北京数字证书认证中心
电子认证业务规则

2.0.1 版

发布日期：2005 年 7 月 18 日

生效日期：2005 年 7 月 18 日

北京数字证书认证中心有限公司

目 录

1. 概括性描述

1.1 概述

北京数字证书认证中心电子认证业务规则（以下简称《电子认证业务规则》）由北京数字证书认证中心有限公司按照信息产业部《电子认证服务管理办法》的要求，依据《电子认证业务规则规范(试行)》制定，并报信息产业部备案。

北京数字证书认证中心有限公司（Beijing Certificate Authority，简称 BJCA）于 2001 年 2 月开始运营，是权威、公正的电子认证服务机构。BJCA 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，提供数字证书申请、颁发、存档、查询、废止等服务，并通过以 PKI 技术、数字证书应用技术为核心的应用安全解决方案，为电子政务、电子商务、企业信息化构建安全、可靠的信任环境。

本《电子认证业务规则》详细阐述了 BJCA 在实际工作和运行中所遵循的各项规范。本《电子认证业务规则》适用于 BJCA 及其员工、注册机构、证书申请人、订户和依赖方，各参与方必须完整地理解和执行本《电子认证业务规则》所规定的条款，并承担相应的责任和业务。

1.2 文档名称与标识

本文档名称是《北京数字证书认证中心电子认证业务规则》。

1.3 电子认证活动参与方及其职责

1.3.1 电子认证服务机构

BJCA 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。

电子认证服务机构是受用户信任，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

注册机构做为电子认证服务机构授权委托的下属机构，包括注册系统（RA 系统）和证书本地受理点，负责受理证书申请。

1.3.3 订户

订户是从 BJCA 接收数字证书的实体。在电子签名应用中，订户即为电子签名人。

1.3.4 依赖方

依赖方是依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个订户。在 BJCA 证书服务体系中，是信任 BJCA 证书，可以对使用 BJCA 证书机制进行的数字签名进行验证，使用其他 BJCA 证书的公钥的实体。

1.3.5 其他参与者

其他参与者指为 BJCA 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

证书类型及用途参见 BJCA 网站(http://www.bjca.org.cn)上的介绍，证书申请人根据实际需要，决定采用哪种证书类型。

1.4.2 限制的证书应用

BJCA 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《电子认证业务规则》的管理机构是 BJCA CPS 策略管理委员会。由 BJCA CPS 策略管理委员会负责本《电子认证业务规则》的制订、发布、更新等事宜。

1.5.2 联系人

本《电子认证业务规则》在 BJCA 网站发布，对具体个人不另行通知。

网站地址：http://www.bjca.org.cn

电子邮箱地址：cps@bjca.org.cn

联系地址：中华人民共和国北京市西城区裕民东路 3 号京版信息港 2 层(100029)

电话号码：8610-82031677

传真号码：8610-82031599

1.5.3 决定 CPS 符合策略的机构

本《电子认证业务规则》由 BJCA CPS 策略管理委员会，组织制定，报 BJCA CPS 策略管理委员会批准实行。

1.5.4 CPS 批准程序

本《电子认证业务规则》由 BJCA CPS 策略管理委员会，组织 CPS 编写小组。编写小组完成编写 CPS 草案后，由 BJCA CPS 策略管理委员会组织对 CPS 草案进行初步评审。初步评审后，将 CPS 评审稿提交 BJCA CPS 策略管理委员会审批。经 BJCA CPS 策略管理委员会审批通过后，在 BJCA 的网站上对外公布。

本《电子认证业务规则》经 BJCA CPS 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信息产业部备案。

1.6 定义和缩写

下列定义适用于本《电子认证业务规则》：

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) 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。

c) 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。

d) 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，在某些环境下主动撤销或挂起证书，处理订户撤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）。

e) 电子签名认证证书(证书)Digital Certificate

是电子认证服务提供者签发的用以证明证书持有人的电子签名、身份、资格及其他有关信息的电子文件。证书包含有公开密钥拥有者的信息、公开密钥、签名算法和 CA 的数字签名。

f) 证书撤销列表 (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。

g) CA 注销列表(ARL)：Certificate Authority Revocation List

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

h) 私钥(电子签名制作数据) Private Key

指在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。

私钥是经由数字运算产生的密钥，用于制作电子签名数据，亦可依据其运算方式，就相对应的公开密钥加密的文件或信息予以解密。

i) 公钥(电子签名验证数据) Public Key

公钥是经由数字运算产生的密钥，用于解密电子签名，确认电子签名人的身份及电子签名的真实性。

公钥可以公开，一般标示于在线数据库、存储库或其他公共目录中，使任何希望得到公钥的人都能得到。

电子签名验证数据是指用于验证电子签名的数据，包括代码、口令、算法或者公钥等。如果电子签名制作数据表现为私钥，则电子签名验证数据就是公钥。

2. 信息发布与信息管理

2.1 认证信息的发布

BJCA 通过网站公布以下信息：《电子认证业务规则》修订以及其他由 BJCA 不定时发出的信息。BJCA 网址：http://www.bjca.org.cn。

本《电子认证业务规则》发布在 BJCA 的网站上，供相关方下载、查阅。

BJCA 通过目录服务器发布订户的证书和 CRL，订户或信赖方可以通过访问 BJCA 的目录服务器获取证书的信息和吊销证书列表。同时，BJCA 提供在线证

书状态查询服务。

2.2 发布时间或频率

a) 《电子认证业务规则》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。对具体个人不另行通知。
b) 证书的发布：在证书签发时，BJCA 通过目录服务器自动将该证书公布。
c) BJCA 的 CRL 每 24 小时发布一次。

2.3 信息库访问控制

对于公开发布的 CPS、证书、CRL 等公开信息，BJCA 允许公众自行通过网站和目录服务器进行查询和访问。

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

3. 身份标识与鉴别

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。

证书主体名称标识本证书所提到的最终实体的特定名称，描述了与主体公钥中的公钥绑定的实体信息。

3.1.3 订户的匿名或伪名

在 BJCA 证书服务体系中，订户（证书申请人）不宜使用匿名或伪名。

3.1.4 理解不同名称形式的规则

DN 的具体内容依次由 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。

3.1.5 名称的唯一性

在 BJCA 证书服务体系中，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

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。在 BJCA 证书服务体系中，私钥在用户端生成，证书请求信息中包含用私钥进行的数字签名，CA 用其对应的公钥来验证这个签名。

BJCA 要求证书申请人妥善保管自己的私钥，因此，证书申请人视作其私钥的唯一持有者。

3.2.2 组织身份的鉴别

对于组织身份的鉴别，BJCA 需要验证组织的合法证件。证书申请人需持工商营业执照或全国组织机构代码证书等证件，以及组织给经办人的授权和经办人身份证件，向 CA 机构提出申请。如该企业需申请服务器类型的证书，还需向注册机构提交域名证明文件。

组织身份的鉴别规范简要说明了如何进行组织身份鉴别。BJCA 保留根据最新国家政策法规的要求更新组织身份鉴别规范的权利。更新后的组织身份鉴别规范将发布在 BJCA 的网站上：http://www.bjca.org.cn。

经办人经组织授权，并携带组织授权给经办人申请办理证书事宜的授权文件及本人身份证的原件和复印件，到 BJCA 授权的注册机构提交书面数字证书申请表(一式两份)及下述组织证明文件等申请资料，并缴纳证书服务费用。

a) 组织机构代码证的副本及复印件；
b) 法人营业执照副本及复印件，如果组织没有营业执照，则书面申请表上可选其他有效证件的的副本及复印件，部分有效证件如下：
    1) 企业法人营业执照
    2) 事业单位法人登记证
    3) 事业单位登记证
    4) 社会团体登记证
    5) 地税税务登记证
    6) 政府批文
    7) 其他有效证件
c) 经办人有效身份证件的原件和复印件；
d) 如该组织需申请服务器类型的证书，还需向注册机构提交域名使用权证明材料。

（注：以上 a)、b) 和 d)证明文件的复印件需加盖申请单位公章）。

BJCA 授权的注册机构按照 BJCA 组织身份鉴别规范对申请资料的原件和复印件真实性进行审核，并进行批准申请或拒绝申请的操作。

批准申请后，BJCA 或注册机构将保留相关盖单位公章的证明材料复印件，与证书申请表一并存档保存。

3.2.3 个人身份的鉴别

个人身份的鉴别可以使用以下有效的身份证件：港澳台居民身份证、户口簿、护照、军官证、警官证、外国人永久居留证、士兵证、身份证、士官证和文职干部证。

个人身份的鉴别规范简要说明了如何进行个人身份鉴别。BJCA 保留根据最新国家政策法规的要求更新个人身份鉴别规范的权利。更新后的个人身份鉴别规范将发布在 BJCA 的网站上：http://www.bjca.org.cn。

个人需持上述个人有效身份证件，到 BJCA 授权的注册机构提交书面数字证书申请表(一式两份)和上述有效身份证件的复印件等申请资料，并缴纳证书服务费用。

BJCA 授权的注册机构按照 BJCA 个人身份鉴别规范对申请资料的原件和复印件真实性进行审核，并进行批准申请或拒绝申请的操作。

批准申请后， BJCA 或注册机构将保留复印件，与证书申请表一并存档保存。

3.2.4 没有验证的订户信息

订户提交鉴证文件以外的信息为没有验证的订户信息。

3.2.5 授权确认

为确保办理人具有特定的许可，代表组织获取数字证书，需要出具组织授权其该组织为办理 BJCA 数字证书事宜的授权文件。

组织在 BJCA 的数字证书申请表上加盖单位公章后，则证明本组织对办理人的授权确认。

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。

BJCA 将根据业务需要，在遵循本《电子认证业务规则》的各项控制要求的基础上，与 BJCA 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 BJCA 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

在常规密钥更新中，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，BJCA 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

吊销后密钥更新中对身份标识和鉴别的要求，使用原始身份验证相同的流程，详见§3.2.2 组织身份的鉴别和 3.2.3 个人身份的鉴别。

3.4 吊销请求的标识与鉴别

订户本人吊销时的身份标识和鉴别使用原始身份验证相同的流程，详见§3.2.2 组织身份的鉴别和 3.2.3 个人身份的鉴别。

如果是因为订户没有履行本《电子认证业务规则》所规定的义务，由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《电子认证服务规则》所规定的要求，填写证书申请表，并准备相关的身份证明材料。BJCA 或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：订户要按照本《电子认证服务规则》的要求准备证书申请材料，并确保申请材料真实准确。

注册机构负责接收证书申请人的请求材料，当面对订户所提供的证书申请信息与身份证明资料的一致性进行查验。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

BJCA 或授权的注册机构按照本《电子认证业务规则》所规定的身份鉴别流程对申请人的身份进行识别与鉴别。具体的鉴别流程详见§3.2.2 组织身份的鉴别和 3.2.3 个人身份的鉴别。

4.2.2 证书申请批准和拒绝

BJCA 或授权的注册机构根据本《电子认证业务规则》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。

如果证书申请人通过本《电子认证业务规则》所规定的身份鉴别流程且鉴证结果为合格，BJCA 或注册机构将批准证书申请，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，BJCA 或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

BJCA 授权的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 24 小时内处理证书申请。

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 BJCA 的管理要求。

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

BJCA 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。

通常，BJCA 所签发的证书在 24 小时后才生效。

4.3.2 电子认证服务机构对订户的通告

电子认证服务机构通过注册机构，对订户的通告有以下几种方式：

a) 通过面对面的方式，通知订户到注册机构领取数字证书；注册机构把密码信封和证书等直接提交给订户，来通知订户证书信息已经正确生成；
b) 邮政信函通知订户；
c) 其他 BJCA 认为安全可行的方式通知订户。

4.4 证书接受

4.4.1 构成接受证书的行为

数字证书签发完成后，注册机构将数字证书及其密码信封当面或寄送给证书申请人，证书申请人从获得数字证书起，就被视为同意接受证书。

4.4.2 电子认证服务机构对证书的发布

BJCA 在签发完证书后，就将证书发布到数据库和目录服务器中。

BJCA 采用主、从目录服务器结构来分布所签发证书。签发完成的数据直接写入主目录服务器中，然后通过主从映射，将主目录服务器的数据自动发布到从目录服务器中，供订户和依赖方查询和下载。

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

其他实体可以通过从目录服务器中查询到 BJCA 已经签发的数字证书。

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 BJCA 所签发的证书后，均视为已经同意遵守与 BJCA、依赖方有关的权利和义务的条款。订户接受到数字证书，应妥善保存其证书对应的私钥。

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吊销之后，订户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，可以通过查看对方的证书了解对方的身份，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三个方面的内容：

a) 用 BJCA 的证书验证证书中的签名，确认该证书是 BJCA 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) 查询证书状态，确认该证书没有被注销。

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 证书更新

4.6.1 证书更新的情形

证书更新是指在不改变证书中订户的公钥或其他任何信息的情况下，为订户签发一张新证书。

在证书上都有明确的证书有效期，表明该证书的起始日期与截至日期。订户应当在证书有效期到期前，到 BJCA 授权的注册机构申请更新证书。

证书更新的具体情形如下：

a) 证书的有效期将要到期；

b) 密钥对的使用期将要到期；

c) 因私钥泄漏而吊销证书后，就需要进行证书更新；

d) 其他。

4.6.2 请求证书更新的实体

订户可以请求证书更新。订户包括持有 BJCA 签发的个人、组织及设备等各类证书的证书持有人。

4.6.3 证书更新请求的处理

处理证书更新请求可以采用两种方式：

一种方式是在线自动更新。对于证书信息无须改变的订户，在证书即将过期的时，在获得 BJCA 授权后，自助进行在线证书更新操作，获得新证书。

另一种方式是人工方式更新。对于证书信息发生改变的订户，由注册机构来处理证书更新请求，为订户制作新的证书。

注册机构对申请证书更新订户的进行查验与鉴别，鉴别要求同本《电子认证业务规则》3.2.2 和 3.2.3。

4.6.4 颁发新证书时对订户的通告

在线自动更新方式，在自动完成更新，给订户颁发新证书时，在线更新系统会自动通知证书更新已完成，新证书已颁发。

人工更新方式，对订户的通告有以下几种方式：

a） 通过面对面的方式，通知证书更新已完成，新证书已颁发；

b） 邮政信函通知订户；

c) 其他 BJCA 认为安全可行的方式通知订户。

4.6.5 构成接受更新证书的行为

在线更新方式，当订户对在线系统提示证书更新已完成，新证书已颁发进行确认时，就表示订户接受更新证书。

人工更新方式，当更新证书签发后，注册机构将证书及其密码信封当面或寄送给订户，就表示订户接受更新证书。

4.6.6 电子认证服务机构对更新证书的发布

BJCA 在签发更新证书后，就将更新证书发布到数据库和目录服务器中，对外进行发布。

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

其他实体可以通过从目录服务器中查询已更新的数字证书。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

a) 证书的有效期将要到期，证书更新；
b) 因私钥泄漏而吊销证书；
c) 其他。

4.7.2 请求证书密钥更新的实体

请求证书密钥更新的实体同 4.6.2。

4.7.3 证书密钥更新请求的处理

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

颁发新证书给订户的通告同 4.6.4。

4.7.5 构成接受密钥更新证书的行为

正式接受密钥更新证书的行为同 4.6.5。

4.7.6 电子认证服务机构对密钥更新证书的发布

BJCA 对密钥更新证书的发布同 4.6.6。

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

BJCA 在颁发证书时对其他实体的通告同 4.6.7。

4.8 证书吊销和挂起

4.8.1 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数字证书认证业务规则。
b) 发生下列情形之一的，BJCA 可以吊销其签发的数字证书：
   1) 订户申请吊销数字证书；
   2) 订户提供的信息不真实；
   3) 订户没有履行双方合同规定的义务；
   4) 数字证书的安全性得不到保证；
   5) 法律、行政法规规定的其他情形。

4.8.2 请求证书吊销的实体

根据不同的情况，订户、BJCA、注册机构可以请求吊销最终用户证书。

4.8.3 吊销请求的流程

证书吊销请求的处理采用与原始证书签发相同的过程。

a) 证书吊销的申请人到 BJCA 授权的注册机构书面填写《证书吊销申请表》，并注明吊销原因；
b) BJCA 授权的注册机构根据 3.2 的要求对订户提交的吊销请求进行审核；

c) BJCA 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 BJCA 或 BJCA 授权的注册机构确认用户违反本《电子认证业务规则》的情况发生时，对订户证书进行强制吊销，吊销后将立即通知该订户。

4.8.4 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。

4.8.5 电子认证服务机构处理吊销请求的时限

发证机构接到吊销请求后立即处理，24 小时生效。BJCA 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(issure)
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) CRL 条目扩展项(crl entry extensions)
h) CRL 扩展域(crl extensions)
i) 签名算法(signature algorithm)
j) 签名(signature value)

4.8.6 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 BJCA 发布并且签名的。

4.8.7 CRL 的颁发频率

BJCA 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。

4.8.8 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 证书状态服务

4.9.1 操作特点

BJCA 通过目录服务器为用户提供证书状态服务。

4.9.2 服务可用性

BJCA 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。

4.9.3 可选特征

根据请求者的要求，在请求者支付相关费用后，BJCA 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，BJCA 将通知请求该项服务的请求者。

4.10 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。

4.11 密钥生成、备份与恢复

4.11.1 密钥生成、备份与恢复的策略和行为

订户的签名密钥对由订户的密码设备（如智能 USB KEY 或智能 IC 卡）生成，加密密钥对由密钥管理中心生成。

签名密钥对由订户的密码设备保管。

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。

a) 订户密钥恢复：当订户的密钥损坏或丢失后，某些密文数据将无法还原，此时订户可申请密钥恢复。订户在 BJCA 授权的发证机构申请，经审核后，通过 BJCA 向 KMC 请求；密钥恢复模块接受订户的恢复请求，恢复订户的密钥并下载于订户证书载体中。

b) 司法取证密钥恢复：司法取证人员在 KMC 申请，经审核后，由密钥恢复模块恢复所需的密钥并记录于特定载体中。

具体策略在 6.1 和 6.2 中详细描述。

4.11.2 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. 电子电子认证服务机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

a) BJCA 的建筑物和机房建设按照下列标准实施：
   1) GB 50174-93：《电子计算机机房设计规范》
   2) GB 2887-89：《计算站场地技术条件》
   3) GB 9361-88：《计算站场地安全要求》
   4) GB 6650-1986：《计算机机房用活动地板技术条件》
   5) GB 50034-1992：《工业企业照明设计标准》
   6) GB 5054-95：《低压配电装置及线路设计规范》
   7) GBJ 19-87：《采暖通风与空气调节设计规范》
   8) GB 157：《建筑防雷设计规范》
   9) GBJ 79-85：《工业企业通信接地设计规范》

b) BJCA 机房位于北京市中央电视塔首层机房，实行分层访问的安全管理：BJCA 的功能区域划分为六个层次，四个区域。

六个层次由外到里分别是：入口、办公、敏感、数据中心、屏蔽机房、保密机柜。

四个区域由外到里分别是：公共区域、DMZ 区域（非军事区）、操作区域和安全区域。

其中，入口之外的区域为公共区域，入口和办公层位于 DMZ 区，敏感层位于操作区，其他各层位于安全区。

5.1.2 物理访问

为了保证本系统的安全，采取了一定的隔离、控制、监控手段。机房的所有门都足够结实，能防止非法的进入。机房通过设置门禁和侵入报警系统来重点保护机房物理安全。

物理访问控制包括如下几个方面：

a) 门禁系统：控制各层门的进出。工作人员需使用身份识别卡结合指纹鉴定才能进出，进出每一道门应有时间纪录和信息提示。
b) 报警系统：当发生任何非法闯入、非正常手段的开门、长时间不关门等异常情况都应触发报警系统。报警系统明确指出报警位置。

c) 监控系统：与门禁和物理侵入报警系统配合使用的还有录像监控系统，对安全区域和操作区域进行 24 小时不间断录像。所有录像资料需要保留，以备查询。

门禁和物理侵入报警系统备有 UPS，并提供至少 8 小时的不间断供电。

5.1.3 电力与空调

机房电源供电系统包括机房区的动力、照明、监控、通讯、维护等用电系统，按负荷性质分为计算机设备负荷和辅助设备负荷，计算机设备和动力设备分开供电。供配电系统的组成包括配电柜、动力线缆、线槽及插座、接地防雷、照明箱及灯具、应急灯、照明线管等。计算机设备专用配电柜和辅助设备配电柜独立设置。

使用不间断电源（UPS）来保证供电的稳定性和可靠性。采用双电源，在单路电源损坏时，可以自动切换，维持系统正常运转。

根据机房环境及设计规范要求，主机房和基本工作间，均设置了空气调节系统。空调系统使用中央空调，并采用独立空调作为备份。其组成包括精密空调、通风管路、新风系统。

BJCA 的要求参照电信设施管理的规定，而且每年对物理系统的安全性进行检查。

5.1.4 水患防治

机房内无渗水、漏水现象，主要设备采用专用的防水插座，并采取必要措施防止下雨或水管破损，造成天花板漏水、地板渗水和空调漏水等现象。

BJCA 的系统有充分保障，能够防止水侵蚀。

目前机房内无上下水系统，空调间做了严格防水处理，由漏水检测系统提供（7X24）实时检测。

5.1.5 火灾预防和保护

火灾预防：

a) 敏感区（物理三层）、高度敏感区域（物理四、五、六层），其建筑物的耐火等级必须符合 GBJ45《高层民用建筑设计防火规范》中规定的二级耐火等级。
b) BJCA 设施内设置火灾报警装置。在机房内、各物理区域内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位设置烟、温感探测器。
c) 敏感区及高敏区配置独立的气体灭火装置，使用七氟丙烷（HFC-227ea）

等洁净气体灭火系统，备有相应的气体灭火器，非敏感区根据实际情况可配置水喷淋灭火装置。BJCA 内除对纸介质等易燃物质进行灭火外，禁止使用水、干粉或泡沫等易产生二次破坏的灭火剂。

d) 火灾自动报警、自动灭火系统避开可能招致电磁干扰的区域或设备，同时配套设置消防控制室。还设有不间断的专用消防电源和直流备用电源，并具有自动和手动两种触发装置。

e) 火灾自动灭火设施的区域内，其隔墙和门的耐火极限不低于 1 小时，吊顶的耐火极限不得低于 15 分钟。

f) 在非敏感区及敏感区的办公区域内，须设置紧急出口，紧急出口必须设有消防门，消防门符合安全要求。紧急出口门外部不能有门开启的装置，且紧急出口门须与门禁报警设备联动外，需装配独立的报警设备。

g) 紧急出口有监控设备进行实时监控，并保证紧急出口门随时可用。BJCA 采取适当的管理手段来保障非紧急避险状态下，紧急出口门不能被内部人员任意打开。

灭火系统采用电动，手动，紧急启动三种方式：

a) 电动方式：防护区报警系统第一次火警确认后，发出声光警示信号，切断非消防电源（如：空调电源、照明电源等）。并送排风（烟），防火阀关闭。第二次火警确认后，经延时，同时发出气体释放信号，并发出启动电信号，送给对应的管网启动钢瓶，喷气灭火。

b) 手动方式：人员对钢瓶或药剂瓶直接开启操作。

c) 紧急启动：防护区外设有紧急启动按钮供紧急时使用。

BJCA 通过与专业防火部门协调，实施消防灭火等应急响应措施。

5.1.6 介质存储

BJCA 的存储介质包括硬盘、软盘、磁带、光盘等，介质存储地点和 BJCA 系统分开并且保证物理安全，注意防磁、防静电干扰、防火、防水，由专人管理。

5.1.7 废物处理

当 BJCA 存档的敏感数据或密钥已不再需要或存档的期限已满时，应当将这些数据进行销毁。写在纸张之上的，必须切碎或烧毁。如果保存在磁盘中，应多次重写覆盖磁盘的存储区域，其他介质以不可恢复原则进行相应的销毁处理。

5.1.8 异地备份

BJCA 办公区位于北京市西城区裕民东路 3 号，与机房在不同的地方。所备份的业务数据磁带每周运送到位于异地的 BJCA 办公区，进行异地备份保存。

5.2 程序控制

5.2.1 可信角色

电子认证服务机构、注册机构、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：

a) 系统管理员

系统管理员负责对数字证书服务体系在本单位的系统进行日常管理，执行系统的日常监控，并可根据需要签发服务器证书和下级操作员证书。

b) 安全管理员

安全管理员对数字认证中心的物理、网络、系统的安全全面负责。并且拟订安全管理制度和操作流程，监督各岗位安全管理的执行情况。

c) 审计管理员

审计管理员控制、管理、使用安全审计系统，安全审计系统分布于证书管理系统的各个子系统中，负责各个子系统的运行和操作日志记录。

d) 密钥管理员

密钥管理员负责管理数字认证中心的密钥相关设备，进行 CA 中心密钥的生成、备份、恢复、销毁等操作。

e) 证书业务管理员

证书业务管理员对注册机构操作员进行管理，并对注册机构业务进行管理。

f) 证书业务操作员

证书业务操作员进行录入、审核、制作等证书业务操作，直接对用户提供服务。

5.2.2 每个角色的识别与鉴别

所有 BJCA 的在职人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用门禁卡和指纹识别；进入系统需要使用数字证书进行身份鉴别。BJCA 将独立完整地记录其所有的操作行为。

5.2.3 需要职责分割的角色

为保证系统安全，遵循可信角色分离的原则，即 BJCA 的可信角色由不同的人担任。

至少两个人以上才能使用一项对参加操作人员保密的密钥分割和合成技术，来进行任何密钥恢复的操作。

5.3 人员控制

5.3.1 资格、经历和无过失要求

所有的员工与 BJCA 签定保密协议。对于充当可信角色或其他重要角色的人员，必须具备的一定的资格，具体要求在人事管理制度中规定。BJCA 要求充当可信角色的人员至少必须具备忠诚、可信赖及工作的热诚度、无影响 CA 运行的其它兼职工作、无同行业重大错误记录、无违法记录等。

5.3.2 背景审查程序

BJCA 与有关的政府部门和调查机构合作，完成对 BJCA 可信任员工的背景调查。

所有目前的可信任员工和申请调入的可信任员工都必须书面同意对其进行背景调查。

背景调查分为：基本调查和全面调查。

基本调查包括对工作经历，职业推荐，教育，社会关系方面的调查。

全面调查除包含基本调查项目外还包括对犯罪记录，社会关系和社会安全方面的调查。

调查程序包括：

a) 人事部门负责对应聘人员的个人资料予以确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。
b) 人事部门通过电话、信函、网络、走访、等形式对其提供的材料的真实性进行鉴定。
c) 用人部门通过现场考核、日常观察、情景考验等方式对其考察。
d) 经考核，人事部门和用人部门联合填写《可信雇员调查表》，报主管领导批准后准予上岗。

5.3.3 培训要求

BJCA 对运营人员按照其岗位和角色安排不同的培训。培训有：系统硬件安装与维护、系统软件运行与维护、系统安全、应用软件的运行和维护、CA 中心的运行管理、CA 中心的内部管理、政策和规定及系统备份与恢复等。

对于运营人员，其 CA 的相关知识与技能，每年至少要总结一次并由 BJCA 组织培训。技术的进步、系统功能更新或新系统的加入，都需要对相关人员进行培训。

5.3.4 再培训周期和要求

对于充当可信角色或其他重要角色的人员，每年至少接受 BJCA 组织的培训一次。

认证策略调整、系统更新时，应对全体人员进行再培训，以适应新的变化。

5.3.5 工作轮换周期和顺序

对于可替换角色，BJCA 将根据业务的安排进行工作轮换。轮换的周期和顺序，视业务的具体情况而定。

5.3.6 对未授权行为的处罚

当 BJCA 员工被怀疑，或者已进行了未授权的操作，例如滥用权利或超出权限使用 BJCA 系统或进行越权操作，BJCA 得知后将立即对该员工进行工作隔离，随后对该员工的未授权行为进行评估，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施。对情节严重的，依法追究相应责任。

5.3.7 独立合约人的要求

对不属于 BJCA 内部的工作人员，但从事 BJCA 有关业务的人员等独立签约者(如注册机构的工作人员)，BJCA 的统一要求如下：

a) 人员档案进行备案管理；
b) 具有相关业务的工作经验；
c) 必须接受 BJCA 组织的为期一周的岗前培训。

5.3.8 提供给员工的文档

为使得系统正常运行，必须提供给具有权限的相关人员各种文档，包括：

a) 加密机用户手册；
b) 机房设备管理办法；
c) 密码信封打印工具用户手册；
d) 数字证书运营规范；
e) 灾难备份和恢复方案；
f) 目录服务器安装配置手册。

5.4 审计日志程序

5.4.1 记录事件的类型

BJCA 记录与系统相关的事件，这些记录信息称为日志。对于这些日志，无论其载体是纸张还是电子文档的形式，必须包含事件发生的日期、事件的发生时间段、事件的内容和事件相关的实体等。

BJCA 还可能记录与系统不直接相关的事件，例如：物理通道参观记录、人事变动等。

5.4.2 处理或归档日志的周期

BJCA 每周对日志进行审查，并对审查日志的行为进行备案。

5.4.3 审计日志的保存期限

BJCA 在数据库保存审计日志至少两个月，离线保存至少为十年。

5.4.4 审计日志的保护

BJCA 执行严格的管理，确保只有 BJCA 授权的人员才能对审查日志进行相应操作。日志处于严格的保护状态，严禁在未授权的情况下被访问、阅读、修改和删除等操作，另外对日志要进行异地备份。审计日志的制作和访问进行岗位分离。

BJCA 将审计日志存储到磁带中，并存放到异地，实行安全保管。

5.4.5 审计日志备份程序

BJCA 保证所有的审查记录和审查总结都按照 BJCA 备份标准和程序进行备份。根据记录的性质和要求，分为实时、按天、按周、按月和按年等多种形式的备份，可采用在线和离线两种方式的备份工具。

审计文档由管理员每周进行一次归档。所有档案安全存放在文档库内。

5.4.6 审计日志收集系统

审计日志收集系统涉及：

- 证书管理系统；
- 证书签发系统；
- 证书目录系统；
- 远程通信系统；
- 证书受理系统；
- 访问控制系统；
- 网站、数据库安全管理系统；
- 其他需要审计的系统。

BJCA 使用审计工具满足对上述系统审计的各项要求。

5.4.7 对导致事件实体的通告

BJCA 发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，BJCA 保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

BJCA 有权决定是否对导致事件的实体进行通告。

5.4.8 脆弱性评估

BJCA 每年对系统进行脆弱性评估，以降低系统运行的风险。

5.5 记录归档

5.5.1 归档记录的类型

归档记录包括所有审计数据、证书申请信息、与证书申请相关的信息等。

5.5.2 归档记录的保存期限

所有归档记录的保存期一般规定为十年。

5.5.3 归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能查询。BJCA 保护相关的档案内容，免遭恶劣环境的威胁，如温度、湿度和强磁力等的破坏。

5.5.4 归档文件的备份程序

所有存档的文件和数据库除了保存在 BJCA 的存储库，还在异地保存其备份。存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。BJCA 在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

5.5.5 记录时间戳要求

所有记录都要在存档时加具体准确的时间标识以表明存档时间。系统产生的记录，用标准时间加盖时间戳。

5.5.6 获得和检验归档信息的程序

由两个人分别来保留归档数据的两个拷贝，并且为了确保档案信息的准确，需要对这两个拷贝进行比较。BJCA 每年会验证归档信息的完整性。

5.6 电子认证服务机构密钥更替

电子认证服务机构密钥更替指 BJCA 根证书到期和电子认证服务机构证书到期时，需要更换密钥而采取的措施。

a) BJCA 根密钥由加密机产生，有效期为 20 年，更替办法为：

使用旧的私钥对新的公钥及信息签名生成证书；

使用新的私钥对旧的公钥及信息签名生成证书；

使用新的私钥对新的公钥及信息签名生成证书。

通过以上 3 张证书达到密钥更换的目的，使新旧证书之间互相信任。

b) 电子认证服务机构证书到期之前，BJCA 将采取以下方式更替：

BJCA 将在证书到期前的 60 天内停止颁发新的证书；

旧的证书到期后，BJCA 将用新的密钥对签发证书。

密钥更替时直接把当前 CA 证书吊销，签发到 ARL 并发布，然后签发一个新的 CA 证书，通过证书库和 LDAP 方式下发给证书应用系统。

c) BJCA 将继续使用旧的根私有密钥签发的 CRL，直到旧的私钥签发的证书到期为止。

5.7 损害和灾难恢复

5.7.1 事故和损害处理程序

发生故障时，BJCA 将按照灾难恢复计划实施恢复。

5.7.2 计算资源、软件和/或数据被破坏

BJCA 遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，BJCA 将按照灾难恢复计划实施恢复。

5.7.3 实体私钥损害处理程序

当 BJCA 根证书被作废时，BJCA 通知订户。

当 BJCA 的私钥被攻破或需要作废时，BJCA 根据 BJCA 灾难恢复计划规定的灾难恢复步骤进行操作。

5.7.4 灾难后的业务连续性能力

针对证书系统的核心业务系统，证书签发系统和证书接口系统采用双机热备方式；对核心数据库，证书管理系统数据库采用磁盘阵列方式来确保证书系统的高可靠性和可用性。

发生自然或其它不可抗力性灾难后，BJCA 可采用远程热备站点对运营进行恢复。具体的安全措施按照 BJCA 灾难恢复计划实施。

5.8 电子认证服务机构或注册机构的终止

因各种情况，BJCA 需要终止运营时，将按照相关法律规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。

BJCA 在终止服务九十日前，就业务承接及其他有关事项通知有关各方，包括但不限于 BJCA 授权的发证机构和订户等。

在终止服务六十日前向信息产业部报告，按照相关法律规定的步骤进行操作。

BJCA 采用以下措施终止业务：

a) 起草 BJCA 终止业务声明；
b) 停止认证中心所有业务；
c) 处理加密密钥；
d) 处理和存档敏感文件；
e) 清除主机硬件；
f) 管理 BJCA 系统管理员和安全官员；
g) 通知与 BJCA 终止运营相关的实体。

根据 BJCA 与注册机构签订的运营协议终止注册机构的业务。

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

订户的签名密钥对由订户的密码设备（如智能 USB KEY 或智能 IC 卡）生成，加密密钥对由 KMC 生成。

6.1.2 私钥传送给订户

订户的签名密钥对由自己的密码设备生成并保管。

加密密钥对由 KMC 产生，通过安全通道传到订户手中的密码设备中。

6.1.3 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，经注册机构传递到 BJCA。

订户的加密证书公钥，由 KMC 通过安全通道传递到 CA 中心。

从 RA 到 CA 以及从 KMC 到 CA 的传递过程中，采用国家密码管理局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 BJCA 的网站(http://www.bjca.org.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

BJCA 用于加密和签名的非对称密钥对的模长是 1024 比特，对称密钥的长度是 128 比特。

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局许可的硬件产生。

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

BJCA 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

根 CA 系统的私钥的生成、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，只有其中三至五人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密码设备控制。

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。

KMC 严格保证用户密钥对的安全，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

订户的签名密钥 BJCA 和 KMC 都不备份。加密私钥由 KMC 备份，备份数据以密文形式存在。

6.2.5 私钥归档

订户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。

BJCA 提供过期的托管加密密钥的归档服务。

6.2.6 私钥导入或导出密码模块

使用 BJCA 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，需要三名管理员同时在场。

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，需要三名管理员同时在场。

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，需要三名管理员同时在场。

6.2.11 密码模块的评估

BJCA 使用成都卫士通的 SJY15-C 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 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 RSA 身份鉴别后协商得到；
e) 身份鉴别：采用用户 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为 16Mbps；
模长 1024 的数字签名速度 111 次/秒。

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 BJCA 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 KEY）出厂时设置了缺省的 PIN 值，证书制作时将此 PIN 值更改为密码信封中的密码，从而激活了证书存储介质的 PIN。

6.4.2 激活数据的保护

证书存储介质的 PIN 值用密码信封中的密码进行保护。

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

BJCA 证书系统已通过北京市《党政机关信息系统安全测评规范》等级三的测评。

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

BJCA 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。BJCA 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

BJCA 签发的证书符合 X.509 V3 格式。遵循 RFC3280 标准。

7.1.1 版本号

X.509 V3。

7.1.2 算法对象标识符

使用 SHA1WithRSAEncryption 算法
算法 OID 1.2.840.113549.1.1.5

7.1.3 名称形式

BJCA 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）中的内容分为 2 种：
  a) 证书主体或者证书主体所属单位具有明确的上一级单位，则应为其上一级单位的名称全称；
  b) 不存在 a）中所述的上一级单位，则应为证书主体或者证书主体所属单位的所在省、自治区、直辖市名称全称；
- OU（Organization Unit）应为证书主体或者证书主体所属单位的名称全称；
- CN（Common Name）中的内容分为 4 种：

a) 个人证书中应为证书主体的姓名；
b) 单位机构证书中应为证书主体单位的标准简称；
c) 服务器证书应为证书主体设备的域名或者 IP 地址或者设备编码；
d) 代码签名证书应为负责人的姓名，或者是所属单位的标准简称；

- Email 仅在邮件证书的 DN 中存在，应为证书主体的有效电子邮件地址。

7.1.4 证书扩展项

BJCA 证书扩展项除使用 IETF RFC 3280 中定义的证书扩展项，还支持私有扩展项。

BJCA 采用的 IETF RFC 3280 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
- 企业工商注册号 IC Registration Number
- 企业组织机构代码 Organization Code
- 企业税号 Taxation Number

7.2 证书吊销列表

BJCA 签发的证书吊销列表符合 X.509 V2 格式。遵循 RFC3280 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 BJCA 是否按照《电子认证业务规则》及其业务规范、管理制度和安全策略开展业务，发现存在的可能风险。审计分内部审计和外部审计。

内部审计是由 BJCA 自己组织内部人员进行的审计，审计的结果可供 BJCA 改进、完善业务，内部审计结果不需要公开。

外部审计由 BJCA 委托第三方审计机构来承担，审计的依据包括 BJCA 所有与业务有关的安全策略、《电子认证业务规则》、业务规范、管理制度，以及国家或行业的相关标准。

8.2 评估者的资质

内部审计人员的选择一般包括：

- BJCA 的安全负责人及安全管理人员；
- BJCA 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。

8.3 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：

- 人事审查；
- 物理环境建设及安全运营管理规范审查；
- 系统结构及其运行审查；
- 密钥管理审查；

- 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

对审计中发现的问题，BJCA 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。BJCA 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，BJCA 一般不公开评估结果。

对 BJCA 关联方，BJCA 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

9.1 费用

9.1.1 证书签发和更新费用

数字证书的收费标准按照国家和北京市物价主管部门批准的收费标准执行。根据证书实际应用的需要，BJCA 在不高于收费标准的前提下可以对证书价格进行适当调整。

9.1.2 证书查询费用

在证书有效期内，对该证书信息进行查询，BJCA 不收取查询费用。

9.1.3 证书吊销或状态信息的查询费用

查询证书是否吊销，BJCA 不收取信息访问费用。

对于在线证书状态查询(OCSP)，由 BJCA 与订制者在协议中约定。

9.1.4 其他服务的费用

CA 可根据请求者的要求，订制各类通知服务，具体服务费用，在与订制者签订的协议中约定。

9.1.5 退款策略

在实施证书操作和签发证书的过程中，BJCA 遵守并保持严格的操作程序和策略。一旦订户接受数字证书，BJCA 将不办理退证、退款手续。

如果订户在证书服务期内退出数字证书服务体系，BJCA 将不退还剩余时间的服务费用。

9.2 财务责任

BJCA 保证其具有维持其运作和履行其责任的财务能力。它应该有能力承担对订户、依赖方等造成的责任风险，并依据 CPS 规定，进行赔偿担保。

9.3 业务信息保密

9.3.1 保密信息范围

保密的业务信息包括但不限于以下方面：

a) 在双方披露时标明为保密(或有类似标记)的；
b) 在保密情况下由双方披露的或知悉的；
c) 双方根据合理的商业判断应理解为保密数据和信息的；
d) 以其他书面或有形形式确认为保密信息的；
e) 或从上述信息中衍生出的信息。

对于 BJCA 来说，保密信息包括但不限于以下方面：

a) 最终用户的私人签名密钥都是保密的；
b) 保存在审计记录中的信息；
c) 年度审计结果也同样视为保密；
d) 除非有法律要求，由 BJCA 掌握的，除作为证书、CRL、认证策略被清楚发布之外的个人和公司的信息需要保密。

BJCA 不保存任何证书应用系统的交易信息。

除非法律明文规定，BJCA 没有义务公布或透露订户数字证书以外的信息。

9.3.2 不属于保密的信息

与证书有关的申请流程、申请需要的手续、申请操作指南等信息是公开的。BJCA 在处理申请业务时可以利用这些信息，包括发布上述信息给第三方。

订户数字证书的相关信息可以通过 BJCA 目录服务等方式向外公布。

BJCA 在其目录服务器中公布证书的吊销信息，供网上查询。

9.3.3 保护保密信息的责任

a) 各方有保护自己和其他人员或单位的机密信息的并保证不泄露给第三方的责任。不将机密数据和信息(也不会促使或允许他人将机密数据和信息)用于协议项下活动目的之外的其他用途，包括但不限于将此保密信息的全部或部分进行仿造、反向工程、反汇编、逆向推导；在披露当时，如果已明确表示机密数据和信息不得复印、复制或储存于任何数据存储或检索系统，接受方不得复印、复制或储存机密数据和信息。
b) 当 BJCA 在任何法律、法规或规章的要求下，或在法院的要求下必须提

供本《电子认证业务规则》中具有保密性质的信息时，BJCA 应按照要求，向执法部门公布相关的保密信息，BJCA 无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

9.4 个人隐私保密

9.4.1 隐私保密方案

除非证书申请人主动提供，BJCA 保证不会截取任何证书申请人的资料。

BJCA 应保护证书申请人所提供的，证明其身份的资料。BJCA 应采取必要的安全措施防止证书申请人资料被遗失、盗用与篡改。

9.4.2 作为隐私处理的信息

证书申请人提供的不构成数字证书内容的资料被视为隐私信息。

9.4.3 不被视为隐私的信息

证书申请人提供的用来构成数字证书内容的资料不认为是隐私信息。

数字证书是公开的，通过 BJCA 目录服务等方式向外公布。

9.4.4 保护隐私的责任

接收到隐私信息的参与者有责任保护隐私信息不被泄漏、使用或发布给第三方。

9.4.5 使用隐私信息的告知或同意

使用隐私信息，须获得本人同意。

9.4.6 依法律或行政程序的信息披露

当 BJCA 在任何法律、法规或规章的要求下，或在法院的要求下必须提供证书申请人的特定资料或隐私信息时，BJCA 按照法律、法规或规章的要求或法院的要求，向执法部门公布相关信息，BJCA 无须承担任何责任。这种提供不能被视为违反了隐私保护的责任和义务。

9.4.7 其他信息披露情形

其他信息的披露遵循国家的相关规定处理。

9.5 知识产权

除非额外声明，BJCA 享有并保留对证书以及 BJCA 提供的全部软件的一切知识产权，包括所有权、名称权和利益分享权等。BJCA 有权决定关联机构采用的软件系统，选择采取的形式、方法、时间、过程和模型，以保证系统的兼容和互通。

按本《电子认证业务规则》的规定，所有由 BJCA 签发的证书和提供的软件中使用、体现和相关的一切版权、商标和其他知识产权均属于 BJCA 所有，这些知识产权包括所有相关的文件和使用手册。注册机构应征得 BJCA 的同意使用相关的文件和手册，并有责任和义务提出修改意见。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

BJCA 在提供电子认证服务活动过程中的承诺如下：

a) BJCA 遵守《中华人民共和国电子签名法》及相关法律的规定，接受信息产业部的领导，对签发的数字证书承担相应的法律责任。
b) BJCA 保证使用的系统及密码符合国家政策与标准，保证其 CA 本身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定。
c) 除非已通过 BJCA 证书库发出了 BJCA 的私钥被破坏或被盗的通知，BJCA 保证其私钥是安全的。
d) BJCA 签发给订户的证书符合 BJCA 的 CPS 的所有实质性要求。
e) BJCA 将向证书订户通报任何已知的、将在本质上影响订户的证书的有效性和可靠性事件。
f) BJCA 将及时吊销证书。
g) BJCA 拒绝签发证书后，将立即向证书申请人归还所付的全部费用。
h) 证书公开发布后，BJCA 向证书依赖方证明，除未经验证的订户信息外，证书中的其他订户信息都是准确的。

9.6.2 注册机构的陈述与担保

BJCA 的注册机构在参与电子认证服务过程中的承诺如下：

a) 提供给证书订户的注册过程完全符合 BJCA 的 CPS 的所有实质性要求。
b) 在 BJCA 生成证书时，不会因为注册机构的失误而导致证书中的信息与证书申请人的信息不一致。
c) 注册机构将按 CPS 的规定，及时向 BJCA 提交证书申请、吊销、更新等服务请求。

9.6.3 订户的陈述与担保

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

a) 订户需熟悉本《电子认证业务规则》的条款和与其证书相关的证书政策，还需遵守证书持有人证书使用方面的有关限制。
b) 订户在证书申请表上填列的所有声明和信息必须是完整、真实和正确的，可供 BJCA 或注册机构检查和核实。
c) 订户应当妥善保管私钥，采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件的发生。
d) 私钥为订户本身访问和使用，订户对使用私钥的行为负责。
e) 一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘、泄密以及其他情况，订户应立刻通知 BJCA 和注册机构，申请采取吊销等处理措施。
f) 订户已知其证书被冒用、破解或被他人非法使用时，应及时通知 BJCA 吊销其证书。

9.6.4 依赖方的陈述与担保

依赖方必须熟悉本《电子认证业务规则》的条款以及和订户数字证书相关的证书政策，并确保本身的证书用于申请时预定的目的。

依赖方在信赖订户的数字证书前，必须采取合理步骤，查证订户数字证书及数字签名的有效性。

所有依赖方必须承认，他们对证书的信赖行为就表明他们承认了解本《电子认证业务规则》的有关条款。

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 9.6.4。

9.7 赔偿责任限制

9.7.1 赔偿责任范围

BJCA 的赔偿责任范围：

a) 证书信息与订户提交的信息资料不一致，导致订户损失。
b) 因 BJCA 原因，致使订户无法正常验证证书状态，导致订户利益受损。
c) BJCA 在证书有效期限内承担损失或损害赔偿。

9.7.2 对最终实体的赔偿担保

BJCA 对所有当事实体（包括但不限于订户、申请人或信赖方）的合计责任不超过证书的适用的责任封顶。对于一份证书产生的所有数字签名和交易处理，BJCA 对于任何人有关该特定证书的合计责任应该限制在一个不超出赔偿责任上限的范围内，这种赔偿上限可以由 BJCA 根据情况重新制定，BJCA 会将重新制定后的情况立刻通知相关当事人。

BJCA 所颁发数字证书的赔偿责任上限如下。

个人证书：800 元人民币。

机构证书：4000 元人民币。

服务器证书：12000 元人民币。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任。每份证书的责任均有封顶而不考虑数字签名和交易处理等有关的其他索赔的数量。当超过责任封顶时，可用的责任封顶将首先分配给最早得到索赔解决的一方。BJCA 没有责任为每个证书支付高出责任封顶的赔偿，而不管责任封顶的总量在索赔提出者之间如何分配的。

9.7.3 责任免除

有下列情况之一的，应当免除 BJCA 之责任。

a) 如果证书申请人故意或无意地提供了不完整、不可靠或已过期的信息，又根据正常的流程提供了必须的审核文件，得到了 BJCA 签发的数字证书，由此引起的经济纠纷应由证书申请人全部承担，BJCA 不承担与证

书内容相关的法律和经济责任，但可以根据受害者的请求提供协查帮助。

b) BJCA 不承担任何其他未经授权的人或组织以 BJCA 名义编撰、发表或散布的不可信赖的信息所引起的法律责任。
c) BJCA 不承担在法律许可的范围内，根据受害者或法律的要求如实提供网上业务中“不可抵赖”的数字签名依据所引起的法律责任。
d) BJCA 不对任何一方在信赖证书或使用证书过程中引起的直接或间接的损失承担责任。
e) BJCA 和注册机构不是证书持有人或依赖方的代理人、受托人、管理人或其他代表。BJCA 和证书持有人间的关系以及 BJCA 和依赖方间的关系并不是代理人和委托者的关系。证书持有人和依赖方都没有权利以合同形式或其他方法让 BJCA 承担信托责任。
f) 由于客观意外或其他不可抗力事件原因而导致数字证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的。关于不可抗力的描述参见§9.16.4。
g) 因 BJCA 的设备或网络故障等技术故障而导致数字证书签发延迟、中断、无法签发，或暂停、终止全部或部分证书服务的；本项所规定之“技术故障”引起原因包括但不限于：（1）不可抗力；（2）关联单位如电力、电信、通讯部门而致；（3）黑客攻击；（4）设备或网络故障。
h) BJCA 已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的。

9.8 有限责任

BJCA 根据与订户的合同承担相应的有限责任。

BJCA 在与订户和依赖方签定的协议中，对于因订户或依赖方的原因造成的损害不具有赔偿义务。

9.9 赔偿

BJCA 按照本《电子认证业务规则》§9.7 条款承担赔偿责任。

证书订户和依赖方在使用或信赖证书时，若有任何行为或疏漏而导致 BJCA 和注册机构产生损失，订户和依赖方应承担赔偿责任。

订户接受证书就表示同意在以下情况下承担赔偿责任。

a) 未向 BJCA 提供真实、完整和准确的信息，而导致 BJCA 或有关各方损失。

b) 未能保护订户的私钥，或者没有使用必要的防护措施来防止订户的私钥遗失、泄密、被修改或被未经授权的人使用时。
c) 在知悉证书密钥已经失密或者可能失密时，未及时告知 BJCA，并终止使用该证书，而导致 BJCA 或有关各方损失。
d) 订户如果向依赖方传递信息时表述有误，而依赖方用证书验证了一个或多个数字签名后理所当然地相信这些表述，订户必须对这种行为的后果负责。
e) 证书的非法使用，即违反 BJCA 对证书使用的规定，造成了 BJCA 或有关各方的利益受到损失。

9.10 有效期限与终止

9.10.1 有效期限

本《电子认证业务规则》自发布之日起正式生效。
本《电子认证业务规则》中将详细注明版本号及发布日期。

9.10.2 终止

当新版本的《电子认证业务规则》正式发布生效时，旧版本的《电子认证业务规则》自动终止。

9.10.3 效力的终止与保留

《电子认证业务规则》的某些条款在终止后继续有效，如知识产权承认和保密条款。另外，各参与方应返还保密信息到其拥有者。

9.11 对参与者的个别通告与沟通

认证活动的某一参与方与另一参与方进行通信时必须使用安全通道，以使其通信过程在法律上有效。

9.12 修订

9.12.1 修订程序

当本《电子认证业务规则》不适用时，由 BJCA CPS 策略委员会组织 CPS

编写小组进行修订。

修订完成后，BJCA CPS 策略委员会进行审批，审批通过后将在 BJCA 的网站(http://www.bjca.org.cn)上发布新的《电子认证业务规则》。

《电子认证业务规则》将进行严格的版本控制。

9.12.2 通告机制和期限

本《电子认证业务规则》在 BJCA 的网站(http://www.bjca.org.cn)上发布。

版本更新时，最新版本的《电子认证业务规则》在 BJCA 的网站发布，对具体个人不做另行通知。

9.12.3 必须修改业务规则的情形

当管辖法律、适用标准及操作规范等有重大改变时，必须修改《电子认证业务规则》。

9.13 争议处理

BJCA、证书订户、依赖方等实体在电子认证活动中产生争端可按照以下步骤解决：

a) 当事人首先通知 BJCA，根据本《电子认证业务规则》中的规定，明确责任方；
b) 由 BJCA 相关部门负责与当事人协调；
c) 若协调失败，可以通过仲裁或司法途径解决；
d) 任何因与 BJCA 或授权机构就本《电子认证业务规则》所产生的任何争议而提起诉讼的，受 BJCA 工商注册所在地的人民法院管辖。

9.14 管辖法律

本《电子认证业务规则》在各方面服从中国法律和法规的管制和解释，包括但不限于《中华人民共和国电子签名法》及《电子认证服务管理办法》等。

9.15 与适用法律的符合性

无论在任何情况下，本《电子认证业务规则》的执行、解释、翻译和有效性均适用中华人民共和国的法律。

9.16 一般条款

9.16.1 完整协议

本《电子认证业务规则》将替代先前的、与主题相关的书面或口头解释。

9.16.2 分割性

当法庭或其他仲裁机构判定协议中的某一条款由于某种原因无效或不具执行力时，不会出现因为某一条款的无效导致整个协议无效。

9.16.3 强制执行

免除一方对合同某一项的违反应该承担的责任，不意味着继续免除或未来免除这一方对合同其他项的违反应该承担的责任。

9.16.4 不可抗力

不可抗力是指不能预见、不能避免并不能克服的客观情况。不可抗力既可以是自然现象或者自然灾害，如地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；也可以是社会现象、社会异常事件或者政府行为，如合同订立后政府颁发新的政策、法律和行政法规，致使合同无法履行，再如战争、罢工、骚乱等社会异常事件。

在数字证书认证活动中，BJCA 由于不可抗力因素而暂停或终止全部或部分证书服务的，可根据不可抗力的影响而部分或者全部免除违约责任。其他认证各方（如订户）不得提出异议或者申请任何补偿。

9.17 其他条款

BJCA 对本《电子认证业务规则》拥有最终解释权。