

北京数字认证股份有限公司 事件型证书策略（CP2）

1.0.7 版

发布日期：2024 年 10 月 24 日

生效日期：2024 年 10 月 24 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
1.0.1	版本发布	新版本发布	公司安全策略管理委员会	2017年11月9日
1.0.2	版本发布	内容修订更新	公司安全策略管理委员会	2019年9月27日
1.0.3	版本发布	内容修订更新	公司安全策略管理委员会	2020年4月26日
1.0.4	版本发布	内容修订更新	公司安全策略管理委员会	2021年9月3日
1.0.5	版本发布	内容修订更新	公司安全策略管理委员会	2022年8月15日
1.0.6	版本发布	内容修订更新	公司安全策略管理委员会	2023年2月6日
1.0.7	版本发布	内容修订更新	公司安全策略管理委员会	2024年10月24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

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. 引言	7
1.1. 概述	7
1.2. 文档名称与标识	7
1.3. PKI 参与者	8
1.3.1. 电子认证服务机构	8
1.3.2. 注册机构	8
1.3.3. 订户	8
1.3.4. 依赖方	8
1.3.5. 其他参与者	8
1.4. 证书应用	9
1.4.1. 适合的证书应用	9
1.4.2. 限制的证书应用	9
1.5. 策略管理	9
1.5.1. 策略文档管理机构	9
1.5.2. 联系人	9
1.5.3. 决定 CP 符合策略的机构	9
1.5.4. CP 批准程序	10
1.6. 定义和缩写	10
2. 信息发布与信息管理	11
2.1. 信息库	11
2.2. 认证信息的发布	11
2.3. 发布时间或频率	11
2.4. 信息库访问控制	11
3. 标识与鉴别	12
3.1. 命名	12
3.1.1. 名称类型	12
3.1.2. 对名称意义化的要求	12
3.1.3. 订户的匿名或伪名	12
3.1.4. 理解不同名称形式的规则	12
3.1.5. 名称的唯一性	12
3.1.6. 商标的承认、鉴别和角色	12
3.2. 初始身份确认	13
3.2.1. 证明持有私钥的方法	13
3.2.2. 订户身份的鉴别	13
3.2.3. 没有验证的订户信息	13
3.2.4. 授权确认	13
3.2.5. 互操作准则	13
3.3. 密钥更新请求的身份标识与鉴别	14
3.3.1. 常规密钥更新的标识与鉴别	14
3.3.2. 吊销后密钥更新的标识与鉴别	14



3.3.3. 证书变更的标识与鉴别	14
3.4. 吊销请求的标识与鉴别	14
4. 证书生命周期操作要求	15
4.1. 证书申请	15
4.1.1. 证书申请实体	15
4.1.2. 申请过程与责任	15
4.2. 证书申请处理	15
4.2.1. 执行识别与鉴别功能	15
4.2.2. 证书申请批准和拒绝	15
4.2.3. 处理证书申请的时间	16
4.3. 证书签发	16
4.3.1. 证书签发过程中电子认证服务机构的行为	16
4.3.2. 电子认证服务机构对订户的通告	16
4.4. 证书接受	16
4.4.1. 构成接受证书的行为	16
4.4.2. 电子认证服务机构对证书的发布	16
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	17
4.5. 密钥对和证书的使用	17
4.5.1. 订户私钥和证书的使用	17
4.5.2. 依赖方对公钥和证书的使用	17
4.6. 证书更新	17
4.7. 证书密钥更新	17
4.8. 证书变更	18
4.9. 证书吊销和挂起	18
4.9.1. 证书吊销的情形	18
4.9.2. 请求证书吊销的实体	18
4.9.3. 吊销请求的流程	18
4.9.4. 吊销请求宽限期	19
4.9.5. 电子认证服务机构处理吊销请求的时限	19
4.9.6. 依赖方检查证书吊销的要求	19
4.9.7. CRL 的颁发频率	19
4.9.8. CRL 发布的最长滞后时间	19
4.9.9. 吊销信息的其他发布形式	20
4.10. 证书状态服务	20
4.10.1. 操作特点	20
4.10.2. 服务可用性	20
4.10.3. 可选特征	20
4.11. 订购结束	20
4.12. 密钥生成、备份与恢复	20
4.12.1. 密钥生成、备份与恢复的策略和行为	20
4.12.2. 会话密钥的封装与恢复的策略和行为	21
5. 电子认证服务机构设施、管理和操作控制	22
6. 认证系统技术安全控制	23
6.1. 密钥对的生成和安装	23



6.1.1. 密钥对的生成	23
6.1.2. 私钥传送给订户	23
6.1.3. 公钥传送给证书签发机构	23
6.1.4. 电子认证服务机构公钥传送给依赖方	23
6.1.5. 密钥的长度	23
6.1.6. 公钥参数的生成和质量检查	23
6.1.7. 密钥使用目的	24
6.2. 私钥保护和密码模块工程控制	24
6.2.1. 密码模块标准和控制	24
6.2.2. 私钥的多人控制	24
6.2.3. 私钥托管	24
6.2.4. 私钥备份	24
6.2.5. 私钥归档	24
6.2.6. 私钥导入或导出密码模块	24
6.2.7. 私钥在密码模块中的存储	25
6.2.8. 激活私钥的方法	25
6.2.9. 解除私钥激活状态的方法	25
6.2.10. 销毁密钥的方法	25
6.2.11. 密码模块的评估	25
6.3. 密钥对管理的其他方面	25
6.3.1. 公钥归档	25
6.3.2. 证书操作期和密钥对使用期限	25
6.4. 激活数据	26
6.5. 计算机安全控制	26
6.5.1. 特别的计算机安全技术要求	26
6.5.2. 计算机安全要求	26
6.6. 生命周期技术控制	26
6.6.1. 系统开发控制	26
6.6.2. 安全管理控制	26
6.6.3. 生命周期的安全控制	26
6.7. 网络的安全控制	27
6.8. 时间戳	27
7. 证书格式	28
7.1. 证书	28
7.1.1. 版本号	28
7.1.2. 算法对象标识符	28
7.1.3. 名称形式	28
7.1.4. 证书扩展项	29
8. 电子认证服务机构审计和其他评估	30
8.1. 评估的频率或情形	30
8.2. 评估者的资质	30
8.3. 评估者与被评估者之间的关系	30
8.4. 评估内容	30
8.5. 对问题与不足采取的措施	30



8.6. 评估结果的传达与发布	30
9. 法律责任和其他业务条款	31

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，为电子活动提供网络信任环境。

数字认证公司面向即时业务等特定场景签发出事件型数字证书。事件型数字证书一般用于一次性事件型电子签名，签名过后私钥销毁。通过对签名行为业务场景的信息数据签名，证明业务数据自签名后未发生篡改，保证业务场景信息数据的完整性和签名行为的不可抵赖性。

证书策略（Certificate 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事件型证书策略》（以下简称“《事件型证书策略》”）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《事件型证书策略》适用范围为数字认证公司发放的事件型证书。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事件型证书策略（CP2）》，简称《事件型证书策略》，本证书策略 CP 的对象标识符为：1.2.156.112562.2.2.2。

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。

CA 机构可以授权下属机构或委托外部机构作为注册机构，负责提供证书业务办理、身份鉴证与审核等服务。

CA 机构授权外部机构作为注册机构，应在与外部机构签署的合同中，明确双方的权利与义务，以及承担的法律风险。

1.3.3. 订户

订户是指向 CA 机构申请数字证书的实体。

根据业务场景，事件型证书的订户分为两种，一种是电子签名人，一种是申请对签名行为业务场景的相关信息固化的实体。

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。

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 机构签发的证书适合应用在企业信息化、电子政务和电子商务等领域，用于证明业务场景中所进行的电子签名行为。

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。

1.5. 策略管理

1.5.1. 策略文档管理机构

本《事件型证书策略》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《事件型证书策略》的制订、发布、更新等事宜。

本《事件型证书策略》由北京数字认证股份有限公司拥有完全版权。

1.5.2. 联系人

本《事件型证书策略》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《事件型证书策略》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《事件型证书策略》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《事件型证书策略》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《事件型证书策略》：

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）**Certificate 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**

关于证书电子认证服务机构在签发、管理、吊销或更新证书(或更新证书中的密钥)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。但是，RA 并不签发证书（即 RA 代表 CA 承担某些任务）。

f) 事件型数字证书：**AnySign Certificate**

数字认证公司面向即时业务等特定场景签发出的数字证书。在业务过程中，根据订户提交的业务场景中相关信息（电子文档、签名行为特征信息、手写笔迹或其他签名行为证据信息等）自动固化至数字证书的扩展域，签发出事件型数字证书。事件型数字证书所对应的私钥为一次性使用，对业务场景的信息数据进行电子签名，在使用后即被销毁。

在本 CP 中，如无特殊定义，所述的数字证书，均指事件型数字证书。

g) 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。

h) 公钥 **Public Key**

非对称密码算法中可以公开的密钥。

2. 信息发布与信息管埋

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 和 CP 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

本《事件型证书策略》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

本《事件型证书策略》一经网站发布，即时生效。

2.4. 信息库访问控制

对于公开发布的 CP 和 CPS 等公开信息，数字认证公司允许公众自行通过网站进行查询和访问。

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

事件型证书的甄别名(DN)通常包含业务场景的相关数据信息，包括但不限于业务场景中的实体名称信息、笔迹信息、电子数据信息以及其他场景信息。

3.1.3. 订户的匿名或伪名

在 CA 证书服务体系中，除在特定场景下的事件型证书，原则上订户不使用匿名或伪名。

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 认证服务体系中，不同订户的证书主体的名称是唯一的。但对于同一订户，可以用其主体名为其签发多张证书，但证书的扩展项不同。

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

通过证书请求中所包含的数字签名来证明证书申请人持有与注册公钥对应的私钥。本 CA 机构在签发证书前，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，以此来判断证书使用者拥有私钥。

3.2.2. 订户身份的鉴别

事件型证书订户身份的鉴别参照个人或机构身份鉴别方法，CA 机构或授权的注册机构将验证申请文件的真实性，并进行批准申请或拒绝申请的操作。

订户身份的鉴别流程应当明确记录在按照本 CP 制定的 CPS 中。

3.2.3. 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。

3.2.4. 授权确认

当申请人代表委托人申请证书时，需要出示足够的证明信息或授权委托条款以证明个人或机构是否真实存在，申请人是否已获得委托人的授权。CA 机构和授权的注册机构有责任确认该授权信息，并将授权信息妥善保存。

3.2.5. 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《事件型证书策略》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力。

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

事件型证书的密钥只适用于一次性签名事件，没有证书密钥更新服务。

3.3.2. 吊销后密钥更新的标识与鉴别

事件型证书吊销后的密钥更新等同于订户重新申请证书，其要求与本 CP § 3.2 相同。

3.3.3. 证书变更的标识与鉴别

事件型证书的密钥只适用于一次性签名事件，没有证书变更服务。

3.4. 吊销请求的标识与鉴别

事件型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，其要求与本 CP § 3.2 相同。

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(包括政府机构、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《事件型证书策略》和《电子认证服务规则》所规定的要求,准备相关的身份证明材料提交至 CA 机构或授权的注册机构, CA 机构或授权的注册机构依据身份鉴别规范对证书申请人的身份进行鉴别,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 3.2 所述的有效身份证明材料,并确保材料真实准确,配合 CA 机构或授权的注册机构完成对身份信息的采集、记录和审核。

CA 机构: CA 机构参照 3.2 的要求对订户的身份信息进行采集、记录,审核。通过鉴证后, CA 机构向订户签发证书。如果用户身份信息的鉴别由授权的注册机构完成, CA 机构应对授权的注册机构进行监督管理和审计。

证书申请人应当提供真实、完整和准确的信息, CA 机构或其注册机构须按 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 CA 机构提供真实、完整和准确的信息,或者有其他过错,给 CA 机构或电子签名依赖方造成损失的,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 CA 机构或授权的注册机构提交初始的证书申请请求,注册机构须参照 3.2.2 节的规定对订户的申请材料进行审查。

4.2.2. 证书申请批准和拒绝

CA 机构或授权的注册机构根据本《事件型证书策略》所规定的身份鉴别流程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，CA 机构或授权的注册机构将批准证书申请，CA 为证书申请人制作并颁发数字证书。

证书申请人未能通过身份鉴证，CA 机构或授权的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。

4.2.3. 处理证书申请的时间

事件型证书申请为即时处理。

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為

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

事件型证书用于标识和证明订户的电子签名行为。CA 机构为订户签发证书后，将直接应用于对应的业务场景相关信息的电子签名。订户成功完成电子签名，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。

4.4. 证书接受

4.4.1. 构成接受证书的行为

事件型证书签发完成后，并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。

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

对于 CA 签发事件型证书，CA 机构不对其他实体进行通告。

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 机构和依赖方有关的权利和义务的条款。

事件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。私钥将在完成本次电子签名数学运算后进行销毁，之后订户须停止使用该证书对应的私钥。

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）。依赖方获得证书和公钥后，可以通过查看证书了解签名行为业务场景相关信息，并通过公钥验证电子签名的真实性。

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. 证书更新

事件型证书仅用于业务场景的一次性的电子签名，不提供证书更新服务。

4.7. 证书密钥更新

事件型证书私钥在使用过一次后即销毁，不提供证书密钥更新服务。

4.8. 证书变更

事件型证书仅用于业务场景的一次性的电子签名，不提供证书变更服务。

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) 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 CA 机构或授权的注册机构书面或在线提交证书吊销申请，并注明吊销原因；

b) CA 机构或授权的注册机构根据本 CP 3.2 的要求对订户提交的吊销请求进行审核；

c) CA 吊销订户证书后，订户证书即无法进行任何电子签名，订户证书在 24 小时内进入 CRL，向外界公布；

强制吊销是指当 CA 机构或授权的注册机构确认发生本 CP 4.9.1 b) 强制吊销证书情形时，对订户证书进行强制吊销，吊销后将通过官网公告、注册机构或其他安全可行的方式通告订户。

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，依赖方可以使用 CRL 查询功能进行所依赖证书的状态查询：

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。

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 发布的最长滞后时间

CRL 发布的最长滞后时间为 24 小时。

4.9.9. 吊销信息的其他发布形式

证书吊销信息通过 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

事件型证书状态可以通过 CA 机构提供的 CRL 服务查询。

4.10.2. 服务可用性

提供 7X24 小时的证书状态查询服务。即在网络允许的情况下，订户能够实时获得证书状态查询服务。

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

事件型证书订购结束是指当订户使用数字证书完成电子签名后，该证书的服务时间结束。

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签名设备生成密钥并执行签名后，即时销毁，签名密钥不进行保管。

订户的加密密钥对由密钥管理中心生成。

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。

事件型证书的签名密钥对由签名设备生成，加密密钥对由密钥管理中心生成。

6.1.2. 私钥传送给订户

事件型证书的签名密钥对由签名设备生成并保管。加密密钥对由密钥管理中心产生，通过安全通道传递给证书申请方。

6.1.3. 公钥传送给证书签发机构

事件型证书的签名公钥通过安全通道，经注册机构传递到 CA 机构。

从 RA 到 CA 以及从密钥管理中心到 CA 的传递过程中，采用国家密码管理部门许可的通讯协议及密钥算法，保证了传输中数据的安全。

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，实现身份认证、不可抵赖性和信息的完整性等，用于签署具备法律效力的电子文档和电子交易数据。

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，其接口、协议、密钥和物理安全要符合国家相关规范要求。

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管理员在场并许可的情况下，才能对私钥进行上述操作。

6.2.3. 私钥托管

无。

6.2.4. 私钥备份

CA 私钥备份在专用密码设备中。

6.2.5. 私钥归档

通过数据库备份出来进行归档保存。

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，CA 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

CA 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 机构应使用具有国家密码管理部门认可的商用密码产品，采用的服务器密码机符合国家有关标准。

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

所有事件型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

无。

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。

6.5.2. 计算机安全要求

CA 系统建设应符合 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》的第三级要求。

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主管部门鉴定，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. 证书格式

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。除 C 项外，其余各项使用 UTF8String 编码。

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

C=CN;

O=××

OU= ××

CN=××

- C (Country) 应为 CN，表示中国；
- O (Organization) 应为证书主体或者签名行为业务场景所关联组织的上一级单位名称，或所在省、自治区、直辖市名称全称。可选部分；
- OU (Organization Unit) 应为证书主体或者签名行为业务场景所关联组织的名称全称。可选部分；
- CN (Common Name) 中的内容代表签名行为业务场景的相关信息，分两种：
 - a) 当订户是电子签名人时，CN 中的内容是订户的名称；
 - b) 当订户是申请对签名行为业务场景相关信息进行固化的实体时，CN 中的内容可以是实体名称，也可以是需要固化的签名行为相关信息。

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，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
- 使用者密钥标识符 Subject Key Identifier
- 密钥用法 Key Usage

私有扩展项可支持以下类型：

- 个人身份证号码 Identify Card Number
- 企业营业执照（统一社会信用代码）IC Registration Number
- 签名证据项：Signature Evidences，应包含签名相关证据内容，如声音、图像等。

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《事件型证书策略》和《电子认证业务规则》及其理制度和策略开展业务，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。