电子认证业务规则
（CPS）

起草部门：技术支撑部

起草人：史炳荣、孙森田等

批准人：安全管理委员会

版本号：Version 2.3

编制日期：2018 年 2 月

中网威信电子安全服务有限公司

China SecTrust Corporation Limited.

版本控制表

版本	修改状态	修改说明	修改人	审核人/批准人	生效日期
Version 1.0	形成版本并审核通过			安全管理委员会	2007.01
Version 2.1		1、 更改了备份中心地址。 2、 修改了联系人信息。 3、 修订了部分错误。	孙森田	安全管理委员会	2017.11
Version 2.2		1、 更改了门禁系统的描述。 2、 修订了部分错误。	孙森田	安全管理委员会	2017.12
Version 2.3		1、 补充在线业务订户身份审核方式的说明（见 3.2.2,3.2.3）。 2、 补充在线业务申请材料及订户身份证明材料包保存备份方式的说明。 3、 修订了部分错误。	迟百顺	安全管理委员会	2018.02

版权声明

公司名称：中网威信电子安全服务有限公司综合管理部

法定地址：北京市西城区西单北大街甲 133 号中国联通 12 层。

联系人：迟百顺

邮编：100032

电　话：010-66504510

传　真：010-66505289

E-Mail：chibs@chinaunicom.cn

特别注意：

中网威信电子安全服务有限公司拥有对本文件的最终解释权。

中网威信电子认证服务遵从中华人民共和国的法律。对于任何因违反法律行为而影响中网威信电子认证服务的个人、机构或者其他组织，中网威信电子安全服务有限公司将保留所有的法律权利，以维护本单位的利益。

关于中网威信 CA 的 CPS 中主要权利及义务的概述

此概述仅就本 CPS 重要部分进行简单描述，有关条款的完整论述以及其他重要条款和细节请阅读 CPS 全文。

1、本 CPS 文件规定了中网威信 CA 电子认证服务的实施及使用，本文件所指的电子认证包括证书发放、证书验证、证书管理等方面，从功能上讲包括证书申请程序、证书申请的物理身份的验证、证书的签发、证书私钥的保护、证书的吊销和发布、证书的更新、证书状态的在线查询、证书的目录服务等。

2、证书申请者须知

(1) 申请者在证书申请前建议接受适当的数字认证相关方面的培训。

(2) 从中网威信 CA 网站及其他渠道可以得到有关数字签名、证书及 CPS 文件，证书申请者可以参加相关的培训和学习。

3、中网威信 CA 提供不同类型的证书，申请者应自行或向中网威信 CA 咨询决定何种证书适合自己的需求。

4、证书申请者在接受证书后方可使用证书。申请者在接受证书的同时就已经表明其接受了本 CPS 规定的权利和义务，并承担相应的责任。

5、证书依赖方必须自己决定是否信赖由中网威信 CA 签发的证书。在此之前，中网威信 CA 建议应检查中网 CA 的证书目录服务以确保证书是正确和即时有效的，签名是在证书有效期内使用创建的，而且有关信息并未改动。

6、证书持有人同意，如果发生危及私钥安全的状况时，及时通知中网威信 CA 及其授权的证书服务机构。

7、意见与建议

任何人或实体如果对以后 CPS 版本的编辑工作有任何意见与建议请

Email 至： chibs@chinaunicom.cn

或邮寄至：北京市西城区西单北大街 133 号联通大楼 12 层

目 录

1. 概括性描述

1.1 概述

中网威信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》）由中网威信电子安全服务有限公司按照工业和信息化部《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，并报工业和信息化部备案。

中网威信电子安全服务有限公司 CA 中心（简称中网威信 CA）是由中国联通集团于 2005 年提出、设计、建设并交由中网威信公司运营的权威、公正的电子认证服务机构。中网威信 CA 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，为电子商务、电子政务、企业信息化构建安全、可靠的信任环境。中网威信 CA 是经国家工业和信息化部、国家密码管理局批准成立的，全国性、公正可信的第三方认证机构。

本《电子认证业务规则》详细阐述了中网威信 CA 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》适用于中网威信 CA 及其员工、注册机构、中网威信 CA 授权或协议单位、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义务。

1.2 文档名称与标识

本文档名称是《中网威信数字证书认证中心电子认证业务规则》。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

中网威信 CA 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，负责创建和分发公钥数字证书的权威机构，是颁发证书的实体。

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，是为最终证书申请者建立注册过程的实体，包括注册系统（RA 系统）和各地证书业务受理点，负责受理证书的申请、对证书申请者进行身份鉴别，发起或传递证书吊销请求等职能。

1.3.3 订户

订户是从中网威信 CA 接收证书的实体。在电子签名应用中，订户即为电子签名人。

订户包括个人、企业、服务器、网站等提供网上服务和享受网上服务的各种实体，以及其他持有中网 CA 各类证书的人、物或单位组织。

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。在中网威信 CA 证书服务体系中，依赖方是指信任中网威信 CA 证书，使用中网威信 CA 颁发证书，利用中网威信 CA 证书机制进行电子签名验证的公钥实体。

1.3.5 其他参与者

其他参与者指以上未提及的为中网威信 CA 证书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

中网威信 CA 数字证书能够在电子政务公共服务、电子交易、电子办公、电子公证、公共服务等领域应用，为建设互联网络的信任环境开展基础性的安全服务。

证书类型及用途参见中网威信 CA 网站（http://www.uni-ca.com.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

中网威信 CA 颁发的数字证书禁止在任何违反国家法律、法规或破环国家安全的情形下使用，否则由此造成的任何后果由订户负责。

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》的管理机构是中网威信电子安全服务有限公司安全管理委员会。由中网威信公司安全管理委员会负责本《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》在中网威信 CA 网站发布，并由中网威信公司进行严格的版本控制，对具体个人不另行通知。

网站地址： http://www.uni-ca.com.cn;

电子邮箱地址：chibs@chinaunicom.cn

电话：010-66504510

联系地址：北京市西城区西单北大街甲 133 号中国联通 12 层

1.5.3 决定 CPS 符合策略的机构

中网威信公司对本 CPS 文件具有决定权和最终解释权。

1.5.4 CPS 批准程序

本《电子认证业务规则》由中网威信公司安全管理委员会组织编写小组起草，编写小组完成 CPS 草案后，由安全管理委员会组织专家组对 CPS 草案进行初步评审。初步评审并完成修改后，组织第二轮专家评审，再次完成修改后，由安全管理委员会将 CPS 评审稿提交中网威信公司领导组审批。审批通过后，在中网威信 CA 网站上对外公布。

本《电子认证业务规则》自对外公布之日起三十日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《电子认证业务规则》：

1. 公开密钥基础设施（PKI）Public Key Infrastruture

指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。

2. 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、更新证书或更新密钥过程中所采纳的业务实践的声明。

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

又称为认证中心或CA，它是被用户所信任的签发公钥证书及证书注销列表的管理机构。

4. 注册机构（RA）Registration Authority

证书认证体系中的一个组成部分，它是接收用户证书及证书注销列表申请信息、审核用户真实身份、为用户颁发证书的管理机构。

5. 电子签名认证证书(证书)Digital Certificate

指电子认证服务机构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。证书中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。

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

标记一系列不再被证书发布者所信任的证书的签名列表

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

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。

8. 数字签名：Digital Signature

由证书认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

9. 私钥(电子签名制作数据)： Private Key

在公钥密码系统中，用户的密钥对中只有用户本身才能持有的密钥。

10. 公钥(电子签名验证数据)： Public Key

在公钥密码系统中，用户的密钥对中可以被其它用户所持有的密钥。

11. 在线证书状态查询协议（OCSP）：Online Certificate Status Protocol

指在线查询数字证书状态协议，用于支持实时查询数字证书状态。

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

该协议用于查询、下载数字证书以及数字证书废止列表（CRL）。

2. 信息发布与信息管理

2.1 认证信息的发布

中网威信 CA 通过网站公布以下信息：《电子认证业务规则》修订以及其他由中网威信 CA 不定时发出的信息。CA 中心网址：http://www.uni-ca.com.cn。

本《电子认证业务规则》发布在中网威信 CA 中心的网站上，供相关方下载、查阅。

中网威信 CA 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中网威信 CA 的目录服务器获取证书的信息和吊销证书列表。同时，中网威信 CA 还提供在线证书状态查询（OCSP）服务。

2.2 发布的时间或频率

1. 本《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。
2. 证书的发布：在证书签发时，中网威信 CA 将自动将该证书公布。
3. 中网威信 CA 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，中网威信 CA 允许公众自行通过网站或目录服务器进行查询和访问。

中网威信 CA 设置了信息访问控制和安全审计措施，只有经授权的 RA/CA 管理人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

中网威信 CA 不推荐订户(证书申请人)使用匿名或伪名。

3.1.4 理解不同名称形式的规则

依 X.500 甄别名命名规则解释。

3.1.5 名称的唯一性

中网威信 CA 签发给某个实体的证书，其主题甄别名，在 CA 信任域内是唯一的，其中的例外是签发双证书时（一个签名证书、一个加密证书），属于同一实体的两个证书具有同样的主题甄别名，但证书的密钥用法扩展项不同。

3.1.6 商标的承认、鉴别和角色

中网威信 CA 签发的证书的主题甄别名中将不包含商标名。

本文件中涉及的“中网威信 CA”及其图标等是由中网威信电子安全服务有限公司独立持有的专有商标。其他参与者的商标为其拥有方所有。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

中网威信 CA 使用经数字签名的 PKCS#10 格式的证书请求，或其它相当的密码格式，或其它中网威信批准的方法，验证证书申请者拥有私钥。如果中网威信 CA 代表订户产生一个密钥对（如签发加密证书），则这个要求不适用。

中网威信 CA 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 组织机构身份的鉴别

对于组织机构身份的鉴别，中网威信 CA 需要验证提出证书申请的组织机构的合法证件。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书和经办人身份证件，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。

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

1. 组织机构代码证的副本及复印件；
2. 企业法人营业执照副本及复印件。
3. 如果组织机构没有营业执照，则书面申请表上应选其他有效证件，提供以下证件副本及复印件：
   1) 事业单位法人登记证
   2) 事业单位登记证
   3) 社会团体登记证
   4) 地税税务登记证
   5) 政府批文
   6) 其它有效证件
4. 经办人有效身份证件的原件和复印件；
5. 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 1、2、4证明文件的复印件需加盖申请单位公章）。

对于不能安排经办人到中网威信CA 授权的注册机构提交申请材料的机构，可以通过网络在线方式提交数字证书申请和有效身份证件的复印件。中网威信CA注册机构将对其提交申请资料真实性进行审核，必要时可以通过电话、手机短信或查询第三方权威数据库等可靠方式进一步验证机构及代理人身份的真实性。中网威信CA通过技术手段保证用户提交的申请材料在网络传输过程、存储及备份的安全。

中网威信 CA 授权的注册机构对申请资料的原件和复印件进行审核，并进行批准申请或拒绝申请的操作。

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。

个人需持上述个人有效身份证件，到中网威信 CA 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。

对于不能到中网威信 CA 授权的注册机构提交申请材料的个人，可以通过在线方式提交数字证书申请和有效身份证件的复印件。中网威信 CA 注册机构将对其提交申请资料真实性进行审核，必要时可以通过电话、手机短信或查询第三方权威数据库等可靠方式进一步验证申请者身份的真实性。中网威信 CA 通过技术手段保证用户提交的申请材料在网络传输过程、存储及备份的安全。

中网威信 CA 授权的注册机构对申请资料的原件和复印件进行审核，并进行批准申请或拒绝申请的操作。

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，代表组织机构获取数字证书，需要出具组织机构为其办理该组织中网威信 CA 数字证书事宜的授权文件。

组织机构在中网威信 CA 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。

中网威信 CA 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，与中网威信 CA 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中网威信 CA 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，中网威信 CA 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

中网威信 CA 对吊销后的证书不进行密钥更新。要获得证书，必须重新进行初始身份确认过程。

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初始身份确认相同的流程，参见第 3.2 节。

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 注册过程与责任

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。中网威信 CA 注册机构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申请材料，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

中网威信 CA 授权的注册机构（具体执行操作的业务受理点）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。具体的鉴别流程参见第 3.2.节初始身份确认。

4.2.2 证书申请批准和拒绝

中网威信 CA 授权的注册机构（具体执行操作的业务受理点）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，中网威信 CA 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，中网威信 CA 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，告知失败原因(法律禁止的除外)。

被拒绝的证书申请人可以在重新准备材料后，再次提出申请。

4.2.3 处理证书申请的时间

中网威信 CA 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中网威信 CA 的管理要求。

4.3 证书签发

4.3.1 证书签发中注册机构和电子认证服务机构的行为

中网威信 CA 作为电子认证服务提供方，建设了注册机构受理用户证书申请。在证书签发前，注册机构的业务受理点审核员负责对证书申请人进行身份鉴证，鉴证通过后，审核员使用证书登录到 RA 系统，查询系统记录的对应请求并批准请求。被批准的证书申请信息将会发送到中网威信 CA 系统，由 CA 系统签发证书并返回给 RA 系统供证书申请者下载。

4.3.2 电子认证服务机构和注册机构对订户的通告

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：

1. 通过面对面的方式，通知订户到注册机构领取数字证书；注册机构把证书等直接提交给订户，通知订户证书信息已经正确生成；
2. 邮政信函通知订户；
3. 其它中网威信 CA 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

证书申请者从获得证书起就被视为已同意接受证书。证书申请者接受数字证书后，应妥善保存其证书对应的私钥。

4.4.2 电子认证服务机构对证书的发布

中网威信 CA 在签发完证书后，就将证书发布到数据库和目录服务器中。中网威信 CA 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 电子认证服务机构对其他实体的通告

电子认证服务机构在颁发完证书后，不对其他实体发出通告，其他实体可以通过从目录服务器中查询到中网威信 CA 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中网威信 CA 所签发的证书后，均视为已经同意遵守与 中网威信 CA、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。

对于签名证书，其私钥可用于对信息的签名。在可能的情况下，签名证书及信任链上的证书（根证书除外）应同被签名信息一起提交给依赖方。证书持有人使用私钥对信息签名时，应该知晓并确认签名的内容。对于具有身份鉴别用途的证书，其私钥可用于对鉴别方提交的挑战信息签名；在可能的情况下，具有身份鉴别用途的证书及信任链上的证书（根证书除外）应提交给验证方。对于加密证书，其私钥可用于对采用对应公钥加密的信息解密。

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 依赖方公钥和证书的使用

获得对方的证书和公钥后，可以通过查看证书以了解对方的身份，通过公钥验证对方电子签名的真实性，实现通信的不可抵赖性，并实现通信双方数据传输的保密性和完整性。

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订户任何信息的情况下，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，到中网威信 授权的注册机构申请更新证书。

证书更新的具体情形如下：

1. 证书的有效期将要到期；
2. 密钥对的使用期将要到期；
3. 因私钥泄漏而吊销证书后，需要进行证书更新；
4. 其它需要更新证书的原因。

4.6.2 请求证书更新的实体

订户可以请求证书更新。订户包括持有中网威信 CA 签发的个人、组织及设备服务器等各类证书的证书持有人。

4.6.3 证书更新请求的处理

处理证书更新请求采用人工方式更新。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。注册机构要求对申请证书更新订户进行查验与鉴别，鉴别要求同本规则第 3.2 节。

4.6.4 颁发新证书时对订户的通告

对订户的通告有以下几种方式：

1. 通过面对面的方式，通知证书更新已完成，新证书已颁发；
2. 邮政信函通知订户；
3. 其他中网威信 CA 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

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

中网威信 CA 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 电子认证服务机构对其他实体的通告

电子认证服务机构在颁发完证书后，不对其他实体发出通告，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

1. 证书的有效期将要到期，证书更新；
2. 因私钥泄漏而吊销证书；
3. 其他需要密钥更新的原因。

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 颁发新证书时对订户的通告

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

构成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更新证书的发布

对密钥更新证书的发布同 4.6.6。

4.7.7 电子认证服务机构对其他实体的通告

在颁发证书时对其他实体的通告同 4.6.7。

4.8 证书变更

4.8.1 证书变更的情形

无

4.8.2 请求证书变更的实体

无

4.8.3 证书变更请求的处理

无

4.8.4 颁发新证书时对订户的通告

无

4.8.5 构成接受变更证书的行为

无

4.8.6 电子认证服务机构对变更证书的发布

无

4.8.7 电子认证服务机构对其他实体的通告

无

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

1. 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）订户不能实际履行数字证书认证业务规则。
2. 发生下列情形之一的，中网威信 CA 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、中网威信 CA、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

1. 证书吊销的申请人到中网威信 CA 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；
2. 中网威信 CA 授权的注册机构按照本规则 3.2 的要求对用户提交的证书

吊销申请进行审核；

3. 中网威信 CA 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；
4. 强制吊销是指当中网威信 CA 或其授权的注册机构确认用户违反本《电子认证业务规则》或违反其他法规需要进行强制吊销证书的情况发生时，对订户证书进行强制吊销，吊销后将按订户开户提供的联系方式通知该订户。

4.9.4 吊销请求宽限期

如果出现私钥泄露等事件，订户应当在发现泄露或有泄露嫌疑时立即提出吊销请求。其他吊销原因的吊销请求应当在 24 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

中网威信 CA 在收到吊销请求后应立即处理并在 24 小时内完成。

4.9.6 依赖方检查证书吊销的要求

在具体应用中，依赖方必须使用以下两种功能之一进行所依赖证书的状态查询：

1. 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。
2. 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，确保是由中网威信 CA 发布并且签名。

4.9.7 CRL 发布频率

中网威信 CA 可采用定期的方式发布 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 发布的最大滞后时间

CRL 发布的最长滞后时间为 24 小时。

4.9.9 在线状态查询的可用性

中网威信 CA 提供在线证书状态查询服务，订户可通过 OCSP 服务进行证书状态的实时查询。

4.9.10 在线状态查询要求

依赖方是否进行在线状态查询完全取决于应用的安全要求。很多的应用本身建有用户帐户数据库并基于用户帐户进行应用控制，数字证书在此只起身份鉴别的，在这种情况下，在线状态查询不一定是必需的。对于安全保障要求高并且完全依赖证书进行身份鉴别与授权的应用，依赖方在信赖一个证书前必须通过证书状态在线查询检查该证书的状态。

4.9.11 吊销信息的其他发布形式

除了 CRL、OCSP 外，中网威信 CA 的 LDAP 提供 CRL 查询。

4.9.12 密钥损害的特别要求

无论是最终订户还是中网威信 CA 及其注册机构，发现证书密钥受到安全损害时应立即吊销证书。

4.9.13 证书挂起的情形

1. 证书订户暂停使用证书，例如：用户发现证书载体不见了但不能确认丢失，可以先申请冻结该证书，后续再根据用户要求再进行吊销或者解挂。
2. 中网威信 CA 或其注册机构认为需要将订户证书挂起的情形。
3. 其他情形。

4.9.14 请求证书挂起的实体

根据不同的情况，订户、中网威信 CA、注册机构可以请求挂起最终用户证书。

4.9.15 挂起请求的流程

1. 申请者到中网 CA 授权的发证机构书面填写“证书挂起申请表”，并注明挂起的原因。
2. 中网威信 CA 授权的注册机构按照本规则 3.2 的要求对用户提交的证书挂起申请进行审核；
3. 中网 CA 挂起用户证书后，发证机构将当面通知或通过邮寄的方式通知用户证书被挂起；
4. 用户证书被挂起后，用户必须在证书有效期到期前恢复证书，否则中网威信 CA 或其授权的注册机构将对到期证书注销。对此造成的任何后果，由订户负责。
5. 强制挂起：中网威信 CA 或其授权的注册机构可以依法对订户证书进行强制挂起，挂起后将按订户开户提供的联系方式通知该证书用户。

4.9.16 挂起的期限限制

无论是订户发起的证书挂起，还是中网威信 CA 或其授权的注册机构发起的强制挂起，挂起期限为 15 个工作日，到期后未能进行解挂或者吊销的，系统强制吊销。

4.10 证书状态服务

4.10.1 操作特征

中网威信 CA 通过目录服务器为用户提供证书状态服务。

4.10.2 服务可用性

中网威信 CA 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

无

4.11 定购结束

定购结束是指证书订户终止与中网威信 CA 的服务，它包含以下两种情况：

1. 当证书到期时，证书订户不再延长证书使用期或者不再重新申请证书时，证书订户可以提出服务终止。
2. 在证书的有效期内，由于证书订户的原因而单方面要求终止证书服务。中网威信 CA 将根据证书订户的要求吊销证书。证书订户与中网 CA 的服务终止。

4.12 密钥生成、备份与恢复

4.12.1 密钥生成、备份与恢复的策略与行为

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，加密密钥对由吉林省密码管理委员会办公室的密钥管理中心生成。

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，吉林省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。

1. 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。订户在中网威信 CA 授权的发证机构申请，经审核后，通过中网威信 CA 向吉林省密钥管理中心请求进行加密密钥恢复，恢复后的密钥下载于订户证书载体中。

2. 司法取证密钥恢复：司法取证人员在吉林省密钥管理中心申请，经审核后，由订户加密密钥做恢复处理并存储于特定载体中。

4.12.2 会话密钥的封装与恢复的策略与行为

中网威信 CA 通过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. 认证机构设施、管理和操作安全控制

5.1 物理安全控制

5.1.1 场地位置与建筑

中网威信 CA 主机房位于吉林省长春市第二枢纽大楼，机房除了满足基础标准和建筑物标准外，针对 CA 运营的实际风险，划分为 4 个安全区域，共 6 个物理安全层次。4 个安全区域由外到内包括：公共区域、DMZ 区、操作区域和安全区域。6 个物理安全层次由外到内包括：入口、办公、敏感、数据中心、屏蔽机房（CA 屏蔽机房、KMC 屏蔽机房）、屏蔽机柜（CA 屏蔽机柜）。所有机房严格按照国家密码管理局《证书认证系统密码及其相关安全技术规范》和信息化部《电子商务认证机构建设、运营和管理规范指南（试行）》等规范要求进行建设和管理。机房采用高安全性的监控技术，包括视频实时监测、指纹、身份识别卡等控制技术，以确保物理通道的安全。机房内部一律禁止参观，只有经过中网威信 CA 严格授权的人员才能进入授权的部门和工作地点。

5.1.2 物理访问

为了保证中网威信 CA 物理设施的安全，机房采取了隔离、控制、监控等手段。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入侵报警系统来保护机房物理安全。

物理访问控制包括如下几个方面：

1. 进出每一道门应有记录作为审计依据；
2. 系统采用身份识别卡结合指纹识别控制方法，控制每道门的进出；
3. 授权人员进出每一道门都会有时间记录和相关信息提示；
4. 门禁系统能够自动判断人员所在的区域，如果有授权的人员没有正常程序进入合法授权区，那么该人员也不能正常离开此区域；
5. 任何未授权的访问，系统都将会有相应的提示；
6. 整套系统具有报警系统，任何非法的闯入，都将会触发报警系统，并且系统会明确地指出是哪一处在报警；
7. 所有的门都设有强行开门报警，如果用非正常手段打开任何一道门，系统都会报警。如果任意一道门打开超过一定时间（一般定义为 10 秒）即会报警；
8. 四层以上的区域安装有移动报警器，当所有的授权人刷卡离开房间后，如果房间内还有其他人，就会触发移动报警器，以防止有任何未经允许的人员滞留在房间内；
9. 整套访问控制系统配有断电保护装置，还配有发电机、UPS 提供紧急用电;，至少能提供 8 小时的电力。
10. 每个门（包括消防紧急门）都被摄像覆盖，所有进出情况被记录下来，并且摄像能够辨别出进出人员；
11. 录像系统对这些画面进行 24 小时不间断的录像；

5.1.3 电力与空调

1. 为了确保计算机设备安全可靠连续运行，本工程引入三路电源，其一，引自配电室，进入屏蔽机房配电柜，供给专用空调机；其二，由大楼总配电室 UPS 接至屏蔽机房内计算机配电柜再分别供给各计算机设备用电；其三，由监控室照明配电箱，引三个支路供给屏蔽机房照明及维修插座。全部电气系统均为三相五线制。大量的动力布线按安装规范均穿金属管槽保护。安全可靠，经检验整个系统运行正常。
2. 机房采用两台机房专用空调机，活动地板下送风，顶部侧回风，温度 23±2℃，湿度 45±65%，能够满足机房高热湿比、长时间运行、高可靠性、

安全性的要求。新风系统采用吊顶式新风机，由大楼新风管道引入，对新风进行过滤处理，然后用风管送至的空调机顶部，经检测达到设计要求。

5.1.4 水患防治

中网 CA 在机房建设时已采取相应措施，防止水侵蚀，充分保障系统安全。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。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 火灾防护

中网威信 CA 通过与专业防火部门协调，实施消防灭火等应急响应措施，避免火灾的威胁，充分保障系统安全。其建筑物的耐火等级按照 GBJ45《高层民用建筑设计防火规范》中规定的二级耐火等级设计实施。

5.1.6 介质存储

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

5.1.7 废物处理

当 CA 机构保存的相关数据已不再需要或存档的期限已满时，中网威信 CA 将完全销毁这些数据。所有处理行为将记录在案，以供审查的需要，销毁行为遵守我国的法律。

5.1.8 异地备份

中网威信 CA 中心具备完善的备份措施，备份内容包括各级 CA 系统、系统配置文件、中网威信 CA 网站、加密机、RA、网络设备配置、数据库等，同时

提供异地备份，在北京京门大厦建立了中网威信 CA 异地备份中心，存储中网 CA 系统的备份数据和介质，异地备份介质安全要求符合中网威信 CA 备份标准和程序。京门备份中心拥有备份系统与场地、配备了专职人员、建立并制定了一系列运行管理制度、数据备份策略和灾难恢复程序，可以承担灾难恢复任务。当整个 CA 系统出现灾难时，可以通过异地备份中心的备份数据恢复 CA 系统。

系统备份

1、当第一次安装系统后就保存每个文件的拷贝。执行防火墙、交换机的相关命令和软件备份防火墙、交换机的配置文件。并备份各主机系统初始配置。

2、每周/月定期备份重要的操作系统和应用程序配置文件，系统改动的程序和配置文件修改后及时备份。

数据库备份

1、通过数据库同步功能将数据实时远程复制到京门备份中心

2、吉林CA中心通过磁带库进行备份，每周一次全备份，每天进行数据库的增量备份

3、在京门备份中心，通过磁带库对复制过来得数据库进行备份，每周一次全备份，每天进行数据库的增量备份

根据数据重要性和备份的复杂程度安排日常备份和阶段性备份。

日常备份采用实时的磁带机备份，或者每日/周采用手工保存备份数据的压缩包到硬盘或磁带上。

阶段性备份是在日常备份的基础上为了较长时间的保存数据，采用的通常以月、季度或半年为时间单位的备份。操作上，采用手工备份数据到异地或光盘的方式。此外，在对系统进行变更前后也应该采用阶段性备份的方式，用于较长时间的保存备份成果。

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。

1. 超级管理员

负责 CA 中心系统的策略设置，设置各子系统的业务管理员并对其管理的业务范围进行授权。超级管理员由系统初始化时产生，主要职责是设置业务管理员并进行权限分配。

2. 超级审计管理员（安全管理员）

系统初始化时随 CA 超级管理员一起生成。签发审计管理员。作为 CA 中心系统的安全管理员，就是要开发内部过程和具体操作，以满足本规则中提出的指导方针。

3. CA 系统管理员

由 CA 超级管理员设置并分配权限。负责 CA 中心系统的某个子系统的业务管理，设置本子系统的业务操作员并对其操作的权限进行授权等。

4. 审计管理员

由超级审计管理员进行设置。负责对涉及系统（CA、RA）安全的事件和各类管理和操作人员的行为进行审计和监督。并定期向 CA/RA 中心主管领导汇报。

5. CA 设备管理员

由 CA 超级管理员设置并分配权限，负责维护管理 CA 的设备及应用系统如主机、加密机、数据库等的安全运行以及服务器证书的配置、更新等。

6. CA 操作员

由 CA 管理员设置并分配权限，按其权限进行具体的业务操作，如统计、计费管理、价格设置、证书归档等。

7. RA 管理员

由 CA 超级管理员签发证书并分配权限，负责 RA 中心的业务管理，设置 RA 系统的操作员并对其操作的权限进行授权等。

8. RA 操作员

由 RA 管理员设置并分配权限，负责管理普通用户和按其权限进行具体的业务操作。

9. 审核员

由 RA 管理员设置并分配权限，负责审核用户证书申请操作。

10. LA 操作员

由 RA 管理员设置并分配权限，用于管理本业务受理点内的普通用户。

5.2.2 每项任务需要的人数

中网威信 CA 确保单个人不能接触、导出、恢复、更新、吊销中网威信 CA 的 CA 系统存储的根证书对应的私钥。

访问 CA 密钥离线生成室和 CA 密钥离线存放室，至少两名有访问权限的人员。

掌管秘密分割，至少 5 人。

操作存放有 CA 密钥的密码设备，包括密钥生成，至少需要 3 个秘密分割持有人。

中网威信 CA 对与运行和操作相关的职能有明确的分工，贯彻互相牵制的安全机制。

5.2.3 每个角色的识别与鉴别

所有中网威信 CA 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身份识别卡和指纹识别;进入管理系统需要使用数字证书进行身份鉴别。中网威信 CA 将独立完整地记录其所有的操作行为。

5.2.4 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，即中网威信 CA 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

所有的员工与中网威信 CA 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。中网威信 CA 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

CA 中心员工的录取经过严格的审查， 根据岗位需要增加相应可信任的员工。 员工需要有 3 个月的考察期，关键岗位的员工考察期为半年，核心岗位的员工考察期为一年。根据考察的结果安排相应的工作或者辞退并且剥离岗位。CA 中心根据需要对员工进行职责、岗位、技术、政策、法律、安全等方面的培训。

CA 中心会对其关键的 CA 职员进行严格的背景调查。受理点操作员的审查可以参照 CA 中心对可信任员工的考察方式。受理点责任单位可以在此基础上，增加考察和培训条款，但不得违背 CA 中心证书受理的规程和 CA 中心证书业务声明。

CA 中心确立流程管理规则，据此 CA 员工受到合同和章程的约束，不许泄露 CA 中心证书服务体系的敏感信息。所有的员工与 CA 中心签定保密协议， 合同期满以后 3 年内仍然不得从事与 CA 中心相类似的工作，并报第三方公证。

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

5.3.3 培训要求

中网威信 CA 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中网威信 CA 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 中网威信 CA 组织的培训一次。

根据 CA 中心策略调整、系统更新等情况，CA 中心可能要求员工进行再培训，以适应新的变化。

5.3.5 工作岗位轮换周期和顺序

CA 中心负责运营的员工和负责 CA 设计、开发、维护的员工承担不同的职责， 双方的岗位互相分离，为了保证安全，后者不能成为前者。即开发员工和运营员工分离的原则。

可根据实际情况，CA 中心的关键岗位可采取轮换制度，轮换周期根据具体情况而定，定期或不定期均可。

5.3.6 未授权行为的处罚

当 CA 中心员工被怀疑，或者已进行了未授权的操作，例如未经授权滥用权利或超出权限使用 CA 中心系统或进行越权操作，中网威信 CA 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 独立和约人的要求

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

1. 人员档案进行备案管理；

2. 具有相关业务的工作经验；
3. 必须接受中网威信 CA 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：

1. 中网威信 CA 中心技术白皮书；
2. 各级用户使用手册；
3. 中网威信 CA 管理制度；
4. 机房设备管理办法；
5. 客户服务规范；
6. 数字证书运营规范；
7. 相关法律、政策、制度说明；
8. 灾难备份和恢复方案等。

5.4 审计日志程序

5.4.1 记录事件的类型

中网威信 CA 的 CA 和 RA 运行系统，记录所有与系统相关的事件，以备审查。这些记录，无论是手写、书面或电子文档形式，都包含事件日期、事件的内容、事件的发生时间段、事件相关的实体等。

中网威信 CA 记录其它与 CA 系统本身不相关的事件，例如：物理通道参观记录、人事变动等。

5.4.2 处理日志的周期

中网威信 CA 每周对记录进行审查，对审查记录行为备案。

5.4.3 审计日志的保存期限

中网威信 CA 在数据库保存审查记录至少三个月，离线存档至少七年。

5.4.4 审计日志的保护

中网威信 CA 执行严格的访问控制管理，确保只有中网威信 CA 授权的人员才能接近这些审查记录。这些记录处于严格的保护状态，严格禁止访问、阅读、修改和删除等操作。

5.4.5 审计日志备份程序

中网威信 CA 保证所有的审查记录和审查总结都按照中网威信 CA 备份标准和程序进行。根据记录的性质和要求，采用在线和离线的各种备份工具，有实时、每天、每周、每月和每年等各种形式的备份。

5.4.6 审计收集系统

中网 CA 审计收集系统涉及：

1. 证书管理系统；
2. 证书签发系统；
3. 证书目录系统；
4. 远程通信系统；
5. 证书审批受理系统；
6. 访问控制系统（包括防火墙）；
7. 网站、数据库安全保障系统；
8. 其他中网威信 CA 认为有必要审查的系统。

中网 CA 全天候准备上述系统的检查管理和审查工具。在需要的时候，中网威信 CA 会随时应用这些工具来满足各项审查的要求。

5.4.7 对导致事件实体的通告

中网威信 CA 对审查中发现的攻击现象将做详细记录，在法律许可的范围内追溯攻击者，并保留采取相应对策措施的权利，如：切断对攻击者已经开放的服务、递交司法部门处理等措施。

中网威信 CA 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

对在审查过程中发现的系统的脆弱性，中网威信 CA 的相关关键人员，包括审计管理员、安全管理员、系统超级管理员等，或者聘请专业的系统安全评估单位，共同进行相应的脆弱性评估，出具评估报告，并在 1 个月内对系统脆弱性进行修补。

对在审查过程中发现的物理安全、制度安全、人员安全等方面问题，要及时进行相应的处理和解决。

5.5 记录归档

5.5.1 归档记录的类型

中网威信 CA 会对 CA 的数据库定期存档，间隔时间由中网威信 CA 自行决定，存档的内容包括中网威信 CA 发行的证书和 CRL、审查数据记录、订户提交的证书申请材料、证书申请审批资料等。（签名私钥由实体本身保存，有关私钥的责任由实体本身承担）。

5.5.2 归档记录的保存期限

中网威信 CA 中的存档期限一般规定为七年。

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接近它们。

中网威信 CA 保护相关的档案免遭恶劣环境的威胁，例如温度、湿度和磁力的破坏。

中网威信 CA 每年会验证存档信息的完整性。

5.5.4 归档文件的备份程序

所有存档文件的数据库除了保存在中网威信 CA 的主要存储库，还将在异地保存其备份。

存档的数据库采取物理或逻辑隔离的方式，与外界不发生信息交互。

只有授权的工作人员才能在监督的情况下，对档案进行读取操作。

中网威信 CA 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

所有存档内容都要加时间标识。系统产生的记录，用标准时间加盖时间戳。

5.5.6 归档收集系统

中网威信 CA 中的档案收集系统由人工操作和自动操作两部分组成。

5.5.7 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。中网威信 CA 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

电子认证服务机构的密钥更替是指当中网威信 CA 根证书到期而需要更换根密钥对时所采取的措施。

1. 中网威信 CA 根密钥对由加密机产生，有效期为 30 年。证书到期更换密钥时将签发 3 张证书。
   1) 使用旧的私钥对新的公钥及信息签名生成证书；
   2) 使用新的私钥对旧的公钥及信息签名生成证书；
   3) 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认证、信

任。

2. 在中网威信 CA 证书到期之前，中网威信 CA 将对根私钥进行更换。密钥转换程序在旧密钥对向新密钥对的转换起着过渡的作用。中网威信 CA 密钥转换采用以下方式：

1) 中网威信 CA 将在证书到期前的 60 天内停止颁发新的证书；
2) 旧的中网威信 CA 证书到期后，中网威信 CA 将用新的 CA 密钥对签发证书。
3) 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。

3. 中网威信 CA 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 损害与灾难恢复

5.7.1 事故和损害处理程序

发生故障时，中网威信 CA 将按照灾难恢复计划实施恢复。

流程为：

1. 保证现有的对外提供的所有设备能够正常提供服务，并且针对每个环节设置紧急预案。
2. 所有的 CA 应用服务都具备基本的监控。
3. 出现故障时，应以尽快正常对外提供服务为目标，记录故障现场，对于影响面大的故障，发现问题 5 分钟内不能快速解决问题的，应考虑启动紧急预案。
4. 严重影响对外服务的故障，应该及时上报主管领导。

5.7.2 计算资源、软件和/或数据的损坏

当计算资源、软件和/或数据收到破坏时，进行以下操作：

1. 恢复环境、CA 系统和备份数据并上线；

2. 为用户恢复证书，重新进行认证；
3. 尽快启动原系统。

5.7.3 实体私钥损害处理程序

参照 4.7 节进行密钥更新。

5.7.4 灾难后的业务连续性能力

灾难发生后中网威信 CA 立即从备份系统或异地备份中心恢复系统和数据，系统上线并对用户提供服务，保持业务持续性。

5.8 电子认证服务机构或注册机构的业务终止

因各种情况，中网威信 CA 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。

中网威信 CA 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，包括但不限于中网威信 CA 授权的发证机构和订户等。

在终止服务六十日前向工业和信息化部报告，按照相关法律规定的步骤进行操作。

中网威信 CA 采用以下措施终止业务：

1. 起草中网威信 CA 终止业务声明；
2. 停止认证中心所有业务；
3. 处理加密密钥；
4. 处理和存档敏感文件；
5. 清除主机硬件；
6. 管理中网威信 CA 系统管理员和安全管理员；
7. 通知与中网威信 CA 终止运营相关的实体。
8. 根据中网威信 CA 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

1. 加密密钥对

加密密钥对是由中华人民共和国国家密码管理局许可的、中网威信 CA 数字证书签发系统支持的加密机设备生成的，由中网威信 CA 所连接的省级国密办 KMC 控制管理。

2. 签名密钥对

签名密钥对由客户端产生，证书申请者可使用国家密码管理局认可的、中网威信 CA 数字证书签发系统支持的介质生成签名密钥对。此签名密钥存储在介质中不可导出，保证中网威信 CA 无法复制签名密钥对。

中网威信 CA 支持多种介质，如 USBkey、软盘等。中网威信 CA 可根据证书申请者要求或自身选择签名密钥对生成介质。

3. 服务器证书的密钥对由用户自己产生，用户应妥善保管。
4. 中网威信 CA 在技术、流程和管理上保证密钥对产生的安全性。

6.1.2 私钥传送给订户

证书订户的加密私钥是在吉林省密钥管理中心产生的，该私钥只保存在密钥管理中心。在加密私钥从密钥管理中心到订户的传递过程中采用订户的签名公钥和国家密码管理局许可的对称密钥算法对加密私钥进行加密，中网威信 CA 无法获得，保证了证书用户的密钥安全。

6.1.3 公钥传送给证书签发机构

中网威信 CA 从吉林省密钥管理中心取得用户公钥后为其签发证书，在此过程中也采用国家密码管理局许可的对称密钥算法加密，保证传输中数据的安全。

6.1.4 电子认证服务机构公钥传送给依赖方

中网威信 CA 的根公钥包含在中网威信 CA 自签的根证书中。证书订户可以从中网威信 CA 的网站上下载中网威信 CA 根证书。

6.1.5 密钥的长度

中网威信 CA 用于加密和签名的非对称密钥对的模长是 1024 比特。

6.1.6 公钥参数的生成和质量检查

公钥参数由国家商用密码管理局许可的、中网威信 CA 数字证书签发系统支持的硬件产生。

6.1.7 密钥使用目的

在中网威信 CA 证书服务体系中的密钥用途和证书类型紧密相关。

1. 中网 CA 的签名密钥用于签发 RA 证书和证书废止列表（CRL）；
2. RA 的签名密钥用于确认 RA 所做的审批证书等操作；
3. 签名密钥用于提供网络安全服务，如信息在传输过程中不被篡改、接收方能够通过数字证书来确认发送方的身份、发送方对于自己发送的信息不能抵赖等；
4. 加密密钥用于对网络上传送的信息进行加密，保证信息除发送方和接受方外不被其他人窃取、篡改。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块的标准和控制

中网威信 CA 使用国家商用密码管理局许可的产品，密码模块的标准符合国家规定的要求。

6.2.2 私钥多人控制（m 选 n）

中网威信 CA 采用 M 选 N 多人控制策略激活、使用、停止中网威信 CA 的签名密钥。M>=N，M 为 5，N 为 3。

6.2.3 私钥托管

吉林省密钥管理中心根据客户和法律的需要，对加密密钥进行托管。签名私钥从不进行托管，以保证其不可否认性。

6.2.4 私钥备份

证书订户可以备份他们的私钥，以确保这些私钥的安全。

吉林省密钥管理中心备份托管的加密私钥，确保加密私钥的安全。

6.2.5 私钥归档

吉林省密钥管理中心提供过期的托管私钥的存档服务。

6.2.6 私钥导入、导出密码模块

在中网威信 CA 证书服务体系中，使用中网威信 CA 的软件可以把私钥导入密码模块中。私钥无法从硬件及软件密码模块中导出。必须通过密码验证之后，才可能使用存储在密码模块中的私钥进行加解密操作。

6.2.7 私钥在密码模块的存储

中网威信CA私钥以加密的形式存放在硬件密码模块中，在密码模块内部使用。

6.2.8 激活私钥的方法

1. 个人证书：最终订户的个人证书私钥可以存放在订户计算机的软件密码模块中也可以存放在如 USB Key 和智能卡等硬件密码模块。对于存放在软件模块中的私钥，订户应该采用合理的措施从物理上保护计算机以

防止在没有得到订户授权的情况下其他人员使用订户的计算机。如果存放在软件密码模块中的私钥没有口令保护，那么，软件密码模块的加载意味着私钥的激活。如果该私钥有口令保护，软件密码模块加载后，还需要输入口令才能激活私钥。对于存放在硬件模块中的私钥，私钥可以通过 PIN 码（口令）等安全机制保护激活。如果私钥没有 PIN 码（口令）保护，那么，当用户计算机上安装了相应的硬件密码模块驱动程序后，将 USB Key 或智能卡插入到相应的读卡设备中，私钥将会被激活可以使用。如果私钥有 PIN 码（口令）保护，将 USB Key 或智能卡插入到相应的读卡设备中后，只有输入 PIN 码（口令）后，私钥才被激活可以使用。

2. 企业证书：对于中网威信 CA 签发的组织机构身份证书、组织机构代表人证书，订户必须使用 USB Key、智能卡等硬件密码设备存放私钥，私钥不能出卡，并且订户要使用 PIN 码（口令）等机制保护私钥，要激活私钥，用户计算机上需安装相应的驱动程序并将 USB Key 或智能卡插入相应的读卡设备，输入相应的 PIN 码（口令）后私钥才可以激活使用。
3. 服务器证书：对于中网威信 CA 签发的服务器证书，如果没有使用硬件密码模块产生、保存私钥，则私钥是存放在服务程序的软件密码模块中，这时订户应该使用口令对私钥进行保护。当服务程序启动，软件加密模块被加载，并输入相应的私钥保护口令后，证书私钥被激活。如果使用硬件密码模块，则私钥需要被口令保护。当硬件密码模块被安装到订户服务器上，服务程序启动，并输入相应私钥保护口令后，证书私钥被激活。
4. 中网威信 CA 私钥：中网威信 CA 私钥存放在硬件密码模块中，并且其激活数据按 6.2.2 要求进行分割。当需要使用 CA 私钥时，将硬件密码模块加载并按 5 选 3 的原则输入激活数据的分割。

6.2.9 解除私钥激活状态的方法

对于存放在软件密码模块中最终订户私钥，当软件密码模块被下载、订户退出登录状态、操作关闭或计算机断电时，私钥被解除激活状态。对于存放在硬件

密码模块中最终订户私钥，当每次操作后注销计算机，或者把硬件密码模块从读卡器中取出时，私钥成为非激活状态。对于服务器证书，当服务程序下载、系统注销或系统断电后私钥即进入非激活状态。

对于中网威信 CA 私钥，当存放私钥的硬件密码模块断电,，私钥即进入非激活状态。

6.2.10 销毁私钥的方法

私钥不再使用、不需要保存时，应该将私钥销毁，从而避免丢失、偷窃、泄露或非授权使用。

对于中网威信 CA 签发的最终订户加密证书私钥，在其生命周期结束后，订户应该妥善保存一定期限，以便于解开加密信息。对于中网威信 CA 签发的最终订户签名私钥，在其生命周期结束后，无需再保存，可以通过私钥的删除、系统或密码模块的初始化来销毁。

在中网威信 CA 私钥生命周期结束后，中网威信将 CA 私钥继续保存在一个备份硬件密码模块中，并进行归档，其他的 CA 私钥备份被安全销毁。归档的 CA 私钥在其归档期限结束后，需在多名可信人员参与的情况下安全销毁。CA 私钥的销毁将确保 CA 私钥从硬件密码模块中彻底删除，不留有任何残余信息。

6.2.11 密码模块的评估

中网威信 CA 使用济南得安的 SJY05-B 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。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

中网威信 CA 对所有的公钥进行归档处理，通过专门的归档软件对公钥进行归档，并加密保存在数据库中，保证了公钥的安全性。

6.3.2 证书操作期和密钥对使用期限

中网威信 CA 会在用户申请审核鉴定通过，用户并付款后 5 个工作日内将证书颁发给用户，密钥对的使用期限与证书有效期相一致，一般为 1 年。

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：USBKEY、智能 IC 卡）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

中网威信 CA 采取加解密机制等多种方式保护敏感数据，以避免未授权使用。未授权用户企图使用敏感数据达到预定目的时，敏感数据会自动锁定。

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

中网威信 CA 的数字证书签发系统的数据文件和设备由中网威信 CA 系统管理员维护，未经中网威信 CA 管理员授权，其它人员不能操作和控制中网 CA 系统。中网威信 CA 系统部署在多级不同厂家的防火墙之内，确保系统网络安全。

中网威信 CA 系统内的计算机均采用了如防火墙、入侵检测、主机服务端口限制、操作系统安全补丁等防范措施，充分保证了计算机的安全可靠。

对于设备有一套完整的保管和维护制度：

1. 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。
2. 对设备定期进行检查、清洁和保养维护。
3. 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。
4. 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
5. 维修过程及与维修有关的情况等。
6. 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

中网威信 CA 使用的密码设备是通过国家密码管理局批准生产的密码设备。其他涉及安全的网络设备、主机、系统软件等都通过了国家相关部门的检测，属合格产品。

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

中网威信 CA 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。中网威信 CA 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

中网威信 CA 签发的证书均符合 X.509 V3 证书格式。证书的具体格式、内容和 OID 定义遵循国家推荐的 X.509C 标准。

7.1.1 版本号

X.509V3。

7.1.2 证书标准项

1. 证书序列号

   唯一标识该证书。

2. 证书有效期

   证书的起止时间。

3. 主题

   为证书用户申请证书时所填写的申请信息。即用户的甄别名。

4. 发行者

包括 CN 等

7.1.3 算法对象标识符

使用 SHA1WithRSAEncryption 算法

算法 OID 1.2.840.113549.1.1.5

7.1.4 名称形式

采用 X.500 甄别名格式。

7.1.5 名称限制

除了针对互联网增值业务等虚拟实体所颁发的证书外，中网威信 CA 签发的其他证书中的通用名不能使用假名、伪名。

7.1.6 证书策略对象标识符

中网威信的每类证书（个人证书、企业证书、服务器证书）对应一个证书策略对象标识符。当使用证书策略扩展项时，中网威信 CA 签发证书中包含证书策略对象标识符，该对象标识符与相应的证书类别对应。

7.1.7 策略限制扩展项的方法

没有使用。

7.1.8 策略限定符的语法和语义

没有使用。

7.1.9 关键证书策略扩展项的处理规则

没有规定。

7.1.10 证书扩展项

包括授权密钥标识符、主题密钥标识符、密钥使用范围、密钥扩展使用、证书策略、基本限制、CRL 发布点等内容，与 X509 和 PKIX 规定一致。

7.2 证书吊销列表

中网威信 CA 定期签发 CRL（证书废除列表）。

7.2.1 版本号

X.509：V2。

7.2.2 CRL 和 CRL 条目扩展项

包含 CRL 颁发者、签名算法等内容，中网 CA 每隔 24 小时自动发布最新的 CRL。

7.3 在线证书状态协议

中网威信 CA 为证书用户提供 OCSP（在线证书状态查询）服务，OCSP 为 CRL 的有效补充，方便证书订户及时查询证书状态信息。采用 RFC 2560 OCSP 协议。

7.3.1 版本号

V1。

7.3.2 OCSP 扩展项

与 RFC2560 一致。

8. 认证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、确认中网威信 CA 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。

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

外部审计由中网威信 CA 委托第三方审计机构来承担，审计的依据包括 中网威信 CA 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

对中网威信 CA 实施规范审计的审计者所具有的资质和经验必须符合监管法律和行业准则规定的要求，包括：

1) 必须是经许可的、有营业执照的、具有计算机安全专门技术知识的的审计人员或审计评估机构，且在业界享有良好的声誉。
2) 了解计算机信息安全体系、通信网络安全要求、PKI 技术、标准和操作。
3) 具备检查系统运行性能的专业技术和工具。

8.3 评估者与被评估者之间的关系

独立的第三方审计机构。

8.4 评估内容

评估的内容包括：CA 环境控制、密钥管理操作和 CPS 的执行情况等。

8.5 对问题与不足采取的措施

对审计中发现的问题，中网威信 CA 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。中网威信 CA 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

审计结果将传达给中网威信中层以上管理者。除非法律明确要求，中网威信 CA 一般不公开评估结果。

对中网威信 CA 关联方，中网威信 CA 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各省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，中网威信 CA 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，中网威信 CA 暂不收取查询费用。对此规定有任何变换，中网威信 CA 将会在网站公示。

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，中网威信 CA 暂不收取信息访问费用。对此规定有任何变换，中网威信 CA 将会在网站公示。

对于在线证书状态查询(OCSP)，由 中网威信 CA 与订制者在协议中约定。

9.1.4 其他服务费用

暂无规定。

9.1.5 退款策略

在实施证书操作和签发证书的过程中，中网威信 CA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，中网威信 CA 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，中网威信 CA 将 不 退 还剩余时间的服务费用。

9.2 财务责任

中网威信 CA 每年定期委托公正、客观的第三方进行财务审计。

9.2.1 保险范围

中网威信 CA 保证其具有维持其运作和履行其责任的财务能力，向证书订户提供证书使用保障。如果由于中网威信 CA 原因造成用户使用证书过程中遭受损失，中网威信公司将向证书订户、依赖方提供赔偿。

9.2.2 其他资产

无。

9.2.3 对最终实体的保险或担保

中网威信客户保障计划提供的服务保障针对的最终实体主要是证书订户和证书依赖方。

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：

1. 双方之间的协议、往来函件等，未经对方书面许可，不得对任何第三方公开；
2. 明示为不可对外披露的信息的；
3. 在保密情况下由双方披露的或知悉的；
4. 双方根据合理的商业判断应理解为保密数据和信息的；
5. 以其他书面或有形形式确认为保密信息的；
6. 或从上述信息中衍生出的信息。

对于中网威信 CA 来说，保密信息包括但不限于以下方面：

1. 最终用户的私人签名密钥都是保密的；
2. 保存在审计记录中的信息；
3. 年度审计结果也同样视为保密；
4. 除非有法律要求，由中网威信 CA 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。

中网威信 CA 不保存任何证书应用系统的交易信息。

除非法律明文规定，中网威信 CA 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、手续、申请操作指南等信息是公开的。中网威信 CA 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 中网威信 CA 目录服务等方式向外公布。

中网威信 CA 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

1. 各方应遵守本规则之规定，承担保密责任。不将保密数据和信息(也不会促使或允许他人将保密信息)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，如果已明确表示保密信息不得复印、复制或储存于任何数据存储或检索系统，接受方不必须严格遵守。
2. 当 中网威信 CA 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，中网威信 CA 应按照要求进行合理披露，中网威信 CA 无须承担任何责任。这种提供不被视为违反了保密义务。

9.4 个人隐私保密

9.4.1 隐私保密方案

中网威信 CA 按照中华人民共和国相关法律法规之规定尊重和保护证书申请人和用户的个人隐私。除非证书申请人主动提供，中网威信 CA 保证不会截取任何证书申请人的资料。中网威信 CA 应保护证书申请人所提供的，证明其身份的资料。中网威信 CA 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，通过中网威信 CA 目录服务等方式向外公布。

9.4.4 保护隐私的责任

任何接收到隐私信息的参与者有责任保护隐私信息不被泄漏给任何第三方。

9.4.5 使用隐私信息的告知与同意

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

依照法律或行政程序进行的信息披露，应当符合下列条件：

1. 政府法律法规的规定并且经相关部门通过合法程序提出申请。
2. 法院以及公权力部门处理因使用证书产生的纠纷时合法的提出申请。
3. 具有合法司法管辖权的仲裁机构的正式申请。
4. 证书订户以书面形式进行授权。

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及与订户相关协议处理。

9.5 知识产权

中网威信 CA 享有并保留对证书以及 CA 系统软件完整的知识产权，依法享有各项权利。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

中网威信 CA 在提供电子认证服务活动过程中的承诺如下：

1. 中网威信 CA 遵守《中华人民共和国电子签名法》及相关法律的规定，接受工业和信息化部的领导，对签发的数字证书承担相应的法律责任。
2. 中网威信 CA 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相关规定。

3. 除非已通过中网威信 CA 证书库发出了中网威信 CA 的私钥被破坏或被盗的通知，中网威信 CA 保证其私钥是安全的。
4. 中网威信 CA 签发给订户的证书符合中网威信 CA 的 CPS 的所有实质性要求。
5. 中网威信 CA 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。
6. 中网威信 CA 将及时吊销证书。
7. 中网威信 CA 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。
8. 证书公开发布后，中网威信 CA 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

中网威信 CA 的注册机构在参与电子认证服务过程中的承诺如下：

1. 提供给证书订户的注册过程完全符合中网威信 CA 的 CPS 的所有实质性要求。
2. 在中网威信 CA 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。
3. 注册机构将按 CPS 的规定，及时向中网威信 CA 提交证书申请、吊销、更新等服务请求。

注册机构必须遵守和符合本认证业务声明的条款。

9.6.3 订户的陈述与担保

所有的证书订户必须严格遵守关于证书申请以及私钥的所有权和安全保存相关的程序：

1. 证书订户在证书申请表上填列的所有声明和信息必须是完整、准确、真实和有效的，可供中网威信 CA 或受理点检查和核实；

2. 证书订户必须严格遵守认证业务声明规定或者由中网威信 CA 推荐使用的安全措施；
3. 证书订户需熟悉本认证业务声明的条例和与证书相关的证书政策，还需遵守证书订户证书使用方面的有关限制；
4. 一旦发生任何可能导致安全性危机的情况，如证书订户遗失私钥、遗忘或泄密以及其他情况，证书订户应立刻通知中网威信 CA 或中网威信 CA 授权的发证机构，申请采取挂失、吊销等处理措施。
5. 订户已知其证书被冒用、破解或被他人非法使用时，应及时通知中网威信 CA 吊销其证书。

9.6.4 依赖方的陈述与担保

依赖方在信赖中网 CA 证书的时候，必须保证遵守和实施以下条款：

1. 依赖方熟悉相关的证书政策，了解证书的使用目的。
2. 依赖方在信赖任何 CA 证书前，必须查最新的 CRL 以检查证书的状态，只有确认该证书没有被作废时，该证书才有效。
3. 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这里的有关条例。

9.6.5 其他参与者的陈述与担保

其他参与者如目录服务提供者、以及其他提供电子认证相关服务的实体需要遵守中网威信 CA 的 CPS。

9.7 担保免责

因证书申请人的原因导致的法律责任应由申请人全部承担，中网威信 CA 不承担与申请人、用户、依赖方陈述相关的、与证书内容相关的法律和经济责任。

中网威信CA不承担任何其他未经授权的人或组织以中网威信CA名义编撰、发表或散布不可信赖的信息所引起的法律责任。

中网威信 CA 在法律许可的范围内，可以根据受害者或法律的要求提供协查帮助，但并不对此承担法律责任。

中网威信 CA 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。

9.8 有限责任

中网威信 CA 在对外服务过程中只承担对外声明的、本 CPS 中规定的、对外签署的任何协议中所规定的有限责任。

中网威信 CA 在与用户和依赖方签署的协议中，对于因用户或依赖方的原因造成的损害不承担任何责任。

9.9 赔偿

9.9.1 赔偿条件

对于由如下原因给订户或依赖方造成损失，中网威信应对订户或依赖方进行赔偿。

1. 由于中网威信 CA 的未授权使用或泄露造成的用户私钥泄露；
2. 由于中网威信 CA 自身原因造成的用户证书的错误发放；
3. 当中网威信 CA 由于故意违反本 CPS，给用户造成客户的经济损失的；
4. 由于中网威信 CA 自身原因造成颁发给用户的证书信息出现实质性错误的。

对于因如下原因给中网威信或依赖方造成损失的，订户应承担赔偿责任：

1. 订户在证书申请时作虚假、错误陈述的；
2. 订户在证书申请中故意或过失遗漏披露重要信息的；
3. 订户没有采取合理的防护措施，造成订户私钥的安全损害、丢失、泄漏、修改或非授权使用的；
4. 订户使用的名字（包括但不限于通用名、域名和 e-mail 地址）侵害了第三方的知识产权法。
5. 其它仅因订户原因，给中网威信或依赖方造成损失的。

对于因如下原因给中网威信造成损失的，依赖方应承担赔偿责任：

1. 依赖方没有履行依赖方职责义务；
2. 依赖方不合理的信赖一个证书；
3. 依赖方没有检查证书状态确定证书是否过期或吊销。

9.10 有效期限与终止

9.10.1 有效期限

中网威信 CA 的 CPS 自发布之日起生效，CPS 中将详细注明版本号及发布日期，最新版本的 CPS 通过访问中网威信 CA 网站获得，对具体个人不做另行通知。

9.10.2 终止

当新版本的 CPS 正式发布生效，则旧版本的 CPS 将自动终止。公钥到了有效使用期，对应的依赖方协议终止。当证书到期或吊销后，订户协议即终止。

9.10.3 效力的终止与保留

中网威信 CPS 的终止（而非更新），意味着中网威信认证业务的终止。中网威信终止认证业务的过程将按国家有关主管部门的规定进行，并根据规定对受影响的客户进行安排，保证客户的利益不受影响或将受影响的程度减少到最小。

当由于某种原因，如内容修改、与适用法律相冲突，CPS、订户协议、依赖方协议和其他协议中的某些条款失效后，不影响文件中其他条款的法律效力。

9.11 对参与者的个别通告与沟通

9.12 修订

9.12.1 修订程序

本认证业务规则将尽量避免不必要的修改，但当出现以下情形时。中网威信 CA 将对 CPS 进行修订：

1. 因相关法律法规要求而引起本业务规则发生改变。
2. 因相关技术条件变化而引起本业务规则发生改变。
3. 因其它原因而引起本业务规则发生改变。

中网威信安全管理委员会将对本 CPS 及其他相关文档、协议提出修改建议，获得中网威信管理层批准后，由中网威信安全管理委员会负责组织有关文档、文件的修改。修改后的 CPS 及其他相关文档、协议经中网威信管理层批准后正式发布。

9.12.2 通知机制和期限

本《电子认证业务规则》在 中网威信 CA 的网站(http://www.uni-ca.com.cn)上发布。

版本更新时，最新版本的《电子认证业务规则》在 中网威信 CA 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

当相关法律、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

中网威信 CA 与订户、依赖方发生争议时，应向中网威信 CA 所在地仲裁机构提请仲裁。

9.14 管辖法律

本认证业务规则的制订均依据我国相关法律法规。

9.15 与适用法律的符合性

在任何情况下，中网威信 CA 认证业务规则的执行、解释、翻译和有效性均应遵守和适应中华人民共和国的相关法律和法规。如有冲突，应以中华人员共和国的相关法律和法规为准。

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 转让

中网威信 CA、注册机构、订户及依赖方之间的责任、义务，不可通过任何形式转让给他方。

9.16.3 分割性

当仲裁机构或司法机关认定合同（协议）某一条款无效力，不影响合同（协议）其它条款效力。

9.16.4 强制执行

合同（协议）一方或几方不履行合同（协议）条款的，其他方可以要求强制执行。

9.16.5 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。在数字证书认证

活动中，中网威信 CA 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依法免除法律责任。

9.17 其他条款

中网威信 CA 与具体用户协商后另行确定其他条款，包括未在上述说明的其他相关内容条款。

中网威信 CA 对本《电子认证业务规则》拥有最终解释权。