# 北京数字认证股份有限公司
# 预签证书策略
# （CP5）

1.0.2 版

发布日期：2023 年 7 月 11 日

生效日期：2023 年 7 月 11 日

北京数字认证股份有限公司

版本控制表

| 版本 | 状态 | 修订说明 | 审核/批准人 | 生效时间 |
|---|---|---|---|---|
| 1.0.1 | 版本发布 | 新版本发布 | 公司安全策略管理委员会 | 2022 年 3 月 31 日 |
| 1.0.2 | 版本发布 | 内容更新修订 | 公司安全策略管理委员会 | 2023 年 7 月 11 日 |

声明

本 CP 全部或者部分支持下列标准：

RFC3647：互联网 X.509 公钥基础设施-证书策略和证书业务声明框架

RFC5280：互联网 X.509 公钥基础设施证书和 CRL 属性

RFC2560：互联网 X.509 公钥基础设施-在线证书状态协议-OCSP

GB/T 26855-2011：信息安全技术公钥基础设施证书策略与认证业务声明框架

# 目　录

# 1. 引言

## 1.1. 概述

北京数字认证股份有限公司（Beijing Certificate Authority Co.,Ltd.，以下简称数字认证公司）于 2001 年 2 月开始运营，是权威、公正的电子认证服务机构。数字认证公司严格按照《中华人民共和国电子签名法》和《电子认证服务管理办法》的要求，以及相关管理规定，提供数字证书签发、更新、吊销或管理等服务，并通过以 PKI 技术、数字证书应用技术为核心的产品和服务，为电子活动提供可信身份、可信时间和可信行为的网络信任环境。

预签证书是数字认证公司预先在安全的商用密码产品（如：智能 USBKEY）中签发的一类证书。该类证书由注册机构对订户身份进行鉴别，将订户身份信息与预先签发的证书进行绑定，并与注册机构的业务系统关联。预签证书与订户身份信息的绑定信息经注册机构数字签名后提交到 CA 机构，该预签证书方可生效。预签证书适用于注册机构自身业务系统中身份标识、电子签名或数据加密等安全服务，用于证明业务操作的不可否认性和保障数据的安全性。

证书策略（Certification Policy，以下简称 CP）是关于电子认证服务机构制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。

本《北京数字认证股份有限公司预签证书策略》（以下简称《预签证书策略》）满足互联网标准组织制定的 RFC3647《互联网 X.509 公钥基础设施-证书策略和证书业务声明框架》，以及国内标准 GB/T 26855-2011《信息安全技术公钥基础设施证书策略与认证业务声明框架》的框架和内容要求。本《预签证书策略》适用范围为数字认证公司发放的预签证书。具体设定了证书策略、生命周期、使用、依赖和管理的角色、责任与要求，以及各相关主体的职责。为批准、签发、管理和使用证书和相关的可信服务制定业务，提供技术、策略和法律上的要求和规范。

## 1.2. 文档名称与标识

本文档的名称为《北京数字认证股份有限公司预签证书策略（CP5）》，简称《预签证书策略》，本证书策略 CP 的对象标识符为：1.2.156.112562.2.2.6。

## 1.3. PKI 参与者

### 1.3.1. 电子认证服务机构

数字认证公司是根据《中华人民共和国电子签名法》、《电子认证服务管理办法》规定，依法设立的第三方电子认证服务机构（简称：CA 机构）。

CA 机构是受用户信任，负责创建和分配公钥证书的权威机构，是颁发数字证书的实体。

### 1.3.2. 注册机构

注册机构（简称：RA 机构）是受理数字证书的申请、更新、恢复和吊销等业务的实体。

在预签证书服务体系中，注册机构通常是与 CA 机构合作的银行等金融机构。注册机构为满足其用户在其业务系统中的应用安全，与 CA 机构合作受理预签证书的业务办理，承担身份鉴证与审核、证书与订户身份绑定及业务关联、证书交付等工作。

CA 机构应在与注册机构签署合同中，明确双方的权利与义务，以及承担的法律责任。

### 1.3.3. 订户

订户是指向 CA 机构申请数字证书的实体。

### 1.3.4. 依赖方

依赖方是指为某一应用而使用、信任本 CA 机构签发的证书，并验证证书和相应签名的实体。

预签证书中的依赖方，是受理该预签证书的注册机构自身业务系统内的依赖实体，可以是注册机构自身，也可以是其业务系统中的某个用户。

### 1.3.5. 其他参与者

其他参与者指为 CA 证书服务体系提供相关服务的其他实体。

## 1.4. 证书应用

### 1.4.1. 适合的证书应用

本 CA 机构签发的预签证书，由注册机构将预签证书与订户身份信息绑定，并在注册机构的业务系统中与订户标识信息（例如网络账号）关联后，方可被订户有效使用。主要适用于银行等金融领域的应用场景，用于证明订户在注册机构的业务系统所进行的身份标识和电子签名，以及数据加密等服务。

### 1.4.2. 限制的证书应用

本 CA 机构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的情况下使用，由此造成的法律后果由订户负责。

订户不得在其注册机构关联的业务系统以外使用预签证书，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

本《预签证书策略》的管理机构是数字认证公司安全策略管理委员会。由数字认证公司安全策略管理委员会负责本《预签证书策略》的制订、发布、更新等事宜。



### 1.5.2. 联系人

本《预签证书策略》在数字认证公司网站发布，对具体个人不另行通知。

网站地址：http://www.bjca.cn

电子邮箱地址：cps@bjca.org.cn

联系地址：北京市海淀区北四环西路 68 号双桥大厦 15 层(左岸工社)(100080)

电话号码：8610-58045600

传真号码：8610-58045678

### 1.5.3. 决定 CP 符合策略的机构

本《预签证书策略》由数字认证公司安全策略管理委员会组织制定，报数字认证公司安全策略管理委员会批准实行。

### 1.5.4. CP 批准程序

本《预签证书策略》由数字认证公司安全策略管理委员会审批通过后，在数字认证公司的网站上对外公布。

本《预签证书策略》经数字认证公司安全策略管理委员会审批通过后，从对外公布之日起三十日之内向工业和信息化部备案。

## 1.6. 定义和缩写

下列定义适用于本《预签证书策略》：

a) 公开密钥基础设施（PKI）Public Key Infrastructure

支持公开密钥体制的安全基础设施，提供身份鉴别、加密、完整性和不可否认性服务。

b) 证书策略（CP）Certification Policy

是关于电子认证服务机构制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。

c) 电子认证业务规则(CPS) Certification Practice Statement

关于电子认证服务机构在证书签发、证书更新(或密钥更新)、证书吊销或证书管理过程中所采纳的业务实践的声明。

d) 电子认证服务机构（CA）Certification Authority

受用户信任，负责创建和分配公钥证书的权威机构。

e) 注册机构（RA）Registration Authority

具有下列一项或多项功能的实体：识别和鉴别证书申请人，同意或拒绝证书申请，在某些环境下主动吊销或挂起证书，处理订户吊销或挂起其证书的请求，同意或拒绝订户更新其证书或密钥的请求。但是，RA 并不签发证书（即 RA 代表 CA 承担某些任务）。

f) 预签证书：Pre-issued Certificate

预签证书是数字认证公司预先在安全的商用密码产品（如：智能 USBKEY）中签发出的一类证书。该类证书由注册机构对订户身份进行鉴别，将订户身份信息与预先签发的证书进行绑定，并在注册机构的业务系统关联，预签证书与订户身份信息的绑定信息经注册机构数字签名后提交到 CA 机构，该预签证书方可生

效。

此处的绑定是指建立数字证书与订户的身份信息的对应关系，以便明确证书对应的订户身份。

此处的关联是指建立数字证书的信息与注册机构业务系统中的订户标识信息的对应关系，以便证书能够在所关联的业务系统中使用。

在本 CP 中，如无特殊定义，所述的数字证书，均指预签证书。

g）证书吊销列表 (CRL)：Certificate Revocation List

一个经电子认证服务机构数字签名的列表，它指定了一系列证书颁发者认为无效的证书，也称黑名单服务。

h）CA 吊销列表(ARL)：Certificate Authority Revocation List

一个经电子认证服务机构数字签名的列表，标记已经被吊销的 CA 的公钥证书的列表，表示这些证书已经无效。

i）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。

j） 公钥 Public Key

非对称密码算法中可以公开的密钥。

# 2. 信息发布与信息管理

## 2.1. 信息库

本 CA 机构的信息库是一个对外公开的信息库，面向订户及依赖方提供信息服务。提供信息服务包括但不限于以下内容： CPS、CP 和 CRL 以及数字认证公司不定期发布的信息。

## 2.2. 认证信息的发布

证书状态可以通过 CA 机构的 OCSP 和 CRL 获得。

本《预签证书策略》发布在数字认证公司的网站上，供相关方下载、查阅。

## 2.3. 发布时间或频率

a)《预签证书策略》一经网站发布，即时生效。对数字证书的订户及证书申请人均具备约束力。

## 2.4. 信息库访问控制

对于公开发布的 CP、CPS 和 CA 证书等公开信息，CA 机构允许公众自行通过网站进行查询和访问。

只有经授权的 RA/CA 管理员可以查询 CA 机构和注册机构数据库中的其他数据。

# 3. 标识与鉴别

## 3.1. 命名

### 3.1.1. 名称类型

每个订户对应一个甄别名（Distinguished Name，简称 DN）。

数字证书中的主体的X.500 DN是C=CN命名空间下的X.500目录唯一名字。

### 3.1.2. 对名称意义化的要求

订户的甄别名(DN)必须具有一定的代表意义，预签证书的甄别名按照预定义规则生成。

### 3.1.3. 订户的匿名或伪名

预签证书中的 DN 采用预定义规则生成，与其所对应的订户真实名称绑定。

### 3.1.4. 理解不同名称形式的规则

数字证书符合 X.509 标准，甄别名格式遵守 X.500 标准。甄别名的命名规则由数字认证公司定义。

### 3.1.5. 名称的唯一性

在 CA 的证书服务体系中，预签证书主体名称必须是唯一的。

### 3.1.6. 商标的承认、鉴别和角色

CA 机构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。

## 3.2. 初始身份确认

### 3.2.1. 证明持有私钥的方法

在预签证书服务体系中，订户私钥由 CA 机构在安全的商用密码产品（如：智能 USBKEY）中预生成。CA 机构应保证在生产过程中订户证书及私钥的安全。

订户申领证书时，注册机构应对订户身份进行审核，将订户身份信息与证书绑定，与业务系统关联后，订户方可使用证书及对应私钥。此时，订户是其私钥的唯一持有者。订户应妥善保管其证书及私钥。

### 3.2.2. 个人身份的鉴别

个人在申领证书前应持个人有效身份证件提出证书申请，并接受证书申请的有关条款，承担相应的责任。由注册机构对证书申请人身份的真实性进行鉴别，做出批准申请或拒绝申请的操作。

个人有效身份证件指政府部门签发的证件，包括但不限于：身份证、港澳台居民身份证、户口簿、护照、军官证等。

身份鉴别除采用传统线下方式提交材料进行鉴别，也可以通过移动化、在线化的方式来进行鉴别。注册机构可通过公安部身份核实接口、电信运营商身份库等进行身份鉴别审核。

注册机构应妥善保存订户的身份信息，包括能证明订户有效身份的纸质材料或电子数据等。

### 3.2.3. 组织身份的鉴别

组织或机构在申领证书前应授权证书申请的经办人，并接受证书申请的有关条款，承担相应的责任。组织授权的经办人应持组织有效身份证件、组织的授权证明、以及经办人的个人有效身份证件提出证书申请。由注册机构对订户身份的真实性进行鉴别，做出批准申请或拒绝申请的操作。

组织有效身份证件指政府部门签发的证件或文件，包括但不限于营业执照、事业单位登记证、社会团体登记证、政府批文等。

身份鉴别除采用传统线下方式提交材料进行鉴别，也可以通过移动化、在线化的方式来进行鉴别。注册机构可通过权威第三方数据库查询系统来进行身份鉴别审核。

注册机构应妥善保存订户的身份信息，包括能证明订户有效身份的纸质材料

或电子数据等。

### 3.2.4. 没有验证的订户信息

订户提交鉴证文件不属于鉴别范围内的信息，为没有验证的订户信息。

### 3.2.5. 授权确认

当申请者代表个人或组织机构申请证书时，需要出示足够的证明信息以证明个人或组织机构是否真实存在，申请者是否已获得个人或组织机构的授权。注册机构有责任确认该授权信息，并将授权信息妥善保存。

### 3.2.6. 互操作准则

互操作可能是交叉认证、单身交叉认证或其他形式的互操作。交叉认证是指两个完全独立的、采用各自认证策略的 CA 中心之间建立相互信任关系，从而使双方的订户可以实现互相认证。

CA 机构将根据业务需要，在遵循本《预签证书策略》的各项控制要求的基础上，与 CA 的证书服务体系中未涉及的其他电子认证服务机构建立交叉认证关系。但交叉认证并不表示本 CA 机构批准了或赋予了其他 CA 中心或电子认证服务机构的权利。

## 3.3. 密钥更新请求的身份标识与鉴别

### 3.3.1. 常规密钥更新的标识与鉴别

预签证书的常规密钥更新中，通过订户使用当前有效私钥对包含新公钥的密钥更新请求进行签名，CA 机构使用订户原有公钥验证确认签名来进行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

预签证书吊销后的密钥更新对身份标识和鉴别的要求，使用初始身份验证相同的流程，详见本 CP § 3.2。

### 3.3.3. 证书变更的标识与鉴别

预签证书没有证书变更。

## 3.4. 吊销请求的标识与鉴别

预签证书吊销请求的标识与鉴别，使用初始身份验证相同的流程，详见本CP § 3.2。

如果是因为订户没有履行本《预签证书策略》和《电子认证业务规则》所规定的义务，由 CA 机构或注册机构申请吊销订户的证书时，不需要对订户身份进行标识和鉴别。

# 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(包括行政机关、事业单位、企业单位、社会团体和人民团体等)。

### 4.1.2. 申请过程与责任

证书申请人按照本《预签证书策略》所规定的要求，准备相关的身份证明材料提交至注册机构。注册机构依据本 CP § 3.2 要求对证书申请人进行的身份鉴别，并决定是否受理申请。

申请过程中各方责任为：

订户：订户需要提供本 CP § 3.2 所述的有效身份证明材料，并确保材料真实准确，配合注册机构完成对身份信息的采集、记录和审核。

注册机构：注册机构负责受理订户证书申请，鉴别订户的身份。鉴别过程参照本 CP § 3.2 的要求对订户的身份信息进行采集、记录和审核。鉴证通过后，注册机构应将订户身份信息与预先签发的数字证书进行绑定，与注册机构的业务系统进行关联，并通过安全通道将证书绑定信息提交至 CA 机构后，向订户发放证书。

注册机构应按照本 CP 和《注册机构电子认证服务运营管理规范》要求，履行注册机构相关责任与义务，并接受 CA 机构的监督管理和审计。

CA 机构：CA 机构负责管理、记录订户身份信息、以及证书绑定信息等。

证书申请人应当提供真实、完整和准确的信息，注册机构须按本 CP § 3.2 的要求和流程对申请人身份材料信息进行审查。如证书申请人未向注册机构提供真实、完整和准确的信息，或者有其他过错，给相关方造成损失的，由证书申请人承担赔偿责任。

## 4.2. 证书申请处理

### 4.2.1. 执行识别与鉴别功能

证书申请人向注册机构提交初始的证书申请请求，注册机构须按照以下规定对订户的申领材料进行审查：

个人订户：参照本 CP § 3.2.2 节的规定。

机构订户：参照本 CP § 3.2.3 节的规定。

### 4.2.2. 证书申请批准和拒绝

注册机构根据本《预签证书策略》所规定的身份鉴别要求对证书申请人身份进行识别与鉴别后，根据鉴别结果决定批准或拒绝证书申请。

证书申请人通过身份鉴别流程且鉴证结果为合格，注册机构将批准证书申请，为证书申请人发放数字证书。

证书申请人未能通过身份鉴证，注册机构将拒绝申请人的证书申请，并通知申请人鉴证失败，同时向申请人提供失败的原因(法律禁止的除外)。

被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

在必要时 CA 机构有权复核注册机构提交的订户申请材料，并有权拒绝不符合本 CP 的高风险申请。

### 4.2.3. 处理证书申请的时间

注册机构将做出合理努力来尽快确认证书申请信息，一旦注册机构收到了所有必须的相关信息，将在 1 个工作日内处理证书申请。

注册机构能否在上述时间期限内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地响应了注册机构的要求。

## 4.3. 证书签发

### 4.3.1. 证书签发过程中电子认证服务机构的行为

CA 机构预先在安全的商用密码产品（如：智能 USBKEY）中签发证书，并保证在生产过程中订户证书及私钥的安全。

注册机构受理证书申请后，应将订户身份信息及证书绑定信息提交至 CA 机

构。CA 机构记录上述信息，则意味着电子认证服务机构最终完全正式地批准了证书申请。

### 4.3.2. 电子认证服务机构对订户的通告

CA 机构通过注册机构对证书订户进行通告。注册机构审核订户身份后，应当主动告知证书申请人批准或拒绝了证书申请。

注册机构宜采取面对面、邮政信函、电子邮件等安全的方式通告订户。

## 4.4. 证书接受

### 4.4.1. 构成接受证书的行为

注册机构将数字证书发放给证书申请人，证书申请人自获得数字证书起，即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

CA 机构不提供预签证书的发布。根据与依赖方的约定，可向依赖方提供证书查询服务。

### 4.4.3. 电子认证服务机构在颁发证书时对其他实体的通告

CA 机构不对其他实体进行通告，其他实体可以在信息库上自行查询。

## 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 CA 机构所签发的证书后，均视为已经同意遵守与 CA 机构、依赖方有关的权利和义务的条款。

预签证书仅能在关联的业务系统中使用。订户接受证书后，应妥善保存其证书及私钥。在证书到期或被吊销后，必须停止使用该证书对应的私钥。

### 4.5.2. 依赖方对公钥和证书的使用

依赖方只能在恰当的应用范围内依赖于证书，并且与证书要求相一致（如密钥用途扩展等）。依赖方获得对方的证书和公钥后，可通过公钥验证对方电子签名的真实性。验证证书的有效性包括：

a) 用 CA 机构的证书验证证书中的签名，确认该证书是 CA 机构签发的，并且证书的内容没有被篡改。

b) 检验证书的有效期，确认该证书在有效期之内。

c) 检验证书有效性，需要检查该证书没有被吊销。

在验证电子签名时，依赖方应准确知道什么数据已被签名。在公钥密码标准里，标准的签名信息格式被用来准确表示签名过的数据。

依赖方获得对方的证书和公钥后，可通过注册机构的业务系统查询证书所绑定的订户身份，并可以通过业务系统向 CA 机构比对核实。但 CA 机构不会向该证书注册机构所关联业务系统外的其他实体提供订户身份核实。

## 4.6. 证书更新

预签证书仅支持证书密钥更新。

## 4.7. 证书密钥更新

### 4.7.1. 证书密钥更新的情形

证书密钥更新是指订户生成新密钥并申请为新公钥签发新证书，CA 机构提供证书更新时，密钥必须同时更新。

证书更新的具体情形如下：

a) 当订户证书即将到期或已经到期时；

b) 当订户证书密钥遭到损坏时；

c) 当订户证实或怀疑其证书密钥不安全时；

d) 其它可能导致密钥更新的情形。

### 4.7.2. 请求证书密钥更新的实体

订户可以请求证书密钥更新。订户包括持有 CA 机构签发的预签证书的证书持有人。

### 4.7.3. 证书密钥更新请求的处理

同 3.3。

### 4.7.4. 颁发新证书对订户的通告

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. 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3。

## 4.8. 证书变更

预签证书没有证书变更服务。

## 4.9. 证书吊销和挂起

### 4.9.1. 证书吊销的情形

a) 发生下列情形之一的，订户应当申请吊销数字证书：
   1) 数字证书私钥泄露；
   2) 订户身份信息发生重大变更；
   3）认为本人不能实际履行本 CP；
   4) 认为当前密钥管理方式的安全性得不到保证。
b) 发生下列情形之一的，CA 机构可以强制吊销其签发的数字证书：
   1) 订户提供的信息不真实；
   2) 订户没有履行双方合同规定的义务，或违反本 CP；
   3) 数字证书的安全性得不到保证；

4) 法律、行政法规规定的其他情形。

### 4.9.2. 请求证书吊销的实体

根据不同的情况，订户、CA 机构、注册机构可以请求吊销最终用户证书。

### 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过程。

a) 证书吊销的申请人到注册机构书面填写《证书吊销申请表》，并注明吊销原因；

b)注册机构根据本 CP § 3.2 的要求对订户提交的吊销请求进行审核；

c) CA 机构吊销订户证书后，注册机构将当面通知订户证书被吊销，订户证书在 24 小时内进入 CRL，向外界公布；

d) 强制吊销是指当 CA 机构或注册机构确认发生本 CP§4.9.1b）强制吊销证书情形时，对订户证书进行强制吊销，吊销后将通过注册机构通告订户。

### 4.9.4. 吊销请求宽限期

如果出现私钥泄露等事件，吊销请求必须在发现泄露或有泄露嫌疑 8 小时内提出。其他吊销原因的吊销请求必须在 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

注册机构接到吊销请求后立即处理，24 小时生效。CA 机构每日签发一次 CRL，并将最新的 CRL 发布到目录服务器指定的位置，供请求者查询下载。

CRL 的结构如下：

a) 版本号(version)

b) 签名算法标识符(signature)

c) 颁发者名称(issuer)

d) 本次更新(this update)

e) 下次更新(next update)

f) 用户证书序列号/吊销日期(user certificate/revocation date)

g) 签名算法(signature algorithm)

h) 签名(signature value)

### 4.9.6. 依赖方检查证书吊销的要求

在具体应用中，依赖方必须使用 CRL 查询或 OCSP 在线证书状态查询的方式对所依赖证书的状态进行查询。

### 4.9.7. CRL 的颁发频率

CA 机构可采用实时或定期的方式发布 CRL。颁发 CRL 的频率一般为 24 小时定期发布。

### 4.9.8. CRL 发布的最长滞后时间

CRL 发布的最长滞后时间为 24 小时。

## 4.10. 证书状态服务

### 4.10.1. 操作特点

证书状态可以通过 CA 机构提供的 OCSP 服务获得。

### 4.10.2. 服务可用性

根据与依赖方约定，可向依赖方提供状态查询服务。

### 4.10.3. 可选特征

根据请求者的要求，在请求者支付相关费用后，CA 机构可以提供以下通知服务：

a) 收到证书主题的电子签名消息的接受者要求，确认该证书是否已被吊销；

b) 提供通知服务，当指定的证书被吊销时，CA 机构将通知请求该项服务的请求者。

## 4.11. 订购结束

订购结束是指当证书有效期满或证书吊销后，该证书的服务时间结束。

订购结束包含以下两种情况：

a) 证书有效期满，订户不再延长证书使用期或者不再重新申请证书时，订

户可以终止订购；

b) 在证书有效期内，证书被吊销后，即订购结束。

## 4.12. 密钥生成、备份与恢复

### 4.12.1.密钥生成、备份与恢复的策略和行为

订户的签名密钥对由 CA 机构在安全的商用密码产品（如：智能 USBKEY）中预生成，加密密钥对由密钥管理中心生成。

预签证书的密钥恢复是指加密密钥的恢复，密钥管理中心不负责签名密钥的恢复。密钥恢复分为两类：订户密钥恢复和司法取证密钥恢复。

### 4.12.2.会话密钥的封装与恢复的策略和行为

非对称算法组织数字信封的方式来封装会话密钥。数字信封使用信息接受者的公钥对会话密钥加密，接受者用自己的私钥解开并恢复会话密钥。

# 5. 电子认证服务机构设施、管理和操作控制

本章规定参见 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 系统和 RA 系统的密钥对是在密码机内部产生，密码机应具有商用密码产品认证证书。在生成 CA 密钥对时，CA 机构按照密码机密钥管理制度，执行详细的操作流程控制计划，选定并授权 5 个密钥管理员，密钥管理员凭借智能 IC 卡对密钥进行控制。

订户的签名密钥对由 CA 机构在安全的商用密码产品（如：智能 USB KEY）中预生成，加密密钥对由密钥管理中心生成。

### 6.1.2. 私钥传送给订户

订户密钥对由 CA 机构在安全的商用密码产品（如：智能 USB KEY）中预生成。订户申领证书时，注册机构对订户身份进行审核，将订户身份信息与证书绑定，与业务系统关联后，会采取安全地方式将证书及对应私钥交付订户。

### 6.1.3. 公钥传送给证书签发机构

CA 机构在预生成订户证书时，会获取订户证书的公钥。

### 6.1.4. 电子认证服务机构公钥传送给依赖方

依赖方可以从数字认证公司的网站(http://www.bjca.cn)下载根证书和 CA 证书，从而得到 CA 的公钥。

### 6.1.5. 密钥的长度

密钥算法和长度符合国家密码管理部门的规定。

### 6.1.6. 公钥参数的生成和质量检查

公钥参数由国家密码管理部门认可的密码设备生成。对生成的公钥参数的质量检查标准，这些设备内置的协议、算法等均符合国家密码管理部门要求。

### 6.1.7. 密钥使用目的

订户的签名密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等，加密密钥对可以用于信息加密和解密。

签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

## 6.2. 私钥保护和密码模块工程控制

### 6.2.1. 密码模块标准和控制

CA 机构所用的密码设备都是经国家相关部门认可的产品，其安全性达到以下要求：

- 接口安全：不执行规定命令以外的任何命令和操作；
- 协议安全：所有命令的任意组合，不能得到私钥的明文；
- 密钥安全：密钥的生成和使用必须在硬件密码设备中完成；
- 物理安全：密码设备具有物理防护措施，任何情况下的拆卸均立即销毁在设备内保存的密钥。

### 6.2.2. 私钥的多人控制

CA 证书的私钥的生成、更新、吊销、备份和恢复等操作采用多人控制机制，即采取五选三方式，将私钥的管理权限分散到 5 张管理员卡中，只有其中超过半数以上的管理员在场并许可的情况下，才能对私钥进行上述操作。

订户的私钥由订户自己通过商用密码产品（如：智能 USB KEY）控制。

### 6.2.3. 私钥托管

订户加密证书对应的私钥由密钥管理中心托管，订户的签名证书对应的私钥由自己保管，密钥管理中心不负责托管。

密钥管理中心严格保证订户密钥对的安全，密钥以密文形式保存，密钥库具

有最高安全级别，禁止外界非法访问。

### 6.2.4. 私钥备份

CA 机构和密钥管理中心不备份订户的签名密钥。

加密私钥由密钥管理中心备份，备份数据以密文形式存在。

### 6.2.5. 私钥归档

订户加密密钥对的归档是将已过生命周期或决定暂不使用的加密密钥以密文形式保存在数据库中，并通过数据库备份出来进行归档保存，归档后的密钥形成历史信息链，供查询或恢复。

### 6.2.6. 私钥导入或导出密码模块

使用 CA 软件可以把私钥安全导入到密码模块中，私钥无法从硬件密码模块中导出。

### 6.2.7. 私钥在密码模块中的存储

私钥在硬件密码模块中加密保存。

### 6.2.8. 激活私钥的方法

具有激活私钥权限的管理员使用含有自己的身份的加密 IC 卡登录，启动密钥管理程序，进行激活私钥的操作，需要超过半数以上的管理员同时在场。

### 6.2.9. 解除私钥激活状态的方法

具有解除私钥激活状态权限的管理员使用含有自己的身份的加密 IC 卡登录，启动密钥管理程序，进行解除私钥的操作，需要超过半数以上的管理员同时在场。

### 6.2.10. 销毁密钥的方法

具有销毁密钥权限的管理员使用含有自己的身份的加密 IC 卡登录，启动密钥管理程序，进行销毁密钥的操作，需要超过半数以上的管理员同时在场。

### 6.2.11. 密码模块的评估

CA 机构应使用国家密码管理部门认可的商用密码产品，符合国家有关标准。密码机采用以分组密码体制为核心的高强度密码算法和非对称密码体制，密钥采取分层结构，逐层提供保护。主要技术指标如下：

a) 通信接口：符合国际 ITU Ethernet RJ45 标准；

b) 带宽控制：10M/100M/1000M 自适应，充分满足突发业务需要；

c) 并发容量：可支持同时并发 100 个的独立安全处理容量；

d) 密钥管理：密钥不以明文形式出现在服务器密码机以外；通信密钥通过身份鉴别后协商得到；

e) 身份鉴别：采用 IC 卡对用户进行身份鉴别管理，以控制对加密系统的使用；

f) 处理速度：数据加解密处理能力大于 100Mbps；

## 6.3. 密钥对管理的其他方面

### 6.3.1. 公钥归档

订户证书中的公钥包括签名证书中的公钥和加密证书中的公钥。它们由 CA 机构和密钥管理中心定期归档。

### 6.3.2. 证书操作期和密钥对使用期限

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

激活数据是私钥保护密码，证书存储介质（如：智能 USB KEY）出厂时设置了缺省的 PIN 值。为保证订户私钥的安全，订户接受证书后应立即修改 PIN 值。

### 6.4.2. 激活数据的保护

证书使用 PIN 值保护私钥，订户接受证书后应立即修改 PIN 值，并妥善保

管 PIN 值，防止泄露或窃取。

### 6.4.3. 激活数据的其他方面

只有在拥有证书介质并知道证书介质的 PIN 值时才能激活证书存储介质，进而使用私钥。

## 6.5. 计算机安全控制

### 6.5.1. 特别的计算机安全技术要求

为了保证系统的正常运行，对所需要的计算机设备进行正确的选型、验收，制定操作规范。另外，本系统采用增加冗余资源的方法，使系统在有故障时仍能正常工作。

对于设备有一套完整的保管和维护制度：

a) 专人负责设备的领取和保管，做好设备的领用、进出库和报废登记。

b) 对设备定期进行检查、清洁和保养维护。

c) 制定设备维修计划，建立满足正常运转最低要求的易损坏备件库。

d) 对设备进行维修时，必须记录维修的对象、故障原因、排除方法、主要维修过程及与维修有关的情况等。

e) 设备维修时，必须有派专人在场监督。

### 6.5.2. 计算机安全评估

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，并取得了相应资质。

CA 系统使用的网络设备、主机、系统软件等均取得了国家有关认证检测机构出具安全标准的凭证。

## 6.6. 生命周期技术控制

### 6.6.1. 系统开发控制

系统开发采用先进的安全控制理念，同时应兼顾开发环境的安全、开发人员的安全、产品维护期的配置管理安全。系统设计和开发运用软件工程的方法，做到系统的模块化和层次化，系统的容错设计采用多路并发容错方式，确保系统在

出错的时候尽可能不停止服务。

### 6.6.2. 安全管理控制

CA 机构对系统的维护保证操作系统、网络设置和系统配置安全。通过日志检查来检查系统和数据完整性和硬件的正常操作。

### 6.6.3. 生命周期的安全控制

整个系统从设计到实现，系统的安全性始终是重点保证的。完全依据国家有关标准进行严格设计，使用的算法和密码设备均通过了管理部门鉴定，使用了基于标准的强化安全通信协议确保了通信数据的安全，在系统安全运行方面，充分考虑了人员权限、系统备份、密钥恢复等安全运行措施，整个系统安全可靠。

## 6.7. 网络的安全控制

系统网络安全的主要目标是保障网络基础设施、主机系统、应用系统及数据库运行的安全。CA 机构采取防火墙、病毒防治、入侵检测、漏洞扫描、数据备份、灾难恢复等安全防护措施。

## 6.8. 时间戳

时间戳系统提供的时间戳服务在技术实现上严格遵循国际标准时间戳协议（RFC3161），采用标准的时间戳请求、时间戳应答以及时间戳编码格式，时间源采用国家授时中心提供的标准时间。

# 7. 证书、证书吊销列表和在线证书状态协议

## 7.1. 证书

CA 签发的证书符合 X.509 V3 格式。遵循 RFC5280 标准。

### 7.1.1. 版本号

X.509 V3。

### 7.1.2. 算法对象标识符

符合国家密码管理部门批准的算法对象标识符。

### 7.1.3. 名称形式

CA 数字证书中的主体 Subject 的 X.500 DN 是 C=CN 命名空间下的 X.500 目录唯一名字，各属性的编码一律使用 UTF8String。

主体 Subject 的 X.500 DN 支持多级 O 和 OU，其格式如下：

C=CN;

O=××

O=××

OU= ××;

OU=××;

CN=××

- C（Country）应为 CN，表示中国；
- O（Organization）中的内容为 CA 机构自定义的信息标识，如：注册机构的信息标识、应用单位的信息标识等；
- OU（Organization Unit）中的内容为证书主体类型，其中个人为 Individual，组织机构为 Organization；
- CN（Common Name）中的内容为按照预定义规则生成的用户标识。

### 7.1.4. 证书扩展项

CA 证书扩展项除使用 IETF RFC 5280 中定义的证书扩展项。

CA 采用的 IETF RFC 5280 中定义的证书扩展项：

- 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
- 私有密钥使用期 Private Key Usage Period
- 主体可选替换名称 Subject Alternative Name
- 基本限制 Basic Constraints
- 证书吊销列表分发点 CRL Distribution Points

## 7.2. 证书吊销列表

CA 签发的证书吊销列表符合 X.509 V2 格式。遵循 RFC5280 标准。

### 7.2.1. 版本号

X.509 V2。

### 7.2.2. CRL 和 CRL 条目扩展项

CRL 扩展项：颁发机构密钥标识符 Authority Key Identifier。
CRL 条目扩展项：不使用 CRL 条目扩展项

## 7.3. 在线证书状态协议

### 7.3.1. 版本号

使用 OCSP 版本 1（OCSP v1）。

### 7.3.2. OCSP 扩展项

不使用 OCSP 扩展项。

# 8. 电子认证服务机构审计和其他评估

## 8.1. 评估的频率或情形

审计是为了检查、确认 CA 是否按照《预签证书策略》和《电子认证业务规则》及其管理制度和安全策略开展业务，发现存在的可能风险。根据工作需要，定期组织开展审计评估。

## 8.2. 评估者的资质

内部审计人员由 CA 机构内部人员组成，外部审计的审计人员的资质由第三方确定。

## 8.3. 评估者与被评估者之间的关系

评估者与被评估者应无任何业务、财务往来或其它利害关系，足以影响评估的客观性。

## 8.4. 评估内容

审计所涵盖的主题包括：人事、机房物理安全、安全运营管理、密钥安全和运行服务、客户服务等内容。

## 8.5. 对问题与不足采取的措施

对审计中发现的问题，CA 机构将根据审计报告的内容准备一份解决方案，明确对此采取的行动。CA 机构将根据国际惯例和相关法律、法规迅速解决问题。

## 8.6. 评估结果的传达与发布

除非法律明确要求，CA 机构一般不公开评估结果。

对 CA 关联方，CA 机构将依据签署的协议来公布评估结果。

# 9. 法律责任和其他业务条款

本章规定参见 CPS。