陕西省数字证书认证中心有限责任公司
SHAANXI DIGITAL CERTIFICATE AUTHORITY CO.,LTD.

陕西省数字证书认证中心
证书策略（CP）

文件编号：SNCAG(s)303
文件版号：V2.0
文件页数：55 页
生效日期：2009 年 5 月 20 日

拟　　制：		**日　　期：**	
审　　核：		**日　　期：**	
批　　准：		**日　　期：**	

目 录

陕西省数字证书策略

陕西省数字证书认证中心有限责任公司版权所有

版权声明

1 简介

本文是陕西省数字证书认证中心证书策略(CP)。SNCA(以下 SNCA 为其简称)是经中华任命共和国工业和信息化部审核批准的电子认证机构，是重要的国家信息安全基础设施之一，也是《中华人民共和国电子签名法》颁布后，国内首批获得电子认证服务许可证的 CA 之一。SNCA 向用户提供各种应用的数字证书。SNCA 提供的服务适合于广大、对通信和信息安全方面有各种各样需求的公众用户。

证书策略（CP，Certification Policy）是关于认证机构（CA,Certification Authority）制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。本证书策略的适用范围为 SNCA 发放的所有证书。在 SNCA 证书策略中，它为批准、签发、管理、使用、吊销、更新证书和相关的可信服务制定商务、法律和技术上的规范。这些规范是 SNCA 证书的标准，它应用于保护 SNCA 证书的完整性和安全性。

SNCA 安全管理委员会负责 CP 的修改、更新、及评述整理工作。同时还负责监督对 CP 的要求遵循情况。

本 CP 的结构符合“互联网 X.509 公开密钥基础设施证书策略和证书业务框架”即由互联网标准组织“互联网工程工作组”制定的 RFC3647 标准。RFC3647 框架已经成为 PKI 行业的一个标准。本 CP 服从 RFC3647 标准，这样使得使用和考虑使用 SNCA 服务的用户很容易实现证书策略的映射、比较、评估和操作。

1.1 概述

本证书策略为 SNCA 证书制定了要求，它负责管辖所有参与者的个人和实体。在本策略中 SNCA 和每个用户、合作伙伴都建立权威的可信任域。SNCA 的可信任域包括：下级实体，如客户、订户和可信赖方。对于一些 PKI 和数字证书的基础常识可登陆 http://www.snca.com.cn SNCA 的网站上查阅。在本网站中还提供公开密码技术和公钥基础设施方面的培训资料。

本策略中的数字证书是指由 SNCA 按照 CPS 定义证书 DN 后，预先在安全的存储介质（如 USBKey）中生成并植入的数字证书；订户申领该证书时，发证机构须对订户的身份进行审核，将证书的 DN 信息与订户的身份信息绑定，并与应用

系统进行关联。当证书与订户身份信息的绑定信息经发证机构和 SNCA 数字签名确认后，该数字证书方可生效。

此处的绑定是指将证书的 DN 信息与订户的身份信息（包括但不限于姓名、证件类型、证件号码）在数据库中建立对应的关系，以便使该证书对应确定的实体。

此外的关联是指将证书的 DN 信息与应用系统的信息（包括但不限于发证机构名称、应用系统类型等）在数据库中建立对应的关系，以便使该证书用于特定的应用当中。

SNCA 包括 3 类证书，对应不同的安全保障级别、信任级别。SNCA 证书策略描述了这三类证书如何符合三类应用的一般安全要求。除非特别说明，本证书策略的内容、要求、规定应适应于所有三类证书。

1.1.1 第 1 类证书

在 SNCA 信任域中，1 类证书是自然人证书，包括自然人身份证书，在网路通讯中标示证书持有者的个人身份，可以用于个人网上进行合同签订、订单、支付信息等活动中表明身份；自然人代码签名证书为独立软件开发人员提供对软件代码做数字签名的数字证书，可以有效确认开发者身份，防止软件代码被篡改。

1.1.2 第 2 类证书

第 2 类证书是设备证书，第 2 类证书包括：服务器证书和支付网关证书，它们主要用于提供网络信息认证确认访问者真实身份。

1.1.3 第 3 类证书

第 3 类是机构证书，包括：机构身份证书、机构岗位证书、机构业务证书、组织机构代码证书、企业代码签名证书。3 类证书用户提供的身份保证必须确认：订户组织机构确实存在，该组织机构授权证书申请，并且订户代表提交证书申请要获得授权审核。机构身份证书是以单位或机构作为可信实体对象，发放的“企业或机构身份证书”，简称“机构证书”。 机构岗位证书指以单位或机构内部岗位人员为实体对象，面向单位工作人员发放行使企业或机构内部岗位的用户证书，由单位工作人员持有，作为在网上行使“单位机构赋予单位工作人员（证书

持有人）相关权利”的真实身份证明。组织机构代码证书是在网上能够标识组织机构代码使用的证书。企业代码签名证书是为软件开发商提供的用以对其软件代码进行数字签名，以便用户下载时可以确信此代码开发者的真实身份，并且确信此代码在传输过程中没有被非法篡改和被破坏。

1.2 文档名称与标示

本文档的名称为《SNCA 证书策略（CP）》，已注册的对象标识符（OID）为：

●第 1 类 自然人证书策略 1.2.86.11.7.11

●第 2 类 设备证书策略 1.2.156.10260.4.1.4，

●第 3 类机构类证书策略 1.2.156.10260.4.1.3，1.2.156.10260.4.1.5，1.2.156.10260.4.1.6

这些标示符合于相应的本 CP 中的版本号相对应，CA 证书包括的对象标识符可能会略掉 CP 版本号，表明它们不受限于本 CP 的版本。

1.3 PKI 的参与者

1.3.1 电子认证服务机构

认证机构（Certification Authority,简称 CA）作为可信任第三方，对个人、实体及设备进行主题信息及其他属性与公钥绑定的确认。CA 是向最终用户或其下 CA 签发证书的实体术语。它的一个特列是根 CA。一个根 CA 是一类证书体系的最高层。在 SNCA 系统中有三类证书，对应于三类证书有三个根 CA。

1.3.2 注册机构（Registration Authority）

注册机构（Registration Authority，简称 RA）代表 CA 建立起注册过程，确认证书申请者的身份，批准或拒绝证书申请者。在用户获得证书前，它必须以申请者的身份来注册证书。证书申请者必须从 CA 或 RA 建立的注册过程来完成注册，并将注册信息提交给 CA 或 RA，CA 或 RA 将对申请者的身份及其它属性进行确认，然后决定是签发还是拒绝该请求。如果签发证书，则证书将被发送给申请者。RA 还可以根据用户需要吊销证书，尽管是 CA 的系统完成最终的吊销

工作，并将证书加入到证书吊销列表(“CRL”)中去，或是在 CA 信息库中显示证书已吊销。

1.3.3 受理点（Registration Authority Terminal,RAT）

经过 SNCA 审查，SNCA 授权特定单位或实体，负责办理和审批数字证书申请。数字证书申请手续、过程和要求，必须与 SNCA 正在实施的数字证书策略（CP），电子认证业务规则以及 SNCA 的 CA 受理点授权协议书相一致。受理点负责向 SNCA 或 SNCA 授权的注册机构提供证书申请实体的信息，包括申请实体的名称、可以表明身份的证件号码和联系方法（通信地址、电子邮件信箱、电话等），并为申请实体提供技术支持。

1.3.4 依赖方

证书依赖方是指在 SNCA 证书服务体系之内作为依赖于数字证书真实性的实体，在电子签名应用中，即为电子签名依赖方。依赖方可以是订户，但不仅限于订户。

1.3.5 证书种类和订户

从电子认证服务机构接收证书的实体。在电子签名应用中，订户即为电子签名人。指证书和证书相关服务的使用者。如 CP § 1.1.1-1.1.3 所描述的那样，SNCA 中有三类证书。个人或组织因其应用需要而申请证书。1 类证书是仅签发给个人最终订户的个人证书。2 类证书有些可以签发给个人，有些可以签发给组织机构，还有些可以签发给组织机构的服务器。3 类机构证书只可以签发给一个组织机构的相关个人，相关个人是指与组织机构相关的自然人，如主管、经理、职员、合伙者、合同契约者、实习者或有共同利益的成员。因此，3 类证书所对应的组织机构将作为注册机构。

1.3.6 其他参与者

指在 SNCA 证书应用体系和服务体系中除上述的电子认证机构、数字证书注册机构、数字证书受理点、证书持有者、证书依赖方、证书申请者之外的其他实

体，在 SNCA 用户证书申请审批过程中，有权威为第三方提供组织身份确认服务，或域名所有权的确认信息的实体。

1.4 证书应用

1.4.1 合适的证书应用

SNCA 拥有下表所述的数字证书类型。每个证书申请者可自由选择 SNCA 的证书类型。鉴于 SNCA 对不同类型证书所提供的服务及承担的义务也有所不同，因此SNCA采取不同的证书价格规定并已经过物价部门审批,发布在SNCA的网站上：Http://www.snca.com.cn 。 证书类型见下表：

1.4.1.1 自然人证书的应用

订户	证书类型	证书用途及说明
自然人	自然人身份证书	在网路通讯中标示证书持有者的个人身份，可以用于个人网上进行合同签订、订单、支付信息等活动中表明身份。
	代码签名证书	为独立软件开发人员提供对软件代码做数字签名的数字证书，可以有效确认开发者身份，防止软件代码被篡改。

1.4.1.2 设备证书的应用

订户	证书类型	证书用途及说明
设备	服务器证书	以信息设备作为可信实体对象，根据需要发放的数字证书，简称“服务器证书”，并以此作为网上设备真实身份的证明。
	支付网关证书	支付网关证书是支付网关实现数据加解密的主要工具，用于数字签名和信息加密，支付网关证书仅用于支付网关提供的服务（Internet 上各种安全协议与银行现有网络数

据格式的转换）。

1.4.1.3 机构证书的应用

订户	证书类型	证书用途及说明
机构	机构身份证书	以单位或机构作为可信实体对象，发放的“企业或机构身份证书”，简称“机构证书”。
	机构岗位（内部用户证书）	指以单位或机构内部岗位人员为实体对象，面向单位工作人员发放“企业或机构内部用户”证书，由单位工作人员持有，作为在网上行使“单位机构赋予单位工作人员（证书持有人）相关权利”的真实身份证明。
	机构业务证书	指单位或机构在网上进行某一项特定业务时使用的证书。
	组织机构代码证书	在网上能够标识组织机构代码使用的证书。
	企业代码签名证书	为软件开发商提供的用以对其软件代码进行数字签名，以便用户下载时可以确信此代码开发者的真实身份，并且确信此代码在传输过程中没有被非法篡改和被破坏。

1.4.2 限制的证书应用

禁止证书在任何违反国家法律法规或破坏国家安全的情形下使用，否则由此造成的法律后果由用户自己承担。

1.4.3 受禁用的使用

证书不设计用于、不打算用于、也不授权用于危险换进中的控制设备，或用于要求防失败的场合，如核设备的操作、航天飞机的导航或通讯系统、空中交通控制系统或武器控制系统中，因为它的任何故障都可能导致死亡、人员伤害或

者严重的环境破坏。

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》、工业和信息化部《电子认证服务管理办法》和《电子认证业务规则规范》的要求，SNCA 制定本认证证书策略（CP），并指定专门的机构—SNCA 运营策略委员会作为策略的管理机构。

SNCA 运营策略委员会，作为 SNCA 认证服务体系所有策略的制定管理机构，负责召集管理者、PKI 专家、法律顾问审核批准 CP，并作为 CP 实施检查监督的决定机构。

SNCA 运营管理部作为 CP 的工作机构，负责起草 CP 并根据要求提出修改报告，并负责此方面的对外咨询服务。

1.5.2 联系人

SNCA 将对电子认证服务规则进行严格的版本控制，并由 SNCA 指定专门的机构和人员负责相关的事宜。任何人有关 CPS 的问题、建议、疑问等，都可以与此联系人进行联系。

联系人： 陕西省数字证书认证中心有限责任公司运营管理部

地址：西安高新技术开发区高新三路九号信息港大厦七层

电话：029-88311561

邮编：710075

传真：029-88311503

电子邮址： yyglb@snca.com.cn

1.5.3 决定 CP 符合策略的机构

作为电子认证业务的主管部门，工业和信息化部发布了《电子认证业务规则规范》，SNCA 根据规范要求，制定本电子认证证书策略（CP），并提交工业和信息化部备案。SNCA 运营策略委员会作为策略管理机构，是 CP 符合策略的决定

结构。

SNCA 保证制定和发布的 CP，其执行、解释、翻译和有效性均遵循中华人民共和国的法律规定。

SNCA 运营策略委员会根据法律法规和本 CP 的要求，为用户解决证书使用时产生的争议。运营策略委员会收集相关的证据以促进争议解决，会同运营管理部协调 SNCA、当事人之间的相互关系，并作为建议报告的最终撰写人。

运营管理部作为 CP 的工作部门，保证 SNCA 认证服务体系的运行符合本 CP 的要求。

1.5.4 CP 批准程序

SNCA 的 CP 由运营管理部起草拟定后，提交 SNCA 运营策略委员会审核。如果因为标准的变化、技术提高、安全机制的增强、运营环境的变化和法律法规的要求等对 CP 进行修改，由运营管理部提交修改建议报告，提交 SNCA 运营策略委员会批准。

1.5.5 CP 发布

在 CP 修改审批之后，由运营管理部在 SNCA 网站 http://www.snca.com.cn 上公布变更后的 CP。对本 CP 所做的修改，将于 SNCA 发布之日起立即生效。所进行的修改将取代以往 CP 各版本中的任何冲突和指定条款。

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，SNCA 在公布 CP 后向工业和信息化部备案。

1.6 定义和缩写

1.6.1 定义

定义表

术语	定义
关联个人	与给定实体有一定合作关系的自然人。他可以是（1）政府的一名官员、该组织机构的主管、雇员、合伙人、合约人、

	实习人员或者其他人员；（3）也可以是和某实体保持一定关系的人员，该实体提供这个人身份担保的商业或其他记录
证书	是指一段信息，它至少包含了一个名字或标识特定的 CA，标识有关订户，包含了订户的公钥、证书有效期、证书序列号，及 CA 数字签名。
证书申请人	要求一个发证机关签发证书的个人或者组织机构。
证书申请	来自证书申请者(或证书申请者授权代理)的、要求 CA 签发证书的请求
证书链	一个有序的证书列表，包含了最终用户的证书和发证机关的证书，该列表最终证书为根证书。
证书策略	是指本证书策略文档，是一个有关 CTN 业务策略的主要说明。
证书吊销列表（CRL ）	一个定期(或根据要求)发行的、并由发证机关数字签名的信息列表，用来识别在有效期内提前被吊销的证书。这个列表通常标明 CRL 发布者的名字，发布的日期，下一次 CRL 发布的日期，被吊销证书的序列号，吊销证书的时间和原因。
证书签名请求	包含希望签发的证书请求的信息。
认证机构（CA）	一个授权签发、管理、吊销和更新证书的实体。
认证业务声明(CPS)	认证机构批准或拒绝证书申请，签发、管理和吊销证书时必须遵守的业务规则的描述。
一致性审计	一个处理中心、服务中心或客户要定期经历的审计，通过该审计确定它是否满足有关的 SNCA 标准。
安全损害	对安全策略的违反（或怀疑违反），包括出现敏感信息未经授权的泄漏或失去对其的控制。对于私钥，安全损害是指丢失、失窃、公开、修改、未经授权的使用或密钥受到的其它安全危害威胁。
服务器证书	3 类证书，用于支持浏览器和服务器之间的 SSL 会话。
知识产权	在版权、专利、商业秘密、商标和其他知识产权下拥有的权利。

密钥生成规程参考指南	描述密钥生成规程要求和业务操作的文档。
密钥生成规程	CA 密钥对产生、其私钥被传送到密码模块、私钥备份和签发它的公钥的过程。
未经验证的订户信息	指证书申请人提交给 CA 或 RA 的、包含在证书中的信息，但该信息未经 CA 或 RA 证实，因此 CA 或 RA 除确认该信息是由证书申请人提出外，对其它信息不作确认。
抗抵赖	一种提供通信保护的属性，它可以防止通信一方否认信息的出处，否认它已经提交或传送了这些信息。否认出处包括否认某一通信与先前的一系列消息源来自同一地方，即：使不知发送者是谁。注：只有法院的判决、仲裁或其它的裁决才能够最终阻止抵赖。例如，可用证书的数字签名是裁判所作出抗抵赖裁决的支持证据，但它本身不能够抗抵赖。
在线证书状态协议(OCSP)	为信赖方提供实时证书状态信息的协议。
操作期限	指从证书签发日期和时间（或者证书上指定的一个较晚的日期和时间）开始，到证书过期或被吊销时的日期和时间为止的这段时间。
PKCS #10	公钥密码标准#10，由 RSA 安全公司开发。它定义了证书签名请求的结构。
PKCS #12	公钥密码标准#12，由 RSA 安全公司开发。定义了私钥安全传送的方法。
公钥基础设施(PKI)	所有支持基于证书的公开密钥系统实施和操作的体系的组织机
注册机构(RA)	CA 批准的一个实体，它帮助证书申请者申请证书，批准或拒绝证书申请，吊销证书或更新证书。
依赖方	依赖一个证书和/或一个数字签名的个人或组织机构。
依赖方协议	一个 CA 使用的协议，这个协议规定了一个组织机构或个

	人成为依赖方的条款和条件。
RSA	由 Rivest, Shamir, and Adelman 发明的公钥密钥密码系统
秘密分割	根据秘密分割算法，将激活 CA 私钥需要的数据的分割成多个部分，使用多个分割可以恢复原激活数据。
安全套接层协议（SSL）	由保护 Web 通信的一个工业标准。SSL 为一个 TCP/IP 连接提供数据加密、服务器验证、信息完整性和可选的客户端验证等。
主题	与公钥对应的私钥的持有者。在组织机构证书中，主题指的是持有私钥的设备或装置。一个主题只有唯一的、确切的命名。它和该主题证书中的公钥绑定在一起。
订户	在个人证书的情况下，订户是指人，它是签发的证书的主题；在组织机构证书的情况下，订户是指组织机构，它是所签发证书的主题所对应设备或装置的拥有者。一个订户可以使用或被授权使用证书所含公钥对应的私钥。
订户协议	一个 CA 或 RA 拟定的协议，规定一个人或组织机构作为证书订户需要遵循的条款和条件。
可信人员	在认证机构的雇员、合同商或顾问，他们负责保证实体基础设施，及管理产品、服务、设施和业务的可信性。
安全可信系统	是指这样的计算机硬件、软件与程序，它能相当有效地避免入侵与滥用，提供合理程度的可用性、可靠性与正确操作保障，能恰当地完成预定功能，并实施适当的安全策略。安全可信系统不一定是政府信息系统分级中所定义的“可信系统”。
信息库	认证机构提供的、可在线访问的证书和其他证书有关信息的数据库。
陕西 CA（SNCA）	陕西省数字证书认证中心有限责任公司

1.6.2 缩略语

缩写表

缩写	全称（英文）	全称（中文）
ARL	JIT Authority Revocation List	授权注销列表
ACL	Access Cortrol List	访问控制列表
CA	Certification JIT Authority	认证权威
CP	Certificate Policy	认证策略
CPS	Certification Practice Statement	认证实施说明
CRL	Certificate Revocation List	证书注销列表
DAP	Directory Access Protocol	目录访问协议
DES	Data Encryption Standard	数据加密标准
DN	Distinguished Name	甄别名称
LDAP	Lightweight Directory Access Protocol	轻量目录访问协议
RA	Registration Authority	注册权威
RAT	Registration Authority Terminal	受理点
PKI	Public Key Infrastructure	公钥基础设施
RFC	(IETF)Request For Comments	请求注解（一种互联网建议标准）
RSA	Rivest-Shamir-Adleman	RSA 算法
SPKM	Simple Public-Key GSS-API Mechanism	简单公钥接口机制
SSL	Secure Sockets Layer	安全套接字层

2 信息发布与信息管理

2.1 信息库

SNCA 的 http://www.snca.com.cn 网站，认证系统的证书服务站点，LDAP、

CRL、OCSP 服务及注册机构的证书服务站点构成 SNCA 认证信息发布的信息库。

2.2 认证信息的发布

SNCA 将在目录或存储库中出版下列信息：

发布的所有证书；

证书注销表(CRL)；

电子认证业务规则(CPS)的拷贝；

它所发布的证书的其它相关信息。

2.3 发布的时间或频率

SNCA 的发布的认证信息，可以通过信息库 7*24 获得；

SNCA 签发的证书在最终用户收到证书之后都应立即发布；

SNCA 的 CRL（证书撤销列表）的更新频率，一般是 24 小时，在特别情况下将会根据实际情况实时发布和定期发布；

CPS 在改版后立即在网站(http://www.snca.com.cn)更新发布。

2.4 信息库访问控制

对于 CPS 中所述的认证信息的查询，获取是公开、没有限制的。SNCA 通过网络安全防护、系统安全设计、安全管理制度确保这些信息只有授权人员才能修改、发布。

3 识别与鉴别

3.1 命名

3.1.1 名称类型

根据实体的类型不同，SNCA 证书采用 X.509 定义的甄别名称（DN）标准来唯一标识，实体名字可以是姓名、组织机构名、域名、IP 地址等。

3.1.2 对名称意义化的要求

DN（Distinguished Name）：唯一甄别名，在数字证书的主体名称域中，用来唯一标识一个安全的证书。自然人证书和机构证书包含的命名应具有通常理解的语义，用它可以确定证书主题中的个人、机构的身份。使用假名是不允许的。

DN 的定义有特定的规则，并具有特定的意义，见本 CP7.1.4。

3.1.3 订户的匿名或伪名

订户不能使用匿名或伪名申请证书。

3.1.4 解释不同名称形式的规则

DN 的命名规则由 SNCA 定义，详见本 CP 7.1.4 的说明。

3.1.5 名称的唯一性

SNCA 保证签发的某个实体证书，其主题甄别名，在 SNCA 的信任域内是唯一的。

3.1.6 商标的识别、鉴别和角色

无。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

在证书业务中，SNCA 制订了严格的管理流程，从技术与制度上保证了在生成证书时，与此张证书相对应的私钥只留存在安全的存储介质中，不会留存任何备份。当订户申领证书时，发证机构须对其身份进行审核，并将证书的 DN 信息与订户的身份信息进行绑定，并与应用系统进行关联后，此证书才能被订户有效使用。此时，订户是其签名私钥的唯一持有者。SNCA 要求订户妥善保管自己的签名私钥。

3.2.2 组织机构身份的鉴别

组织机构订户在申领组织机构证书或组织机构拥有的设备等证书前应指定并授权证书的申领代表，接受证书申领的有关条款，承担相应的责任。对组织机构身份鉴证应该包括如下两个内容：

- 确认组织机构确实存在的、合法的实体。确认方式可以是，政府签发的组织机构的有效文件。
- 鉴别组织机构的身份时，指定证书申领者须向发证机构审核人员提供有效证明文件，在填写申领表时加盖企业公章以证明该申领的有效性。SNCA 授权的发证机构将复核并验证申领文件的真实性，并进行批准申领或拒绝申领的操作。

3.2.3 个人身份的鉴别

个人订户在申领证书前或在其它发证机构绑定新的应用前应持个人有效身份证件，包括：身份证、军官证、士兵证、护照、(以上可任择其一)，提出证书申领,并接受证书申领的有关条款，承担相应的责任，并进行批准申领或拒绝申领的操作。

3.2.4 没有验证的订户信息

无。

3.2.5 授权确认

确认证书申请时，必须通过可靠地途径确认申请者获得了所在组织机构的授权。SNCA 或发证机构有责任确认该授权信息，并将授权信息妥善保存。

3.2.6 互操作准则

订户在某个注册机构申领了 SNCA 签发的证书后，也可至 SNCA 授权的其它注册机构进行新的注册过程，将原有的证书与新的应用系统进行关联后，可实现一张证书在不同发证机构应用系统中的应用。

3.3 密钥更新请求的标识与鉴别

订户证书到期后，订户需对原有证书进行更新。在更新时产生一个新的密钥对代替过期的密钥对，称作“密钥更新”。在密钥更新时，证书的 DN 未改变。

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新密钥申请，订户须提交能够识别原证书的足够信息，如订户甄别名、证书序列号等，对申请的鉴别基于以下几个方面：

- 申请对应的原证书存在并且由认证机构签发；
- 用原证书上的订户公钥对申请的签名进行验证；
- 基于原注册信息进行身份鉴别。

3.3.2 吊销后密钥更新的标识与鉴别

证书吊销后不能进行重新申请密钥。

3.4 吊销请求的标识与鉴别

证书吊销请求可以来自订户，也可以来自认证机构、注册机构。证书吊销的方式可以是要求认证机构、注册机构吊销。批准证书申请时，认证机构有权发起吊销订户证书的操作。

订户通过认证机构吊销时，鉴别过程如下：

订户通过一定得方式，如传真、申请书等向认证机构提交请求，认证机构或注册中心通过相应的通讯方式与订户联系，确认要吊销的证书是订户本人。审核后为订户吊销证书。

4 生命周期操作要求

4.1 证书申请

4.1.1 提交证书请求

任何自然人、具有独立法人资格的企事业单位、社会团体等各类组织机构需

要在应用中进行基于数字证书的身份鉴别、需要采用数字签名及实现信息加密时，可向 SNCA 的发证机构提出证书申请。

个人证书由证书使用者本人提出申请；企业证书由企业、组织机构授权的人员申请。

4.1.2 注册过程与责任

1、最终订户

最终订户须明确表示其愿意接受订户协议中所规定的相关责任与义务，并需要提供真实、准确的申请信息；

2、发证机构

发证机构须与 SNCA 签订相关合同或合作协议。

在证书业务中，发证机构须对订户提交的资料进行审核，以决定是否为该订户发放证书；并须将证书的 DN 信息与订户的身份信息进行绑定、与应用系统进行关联后，此证书方可被有效使用。

4.2 证书申领处理

4.2.1 执行识别与鉴别功能

证书申领者向发证机构提交初始的证书申领请求，以及申请将证书关联新的应用时，发证机构须按照以下规定对订户的申领材料进行审查:

机构订户：参照 3.2.2 节的规定。

个人订户：参照 3.2.3 节的规定。

发证机构需要审查订户的证书申领表格是否按照要求填写、申领材料是否齐全、资质证明材料是否符合要求（如机构订户是否在申请表上加盖审核公章）。

4.2.2 证书申领批准和拒绝

发证机构对证书申领者提交的申领信息及身份信息进行鉴别，鉴别其是否完整、真实、有效。经鉴别符合要求后，将批准申领。如果申领者未能通过审核，发证机构将拒绝申领者的申领，并通知申领者。

4.2.3 处理证书申领的时间

发证机构将在合理的时间内完成证书申领处理。在申领者提交的资料齐全且符合要求的情况下，处理证书申领的时间不超过 5 个工作日。

4.3 证书签发

4.3.1 证书签发中发证机构和电子认证服务机构的行为

在证书的签发过程中 RA 的管理员负责证书申请的审批，并通过操作 RA 系统将签发证书的请求发往 CA 签发系统，证书签发的请求信息满足必须具有身份鉴别与信息保密措施，并确保请求发到正确的证书签发系统。

4.3.2 电子认证服务机构和发证机构对订户的通告

SNCA 签发证书后，对于其签发的证书会通过在线、电话等多种方式对订户进行通告。

发证机构在审核订户身份后，无论是拒绝还是批准订户的证书申请，发证机构有义务告知订户申请结果。

4.4 证书接受

4.4.1 构成接受证书的行为

当订户填写证书申请表，并提供真实、准确的身份信息经发证机构审核通过，并同意《证书服务协议》的约定，申领到证书后即视为订户已经接受此证书。

SNCA 通过面对面的受理方式提交用户证书。

4.4.2 电子认证服务机构对证书的发布

对于订户证书，CA 将证书发布到目录系统上，并通过 OCSP 发布到相应的应用服务数据库中，在绑定身份及关联信息后为用户提供安全机制向依赖方提供查询服务。

4.4.3 电子认证服务机构对其他实体的通告

证书与证书状态信息向其它实体进行通告。

证书关联的应用信息与绑定的身份信息不对其它实体进行通告。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户在使用私钥和证书时须遵循以下约定：

1、 订户只能在规定的范围内（在本 CP1.4 中定义）使用私钥和证书，并对使用行为承担责任；

2、 订户在使用证书时必须遵守《证书服务协议》及 CPS 和本 CP 的要求；

3、 订户应当妥善保存其私钥和证书，避免他人未经本人授权而使用本人证书情形的发生。

4.5.2 依赖方公钥和证书的使用

在依赖方接受数字签名信息后需要：

1、 获得数字签名对应的证书及信任链；

2、 确认该签名对应的证书是依赖方信任的证书；

3、 证书的用途适用于对应的签名；

4、 使用证书上的公钥验证签名；

5、 确认数字签名对应的证书状态正常，没有进入 CRL 列表。

以上任何一个环节失败，信赖方应该拒绝接受签名信息。

依赖方需要采用合适的软（硬）件进行数字签名的验证工作，包括验证证书链及链中所有证书的数字签名。

当依赖方需要发送加密信息给接受方时，须先通过适当的途径获得接受方的加密证书，然后使用证书上的公钥对信息加密。信赖方应将加密证书连同加密信息一起发送给接受方。

4.6 证书更新

在证书有效期内，证书订户的旧加密密钥丢失或损坏的情况下可以申请证书更新。证书更新的规定与证书密钥更新的相同。

4.6.1 证书密钥更新

每个证书都有有效期，在一个订户的证书到期前 30 天内或已到期 30 天内，如果订户的注册信息没有改变，订户可以申请证书更新。

在证书更新时，订户须提交能够识别原证书的足够信息，如订户甄别名、证书序列号、证书申请提交的注册信息等。

证书吊销后将不能更新。

4.6.2 证书密钥更新的情形

当订户证书即将到期或已经到期时应当进行证书密钥更新。由证书的订户、证书订户的授权代表（机构证书）或证书对应实体的拥有者（设备证书）可以要求更新证书。

4.6.3 请求证书密钥更新的实体

个人证书由证书使用者本人提出申请；机构证书由企业、组织机构授权的人员申请；设备证书由实体的授权拥有者申请。

4.6.4 证书密钥更新请求的处理

处理证书更新请求的过程包括申请验证、鉴别、签发证书过程。对申请的验证和鉴别基于以下几个方面：

申请对应的原证书是否为本认证机构签发；

用原证书上的订户公钥对申请的签名进行验证；

基于原注册信息进行身份鉴别；

审查通过后，发证机构进行密钥更新，并将装有已更新证书的存储介质返还给订户。

4.6.5 颁发更新证书时对订户的通告

证书更新完成后，当面将更新的证书交于用户。

订户向发证机构提出密钥更新申请时，发证机构在审核订户身份后，无论是拒绝还是批准订户的密钥更新申请，均有义务告知订户申请结果。

4.6.6 构成接受密钥更新证书的行为

当订户向发证机构提出证书更新请求，并提供真实、准确的身份信息经发证机构审核通过，发证机构将更新后的证书交还给订户，亦视为订户接受更新证书密钥的行为。

4.6.7 电子认证服务机构对密钥更新证书的发布

密钥更新后的证书会在更新的同时被 CA 机构发布到公开的信息库和指定的数据库中。

4.6.8 电子认证服务机构对其他实体的通告

密钥更新后的证书会在更新的同时被 CA 机构发布到公开的信息库和指定的数据库中，订户和依赖方可以在信息库上自行查询。

4.7 证书密钥再造

证书密钥再造即产生新的密钥对，使用与原证书一样的主题甄别名签发新证书。

4.7.1 证书密钥再造的情形

每个证书都有其有效期，在一个订户的证书到期前 30 天内或已到期 30 天内，如果订户的注册信息没有改变，订户可以申请证书密钥再生，证书密钥再造将使用新的公钥，订户吊销后不允许证书密钥再造。

4.7.2 谁能要求新公钥的认证

证书订户、证书订户的授权代表或证书对应实体的拥有者可以要求对新公钥的认证。

4.7.3 处理证书密钥再造要求

见 CP&3.3.1。

4.7.4 通知订户新证书签发

同 CP&4.3.2。

4.7.5 构成接受密钥再造证书的行为

同 CP&4.4.1。

4.7.6 CA 对密钥再造证书的发布

同 CP&4.4.2。

4.7.7 CA 通知其他实体证书的签发

同 CP&4.4.3。

4.8 证书修改

无。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

如有下列情况中的任何一种情况发生，则订户的证书将被吊销：

1)私钥失盗、篡改、未经授权的泄露和其他安全威胁；

2)证书主体违反了证书协议中的重要职责；

3)法律、规章或其他法律的改变；

4)政府行为；

5)其他超过个人控制的原因并且对他人信息构成威胁的；

6）订户在申请时提供的证明材料不真实；

7）SNCA 已经履行催缴义务后，订户仍未缴纳服务费。

吊销分为主动吊销和被动吊销。主动吊销是指由订户提出吊销申请，由发证机构审核通过后吊销证书的情形；被动吊销是指当发证机构或 CA 确认订户违反证书应用规定、约定或订户主体已经消亡等情况发生时，采取吊销证书的手段以停止对该证书的证明。当出现上述提到的第 1、2、5、6、7 种情况时，适用于被动吊销，第 3、4 种情况适用于主动吊销。

4.9.2 请求证书吊销的实体

在符合本 CP4.9.1 所述的情形下，请求证书吊销的实体与本 CP4.1.1 证书申请实体相同。

另外，发证机构或 SNCA 也可以在本 CP4.9.1 所述的情形下主动吊销订户的证书。

4.9.3 请求吊销的流程

最终订户吊销证书时可按以下流程进行：

1）订户（或其授权委托人）填写书面申请表并签名或盖章，同时提交相应的证明材料，向发证机构或关联过新应用的发证机构提出吊销证书请求。

2）接到吊销申请的发证机构，验证申请者身份及吊销理由的正当性，并对审核资料进行归档保存。

3）发证机构在验证吊销申请后吊销证书。

4）SNCA 及时将证书吊销信息发布到 SNCA 信息库中，并且吊销信息会及时通过订户电话、EMAIL 地址等方式通知订户。

4.9.4 吊销请求宽限期

当订户一旦发现出现 CP&4.9.1 中的情况时，应尽快提出吊销请求，从发现

需要吊销证书到向认证机构、注册机构提出吊销请求的时间间隔不得超过 24 小时。

4.9.5 电子认证服务机构处理吊销请求的时限

SNCA 收到吊销请求到审核完成，做出吊销决定并将吊销证书发布到信息库，全部工作应当在 24 小时内完成。

说明：订户在正式提出证书吊销申请后不得在交易中继续使用此证书，否则由此产生的后果，由订户自行承担。

4.9.6 依赖方检查证书吊销的要求

对于安全保障要求比较高并且完全依赖证书进行身份鉴别与授权的应用，信赖方在信赖一个证书前必须查询证书吊销列表确认该证书的状态。

4.9.7 CRL 发布频率

认证机构定时发布最新的证书吊销列表。证书吊销列表更新的时间间隔不超过 24 小时。

4.9.8 CRL 发布的最大滞后时间

证书从它被吊销到被发布到 CRL 上的滞后时间不超过 24 小时。

4.9.9 在线的吊销/状态查询的可用性

SNCA 提供在线的吊销/状态查询，该服务 7X24 小时可用。

4.9.10 在线的吊销查询要求

依赖方在信赖一张证书前须确定证书的状态，查询方式为检查 CRL 或 OCSP。

4.9.11 吊销信息的其他发布形式

除 CRL 与 OCSP 之外，尚无其它发布形式。

4.9.12 对密钥遭受安全威胁的特别处理要求

当订户发现、或有充足的理由发现其密钥遭受安全威胁时，应及时地提出证书吊销请求。

4.9.13 证书挂起

SNCA为用户提供证书挂起服务，用户在证书有效期内可以申请证书挂起服务，证书挂起期间用户不能正常使用用户证书。

4.10 证书状态服务

4.10.1 操作特征

认证机构提供的证书状态查询以网络服务的形式，让依赖方能够随时查询、下载。CRL 的发布频率和迟延必须符合 CP&4.9.7、4.9.8.OCSP 应能立即反映证书的当前状态。证书状态服务的提供应该使标准、通用的方式。对服务请求应该有合理的响应时间和并发处理能力。

4.10.2 服务可用性

SNCA 提供 7X24 小时不间断证书状态查询服务。

4.11 订购结束

以下三种情形将被视为订购结束：

1、 证书到期后即视为订购结束。

2、 在证书有效期内，订户主动提出对证书进行吊销视为订购结束，SNCA 将按照“证书吊销流程”处理订户申请。

3、 被动吊销视为订购结束。

4.12 密钥生成、备份与恢复

在证书业务中，SNCA 制订了严格的管理流程，从技术与制度上保证了在生成证书时，与此张证书相对应的私钥在存储介质中生成且只留存在存储介质中，

不会留存任何备份。

5 证书、证书吊销列表和在线证书状态协议

5.1 证书

依本证书策略签发的证书符合（a）ITU-T X.509V3（1997):信息技术-开放系统互连目录：认证框架（1997 年 6 月）标准；（b）RFC 3280：Iternet X.509 公钥基础设施证书和 CRL 结构，（c）《信息安全技术 公钥基础设施 数字证书格式》（GB/T 20518-2006)。证书包含基本域。

5.1.1 版本号

SNCA 签发的证书格式符合 X.509 V3 标准，这一版本信息包含在证书版本属性内。

5.1.2 证书扩展项

X.509 V3 证书的扩充部分主要包括以下 CP&7.1.2.1-7.1.2.8 中所述内容。

5.1.2.1 颁发机构密钥标识符

SNCA 最终订户证书及 CA 证书中包含颁发机构密钥标识符扩展项，当证书签发者包含主题密钥标识符扩展项时，颁发机构密钥标识符由签发证书的 CA 进行 SHA-1 散列运算后的值构成。

5.1.2.2 主题密钥标识符

当证书包含主题密钥标识符扩展项时，该值由证书主题的公钥产生。使用该扩展项时，其扩展域的 criticality 域设为 FALSE。

5.1.2.3 密钥用法

密钥用法指明已认证的公开密钥用于何种用途，该项定义遵照 RFC3280 之规定。

5.1.2.4 Basic constraints:基本限制

基本限制项用来标识证书的主体的密钥用法，没有标识 CA 可能存在的认证路径有多长，该项定义遵照 RFC3280 之规定。

5.1.2.5 CRL 分布点

系统签发的证书包含 CRL 的分发点扩展项，依赖方可根据该扩展项提供的地址和协议下载 CRL。

5.1.2.6 主题备用名称

无。

5.1.3 算法对象标识符

SNCA签发的证书符合RFC 3280标准，采用SHA-1 RSA算法签名。

5.1.4 名称形式

SNCA 签发的证书采用 X.509 定义的甄别名称（DN）标准来唯一标识一张证书使用者的身份信息。DN 必须包括以下部分：

DN 项：

C=CN

S=陕西省

L=XXX

O=XXX

OU=XXX

CN=XXX

详细说明：

C=CN(CN 表示中国)

S= （申请用户所属省份）

L=(申请用户所属地市，对于省政府各级部门、公务员以及设备，该项不填；对地市各级部门、公务员以及设备该项要填写;对于自然人申请者按实际地市填写；对于企业按其注册地填写即可)

O= （对政府机构、自然人、设备来说，

（1）.L 规定了所属地市，如果证书主体所属单位具有 L 管辖内明确的上一级单位则 O 为其上一级单位的全称；

（2）L 规定了所属地市，但证书主体所属单位不具有明确的上一级单位，则该项为证书主体所在地市的所属单位全称；

（3）L 没有值（意味着省级单位），如果证书主体所属单位具有明确的上一级单位，则 O 为其上一级单位的全称；

（4）L 没有值，且证书主体所属单位不具有明确的上一级单位，则该项为证书主体所属省级单位全称；）

OU=证书主体所属单位的全称。如果 O 已经是证书主体所属单位的全称，则 OU 可以空缺。

CN=(通用名称，

（1）自然人证书应为证书主体的姓名，姓在前，名在后，中间无间隔符。

（2）机构证书应是证书主体单位的标准全称；

（3）设备证书应是证书主体设备的域名或 IP；

（4）企业证书应为企业的标准全称)

5.1.5 名称限制

SNCA 签发的证书，其名称须严格按照 7.1.4 的规则来定义。

5.1.6 证书策略对象标识符

无。

5.1.7 策略限制扩展项的用法

未使用本扩展域。

5.1.8 策略限定符的语法和语义

未使用本扩展域。

5.1.9 关键证书策略扩展项的处理规则

未使用本扩展域。

5.2 CRL

同 CPS。

5.3 在线证书状态协议

同 CPS。

6 法律责任和其他业务条款

6.1 费用

6.1.1 证书签发和更新费用

陕西 CA 采用政府主导，企业运营的运行机制，向社会各界提供服务。对数字证书的发放、验证和管理实行有偿服务，用户有义务按照规定向陕西 CA 交纳相关费用。

陕西省物价管理部门已正式批准了陕西 CA 数字证书收费标准。陕西 CA 已在公司的网站（Http://www.snca.com.cn）上予以发布，如果陕西 CA 签署的协议中指明的价格和陕西 CA 公布的价格不一致，以协议中的价格为准。

6.1.2 证书查询费用

陕西 CA 目前没有对用户证书查询收取费用，陕西 CA 保留对用户证书查询操作进行收费的权利。

6.1.3 证书吊销或状态信息的查询费用

陕西 CA 目前没有对用户证书吊销或状态信息的查询收取费用，陕西 CA 保留对用户证书吊销和状态信息查询操作进行收费的权利。

6.1.4 其它服务费用

陕西 CA 保留收取其他服务费的权利。

6.1.5 退款策略

当用户对所收到的陕西 CA 签发的数字证书予以确认后，陕西 CA 不办理退证、退款手续。其它费用按照陕西 CA 与订户的商业合同执行。

9.2 财务责任

6.2.1 保险范围

对于操作中涉及的其它用户财务相关信息的保险，例如财务报表、担保合同、信用证明和各种权益证明，目前没有开设相应险种。

对于终端用户由于使用陕西 CA 证书服务造成的事故的保险和担保目前没有开设相应险种。

由于没有开设相应险种因此，目前没有保险。 如果在证书的使用过程中，因陕西 CA 的原因给订户造成的损失，陕西 CA 将向订户提供赔偿。

6.2.2 其他资产

无。

6.2.3 对最终实体的保险或担保

陕西 CA 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用户和证书依赖方。

6.3 业务信息保密

陕西 CA 根据国家相应的法律法规制定并落实严格的信息保密规章制度，所有相关人员（包括陕西 CA 及其业务代理机构的工作人员、证书持有者）必须遵守该规章制度。

6.3.1 保密信息范围

（1）保密信息包括陕西CA 和其授权的证书服务机构、陕西CA 与订户、陕西CA与其他证书服务相关方、陕西CA 关联实体之间的协议、往来函和商务协定等。除非法律明确规定和陕西CA 明确进行了书面许可，一般不能在未经另一方许可的情况下擅自公开。

（2）与证书持有者证书公钥配对的私钥是机密的，证书订户应该遵照本CPS的规定妥善保管，不能公布给未经授权的任意第三方。如果因证书订户泄露私钥，订户应自行承担一切责任。

（3）对陕西CA 或陕西CA 对关联实体的审计报告、审计结果等相关信息是机密信息，除了陕西CA 授权和信任的员工，不能泄露给其他任何人。这些信息除了审查目的或法律规定的目的，不能用于其他用途。

（4）有关陕西CA 认证系统的运营信息只能在严格指定的情况下，才能提供给经陕西CA 授权的员工，这种授权并不意味着对信息公开的授权。对陕西CA 来讲，所有涉及系统运营的信息，都在保密范围之内。

（5）除非法律明文规定，陕西 CA 没有义务，也不会公布或透露订户证书中已经包括的信息以外的任何信息；同时，陕西 CA 在与其授权的证书服务机构或其他形式的关联实体签署协议时，都将此作为必须满足的要求。

6.3.2 不属于保密的信息

以下信息可视为不保密信息

（1）与证书有关的申请流程、申请需要的手续、申请操作指南、证书收费价格等信息是可以公开的。而且陕西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。

（2）非保密信息还包括证书中包括的相关订户信息。证书中的订户信息是可以公开的。

（3）证书、证书内包括的公钥，供用户公开、自由查询和验证。

（4）证书被吊销的信息，属于公开信息，陕西CA 在目录服务器中公布这些信息。

（5）这些非保密信息，并不能够被任意不被授权的第三方使用，陕西 CA 和信息的所有人保留所有这些信息的相关权利。

6.3.4 保护机密信息的责任

陕西CA、其订户、关联实体以及与认证业务相关的参与方，都有义务按照本CPS 的规定，承担相应的保护保密信息的责任。

当陕西CA 在任何法律法规要求或者法院以及其它公权力部门通过合法程序的要求下，必须披露本CPS 中规定的保密信息时，陕西CA 可以按照法律、法规、或法规条令以及法院判决的要求，向执法部门公布相关的保密信息。陕西CA 无须承担任何责任。这种披露不能被视为违反了保密要求和义务。

当保密信息的所有者出于某种原因，要求陕西CA 公开或披露他所拥有的保密信息时，陕西CA 应满足其要求；同时，陕西CA 将要求该保密信息的所有者对这种申请进行书面授权，以表示其自身的公开或者披露的意愿。

如果这种披露保密信息的行为涉及任何其他方的赔偿义务，陕西 CA 不应承担任何与此相关的或由于公开保密信息所造成的损失。保密信息的所有者应承担与此相关的或由于公开保密信息引起的所有赔偿责任。

9.4 个人隐私保密

6.4.1 隐私保密方案

个人隐私保密方案遵守现行法律和政策。任何人选择使用陕西CA 的任何服务，那么就表示已经同意接受陕西CA 有关隐私保护的声明。

6.4.2 作为隐私处理的信息

陕西 CA 在管理和使用订户提供的相关信息时，除了证书中已经包括的信息外，该订户的基本信息和身份认证资料，都将被作为隐私处理，非经订户同意或者法律法规及公权力部门的合法要求，不会任意对外公开。

6.4.3 不被视为隐私的信息

证书中的信息及证书状态是可以公开的，通过陕西 CA 目录服务等方式向外公布。

6.4.4 保护隐私的责任

个人有保护自己和其他人员或单位的机密信息的责任，并保证不泄露给第三方。

除非司法方面的强制需要，陕西 CA 及其注册机构在没有获得客户授权的情况下，不得将客户隐私信息透露给第三方。

9.4.5 使用隐私的告知与同意

在客户书面授权下可以使用私密信息，只用于订户身份识别、管理、和服务订户的目的。陕西 CA 在任何法律法规或者法院以及公权力部门通过合法程序的要求下向特定对象披露隐私信息时，没有告知订户的义务，并且不需得到订户的同意。

6.4.6 依法律或行政程序的信息披露

除非符合下列条件之一，否则陕西CA 不会将订户的保密信息和隐私信息提供给任何对象：

（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。

6.4.7 其它信息披露情形

当保密信息的所有者出于某种原因，要求陕西 CA 公开或披露其所拥有的保密信息，陕西 CA 应当满足其要求。如果这种保密信息的披露行为涉及或有可能引起对其他方的赔偿义务，陕西 CA 有权拒绝其要求，且不应该承担任何由此相关的或由于公开保密信息引起的损失和损坏的赔偿责任。保密信息的所有者应负责陕西 CA 与此相关的或由于保密信息公开引起的损失和损坏的赔偿责任。

6.5 知识产权

陕西CA享有并保留对证书以及陕西CA提供的全部软件的独一无二的一切知识产权，包括（所有权、名称权、利益分享权等）。

陕西 CA 对数字证书系统软件具有所有权、名称权、利益分享权。

陕西 CA 有权决定关联机构采用何种软件系统，选择采取的形式、方法、时间、过程和模型，以便保证系统的兼容和互联互通。

陕西 CA 网站上公布的一切信息均为陕西 CA 财产，他人不能转载用于商业行为。

陕西 CA 签发的证书、CRL、提供的软件、相关的文件和使用手册均属于陕西 CA 的知识产权范围。

陕西 CA 电子认证业务规则为陕西 CA 财产。

在没有陕西 CA 预先书面同意的情况下，证书持有者不能在任何证书到期、废止、或终止的期间或之后，使用或接受任何陕西 CA 使用的名称、商标、交易形式或可能与之相混淆的名称、商标、交易形式或商务称号。

证书申请人（于接受申请时即为用户） 声明并保证其交付（给陕西 CA） 使用的网域与辨识名称（及所有其它证书申请书的资料）不得在任何管辖区域内干预或侵犯第三人的商标、服务标志、商标名称、公司名称或其它知识产权等权利，而且不用于非法目的，包括侵害、干扰协议或预期的商业利益、不公平竞争、损害他人信誉及干扰或误导他人。

6.6 CA 的陈述与担保

6.6.1 陕西 CA 的陈述与担保

陕西 CA 享有的权利主要有以下方面：

（1）要求数字证书申请者提供真实资料的权利，有权按申请不同类型的数字证书，要求申请者提供不同的真实资料：对个人数字证书申请者、单位数字证书申请者、服务器数字证书申请者要求提供的有关资料。陕西 CA 或陕西 CA 授权的受理审核单位在遵循合法程序的条件下有权对上述内容进行调查、审核。

（2）根据业务发展的需要，有权委托相关法人单位作为业务受理审批单位（即业务受理点）从事数字证书的受理、数字证书用户的身份审核和发放等。

（3）有权提供不同类型的数字证书，满足不同的数字证书用户的不同需要。

（4）陕西 CA 有权向证书申请者颁发证书、撤销证书、发布证书注销列表等对证书操作的一系列流程，并为陕西 CA 制定出相关的规则。

（5）陕西 CA 有权根据国家相应的法律制定陕西 CA 法律责任书，并有权让证书用户遵守陕西 CA 的规定。

（6）陕西 CA 有权制定财务责任书，并有权让证书用户遵守陕西 CA 的规定。

（7）收取费用的权利：陕西 CA 有权向证书申请者收取费用。

（8）陕西 CA 在法律许可范围内可以有权对所有数字证书遭受破坏或盗用的情况协助调查，其调查包括但不限于面谈、记录与相关程序、相关设施的检查等。

（9）陕西 CA 对于下列情况之一，将有权主动废止所签发给证书持有者的证书：

- 发现证书申请人提供的材料真实性存在问题；
- 违反国家法律或者其它规章制度，不应签发证书的；
- 有盗用、冒用、伪造或者篡改他人证书的；
- 与证书中的公钥相对应的私钥被泄密；
- 证书中的相关信息有所变更；
- 由于证书不再需要用于原来的用途而要求终止；
- 用户未履行证书更新手续（该手续包括提出证书更新的书面申请，以及

按规定缴纳相关费用）；

- 其他情况。

（10）陕西 CA 有权确认：证书申请人确为证书申请书所说明的实体（依据证书类型描述的内容）；证书申请人合法地持有证书中所列的公开密钥所对应的私人密钥；除未经证实的证书用户资料外，证书中所记载的资料均准确无误，任何列有申请证书申请人公开密钥证书的代理人是经过合法授权提出申请的。

a） 当使用或信赖证书的证书依赖方或陕西 CA 的业务代理机构和雇员的违约行为或其他行为导致陕西 CA 发生任何损失、损坏或债务责任和法律费用以及成本损耗，陕西 CA 有权要求赔偿。

陕西 CA 对所担负的法律规范的有限责任做出如下承诺：

（1）陕西 CA 的运作遵守《中华人民共和国电子签名法》等法律，接受国家和地方信息产业主管部门和密码管理主管部门的领导。

（2）为进行网上业务的各方提供信息安全基础设施，并且经过国家有关管理机关鉴定和审批，合法许可经营。

（3）建立和执行符合国家政策的规定的安全机制，管理所拥有的信息安全基础设施并使其处于良好运行状态，并使陕西 CA 的签名私钥在陕西 CA 内部得到安全的存放和保护。

（4）对申请证书登记人的身份进行严格的审查和认证，保证发放的证书具有可靠的权威性和信任度，保证数字证书的真实有效性，即所发放数字证书中的公共密钥同某个确定身份的人是一一对应的。

（5）陕西 CA 有告知的责任，应向社会公开披露以下内容并保证该内容的准确完整：一是根证书；二是数字证书上所列明的数字信息；三是用户的公钥；四是认证业务操作规范（CPS）；五是废止名单（CRL）。

（6）负责证书签发和管理，包括控制实际的证书产生过程，证书的发布，证书的注销和证书的更新；及负责确保根据本电子认证业务规则的要求说明和做好与证书有关的服务、操作等各方面的工作。

（7）遵守陕西 CA 电子认证业务规则的规定，做好电子认证业务规则的版本管理与控制，对修订后的电子认证业务规则及时予以发布。

（8）陕西 CA 承诺使用陕西 CA 提供的数字证书与安全软件的用户的网上交

易信息对无关者是保密的，而且在网上传输中是不可篡改的。

（9）陕西 CA 承诺在现有技术条件下，除非陕西 CA 私钥丢失，陕西 CA 签发的数字证书不会被成功地伪造、篡改；如果由于陕西 CA 的私钥管理问题造成数字证书被伪造、篡改，陕西 CA 将承担相应责任。

（10）陕西 CA 承诺在现有技术条件下所采用的密码机制无法攻破。如果发生数字证书密码机制问题，而陕西 CA 没有及时采取应对措施，陕西 CA 将承担责任。

除上述的责任条款，陕西 CA、陕西 CA 的服务机构、陕西 CA 的授权发证机关、陕西 CA 的雇员不做任何其他保证和履行任何进一步的义务。

需要明确的是，本电子认证业务规则的内容，没有任何信息可以暗示或解释为陕西 CA 必须承担其它的义务或陕西 CA 必须对其行为做出其它的承诺。

6.6.2 注册机构的陈述与担保

注册机构以下简称 RA。RA 的职责是：

（1）RA 应遵守由陕西 CA 制定的所有运营政策、操作管理规范、规定登记程序和安全保障措施。陕西 CA 有权根据情况修改有关内容。

（2）RA 有责任验证申请人提供信息的准确性和可靠性。验证过程由 RA 审核执行，通过陕西 CA 制定的审核步骤，确定颁发的证书的有效性和真实性。

（3）RA 应使用陕西 CA 确定的信息传输协议和标准与陕西 CA 交换信息。

（4）RA 应承担因在 CPS 规定的用途外使用 RA 管理员证书所造成的损失的责任。

（5)对于陕西 CA 提供的属于陕西 CA 专有的技术、软件开发包只有使用权，并对其承担保密义务。无权将未经陕西 CA 授权的属于陕西 CA 独有的技术/产品以任何方式让第三方知道和使用，并应对泄密承担相应责任。

6.6.3 订户的陈述与担保

证书持有者（或证书用户）是陕西 CA 的客户，是接受电子认证服务的一方。

证书持有者应享有以下权利：

（1）获得有效合格的数字证书的权利：证书持有者在提供了符合要求的信

息资料并交纳相应费用后，有权利取得有效的、具有所需功能的数字证书。

（2）提出中止或废止数字证书的权利： 在前述的有关陕西 CA 应该中止或废止数字证书的条件下，证书持有者或其代理人有权提出中止或废止证书的申请。

证书持有者负有以下责任：

（1）证书持有者对其私钥应保持控制，采取合理的预防措施避免遭受破坏或盗用，并不得向未经授权的人泄露，确保私人密钥的安全，以防止任何遗失、泄漏、修改或密钥的未经授权使用。因私钥的不安全控制而造成的损失，由证书持有者承担。

（2）如果证书持有者的私钥出现问题，例如遗失、盗用、破坏或者泄密等，证书持有者应当在察觉后的第一时间内通知所有所能预见到的受证书影响的单位及个人，包括陕西 CA；同时向陕西 CA 申请吊销该证书。

（3）证书用户（即证书持有者）在申请证书时应真实陈述陕西 CA 颁发证书时要求其提供的事项，提供真实准确的信息作为证书申请材料。证书持有者应为其在证书中的错误陈述承担责任，并应承担因其所提供的申请信息侵犯他人权利而造成后果的责任。

（4）证书持有者应向陕西 CA 按时交纳服务费用以享受相关服务。

6.6.4 依赖方的陈述与担保

（1）证书依赖方须熟悉本电子认证业务规则以及和证书持有者证书相关的证书政策，还须了解和遵守证书的使用目的。证书依赖方必须确保证书的确用于预定的目的。

（2）证书依赖方在信赖证书持有者的证书前，必须根据相应的最新的证书废止列表（即 CRL）检查证书的状态，查明证书是否还在有效期内。

（3）当证书依赖方在网上进行电子商务时，有权审查自己或对方的证书是否在有效期内，是否已被列为“黑名单”，证书依赖方应该在做出决定是否相信某个证书之前，先查看证书状态，以确定该证书是否为有效的证书，然后再用该证书来确认该电子签名是否在证书有效期内，并对签名作验证，必要时有权向陕西 CA 联系和查询。

6.6.5 其他参与者的陈述与担保

具有与依赖方同样的责任与义务。

6.7 担保免责

陕西 CA 在与用户和依赖方签定的协议中，对于因用户或依赖方的原因造成的损害不承担赔偿义务。

对于由于数字证书、数字签名或根据陕西 CA 电子认证业务规则而提供或设计的任何其他交易或服务的使用、签发、授权、执行或拒绝执行而导致的或与之有关的任何间接性的、特别性的、附带性的、或结果性的损失，或任何利益损失、数据丢失，或其他间接性的、结果性的或惩罚性的损失，无论是否可以合理预见，陕西 CA 将不会对此承担任何责任。

具体免责条款如下：

（1）陕西 CA 不对由于客观意外或其它不可抗拒力事件造成的操作失败或延误承担任何损失、损坏和赔偿责任。

（2）陕西 CA 在签发数字证书之前，事先就与证书申请者签定电子认证服务协议，都有事先告知证书持有者的免责条款规定：陕西 CA 发放的各类型数字证书只能用于在网络上标识身份、加密数据、签名认证、保证网络安全通讯等相应证书规定的用途，不能作为其他任何用途，不承担任何形式的担保和义务，包括：任何销路担保；保证一定适用于特定目标的担保；以及提供的任何相关信息的精确性的承诺，和所有由于缺乏妥善管理和疏忽引起的责任。若证书持有者将其数字证书用于其他用途，陕西 CA 不承担任何责任。

（3）如果证书申请者故意或无意地提供不完整、不可靠或已过期的信息，而他又根据正常的流程提供了必须的审核文件，由此得到了陕西 CA 签发的数字证书，由此引起的经济纠纷由证书申请者全部承担，陕西 CA 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。

（4）与证书持有者公钥配对的私钥是保密的，证书持有者应当妥善保管，不得泄漏或交付他人。如因故意、过失导致他人知道或遭盗用、冒用、伪造或者篡改，证书持有者应当自行负责承担一切责任。

（5）陕西 CA 在进行身份认证或证书持有者下载数字证书时，将充分遵守

陕西 CA 的安全操作流程。如果由于非陕西 CA 自身的原因而造成的陕西 CA 设备故障、线路中断，导致签发数字证书错误、延迟、中断或者无法签发，陕西 CA 不负任何赔偿责任。

（6）陕西 CA 仅仅提供电子沟通或交易中签名的“不可抵赖”的依据，但并不对此承担法律责任等方面的约定。

（7）当陕西 CA 在任何法律、法规的要求下，必须披露本电子认证业务规则中具有保密性质的信息时，陕西 CA 可以依据法院的判定的要求，向执法部门公布相关的保密信息。此种信息披露不视为违反了保密的要求和义务。

（8）当保密信息的所有者出于某种原因，要求陕西 CA 公开或披露其所拥有的保密信息，陕西 CA 应当满足其要求。如果这种保密信息的披露行为涉及或有可能引起对其他方的赔偿义务，陕西 CA 有权拒绝其要求，且不应该承担任何由此相关的或由于公开保密信息引起的损失和损坏的赔偿责任。保密信息的所有者应负责陕西 CA 与此相关的或由于保密信息公开引起的损失和损坏的赔偿责任。

（9）陕西 CA 不对交叉认证的其他 CA 私钥遭到泄露、破坏而造成的损害承担任何赔偿责任。

（10）陕西 CA 不承担任何其他未经授权的人或组织以陕西 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。

a） 证书主体提交的并最终列入证书中的信息侵犯了他人的专利、商标、著作权、商业秘密或其他知识产权及其他任何权利， 陕西 CA 不承担任何责任。

b） 用户必须在证书失效前 20 天向 CA 中心或受理点提出证书更新请求，否则证书到期后将自动失效，陕西 CA 不对因用户使用被取消或过期证书而造成的损害承担任何责任。

c） 证书用户出于某种原因不希望继续使用数字证书时，应当立即到当地证书受理点申请废除数字证书。废除手续遵循各受理点的规定。陕西 CA 在接到废除申请后，在 24 小时之内正式废除用户的数字证书。陕西 CA 不对数字证书正式废除前造成的损害承担任何责任。

6.8 有限责任

根据《中华人民共和国公司法》、《中华人民共和国电子签名法》和其他法

律法规的规定，作为依法设立的有限责任公司，陕西CA在承担任何责任和义务时，只承担法律范围内的有限责任。

在本CPS 和陕西CA 与任何一方签订的协议中，陕西CA不做任何其他保证和履行任何进一步的义务。

6.9 赔偿

6.9.1 赔偿范围

在认证活动中产生的赔偿，都以本CPS 的规定为处理依据，法律法规另有要求的除外。

（1）陕西CA 的赔偿责任

- 在签发证书时，如果未按照本CPS 的规定进行处理，或者违反法律法规的要求而造成证书订户损失的，陕西CA 应承担赔偿责任。
- 因为操作人员恶意、故意或者疏忽，未按照本CPS 的规定办理证书的签发、吊销等请求，而造成证书订户损失的，陕西CA 应赔偿订户的损失。
- 因陕西CA 的根密钥出现问题，造成订户证书出现问题的，陕西CA 应赔偿相关的损失。
- 证书订户或者其它有权提出吊销证书的人提出吊销请求后，到陕西CA 将该证书吊销信息予以发布的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果陕西CA 按照本CPS 的规范进行了有关操作，陕西CA 不承担任何损害赔偿责任。
- 证书订户赔偿的追溯有效期限，按照有关法律法规的要求进行操作。

（2）注册机构（包括分理中心和受理点）的赔偿责任

- 注册机构及其操作人员没有妥善保管订户的注册和身份验证的相关隐私信息，而造成订户信息泄漏、被冒用、篡改或者任意使用导致产生损失的，注册机构应负担损害赔偿责任。
- 如果因为操作人员故意、恶意或者疏忽，没有按照本CPS 的规定办理证书服务注册，或者违反法律法规而造成订户损失的，注册机构应赔偿用户的直接损失，以及其他随之产生的附带损失和相关补偿。
- 因为注册机构的原因造成系统或者软件错误，未能在本CPS 规定的时间

内，将订户的证书申请、吊销、更新等请求信息发给陕西CA，而导致订户或者依赖方损失的，注册机构应负担所有的损害赔偿责任。

- 该类赔偿的追溯有效期限，按照有关法律法规的要求进行操作。

（3）订户的赔偿责任

- 订户申请注册证书时，因故意、过失或者恶意提供不真实资料，导致造成陕西CA 及其授权的证书服务机构或者第三方遭受损害的，订户应赔偿一切损害责任。
- 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知陕西CA 及其授权的证书服务机构，以及不当交付他人使用造成陕西CA 及其授权的证书服务机构、第三方遭受损害的，订户应承担一切损害赔偿责任。
- 订户使用证书或者依赖方信任证书的行为，有违反本CPS 及相关操作规范，或者将证书用于非本CPS 规定的业务范围的，订户或者依赖方应自行承担一切损害赔偿责任。
- 用户使用或信赖证书时，未能依照本CPS 等规范进行合理审核，导致陕西CA 及其授权的证书服务机构或第三方遭受损害的，应由该用户承担一切损害赔偿责任。
- 证书订户或者其它有权提出吊销证书的实体提出吊销请求后，到陕西CA 将该证书吊销信息予以发布的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果陕西CA 按照本CPS 的规范进行了有关操作，那么该证书订户必须承担所有损害赔偿责任。
- 陕西CA 与之签署的协议另有赔偿规定的，参照其规定。

6.9.2 赔偿限额

陕西CA 及其授权的发证机构，对所有当事人（包括但不限于订户、申请者、接受者或信赖方）的合计赔偿责任，陕西CA将按照赔偿责任不超过用户当年实际缴纳的SNCA数字证书年维护费10倍的原则予以赔付：

（单位：人民币元）：

序号	证书种类	赔偿责任上限
1	支付网关证书	20000 元
2	服务器证书	8000 元
3	企业或机构身份证书	5000 元
4	个人身份证书	500 元
6	企业或机构代码签名证书	1000 元
7	个人代码签名证书	300 元
8	机构业务证书	2000 元
9	机构岗位证书	2000 元

本条款限制适用于一定形式的损害，包括但不局限于任何人或实体（包括但不限于订户、证书申请者、接收方或信赖方）由于信任或使用陕西CA 签发、管理、使用或吊销的证书或已过期证书而导致的直接的、补偿性的、间接的、特别的、结果的、惩戒性的或意外的损害。

6.10 有效期限与终止

6.10.1 有效期限

陕西 CA 的 CPS 自发布之日起正式生效。CPS 中将详细注明版本号及发布日期。最新版本的 CPS 请访问陕西 CA 网站以获得，对具体个人不做另行通知。当新版本的 CPS 正式发布生效，则旧版本的 CPS 将自动终止。

6.10.2 终止

当陕西 CA 中止业务时，陕西 CA 的 CPS 也将自行终止。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。

6.10.3 效力的终止与保留

当陕西 CA 的认证业务终止时，其 CPS 也将自行终止，终止过程将严格按照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妥当安排，保证客户利益不受影响或将所受影响程度减少到最小。

当出现如内容修改、与适用法律相冲突， CPS、订户协议、依赖方协议和其它协议中的某些条款失效后，并不影响文件中其它条款的法律效力。

6.11 对参与者的个别通告与沟通

电子认证活动中的参与各方在进行通信时，要严格依照《中华人民共和国电子签名法》去执行，保证通信过程在法律上有效。

6.12 修订

6.12.1 修订程序

当出现以下情形时。陕西 CA 将对 CPS 进行修订：

（1）因相关法律法规要求而引起陕西 CA 业务规则发生改变。

（2）因相关技术条件变化而引起陕西 CA 业务规则发生改变。

（3）因其它原因而引起陕西 CA 业务规则发生改变。

CPS 修正的流程为：

（1）组建 CPS 修订小组；

（2）搜集各方意见和建议，包括用户和依赖方；

（3）CPS 修订小组提出修订意见；

（4）CPS 进行修改后报公司决策层批准；

（5）进行审议和生效，并通过公司网站或其它方式发布。

6.12.2 通知机制和期限

陕西 CA 会及时将修改并批准后的 CPS 通过公司官方网站进行发布，其网址为：http://www.snca.com.cn。在必要时，陕西 CA 会以其他方式通知有关各方。

6.12.3 必须修改业务规则的情形

根据法律、法规或公司业务情况决定。

6.13 争议处理

当陕西 CA 与订户或依赖方出现争议，如通过协商仍未能达成一致意见时，当事人有权将争议提交仲裁机构（约定为“西安仲裁委员会”），根据仲裁条例在时效内裁决。

6.14 管辖法律

陕西 CA 的电子认证业务规则（CPS）及协议中条款的制定均依从《中华人民共和国合同法》、《中华人民共和国电子签名法》以及中华人民共和国相关法律。

9.15 与适用法律的符合性

陕西 CA 的各项策略的执行、解释、翻译、和有效性均适用中华人民共和国法律法规和国家信息安全主管部门要求。 法律的选择是确保对所有用户有统一的程序和解释，而不论他们在何地居住以及在何处使用证书。

6.16 一般条款

6.16.1 完整协议

CP、CPS、订户协议、依赖方协议及其它补充协议将构成陕西 CA 信任域参与者之间的完整协议。现行条款完全替代所有以前或同时期的、与相同主题相关的书面或口头解释的条款。

6.16.2 转让

陕西 CA、注册机构、订户及依赖方之间的责任、义务不能通过任何形式转

让给其他方。

6.16.3 分割性

在法律允许的范围内，当陕西 CA 订户协议、依赖方协议及其它补充协议内出现可以同其它条款分割的条款时，协议中的可分割条款的无效不应导致协议中其它条款无效。

6.16.4 强制执行

合同一方或几方不履行合同条款的，其它相关方可以依法要求强制执行。

可以声明在合同纠纷中有利的一方有权将代理费作为偿还要求的一部分，或者声明免除一方对合同某一项的违反应该承担的责任，但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。

6.16.5 不可抗力

由于不可预见的原因和不可控的原因，视为不可抗力，会导致合同或协议的终止。例如战争、恐怖行动、罢工、自然灾害、供货商或代理商倒闭、互联网或其它基础设施无法使用等。但各方都有义务建立灾难恢复和业务连续性机制。

6.17 其他条款

若本电子认证业务规则与其它规定、指导方针相互抵触，用户必须接受本电子认证业务规则的约束，除非本电子认证业务规则的规定在法律禁止的范围之内，或有关规定、指导方针明确地言明优于本电子认证业务规则。

在陕西 CA 与包括用户在内的其它方签订的仅约束签约双方的协议中，对协议中未约定的内容，均视为双方均同意按本电子认证业务规则的规定执行；对协议中不同于本电子认证业务规则内容的约定，按双方协议中约定的内容执行。