中网威信数字证书认证中心全球认证体系证书策略（CP）

起草部门：技术支撑部

起草人：史炳荣、迟百顺

批准人：高文龙

版本号：Version 3.0

编制日期：2017 年 3 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
1.0	**形成版本并审核通过**			**安全管理委员会**	

对任何复制本文件的其他请求，请通过下述联络方式与中网威信电子安全服务有限公司进行商议：

公司名称：中网威信电子安全服务有限公司。

法定地址：中华人民共和国北京市西城区西单北大街 133 号甲 1209 室。

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。

关于中网威信数字证书认证中心全球认证体系 CP 中主要权利及义务的概述

此概述仅就本 CP 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 CP 全文。

1、本 CP 文件规定了中网威信数字证书认证中心全球认证体系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) 从中网威信全球数字认证中心网站及其他渠道可以得到有关数字签名、证书及 CP 文件，证书申请者可以参加相关的培训和学习。

3、中网威信全球数字认证中心提供不同类型的证书，申请者应自行或向中网威信全球数字认证中心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 CP 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全球数字认证中心签发的证书。在此之前，中网威信全球数字认证中心建议应检查中网威信全球数字认证中心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，及时通知中网威信全球数字认证中心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 CP 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

证书策略（CP，Certificate Policy）是认证机构（CA，Certification Authority）制定的一组策略，表明中网威信数字证书认证中心（以下简称中网 CA）全球认证体系中各个参与者的划分以及义务，并包含中网 CA 证书基本策略。

本 CP 的适用范围为中网 CA 全球认证体系发放的证书。

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全球认证体系证书策略》。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

包括CHINA UNICOM GLOBAL ROOT CA和CHINA UNICOM EV SSL CA和CHINA UNICOM SSL CA。均由中网威信数字证书认证中心建设和运营。此外，中网威信数字证书认证中心设立安全认证委员会，作为中网威信数字证书认证中心证书认证业务的策略管理机构。

（1）CHINA UNICOM GLOBAL ROOT CA

CHINA UNICOM GLOBAL ROOT CA是最高证书签发机构，主要职责包括：

- 签发和管理自身证书和下级CA证书
- 管理和发布相关证书、证书撤销列表（CRL）
- 管理和运营证书信息库

（2）CHINA UNICOM SSL CA

CHINA UNICOM SSL CA的主要职责包括：

- 签发和管理订户普通SSL证书
- 管理和发布相关订户证书及证书撤销列表（CRL）

- 管理和运营证书信息库

（3） CHINA UNICOM EV SSL CA

CHINA UNICOM EV SSL CA的主要职责包括：

- 签发和管理订户 SSL证书
- 管理和发布相关订户证书及证书撤销列表（CRL）
- 管理和运营证书信息库

（4） CHINA UNICOM INDIVIDUAL CA

CHINA UNICOM INDIVIDUAL CA的主要职责包括：

- 签发和管理个人订户证书
- 管理和发布相关订户证书及证书撤销列表（CRL）
- 管理和运营证书信息库

（5） CHINA UNICOM ENTERPRISE CA

CHINA UNICOM ENTERPRISE CA的主要职责包括：

- 签发和管理机构订户证书
- 管理和发布相关订户证书及证书撤销列表（CRL）
- 管理和运营证书信息库

（6）安全认证委员会

安全认证委员会由中网威信数字证书认证中心发起设立，是中网威信数字证书认证中心全球认证业务的策略管理机构，主要职责包括：

- 制定和发布证书策略（CP）
- 制定和发布证书认证业务规则（CP）
- 制定和发布运营相关规范
- 制定和发布相关服务规范
- 监督和指导中网威信全球数字认证中心运营服务

1.3.2 注册机构

注册机构 RA（Registration Authority）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。中网威信全球认证体系下的注册机构设置在中网CA 内部，由中网 CA 本身承担 RA 职责，不委托其他机构行使此职责。

1.3.3 订户

订户是从中网威信全球数字认证中心接收证书的实体。在电子签名应用中，订户即为电子签名人。

订户包括个人、机构、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。在中网威信全球数字认证中心证书服务体系中，依赖方是指信任中网威信全球数字认证中心证书，使用中网威信全球数字认证中心颁发证书，利用中网威信全球数字认证中心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全球数字认证中心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CA证书支持相应的合法应用，具体应用场景和配套软件（如浏览器）在相应CPS的1.4节中说明。

1.4.2 限制的证书应用

除用于上述规定的范围外，禁止使用于任何可能会造成人身伤亡、精神伤害，

或者对社会秩序与公共利益有重大危害的应用或业务，并且不得用于《电子签名法》或其他相关法律法规明确禁止或排除的应用。

CA 机构证书不能用来做任何 CA 功能以外的用途，订户证书不得作为 CA 机构证书来使用。

1.5 策略管理

1.5.1 策略文档管理机构

本 CP 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 CP 的制订、发布、更新等事宜。

本 CP 由中网威信电子安全服务有限公司拥有完全版权。

1.5.2 联系人

本 CP 在中网威信全球数字认证中心网站发布，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 CP 符合策略的机构

中网威信公司对本 CP 文件具有决定权和最终解释权。

1.5.4 CP 批准程序

本 CP 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 CP 草案（或 CP 修订内容）后，由安全管理委员会组织专家组对 CP 草案（或 CP 修订内容）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 CP 评审稿提交中网威信公司领导组审批。

审批通过后，由安全管理委员会确定 CP 的文件格式以及版本号，在中网威信全球数字认证中心网站上对外公布。

安全管理委员会定期对 CP 的内容进行审查（通常一年一次），以确定是否进行修订。各部门也可根据业务发展变化需要及时向安全管理委员会提出修改申请。本 CP 也可根据所遵循标准的要求，提出修订申请。

根据《中华人民共和国电子签名法》、《电子认证服务管理办法》的规定，本 CP 自对外公布之日起三十日内向主管部门备案。

1.6 定义和缩写

下列定义适用于本 CP：

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（CP）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

中网威信全球数字认证中心通过网站公布以下信息：本 CP 修订以及其他由中网威信全球数字认证中心不定时发出的信息。CA 中心网址：http://www.uni-ca.com.cn。

本 CP 发布在中网威信全球数字认证中心中心的网站上，供相关方下载、查阅。

中网威信全球数字认证中心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全球数字认证中心的目录服务器获取证书的信息和吊销证书列表。同时，中网威信全球数字认证中心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. CP、CP 以及相关业务规则在完成 1.5.4 所述的批准流程后的 15 个工作日内发布到中网威信全球数字认证中心网站上，并确保 7X24 小时可访

问。中网威信全球数字认证中心也会对其商业行为进行审计（见 8.1 章节）。

2. 证书的发布：在证书签发时，中网威信全球数字认证中心将自动将该证书公布。
3. 中网威信全球数字认证中心的 CRL 每 24 小时发布一次。
4. 中网威信全球数字认证中心的 CA 证书的撤销列表（ARL）每 7 天发布一次。
5. 订户有特殊要求的，将根据订户的需求，适当更新 CRL 的发布频率。
6. 中网威信全球数字认证中心签发的 CRL 信息，根据需要，也可以人工方式实时发布。

2.3 高风险识别库

中网 CA 将维护内部数据记录，用于记录所有曾经因为网络钓鱼可疑或可能被其他欺诈手段利用的原因被吊销或拒绝申请的证书信息。这些证书的申请机构在今后的身份验证中标识为可能的高风险证书申请。

在进行身份验证时，中网 CA 将申请机构与一些高风险机构名单进行对比，主要是指最有可能成为网络钓鱼或其他身份欺诈目标的组织机构，将其标记为“高风险申请者”，确保证书在签发前申请机构的身份得到充分验证。

这些组织名单有：

1、 参考国际反钓鱼工作组（APWG）及中国反钓鱼联盟（APAC）公布的钓鱼目标名单；

2、 中网 CA 将因为可能遭到网络钓鱼或其他身份欺诈攻击而吊销其 OV SSL 证书、EV SSL 证书，中网 CA 将把这些被拒绝的申请者的组织机构标记为“高风险申请者”，并且作为今后识别高风险机构的依据。

中网 CA 将拒绝处于高风险信息库中的证书申请。

2.4 信息库访问控制

对于公开发布的 CP、证书、CRL 等公开信息，中网威信全球数字认证中心允许公众自行通过网站或目录服务器进行查询和访问。

中网威信全球数字认证中心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

数字证书中的主体的 X.501 DN 是 C=CN 命名空间下的 X.501 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。应当符合法律法规等相关规定的要求。

3.1.3 订户的匿名或伪名

中网威信全球数字认证中心不允许订户(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 ITU-T X.520 甄别名命名规则解释。

3.1.5 名称的唯一性

中网威信全球数字认证中心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，其中的例外是一个订户可以拥有两张或以上的使用同一主体甄别的证书。

中网威信全球数字认证中心将审核订户提交的机构中英文名称、域名等的唯

一性。

3.1.6 命名纠纷的处理

中网威信全球数字认证中心不承担解决证书申请中关于命名纠纷的责任，发生纠纷时，订户应自行向司法机构或主管部门提出解决申请。

通常，当申请人提交的名称有纠纷时，中网威信全球数字认证中心按照先申请先得到的方式进行处理。

3.1.7 商标的承认、鉴别和角色

中网威信全球数字认证中心尊重订户的商标等知识产权。但没有任何、验证商标等知识产权的义务。

订户不得在其证书申请中使用侵犯他人知识产权的名称。中网威信全球数字认证中心不会去决定证书申请人在申请证书时是否包含着知识产权信息，也不承担任何关于调解、仲裁或以其他方式解决域名、商标等知识产权纠纷的责任。中网威信全球数字认证中心有权不因此类纠纷拒绝或暂停任何证书申请。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

中网威信全球数字认证中心使用经数字签名的 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。如果中网威信全球数字认证中心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。

中网威信全球数字认证中心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 订户身份的鉴别

订户在申请中网 CA 全球认证体系签发的证书前应指定并书面授权证书的代

理人，提供有效身份证明文件、证书申请文件，并接受证书申请的有关条款，同意承担相应的责任。

中网 CA 接受订户的证书申请后，应对订户身份的真实性进行审核，并按照双方的约定妥善保存订户申请材料。

中网 CA 对订户身份的鉴别过程如下：

客户经理收集订户的申请材料，审核员对订户身份以及材料进行审核。RA 操作员录入订户申请信息，系统审核员审核操作员录入信息并协助订户下载证书。

详见 CPS3.2.2 章节。

3.2.3 没有验证的订户信息

中网 CA 签发的证书信息没有未经过验证的信息。

3.2.4 授权确认

当机构订户授权经办人办理证书业务时，应当进行如下验证：

1、 通过第三方身份证明服务或数据库提交政府主管部门签发的文件等方式确认该机构存在；

2、 通过电话、有回执的邮政信函、雇佣证明或任等同方式来验证该人属于上述机构以及其代表行为为该机构授权。授权文件要有公司公章以及授权有效期。

3.2.5 互操作准则

对于申请中网 CA 全球认证体系下的证书，中网 CA 承担订户身份的鉴别职能，暂不委托其他机构行使此职责。

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

随着密钥使用时间的增加，其可能遗失或遭破解的风险随之增加。订户应定期更新密钥，以确保密钥的安全性。

证书到期前，订户应重新按照 3.2 关于证书私钥拥有方法的规定提交证书申请。

3.3.2 吊销后密钥更新的标识与鉴别

吊销后的证书必须重新生成新的公私钥对并按照 3.2 的规定申请新的证书。

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 CP 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

任何实体需要使用中网 CA 全球求认证体系下签发的证书时，均可向中网 CA 提出证书申请。

4.1.2 注册过程与责任

申请者应事先了解订户协议、CP 及本 CP 等文件约定的事项，特别是其中关于证书适用范围、权利、义务和担保的相关内容。

申请者应向中网威信全球数字认证中心递交证书申请表及相应证明文件，此行为即意味着申请者已经了解和接受订户协议。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

1、 中网 CA 处理证书申请至少需要设置三个可信角色：信息收集、信息验证、签发证书。其中信息收集、信息验证可以由同一人完成，但是签发人员必须与信息收集、信息验证职责分开。

2、 对于证书申请的处理，签发证书人员需要对申请机构信息做最终审核

1、 对所有用以验证申请机构证书申请的信息和文件进行复核，查找冲突的信息或是需要进一步验证的信息；

2、 如复核人提出的问题确实需要得到进一步的验证，中网 CA 必须从申请机构、协议签署人、申请审批人或其他合格的独立信息来源取得进一步验证的资料或证据；

3、 中网 CA 必须保证已收集的与证书申请相关的信息和资料足以确保签发的证书不含中网 CA 已知或应发现的错误信息，否则中网 CA 将会拒绝证书的申请并同时申请机构；

4、 如果部分或所有身份验证资料内容使用的语言不是中网 CA 的官方语言，那么中网 CA 将会进行经过适当的培训、具备足够的经验和判断能力的人员完成最终的交叉审核以及尽职调查。

具体的鉴别流程参见第 3.2.节以及 2.3 完成初始身份确认。

4.2.2 证书申请批准和拒绝

中网威信全球数字认证中心授权的注册机构（具体执行操作的业务受理点）根据本 CP 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 CP 所规定的身份鉴别流程且鉴证结果为合格，中网威信全球数字认证中心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，中网威信全球数字认证中心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 CA 将在合理的时间内完成证书申请处理，具体时间在证书相应 CPS 中规定。

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

中网威信全球数字认证中心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全球数字认证中心系统，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. 其它中网威信全球数字认证中心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

中网威信全球数字认证中心在签发完证书后，就将证书发布到数据库和目录服务器中。中网威信全球数字认证中心采用主、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全球数字认证中心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全球数字认证中心所签发的证书后，均视为已经同意遵守与中网威信全球数字认证中心、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；

其它需要更新证书的原因

中网威信全球数字认证中心不提供 SSL 证书更新服务。

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全球数字认证中心签发的个人、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；

其他中网威信全球数字认证中心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

中网威信全球数字认证中心在签发更新证书后，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

证书密钥更新是指在不改变证书中包含的信息的情况下，由订户生成新的秘钥对向中网威信全球数字认证中心申请签发一张新证书。

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 订户证书吊销的情形

1、 订户书面申请吊销数字证书；
2、 订户通知中网 CA 最初的证书申请没有经过授权；
3、 订户相信或怀疑密钥泄露或遭受攻击，存放证书的服务器损坏或被锁定等情形；或者 CA 有证据表明订户证书私钥泄露的情形；
4、 当中网 CA 有证据表明订户将使用与行政法规定义为非法事项上，或者中网 CA 发现订户证书未恰当使用；
5、 当中网 CA 有证据表明订户未履行本 CP 或订户协议中约定的义务；或是订户证书本身不符合本 CP 的相关要求；
6、 当中网 CA 有证据表明订户已丧失证书中域名的使用权，或订户未能更新其域名使用权；
7、 中网 CA 获知通配符证书被用于验证具有欺诈误导性质的域名；
8、 中网 CA 取得了合理的证据表明或意识到订户证书中的重要信息内容已

经变更；

9、 中网 CA 正式签发时未能满足证书策略或证书标准中的要求和条件，或者证书有的任何信息不准确；

10、 中网 CA 认定证书中所显示的信息为不准确或具有误导性，或者订户申请证书时，提供的资料不真实；

11、 中网 CA 因为某些原因停止业务，并且没有安排其他的 CA 提供证书撤销服务；

12、 当中网 CA 从事电子认证业务的资格被吊销，中网 CA 除继续位置 CRL/OCSP 信息库的情况外，将吊销或终结所有已签发的证书；

13、 中网 CA 用于签发证书的 CA 证书私钥可能被泄露时，将根据应急预案吊销所有已签发的证书；

14、 中网CA取得了合理的证书材料表明或意识到订户已经被列在相关的黑名单中，或其经营地区被中网 CA 所在国家的监管机构禁止；

15、 证书的重要参数被国内外主要标准认为有重大风险时；

16、 法律、行政法规规定的其他情形。

4.9.2 中级证书吊销的情形

1、 中级 CA 书面申请吊销数字证书；

2、 中级 CA 通知中网 CA 最初的证书申请没有经过授权；

3、 中网 CA 获得证据表明中级证书被滥用；

4、 当中网 CA 有证据表明中级 CA 未履行本 CP 或订户协议中约定的义务；或是中级 CA 本身不符合本 CP 的相关要求；

5、 中级 CA 相信或怀疑密钥泄露或遭受攻击，存放证书的服务器损坏或被锁定等情形；或者中网 CA 有证据表明中级证书私钥泄露的情形

6、 中网 CA 认定中级证书中所显示的信息为不准确或具有误导性；

7、 中网 CA 因为某些原因停止业务，并且没有安排其他的 CA 提供证书撤销服务；

8、 当中网 CA 从事电子认证业务的资格被吊销，中网 CA 除继续位置 CRL/OCSP 信息库的情况外，将吊销或终结所有已签发的证书；

9、 中级证书中签发的策略在 CP 或 CP 中已经被删除；

10、 证书的重要参数被国内外主要标准认为有重大风险时。

4.9.3 请求证书吊销的实体

已经申请中网 CA 证书的订户可请求证书撤销。

同时，中网 CA 也可在 4.9.1 以及 4.9.2 所述的情形下主动吊销订户的证书。

4.9.4 吊销请求的流程

吊销分为主动吊销和被动吊销。主动吊销是指订户提出吊销申请，由中网 CA 审核通过后吊销证书的情形；被动吊销是指当中网 CA 确定订户违反证书使用规定、约定、或是订户主体已经消亡等情况发生时，采取吊销证书的手段已停止对该证书的证明。

4.9.4.1 主动吊销

订户申请吊销证书前应制定并书面授权证书吊销申请代表，提供有效的证明材料以及证书吊销申请文件，并接受证书吊销申请的有关条款，同意承担相应的责任。

中网 CA 7X24 小时接受订户证书的吊销申请，并处理订户证书吊销请求。订户可通过中网 CA 热线、中网 CA 在线服务等方式提出申请。

中网 CA 收到订户的吊销申请材料后，将查询订户需吊销的证书是否是中网 CA 发放的，证书是否还在有效期内，吊销里有是否属实，若均通过则对证书进行吊销。

4.9.4.2 被动吊销

当出现被动吊销的情形时，中网 CA 将以适当形式通知订户，告知拟吊销的证书内容、吊销原因、吊销操作时限等事项，在确认订户收到吊销通知无异议后予以吊销。

4.9.5 吊销请求宽限期

在主动吊销的情形下，订户一旦发现需要吊销证书，应及时向中网 CA 提出吊销请求。

在被动吊销的情形下，订户收到吊销通知后的 3 个工作日内可向中网 CA 提出申辩理由，中网 CA 将会对申辩理由进行评估，若确认理由正当则不对证书进行吊销；若订户在 3 个工作日内未回复或回复无异议则中网 CA 将对证书进行吊销。

4.9.6 电子认证服务机构处理吊销请求的时限

主动吊销的情况下，中网 CA 收到吊销请求并审核完成后，24 小时内吊销证书。

在被动吊销的情形下，订户收到吊销通知后的 3 个工作日内可向中网 CA 提出申辩理由，中网 CA 将会对申辩理由进行评估，若确认理由正当则不对证书进行吊销；若订户在 3 个工作日内未回复或回复无异议则中网 CA 将在 24 小时内对证书进行吊销。

4.9.7 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，确保是由中网威信全球数字认证中心发布并且签名。

4.9.8 CRL 发布频率

中网威信全球数字认证中心可采用定期的方式发布 CRL。订户 CRL 的频率

根据证书策略确定，一般为 24 小时内发布。中级证书的 CRL 一般为每 7 天发布一次。当然根据需要，也可以人工方式实时发布。

4.9.9 CRL 发布的最大滞后时间

CRL 发布的最长滞后时间为 24 小时。

4.9.10 在线状态查询的可用性

中网威信全球数字认证中心提供在线证书状态查询（OCSP）服务，订户可通过 OCSP 服务进行证书状态的实时查询。

4.9.11 在线状态查询要求

中网 CA 提供 OCSP 查询服务，服务 7X24 小时可用。

信赖方是否进行在线状态查询完全取决于信赖方的安全要求。对于安全保障要求高并且完全依赖证书进行身份认证的应用，信赖方在信赖一个证书前可通过证书状态查询系统检查该证书的状态。

中网 CA 的 OCSP 响应符合 RFC2560 标准。

客户通过 http 协议访问中网 CA 的 OCSP 服务，中网 CA 会对查询请求进行检查，检查的内容包括：

1、验证是否强制请求签名；

2、用 CA 证书验证签名是否通过；

3、验证证书是否生效或已经过期；

4、验证证书颁发者是否在信任证书列表内。

OCSP 响应包含如下表所述基本域和内容

域	值或者值的限制
状态	响应状态，包括成功、请求格式错误、系统内部错误、稍后重试、请求没有签名、或请求签名证书无授权，当状态未成功时包括以下几项。

版本	V1
签名算法	签发 OCSP 的算法。SHA1RSA、SHA256RSA。
颁发者	签发 OCSP 的实体。签发者公钥的数据摘要值和证书甄别名。
产生时间	OCSP 响应的产生时间。
证书状态列表	包括请求中所查询的证书状态列表。每个证书状态包含证书标识、证书状态以及证书废止信息。
证书标识	包括数据摘要算法、证书甄别名数据值、证书公钥数据摘要值和证书序列号。
证书状态	证书的最新状态，包括有效、吊销和未知
证书状态废止信息	当返回证书状态为废止时包含废止时间和废止原因

OCSP 的扩展信息与 RFC2560 一致。

中网 CA 的 OCSP 信息的更新频率不超过 4 小时，OCSP 服务响应时间不超过 10 秒，OCSP 服务响应信息最大有效期不超过 1 天。

4.9.12 吊销信息的其他发布形式

除了 CRL、OCSP 外，中网威信全球数字认证中心的 LDAP 提供 CRL 查询。

4.9.13 密钥损害的特别要求

无论是最终订户还是中网威信全球数字认证中心及其注册机构，发现证书密钥受到安全损害时应立即吊销证书。

4.9.14 证书挂起的情形

中网威信全球数字认证中心不提供证书挂起服务。

4.9.15 请求证书挂起的实体

无。

4.9.16 挂起请求的流程

无。

4.9.17 挂起的期限限制

无。

4.10 证书状态服务

4.10.1 操作特征

证书状态可以通过中网 CA 提供的 OCSP 以及 CRL 获取（在证书到期之前）。上述方式的证书状态查询服务对查询请求有合理的响应时间和并发处理能力。

4.10.2 服务可用性

中网 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。

中网 CA 在内部对高优先级的证书问题报告进行内部响应，并在适当的情况下向执法部门提出这样的投诉，并撤销该投诉的相关证书。

证书状态服务的可用性符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南第 23 部分的要求。

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全球数字认证中心的服务，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。中网威信全球数字认证中心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

中网威信全球数字认证中心不托管任何 SSL 证书订户的私钥，因此也不提供密钥恢复服务。

4.12.2 会话密钥的封装与恢复的策略与行为

不做规定。

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

中网威信全球数字认证中心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）。所有机房严格按照中华人民共和国密码管理局《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，只有经过中网威信全球数字认证中心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

为了保证中网威信全球数字认证中心物理设施的安全，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；
10. 门禁系统自带有蓄电池，至少能提供 8 小时的电力。
11. 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；
12. 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. 机房采用三台机房专用空调机，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

中网威信全球数字认证中心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

中网威信全球数字认证中心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，中网威信全球数字认证中心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

中网威信全球数字认证中心采取安全的异地备份方式，保持对关键系统数据或任何其它敏感信息（包括审计数据）的备份：

- 设置有异地备份机房，并配备相应设备，当日常营运的系统因外力因素无法正常运作时，备份系统可提供持续营运的能力
- CA运营所需的相关数据，经备份后储存于具备温湿度控制、防磁、防静电干扰，且具有视频监控和物理访问控制措施的备份环境中
- 建立灾难恢复计划，每年4月份进行灾备演练，以保持备份设施的可用性。

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 CA 制定了规范的策略，严格控制任务和职责的分割，对于敏感的操作，例如访问或管理 CA 的加密设备以及其密钥，需要 3 个可信角色。

其他操作，例如发放证书，需要两个可信角色。

中网 CA 对于人员有明确的分工，贯彻互相牵制、互相监督的安全机制。

5.2.3 每个角色的识别与鉴别

所有中网威信全球数字认证中心的在职人员，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。中网威信全球数字认证中心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，即中网威信全球数字认证中心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全球数字认证中心签定保密协议。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。中网威信全球数字认证中心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

中网威信全球数字认证中心对运营人员按照其岗位和角色安排不同的培训。培训有：内部规章制度、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、CP 等。

中网 CA 处理证书业务相关的员工必须接受下列培训：

1、 负责信息身份验证的员工（认证专员）提供技能培训。包括基础 PKI 知识、审核与验证制度和流程、对验证过程的主要威胁（如网络钓鱼以及起亚社会工程学策略）以及 EV 证书标准；

2、 保留人员培训记录，并且确保认证专员能够胜任身份信息验证工作的技术要求；

3、 认证专员必须按照不同的技术水平等级授予不同的证书发放权限，技术

水平分级标准应与培训内容以及业绩考核标准一致；

4、 确保为认证专员分配签发证书权限前，不同技术等级的认证专员都有足够的胜任能力；

5、 要求所有的认证专员通过关于证书标准中身份验证要求的 CA 内部考试。

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 中网威信全球数字认证中心组织的培训一次。

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，中网威信全球数字认证中心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

对不属于中网威信全球数字认证中心内部的工作人员，但从事 中网威信全

球数字认证中心有关业务的人员等独立签约者(如注册机构的工作人员)，中网威信全球数字认证中心的统一要求如下：

1. 人员档案进行备案管理；
2. 具有相关业务的工作经验；
3. 符合 5.3.3 的要求。

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. 中网威信全球数字认证中心技术白皮书；
2. 各级用户使用手册；
3. 中网威信全球数字认证中心管理制度；
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

中网威信全球数字认证中心的 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。包括但不限于：

1. 证书订户服务申请和撤销的信息，如申请表、协议、身份资料和其他相关信息等；
2. 服务器密码机生命周期管理；
3. CA 密钥的生成、存储、备份、恢复、归档和销毁等；
4. 认证系统各类服务系统密钥对的生成、内置、变更等成功和失败的纪录；
5. 认证系统日常运作产生的日志记录文件；

6. CRL 的操作记录；
7. 进出中网威信全球数字认证中心控制区域内的表格、身份识别卡进出敏感区域的纪录、机房工作日志、系统日常维护记录、监控录像等；
8. 系统软硬件设备上线、更换、下线等的纪录；
9. 认证机构、注册机构和受理点之间的协议、规范和相关工作记录；
10. 系统安全事件，包括：成功或不成功访问 CA 系统的活动，对于 CA 系统网络的非授权访问及访问企图，对于系统文件的非授权的访问及访问企图，安全、敏感的文件或记录的读、写或删除，系统崩溃，硬件故障和其他异常；
11. 防火墙和入侵检测系统记录的安全事件。

中网威信全球数字认证中心记录其它与 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

中网威信全球数字认证中心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

中网威信全球数字认证中心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

中网威信全球数字认证中心执行严格的访问控制管理，确保只有中网威信全球数字认证中心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

中网威信全球数字认证中心保证所有的审查记录和审查总结都按照中网威信全球数字认证中心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. 其他中网威信全球数字认证中心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，中网威信全球数字认证中心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

中网威信全球数字认证中心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。

中网威信全球数字认证中心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

中网 CA 每年进行一次风险评估，内容如下：

1、 标识可预见的内部和外部威胁，可能导致未经授权的访问、公开、误用、更改或销毁任何证书数据或证书管理流程；
2、 评估这些威胁的可能性和潜在危害，考虑到证书数据和证书管理过程的敏感性；
3、 评估在应对这些威胁时所采取的政策、程序、信息系统、技术和其他安

条件。

5.5 记录归档

5.5.1 归档记录的类型

中网威信全球数字认证中心会对 CA 的数据库定期存档，间隔时间由中网威信全球数字认证中心自行决定，存档的内容包括中网威信全球数字认证中心发行的证书和 CRL、审查数据记录、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

中网威信全球数字认证中心中的存档期限规定为证书失效后七年。

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。

中网威信全球数字认证中心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。

中网威信全球数字认证中心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全球数字认证中心的主要存储库，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。

中网威信全球数字认证中心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

中网威信全球数字认证中心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。中网威信全球数字认证中心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

为了降低 CA 密钥被破解的风险，中网威信全球数字认证中心定期对 CA 证书电子认证服务机构的密钥更替是指当中网威信全球数字认证中心根证书到期而需要更换根密钥对时所采取的措施。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

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，中网威信全球数字认证中心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全球数字认证中心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，中网威信全球数字认证中心需要终止运营时，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。

中网威信全球数字认证中心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全球数字认证中心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。

中网威信全球数字认证中心采用以下措施终止业务：

1. 起草中网威信全球数字认证中心终止业务声明；

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. 管理中网威信全球数字认证中心系统管理员和安全管理员；
7. 通知与中网威信全球数字认证中心终止运营相关的实体。
8. 根据中网威信全球数字认证中心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

本章节参见相关 CPS 内容。

7. 证书、证书吊销列表和在线证书状态协议

7.1 证书

中网威信全球数字认证中心签发的证书均符合 X.509 V3 证书格式。均按照 RFC5280 设置，符合 CA/Browser 的当前版本要求。证书的最基本字段与内容见下表。

字段	内容
Serial Number	中网威信全球数字认证中心自动生成并在中网威信全球数字认证中心体系内唯一的值。
Signature Algorithm	证书签名算法的对象标识，见本 CSP7.1.3
Issuer DN	证书的颁发者 DN，见 CSP7.1.4
Valid From	证书有效起始时间，符合 RFC 5280。
Valid To	证书失效时间，符合 RFC 5280。
Subject DN	证书的主题 DN 见 CSP7.1.4
Subject Public Key	证书主题公钥，编码格式符合 RFC 5280
Signature	上级 CA 对证书信息的签名值，编码格式符合 RFC 5280

7.1.1 证书版本号

X.509 V3。

7.1.2 证书扩展项

中网威信数字证书认证中心签发的证书，其证书扩展项遵循 IETF RFC 5280 标准要求。

7.1.2.1 个人证书扩展项

1、 密钥用法（Key Usage）

按照 RFC5280 进行填充。该项的 criticality 域设置为 true。

2、 证书策略（Certificate Policies Extension）

按照 RFC5280 进行填充，该项的 criticality 域设置为 false。

3、 基本约束（Basic Constraints）

Path Length Constraint =None，该项的 criticality 域设置为 false。

4、 扩展密钥用法（Extended Key Usage）

如果有将按照 RFC5280 进行填，该项的 criticality 域设置为 false。

5、 CRL 发布点（CRL Distribution Points）

所有个人证书都包含 CRL 发布点，该发布点包含了一个 URL，用于获得 CRL 文件，该项的 criticality 域设置为 false。

6、 颁发者机构密钥标识符（Authority Key Identifier）

颁发者机构密钥标识符由上级 CA 证书公钥的 160 位 SHA1 散列组成。该项的 criticality 域设置为 false。

7、 主体密钥标识符（Subject Key Identifier）

主体密钥标识符由订户证书公钥的 160 位 SHA1 散列组成。该项的 criticality 域设置为 false 非关键扩展。

7.1.2.2 企（事）业证书扩展项

1、 密钥用法（Key Usage）

按照 RFC5280 进行填充。该项的 criticality 域设置为 true。

2、 证书策略（Certificate Policies Extension）

按照 RFC5280 进行填充。该项的 criticality 域设置为 false。

3、 基本约束（Basic Constraints）

Path Length Constraint =None，该项的 criticality 域设置为 false。

4、 扩展密钥用法（Extended Key Usage）

如果有将按照 RFC5280 进行填，该项的 criticality 域设置为 false。

5、 CRL 发布点（CRL Distribution Points）

所有企业证书都包含 CRL 发布点，该发布点包含了一个 URL，用于获得 CRL 文件，该项的 criticality 域设置为 false。

6、 颁发者机构密钥标识符（Authority Key Identifier）

颁发者机构密钥标识符由上级 CA 证书公钥的 160 位 SHA1 散列组成。内容为 45 68 a5 f7 a2 59 e8 a4 07 4c 99 59 06 96 63 96 ae 86 2c 25。该项的 criticality 域设置为 false。

7、 主体密钥标识符（Subject Key Identifier）

主体密钥标识符由订户证书公钥的 160 位 SHA1 散列组成。该项的 criticality 域设置为 false 非关键扩展。

7.1.2.3 OV SSL 服务器证书扩展项

1、 密钥用法（Key Usage）

按照 RFC5280 进行填充，内容为 Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment。该项的 criticality 域设置为 true。

2、 证书策略（Certificate Policies Extension）

按照 RFC5280 进行填充。该项的 criticality 域设置为 false。

3、 主题备用名称（Subject Alternative Names）

包含一个或多个可替换名（可使用多种名称形式中的任意一个）供实体使用，CA 把该实体与认证的公开密钥绑定在一起。该项按照 RFC5280 进行填充，OV SSL 证书中该项的内容为一个或多个 DNS NAME。该项的 criticality 域设置为 false。

4、 基本约束（Basic Constraints）

Path Length Constraint =None，该项的 criticality 域设置为 false。

5、 扩展密钥用法（Extended Key Usage）

如果有将按照 RFC5280 进行填，内容为客户端身份验证 (1.3.6.1.5.5.7.3.2)，服务器身份验证 (1.3.6.1.5.5.7.3.1)。该项的 criticality 域设置为 false。

6、 CRL 发布点（CRL Distribution Points）

所有 OV SSL 证书都包含 CRL 发布点，该发布点包含了一个 URL，用于获得 CRL 文件，该项的 criticality 域设置为 false。

7、 颁发者机构密钥标识符（Authority Key Identifier）

颁发者机构密钥标识符由上级 CA 证书公钥的 160 位 SHA1 散列组成。该项的 criticality 域设置为 false。

8、 主体密钥标识符（Subject Key Identifier）

主体密钥标识符由订户证书公钥的 160 位 SHA1 散列组成。该项的 criticality 域设置为 false 非关键扩展。

7.1.2.4 EV SSL 服务器证书扩展项

1、 密钥用法（Key Usage）

按照 RFC5280 进行填充，内容为 Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment。该项的 criticality 域设置为 true。

2、 证书策略（Certificate Policies Extension）

按照 RFC5280 进行填充，该项的 criticality 域设置为 false。

3、 主题备用名称（Subject Alternative Names）

包含一个或多个可替换名（可使用多种名称形式中的任意一个）供实体使用，CA 把该实体与认证的公开密钥绑定在一起。该项按照 RFC5280 进行填充，OV SSL 证书中该项的内容为一个或多个 DNS NAME。该项的 criticality 域设置为 false。

4、 基本约束（Basic Constraints）

Path Length Constraint =None，该项的 criticality 域设置为 false。

5、 扩展密钥用法（Extended Key Usage）

如果有将按照 RFC5280 进行填，内容为客户端身份验证 (1.3.6.1.5.5.7.3.2)，服务器身份验证 (1.3.6.1.5.5.7.3.1)。该项的 criticality 域设置为 false。

6、 CRL 发布点（CRL Distribution Points）

所有 EV SLL 证书都包含 CRL 发布点，该发布点包含了一个 URL，用于获得 CRL 文件，该项的 criticality 域设置为 false。

7、 颁发者机构密钥标识符（Authority Key Identifier）

颁发者机构密钥标识符由上级 CA 证书公钥的 160 位 SHA1 散列组成。该项的 criticality 域设置为 false。

8、 主体密钥标识符（Subject Key Identifier）

主体密钥标识符由订户证书公钥的 160 位 SHA1 散列组成。该项的 criticality 域设置为 false 非关键扩展。

7.1.2.5 CHINA UNICOM ENTERPRISE CA 证书扩展项

1、 密钥用法（Key Usage）

按照 RFC5280 进行填充，内容为 Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing。该项的 criticality 域设置为 true。

2、 证书策略（Certificate Policies Extension）

按照 RFC5280 进行填充。该项的 criticality 域设置为 false。

3、 基本约束（Basic Constraints）

Path Length Constraint=0，该项的 criticality 域设置为 true。

4、 扩展密钥用法（Extended Key Usage）

如果有将按照RFC5280进行填，内容为客户端身份验证 (1.3.6.1.5.5.7.3.2)，代码签名 (1.3.6.1.5.5.7.3.3)，安全电子邮件 (1.3.6.1.5.5.7.3.4)，OCSP 签名 (1.3.6.1.5.5.7.3.9)。该项的criticality域设置为false。

5、 CRL 发布点（CRL Distribution Points）

该发布点包含了一个 URL，URL 地址为 http://61.138.142.22/download/arl2.crl，用于获得 CRL 文件，该项的 criticality 域设置为 false。

6、 颁发者机构密钥标识符（Authority Key Identifier）

颁发者机构密钥标识符由根CA证书公钥的160位SHA1散列组成。内容为dc 20 31 4a dd 67 a1 53 cd 90 21 80 d1 b9 54 0e 91 d4 60 e3。该项的criticality域设置为false。

7、 主体密钥标识符（Subject Key Identifier）

主体密钥标识符由中级CA证书公钥的160位SHA1散列组成。内容为45 68 a5 f7 a2 59 e8 a4 07 4c 99 59 06 96 63 96 ae 86 2c 25
。该项的 criticality 域设置为 false 非关键扩展。

8、 颁发者机构访问（Authority Info Access）

颁发者机构访问为联机证书状态协议，内容为 http://vra.uni-ca.com.cn:7182/ocsp/

7.1.2.6 CHINA UNICOM EV SSL CA 证书扩展项

1、 密钥用法（Key Usage）

按照 RFC5280 进行填充，内容为 Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing。该项的 criticality 域设置为 true。

2、 证书策略（Certificate Policies Extension）

按照 RFC5280 进行填充。该项的 criticality 域设置为 false。

3、 基本约束（Basic Constraints）

Path Length Constraint=0，该项的 criticality 域设置为 true。

4、 CRL 发布点（CRL Distribution Points）

该发布点包含了一个 URL，URL 地址为 http://61.138.142.22/download/arl2.crl，用于获得 CRL 文件，该项的 criticality 域设置为 false。

5、 颁发者机构密钥标识符（Authority Key Identifier）

颁发者机构密钥标识符由根CA证书公钥的160位SHA1散列组成。内容为dc 20 31 4a dd 67 a1 53 cd 90 21 80 d1 b9 54 0e 91 d4 60 e3。该项的criticality域设置为false。

6、 主体密钥标识符（Subject Key Identifier）

主体密钥标识符由中级CA证书公钥的160位SHA1散列组成。内容为26 47 34

08 16 5a 44 5c 07 f5 11 0d a1 66 e7 32 19 2b 0a 5f。该项的criticality域设置为false非关键扩展。

7、 颁发者机构访问（Authority Info Access）

颁发者机构访问为联机证书状态协议，内容为
http://vra.uni-ca.com.cn:7182/ocsp/

7.1.2.7 CHINA UNICOM INDIVIDUAL CA 证书扩展项

1、 密钥用法（Key Usage）

按照 RFC5280 进行填充，内容为 Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing。该项的 criticality 域设置为 true。

2、 证书策略（Certificate Policies Extension）

按照 RFC5280 进行填充。该项的 criticality 域设置为 false。

3、 基本约束（Basic Constraints）

Path Length Constraint=0，该项的 criticality 域设置为 true。

4、 扩展密钥用法（Extended Key Usage）

如果有将按照RFC5280进行填，内容为客户端身份验证 (1.3.6.1.5.5.7.3.2)，代码签名 (1.3.6.1.5.5.7.3.3)，安全电子邮件 (1.3.6.1.5.5.7.3.4)，OCSP 签名 (1.3.6.1.5.5.7.3.9)。该项的criticality域设置为false。

5、 CRL 发布点（CRL Distribution Points）

所有企业证书都包含 CRL 发布点，该发布点包含了一个 URL，URL 地址为 http://61.138.142.22/download/arl2.crl，用于获得 CRL 文件，该项的 criticality 域设置为 false。

6、 颁发者机构密钥标识符（Authority Key Identifier）

颁发者机构密钥标识符由根CA证书公钥的160位SHA1散列组成。内容为dc 20 31 4a dd 67 a1 53 cd 90 21 80 d1 b9 54 0e 91 d4 60 e3。该项的criticality域设置为false。

7、 主体密钥标识符（Subject Key Identifier）

主体密钥标识符由中级CA证书公钥的160位SHA1散列组成。内容为1e 16 f9 8f 9c 3c 32 82 6f b3 09 58 0a 12 84 97 61 ec 98 40
。该项的 criticality 域设置为 false 非关键扩展。

8、 颁发者机构访问（Authority Info Access）

颁发者机构访问为联机证书状态协议，内容为
http://vra.uni-ca.com.cn:7182/ocsp/

7.1.2.8 CHINA UNICOM SSL CA 证书扩展项

1、 密钥用法（Key Usage）

按照 RFC5280 进行填充，内容为 Digital Signature, Certificate Signing, Off-line

CRL Signing, CRL Signing。该项的 criticality 域设置为 true。

2、 证书策略（Certificate Policies Extension）

按照 RFC5280 进行填充。该项的 criticality 域设置为 false。

3、 基本约束（Basic Constraints）

Path Length Constraint=0，该项的 criticality 域设置为 true。

4、 扩展密钥用法（Extended Key Usage）

如果有将按照RFC5280进行填，内容为客户端身份验证 (1.3.6.1.5.5.7.3.2)，服务器身份验证 (1.3.6.1.5.5.7.3.1)。该项的criticality域设置为false。

5、 CRL 发布点（CRL Distribution Points）

该发布点包含了一个 URL，URL 地址为 http://61.138.142.22/download/arl2.crl，用于获得 CRL 文件，该项的 criticality 域设置为 false。

6、 颁发者机构密钥标识符（Authority Key Identifier）

颁发者机构密钥标识符由根CA证书公钥的160位SHA1散列组成。内容为dc 20 31 4a dd 67 a1 53 cd 90 21 80 d1 b9 54 0e 91 d4 60 e3。该项的criticality域设置为false。

7、 主体密钥标识符（Subject Key Identifier）

主体密钥标识符由中级CA证书公钥的160位SHA1散列组成。内容为41 53 b9 92 2f 0e 35 a3 44 25 99 a7 0a 5f 5e c0 38 0d 30 01。该项的criticality域设置为false 非关键扩展。

8、 颁发者机构访问（Authority Info Access）

颁发者机构访问为联机证书状态协议，内容为 http://vra.uni-ca.com.cn:7182/ocsp/

7.1.2.9 CHINA UNICOM GLOBAL ROOT CA 证书扩展项

1、 密钥用法（Key Usage）

按照 RFC5280 进行填充，内容为 Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing。该项的 criticality 域设置为 true。

2、 证书策略（Certificate Policies Extension）

按照 RFC5280 进行填充。该项的 criticality 域设置为 false。

3、 基本约束（Basic Constraints）

Path Length Constraint=None，该项的 criticality 域设置为 true。

4、 颁发者机构密钥标识符（Authority Key Identifier）

颁发者机构密钥标识符由根CA证书公钥的160位SHA1散列组成。内容为dc 20 31 4a dd 67 a1 53 cd 90 21 80 d1 b9 54 0e 91 d4 60 e3。该项的criticality域设置为false。

5、 主体密钥标识符（Subject Key Identifier）

主体密钥标识符由根CA证书公钥的160位SHA1散列组成。内容为4 dc 20 31 4a dd 67 a1 53 cd 90 21 80 d1 b9 54 0e 91 d4 60 e3。该项的criticality域设置为false非关键扩展。

7.1.3 算法对象标识符

中网CA全球认证体系证书（包括根证书，中间证书以及订户证书）的算法对象标识符（OID）如下：

- sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

7.1.4 名称形式

中网 CA 签发的证书（包括根证书、中间证书以及订户证书）的 DN 都采用 X.500 （Distinguished Name；DN）命名方式，遵循 RFC5280 相关规定。

7.1.5 证书颁发者

- 个人普通证书

CHINA UNICOM INDIVIDUAL CA

- 企业普通证书

CHINA UNICOM ENTERPRISE CA

- OV SSL 证书

CHINA UNICOM SSL CA

- EV SSL 证书

CHINA UNICOM EV SSL CA

- 个人中级证书

CHINA UNICOM GLOBAL ROOT CA

- 企业中级证书

CHINA UNICOM GLOBAL ROOT CA

- OV SSL 中级证书

CHINA UNICOM GLOBAL ROOT CA

- EV SSL 中级证书

CHINA UNICOM GLOBAL ROOT CA

- 根证书

CHINA UNICOM GLOBAL ROOT CA

7.1.6 证书主题

中网 CA 签发证书的甄别名符合 X.500 关于甄别名的规定。中网 CA 保证签发的每一个证书的甄别名都是唯一的。

DN 项中包含的国家、省市级名称必须使用权威部门发布的标准名称。（如 SO country code）。

7.1.6.1 个人证书 DN 要求

个人证书的 DN 项可以包含以下 7 部分。

1、 CN 部分：个人订户的真实名称；

2、 OU 部分：可选部分，可以表示为个人订户的部门名称；

3、 O 部分：可选部分，可以表示为个人订户的组织名称；

4、 L 部分：必选部分，可以表示为个人订户所在的市；

5、 S 部分：必选部分，可以表示为个人订户所在的省；

6、 C 部分：必选部分，可以表示为个人订户所在的国家货地租的英文简称，全部大写，如中国订户标识为 C=CN。

对于个人安全邮件证书，必须包含 E 项，且 CN 部分必须是订户的真实名称。

7.1.6.2 企（事）业证书 DN 要求

企（事）业证书的 DN 项可以包含以下 6 部分。

1、 CN 部分：订户的真实名称；

2、 L 部分：必选部分，可以表示为营业所在的市；

3、 S 部分：必选部分，可以表示为营业所在的省；

4、 C 部分：必选部分，可以表示为营业所在的国家货地租的英文简称，全

部大写，如中国订户标识为 C=CN。

7.1.6.3 OV SSL 证书 DN 要求

OV SSL 证书的 DN 项必须包含以下 6 部分。

1、 CN 部分：必选部分，为域名或外网 IP；

2、 OU 部分：必选部分，可以表示为实体的部门名称；

3、 O 部分：必选部分，可以表示为实体的组织名称；

4、 L 部分：必选部分，可以表示为营业所在的市；

5、 S 部分：必选部分，可以表示为营业所在的省；

6、 C 部分：必选部分，可以表示为营业所在的国家货地租的英文简称，全部大写，如中国订户标识为 C=CN。

7.1.6.4 EV SSL 证书 DN 要求

EV SSL 证书的 DN 必须包含以下 6 部分。

1、 CN 部分：必选部分，为域名；

2、 OU 部分：必选部分，可以表示为实体的部门名称；

3、 O 部分：必选部分，可以表示为实体的组织名称；

4、 L 部分：必选部分，可以表示为营业所在的市；

5、 S 部分：必选部分，可以表示为营业所在的省；

6、 C 部分：必选部分，可以表示为营业所在的国家货地租的英文简称，全部大写，如中国订户标识为 C=CN。

7.1.6.5 CHINA UNICOM ENTERPRISE CA

1、 CN 部分：CHINA UNICOM ENTERPRISE CA；

2、 OU 部分：CUCA；

3、 O 部分：CU；

4、 L 部分：CHANGCHUN；

5、 S 部分：JILIN；

6、 C 部分：CN。

7.1.6.6 CHINA UNICOM EV SSL CA

1、 CN 部分：CHINA UNICOM EV SSL CA；

2、 OU 部分：CUCA；

3、 O 部分：CU；

4、 L 部分：CHANGCHUN；

5、 S 部分：JILIN；

6、 C 部分：CN。

7.1.6.7 CHINA UNICOM SSL CA

1、 CN 部分：CHINA UNICOM EV SSL CA；

2、 OU 部分：CUCA；

3、 O 部分：CU；

4、 L 部分：CHANGCHUN；

5、 S 部分：JILIN；

6、 C 部分：CN。

7.1.6.8 CHINA UNICOM INDIVIDUAL CA

1、 CN 部分：CHINA UNICOM EV INDIVIDUAL CA；

2、 OU 部分：CUCA；

3、 O 部分：CU；

4、 L 部分：CHANGCHUN；

5、 S 部分：JILIN；

6、 C 部分：CN。

7.1.6.9 CHINA UNICOM GLOBAL ROOT CA

1、 CN 部分：CHINA UNICOM GLOBAL ROOT CA；

2、 OU 部分：CUCA；

3、 O 部分：CU；

4、 L 部分：CHANGCHUN；

5、 S 部分：JILIN；

6、 C 部分：CN。

7.1.7 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，中网威信全球数字认证中心签发的其他证书中的通用名不能使用假名、伪名。

7.1.8 证书策略对象标识符

中网威信全球数字认证中心签发的证书应包含策略标识符。证书策略标识符包含一个证书策略对象标识符OID和URL地址。订户证书的证书策略对象标识符见1.2，中级证书的证书策略对象标识符是所有策略，根证书没有证书策略对象标识符。订户证书、中级证书策略表述URL为 http://www.cacnc.com.cn/download3.htm。

7.1.9 保留证书策略标识符

中网 CA 保留的证书策略标识符为 2.23.140.1.2.2 那么证书主题中必须包含组织名称、省市、国家信息。

7.1.10 策略约束

无规定。

7.2 证书吊销列表

中网威信全球数字认证中心定期签发 CRL（证书废除列表），供订户查询使用。

7.2.1 版本号

X.509：V2。

7.2.2 CRL 和 CRL 条目扩展项

CRL 符合 RFC5280 要求。列表包含最基本的字段和内容中指定下面的表：

字段	内容
Version	参考 7.2.1 章节
Signature Algorithm	用于对 CRL 进行签名的算法。参考 RFC3279
Issure	签发 CRL 的实体，CRL 的颁发者。
Effective Date	CRL 文件的发布时间
Next Update	CRL 的下一步发布时间。CRL 的发布频率参考 4.9.7.
Revoked Certificates	插销的证书清单。包括证书序列号以及撤销日期，撤销原因。

CRL 基本字段

7.3 在线证书状态协议

中网威信全球数字认证中心为证书用户提供 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

此章节与 CPS 内容相同。

9. 法律责任和其他业务条款

9.1 费用

此章节与 CPS 内容相同。

9.2 财务责任

此章节与 CPS 内容相同。

9.3 业务信息保密

此章节与 CPS 内容相同。

9.4 个人隐私保密

此章节与 CPS 内容相同。

9.5 陈述与担保

9.5.1 电子认证服务机构的陈述与担保

中网威信全球数字认证中心在提供电子认证服务活动过程中的承诺如下：

1. 中网威信全球数字认证中心遵守《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. 中网威信全球数字认证中心保证使用的系统及密码符合中华人民共和国政策与标准，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中华人民共和国相关规定。
3. 除非已通过中网威信全球数字认证中心证书库发出了中网威信全球数字认证中心的私钥被破坏或被盗的通知，中网威信全球数字认证中心保证其私钥是安全的。
4. 中网威信全球数字认证中心签发给订户的证书符合中网威信全球数字

认证中心的 CP 的所有实质性要求。

5. 中网威信全球数字认证中心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. 中网威信全球数字认证中心将及时吊销证书。
7. 中网威信全球数字认证中心拒绝签发证书后，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，中网威信全球数字认证中心向证书依赖方证明，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。

9.5.2 注册机构的陈述与担保

中网威信全球数字认证中心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全球数字认证中心的 CP 的所有实质性要求。
2. 在中网威信全球数字认证中心生成证书时，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 CP 的规定，及时向中网威信全球数字认证中心提交证书申请、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。

9.5.3 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，可供中网威信全球数字认证中心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全球数字认证中心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全球数字认证中心或中网威信全球数字认证中心授权的发证机构，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全球数字认证中心吊销其证书。

9.5.4 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。

9.5.5 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全球数字认证中心的 CP。

9.6 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，中网威信全球数字认证中心不承担与申请人、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。

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

中网威信全球数字认证中心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。

中网威信全球数字认证中心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。

9.7 有限责任

中网威信全球数字认证中心在对外服务过程中只承担对外声明的、本 CP 中规定的、对外签署的任何协议中所规定的有限责任。

中网威信全球数字认证中心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。

9.8 赔偿

9.8.1 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. 由于中网威信全球数字认证中心的未授权使用或泄露造成的用户私钥泄露；

2. 由于中网威信全球数字认证中心自身原因造成的用户证书的错误发放；

3. 当中网威信全球数字认证中心由于故意违反本 CP，给用户造成客户的经济损失的；

4. 由于中网威信全球数字认证中心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。

9.9 有效期限与终止

9.9.1 有效期限

中网威信全球数字认证中心的 CP 自发布之日起生效，CP 中将详细注明版本号及发布日期，最新版本的 CP 通过访问中网威信全球数字认证中心网站获得，对具体个人不做另行通知。

9.9.2 终止

当新版本的 CP 正式发布生效，则旧版本的 CP 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。

9.9.3 效力的终止与保留

中网威信 CP 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中华人民共和国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，CP、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。

9.10 对参与者的个别通告与沟通

除非法律法规或者协议有特别的规定，中网威信全球数字认证中心将以合理的方式与相关各方进行沟通，不会采取个别的方式进行。

无论何时任何人打算或要求发布任何本 CP 中提及的服务、规范、操作等的通知、要求或请求，这些信息将用书面形式进行传达。

书面通信必须由提供书面单据的快递服务送达，或经由挂号邮件确认，须附回邮及回函。邮递地址如下：

中华人民共和国北京市西城区西单北大街甲133号（北京君太百货）1209室（100032）

中网威信电子安全服务有限公司

如果通过电子邮件方式发送通知给中网威信全球数字认证中心，则这种通知只有在中网威信全球数字认证中心收到电子邮件通知后 24 小时内，收到书面确认材料，方为有效。

9.11 修订

9.11.1 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。中网威信全球数字认证中心将对 CP 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 CP 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 CP 及其他相关文档、协议经中网威信管理层批准后正式发布。

9.11.2 通知机制和期限

本 CP 在中网威信全球数字认证中心的网站(http://www.uni-ca.com.cn)上发布。

版本更新时，最新版本的 CP 在中网威信全球数字认证中心的网站发布，对具体个人不做另行通知。

9.11.3 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 CP。

9.12 争议处理

中网威信全球数字认证中心与订户、依赖方发生争议时，应向中网威信全球数字认证中心所在地仲裁机构提请仲裁。

9.13 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。

9.14 与适用法律的符合性

在任何情况下，中网威信全球数字认证中心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。

本 CP 必须符合《中华人员共和国电子签名法》、《电子认证服务管理办法》规定。

9.15 一般条款

9.15.1 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。

9.15.2 转让

中网威信全球数字认证中心、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。

9.15.3 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。

9.15.4 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。

9.15.5 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，中网威信全球数字认证中心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。

9.16 其他条款

中网 CA 承诺遵循 CA/Browser Form（http://www.cabforum.org）发布的最新版本的《EV 证书指导准则 Guidelines for the Issuance and Management of Extended Validation Certficates》，若 CSP 与以上准则不符，则以准侧为准