北京数字认证股份有限公司
云端协同移动证书策略
（CP3）

1.0.1 版

发布日期：2017 年 11 月 9 日

生效日期：2017 年 11 月 9 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 CPS 策略管理委员会	2017 年 11 月 9 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

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。

云端协同移动证书是面向移动互联网和云服务等新技术领域，数字认证公司创新出一类特定的云端协同证书，专门提供云认证和云签名等服务。通过云端协同移动证书与服务，在移动互联网、云服务和传统业务等领域实现各参与主体身份的真实性、信息的完整性以及签名行为的不可抵赖性。

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云端协同移动证书策略》（以下简称《云端协同证书策略》）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《云端协同证书策略》适用范围为数字认证公司发放的云端协同移动证书。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云端协同移动证书策略（CP3）》，简称《云端协同证书策略》，本证书策略 CP 的对象标识符为：1.2.156.112562.2.2.3。

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

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

1.3.3. 签名服务云端

签名服务云端是基于云的电子签名服务的最主要部分，以云服务的方式为订户和依赖方提供数字证书和电子签名服务。

1.3.4. 订户

订户是从 CA 机构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。

1.3.5. 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 CA 证书服务体系中，是信任 CA 机构证书，可以对使用 CA 机构证书机制进行的数字签名进行验证，使用 CA 机构证书的公钥的实体。

1.3.6. 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 机构签发的云端协同移动证书适合应用在移动互联网、云服务和传统业务等各领域，用于证明订户在移动化和云服务环境中所进行的身份认证与电子签名。

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《云端协同证书策略》的管理机构是数字认证公司 CPS 策略管理委员会。由数字认证公司 CPS 策略管理委员会负责本《云端协同证书策略》的制订、发布、更新等事宜。

1.5.2. 联系人

本《云端协同证书策略》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《云端协同证书策略》由数字认证公司 CPS 策略管理委员会组织制定，报数字认证公司 CPS 策略管理委员会批准实行。

1.5.4. CP 批准程序

本《云端协同证书策略》由数字认证公司 CPS 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《云端协同证书策略》经数字认证公司 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工业和信息化部备案。

1.6. 定义和缩写

下列定义适用于本《云端协同证书策略》：

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 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）。

f) 云端协同移动证书：MSSP Certificate

面向移动互联网和云服务等新技术领域，数字认证公司创新出一类特定的云端协同证书。适用于证明订户在移动化和云服务环境中所进行的身份认证与电子签名，协同数字证书必须由订户移动终端和签名服务云端协同配合才能完成可靠数字签名。

在本 CP 中，如无特殊定义，所述的数字证书，均指云端协同移动证书。

g) 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。

h) 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. 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《云端协同证书策略》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《云端协同证书策略》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。对具体个人不另行通知。

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

订户的甄别名(DN)必须具有一定的代表意义，可为个人订户的身份证号码、机构订户的机构代码等。证书申请者应确保不会提交任何侵犯知识产权的名称。

3.1.3. 订户的匿名或伪名

在 CA 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

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 服务体系中，证书申请中存在不同订户存在相同名称时，遵循先申请者优先使用，后申请者增加附加识别信息予以区别的原则。

CA 确保同样主体名称的证书是颁发给同一个用户的。

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

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。

在云端协同移动证书服务体系中，私钥在订户移动终端和签名服务云端共同计算生成，证书请求信息中包含用私钥进行的数字签名，CA 用订户移动终端和签名服务云端共同计算生成的公钥来验证这个签名，视作申请人为其私钥的拥有者。

3.2.2. 个人身份的鉴别

个人订户在申领证书前应持个人有效身份证件，包括：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。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。CA 机构或授权的注册机构将复核并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。

云端协同移动证书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。订户可通过手机拍照、证件照上传等方式来提交材料。CA 机构或授权的注册机构可通过公安部身份核实接口或银行用户查询系统来进行身份鉴别审核。

CA 机构或授权的注册机构依法采集并妥善保存订户身份信息，包括订户的电子影像数据或证明订户有效身份的其他电子数据等。

3.2.3. 组织身份的鉴别

对于组织身份的鉴别，CA 机构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。CA 机构或授权的注册机构按照 CA 审核流程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。

云端协同移动证书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。订户可通过手机拍照、证件照上传等方式来提交材料。CA 机构或授权的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。

CA 机构或授权的注册机构依法采集并妥善保存订户身份信息，包括订户的电子影像数据或证明订户有效身份的其他电子数据等。

3.2.4. 没有验证的订户信息

订户提交鉴证文件以外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。CA 机构或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。

3.2.6. 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《云端协同证书策略》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

云端协同移动证书常规密钥更新中，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。

此过程订户可以通过移动终端 APP 自助完成。

3.3.2. 吊销后密钥更新的标识与鉴别

云端协同移动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

3.2 相同。

3.3.3. 证书变更的标识与鉴别

云端协同移动证书的证书变更是指订户的证书信息发生变更，申请重新签发一张证书，对原证书进行吊销处理。

证书变更的标示与鉴别使用原始身份验证相同的流程，其要求与 3.2 相同。

3.4. 吊销请求的标识与鉴别

云端协同移动证书吊销请求的标示与鉴别使用原始身份验证相同的流程，其要求与 3.2 相同。

如果是因为订户没有履行本《云端协同证书策略》和《数字认证公司电子认证业务规则》所规定的义务，由 CA 机构或授权的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《云端协同移动证书策略》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。

根据《中华人民共和国电子签名法》的规定，证书申请者未向 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，应承担相应的法律责任和经济赔偿。

4.2. 证书申请处理

4.2.1. 执行识别与鉴别功能

证书申请者向 CA 机构或授权的注册机构提交初始的证书申请请求，CA 机构或授权的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 3.2.2 节的规定。

机构订户：参照 3.2.3 节的规定。

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《云端协同证书策略》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

CA 机构或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。

CA 机构或授权的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 CA 机构的管理要求。

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

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 机构签发云端协同移动证书，订户所使用移动终端设备或 APP 应用程序会有数字证书已签发或下载成功的展示，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

CA 机构为订户签发云端协同移动证书，订户所使用移动终端设备或 APP 应用程序接收到数字证书起，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

CA 机构在签发云端协同移动证书，会将该证书信息记录在指定的数据库中，订户移动终端会对证书状态实时检测。

根据依赖方约定，可向依赖方提供状态查询服务。

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。

云端协同移动证书必须由订户和签名服务云端协同配合才能完成一次数字签名。订户只能在指定的应用范围内使用私钥和证书，订户只有在接受了相关证书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。

对于云端协同移动证书，依赖方不需要查询证书状态，云端协同移动证书被注销后，用户即无法使用客户端的密钥进行数字签名。

4.6. 证书更新

4.6.1. 证书更新的情形

证书更新指在不改变证书中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。

云端协同移动证书的证书更新，必须同时进行密钥更新。

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。

在云端协同移动证书到期之前，订户可通过移动终端 APP 自助完成证书密钥更新。CA 会按照之前注册的用户身份签发新的证书，同时必须产生新的密钥。证书到期后更新按照证书新办流程处理。

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 机构签发的云端协同移动证书的证书持有人。

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

4.8.1. 证书变更的情形

证书变更是指订户的证书信息发生变更，申请重新签发一张证书，对原证书进行吊销处理。

云端协同移动证书的证书变更，按照证书新办流程处理。

4.8.2. 请求证书变更的实体

订户可以请求证书变更。订户包括持有 CA 机构签发的云端协同移动证书的证书持有人。

4.8.3. 证书变更请求的处理

同 3.3.3。

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数字证书认证业务规则。
b) 发生下列情形之一的，CA 机构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。

4.9.2. 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原始证书签发相同的过程。

a)证书吊销的申请人提交证书吊销到注册系统，并注明吊销原因；

b) CA 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) CA 吊销订户证书后，订户证书应无法进行任何数字签名；

d) 强制吊销是指当 CA 机构或 CA 机构或授权的注册机构确认用户违反本《云端协同移动证书策略》和《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，吊销后订户应无法进行任何数字签名。

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

云端协同移动证书吊销请求被接收，签名服务云端应销毁其服务端协同密钥，密钥销毁后，用户即无法使用客户端的密钥进行数字签名。

4.9.6. 依赖方检查证书吊销的要求

云端协同移动证书吊销请求被处理之后，证书即无法进行任何数字签名操作。因此，依赖方不需要额外检查该证书的吊销状态。

4.10. 证书状态服务

4.10.1. 操作特点

CA 机构在签发云端协同移动证书，会将该证书信息记录在指定的数据库中，订户移动终端会对证书状态实时检测。

4.10.2. 服务可用性

根据依赖方约定，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

云端协同移动证书的密钥对，由订户移动终端和签名服务云端协同计算产生。由订户移动终端和签名服务云端分别各自进行密钥备份与恢复。

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

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

云端协同移动证书签名密钥对，由订户移动终端和签名服务云端共同计算协同产生。服务端密钥因子应在国家密码主管部门许可的服务器密码机中产生，客户端密钥因子应包含移动终端设备信息、用户知晓的（例如用户设置的 PIN）、随机数等部分计算得到。

6.1.2. 私钥传送给订户

云端协同移动证书的签名密钥对，由订户移动终端和签名服务云端共同计算协同产生，通过安全通道协商传输。

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 CA 机构。

从 RA 到 CA 以及从密钥管理中心到 CA 的传递过程中，采用国家密码主管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主管部门的规定。

6.1.6. 公钥参数的生成和质量检查

公钥参数由国家密码主管部门许可的加密设备生成。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主管部门要求。

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，即采取三选二方式，将私钥的管理权限分散到 3 张管理员卡中，只有其中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

云端协同移动证书的密钥对，由订户移动终端和签名服务云端协同计算产生并分别保管。

6.2.4. 私钥备份

订户移动终端和签名服务云端各自备份各自的私钥因子。

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，签名服务云端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

签名服务云端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 机构使用具有国家密码主管部门颁发商用密码型号证书的服务器密码机，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，由签名服务云端归档。

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，云端协同移动证书使用移动终端设置 PIN 码，输入正确 PIN 码可启动云端协同移动证书 APP。

6.4.2. 激活数据的保护

云端协同移动证书通过使用移动终端的 PIN 码进行保护。

6.4.3. 激活数据的其他方面

只有在拥有移动终端设备并知道 PIN 值时才能激活云端协同移动证书 APP，进而调用订户移动终端和签名服务云端的私钥。

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。

6.5.2. 计算机安全要求

CA 系统建设符合《GB22239-2008 信息系统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 RFC3280 标准。

7.1.1. 版本号

X.509 V3。

7.1.2. 算法对象标识符

符合国家密码主管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；

- 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

CA 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。

CA 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
- 营业执照（统一社会信用代码）IC Registration Number
- 企业组织机构代码 Organization Code
- 企业税号 Taxation Number

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《云端协同证书策略》和《电子认证业务规则》及其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。