吉林省安信电子认证服务有限公司
证书策略
（CP）

版本 V2.1

吉林省安信电子认证服务有限公司

2024 年 11 月

任何需要本文档的个人或单位可以与吉林省安信电子认证服务有限公司的安全策略委员会联系：

电话：**0431-85177688**

版本控制

版本	日期	发布者
V1.0	**2009-5-10**	**安信CA安全策略委员会**
V2.0	**2021-9-26**	**安信CA安全策略委员会**
V2.1	**2024-11-21**	**安信CA安全策略委员会**
V2.0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 公司名称	

第一章	增加了场景型证书和云应用证书的相关描述
第二章	对信息发布的相关内容进行了修改
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
V2.1变更记录	
全文	修订云应用证书相关的管理规则

目　　录

1. 引言

1.1. 概述

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。

《吉林省安信电子认证服务有限公司证书策略》是安信 CA 数字证书服务的策略文档，规定了批准、签发、管理、使用、吊销、更新证书的业务、法律法规以及技术要求。本文适用于所有由安信 CA 签发和管理的数字证书及相关主体。

1.2. 标识

本文档称为《吉林省安信电子认证服务有限公司证书策略》（简称安信 CA CP）。

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（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。

1.3.2. 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。

1.3.3. 订户

证书订户是指向 CA 机构申请数字证书的实体，通常为个人或机构。订户需要与安信 CA 或 RA 签订服务协议并承担相应的责任与义务。

1.3.4. 依赖方

依赖方是指在业务活动中使用或信任本 CA 机构所签发的证书建立信任关系的实体。

1.4. 证书应用

1.4.1. 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。

1.4.2. 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。

1.5. 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《吉林省安信电子认证服务有限公司证书策略》（CP）的最高管理机构，负责制定、维护和解释本 CP。当需要编写或修订本 CP 时，由安信 CA 安全策略委会组织相关人员编写，并制定编写负责人。

1.5.2. 联系方式

安信 CA 的安全策略委员会为本 CP 的联系人，负责本 CP 的对外沟通及其他相关事宜，任何有关本 CP 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

1.5.3. 决定 CP 符合策略的机构

安信 CA 安全策略委员会负责审核批准 CP。

1.5.4. CP 批准程序

本 CP 由安信 CA 安全策略委员会组织人员编写和修订。编写小组形成征求意见稿后，征求公司领导及各部门负责人的意见，征求意见稿经修改后送交安全策略委员会审阅，根据安全策略委员会的意见修改并获得批准。

1.6. 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	证书吊销列表
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，标记了已经被吊销的公钥证书列表，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 的 CP、CPS 可从安信 CA 的官方网站（www.anxinca.com）获得。用户证书可以通过目录服务（ldap://sm2ldap.anxinca.com:390）获取；已被吊销的证书信息可从目录服务器和 CRL 站点查询；证书状态信息（有效、吊销）可通过 OCSP 服务获得。

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），在证书吊销后 24 小时内发布证书吊销列表（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

数字证书查询、CRL、CP、CPS 的查询和下载是公开的。CP、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 的证书的颁发者和主体命名符合 X.500 定义的甄别名规范。

3.1.2. 名称意义化的要求

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。

场景型证书应包含签名事件的电子签名场景特征信息，特殊情况允许匿名或者伪名等出现。

云应用证书的甄别名可参照个人和机构证书的相关要求。

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宜使用匿名或伪名。

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。

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

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。

证书载体为智能密码钥匙、密码模块类的证书，证书私钥在用户端生成，场景证书私钥在签名设备中产生，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。

云应用证书的订户私钥由订户终端和云平台协同运算生成，也可由订户申请在云平台生成，证书请求信息中包含用私钥进行的电子签名，CA 使用订户的公钥来验证私钥签名的有效性和申请数据的完整性，以此来判断申请人持有私钥。

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。如果国家法律法规对此有规定，安信 CA 将严格予以执行。

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。

场景证书没有密钥更新。云应用证书可采用授权认证的方式对订户身份标识和鉴别。

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. 吊销请求的标识与鉴别

当安信 CA 根据本 CP4.9.1 所述理由吊销订户证书时，无需进行鉴别。如果订户主动要求撤销证书，则按照本 CP3.2 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、和社会团体等）。

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 CP 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 CP 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 CP 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 CP 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、有效性。
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 CP 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 CP 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 CP 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 CP 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。

场景型证书申请为即时处理。

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。

场景型证书，订户完成电子签名即视为 CA 机构证书签发成功，CA 机构不再就证书签发向订户进行其他方式的通告。云应用证书，通过发送系统提示、短信或邮件等方式告知订户。

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。

场景型证书签发完后，将证书应用于对应的电子签名时起，就被视为同意接受证书。云应用证书订户的终端设备收到证书、或证书签发到云平台，或订户使用证书进行电子签名或其他密码运算即视为同意接受证书。

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。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。云应用证书，私钥在终端和云平台协同运算生成的，订户必须通过协同运算才能使用私钥签名；私钥在云平台生成的，订户必须通过授权认证才能使用私钥进行签名。

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。

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. 确认该证书是否被吊销；
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

4.6.1. 证书更新的情形

证书更新指在不改变证书中注册信息的情况下，为订户签发一张新证书。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。证书更新可以更换密钥对，也可以使用原有密钥对，视更新的具体情形而定。

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

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。

事件型证书仅用于订户特定一次的电子签名行为，没有证书更新和证书密钥更新。

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. 证书吊销

4.9.1. 证书吊销的情形

如果有以下情况，证书将被吊销：

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 CP 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. 订户根据证书吊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. 请求证书吊销的实体

已申请安信 CA 证书的订户可以请求证书吊销。

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. 吊销请求的流程

证书吊销请求的处理采用与初始证书签发相同的流程

1. 证书吊销的申请人到安信 CA 或其授权的注册机构提交书面资料，并注明吊销理由。
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吊销请求进行审核。
3. 安信 CA 或授权的注册机构吊销订户证书后，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吊销。

4.9.4. 吊销请求的宽限期

如果出现私钥泄露等事件，吊销请求必须在发现泄露嫌疑 8 小时内提出。其他吊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吊销请求的时限

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

4.9.6. 依赖方检查证书吊销的要求

依赖方必须在信任某个证书前查询吊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。

4.9.7. CRL 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。

4.9.8. CRL 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，应当及时提出证书吊销请求。

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吊销流程相同。

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，订户密钥损坏或丢失后，可在安信 CA 提出申请，经审核后，通过安信 CA 向密钥管理中心提出请求，并配合用户完成密钥恢复。在出现法律纠纷时，司法取证人员向密钥管理中心提出申请，经审核后，由密钥管理中心提供司法取证的依据。

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

本章参见 CPS。

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或密码模块生成签名密钥对。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：云应用证书的签名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模块共同运算协同产生。订户签名密钥对也可在云平台生成，签名密钥对应在国家密码管理部门许可的密码模块中生成。

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。

场景型证书的签名密钥对由签名设备生成并保管。

云应用证书，签名密钥由用户终端和云端共同产生的，签名密钥会通过安全通道进行传输；签名密钥由云平台生成的，订户通过授权认证方式使用私钥，不需要传送给订户。

6.1.3. 公钥传送给证书签发机构

订户通过安信 CA 的注册机构，以电子文件的方式将签名证书公钥提交给安信 CA 签发证书。在传递过程中采用国家密码主管部门许可的通讯协议及密钥算法，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 2048 位 RSA 密钥和 256 位 SM2 密钥，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、下级证书和证书吊销列表 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

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。

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。为保障业务连续性，安信 CA 按照密码设备制造商提供的操作规范对 CA 密钥进行备份，CA 私钥从一个密码设备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，并采用多人授权机制（至少 3 人）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。

证书订户私钥需在订户提供 PIN 码等激活数据，或通过其他可靠验证方式授权后才能被激活和使用。

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解除私钥激活状态。

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

CA 证书的有效期不超过 30 年，订户证书有效期最长不超过 5 年 3 个月。CA 密钥对使用期限和 CA 证书的有效期保持一致。订户证书的密钥对使用期限和订户证书的有效期保持一致。

6.4. 激活数据

6.4.1. 激活数据的产生和安装

安信 CA 私钥的激活数据由密码设备产生。

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、密码管理局颁布的相关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 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 CA 系统及其运行环境通过了国家密码管理局和工信部的审查，并取得了相应的资质。

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、证书吊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,信息存放在证书版本属性栏内。

7.1.2. 证书扩展项

证书扩展项是一个或多个证书扩展的序列。针对某些证书，安信 CA 签发的证书可能包含私有扩展项，不能识别私有扩展项的应用、依赖方可以忽略该扩展项。安信 CA 采用的扩展项包括：

颁发机构密钥标识符 Authority Key Identifier

主体密钥标识符 Subject Key Identifier

密钥用法 Key Usage

扩展密钥用途 Extended Key Usage

基本限制 Basic Constraints

证书吊销列表分发点 CRL Distribution Points

个人身份证号码 Identify Card Number

企业营业执照(统一社会信用代码)ICRegistration Number

7.1.3. 名称形式

安信 CA 签发证书的甄别名符合 X.500 关于甄别名的规定。

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，订户证书不宜使用匿名或假名。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。

7.2.2. CRL 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：被吊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。

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

本规章参见 CPS。