

西部安全认证中心（CWCA）

# 电子认证业务规则

## Certification Practices Statement (CPS)

版本1.1



发布日期：[ 2006年12月12日]

生效日期：[ 2006年12月12日]

西部安全认证中心有限责任公司

<http://www.cwca.com.cn/cps.pdf>

# 目 录

<b>1. 概括性描述</b> .....	<b>12</b>
1.1 概述.....	12
1.1.1 西部安全认证中心有限责任公司 (CWCA) .....	12
1.1.2 认证业务规则 (CPS) .....	12
1.1.3 CWCA 的标识.....	13
1.2 文档名称.....	14
1.3 电子认证活动参与者.....	14
1.3.1 电子认证服务机构.....	14
1.3.2 注册机构.....	14
1.3.3 订户.....	15
1.3.4 依赖方.....	15
1.3.5 其他参与者.....	15
1.4 证书应用.....	15
1.4.1 适合的证书应用.....	15
1.4.2 受限制的证书应用.....	17
1.5 策略管理.....	17
1.5.1 策略文档管理机构.....	17
1.5.2 联系人.....	18
1.5.3 决定 CPS 符合策略的机构.....	18
1.5.4 认证业务规则的变更和发布.....	18
1.5.5 CPS 批准程序.....	19
1.6 定义和缩写.....	19
<b>2. 信息发布与信息管理</b> .....	<b>21</b>
2.1 认证信息的发布.....	21
2.2 发布时间或频率.....	21

2.3 信息库访问控制 .....	22
<b>3. 身份标识与鉴别 .....</b>	<b>22</b>
3.1 命名 .....	22
3.1.1 名称类型 .....	22
3.1.2 对名称意义化的要求 .....	22
3.1.3 订户的匿名或伪名 .....	22
3.1.4 理解不同名称形式的规则 .....	23
3.1.5 名称的唯一性 .....	23
3.1.6 商标的识别、鉴别和角色 .....	23
3.2 初始身份确认 .....	23
3.2.1 证明拥有私钥的方法 .....	23
3.2.2 组织机构身份的鉴别规范 .....	23
3.2.3 个人身份的鉴别规范 .....	25
3.2.4 没有验证的订户信息 .....	25
3.2.5 授权确认 .....	25
3.2.6 互操作准则 .....	26
3.3 密钥更新请求的标识与鉴别 .....	26
3.3.1 常规密钥更新的标识与鉴别 .....	26
3.3.2 吊销后密钥更新的标识与鉴别 .....	27
3.4 吊销请求的标识与鉴别 .....	27
<b>4. 证书生命周期操作要求 .....</b>	<b>27</b>
4.1 证书申请 .....	27
4.1.1 证书申请实体 .....	27
4.1.2 证书申请过程与责任 .....	27
4.2 证书申请处理 .....	28
4.2.1 执行识别与鉴别功能 .....	28
4.2.2 证书申请批准和拒绝 .....	28

4.2.3 处理证书申请的时间.....	28
4.3 证书签发.....	29
4.3.1 证书签发过程中电子认证服务机构的行为.....	29
4.3.2 电子认证服务机构对订户的通告.....	29
4.4 证书接受.....	29
4.4.1 构成接受证书的行为.....	29
4.4.2 电子认证服务机构对证书的发布.....	30
4.4.3 电子认证服务机构对其他实体的通告.....	30
4.5 密钥对和证书的使用.....	30
4.5.1 订户私钥和证书的使用.....	30
4.5.2 依赖方对公钥和证书的使用.....	30
4.6 证书更新.....	31
4.6.1 证书更新的情形.....	31
4.6.2 请求证书更新的实体.....	31
4.6.3 证书更新请求的处理.....	32
4.6.4 颁发新证书时对订户的通告.....	32
4.6.5 构成接受更新证书的行为.....	32
4.6.6 电子认证服务机构对更新证书的发布.....	32
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.....	32
4.7 证书密钥更新.....	33
4.7.1 证书密钥更新的情形.....	33
4.7.2 请求证书密钥更新的实体.....	33
4.7.3 证书密钥更新请求的处理.....	33
4.7.4 颁发新证书对订户的通告.....	33
4.7.5 构成接受密钥更新证书的行为.....	34
4.7.6 对密钥更新证书的发布.....	34
4.7.7 对其他实体的通告.....	34
4.8 证书变更.....	34

4.8.1 证书变更的情形	34
4.8.2 请求证书变更的实体	34
4.8.3 证书变更请求的处理	35
4.8.4 颁发新证书时对订户的通告	35
4.8.5 构成接受变更证书的行为	35
4.8.6 对变更证书的发布	35
4.8.7 对其他实体的通告	35
4.9 证书吊销和挂起	36
4.9.1 证书吊销的情形	36
4.9.2 请求证书吊销的实体	36
4.9.3 吊销请求的流程	36
4.9.4 吊销请求宽限期	37
4.9.5 处理吊销请求的时限	37
4.9.6 依赖方检查证书吊销的要求	38
4.9.7 CRL 的发布频率	38
4.9.8 CRL 发布的最大滞后时间	38
4.10 证书状态服务	39
4.10.1 操作特点	39
4.10.2 服务可用性	39
4.10.3 可选特征	39
4.11 订购结束	39
4.12 密钥生成、备份与恢复	40
4.12.1 密钥生成、备份与恢复的策略和行为	40
4.12.2 会话密钥的封装与恢复的策略和行为	40
5. 电子认证服务机构设施、管理和操作控制	41
5.1 物理控制	41
5.1.1 场地位置与建筑	41

5.1.2 物理访问.....	43
5.1.3 电力与空调.....	43
5.1.4 水患防治.....	44
5.1.5 火灾防护.....	44
5.1.6 介质存储.....	45
5.1.7 废物处理.....	45
5.1.8 异地备份.....	45
5.2 程序控制.....	45
5.2.1 可信角色.....	45
5.2.2 每个角色的识别与鉴别.....	46
5.2.3 需要职责分割的角色.....	47
5.3 人员控制.....	47
5.3.1 资格、经历和无过失要求.....	47
5.3.2 背景审查程序.....	47
5.3.3 培训要求.....	48
5.3.4 再培训周期和要求.....	49
5.3.5 工作岗位轮换周期和顺序.....	49
5.3.6 对未授权行为的处罚.....	49
5.3.7 独立合约人的要求.....	49
5.3.8 提供给员工的文档.....	50
5.4 审计日志程序.....	50
5.4.1 记录事件的类型.....	50
5.4.2 处理日志的周期.....	50
5.4.3 审计日志的保存期限.....	50
5.4.4 审计日志的保护.....	51
5.4.5 审计日志备份程序.....	51
5.4.6 审计日志收集系统.....	51
5.4.7 对制造恶意事件实体的通告.....	52

5.4.8 脆弱性评估.....	52
5.5 记录归档.....	52
5.5.1 归档记录的类型.....	52
5.5.2 归档记录的保存期限.....	52
5.5.3 归档文件的保护.....	52
5.5.4 归档文件的备份程序.....	53
5.5.5 记录的时间戳要求.....	53
5.5.6 获得和检验归档信息的程序.....	53
5.6 电子认证服务机构密钥更替.....	53
5.7 损害和灾难恢复.....	54
5.7.1 事故和损害处理程序.....	56
5.7.2 计算资源、软件和/或数据的损坏.....	56
5.7.3 实体私钥损害处理程序.....	56
5.7.4 灾难后的业务连续性能力.....	57
5.8 CWCA 和注册机构的终止.....	57
<b>6. 认证系统技术安全控制.....</b>	<b>58</b>
6.1 密钥对的生成和安装.....	58
6.1.1 密钥对的生成.....	58
6.1.2 私钥传送给订户.....	58
6.1.3 公钥传送给证书签发机构.....	59
6.1.4 电子认证服务机构公钥传送给依赖方.....	59
6.1.5 密钥的长度.....	59
6.1.6 公钥参数的生成和质量检查.....	59
6.1.7 密钥使用目的.....	59
6.2 私钥保护和密码模块工程控制.....	60
6.2.1 密码模块标准和控制.....	60
6.2.2 私钥的多人控制.....	60

6.2.3 私钥托管.....	60
6.2.4 私钥备份.....	61
6.2.5 私钥归档.....	61
6.2.6 私钥导入、导出密码模块.....	61
6.2.7 私钥在密码模块中的存储.....	61
6.2.8 激活、解除激活及销毁私钥的方法.....	61
6.2.9 密码模块的评估.....	62
6.3 密钥对管理的其他方面.....	62
6.3.1 公钥归档.....	62
6.3.2 证书操作期和密钥对使用期限.....	63
6.4 激活数据.....	63
6.4.1 激活数据的产生和安装.....	63
6.4.2 激活数据的保护.....	63
6.4.3 激活数据的其他方面.....	63
6.5 计算机安全控制.....	63
6.5.1 特别的计算机安全技术要求.....	63
6.5.2 计算机安全评估.....	64
6.6 生命周期技术控制.....	64
6.6.1 系统开发控制.....	64
6.6.2 安全管理控制.....	64
6.6.3 生命周期的安全控制.....	65
6.7 网络的安全控制.....	65
6.8 时间戳.....	65
7. 证书、证书吊销列表和在线证书状态协议.....	65
7.1 证书.....	65
7.1.1 版本号.....	66
7.1.2 证书扩展项.....	66

7.1.3 算法对象标识符.....	66
7.1.4 名称形式.....	66
7.2 证书吊销列表.....	67
7.2.1 版本号.....	67
7.2.2 CRL 和 CRL 条目扩展项.....	68
7.3 在线证书状态协议.....	68
7.3.1 版本号.....	68
7.3.2 OCSP 扩展项.....	68
<b>8. 电子认证服务机构审计和其他评估.....</b>	<b>68</b>
8.1 评估的频率或情形.....	68
8.2 评估者的资质.....	69
8.3 评估者与被评估者之间的关系.....	70
8.4 评估内容.....	70
8.5 对问题与不足采取的措施.....	70
8.6 评估结果的传达与发布.....	70
<b>9. 法律责任和其他业务条款.....</b>	<b>71</b>
9.1 费用.....	71
9.1.1 证书签发和更新费用.....	71
9.1.2 证书查询费用.....	71
9.1.3 证书吊销或状态信息的查询费用.....	71
9.1.4 其他服务的费用.....	71
9.1.5 退款策略.....	71
9.2 财务责任.....	72
9.3 业务信息保密.....	72
9.3.1 保密信息范围.....	72
9.3.2 不属于保密的信息.....	73
9.3.3 保护保密信息的信息.....	73

9.4 个人隐私保密 .....	74
9.4.1 隐私保密方案 .....	74
9.4.2 作为隐私处理的信息 .....	74
9.4.3 不被视为隐私的信息 .....	74
9.4.4 保护隐私的责任 .....	74
9.4.5 使用隐私信息的告知或同意 .....	74
9.4.6 依法律或行政程序的信息披露 .....	75
9.4.7 其他信息披露情形 .....	75
9.5 知识产权 .....	75
9.6 陈述与担保 .....	76
9.6.1 电子认证服务机构的陈述与担保 .....	76
9.6.2 注册机构的陈述与担保 .....	76
9.6.3 订户的陈述与担保 .....	77
9.6.4 依赖方的陈述与担保 .....	78
9.6.5 其他参与者的陈述与担保 .....	78
9.7 赔偿与担保免责 .....	78
9.7.1 用户申请 CWCA 赔偿 .....	78
9.7.2 CWCA 申请用户赔偿 .....	79
9.7.3 责任免除 .....	79
9.7.4 有限责任 .....	80
9.8 有效期限与终止 .....	81
9.8.1 有效期限 .....	81
9.8.2 终止 .....	81
9.8.3 效力的终止与保留 .....	81
9.9 对参与者的个别通告与沟通 .....	82
9.10 修订 .....	82
9.10.1 修订程序 .....	82
9.10.2 通告机制和期限 .....	82

9.10.3 必须修改业务规则的情形.....	82
9.11 争议处理.....	83
9.12 管辖法律.....	83
9.13 与适用法律的符合性.....	84
9.14 一般条款.....	84
9.14.1 完整协议.....	84
9.14.2 分割性.....	84
9.14.3 强制执行.....	84
9.14.4 不可抗力.....	84
9.15 其他条款.....	85

# 1. 概括性描述

## 1.1 概述

### 1.1.1 西部安全认证中心有限责任公司（CWCA）

西部安全认证中心有限责任公司（CHINA WEST Certificate Authority CO.,Ltd.，简称 CWCA）成立于 2002 年 4 月。2002 年 4 月 27 日通过国家密码管理委员会办公室技术方案论证（国密办[2002]82 号）；2002 年 10 月 13 日公司屏蔽机房及 CA 认证系统通过国家密码管理委员会办公室的安全审查（国密办字[2002]221 号，国密办字[2002]222 号）；2004 年 12 月 25 日通过国家密码管理委员会办公室组织的技术鉴定（国密办[2005]3 号，国密办[2005]4 号）。

CWCA 是严格按照《中华人民共和国电子签名法》的要求和《电子认证服务管理办法》来设立、通过信息产业部批准的依法提供电子认证服务的机构。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。

### 1.1.2 认证业务规则（CPS）

西部安全认证中心电子认证业务规则（以下简称《电子认证业务规则》（CPS））由西部安全认证中心有限责任公司按照信息产业部《电子认证服务管理办法》的要求制定，并报信息产业部备案。

建立本 CPS 并保障其完整的、正确的得到贯彻和实施，为 CWCA 的

第三方电子认证服务提供安全性、规范性、可靠性和可执行性的保证。

本 CPS 详细阐述了 CWCA 签发和管理证书及运营维护证书服务设施的活动，并提供在实际工作和运行中应遵循的各项规范。本 CPS 是证书管理、证书服务、证书吊销和更新、证书应用、证书分类、证书授权、证书责任等 CWCA 数字证书相关的政策、规则的集合。本 CPS 详细叙述了认证业务的整个过程，监督认证业务的实施，提供法律上的约束并提醒当事人在本 CPS 条款规定的范围内产生、使用证书并进行证书验证。

作为实际应用和操作的文件依据，本 CPS 适用于 CWCA、CWCA 授权的各类注册机构、注册分支机构、受理点等服务机构以及 CWCA 的内部员工、各 CWCA 关联实体及其员工、申请使用证书的单位和个人、和各类证书持有者。所有这些主体都必须完整地理解和执行本 CPS 所规定的条款，承担相应的责任和义务。

作为公告，本 CPS 向社会公布 CWCA 关于证书服务的基本立场和观点，为证书申请者和订户在证书有效期内提供相关的咨询服务。任何和 CWCA 有关联的组织、机构、团体和个人，必须完整理解和准确解释本 CPS 的内容。

### 1.1.3 CWCA 的标识

CWCA 是西部安全认证中心有限责任公司（CHINA West Certificate Authority CO., Ltd.）的缩写和注册商标。同时，“西部 CA”也是西部安全认证中心有限责任公司的有效缩写。

“CWCA”、“西部 CA”及其相关文字、标识、图示等都代表着其所有者——西部安全认证中心有限责任公司的形象，以及在不同场所所代

表的利益主体。

西部安全认证中心有限责任公司、“CWCA”、“西部 CA” 的标准图标为：



## 1.2 文档名称

文档名称是《西部安全认证中心有限责任公司电子认证业务规则》。

## 1.3 电子认证活动参与者

### 1.3.1 电子认证服务机构

CWCA 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（RA 系统）和证书本地受理点（LRA），负责受理证书申请。

### 1.3.3 订户

订户是从 CWCA 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，可以是个人、软硬件设备或组织。在 CWCA 证书服务体系中，依赖方可以是、也可以不是一个订户。

### 1.3.5 其他参与者

其他参与者指为 CWCA 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

CWCA 通过发放数字证书为电子商务和电子政务提供安全保障，确保互联网上信息传递双方身份的真实性、信息的保密性和完整性、以及网上交易的不可否认性。CWCA 证书只能用于证书策略规定的合法目的。

CWCA 证书策略根据安全保证级别、使用实体、用途等定义了三类证书。

其中一类证书分为两种，一种是一类个人证书，提供了基本的安全保证。一类证书可以用于提供自然人的身份证明，能够应用于数字签名、加密和访问控制。其中，根据规定，经过 CWCA 鉴证的实体所拥有的数字证书，在满足《中华人民共和国电子签名法》的其它规定下，由其所

产生的电子签名符合《中华人民共和国电子签名法》的要求。

另一种是一类虚拟实体证书，提供基于虚拟实体的应用的安全保护，比如针对电子邮箱的安全电子邮件证书，能够应用于电子邮件的签名、加密、由于该类证书的最终实体并不真实存在或并不能与现实中的实体一一对应。因此此类证书所产生的电子签名仅代表虚拟实体的意愿。CWCA 并不保证虚拟实体所产生的电子签名代表其所对应的真实实体，即电子签名人的意愿，除非能够证明这个真实实体，即电子签名人对证书认定的虚拟实体具有完全并且是唯一的控制权。CWCA 并不承担此条件下的身份真实性认定。

二类证书也属于个人证书，同其它两类证书相比，二类证书提供了中间级别的安全保证。它们主要用于提供个人的身份证明，能够应用于数字签名、加密和访问控制，以及中等额度交易中的身份证明。二类个人证书可包括签名证书和加密证书。

经过 CWCA 鉴证的二类证书，在满足《中华人民共和国电子签名法》的其他规定下，由其产生的电子签名符合《中华人民共和国电子签名法》的要求。

三类证书包括组织机构身份证书、组织机构代表人证书、服务器证书(SSL 证书)在 CWCA 信任域中，第三类证书提供最高级别的安全保证。

组织机构身份证书可用于信息活动中的组织机构的身份证明，用于签订合同、完成交易等。组织机构代表人证书是签发给组织机构的授权的代表人，证书用途与组织机构身份证书类似。服务器证书用于标识组织机构的 WEB 服务器的身份，将一个域名与一台服务器绑定。该服务器证书确保服务器的拥有机构有权使用证书上的域名，确保当一个用户访问一个以该域名命名的 WEB 服务器时，用户访问的 WEB 服务器就是他

访问的服务器，而不是假冒的服务器，另外它可实现信息从客户端到服务器端的保密传送。

经过 CWCA 鉴证的三类证书，在满足《中华人民共和国电子签名法》的其他规定下，由其所产生的电子签名符合《中华人民共和国电子签名法》的要求。

#### 1.4.2 受限制的证书应用

CWCA 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

根据《中华人民共和国电子签名法》、《电子认证服务管理办法》和《电子认证业务规则规范》的要求，CWCA 制定本《电子认证业务规则》(CPS)，并指定专门的机构——CWCA 认证委员会作为策略的最高管理机构。

CWCA 认证委员会，作为第三方电子认证服务所有策略的最高管理机构，由 CWCA 召集管理人员、PKI 技术人员和法律顾问组成，负责审核批准 CPS，并作为 CPS 实施检查监督的最高决定机构。

CWCA 安全管理部作为 CPS 的维护工作机构，负责提出修改报告，并负责此方面的对外咨询服务。

## 1.5.2 联系人

本《电子认证业务规则》在 CWCA 网站发布，对具体个人不另行通知。 网站地址：<http://www.cwca.com.cn>

电子邮箱地址：cps@cwca.com.cn

联系地址：宁夏银川西桥南巷 1 号信息大厦九楼

电话号码：0086-951-5022639

传真号码：0086-951-6086322-8001

## 1.5.3 决定 CPS 符合策略的机构

作为电子认证业务的主管部门，信息产业部发布了《电子认证业务规则规范》，CWCA 根据规范的要求，制定本电子认证服务业务规则(CPS)，并提交信息产业部备案。CWCA 认证委员会作为最高策略管理机构，是 CPS 符合策略的决定机构。

CWCA 保证其制订和发布的 CPS，其执行、解释、翻译和有效性均符合和适用中华人民共和国的法律规定。

CWCA 安全管理部作为认证服务策略的工作部门，负责 CPS 实施的日常监督检查，保证认证体系的运行符合本 CPS 的要求。

## 1.5.4 认证业务规则的变更和发布

CWCA 有权对《电子认证业务规则》(CPS) 进行预期或非预期的修改。修改过的《电子认证业务规则》，将根据《电子认证服务管理办法》的要求，在规定的时间内向信息产业部进行备案。

在本 CPS 做出任何变动之前，CWCA 认证委员会将对安全管理部提交

的变更建议报告进行研究并做出变更决定，变更后的 CPS 将进行公布。

变更后的 CPS 自公布之日即生效，本 CPS 版本将自动终止。

CWCA 将对 CPS 进行严格的版本控制。所有进行的修改在 CWCA 网站上公布 (<http://www.cwca.com.cn>)。

### 1.5.5 CPS 批准程序

CWCA 的 CPS 由安全管理部起草拟订后，提交 CWCA 认证委员会审核。如果因为标准的变化、技术的提高、安全机制的增强、运营环境的变化和法律法规的要求等对 CPS 进行修改，由安全管理部提交修改建议报告，提交 CWCA 认证委员会审核。经过该委员会批准后，CWCA 通过 <http://www.cwca.com.cn> 进行公布。

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，CWCA 在公布 CPS 后向信息产业部备案。

## 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。

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

一个经电子认证服务机构数字签名的列表，标记已经被吊销的 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

CWCA 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 CWCA 不定时发出的信息。CWCA 网址：<http://www.cwca.com.cn>。

本《电子认证业务规则》发布在 CWCA 的网站上，供相关方下载、查阅。CWCA 通过目录服务器发布订户的证书和 CRL，订户或依赖方可以通过访问 CWCA 的目录服务器获取证书的信息和吊销证书列表。同时，CWCA 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，CWCA 通过目录服务器自动将该证书公布。

c) CWCA 的 CRL 每 24 小时发布一次。

## 2.3 信息库访问控制

在 CWCA 网站或者目录服务器上公布的信息属于公开信息，任何实体可以免费查阅这些信息。CWCA 要求访问 CPS、证书、证书状态、CRL 等信息的任何实体必须遵守本 CPS、依赖方协议和 CRL 使用协议。

## 3. 身份标识与鉴别

### 3.1 命名

#### 3.1.1 名称类型

根据证书对应实体的类型不同，CWCA 签发的证书的实体名字可以是人员姓名、组织机构名、部门名、域名等，命名符合 X. 500 甄别名规定。

CWCA 证书体系中采用 X. 500 定义的甄别名 (DN) 标准来唯一标识一张证书的使用者的身份信息。

每个订户对应一个甄别名 (Distinguished Name, 简称 DN)。

#### 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 CWCA 证书服务体系中，订户不能使用匿名或伪名申请证书，证

书中也不能使用匿名或伪名。

### 3.1.4 理解不同名称形式的规则

对于不同名称形式的各类规则，CWCA 依据 X. 500 甄别名命名规则解释。

### 3.1.5 名称的唯一性

在 CWCA 证书服务体系中，证书主体名称必须是唯一的。

### 3.1.6 商标的识别、鉴别和角色

本《电子认证业务规则》受到完全的版权保护，本文件中涉及的“CWCA”及其图标等是由西部安全认证中心有限责任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

CWCA 通过使用经数字签名的 PKCS#10 格式的证书请求，或其它相当的密码格式，或其他 CWCA 批准的方法，验证证书申请者拥有私钥。

### 3.2.2 组织机构身份的鉴别规范

对于组织机构身份的鉴别，CWCA 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。CWCA 保留根据国家最新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 CWCA 的网站上：<http://www.cwca.com.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 CWCA 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副本及复印件。例举部分有效证件如下：
  - 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) 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)。

CWCA 授权的注册机构按照 CWCA 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，CWCA 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 个人身份的鉴别规范

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。CWCA 保留根据国家最新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 CWCA 的网站上：<http://www.cwca.com.cn>。个人需持上述个人有效身份证件，到 CWCA 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。

CWCA 授权的注册机构按照 CWCA 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，CWCA 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 CWCA 数字证书事宜的授权文件。组织在 CWCA 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。

对于 CWCA 内的其他发证机构，如果双方之间有协议，那么 CWCA 将依据协议的内容，接受非 CWCA 的发证机构鉴别过的信息，并为之签发相应的证书。如果双方之间没有任何类似的协议，那么 CWCA 要求非 CWCA 发证机构严格按照本 CPS 的规定进行身份鉴别。CWCA 会根据情况决定是否接受这些被鉴别审核过的资料，并做出是否进行受理的决定。

如果国家法律法规对此有规定，CWCA 将严格予以执行。

## 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

对于一般正常情况下的密钥更新，订户访问到 CWCA 或其注册机构的证书受理点进行密钥更新申请，在对相关证件进行验证通过后，操作员获取订户原证书相关信息，如订户甄别名、证书序列号等，形成证书密钥更新申请信息，申请信息包含新公钥并由更新前的私钥签名（对于加密证书密钥而言，申请信息不包含新公钥）。

CWCA 的证书认证系统将对密钥更新申请进行验证，包括验证申请签名，然后进行与新证书申请一样的鉴证。

### 3.3.2 吊销后密钥更新的标识与鉴别

CWCA 对吊销后证书不进行密钥更新。

### 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验证相同的流程，详见 § 3.2.2 组织机构身份的鉴别和 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 证书申请过程与责任

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。CWCA 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

CWCA 或授权的注册机构按照本《电子认证业务规则》所规定的身份鉴别规范对申请人的身份进行识别与鉴别。具体的鉴别规范详见 § 3.2.2 组织机构身份的鉴别规范和 3.2.3 个人身份的鉴别规范。

### 4.2.2 证书申请批准和拒绝

CWCA 或授权的注册机构根据本《电子认证业务规则》所规定的身份鉴别规范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》所规定的身份鉴别规范且鉴证结果为合格，CWCA 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，CWCA 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

CWCA 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 7 个工作日内处理证书

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 CWCA 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

CWCA 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，CWCA 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) CWCA 认为其他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

CWCA 在签发完证书后，就将证书发布到数据库和目录服务器中。

CWCA 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

其他实体可以在目录服务器上查询到 CWCA 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 CWCA 所签发的证书后，均视为已经同意遵守与 CWCA、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 CWCA 的证书验证证书中的签名，确认该证书是 CWCA 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，确认该证书没有被吊销。

## 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 45 日，到 CWCA 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) 证书的有效期限将要到期；
- 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 CWCA 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

对订户的通告有以下几种：

- a) 通过面对面的方式；
- b) 邮政信函通知订户；
- c) CWCA 认为其他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

CWCA 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

其他实体可以通过目录服务器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;
- b) 因私钥泄漏而吊销证书;
- c) 其他原因。

### 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 CWCA 签发的个人、组织及设备等各类证书的证书持有者。

### 4.7.3 证书密钥更新请求的处理

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。

### 4.7.4 颁发新证书对订户的通告

对订户的通告有以下几种方式：

- a) 通过面对面的方式;
- b) 邮政信函通知订户;
- c) CWCA 认为其它安全可行的方式通知订户。

### 4.7.5 构成接受密钥更新证书的行为

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。

### 4.7.6 对密钥更新证书的发布

CWCA 在签发密钥更新证书后，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。

### 4.7.7 对其他实体的通告

其他实体可以通过目录服务器查询已更新的数字证书。

## 4.8 证书变更

### 4.8.1 证书变更的情形

- a) 证书的主体内容发生改变；
- b) 证书的 E-mail 地址发生改变；
- c) 其他信息改变。

### 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 CWCA 签发的个人、组织及设备等各类证书的证书持有者。

### 4.8.3 证书变更请求的处理

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。

### 4.8.4 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：

- a) 通过面对面的方式；
- b) 邮政信函通知订户；
- c) CWCA 认为其它安全可行的方式通知订户。

### 4.8.5 构成接受变更证书的行为

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。

### 4.8.6 对变更证书的发布

CWCA 在签发变更新证书后，即将变更新证书发布到数据库和目录服务器中，对外进行发布。

### 4.8.7 对其他实体的通告

其他实体可以通过目录服务器查询已更新的数字证书。

## 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，CWCA 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、CWCA、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) 证书吊销的申请人到 CWCA 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) CWCA 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) CWCA 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 CWCA 或 CWCA 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。

#### 4.9.4 吊销请求宽限期

如果在出现私钥泄露或有泄露嫌疑等紧急情况下事件，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 处理吊销请求的时限

CWCA 接到吊销请求后将立即处理，24 小时后生效。CWCA 每日签发一次 CRL，并将最新的 CRL 发布到目录服务器指定的位置，供请求者查询下载。CRL 的结构如下：

- a) 版本号(version)
- b) 签名算法标识符(signature)
- c) 颁发者名称(issuer)
- d) 本次更新(this update)
- e) 下次更新(next update)
- f) 用户证书序列号/吊销日期(user certificate/revocation date)
- g) 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)

#### 4.9.6 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：

- 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。（依赖方要验证 CRL 的可靠性和完整性，确保是经 CWCA 发布并且签名的。）
- 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。

#### 4.9.7 CRL 的发布频率

CWCA 可采用实时或定期的方式发布 CRL。发布 CRL 的频率根据证书策略确定，每 24 小时自动发布最新 CRL，也可人工发布最新 CRL。

#### 4.9.8 CRL 发布的最大滞后时间

CRL 发布的最大滞后时间为 24 小时。

## 4.10 证书状态服务

### 4.10.1 操作特点

CWCA 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

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

### 4.10.3 可选特征

根据请求者的要求，在请求者支付相关费用后，CWCA 可以提供以下通知服务：

提供通知服务，当指定的证书被吊销时，CWCA 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

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 CWCA 授权的发证机构申请，经审核后，通过 CWCA 向 KMC 请求；KMC 审核通过后，通过密钥恢复系统，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，由密钥恢复系统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。

### 4.12.2 会话密钥的封装与恢复的策略和行为

用非对称算法封装会话密钥，可以用解密密钥来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

### 5.1 物理控制

#### 5.1.1 场地位置与建筑

a) CWCA 的建筑物和机房建设按照下列标准实施:

- (1) GB2887-89 《计算站场地技术条件》
- (2) GB50174-93 《电子计算机机房设计规范》
- (3) GB6650—86 《计算机机房活动地板技术要求》
- (4) GBJ79—85 《通信接地设计规范建筑内部装修设计防火规范》
- (5) GBJ19-87 《采暖通风与空气调节设计规范》
- (6) GB50222—95 《建筑内部装修设计防火规范》
- (7) GB6650—95 《高层民用建筑设计防火规范》
- (8) GB7450—87 《电子设备雷击保护守则》
- (9) GBJ52-82 《工业与民用供电系统设计规范》
- (10) GBJ54-83 《低压配电装置及线路设计规范》
- (11) GB232-82 《电气装置安装工程及验收规范》
- (12) JB16-83 《建筑电气设计技术规范》
- (13) GBJ79-85 《工业企业通信接地设计规范》
- (14) GB50222-95 《建筑内部装修设计防火规范》
- (15) GBJ116-88 《火灾自动报警设计规范》
- (16) CECS89-97 《建筑与建筑群综合布线系统施工及验收规范》
- (17) GBJ300-88 《建筑安装工程质量检验评定统一标准》

- (18) GA75-94 《安全防范工程设计程序和要求》
- (19) GA27-92 《中华人民共和国公共安全行业标准》
- (20) GB115-87 《工业电视监控系统工程设计规范》
- (21) EIA/TIA 568-B 《商业建筑群通信布线标准》
- (22) TSB67 《商业建筑布线系统传输性能测试标准》
- (23) 《建筑装饰工程施工及验收规范》
- (24) GB-12190 《高性能屏蔽室屏蔽效能的测量方法》
- (25) GJBZ20219-94 《军用电磁屏蔽室通用技术要求和检测方法》 C  
级标准

b) 环境条件及相关指标

- (1) 温度：国家标准 B 级  $23^{\circ}\text{C} \pm 5^{\circ}\text{C}$
- (2) 相对湿度：国家标准 B 级 40%–65%
- (3) 温度变化率：小于  $10^{\circ}\text{C}/\text{h}$ ，不凝露。
- (4) 尘埃：粒径  $\geq 0.5\mu\text{m}$  个数  $\leq 18000/\text{dm}^3$
- (5) 噪音：计算机开机条件下，主机操作员位置  $A \leq 68\text{dB}$
- (6) 接地：

计算机系统直流逻辑地电阻值  $\leq 0.8\ \Omega$

计算机系统交流工作地电阻值  $\leq 1\ \Omega$

计算机系统安全保护地电阻值  $\leq 1\ \Omega$

计算机系统防雷保护地电阻值  $\leq 4\ \Omega$

- (7) 电压：国家标准 B 级 三相电压为 380V，波动不大于  $\pm 8\%$   
单相电压为 220V，波动不大于  $\pm 8\%$

- (8) 频率：国家标准 B 级  $50\text{Hz} \pm 0.5\text{Hz}$

- (9) 负荷分配：三相电流不平衡度  $\leq 20\%$ ，三相电压不平衡度  $\leq 5\%$

(10) **配电**：采用双回路供电，设置 UPS 不间断电源，保证系统正常运行。

(11) **照度**：计算机工作区域不应低于 300LX，应急照明不应低于 30LX。

(12) **电磁干扰**：机房内无线电杂波干扰在频率范围 0.15MHz~1000MHz 时不大于 120dB。

电磁干扰场强 $\leq$ 800A/m（相当于 100e）。

(13) **房内计算机工作区域绝缘体静电电位**： $\leq$ 1KV

地板表面到接地系统电阻在 100K-100M 欧姆。

(14) **监控**：场区内设有严密电视监控系统。

### 5.1.2 物理访问

整个 CA 系统的各个房间之间利用隔墙进行保护，防止通过天花板下面的假平顶进入；中心安装厚钢板防盗门，防止窃贼撬门而入。

将整个系统分为多个区，如公共区、DMZ、操作区和安全区，并对这些区进行区域访问控制。在有人操作期间里层门由出入指纹系统进行控制；CWCA 门禁系统设立办公区及大门门禁，对于人员的可出入区域根据工作性质、权限进行严格划分。在员工调出或忘记帐号时立即删除权限和记录。备份设备的设置和主站点分开，以免遭受相同的物理和环境威胁。整个大楼还设有电脑录像监控系统，实行 24 小时实时监控。

### 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。计算机设备专用配电柜使用电信级不间断电源系统（UPS）来保证供电的稳定性和可靠性，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。空调系统使用机房专用空调。其组成包括空调、通风管路、新风系统。CWCA 定期对电力与空调系统的运行状态进行检查。

#### 5.1.4 水患防治

CWCA 屏蔽机房设置在电信标准机房内，有较好的防渗水、漏水系统。机房主要设备采用专用的防水插座，可以有效避免渗、漏水对系统造成的影响。

#### 5.1.5 火灾防护

CWCA 的电器系统符合电子数据处理设备的防火标准、组织政策、职业安全等。所有设备的电源系统与厂商技术规范保持一致，以保证电源的性能。机房内配置了火情警报及处理装置。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感探测器。

敏感区及高敏区配置了独立的气体灭火装置。为确保机房内基础设施及人员的生命财产安全，特制定火灾处理应急方案，以便发生火灾时

能快速有效地扑灭，控制火情，尽量减少因火灾造成的损失。

### 5.1.6 介质存储

CWCA 对储存产品软件和数据、归档、审计或备份信息的介质保存在安全设施中，这些设施受到适当的物理和逻辑访问控制的保护，只允许授权人员的访问，并防止这些介质受到意外损坏（如水、火灾和电磁）。

### 5.1.7 废物处理

CWCA 对敏感的文件和材料在处理之前将其切成碎片，使信息无法恢复。密码设备在作废处置前根据制造商的指南将其物理销毁或初始化。其它废物处理按 CWCA 正常废物处理的要求进行。

### 5.1.8 异地备份

CWCA 中心机房位于银川市西桥南巷一号信息大厦九楼，密钥管理中心位于宁夏回族自治区国家密码管理委员会办公室专用机要机房内。CWCA 每日晚 23:00 进行逻辑备份，备份数据写入磁带机内，在验证数据有效性后，备份数据分别存放在机房数据中心和办公区机要档案室。

## 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，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，并可根据需要授权下级操作员证书。

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 CWCA 的在职人员，按照所担任角色的不同进行身份鉴别。进

入机房需要使用编号和指纹识别；进入系统需要使用个人数字证书进行身份鉴别。CWCA 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

所谓职责分割，是指如果一个人担任了完成某一职能的角色，就不要再担任完成另一特定职能的角色。CWCA 对如下人员进行了职责分割：

- a)、密钥管理员
- b)、安全管理员
- c)、证书录入、审核员
- d)、系统维护人员
- e)、秘密分割持有者

## 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 CWCA 签订保密协议。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。CWCA 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

CWCA 与有关的政府部门和调查机构合作，完成对 CWCA 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

CWCA 对员工进行以下内容的综合性培训：

- CA安全原则和机制；
- CA使用的软件介绍；
- CA操作的系统和网络；
- CA质量控制体系；
- 岗位职责；
- 政策标准和程序；
- 相关法律、仲裁规则、管理办法等。

### 5.3.4 再培训周期和要求

根据 CWCA 策略调整、系统更新等情况，CWCA 可能要求员工进行继续培训以适应新的变化。培训周期 CWCA 根据业务需要进行安排。

### 5.3.5 工作岗位轮换周期和顺序

内部安排。

### 5.3.6 对未授权行为的处罚

当 CWCA 员工被怀疑或者已进行了未授权的操作，例如滥用权利、超出权限使用 CWCA 系统或进行越权操作，CWCA 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 CWCA 内部的工作人员，但从事 CWCA 有关业务的人员等独立签约者(如注册机构的工作人员)，CWCA 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 CWCA 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

CWCA 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，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。CWCA 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 处理日志的周期

CWCA 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

CWCA 在数据库保存审计日志至少两个月，离线保存至少为十五年。

#### 5.4.4 审计日志的保护

CWCA 执行严格的管理，确保只有 CWCA 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，并且对日志进行异地备份。审计日志的制作和访问进行岗位分离。

#### 5.4.5 审计日志备份程序

CWCA 保证所有的审查记录和审查总结都按照 CWCA 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，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。

CWCA 使用审计工具满足对上述系统审计的各项要求。

## 5.4.7 对制造恶意事件实体的通告

CWCA 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，CWCA 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。CWCA 有权决定是否对恶意事件的实体进行通告。

## 5.4.8 脆弱性评估

根据审计记录，CWCA 定期进行系统、物理场地、运营管理、人事管理等方面的安全脆弱性评估，并根据评估报告采取措施。

# 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为十五年。

## 5.5.3 归档文件的保护

CWCA 对各种电子、磁带、纸制形式的归档文件，都有安全的物理和逻辑保护措施和严格的管理程序，确保归档了的文件不会被损坏，防止非授权的访问、修改、删除或其它的篡改行为。

### 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 CWCA 的档案室，还在异地保存其备份。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。CWCA 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 记录的时间戳要求

所有记录都要在存档时加准确的时间标识以表明存档时间。系统产生的记录，用系统时间加盖时间戳。

### 5.5.6 获得和检验归档信息的程序

CWCA 按照内部工作流程获得归档信息。归档信息的两份拷贝由两个管理员分别管理。通过对比两个拷贝来判断归档信息是否准确。并验证信息的有效、完整和正确性。

归档数据由不同的管理员进行保存，CWCA 是通过档案室管理员和安全管理部分别进行管理并且异地保存。

## 5.6 电子认证服务机构密钥更替

CWCA 认证系统需要定期在有效期即将结束时或怀疑密钥遭到攻击的情况下进行密钥更新工作。以下为 CWCA 例行密钥的更新过程：

根密钥更新时，由所有密钥管理员在场，共同启动密钥管理程序，

执行密钥更新指令，硬件加密设备重新生成根密钥。

第二层 CA 的密钥更新时，由所有密钥管理员中的多数在场，共同启动密钥管理程序，执行密钥更新指令。

对于用户，下面两种情况下要进行更新密钥对：

- 加密公钥或签名私钥已经或即将到期。
- 加密密钥对或签名密钥对已经或被怀疑受到侵害。管理员将废除的密钥对的相应证书的序列号放在 CRL 中。

(1)、密钥更新，证书同时进行更新，用户到 CWCA 受理点要求密钥更新。

(2)、CWCA 将原用户的证书吊销。

(3)、CWCA 重新用用户的身份信息组成证书信息并发给用户更新证书用的密码。

(4)、证书受理点管理员登陆访问 CWCA 认证系统，产生密钥对，使用 CWCA 发放的更新证书用的密码与服务器建立安全通信，安全的将公钥发给 CWCA。

(5)、CWCA 将用户证书信息和用户公钥一起合成证书信息并签发。

## 5.7 损害和灾难恢复

CA 系统的灾难恢复，指的是为保证在发和灾害（水灾、风灾、地震等自然灾害或电力中断、火灾、爆炸等结构性破坏以及人为失误、网络黑客攻击、病毒等操作问题）或战争等攻击而导 CA 彻底损毁时，能够恢复 CA 的密钥和该 CA 的用户资料。

通过在异地设立灾难备份中心可以实现灾难恢复。灾难备份中心存放各级 CA 的备用加密机，该加密机中的私钥与运行系统的私钥相同。

CA 中心在更新密钥时同时更新备用加密机中的密钥。同时，根 CA 还定期将系统备份服务器中的数据通过磁带备份，以人工方式送到异地备份中心。

当公钥基础设施（PKI）发生灾难性故障时，CWCA 拥有恢复运营的能力。首先是确定灾难恢复的重要性以及恢复 PKI 运行的可接受时间。它们是确定 PKI 是否需要一个全面冗余灾难恢复站点的关键因素。

在根 CA 没有发生灾难时，各 CA 从根 CA 的系统备份服务器恢复数据，在根 CA 发生灾难时，各 CA 从异地的冗余备份中心恢复数据。

灾难恢复的具体工作包括：

- 制定灾难恢复计划；
- 数据的备份和存储；
- 辅助设备准备；
- 启动灾难恢复计划；
- 灾难恢复所需时间评估

灾难恢复实方施：

(1)、所有的口令经安全部门主管以及相关的安全管理员、政策审批部门进行变更。

(2)、根据灾难的性质，部分或全部证书需要吊销或以后重新认证。

(3)、如果目录无法使用或如果目录有不纯的嫌疑，目录数据，加密证书和 CRL 需要进行恢复及从备份中恢复，一旦目录管理员从备份中恢复了目录，安全部门和政策审批部门授权运营部门可从 CWCA 控制系统的目录恢复 CWCA 数据。

(4)、如需恢复安全专家或 PKI 安全管理员的配置文件，需要由另外一名 PKI 安全管理员或高级安全专家来对这些进行恢复。如果没有足

够的具有有效安全专家或高级安全专家来恢复安全官员配置文件的话，则需由运营主管或安全部门通过 CWCA 控制系统进行恢复。

### 5.7.1 事故和损害处理程序

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、所有对外服务的设备都具备基本的监控。
- 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，对于影响而大的故障，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、软件或数据受到破坏后，进行以下操作：

- (1)、恢复环境，启动备份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)、尽快恢复原系统。

### 5.7.3 实体私钥损害处理程序

参照 4.7 节进行证书密钥更新。

## 5.7.4 灾难后的业务连续性能力

灾难发生后 CWCA 立即用备用系统上线对用户提供服务，保持业务持续性。

## 5.8 CWCA 和注册机构的终止

终止 CA 和 RA 分二步。

第一步是终止 CA 和 RA 前的过渡期，CA 和 RA 提前 90 天向所有未吊销或未过期证书的用户发布即将终止 CA 和 RA 的信息，并采取不同的方式通知下级 CA 和 LRA 以及最终用户，在此期间内停止使用该 CA 或 RA 所发放的证书。CA 在终止服务 60 日前向国务院信息产业主管部门报告，并与其他 CA 就业务承接进行协商。如果未能就业务承接事项与其它 CA 达成协议。申请国务院信息产业主管部门安排其它 CA 承接其业务。

对于 CA 终止步骤为：

- 上报认证中心主管；
- 收回证书；
- 整理存档记录；
- 停止中心所有业务；
- 主目录服务器存档；
- 关闭主目录服务器；
- 关闭备份目录服务器；
- 销毁密钥；
- 存储重要信息；
- 清理认证中心硬盘；

- 在最后终止 CA 的服务前，要取消所有由 CWCA 发布的证书。

## 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

根 CA：根 CA 的根密钥对由硬件加密设备直接产生，并且直接保存在该硬件加密设备中，CWCA 使用的是国家商业密码管理委员会鉴定通过的硬件加密设备。产生密钥的时候必须由三个密钥管理员同时登陆后由硬件加密设备产生，任何单独的一个人均没有办法执行产生密钥的操作。密钥管理员登陆是采用 IC 卡的方式，其他人员无法获知 IC 卡或相应的密码。

第二层 CA：拥有的加密密钥对由根 CA 的加密机产生，签名密钥对在本地的硬件加密设备上产生，私钥不能出此硬件加密设备。产生密钥的时候，必须由三个密钥管理员中的多数同时登陆后由硬件加密设备产生，任何单独的一个人没有办法执行产生密钥的操作。密钥管理员登陆是采用 IC 卡的方式，其他人员无法获知 IC 卡或相应的密码。

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，具有严密且安全的控制措施。

#### 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 CWCA。

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 CWCA 的网站 (<http://www.cwca.com.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

CWCA 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

CWCA 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党委机要部门及 CA 主管部门的 5 名管理员卡中，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。CWCA KMC 设置在宁夏国密局机要机房内，禁止外界非法访问。

#### 6.2.4 私钥备份

订户的签名密钥 CWCA 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。CWCA 提供过期的托管加密密钥的归档服务。

#### 6.2.6 私钥导入、导出密码模块

使用 CWCA 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、解除激活及销毁私钥的方法

具有激活私钥、解除私钥激活状态或销毁私钥权限的管理员使用含有自己身份的加密 IC 卡登录，启动密钥管理程序，进行激活私钥、解

除私钥激活状态或销毁私钥的操作。进行这些操作需要三名管理员同时在场。

## 6.2.9 密码模块的评估

CWCA 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。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 15.6Mbps；模长 1024 的数字签名速度 105 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 CWCA 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。有效期由 CWCA 与订户在服务协议中限定。

## 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，必须派专人在场监督。

## 6.5.2 计算机安全评估

CWCA 证书系统已通过国家密码管理委员会办公室组织的商用密码产品技术鉴定，证书编号：国密办[2005]3 号和国密办[2005]4 号。

## 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，同时兼顾了开发环境的安全、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，做到了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，确保了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

CWCA 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。CWCA 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

CWCA 认证系统的各种系统日志，操作日志有对应的记录时间。

## 7. 证书、证书吊销列表和在线证书状态协议

### 7.1 证书

CWCA 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 证书扩展项

CWCA 支持并使用 X.509 第三版证书扩展项。

CWCA 的证书中添加了证书用途 (Key Usage) 扩展项, 并将其标为关键扩展项。

### 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

CWCA 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：

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。

## 7.2 证书吊销列表

CWCA 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

目前，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

1、根据《中华人民共和国电子签名法》、《电子认证服务管理办法》等要求，每年一次接受主管部门的评估和检查。

2、CWCA按照国家主管部门的要求、国家相关标准和本CPS的规定运营和服务，按照CWCA的内部评估制度，每年至少定期执行一次内部的评估审核，包括对CWCA、CWCA授权的发证机构和其他关联服务机构的评估审核。

CWCA内的关联实体，包括RA、LRA以及其他CWCA授权的证书服务机构

或其他形式的关联体，都必须遵循本CPS，并接受CWCA对其所有的流程和操作进行审计，检验其是否符合本CPS和与之相关的CWCA在授权协议、公示过的信任服务政策的规定。CWCA对关联实体的评估，一般的期限为一年。CWCA在和所有单位的授权协议中，都明确的规定了这一点。评估人员由CWCA根据要求指派，报请CWCA认证委员会备案。评估人员必须熟悉CWCA的规范和信任服务的相关知识，了解运行安全的基本知识，按照CWCA的规范、协议、履行责任业务等情况，独立、公正地对关联实体作出评估。

CWCA授权的证书服务机构可以根据协议，对下属的关联实体进行评估，有权根据上级的评估结果和自己的评估结果，取消对下属单位的授权或重新授权。CWCA的关联实体，被评估的次数一般情况下为一年一次。

## 8.2 评估者的资质

1、依照《中华人民共和国电子签名法》和《电子认证服务管理办法》，CWCA无条件接收信息产业主管部门的评估。对CWCA实施评估的评估者所具有的资质和经验，由主管部门决定。

2、在进行内部评估审计时，CWCA要求评估人员至少具备认证机构、信息安全审计的相关知识，有二年以上的相关经验，并且熟悉本CPS的规范，以及应具备计算机、网络、信息安全等方面的知识和实际工作经验。内部评估CWCA认证委员会组织实施。

3、如果CWCA认为有必要聘请外部的审计者实施内部评估，那么该审计者应该具备以下的资质：

- 必须是经许可的、有营业执照的评估机构，在业界享有良好的声

誉；

- 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；
- 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

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，足以保证评估的客观性。

### 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

CWCA 的管理层对审计报告进行评估，对一致性审计中发现的重大意外或不作为采取行动。从完成审计到采取行动纠正问题的时间不超过 45 天。

### 8.6 评估结果的传达与发布

除非法律明确要求，CWCA 一般不公开评估结果。

对 CWCA 关联方，CWCA 将依据签署的协议来通报评估结果。

## 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、地方及业界的收费标准执行。根据证书实际应用的需要, CWCA 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, CWCA 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, CWCA 不收取信息访问费用。

对于在线证书状态查询(OCSP), 由 CWCA 与订制者在协议中约定。

#### 9.1.4 其他服务的费用

CWCA 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, CWCA 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, CWCA 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，CWCA将不退还剩余时间的服务费用。

## 9.2 财务责任

CWCA 保证其具有维持其运作和履行其责任的财务能力。有能力承担对订户、依赖方等造成的责任风险，并依据《中华人民共和国电子签名法》、《电子认证服务管理办法》和本文有关条款的规定，进行赔偿。

## 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 CWCA 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；
- b) 保存在审计记录中的信息；
- c) 年度审计结果；
- d) 除非有法律要求，由 CWCA 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。

CWCA 不保存任何证书应用系统的交易信息。

除非法律明文规定，CWCA 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。CWCA 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 CWCA 目录服务等方式向外公布。

CWCA 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 保护保密信息责任

a) 各方有保护自己和其他人员或单位的机密信息、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)用于协议声明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；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 CWCA 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，CWCA 应按要求，向执法部门公布相关的保密信息，CWCA 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，CWCA 保证不会截取任何证书申请人的资料。

CWCA 保护证书申请人所提供的证明其身份的资料。CWCA 按照公司内部档案管理制度确保证书申请人资料不被遗失、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 CWCA 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 CWCA 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，CWCA 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，CWCA 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，CWCA 享有并保留对证书以及 CWCA 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。CWCA 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 CWCA 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 CWCA 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 CWCA 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

CWCA 在提供电子认证服务活动过程中的承诺如下：

a) CWCA 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) CWCA 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 CWCA 证书库发出了 CWCA 的私钥被破坏或被盗的通知，CWCA 保证其私钥是安全的。

d) CWCA 签发给订户的证书符合本 CPS 的所有实质性要求。

e) CWCA 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) CWCA 将及时吊销证书。

g) CWCA 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，CWCA 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

CWCA 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本 CPS 的所有实质性要

求。

b) 在 CWCA 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 CWCA 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 CWCA 签发的证书，就被视为向 CWCA、注册机构及信赖证书的有关当事人做出以下承诺：

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 CWCA 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 CWCA 或注册机构，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 CWCA 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。

其他参与者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。

所有其他参与者必须承认，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。

### 9.7 赔偿与担保免责

#### 9.7.1 用户申请 CWCA 赔偿

CWCA 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 CWCA 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) CWCA 在证书有效期内按照《中华人民共和国电子签名法》及相关法律规定承担损失或损害赔偿。

### 9.7.2 CWCA 申请用户赔偿

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 CWCA 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 CWCA 提供真实、完整和准确的信息，而导致 CWCA 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 CWCA 并终止使用该证书，而导致 CWCA 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) 证书的非非法使用，即违反 CWCA 对证书使用的规定，造成了 CWCA 或有关各方的利益受到损失。

### 9.7.3 责任免除

有下列情况之一的，应当免除 CWCA 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 CWCA 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，CWCA 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) CWCA 不承担任何其他未经授权的人或组织以 CWCA 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) CWCA 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) CWCA 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) CWCA 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。CWCA 和证书持有人之间的关系以及 CWCA 和依赖方之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 CWCA 承担信托责任。

f) 由于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 § 9.14.4）。

#### 9.7.4 有限责任

对于 CWCA 自身的原因，如没有严格按业务流程进行证书审批导致证书的错误签发、假冒或管理上的疏忽导致 CA 私钥泄漏、盗用等，造成了证书订户、依赖方的损失，CWCA 将承担相应的赔偿责任，但这种责任是有限的。根据证书的类别，CWCA 所承担的有限责任的赔偿如下表。

## 责任赔偿

证书类别	责任赔偿
一类	人民币 100 元
二类	人民币 500 元
三类	人民币 5000 元

CWCA 只对由于自身原因造成的用户直接损失承担责任,对间接的损失不承担责任。

## 9.8 有效期限与终止

### 9.8.1 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。

### 9.8.2 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。

### 9.8.3 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。

## 9.9 对参与者的个别通告与沟通

CWCA 及其注册机构在必要的情况下，如在主动吊销订户证书、发现订户将证书用于规定外用途及订户其他违反订户议的行为时，会通过适当方式，如电话、电邮、信函、传真等，个别通知订户、依赖方。

## 9.10 修订

### 9.10.1 修订程序

经 CWCA 认证委员会授权，安全管理部每年至少审查一次本 CPS，确保其符合国家法律法规和主管部门的要求，符合认证业务开展的实际需要。

本 CPS 的修订，由安全管理部提出修订报告后，经过 CWCA 策略最高管理部门——CWCA 认证委员会审核并批准后才能开始修订。修订后的 CPS 正式对外发布后，送交信息产业主管部门备案。

### 9.10.2 通告机制和期限

本《电子认证业务规则》在 CWCA 的网站 (<http://www.cwca.com.cn>) 上发布。

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

### 9.10.3 必须修改业务规则的情形

如果出现下列情况，那么必须对本CPS进行修改：

1. 密码技术出现重大发展，足以影响现有CPS的有效性
2. 有关认证业务的相关标准进行更新
3. 认证系统和有关管理规范发生重大升级或改变
4. 法律法规和主管部门要求
5. 现有CPS出现重要缺陷

对CPS 的修订在发布之日起生效。

## 9.11 争议处理

CWCA、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 CWCA，根据本《电子认证业务规则》中的规定，明确责任方；
- b) 由 CWCA 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 CWCA 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，由 CWCA 工商注册所在地的人民法院裁定。

## 9.12 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。

## 9.13 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。

## 9.14 一般条款

### 9.14.1 完整协议

本《电子认证业务规则》将替代旧版本、与主题相关的书面或口头解释。

### 9.14.2 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。

### 9.14.3 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。

### 9.14.4 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，CWCA 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。

## 9.15 其他条款

CWCA 对本《电子认证业务规则》拥有最终解释权。