

北京数字认证 电子签名电子认证证书策略

3.0.1 版

发布日期：2026 年 10 月 31 日

生效日期：2026 年 10 月 31 日

北京数字认证股份有限公司

Copyright © Beijing Certificate Authority Co.,Ltd.



版本控制表

版本	状态	修订说明	审核/批准人	生效时间
3.0.1	版本发布	新版本发布	公司安全策略管理委员会	2026 年 10 月 31 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

本文件所有版权归北京数字认证股份有限公司所有。未经书面授权，本文件中所有的文字、图表不得以任何形式进行抄袭和出版。



目 录

1. 概括性描述	7
1.1. 承诺	7
1.2. 基本信息	7
1.3. 文档名称与标识	9
1.4. 电子认证活动参与者	9
1.4.1. 电子认证服务机构	9
1.4.2. 注册机构	10
1.4.3. 订户	10
1.4.4. 依赖方	10
1.5. 证书应用	10
1.5.1. 证书应用分类	10
1.5.2. 证书应用限制	11
1.6. 策略管理	12
1.6.1. 策略文档管理机构	12
1.6.2. 决定 CP 符合策略的机构	12
1.6.3. CP 批准程序	12
1.6.4. 联系人	12
1.7. 定义和缩写	13
2. 信息发布与信息管理	16
2.1. 信息库	16
2.2. 认证信息的发布	16
2.3. 发布时间或频率	16
2.4. 信息库访问控制	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	17
3.2.1. 证明持有私钥的方法	17
3.2.2. 个人身份的查验	18
3.2.3. 机构身份的查验	18
3.3. 订户意愿记录	18
3.4. 订户协议	19
3.5. 没有验证的订户信息	19
3.6. 互操作准则	19
3.7. 命名	19
3.7.1. 名称类型	19
3.7.2. 对名称意义化的要求	19
3.7.3. 订户的匿名或伪名	20
3.7.4. 解释不同名称形式的规则	20
3.7.5. 商标的识别、鉴别和角色	20
4. 证书生命周期操作要求	21



4.1. 通用要求	21
4.2. 证书申请	21
4.2.1. 证书申请实体	21
4.2.2. 执行识别与查验程序	21
4.2.3. 证书申请批准和拒绝	21
4.2.4. 处理证书申请的时间	22
4.3. 证书签发	22
4.3.1. 证书签发过程中电子认证服务机构的行为	22
4.3.2. 电子认证服务机构对订户的通告	22
4.4. 证书接受	22
4.4.1. 构成接受证书的行为	22
4.4.2. 电子认证服务机构对证书的发布	23
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	23
4.5. 密钥对和证书的使用	23
4.5.1. 订户私钥和证书的使用	23
4.5.2. 依赖方对公钥和证书的使用	24
4.6. 证书续期	24
4.6.1. 证书续期的情形	24
4.6.2. 请求证书续期的实体	25
4.6.3. 证书续期请求的处理	25
4.6.4. 颁发新证书时对订户的通告	25
4.6.5. 构成接受续期证书的行为	25
4.6.6. 电子认证服务机构对续期证书的发布	25
4.6.7. 电子认证服务机构在颁发证书时对其他实体的通告	25
4.7. 证书密钥更新	25
4.7.1. 证书密钥更新的情形	25
4.7.2. 请求证书密钥更新的实体	26
4.7.3. 证书密钥更新请求的处理	26
4.7.4. 颁发新证书对订户的通告	26
4.7.5. 构成接受密钥更新证书的行为	26
4.7.6. 电子认证服务机构对密钥更新证书的发布	26
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	26
4.8. 证书变更	26
4.8.1. 证书变更的情形	26
4.8.2. 请求证书变更的实体	27
4.8.3. 证书变更请求的处理	27
4.8.4. 颁发新证书对订户的通告	27
4.8.5. 构成接受变更证书的行为	27
4.8.6. 电子认证服务机构对变更证书的发布	27
4.8.7. 电子认证服务机构在颁发证书时对其他实体的通告	27
4.9. 证书撤销	27
4.9.1. 证书撤销的情形	27
4.9.2. 请求证书撤销的实体	28
4.9.3. 撤销请求的流程	28



4.9.4. 撤销请求宽限期	28
4.9.5. 电子认证服务机构处理撤销请求的时限	28
4.9.6. 依赖方检查证书撤销的要求	29
4.9.7. CRL 的发布频率	29
4.9.8. CRL 发布的最长滞后时间	29
4.9.9. 撤销信息的其他发布形式	29
4.10. 证书状态服务	30
4.10.1. 操作特点	30
4.10.2. 服务可用性	30
4.10.3. 可选特征	30
4.11. 停止使用认证服务	30
4.12. 密钥托管与恢复	31
4.12.1. 密钥托管与恢复的策略和行为	31
4.12.2. 会话密钥的封装与恢复的策略和行为	31
5. 电子认证服务机构设施、管理和操作控制	32
6. 认证系统技术安全控制	33
6.1. 技术安全管理制度要求	33
6.2. 密钥对的生成和安装	33
6.2.1. CA 密钥对的生成和安装	33
6.2.2. 订户密钥对的生成和交付	33
6.2.3. 公钥传送给证书签发机构	34
6.2.4. 电子认证服务机构公钥传送给依赖方	34
6.2.5. 密钥的长度	34
6.2.6. 公钥参数的生成和质量检查	35
6.2.7. 密钥使用目的	35
6.3. 私钥保护和密码模块工程控制	35
6.3.1. CA 私钥保护和密码模块工程控制	35
6.3.2. 订户私钥保护和密码模块工程控制	35
6.3.3. 私钥备份	36
6.3.4. 私钥归档	36
6.3.5. 私钥导入或导出密码模块	36
6.3.6. 私钥在密码模块中的存储	36
6.3.7. 激活私钥的方法	36
6.3.8. 解除私钥激活状态的方法	37
6.3.9. 销毁密钥的方法	37
6.3.10. 密码模块的评估	37
6.4. 密钥对管理的其他方面	37
6.4.1. 公钥归档	37
6.4.2. 证书操作期和密钥对使用期限	38
6.5. 激活数据	38
6.5.1. 激活数据的产生、传输和使用	38
6.5.2. 激活数据的保护	38
6.5.3. 激活数据的销毁	38
6.6. 计算机安全控制	39



6.6.1. 计算机安全控制要求	39
6.6.2. 计算机安全评估	39
6.7. 生存周期安全控制	39
6.7.1. 证书认证中心运行管理要求	39
6.7.2. 密钥管理中心运行管理要求	39
6.7.3. 证书操作流程	40
6.8. 网络的安全控制	40
6.9. 时间戳	40
7. 证书、证书撤销列表和在线证书状态协议	41
7.1. 证书	41
7.1.1. 版本号	41
7.1.2. 算法对象标识符	41
7.1.3. 证书序列号	41
7.1.4. 证书有效期	41
7.1.5. 名称形式	41
7.1.6. 证书扩展项	43
7.1.7. 订户电子签名验证数据	43
7.1.8. CA 电子签名	43
7.1.9. 其他信息	44
7.2. 证书撤销列表	44
7.2.1. 版本号	44
7.2.2. CRL 和 CRL 条目扩展项	44
7.3. 在线证书状态协议	44
7.3.1. 版本号	44
7.3.2. OCSP 扩展项	45
8. 电子认证服务机构审计和其他评估	46
8.1. 审计评估制度	46
8.2. 认证业务审计	46
8.3. 全面符合性评估	46
8.4. 评估者资质	46
8.5. 评估者与被评估者之间的关系	47
9. 法律责任和其他业务条款	47

1. 概括性描述

1.1. 承诺

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、撤销或管理等服务，并通过以 PKI 技术、数字证书应用技术为核心的产品和服务，为电子认证活动提供可信身份、可信时间和可信行为的网络信任环境。

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。

《北京数字认证电子签名电子认证证书策略》（以下简称《电子认证证书策略》或 CP）适用范围为数字认证公司发放的通用介质证书和云端协同证书。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。数字认证公司承诺：

- a) 开展经营和服务活动时，遵守法律、行政法规，树立以人民为中心的服务理念，承担社会责任；
- b) 与客户建立业务关系前，开展应用业务调研，建立应用接入业务风险评估及内部定责机制，严禁为存在违法违规风险的业务提供电子认证服务；
- c) 使用经过国家密码管理局审查的电子认证服务系统开展电子认证服务；
- d) 接受政府和社会监督，对主管部门检查发现的问题及时整改，建立问题纠治长效机制，持续符合整改要求。

1.2. 基本信息

数字认证公司基本信息如下：

机构名称	北京数字认证股份有限公司	法定代表人	林雪焰
住所地址、经营场所地址	北京市海淀区北四环西路 68 号 1501 号 北京市西城区裕民东路 3 号 京版大厦一层	联系电话	010-58045600
电子认证服	ECP11010820009	发证机关	工业和信息化部

务许可证号			
批准日期	2005 年 10 月 19 日	许可证有效期	2020 年 10 月 19 日至 2025 年 10 月 18 日 (换证中)

本《电子认证证书策略》包含的证书链及其证书信息详见下表：

● 根证书信息

根证书	证书编号	颁发机构名称	密码算法	密钥长度	有效期	计划服务时间
ROOTCA	69e2fec0170 ac67b	国家密码管理局	SM2	256	2012-7-14 至 2042-7-7	
BeiJing ROOT CA	1000000000 0000011001	数字认证公司	RSA	2048	2017-5-11 至 2047-5-10	28 年
Public Trust Root CA	1000000000 0000021001	数字认证公司	RSA	2048	2017-5-11 至 2047-5-10	28 年
UTrust Root CA	1000000000 0000041002	数字认证公司	RSA	2048	2017-5-11 至 2047-5-10	28 年

● CA 证书信息：

上级证书	CA 证书	证书编号	颁发机构名称	密 码 算 法	密 钥 长 度	有效期	计划服 务时间
ROOTCA	Beijing SM2 CA	75dfc8554a8c03 ab35cf59e8b861 3b9e	国家密码 管理局	SM2	256	2012-7-14 至 2042-7-7	28 年
Beijing SM2 CA	BeiJing GCA	1110000000000 000000f	数字认证 公司	SM2	256	2016-1-1 至 2033-1-10	15 年
Beijing SM2 CA	MSSPCA	1110000000000 000000b	数字认证 公司	SM2	256	2015-8-20 至 2033-1-10	16 年
BeiJing ROOT CA	BJCA	1000000000000 0011003	数字认证 公司	RSA	2048	2017-5-11 至 2037-5-10	18 年
BeiJing ROOT CA	BeiJing GCA	1000000000000 0011002	数字认证 公司	RSA	2048	2017-5-11 至 2037-5-10	18 年
Public Trust Root CA	Public Trust CA-1	1000000000000 0021002	数字认证 公司	RSA	2048	2017-5-11 至 2037-5-10	18 年



Public Trust Root CA	Public Trust CA-2	1000000000000 0021003	数字认证 公司	RSA	2048	2017-5-11 至 2037-5-10	18 年
Public Trust Root CA	MSSPCA RSA	1000000000000 0021008	数字认证 公司	RSA	2048	2017-5-11 至 2037-5-10	18 年
UTrust Root CA	SCCA	1000000000000 0041007	数字认证 公司	RSA	2048	2017-5-11 至 2037-5-10	18 年
UTrust Root CA	GZCA	1000000000000 0041011	数字认证 公司	RSA	2048	2017-5-11 至 2037-5-10	18 年

1.3. 文档名称与标识

本文档的名称为《北京数字认证电子签名电子认证证书策略》，版本号为 3.0.1 版，文档发布日期：2026 年 10 月 31 日，依据本文档制定的业务规则为《北京数字认证电子签名电子认证业务规则 3.0.1 版》。原官网发布的《北京数字认证股份有限公司通用介质证书策略（CP1）》、《北京数字认证股份有限公司云端协同证书策略（CP3）》合并到本文档，不再单独发布，上述两个原证书策略文件自本文档发布之日起终止实行；《北京数字认证股份有限公司事件型证书策略（CP2）》自本文档发布之日起终止实行。

本文档下涉及的电子签名认证证书，证书中记载了所遵循的主管部门的证书策略 OID，根据证书等级区分为：

个人高等级证书 OID：2.16.156.339.2.1.1.2

个人基础级证书 OID：2.16.156.339.2.1.1.1

机构高等级证书 OID：2.16.156.339.2.1.2.2

机构基础级证书 OID：2.16.156.339.2.1.2.1

本 CP 下涉及的证书记载了数字认证公司向国家 OID 注册管理中心注册的证书策略 OID，其信息如下：

通用介质证书策略 OID：1.2.156.112562.2.2.1

云端协同证书策略 OID：1.2.156.112562.2.2.3。

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 机构）是指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

靠性验证的活动的实体。

电子认证服务机构应符合《中华人民共和国电子签名法》和《电子认证服务管理办法》有关规定，依据业务主管部门发布的《电子认证业务规则规范》制定本机构的《电子认证业务规则》，并按照业务规则开展电子认证服务。

1.4.2. 注册机构

注册机构（简称：RA 机构）是指具有受理、审核、批准或拒绝数字证书的申请、更新、恢复和撤销等的实体。注册机构应当按照相关法律法规规范和本 CPS 的规定受理和查验证证书服务申请。

数字认证公司除了承担 CA 机构职责，同时也承担注册机构职责。数字认证公司不应将注册机构的身份查验义务委托给外部机构和个人。

1.4.3. 订户

订户是指被颁发给一张证书的证书主体。在不同的阶段，也称为证书申请人、证书持有人。

订户向 CA 机构申请电子签名认证证书，应当提供真实、完整和准确的信息。订户如知悉电子签名私钥数据已经失密或者可能已经失密时，应当及时告知有关各方，并终止使用该电子签名私钥数据。

1.4.4. 依赖方

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有关活动的人。依赖方应当按照本 CPS 以及与 CA 机构间的相关约定验证证书和电子签名。

1.5. 证书应用

1.5.1. 证书应用分类

本 CA 机构签发的数字证书适用于企业信息化和电子商务等领域，用于证明订户在电子化环境中所进行的身份认证和电子签名，以及提供数据加解密等服务。

本 CA 机构签发的数字证书根据证书用途的不同，分为签名证书和加密证书，签名证书在本 CP 中指电子签名认证证书。

a. 签名证书



签名证书按照证书主体对象的类型和风险等级，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，分别适用于对应对象在相应风险等级下的身份认证和电子签名应用场景。四种类型证书的扩展项中记录了主管部门制定发布的证书策略 OID，其具体类型、证书策略 OID、适用的应用场景具体见下表：

证书类型	主管部门 证书策略 OID	适用的应用场景
个人高等级 电子签名认证证书	2.16.156.339.2.1.1.2	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
个人基础级 电子签名认证证书	2.16.156.339.2.1.1.1	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
机构高等级 电子签名认证证书	2.16.156.339.2.1.2.2	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
机构基础级 电子签名认证证书	2.16.156.339.2.1.2.1	适用于低风险业务、符合《电子签名法》的机构电子签名认证证书

b.加密证书

加密证书用于数据加密和解密，保障信息传输的机密性。

根据密钥存储方式的不同，分为通用介质证书、云端协同证书。具体如下：

➤通用介质证书

通用介质证书是数字认证公司签发的保存在订户持有或指定的证书载体中的一类证书。证书载体包括但不限于智能密码钥匙、密码设备、密码模块。

➤云端协同证书

面向移动互联网和云服务新技术领域，数字认证公司创新出一类特定的云端协同证书，适用于订户在移动化和云服务环境中的证书应用。协同数字证书必须由订户终端和云平台协同配合才能完成可靠的电子签名。

数字认证公司还签发预签证书、证据型证书和标识证书等其他类型证书，安全级别属于密码应用级，这些证书不适用于电子签名认证，一般用于身份认证、完整性保护和数据加密等业务场景中。对于这些证书，数字认证公司发布了《北京数字认证股份有限公司安全认证服务证书策略与业务规则》，可通过公司官网查阅、下载。

1.5.2. 证书应用限制

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，具体包含但不限于以下情形：



- a. 涉及人身关系，如婚姻、收养、继承等；
- b. 涉及公共事业服务停止，如停止供水、供热、供气等；
- c. 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；
- d. 国家法律法规禁止的活动。

涉及生命健康、财产权益等高风险活动禁止使用基础级电子签名认证证书。

1.6. 策略管理

1.6.1. 策略文档管理机构

本《电子认证证书策略》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《电子认证证书策略》的制订、发布、更新等事宜。

本《电子认证证书策略》由北京数字认证股份有限公司拥有完全版权。

1.6.2. 决定 CP 符合策略的机构

本《电子认证证书策略》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。

1.6.3. CP 批准程序

本《电子认证证书策略》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《电子认证证书策略》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。

1.6.4. 联系人

本《电子认证证书策略》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

1.7. 定义和缩写

下列定义适用于本《电子认证证书策略》：

加密 Encipherment Encryption

对数据进行密码变换以产生密文的过程。

密码模块 Cryptographic Module

实现密码运算功能，相对独立的软件、硬件、固件或这三者组合。

密码算法 Cryptographic Algorithm

描述密码处理过程的算法。

密钥 Key

控制密码变换操作的符号序列。

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。

公钥 Public Key

非对称密码算法中可以公开的密钥。

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。

SM2 算法 SM2 Algorithm

由 GB/T 32918 定义的一种椭圆曲线公钥密码算法。

SM3 算法 SM3 Algorithm

由 GB/T 32905 定义的一种密码杂凑算法。

公钥基础设施（PKI） Public Key Infrastructure

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。

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。

电子认证服务机构（CA） Certification Authority

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、可靠性验证的活动的实体。

数字证书 Digital Certificate

也称公钥证书，由电子认证服务机构（CA）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。

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关联的数字证书。

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电子签名的信赖从事有关活动的人。

订户 Subscriber

被颁发给一张证书的证书主体。

对象标识符 Object Identifier (OID)

用于无歧义地标识对象的全局唯一值。

证书策略 Certificate Policy (CP)

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。

证书策略对象标识符 CP OID

对某个证书策略进行唯一标识的 OID。

证书链 Certificate Chain

证书链是一个用于证书验证的证书序列。

身份查验 Entity Authentication

证实某个实体就是所声称身份的过程。

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。

时间戳 Time Stamp

对时间和其他待签名数据进行签名得到的，用于表明数据时间属性的数据。

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。

密钥更新 Key Re-key

用新密钥替换旧密钥的过程。

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。

证书撤销列表 Certificate Revocation List (CRL)

由电子认证服务机构（CA）签发并发布的被撤销证书的列表。

CA 撤销列表(CRL) Certificate Authority Revocation List

一个经电子认证服务机构电子签名的列表，标记已经被撤销的 CA 的公钥证书的列表，表示这些证书已经无效。

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存周期进行管理和服务的系统。



高等级电子签名认证证书 Enhanced Electronic Signature Certificate

适用于涉及生命健康、财产权益等高风险场景的电子签名认证证书。

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。

协同运算 Collaborative Computing

协同运算是指用户终端和服务端协同配合完成电子签名的过程。数字认证公司为协同运算申请两项专利：一种协同密钥管理的方法、装置及系统（专利号：201510276343.5）和一种协同数字签名系统及其方法（专利号：201510048860.7）。

云签名服务平台 eSignature Cloud Platform

云签名服务平台（以下简称：云平台）是搭建在云端或服务器端，与订户终端设备协同，共同完成订户电子签名或其他证书应用的平台系统，能够为订户或依赖方提供数字证书和电子签名服务。

安全授权认证 Secure Authorization

安全授权认证是指通过口令、短信验证码、生物识别信息、数字证书等认证凭证对其订户身份进行核验，同时作为订户对其私钥的控制的激活数据。

下列缩略语适用于本《电子认证证书策略》：

CA：电子认证服务机构 (Certification Authority)

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

CP：证书策略 (Certification Policy)

CRL：证书撤销列表(Certificate Revocation List)

DN：甄别名称 (Distinguished Name)

LDAP：轻量级目录访问协议 (Lightweight Directory Access Protocol)

OCSP：在线证书状态协议 (Online Certificate Status Protocol)

OID：对象标识符 (Object Identifier)

RTO：恢复时间目标 (Recovery Time Objective)

RPO：恢复点目标 (Recovery Point Objective)



2. 信息发布与信息管理的

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：电子认证业务规则及其历史版本、证书策略及其历史版本、证书链、证书信息、状态信息、业务办理指南、依赖方协议、投诉处理政策及投诉方式等。

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《电子认证证书策略》发布在数字认证公司的官方网站上，供相关方下载、查阅。

若国家电子认证服务管理平台发布备案要求，CA 机构承诺按要求备案，同时与平台进行证书信息技术对接。

2.3. 发布时间或频率

- a) 《电子认证证书策略》每年至少发布一次，一经网站发布，即时生效。
- b) 证书的发布：在证书签发时，CA 机构通过目录服务器自动将该证书公布。
- c) CA 机构的 CRL 每 24 小时发布一次。

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 机构数据库中的其他数据。

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

CA 机构在受理订户的电子签名认证证书申请时，不会将身份查验服务委托给外部机构或个人，由 CA 机构向订户和/或受委托人进行告知、身份确认、意愿记录 and 协议签署。

3.1.2. 订户告知

CA 机构在受理证书申请时，应告知订户以下内容：

- a) 订户的权利和义务；
- b) 服务收费的项目和标准；
- c) 电子签名认证证书、电子签名的使用条件；
- d) 信息安全保障措施；
- e) CA 机构和订户的责任划分；
- f) 订户签名私钥的存储方式及安全要求；
- g) 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。

CA 机构应区分高等级证书、基础级证书的不同告知方式：

- a) 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告知，并保留告知记录；
- b) 基础级证书可采用高等级证书的告知方式，或采用强制阅读、短信、邮件等方式告知，并保留告知记录。

3.2. 初始身份确认

3.2.1. 证明持有私钥的方法

订户签名密钥对由订户生成或委托 CA 机构生成。订户或 CA 机构应在符合国家安全标准的智能密码钥匙、密码模块中产生签名公私钥，通过证书请求中包含的数字签名来证明订户持有与注册公钥对应的私钥。本 CA 机构签发订户证书

前，系统将自动使用订户的公钥验证其私钥签名的有效性和申请数据的完整性，以此来判断订户拥有私钥。

3.2.2. 个人身份的查验

对于个人订户，CA 机构应查验个人有效身份证件或有效身份证件信息，核实个人订户身份的真实性。个人有效身份证件指政府部门签发的证件，包括但不限于居民身份证、港澳台居民居住证、港澳居民来往内地通行证、台湾居民来往大陆通行证、外国人永久居留身份证、护照、军官证等。

个人身份的查验流程应区分证书等级（个人高等级证书、个人基础级证书），明确记录在按照本 CP 制定的 CPS 中。

3.2.3. 机构身份的查验

对于机构订户，CA 机构应对机构订户的身份和代表机构办理证书的人员的身份的有效性和真实性进行查验，确保查验过程规范、结果可追溯。

机构证书可由法定代表人（包括其他单位、团体、非法人组织等机构的负责人，本 CP 中统称“法定代表人”）或受托人办理，申请过程中需主动提供机构有效身份证件原件或扫描件，配合 CA 机构完成查验工作。

机构有效身份证件指政府部门签发的证件，包括但不限于营业执照、事业单位法人证书、社会团体法人登记证书、民办非企业单位登记证书、统一社会信用代码证书等。

机构身份的查验流程应区分证书等级，明确记录在按照本 CP 制定的 CPS 中。

3.3. 订户意愿记录

CA 机构应当对订户申请证书的意愿进行记录，意愿记录内容，包括但不限于：

- a) 订户身份信息；
- b) CA 的信息；
- c) 签名私钥保存方及其保存义务；
- d) 订户对电子签名的法律责任。
- e) 订户对上述 a) 至 d) 项内容已充分知晓并同意的明确意愿表示。

CA 机构应在按照本 CP 制定的 CPS 中明确记录个人订户和机构订户意愿确认的方式，并妥善留存意愿确认记录，确保意愿确认的真实性、合法性和可追溯性。

3.4. 订户协议

CA 机构应制定电子认证服务协议，约束 CA 机构与订户权利义务，规范证书使用行为。协议中应包含本 CP § 3.1.2 规定的订户告知内容。订户在申请数字证书时，CA 机构应当与订户签订《电子认证服务协议》。

3.5. 没有验证的订户信息

CA 机构签发的电子签名认证证书，应在证书中载明《电子签名法》第二十一条规定的信息内容，其中包含证书持有人名称在内的订户信息，记录在证书甄别名中（详见本 CP § 3.7 规定的命名规则）。证书中不能包含未经验证的订户信息。

3.6. 互操作准则

互操作可能是交叉认证、单向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《电子认证证书策略》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。

3.7. 命名

3.7.1. 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。

3.7.2. 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。

个人证书的甄别名通常包含订户姓名，在 DN 或扩展项中还包含有效证件类型及证件号码（或相关信息的映射，包括但不限于散列值、掩码等）。

机构证书的甄别名通常包含机构名称，在 DN 或扩展项中还包含机构有效证



件类型及证件号码。

DN 项结构定义应符合 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

个人证书、机构证书可以通过证书记录的姓名/单位名称和证件号码信息，追溯到证书对应的唯一实体。

3.7.3. 订户的匿名或伪名

在 CA 证书服务体系中，订户不得使用匿名或伪名。

3.7.4. 解释不同名称形式的规则

甄别名（DN）的内容一般由 CN、OU、O、C 四部分组成。其中 CN 用来表示用户名，OU、O 用来表示组织单位名称、C 用来表示国家。

3.7.5. 商标的识别、鉴别和角色

订户在申请证书时，不得使用可能侵犯他人知识产权的内容作为订户信息用于申请证书。CA 机构在受理证书申请时，查验记载在证书主体甄别名中的订户信息真实性，但并不验证该信息是否包含知识产权或处于知识产权纠纷中。

当发生有关知识产权的争议纠纷时，本 CA 机构有权拒绝相应的证书申请或撤销已发放的证书。



4. 证书生命周期操作要求

4.1. 通用要求

CA 机构按照《电子认证证书策略》所规定的要求，明确自身与订户在证书全生存周期中的责任，确保证书申请、签发、使用、撤销等环节合规有序。

- CA 机构职责：

- a. 承担数字证书注册通道的建立、运营和维护责任；
- b. 承担与证书订户签订电子认证服务协议的责任；
- c. 承担妥善记录并保存证书生存周期相关信息的责任。

- 订户职责：

承担提供准确信息的责任。

4.2. 证书申请

4.2.1. 证书申请实体

证书申请实体包括个人、法人和其他组织机构(包括事业单位、企业单位、社会团体和人民团体等)。

4.2.2. 执行识别与查验程序

CA 机构按照本《电子认证证书策略》所规定的程序对订户的身份进行识别与查验。具体的查验程序参照本 CP § 3 身份标识与查验。

4.2.3. 证书申请批准和拒绝

CA 机构根据本《电子认证证书策略》相关规定，完成订户告知、身份确认、意愿记录、协议签署等动作，并根据身份查验结果决定批准或拒绝证书申请。

如果订户未能通过身份查验，CA 机构将拒绝订户的证书申请，并通知订户验证失败，同时向订户提供失败的原因(法律禁止的除外)。被拒绝的订户可以在准备正确的材料后，再次提出申请。

如果订户身份查验结果为合格，并履行了其应尽的义务（如接受相关协议的内容和要求、支付所需的费用等），CA 机构将批准证书申请，为订户制作并颁



发数字证书。

4.2.4. 处理证书申请的时间

CA 机构应做出合理努力尽快确认证书申请信息，一旦 CA 机构收到了所有必须的相关信息，应在 2 个工作日内处理证书申请。

如有特殊情况，CA 机构应与订户协商，适当延长证书处理时间。

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 机构在批准证书申请之后，将签发证书。证书的签发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 机构对证书订户的通告有以下几种方式：

- a) 通过面对面的方式，通知订户证书签发的结果；
- b) 通过系统提示、短信、电话、电子邮件或邮政信函等方式通知订户；
- c) 通过主管部门认可的其他方式通知订户。

4.4. 证书接受

4.4.1. 构成接受证书的行为

CA 机构交付证书、订户接受证书，可以通过以下几种方式：

- a) CA 机构将数字证书当面、寄送或电子方式交付订户，订户从获得数字证书起，就视为已经接受证书；
- b) CA 机构通过网络下载方式交付证书的，证书下载的系统记录表明订户已经接受证书；
- c) 对于云端协同证书，CA 机构将证书发送到终端模块或云平台的方式交付证书，订户未提出异议即视为订户已经接受证书；
- d) 将证书应用于对应的电子签名或其他密码运算时起，就视为已经接受证书。
- e) CA 机构也可以通过其他安全的方式交付数字证书。



订户如果拒绝接受证书，应当在CA机构交付证书后两个工作日内提出异议，视为订户拒绝接受证书。

CA机构应保存订户接受证书的记录，包括接受时间、方式、操作人等信息。

4.4.2. 电子认证服务机构对证书的发布

CA机构在签发完数字证书后，采用数据库或目录服务方式，实现数字证书的存储与发布。对已发布的数字证书，CA机构提供证书目录信息查询服务。

查询方式包括但不限于用户在线自助或人工受理等。查询申请用户需要提供必要的查询条件信息，包括但不限于序列号、证书主体信息、办理渠道、证书链、有效期。对于订户查询，CA机构核实身份后提供查询服务。对于其他实体查询，为保护证书订户的数据安全和隐私保护，CA机构只承诺对其他实体提交的证书进行核实。

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机构采用数据库或目录服务方式对证书进行发布，其他实体可以通过CA机构提供的查询方式自行查询。

4.5. 密钥对和证书的使用

4.5.1. 订户私钥和证书的使用

CA机构帮助订户生成签名私钥的，在将签名私钥交付订户前，应采取有效措施保护私钥的安全性。证书的密码算法应当符合国家密码主管部门和行业安全需求对密码算法的要求。

CA机构提供订户签名私钥托管服务时，应采取有效技术措施和安全管理保证订户私钥安全，并向订户承诺：

- a) 未经订户书面授权，不保存或委托他人保存其签名私钥；
- b) 对机构证书签名私钥的使用，应设置法定代表人或受托人作为授权主体，如果机构订户需要指定其管理的应用系统代表机构使用签名私钥的，应作出对应授权。
- c) 仅在获得订户明确授权的情况下使用其签名私钥；
- d) 签名私钥以加密形式存储，且存储条件符合安全标准；
- e) 所有涉及签名私钥的操作有完整、可追溯的记录。

订户接受了CA机构所签发的证书后，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。订户应当妥善保管其持有或控制的私钥、证书口令（PIN）或其他私钥保护信息，不得泄露或交付他人。

通用介质证书订户接受到数字证书，使用介质控制证书实施电子签名。订户应妥善保管其证书对应的私钥。

云端协同证书订户必须使用其终端和云平台协同配合才能完成一次电子签名。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进行签名；私钥在云平台生成的，订户必须通过安全授权认证才能使用私钥进行签名，对于机构证书订户，应设置法定代表人或受托人作为授权主体。云端协同证书通过以上两种方式保证私钥仅由订户持有与控制。

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，并且在证书到期或被撤销之后，订户必须停止使用该证书对应的私钥。

CA 机构应建立便捷的外部安全事件反馈渠道，及时受理和处理证书信息错误、私钥失密或证书被盗用等异常情况。

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，查看对方的证书了解对方的身份和证书等级，验证对方证书是否有效，并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撤销。

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。

4.6. 证书续期

4.6.1. 证书续期的情形

证书续期是指在不改变订户证书信息的情况下，为订户签发一张新证书。订户应当在证书有效期到期前，到 CA 机构申请证书续期。

4.6.2. 请求证书续期的实体

证书订户或其受托人可以请求证书续期。

4.6.3. 证书续期请求的处理

证书申请者应在证书到期前，采取面对面或在线的方式向 CA 机构提交证书续期申请。

CA 机构可采取订户有效的原证书进行电子签名验证的方式进行身份确认，或采用与新申请证书相同的身份查验流程进行身份确认。采用原证书签名验证的方式查验的，应满足自上次完成身份查验之日起至本次申请续期申请日未满三年，或经核实查验订户身份的信息未发生改变。CA 机构查验身份通过后为订户签发新的证书。

订户证书失效后申请证书续期，需要对订户身份进行重新验证。

4.6.4. 颁发新证书时对订户的通告

同 4.3.2。

4.6.5. 构成接受续期证书的行为

同 4.4.1。

4.6.6. 电子认证服务机构对续期证书的发布

同 4.4.2。

4.6.7. 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。

4.7. 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。



证书密钥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

订户或其受托人可以请求证书密钥更新。

4.7.3. 证书密钥更新请求的处理

同 4.6.3。

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

4.8.1. 证书变更的情形

证书变更是指在证书有效期内，除证件号码以外订户证书信息发生变化，在不改变订户公钥的情况下，CA 机构经核验后签发一张新证书。

4.8.2. 请求证书变更的实体

订户或其受托人可以请求证书变更。

4.8.3. 证书变更请求的处理

证书变更应采用与本 CPS § 3 章节的流程进行标识与查验，验证变更信息的真实性，若发起方不是证书订户，CA 机构应取得订户同意，验证通过后为订户签发新的证书。

4.8.4. 颁发新证书对订户的通告

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. 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3。

4.9. 证书撤销

4.9.1. 证书撤销的情形

- a) 发生下列情形之一的，订户应当申请撤销数字证书：
 - 1) 数字证书私钥泄露；
 - 2) 数字证书中的信息发生重大变更；
 - 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 机构可以撤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. 请求证书撤销的实体

根据不同的情况，订户、受托人、CA 机构或依赖方可以请求撤销最终用户证书。当发生 CP § 4.9.1 a) 所列情形时，订户本人或受托人可以请求撤销证书；当发生 CP § 4.9.1 b) 所列情形时，依赖方可以请求撤销证书，CA 机构也可以直接启动强制撤销流程。

4.9.3. 撤销请求的流程

CA 机构应提供热线电话等便捷渠道，向相关方提供证书撤销流程咨询服务，并记录影响证书或私钥安全的事件（如密钥遗失、泄露等）。

证书撤销流程如下：

- a) 证书撤销的申请人到 CA 机构现场或在线提交证书撤销申请，并注明撤销原因；
- b) CA 机构审核申请人的身份和权限，以及证书撤销理由、证书是否在有效期内等信息，决定撤销证书或拒绝撤销证书；
- c) CA 机构撤销订户证书后，订户证书在 24 小时内进入 CRL，向外界公布。

强制撤销是指当 CA 机构确认用户发生本 CP §4.9.1b) 强制撤销证书情形时，对订户证书进行强制撤销。撤销后将通过官网公告或其他安全可行的方式通告订户。

4.9.4. 撤销请求宽限期

如果出现私钥泄露等事件，撤销请求必须在发现泄露或有泄露嫌疑 8 小时内提出。其他撤销原因的撤销请求必须在 48 小时内提出。

4.9.5. 电子认证服务机构处理撤销请求的时限

CA 机构接到撤销请求后，在 1 个工作日内，按照本 CPS § 4.9.3 的流程处理证书撤销请求。

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/撤销日期(user certificate/revocation date)
- g) 签名算法(signature algorithm)
- h) 签名(signature value)

4.9.6. 依赖方检查证书撤销的要求

在具体应用中，依赖方必须使用以下两种功能之一进行所依赖证书的状态查询：

a) CRL 查询：利用证书中标识的 CRL 地址，通过目录服务器提供的查询系统，查询并下载 CRL 到本地，进行证书状态的检验。

b) 在线证书状态查询(OCSP)：服务系统接受证书状态查询请求，从目录服务器中查询证书的状态，查询结果经过签名后，返回给请求者。

注意：依赖方要验证 CRL 的可靠性和完整性，确保是经 CA 机构发布并且签名的。

4.9.7. CRL 的发布频率

CA 机构应发布 CRL 和 ARL。对于订户证书一般不超过 24 小时发布 1 次 CRL，对于中级 CA 证书通常不超过 12 个月发布 1 次 ARL。

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。

4.9.9. 撤销信息的其他发布形式

证书撤销信息通过 CRL 服务方式发布，予以公告。

CA 机构还可以采取官网通知的方式公告。



4.10. 证书状态服务

4.10.1. 操作特点

CA 机构提供证书状态信息查询服务，包括证书撤销列表 CRL、在线证书状态查询服务 OCSP 等状态信息查询服务，以供依赖方获取证书有效性信息。

CA 机构对证书状态信息服务的查询请求应有合理的响应时间和并发处理能力。

4.10.2. 服务可用性

CA 机构应提供 7X24 小时的证书状态查询服务，服务可用性指标不低于 99.95%。在服务不可用时，CA 机构应提供备用查询机制。

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

4.11. 停止使用认证服务

以下三种情形，订户应当停止使用认证服务：

- a) 证书有效期已经过期，且订户未重新申请证书，或证书在有效期内被撤销时；
- b) 证书在有效期内，订户主动申请终止认证服务；
- c) 法律法规规定的订户应当停止使用认证服务的其他情形。

对于 b)和 c)的情形，CA 机构应根据订户申请，或按照本 CP 的规定，在 1 个工作日内以证书撤销方式处理。

对于相关认证信息中涉及用户的数据，CA 机构将继续依法保存，保存期限在证书失效后不少于 5 年。当依据法律规定应当销毁用户数据时，CA 机构应在销毁前进行安全审计，形成审计报告并存档备查。如因各种情况，CA 机构需要终止运营时，数据将按要求转移交给承接单位。

由 CA 机构提供密钥托管服务的，停止使用认证服务后，CA 机构应当安全



销毁订户签名私钥，并完整记录操作过程。

停止使用认证服务后，CA 机构按法律规定和双方协议约定，继续拥有保存订户认证信息相关数据的权利，并履行安全、妥善保管的义务。

在停止使用认证服务前，订户已经使用证书及签名私钥实施的签名行为，其效力与法律后果不因停止使用认证服务而终止。

4.12. 密钥托管与恢复

4.12.1. 密钥托管与恢复的策略和行为

CA 机构的根私钥和 CA 私钥不得托管给任何第三方机构或个人，存储私钥的密码设备应放置在安全环境中。CA 私钥备份应采取多人控制，全部密钥管理员到场方可执行备份操作，导出的密钥备份文件应在安全的区域中保存。当遇到异常情况需要恢复密钥时，应由 3 名或以上的密钥管理员到场授权方可执行密钥恢复操作，并在安全物理环境中执行。

订户密钥恢复是指订户加密密钥对的恢复，密钥管理中心不负责签名密钥对的恢复。密钥恢复分为两类：用户密钥恢复和司法密钥恢复。

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《北京数字认证电子签名电子认证业务规则 3.0.1 版》。

6. 认证系统技术安全控制

6.1. 技术安全管理制度要求

CA 机构应建立并实施涵盖密钥管理、系统开发、网络防护等领域的技术安全管理制度，每年至少接受一次安全策略委员会的评审。

6.2. 密钥对的生成和安装

6.2.1. CA 密钥对的生成和安装

CA 系统的密钥对应在屏蔽机房的密码机内部产生，密码机应具有商用密码产品认证证书。所有对 CA 密钥的操作，包括生成、备份、恢复、销毁等，应在安全策略委员会审批后实施。在生成 CA 密钥对时，CA 机构应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 名密钥管理员，采取五选三控制机制，由密钥管理员凭借安全介质（如智能 IC 卡、USBKey）对密钥进行控制。

密钥对生成应进行全程监督并录像，视频记录保存期限不少于操作完成后的十年。

6.2.2. 订户密钥对的生成和交付

（一）订户签名密钥对的生成、交付及控制方式要求

订户签名密钥对的生成、交付及控制方式，应符合以下三种要求之一：

- a) 由订户持有的符合国家安全标准的密码模块产生和存储；
- b) 由 CA 产生、保存，并提供技术措施确保订户对签名私钥的独占控制权；
- c) 采用通过主管部门认可的其他创新保护方案。

（二）各类订户签名密钥对的生成、交付及控制方式

本 CPS 中各类电子签名认证证书订户签名密钥对的生成、交付及控制方式，以及符合上述三种要求的规则方式如下：

a) 通用介质证书

通用介质证书订户签名密钥对的生成、交付及控制方式，符合“由订户持有的符合国家安全标准的密码模块产生和存储”的要求。其订户的签名密钥对在订户持有或指定的符合国家安全标准的证书载体中产生并存储，由订户直接控制实



施电子签名。证书载体包括但不限于智能密码钥匙、密码设备、密码模块。加密密钥对由密钥管理中心生成，通过安全通道传到订户手中的证书载体中。

b) 云端协同证书

云端协同证书订户签名密钥对的生成、交付及控制方式分为协同运算生成和云平台生成两种方式。

协同运算生成的，符合“由订户持有的符合国家安全标准的密码模块产生和存储”的要求。订户签名密钥对分为终端密钥因子和云平台密钥因子，由订户持有的终端密码模块和云平台密码模块中协同运算生成，终端密码模块和云平台密码模块均符合国家安全标准。其中终端密钥因子由终端设备信息、用户知晓的控制因子、随机数等部分协同运算产生，需要终端与云平台协同运算才能完成订户签名密钥对的使用，确保只有持有该终端设备，并知晓用户密码的订户，才能使用签名密钥对实施电子签名，从而保护订户对签名密钥对的唯一控制。

云平台生成的，符合“由 CA 产生、保存，并提供技术措施确保订户对签名私钥的独占控制权”的要求。订户签名密钥对在 CA 机构的云平台，由符合国家安全标准的密码模块生成，并保存在云平台密码模块中。CA 机构云平台提供安全措施确保仅订户可以唯一控制签名私钥。签名用户调用云平台的签名私钥实施电子签名时，CA 机构将通过安全授权认证机制，验证签名用户是签名私钥对应的证书订户本人或其授权的受托人，确保订户对签名私钥的独占控制权。

（三）CA 机构的记录规则

CA 机构参与保管订户签名私钥时，将完整记录所有与订户签名私钥相关的操作日志，包括时间、方式、操作人员等信息，保存期限不少于证书失效后五年。

6.2.3. 公钥传送给证书签发机构

订户的签名证书公钥通过安全通道传递到 CA 机构。

从 RA 到 CA 以及从密钥管理中心到 CA 的传递过程中，采用符合国家安全标准的通讯协议及密钥算法，保证传输中数据的安全。

6.2.4. 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。

6.2.5. 密钥的长度

密钥算法和长度应符合国家或行业相关安全标准要求，对不符合要求的(如



RSA 密钥长度 小于 2048 位、使用 MD5、SHA-1 等不安全算法), CA 机构应拒绝颁发证书。

6.2.6. 公钥参数的生成和质量检查

公钥参数由符合国家安全标准的密码设备或密码模块生成。对生成的公钥参数的质量检查, 同样由密码设备或密码模块进行, 这些设备内置的协议、算法等均符合国家或行业安全标准的要求。

6.2.7. 密钥使用目的

订户的签名密钥可以用于身份认证、不可抵赖性和信息的完整性保护等, 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。

6.3. 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

CA 系统生成密钥的密码模块(密码机)安置在机房屏蔽区域的核心区, 使用通过商用密码产品认证的密码机, 且至少符合 GB/T 37092-2018《信息安全技术密码模块安全要求》二级及以上。

CA 证书私钥的生成、更新、撤销、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 个管理员介质中, 只有其中超过半数以上管理员在场并许可的情况下, 才能对私钥进行上述操作。

CA 证书私钥备份由管理员分别存放在屏蔽机房的保险柜内。

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自己保管的, 订户应依据订户协议中的要求, 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。

CA 机构受订户委托保管签名私钥的, 采用的电子签名模式为 CA 机构的云平台响应订户的电子签名请求, 订户通过云平台的验证后, 调用云平台中托管的签名私钥实施电子签名。订户仅能通过安全授权认证(包括但不限于通过口令、短信验证码、生物识别信息、数字证书等)调用控制签名私钥, 以确保签名私钥控



制权由订户专有。CA 机构应每年对安全控制措施进行安全评估。CA 机构应向订户提供签名私钥及激活数据安全规范使用的指导，每次发起数字签名调用，必须取得订户明确授权，并完整留存相关授权记录。以上电子签名模式和安全控制措施具体应当符合相关标准或采用主管部门认可的其他方式。

订户加密证书对应的私钥由密钥管理中心托管，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。

6.3.3. 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。

6.3.4. 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。

6.3.5. 私钥导入或导出密码模块

CA 私钥在硬件密码模块中产生。在需要备份或迁移 CA 私钥时，从密码模块中导出的私钥必须由多人控制。

CA 机构不提供订户私钥从密码设备或密码模块中导出的方法。

6.3.6. 私钥在密码模块中的存储

CA 私钥存储在符合国家安全标准的密码设备中，这些设备内置的协议、算法等均符合国家或行业相关安全标准要求。

订户私钥在符合国家安全标准的密码设备或密码模块中加密保存。

6.3.7. 激活私钥的方法

对于 CA 私钥，具有激活私钥权限的管理员使用含有自己身份的安全介质（如智能 IC 卡、USBKey）登录，启动密钥管理程序，进行激活私钥的操作，需要超过半数以上管理员同时在场。

对于订户私钥，订户应提供 PIN 码等激活数据，或通过安全授权认证（包



括但不限于通过口令、短信验证码、生物识别信息、数字证书等)后才能被激活和使用。

6.3.8.解除私钥激活状态的方法

对于 CA 私钥,具有解除私钥激活状态权限的管理员使用含有自己身份的安全介质(如智能 IC 卡、USBKey)登录,启动密钥管理程序,进行解除私钥的操作,需要超过半数以上管理员同时在场。

6.3.9.销毁密钥的方法

对于 CA 私钥,具有销毁密钥权限的管理员使用含有自己身份的安全介质(如智能 IC 卡、USBKey)登录,启动密钥管理程序,进行销毁密钥的操作,需要超过半数以上管理员同时在场。

6.3.10.密码模块的评估

CA 机构使用通过检测认证的服务器密码机,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;

6.4. 密钥对管理的其他方面

6.4.1.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,归档最大间隔不超过证书失效后五年。



6.4.2. 证书操作期和密钥对使用期限

CA 证书的有效期和其对应的密钥对的有效期一致，有效期最长不超过 30 年，CA 证书到期后，签名私钥不可用于电子签名。

订户证书的有效期和其对应密钥对的有效期保持一致，有效期最长不超过 5 年，订户证书到期后，签名私钥不可用于电子签名。

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、传输和使用

激活数据用于保护订户的私钥。

CA 私钥的激活数据，必须按照密钥激活数据分割和密钥管理制度的要求，进行生成、分发和使用。

通用介质证书存储介质（如：智能密码钥匙）出厂时设置了缺省的 PIN 值，证书制作时更改此 PIN 值并通过安全的方式告知订户，订户可以自行设置或更改。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。

云端协同证书应通过安全授权认证（包括但不限于通过口令、短信验证码、生物识别信息、数字证书等）激活私钥并使用私钥。

6.5.2. 激活数据的保护

CA 私钥的激活数据按照可靠的方式分割后，由不同的可信人员掌管，且掌管人员必须符合职责分割的要求。

订户私钥的激活数据由订户采取妥善的方式保护，当发现激活数据失密，应告知 CA 机构并申请证书撤销。

6.5.3. 激活数据的销毁

当私钥的激活数据不需要时应该销毁，销毁的结果是无法通过残余信息、介质直接或间接获得激活数据的部分或者全部，比如记录有口令的纸张必须粉碎。



6.6. 计算机安全控制

6.6.1. 计算机安全控制要求

为了保证电子认证服务系统的正常运行，防范计算机系统被攻击、入侵、病毒感染等安全风险，保护订户信息及证书相关数据的保密性、完整性和可用性，CA 机构应建立并实施符合 GB/T 25056-2018 中 8.2 要求的计算机安全控制体系，实施全面的安全防护措施，具体要求包含但不限于以下内容。

- a) 系统升级补丁至少每半年检查一次，安装前需进行影响评估，经审批通过后方可实施，并做好审批及实施过程记录；
- b) 对无官方补丁支持的系统，制定网络隔离、功能限制等加强防护措施和系统更替计划；
- c) 对所有服务器和操作终端安装杀毒软件，并定期更新病毒库；
- d) 每月进行病毒库更新，若遇到重大病毒爆发、新型病毒出现等特殊情况，手动触发病毒库紧急更新；
- e) 每周进行病毒扫描。

6.6.2. 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。

6.7. 生存周期安全控制

6.7.1. 证书认证中心运行管理要求

CA 机构应按照 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》第 10 章要求建立证书认证中心运行管理体系。

6.7.2. 密钥管理中心运行管理要求

CA 机构应按照 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》第 11 章要求建立密钥管理中心运行管理体系。



6.7.3. 证书操作流程

CA 机构证书操作全流程遵循 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》第 12 章规定，覆盖证书申请、更新、撤销、用户加密密钥恢复、司法密钥恢复等全部环节。

6.8. 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 机构应采取防火墙、病毒防治、入侵检测、漏洞扫描等安全防护措施。

6.9. 时间戳

CA 机构部署有时间戳服务，该服务仅面向外部客户使用，通过时间戳接口的方式对外提供服务。保障机制方面，时间戳系统部署于安全的机房环境，并采用防火墙保障服务安全；同时，采用冗余部署方式保证时间戳服务的高可用性。时间源采用国家授时中心提供的标准时间，并配备专业运营团队，定期进行系统维护、数据备份、安全审计。

时间戳服务在技术实现上应遵循 GB/T 20520《网络安全技术 公钥基础设施时间戳规范》、GB/T 36631《信息安全技术 时间戳策略和时间戳业务操作规则》及国际标准时间戳协议（RFC3161）等技术标准。



7. 证书、证书撤销列表和在线证书状态协议

7.1. 证书

本 CA 机构签发的电子签名认证证书适用于企业信息化和电子商务等领域，可为订户提供身份认证、电子签名等服务。

订户可通过 CA 机构建立的数字证书注册通道提交证书申请，CA 机构按照本 CPS § 3 身份标识与查验的要求进行身份查验，查验通过后为订户签发证书。订户应妥善保管私钥和证书，或委托 CA 机构保管私钥。

本 CA 机构签发的数字证书符合《中华人民共和国电子签名法》、《电子认证服务管理办法》及《电子认证服务密码管理办法》等法律法规要求。本 CA 机构签发的数字证书格式符合 GB/T 20518《信息安全技术公钥基础设施 数字证书格式》的要求。

7.1.1. 版本号

X.509 V3。

7.1.2. 算法对象标识符

符合国家密码主管部门批准的算法对象标识符。

7.1.3. 证书序列号

证书序列号是 CA 分配给每张证书的一个十六进制正整数，且在 CA 的信任域内必须唯一。

7.1.4. 证书有效期

证书有效期是证书起始时间和终止时间的时间段，该时间段不应大于 CP 对于证书有效期的规定。

7.1.5. 名称形式

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。除 C 项、E 项外，其余各项使用 UTF8String 编码。

CA 证书 DN 格式如下：

C=CN

O=××

OU= ××

CN=××

- C (Country) 应为 CN，表示中国；
- O (Organization) 中内容通常为 BJCA；
- OU (Organization Unit) 中内容通常为 BJCA 或 CA 证书名称；
- CN (Common Name) 中内容为 CA 机构定义的 CA 证书名称。

订户证书主体 Subject 的 X.500 DN 支持多级 O 和 OU，其格式可选择如下：

C=CN;

S=××

L=××

O=××

O=××

OU= ××

OU=××

CN=××

- C (Country) 应为 CN，表示中国；
- S (State) 为可选项，S 中内容为省份；
- L (Locality) 为可选项，L 中内容为城市/地区；
- O (Organization) 为可选项，O 中的内容为证书主体或者证书主体所属单位名称全称；
- OU (Organization Unit) 为可选项，OU 中的内容为证书主体或者证书主体所属部门的名称全称或简称；
- CN (Common Name) 中的内容为：
 - a) 个人证书中应为证书主体的姓名，还可以包含其他标识信息；
 - b) 机构证书中应为证书主体机构的标准名称或简称，还可以包含其他标识信息（如机构证件代码等）。

订户不得使用可能侵犯他人知识产权的内容作为订户信息用于申请证书。CA 机构在受理证书申请时，查验记载在证书主体甄别名中的订户信息真实性，但并不验证该信息是否包含知识产权或处于知识产权纠纷中。

当发生有关知识产权的争议纠纷时，本 CA 机构有权拒绝相应的证书申请或撤销已发放的证书。



若证书 DN 中存在 E 项，应为证书主体的有效电子邮件地址。

7.1.6. 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，还支持私有扩展项。

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：电子签名认证证书包含的密钥用法为数字签名（digitalSignature）、不可抵赖（nonRepudiation）
- 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
- 证书策略 Certificate Policy：该项包含证书策略标识符，可区分证书等级和密钥存储方式（参考本 CPS § 1.3 的规定），该项还包含 CPS 发布地址
- 证书撤销列表分发点 CRL Distribution Points

私有扩展项可支持以下类型：

- 个人身份证号码 Identify Card Number
- 营业执照（统一社会信用代码）IC Registration Number

对于涉及用户隐私数据的私有扩展项（如个人身份证号码、个人社会保险号码、银行基本帐号信息），应以这些信息的某种映射录入证书，包括但不限于散列值、掩码等。

7.1.7. 订户电子签名验证数据

订户的电子签名验证数据是指用于验证电子签名的公钥。

7.1.8. CA 电子签名

CA 机构在签发数字证书时，使用 CA 的私钥对证书内容的哈希值进行加密，生成数字签名。



7.1.9. 其他信息

订户和依赖方可以通过查看电子签名认证证书中的信息了解证书用途、建立的流程、签名私钥的保存方式和相关的法律符合性。其中：

- 证书用途可以根据证书扩展项中的密钥用法了解，digitalSignature 表示该证书的密钥可以用于数字签名，nonRepudiation 表示该证书的密钥可以用于保护签名行为的不可抵赖，同时查看证书扩展项中证书策略项，根据该项 OID 对应了解该证书是否为高等级电子签名认证证书，判断是否适用于涉及生命健康、财产权益等高风险活动。
- 建立的流程、签名私钥的保存方式，可以从证书扩展项证书策略获取 CPS 的发布地址，浏览 CPS 了解具体的建立流程和签名私钥的保存方式。
- 相关法律法规的符合性：可以查看证书扩展项中证书策略项，证书策略中如果记录了本 CPS § 1.5.1 中主管部门的证书策略 OID，则表明该证书符合《中华人民共和国电子签名法》对电子签名认证证书的法律规定。

7.2. 证书撤销列表

CA 签发的证书撤销列表符合 GB/T 20518《信息安全技术公钥基础设施 数字证书格式》。

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

CA 机构的在线证书状态服务符合 GB/T 19713《信息安全技术公钥基础设施 在线证书状态协议》的要求。

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. 审计评估制度

CA 机构应制定审计评估制度，包括审计评估类型、执行审计评估的频率、参与执行审计评估人员的专业背景及审计评估所涵盖的主题和评估方法。

CA 机构应依据审计评估制度定期开展认证业务审计和全面符合性评估。

8.2. 认证业务审计

CA 机构开展认证业务审计是对业务全生命周期的检查，包括证书申请、续期、密钥变更、更新、撤销等环节，并对各环节中的订户告知、身份查验、意愿记录、协议签署、资料保存情况进行合规性检查。

CA 机构应每季度开展一次认证业务审计工作，审计过程中发现的问题，应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

CA 机构应依据法律法规、标准要求及内部制度规范，每年开展一次全面符合性评估工作。评估内容为 CA 机构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。评估过程中发现的问题，应通知被审计部门及时整改，并跟踪整改落实情况。

CA 机构应在每年 1 月底前将上一年度符合性评估报告报送主管部门。

8.4. 评估者资质

内部审计人员的选择一般包括：

- CA 的安全负责人及安全管理人员；
- CA 业务负责人；
- 认证系统及信息系统负责人；
- 人事负责人；
- 其他需要的人员。

外部审计的审计人员的资质由第三方确定。

8.5. 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。

9. 法律责任和其他业务条款

本章规定参见《北京数字认证电子签名电子认证业务规则 3.0.1 版》。