 CA 将先冻结证书使其暂时失效，待完成身份鉴别后，再办理证书撤销手续。
3. 安信 CA 将在 24 小时内把证书撤销信息发布至信息库与目录服务，供公众查询。

4.9.2.证书冻结

4.9.2.1. 证书冻结的情形

发生以下情况，安信 CA 将会考虑冻结证书：

1. 订户要求暂停使用该证书；
2. 订户未能履行与安信 CA 签订的协议中应尽的责任；
3. 除订户（或者其授权的委托代理人）外的其它实体，如电子认证服务机构及其授权的服务机构、国家法律部门、政府主管部门及其他公共权力部门，向安信 CA 提出冻结证书请求并获得批准。

4.9.2.2. 证书冻结和解冻的流程

1. 证书订户（或者其授权委托代理人）填写书面申请表并签字盖章，向安信 CA 提交冻结申请，同时提交合法证明材料，说明冻结理由。除证书订户外的其他

实体，如安信 CA 的授权机构、国家法律部门、政府公共权力部门等，提出证书冻结请求，也需按规定填写申请表并提交证明材料。

2. 安信 CA 收到冻结申请后，验证申请者的身份、权限以及冻结理由的正当性，并对审核资料进行书面归档，验证确认无误后作出冻结决定并及时处理。
3. 安信 CA 将在 24 小时内把证书冻结信息发布到信息库和目录服务，供公众查询。

如订户需要解冻，需按相关法律法规提交证明材料，证明该证书恢复至合法原始状态后，安信 CA 方可按照规定程序办理解冻手续。证书冻结的最长期限不得超过证书本身的有效期，若超过有效期且用户未提出恢复申请，该证书将被自动注销。

4.9.3. 申请主体

申请证书撤销或冻结的实体可为订户或其合法受托人；此外，当依赖方判断存在本 CPS 4.9.1 所述可能导致订户证书被动撤销的情形时，可向 CA 机构提交证书申请。

4.9.4. 申请渠道与事件记录

本机构为申请人提供以下便捷的证书撤销或冻结申请渠道：

1. 服务热线：0431-85177688；
2. 电子邮箱：anxinca@anxinca.com；
3. 安信 CA 线下服务窗口。

安信 CA 对所有涉及证书或私钥安全的事件进行详细记录，记录内容包括但不限于：事件发生时间、地点、涉及的证书序列号、事件类型（密钥遗失、密钥泄露、主体变更、违规使用等）、事件描述、申请人信息、处理措施及结果。并对所有撤销或冻结请求进行身份与权限验证，确保申请为合法主体。

4.10. 证书状态信息服务

安信 CA 通过 LDAP、OCSP 及 CRL 提供证书状态查询服务，订户可通过此类服务了解证书状态。安信 CA 提供 7×24 小时证书状态查询服务，服务可用率不低于 99%，

响应时间不超过 10 秒。若上述查询服务失效，订户可通过安信 CA 服务热线、邮箱等渠道获取证书状态信息。

4.11. 停止使用认证服务

4.11.1. 停止订户服务的情形

安信 CA 停止向订户提供认证服务的情形分为两类：一是订户主动申请停止，二是本机构单方终止服务。

订户主动申请停止：订户因自身需求向安信 CA 提交有效的停止服务申请，且经安信 CA 审核通过的；

安信 CA 单方终止服务：出现下列情形之一的，安信 CA 有权单方终止向订户提供全部或部分认证服务：

1. 订户证书有效期届满且未在规定时限内完成续期申请的；
2. 订户违反本 CPS 条款、电子认证服务协议或相关法律法规规定的；
3. 订户在证书申请或使用过程中提供虚假、伪造、无效的身份信息或证明材料的；
4. 订户的签名私钥发生泄露、丢失、被冒用或存在其他重大安全风险的；
5. 司法机关、密码管理部门等有权机关依法要求本机构停止向订户提供服务的；
6. 订户主体资格依法终止（如机构注销、自然人死亡等）且无合法权利义务承受人的；
7. 存在其他可能危及电子认证服务安全、公共利益或本机构合法权益的情形的。

4.11.2. 处理停止服务请求的时限和方式

安信 CA 针对停止服务申请实行限时办结制度，严格执行证书撤销、私钥销毁、用户数据处置闭环流程，具体要求如下：

1. 处理时限：对于订户主动提交的停止服务申请，资料齐全、核验无误后 2 个工作日内完成服务终止处置；对于违规、风险类紧急停止服务场景，即刻启动处置流程，当日完成证书冻结及撤销操作。
2. 证书与私钥处置（撤销与销毁）：服务停止后，安信 CA 立即对订户证书执行

证书撤销操作，将证书状态更新为已撤销，并同步推送至证书撤销列表（CRL）及在线证书状态查询（OCSP）服务，对外公示失效状态。

4.11.3. 停止服务后的责任条款

1. 对服务停止前产生的认证服务相关操作，安信 CA 仍按照双方签订的认证服务协议履行相应责任；
2. 订户在服务停止后，仍继续使用已撤销、失效证书进行电子签名或其他密码运算所产生的一切法律责任，由订户自行承担；
3. 因订户违反本 CPS 条款或相关法律法规导致本机构单方终止服务的，由此产生的一切损失及法律责任由订户自行承担。

4.11.4. 记录操作过程

安信 CA 完整记录认证服务终止流程中从申请、审核到执行的全部操作过程，并至少保存至证书失效后五年。

4.12. 密钥托管与恢复

安信 CA 根证书私钥在自身控制的安全环境中保管，不托管给任何第三方机构或个人。安信 CA 已建立根证书密钥备份与恢复策略，对根证书密钥进行安全备份。

5. 认证机构设施、管理和操作控制

5.1. 物理控制

5.1.1. 基础设施

安信 CA 机房位于长春市高新区光谷大街 1300 号正元大厦 5 层，该中心建立在安全可靠的物理环境内，按照以下标准建设：

《数据中心设计规范》（GB 50174-2017）

《数据中心基础设施施工及验收规范》（GB 50462-2015）

《计算机场地通用规范》（GB/T 2887-2011）

《计算机场地安全要求》（GB/T 9361-2011）

屏蔽系统标准和规范

《处理涉密信息的电磁屏蔽室的技术要求和测试方法》（BMB3-2024）

《电磁屏蔽室屏蔽效能的测量方法》（GB12190-2021）

《电磁屏蔽室工程技术规范》（GB/T 50719-2011）

《电磁屏蔽室工程施工及质量验收规范》（GB/T 51103-2015）

装饰系统标准和规范

《防静电活动地板通用规范》（GB/T 36340-2018）

《建筑装饰装修工程质量验收规范》（GB 50210-2018）

《建筑设计防火规范》（GB 50016-2014）

《建筑内部装修设计防火规范》（GB 50222-2017）

电气系统标准和规范

《供配电系统设计规范》（GB 50052-2009）

《低压配电设计规范》（GB 50054-2011）

《建筑照明设计标准》（GB 50034-2013）

《建筑物防雷设计规范》（GB 50057-2010）

弱电系统标准和规范

《综合布线系统工程设计规范》（GB 50311-2016）

《安全防范工程技术规范》（GB 50348-2018）

消防系统标准和规范

《气体灭火系统设计规范》（GB50370-2005）；

《气体灭火系统施工及验收规范》（GB50263-2007）；

《火灾自动报警系统设计规范》（GB50118-2013）；

《火灾自动报警系统施工及验收规范》（GB50166-2007）；

5.1.2.分区管理与访问控制

安信 CA 的物理环境分为四个区域：公共区、管理区、服务区和核心区。公共区为访客接待、人员及物资通行的公共区域，实施基础出入管控；管理区为运维管控专用区域，用于系统监控、设备运维、日志核查、业务配置等管理操作，严格管控人员出入与操作行为；服务区为基础业务与辅助设备运行区域，仅限授权人员进入，落实日常巡检、出入登记及设备安全防护管理；核心区：为最高防护等级区域，专门用于开展密钥生成、证书签发、密钥存储等数字认证高敏感核心操作，仅允许授权核心人员准入，实行最高等级的物理隔离、安防监测与访问管控。

机房核心区和管理区的物理访问实施“双人共管”与“双因素认证”的强制访问控制策略，并记录访问信息。

5.1.3.电力保障

机房在供配电设计满足可靠性、可控性、冗余度、可扩展性等要求。根据数据中心设计对供电方式的要求，配备不间断供电措施，建立不停电配电系统。配电系统的关键设备已采取冗余设计，机房配电系统的任何器件、元件的单点故障，不会影响机房设备的正常供电。

供配电系统的设计从低压配电系统的输入端一直到最终设备的电源输入端，作为一套整体的配电系统考虑设计。

供配电系统包含如下内容：

电力分多级电力保证：双路市电互投+双组智能 UPS 系统。

当双路供电中有一路故障时，系统保证能利用剩余一路供电继续对 UPS 系统进行供电；当双路市电都出现故障，系统保证切换 UPS 系统进行供电。所有切换过程都能够实现自动或手工完成。

安信 CA 机房为三层机房的供配电系统工程，其中包含 UPS 配电、动力配电、双路市电、照明系统（含应急照明系统）、辅助插座、防雷及接地系统工程。

5.1.4.门禁与监控

安信 CA 机房部署门禁管控、红外入侵检测、高清视频监控一体化安防体系，实现机房全域安全监测与准入管控，有效防范非法入侵、违规访问等各类安全风险。机房门禁系统严格执行双人核验机制，采用人脸、密码双因素认证方式，规范人员区域访问行为，严控准入权限。机房全域布设红外入侵报警设备，实现非法闯入行为实时预警、动态监测。高清视频监控系统实行 7×24 小时不间断运行，服务区、管理区、核心区等非公共区域的视频监控记录、门禁访问日志等数据完整留存，保存期限不少于 180 天。安防记录在销毁前，开展专项安全审计形成正式审计报告，统一归档、长期留存。

5.1.5.灾备

安信 CA 建立了异地数据备份中心，采用专用备份软件对关键系统数据、审计日志数据和其他敏感信息每天定期同步备份，异地灾备中心位于山西省太原市，直线距离为 1400 余公里。

5.1.6.环境保障措施

安信 CA 采用精密空调为机房进行温湿度控制，保持相对湿度在 40%—60%范围内，保持温度在 18-28℃范围内。每台精密空调都配置了末端互投配电箱，双路末端进线的配置保证精密空调的不间断运行。双路进线来自不同变压器，箱内 ATS 的设置可帮助其

自动投切，双路市电互为备用，保证设备供电可靠性的同时又避免大功率空调在启动和关闭的时候对其他回路造成冲击。

在机房精密空调下方、冷热通道地板下、水管沿线、机柜底部等易漏水区域，铺设漏水检测绳或安装点式漏水传感器；搭配漏水控制器，支持干接点 / Modbus 协议，可实现漏水点精确定位（定位精度≤1m）。

5.1.7.消防措施

机房消防报警系统核心配套七氟丙烷全淹没灭火系统，分单元独立、组合分配两种装配形式，由火灾探测、灭火控制、气体灭火设备三大核心部分构成，具备自动、电气手动、机械手动三种控制及启动方式，机械应急启动仅作紧急备用。系统通过烟 / 温感探测器探火，经报警控制器联动声光报警、气体灭火控制盘，延时后释放七氟丙烷，借助化学抑制、冷却、窒息三重机理灭火。同时配备专用空气呼吸器或氧气呼吸器。

5.1.8.设备管理

安信 CA 建立完善的机房设备台账管理制度，对机房设备统一建档管理。台账完整登记设备责任人、运行使用状态、维护周期及报废标准等关键信息。同时严格执行设备定期盘点核对机制，常态化开展设备清查核验，及时更新台账信息，确保设备实际情况与台账记录完全一致，实现设备全生命周期规范化、可溯源管理。

5.1.9.存储媒体管理

安信 CA 制定了存储媒体使用与报废管理制度，明确存储媒体使用权限、报废判定标准、安全销毁方式及各环节审批流程。建立全流程登记机制，对存储媒体的领用、归还、报废等行为逐一记录，做到全程留痕、有据可查，实现存储媒体规范化闭环管理。

5.2. 操作过程控制

5.2.1. 可信角色

电子认证服务机构、依赖方等组织中与密钥和证书生命周期管理操作有关的工作人员，都是可信角色，必须由可信人员担任。可信角色包括：

1. 系统管理员：负责系统策略配置、用户与权限管理等；
2. 技术运维员：负责物理环境、网络、服务器及系统软件的日常监控与维护等；
3. 数据库管理员：负责数据库进行日常运维、性能优化及数据备份等；
4. 系统审计员：负责系统和网络日志的审计、管理、审计报告生成等；
5. 密钥管理员：负责根证书密钥材料管理、根证书密钥生命周期管理等；
6. 业务操作员：负责证书申请的受理、审核，订户的身份与意愿签证；
7. 客户档案管理员：负责客户证书相关档案资料的归档与保密等；
8. 运营审计员：负责对客户签发、客户服务等核心业务进行独立

5.2.2. 职责分离

安信 CA 的可信人员遵循职责分离原则，所有涉及关键操作，如密钥管理、审计、鉴证、系统管理的角色应实现双人操作或复核机制；涉及业务连续性相关操作如运维、鉴证、审计等角色按工作量设置人员冗余，在任何一人缺岗时仍能实现双人操作；禁止同一人员掌握可独立完成“发起、审批、执行、审计”全流程的任何组合，以下角色禁止相互兼任：

1. 系统管理员、技术运维员、数据库管理员、系统审计员之间不得兼任；
2. 同一证书业务的录入与审核环节不得由同一业务操作员完成；
3. 业务操作员、客户档案管理员、运营审计员之间不得兼任；
4. 密钥管理员不得与系统管理员、技术运维员兼任；
5. 密钥管理员不宜与除策略管理机构成员外的其他可信角色兼任。

5.3. 人员控制

5.3.1. 可信人员资格要求

安信 CA 对可信角色人员开展背景与资历调查，聘任的可信人员应具备岗位所需的相关工作经验，且无不良记录，具体要求如下：

1. 从业经历调查要求和无犯罪记录；
2. 具备履行岗位职责所必需的专业技能要求；
3. 签署具有法律约束力的保密协议，承诺不得私自保存、复制或泄露电子认证服务的所有秘密或敏感信息；
4. 签署劳动合同。

5.3.2. 可信人员培训要求

安信 CA 建立覆盖所有可信角色的持续培训体系，并规定：

1. 岗前培训：所有可信人员上岗前须完成不少于 20 学时的培训并通过考核；
2. 持续培训：每年至少接受一次培训，每人每年培训时长不少于 20 学时，并通过考核；
3. 培训内容至少包括：
   - ✧ 电子认证服务相关法律法规与标准；
   - ✧ 岗位通用职责要求及各角色特定的工作要求；
   - ✧ 内部管理政策、制度及流程等；
   - ✧ PKI 和密码技术基础知识；
   - ✧ 安信 CA CPS 及 CP；
   - ✧ 安全管理策略和机制；
   - ✧ 订户身份查验和审核策略和流程；
   - ✧ 电子认证服务运营体系构成；
   - ✧ 电子认证服务技术体系构成；
   - ✧ 灾难恢复和业务连续性管理。

5.4. 审计日志程序

5.4.1. 记录范围

安信 CA 持续、完整地记录关键操作与事件，包括但不限于：

1. 根证书密钥操作：包括密钥生成、备份、存储、恢复、归档、销毁，以及密码设备的启用、停用、转移和销毁等；
2. 系统访问行为：包括所有对系统的访问企图，包括成功的和失败的登录、退出、权限使用行为等；
3. 系统操作与变更：包括对系统的各种关键查询、修改、删除等操作，系统组件的安装、升级、维修，以及敏感信息的获取与取阅等；
4. 网络安全事件：包括防火墙、路由器、入侵检测安全设备记录的告警信息，以及针对被攻击事件识别与相应处理过程、结果等；
5. 证书生存周期关键过程：包括记录证书申请、审核、签发、更新、变更、撤销、冻结、恢复等操作，CRL 的签发与发布等，所有操作的通过或拒绝结果均应明确记录；
6. 机房门禁控制等物理环境事件：包括业务人员、安全运维人员、外部人员等在不同安全区域的进出记录等。

5.4.2. 记录内容

安信 CA 对每个事件的记录包含时间、类型、内容、操作人、作用对象及结果。对于系统的关键操作，由操作人员进行电子签名。

5.4.3. 保存期限

安信 CA 的系统日志至少保存至相关证书失效后五年，并实施严格的访问控制以防篡改或删除。

5.4.4.日志审计内容

安信 CA 核实系统和操作人员的合规性包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件。

5.4.5.审计周期

安信 CA 至少每季度对系统日志进行一次审计，形成审计报告，并基于结果采取改进措施。

5.5.记录归档

5.5.1.归档范围

1. 证书申请材料和订户意愿记录；
2. 所有审计日志；
3. 密码设备全生存周期管理记录；
4. 密码设备的日常操作与使用记录；
5. 根证书或密钥生存周期管理相关的全部记录；
6. 证书认证系统运行日志；
7. 已识别的安全事件及处置记录；
8. 证书认证系统关键操作日志；
9. 电子认证服务过程中其他操作记录。

5.5.2.保存期限

安信 CA 保存订户相关档案、系统日志和审计记录至证书失效后五年。

5.5.3.保护措施

安信 CA 对电子归档记录采取技术手段保障其完整性，并存储在安全的物理与数字环境中，建立备份机制。

5.5.4.归档管理

安信 CA 指定运营服务部统一管理归档记录，并配备档案管理员负责电子认证业务记录的归档管理工作。档案管理员的具体职责包括对档案收集、整理、存储、借阅及销毁进行全流程管理，制定标准化的档案归档操作规范，明确各类记录的归档时限、分类标准、存储格式及保管期限要求。同时，安信 CA 建立严格的档案安全管理制度，落实档案存储环境安全、访问权限控制、防篡改、备份与灾备等安全措施，确保归档记录的完整性、保密性与可追溯性。

5.6.电子认证服务机构根密钥更替

5.6.1.密钥更替程序

安信 CA 根证书密钥更替的流程与情形，包括但不限于：

1. 密钥生成：在颁发或更换根证书时，在安全可靠的环境中生成新密钥对，具体见本 CPS 6.6.2；
2. 根证书发布：将新的 CA 公钥证书发布给证书订户和依赖方；
3. 旧密钥处理：在完成签名密钥更替后，按 GB/T 25056-2018 中 8.2.4.3 规定的方式，销毁旧私钥及其备份，并保留相关操作记录。

5.6.2.密钥更替的时间

1. 紧急更替：发现密钥泄露或存在安全隐患，立即启动密钥更替程序；
2. 到期更替：在密钥到期前两年完成密钥更替。

5.7.损害与灾难恢复

当安信 CA 机构遭受攻击，导致通信网络资源损毁、计算机设备系统无法正常服务、软件被破坏或数据库被篡改，或因自然灾害、传染病、政治暴动等不可抗力因素引发运行事故时，将按照灾难恢复计划实施恢复。

5.7.1.业务连续性目标

CA 系统发生故障后，安信 CA 按照灾难恢复计划实施恢复。其中恢复时间目标(RTO)为 48 小时，恢复点目标(RPO)为 24 小时。

5.7.2. 恢复流程

5.7.2.1. 证书库的恢复过程

1. 重建安全运行环境：证书库出现异常后，立即暂停服务、切断业务链路、隔离软硬件设备，防止风险扩散。全面核查服务器、系统、数据库及安全策略，排查隐患并恢复安全基线。依据 CA 规范重新部署系统，完善安全策略，校准系统时间、加密算法与信任链。通过漏洞扫描、渗透测试等方式校验确认安全合规后，启动数据恢复。
2. 生成证书撤销列表：结合故障发生时间、异常日志及操作记录定位受影响证书，核验其签发状态等信息以筛选问题证书；由安全管理员与运维管理员双人复核撤销列表，审核通过后重新生成证书撤销列表（CRL），并正式发布，同步更新至证书查询系统。
3. 订户密钥说明：证书库仅存储订户证书及公钥。
4. 证书更新：安信 CA 将通知订户按照本 CPS 4.7 证书密钥更新要求完成证书更新。

5.7.2.2. 根密钥损害的恢复过程

当安信 CA 的根密钥损害时，将会执行以下程序进行恢复：

1. 重建安全环境：发现根密钥受损后，应立即关停 CA 全部业务及根密钥认证服务，隔离相关设备、封存受损密钥及备份数据，严格管控密钥违规操作。全面排查运行环境、权限设置及操作日志，明确风险范围与安全隐患。重置安全运行环境，整改系统漏洞、优化安全策略、重置权限体系、升级加密防护措施，落实根密钥高等级管控制度。经安全检测验收合格后，启动根密钥重建与证书恢复工作。

2. 重签发订户证书：公示旧根证书作废，批量撤销旧密钥签发的全部证书。在加固环境下，按规范重建根密钥与根证书，完成入根适配及安全审查，搭建全新信任体系。梳理存量信息并制定分批换证方案，通过多渠道通知订户。基于新信任链，依据本 CPS 4.7 证书密钥更新要求，为订户重新签发公钥证书。

5.7.2.3. 其他关键资产恢复过程

1. 物理设施恢复

机房机柜、加密机、电源、安防等物理设施发生故障或损毁时，应第一时间排查故障原因、损坏程度及影响范围，并隔离故障设备。若为轻微故障，可现场维修调试；若设备彻底损毁，则启用备用件替换，优先保障核心 CA 设备、密钥存储及证书服务设备的运行。设备修复或替换后，需完成通电测试、功能调试与安全检测，同步恢复机房供电、温湿度、消防、安防等环境，并排查线路与接地系统隐患，确保机房物理安全。

2. 计算资源恢复

当服务器、虚拟机或集群出现宕机、过载、节点离线等异常时，通过运维监控平台定位故障节点及异常日志。下线并隔离异常节点，重启故障服务；若集群发生故障，启动自愈机制，将核心业务迁移至正常备用节点。修复服务器系统与集群配置，清理异常进程；若资源不足，及时扩容内存与存储。完成后校验算力稳定性、集群同步性及业务承载能力，恢复全量业务运行。

3. 网络环境恢复

针对内外网、专线、防火墙等网络设备及链路出现的中断、入侵、策略失效等问题，应临时关闭异常端口、封禁非法 IP、阻断恶意访问，隔离安全风险。随后修复故障设备与链路连接，还原合规访问策略与路由配置，优化网络防护规则，确保内网隔离、外网可控、专线稳定。最后测试网络连通性、传输稳定性与权限合规性，确认安全后恢复正常业务交互。

4. 软件系统恢复

当 CA 系统、数据库等出现闪退、篡改、瘫痪等故障时，应根据程序漏洞、配置错误、病毒攻击等不同原因分类处置。若为轻微配置异常，可直接还原标准配置；若存在

程序损坏、文件缺失或病毒感染情况，则需彻底清理后通过备份数据进行恢复。修复完成后，需对证书签发、查询、审计等核心功能开展全量测试，确保软件运行稳定、业务功能正常。

5. 业务数据恢复

当证书数据、操作日志、订户信息等发生丢失或篡改时，应首先评估数据损坏范围与恢复难度，采用最近的离线及异地定时备份数据进行恢复；恢复过程中需严格遵循RPO（恢复点目标）、RTO（恢复时间目标）指标，控制恢复时效与数据丢失量，并禁用可疑备份数据。恢复完成后，需核查数据的完整性、准确性与一致性，补录并修正异常数据，确保业务数据完整且可追溯。

5.7.3.根私钥应急处理

安信 CA 发现根私钥泄露后，将依据应急预案在 24 小时内制定根私钥泄露应急处置方案，经安信 CA 安全策略委员会批准后实施。安全策略委员会负责人为应急处置方案实施的第一责任人。实施方案包括但不限于以下步骤：

1. 立即向行业主管部门汇报，并通过公司网站或公共媒体向订户和依赖方进行通告；
2. 撤销所有受影响的订户证书及根证书，更新 CRL 和 OCSP 信息以供订户和依赖方查询；
3. 生成新的根密钥对，签发新的根证书及下级 CA 证书；
4. 新根证书签发完成后，立即通过目录服务器、网站等渠道发布；
5. 新根证书签发后，按照本 CPS 关于证书签发的规定重新签发用户证书。

安信 CA 每年至少开展一次应急演练。

5.7.4.事件报告

见本 CPS 5.9；

5.7.5.定期验证

安信 CA 定期检验备份设备和数据的可用性，包括开展备份恢复测试与功能验证，并每年至少进行一次灾难恢复演练。

5.8.电子认证服务机构终止

安信 CA 因技术性原因或商业原因需要终止服务时的流程和通告机制，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. 安信 CA 起草并发布 CA 终止声明，至少提前九十日通知与证书订户、依赖方等相关实体，至少提前六十日向主管部门报告；
2. 具体资质的电子认证服务业务承接单位，并签署承接协议，明确约定承接机构的工作范围与责任；
3. 向承接方移交密钥及相关关键数据，协调承接单位启动相关运营工作；
4. 停止证书状态服务并归档相关数据；
5. 停止认证中心的服务并归档相关数据；
6. 停止密码设备并归档相关密钥数据；
7. 及时撤销或冻结业务管理员和业务操作员的操作权限；
8. 对所有存档文件记录进行整理和封存；
9. 对所有敏感文档和数据进行安全处理和封存；
10. 清除主机和密码硬件设备中的敏感数据；
11. 其他涉及 CA 运营的数据、密钥安全的操作。

5.9.重大事项报告

5.9.1.重大事件范围

安信 CA 将以下事件定义为重大事件：

1. 证书认证系统迁移或改造：包括系统软件、网络、部署发生的重大变更。符合以下任意之一：
   - ✧ 机房迁移，或机房内服务区、管理区或核心区的规划范围改变；

- ✧ 变更电子签名认证证书的签发逻辑；
- ✧ 新增远程证书注册子系统；
- ✧ 新增、更改或者删除用于签发电子签名认证证书的证书链；
- ✧ 其他对电子认证服务安全、用户资料安全有影响的变更。

2. 重大安全事故：包括电子认证服务系统遭受黑客攻击、病毒入侵、数据泄露等，导致系统无法正常运行或数据安全性受到严重威胁的情形。符合以下任意之一：
   - ✧ 证书签发及验证服务连续停机时间超过 24 小时；
   - ✧ 发生根证书密钥等关键数据泄露；
   - ✧ 出现持续或较大范围未经授权的私钥访问记录或其他异常活动；
   - ✧ 系统日志持续或较大范围显示异常操作（如非授权时间或网络地址访问敏感功能）。
3. 订户信息泄露事件：包括订户身份信息、证书申请资料等敏感数据泄露，符合以下任意之一情形：
   - ✧ 个人信息泄露事件影响范围较广，已造成一定经济损失或引发客户投诉；
   - ✧ 数据丢失导致证书状态信息无法恢复。
4. 合规性事件：包括不符合相关法律法规、标准或监管要求的情形，符合以下任意之一：
   - ✧ 涉及电子认证服务的司法判定；
   - ✧ 收到行政部门出具的违规通知或处罚决定。
5. 人力资源类事件：包括一个月内核心管理层集体离职、大规模劳动纠纷、重大职场安全事件等，符合以下任意之一：
   - ✧ 涉及 2 名及以上管理层人员或 10%以上可信人员离职；
   - ✧ 劳动纠纷参与人数超过员工总数 10%，且经法院或仲裁机构生效裁决确认由 CA 承担法律责任。

5.9.2.重大事件报告流程

任何部门或人员发现重大事件后，须立即向公司安全策略委员会报告。

安全策略委员会需立即对事件性质进行研判与定级，确认事件响应等级，同时启动《安信 CA 应急预案》，通过相应的应急防护措施和恢复手段，将事件影响控制在最小

范围。

5.9.3.报告时限与内容

重大事故报告时限：重大安全事故（含根密钥泄露、系统停机超过 24 小时）、大规模订户信息泄露等严重事件，需在事件确认后 30 分钟内报送公司管理层，2 小时内报送主管部门及相关监管机构。

常规事件报告时限：证书系统迁移或改造、合规性事件、人力资源类事件，需在事件确认后 24 小时内报送公司管理层，3 个工作日内报送主管部门及相关监管机构。

报告内容包括以下信息：

1. 事件基本信息：事件类型、发生时间、地点、涉及系统与业务范围；
2. 影响研判：服务中断情况、受影响订户规模、数据安全风险；
3. 已采取的应急措施：如系统隔离、漏洞封堵、客户安抚等；
4. 事件根本原因分析；
5. 整改措施与长效机制建设计划；
6. 相关附件材料（日志、报告、沟通函件等）；
7. 报告联系人及联系方式；
8. 其他需说明的事项。

6. 认证系统技术安全控制

6.1. 技术安全管理制度要求

安信 CA 已建立并实施覆盖密钥管理、系统开发、网络防护等领域的技术安全管理制度，且制度符合国家相关法律法规及标准，该制度每年至少评审一次，并经安全策略委员会批准。

6.2. 密钥对的生成和安装

6.2.1. 根证书密钥对的生成和安装

安信 CA 根证书密钥对在物理隔离的安全环境中，采用通过国家密码管理部门认可的硬件密码设备生成；在生成、备份、恢复、销毁过程中实施 5 选 3 多人控制机制，操作在安全策略委员会授权下进行，并通过录音录像方式全程记录，保存期限不少于操作完成后十年。

6.2.2. 订户密钥对的生成和交付

订户签名密钥对的生成与交付符合以下要求之一：

1. 由订户持有符合国家密码管理要求的密码模块中生成并存储；
2. 由安信 CA 生成并保存的订户签名密钥对，安信 CA 需通过技术措施确保订户对签名私钥的独占控制权。安信 CA 会完整记录与订户签名私钥相关的所有操作日志，包括操作时间、操作方式、操作人员等信息，保存期限应不少于证书失效后五年；
3. 采用通过主管部门认可的其他创新性保护方案。

订户加密密钥对由吉林省密钥管理中心（以下简称 KMC）负责生成、控制与保存管理。

6.3. 私钥保护和密码模块工程控制

6.3.1. CA 私钥保护和密码模块工程控制

安信 CA 根证书私钥保护采用经国家密码管理局批准许可的密码产品，符合 GB/T 37092-2018 第 5 章要求；根证书私钥实施严格的分割保护机制，实现单人无法获取完整私钥；根证书私钥备份由密钥管理员分别存放于具备防盗措施的安全场所。

6.3.2.订户私钥保护和密码模块工程控制

订户签名私钥由订户持有的，订户应按照与安信 CA 签署的《电子认证服务协议》要求，采取预防措施防止私钥及其激活数据的丢失、泄露、更改或未经授权的使用。

订户签名私钥由安信 CA 受订户委托保管的，采用的电子签名模式和安全控制措施符合 GM/T 0109—2021、GM/T 0120—2022 标准，并定期进行安全评估。每次签名私钥调用前必须获得订户的明确授权，并完整保存授权记录。向订户提供关于签名私钥及激活数据安全使用的指导与建议。若采用其他电子签名模式和控制措施需经主管部门认可或符合相关标准。

6.4.密钥对管理的其他方面

6.4.1.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。公钥归档的最大间隔五年。

6.4.2.证书操作期和密钥对使用期限

无论是订户证书还是安信 CA 证书，证书到期后，签名私钥不可用于电子签名，安信 CA 根证书密钥对有效期不超过 20 年，订户证书密钥对不超过 10 年。特殊情况下，对于签名证书，为验证在证书有效期内签名的信息，公钥可以在证书有效期限以外使用。

6.5. 激活数据

6.5.1.激活数据的产生和安装

保护 CA 私钥的激活数据，在 CA 私钥生成时由智能密码钥匙生成，由经授权的 5 位密钥管理员分持，生成后保存在屏蔽机房区域的保险柜内。

6.5.2.激活数据的保护

存有安信 CA 私钥激活数据的 UKey，由安信 CA 5 位不同的可信密钥管理员分持，保存在屏蔽机房区域的保险柜内。当需要使用 CA 密钥激活数据时，需先填写申请单，再由保险柜管理员将 UKey 分发给 5 位中的 3 位密钥管理员。存放 CA 激活数据的智能密码钥匙或智能 IC 卡需采用口令保护，口令长度至少为 8 位。

6.5.3.激活数据的其他方面

1. 激活数据的传输：存有安信 CA 私钥激活数据的 UKey，通常保存在安信 CA 的安全设施中，不得携带外出或传送。如因特殊情况确需传送时，传送过程需在安信 CA 安全管理人员和密钥管理人员的共同监督下进行。
2. 激活数据的销毁：存有安信 CA 私钥激活数据的 UKey，销毁方法为将 UKey 初始化。

6.6.计算机安全控制

安信 CA 已建立并实施符合 GB/T 25056《信息安全技术 证书认证系统密码及其相关安全技术规范》中 8.2 要求的计算机安全控制体系。采取防火墙、病毒防治、漏洞扫描、入侵防御、数据备份、灾难恢复等安全防护措施。至少每半年开展一次系统升级补丁检查，完整记录系统升级的审批及实施全过程；对无官方补丁支持的系统，提前制定并落实网络隔离、功能限制、替代防护及系统迁移专项计划；为所有服务器和操作终端统一安装合规杀毒软件，确保病毒库每日自动更新，关键业务服务器每日执行实时病毒扫描，所有终端及普通服务器每周至少开展一次全面病毒扫描。

6.7.生存周期安全控制

安信 CA 机构已建立并常态化运行完整的密码与证书生存周期安全控制体系，体系建设、运行管控、证书全流程管理各项要求均严格契合 GB/T 25056-2018《信息安全技术 证书认证系统密码及其相关安全技术规范》第 10 章证书认证中心运行管理、第 12 章证书全生存周期管理相关条款要求，围绕 CA 中心日常运维安全、人员权限管控、

证书申请、签发、更新、撤销、归档、销毁全业务链路配套完善管理制度、密码安全技术防护与全流程审计追溯机制，保障证书全生命周期安全管控措施常态化落地、操作全程可核验追溯。

6.8. 网络安全控制

安信 CA 建立并实施符合 GB/T 25056-2018 中 5.3.8 要求的网络安全控制体系包括但不限于：

1. 安信 CA 的网络结构符合 GB/T 25056-2018 附录 A 中 RA 采用 B/S 模式时 CA 的网络结构要求。
2. 对所有 Web 服务配置防火墙、Web 应用防火墙、入侵检测系统和内容过滤等网络安全防护措施；
3. 建立并定期维护网络拓扑图，包含所有网络设备、连接关系和安全边界，定期更新，与机房实际情况保持一致；
4. 网络访问控制：建立针对证书签发子系统及数据库的访问白名单机制，仅授权证书注册子系统的必要功能模块及必要的管理设备进行访问；建立针对证书注册子系统和数据库的访问白名单机制。
5. 网络监控：至少每月开展一次系统日志分析，分析内容涵盖系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件。

6.9. 时间戳

安信 CA 暂时不提供时间戳服务。

7. 证书、证书撤销列表和在线证书状态协议

7.1. 证书

安信 CA 电子签名认证证书的格式符合 GB/T 20518 的要求，包括但不限于：数字证书格式、版本号、密码算法对象标识符、CA 和订户的名称、证书策略对象标识符，其中必须包含主管部门制定的相应等级证书策略 OID（见本 CPS 1. 5. 1），可包含安

信 CA 制定或遵循的证书策略 OID、证书序列号、证书有效期、订户的电子签名验证数据、安信 CA 的电子签名。

7.2. 证书撤销列表

安信 CA 的证书撤销列表（CRL）的格式符合 GB/T 20518—2018 中 5.3 的要求。

7.3. 在线证书状态协议

安信 CA 在线证书状态服务符合 GB/T 19713—2025 中第 7 章的要求

8. 认证机构审计及相关评估

8.1. 审计评估制度

安信 CA 已制定审计评估制度，制度内容包括但不限于：审计评估类型涵盖认证业务审计与全面符合性评估；明确审计评估的执行频率及触发评估的事件条件；规定内部执行审计评估人员的专业背景要求；若委托外部机构开展审计工作，则明确对外部机构的要求；明确审计评估所涉及的主题及采用的评估方法。

8.2. 认证业务审计

安信 CA 认证业务审计方式，包括但不限于：

1. 审计周期每年至少一次；
2. 审计内容包括但不限于证书申请、续期、密钥变更、更新、撤销、冻结等业务中，订户告知、身份查验、意愿记录、协议签署、资料保存的合规性；
3. 安信 CA 开展审计工作一般采用全面审计或抽样审计，若采用抽样审计，审计抽样率不少于 0.01%。
4. 对于审计发现的问题，需通知相关部门和人员及时整改，并跟踪整改落实情况。

8.3. 全面符合性评估

安信 CA 符合性评估方式，包括但不限于：

1. 评估周期不少于每年一次；
2. 评估内容包括但不限于：年度电子认证服务开展情况、电子认证服务许可条件符合性情况以 及认证规则和证书策略符合性情况等；
3. 审计采用抽样方式的，抽样率不低于本 CPS 8.2 的要求；
4. 对于审计发现的问题，通知被审计部门及时整改，并跟踪整改落实情况；
5. 在 1 月底前将上一年度符合性评估报告报送主管部门。

9. 法律责任和其他业务条款

9.1. 费用

安信 CA 开展了服务成本核算，制定价格策略，并在公司网站上公布各项服务与收费的标准和相关信息，收费标准包括：

1. 证书颁发或更新费用；
2. 证书访问费用；
3. 撤销证书的费用；
4. 状态信息访问费用；
5. 电子签名的费用；
6. 签名验证的费用；
7. 签名验证报告的费用；
8. 其他服务的费用。

9.2. 财务责任

安信 CA 已建立赔付专项备用资金制度，用于承担因本机构过错导致证书持有人或依赖方损失的赔偿责任。该资金保障额度不低于本机构上一年度营业收入的 1.5%，并随年度营业收入变化动态调整。

赔付专项备用资金的来源包括但不限于以下方式：

1. 本机构自有资金划拨；
2. 从年度营业收入中按比例提取的专项准备金；
3. 经监管机构认可的其他合法资金来源。

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. 订户证书信息以外的个人隐私信息；
2. 各类内部及外部审计记录；
3. 安信 CA 订户的电子签名私钥。

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. 订户同意公开的信息；
2. 安信 CA 签发的证书和 CRL 信息；
3. 其他可以通过公共、公开渠道获取的信息；
4. 依据法律、行政法规规定可以公开的信息。

9.4. 个人隐私保护

依据相关法律法规，安信 CA 受理证书及电子签名相关业务申请时，需由证书申请人及经办人提交个人信息，包括姓名、联系电话、身份证件号码、居住地址、身份证件原件及各类复印件等隐私信息。本 CPS 中关于用户个人信息保护条款的完整内容，详见安信 CA 官网公示的《个人信息保护政策》。安信 CA 对用户隐私信息落实如下安全保护措施。

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。

在数字证书全生命周期内，安信 CA 针对用户个人隐私信息的收集、使用、存储全流程落实专项保护措施。安信 CA 妥善保管申请人提交的全部身份佐证材料，配套完善安全防护手段，防范相关资料丢失、被盗及篡改风险。同时，安信 CA 建立完备的信息安全管理制度，运用行业标准安全技术与管控流程，全方位防范用户个人信息出现遗失、泄露、篡改、损毁、违规滥用等情形，切实保障用户隐私数据安全。

9.4.2.作为隐私处理的信息

安信 CA 将证书申请人提供的、不构成数字证书内容的资料视为隐私信息。

9.4.3.不被视为隐私的信息

除法律、行政法规另有规定外，证书申请人提交、用于填充数字证书字段的相关材料，一般不视作个人隐私信息。

9.4.4.用户个人信息的收集

依据《中华人民共和国电子签名法》第二十条，作为第三方合规电子认证服务机构，安信 CA 受理自然人、法人及非法人组织的数字证书申请时，有权核验申请人真实身份。申请人需通过纸质、电子申请表或证书业务系统提交身份佐证材料，申请表及配套协议中已清晰地告知机构将收集姓名、性别、证件号、住址、联系方式等个人信息。

针对业务合作方，安信 CA 要求其建立个人信息管理机制，遵循合法、正当、必要原则，书面告知用户信息收集的用途、方式与范围并取得书面同意。安信 CA 仅以机构名义归集用户信息，严禁员工以个人名义采集数据，且仅收集电子认证业务必需信息，不采集无关个人信息。

9.4.5.个人信息的存储

CA 机构将收集到的用户个人信息统一录入 CA 证书用户管理系统。CA 机构建立独立的机房设备存储已收集到的用户个人信息，采取严格的技术手段对存储的数据信息进行加密处理，确保用户个人信息不被窃取、泄露，但该等措施并不排除 CA 机构的数据信息存储系统受到恶意黑客入侵等特殊情况及地震、洪水等不可抗力的自然因素而可能发生数据信息泄露的风险。

9.4.6.用户个人信息的使用

安信 CA 仅可将证书订户个人信息用于证书业务及配套应用相关场景，不得在无关系统或场景中使用该类信息。出现以下情形时，安信 CA 可依法对外提供用户个人信息：一是依据国家法律、行政法规、部门规章的相关规定予以提供；二是取得订户书面授权或同意后提供。除前述两种法定、约定情形外，安信 CA 不得向任何第三方披露用户个人信息，亦不得将用户个人信息挪作其他无关用途。

9.4.7.用户个人信息的共享

安信 CA 不会出于商业目的，或在未获得用户书面授权与同意的情况下，向任何单位或个人共享证书用户的个人信息。若因合规要求且已取得用户书面许可需对外提供个人信息，安信 CA 将同步要求信息接收方落实完善的安全防护措施，妥善保管所获取的用户信息。

9.4.8.个人信息的管理

安信 CA 通过以下举措规范内部用户个人信息全流程管理：

1. 严格遵循法律法规与行业规范，配套落实个人信息安全防护机制；
2. 建立覆盖信息收集、查询、使用、处置全环节的内部管控体系；
3. 常态化开展员工个人信息保护专项培训，参训人员须签署信息保护承诺书；
4. 要求各注册机构制定信息保护制度，其防护标准不得低于 CA 机构，并将相关制度报送 CA 备案。

9.4.9.个人信息的查阅

订户若需查询、查看本人留存的个人信息，可通过安信 CA 官网公示的联络渠道与安信 CA 对接办理。

9.4.10. 个人信息的删除和更改

1. 个人信息删除

依据法律法规规定及双方证书服务相关协议约定，安信 CA 可依规对证书持有人的个人信息予以删除。

2. 个人信息更改

订户个人信息发生变动的，需在信息变更完成后两个工作日内，通过安信 CA 官网公示的联络渠道提交更正申请；若因订户未及时告知信息变动而产生相关风险，全部责任由订户自行承担。

9.5.知识产权

安信 CA 享有并保留对证书及所提供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 网站上公布的所有信息均归安信 CA 所有，他人不得转载用于商业用途。

9.6.陈述和担保

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，确保 CA 签名私钥在内部得到安全存储与保护，并建立和执行符合国家政策及标准规定的安全机制。

3. 安信 CA 的运营遵守本 CPS 规定，并将根据业务调整对 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 CPS 的所有实质性要求。
5. 安信 CA 向证书订户提供的注册流程，符合电子认证服务机构 CPS 的所有实质性要求。
6. 安信 CA 完成所有必要的鉴别与确认工作，处理证书申请、吊销、更新等服务请求，并妥善保存订户信息及认证相关信息。

9.6.2.注册机构的陈述与担保

安信 CA 的注册机构在参与电子认证服务过程中作出如下承诺：

1. 提供给证书订户的注册流程符合电子认证服务机构 CPS 的所有实质性要求。
2. 注册机构在批准证书前，需完成所有必要的鉴别与确认工作，并确保相关信息正确无误。
3. 注册机构将依据本 CPS 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. 注册机构应对订户信息及认证相关信息妥善保存，并在适当时间移交安信 CA 归档。
5. 注册机构应根据相关协议内容，配合安信 CA 开展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

订户一旦接受安信 CA 签发的证书，就被视为向安信 CA、注册机构及信赖证书的有关当事人作出以下承诺：

1. 订户确认已阅读并理解《电子认证业务规则》（CPS）及相关规定的全部内容，同意接受本 CPS 条款的约束。
2. 订户申请数字证书时，应提供真实、完整、有效且准确的信息与资料；上述信息资料发生变更的，需及时通知安信 CA 或注册机构。
3. 订户应妥善保管私钥，采取安全措施防止私钥遗失、泄露或被篡改，对私钥的使用行为承担全部责任。
4. 一旦发生私钥遗失、遗忘、泄露等可能危害安全性的事件，订户应立即通知安

信 CA 或注册机构，申请吊销等保护措施。

5. 若需变更证书或证书申请信息，订户应及时通知安信 CA 或注册机构，并通过证书策略允许的安全方式提交书面申请。
6. 证书的使用应符合所有适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。

9.6.5.其他参与者的陈述与担保

其他参与者的陈述与担保同本 CPS 9.6.4。

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，由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 不向任何一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. 偿付责任规则

安信 CA 建立健全偿付责任规则，其赔偿范围涵盖本机构在履行电子认证服务职责过程中，因技术故障、人为操作失误、系统安全漏洞等各类履职风险所导致的损失赔付责任。针对不同过错情形、证书类型及责任边界，明确差异化的赔付计算方式，以合法有据的直接经济损失为核算基准，结合责任认定结果，在对应证书的赔偿限额内核定最终赔付金额（机构订户单张证书赔偿上限 4000 元，个人订户单张证书赔偿上限 800 元）。同时，安信 CA 设立赔付全流程监督机制，由独立合规审计部门对赔付申请核查、责任认定、金额核算及款项支付等各环节进行全程监督与定期专项审计，保障偿付处置合规、公正、有序。

9.9. 赔偿

依据《中华人民共和国电子签名法》《电子认证服务管理办法》及本 CPS 约定界定赔付范围，仅对因本机构过错造成订户或合法依赖方的直接经济损失，在对应证书赔偿限额内承担赔付责任（机构订户单张证书赔偿上限 4000 元，个人订户单张证书赔偿上限 800 元）；订户自身操作不当、不可抗力导致的损失，以及间接损失、预期利益损失，不在赔付范围内。

申请人需在法定时效内通过官方指定渠道提交赔偿申请及相关佐证材料，本机构按照分级审核审批机制依次完成初审、合规复核与层级审批，全流程在合理工作期限内推进；若赔付事项进入司法诉讼、仲裁等法定程序，内部审核审批流程即时中止，最终赔偿责任与金额以人民法院、仲裁机构生效法律文书为准。

常规赔付审批通过后，本机构将及时完成资金划转并按规定归档留存；涉诉赔付依据生效法律文书要求执行；申请人对赔付结果有异议的，可提交复核申请，双方协商不成的，可依法通过司法诉讼或仲裁途径解决。

9.10. 有效期和终止

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. 对参与者的个别通告与沟通

电子认证活动中通信的参与方包括 CA 机构、订户、依赖方。

1. CA 机构与订户的通信：安信 CA 通过邮件、短信、书面通知等方式，向订户发送证书受理、签发、续期、撤销等各类通知，并留存记录。
2. CA 机构与依赖方的通信：CA 机构 CA 向依赖方提供带数字签名的 OCSP、CRL 证书状态查询服务，对依赖方的业务咨询在规定时限内予以正式回复，并留存记录。

9.12. 修订和发布

9.12.1. 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。

9.12.2. 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。

9.12.3. 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。

9.13. 争议处理与举证

安信 CA 建立了规范的争议处理与举证机制，保障证书订户、数字签名依赖方及相关方的合法权益，确保争议得到公正、及时解决。

9.13.1. 争议解决程序

当证书持有人或数字签名依赖方对数字签名有效性产生质疑时，安信 CA 可为证书订户和依赖方提供数字签名验证服务。验证服务的执行标准、操作流程及收费价格已在安信 CA 官方网站明示。

关于本规则的争端，相关方应首先与安信 CA 协商解决；协商不成的，任何一方均可向安信 CA 住所地有管辖权的人民法院提起诉讼。

9.13.2. 举证制度与能力体系

安信 CA 建立了覆盖证书全生命周期的举证制度与能力体系，所有相关记录均真实、完整且不可篡改，保存期限不短于证书失效后 5 年。具体包括：

1. 证书签发环节：完整留存身份验证记录、申请材料审查记录、权利义务告知记录、订户意愿确认记录等；
2. 签名环节：完整留存签名请求验证记录、签名操作日志、可信时间戳记录等；
3. 签名验证环节：完整留存验证请求记录、验证结果记录、异常情况处理记录等；
4. 安信 CA 在收到举证请求后 24 小时内予以响应。

9.14. 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。

9.15. 与适用法律的符合性

安信 CA 提供的所有电子认证服务及相关活动，均严格遵守中华人民共和国现行有效的法律法规。所有参与安信 CA 电子认证服务的主体，包括但不限于证书订户、数字签名依赖方及其他合作方，均有义务遵守与电子认证服务相关的适用法律法规。

在中华人民共和国境内开展电子认证服务适用的法律法规包括但不限于：《中华人民共和国电子签名法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《商用密码管理条例》《电子认证服务管理办法》《电子认证服务密码管理办法》。

安信 CA 将持续跟踪相关法律法规的更新情况，及时调整本认证业务声明及内部管理制度，确保电子认证服务始终符合最新的法律要求。任何参与方违反上述法律法规的，应自行承担相应的法律责任。

9.16. 一般条款

CP&CPS、订户协议、依赖方协议及其他补充协议构成电子认证服务各方的完整协议。本 CPS 将替代所有先前的或同时期的相关文档、与相同主题相关的书面或口头解释。

订户协议及依赖方协议中所对应的 CPS 版本号，以协议签署时当期发布的 CPS 版本为准。

9.17. 其他条款

本 CPS 最终解释权由安信 CA 所有，由安信 CA 负责解释和修订。