陕西省数字证书认证中心股份有限公司
SHAANXI CERTIFICATE AUTHORITY CO.,LTD

陕西 CA
电子认证业务规则

版本 4.0
（生效日期：2020 年 9 月）

陕西省数字证书认证中心股份有限公司

陕西 CA 电子认证业务规则

陕西省数字证书认证中心股份有限公司版权所有

版权声明

陕西省数字证书认证中心股份有限公司，陕西省西安市高新技术产业开发区高新三路九号信息港大厦七层（710075）

联系电话：029-82300561，传真：029-88311503

电子邮件：yyglb@snca.com.cn

陕西 CA 电子认证业务规则修订表

版本	发布日期	备注
1.0	2002 年 11 月 1 日	采用 RFC3647 结构
2.0	2005 年 7 月 26 日	根据《电子认证业务规则规范（试行）》修订
3.0	2006 年 9 月	根据《电子认证业务规则规范（试行）》修订 《中华人民共和国电子签名法》 《电子认证服务管理办法》 《RFC3647》
3.1	2008 年 10 月	由于实际操作策略发生变化，需要进行修改
3.2	2018 年 6 月	由于增加了移动端证书（手机盾证书），需要进行修改，修改章节：1.1.2、1.4.1、4.1.2、4.2.1、4.4.1、4.6.3、4.6.4、4.6.5、4.9、7.1.1.4、9.1.1
4.0	2020 年 8 月	增加了云签证书、事件型证书，修改章节：1.4.1、2.1、3.2、第 4 章节、第 6 章节

目　　录

1 概括性描述

1.1 概述

1.1.1 电子认证业务规则

陕西 CA 电子认证业务规则（CPS，Certification Practice Statement）是陕西 CA 对所提供的全部证书服务生命周期中的业务实践（如签发、管理、吊销、更新证书或密钥）所遵循的规范的详细描述和声明，包括责任范围、作业操作规范和信息安全保障措施等内容，是证书管理、证书服务、证书应用、证书分类、证书授权、证书责任等政策规则的集合，陕西 CACPS 的编制遵从依据《电子认证业务规则规范（试行）》，遵从《中华人民共和国电子签名法》，中华人民共和国信息产业部《电子认证服务管理办法》及《RFC3647 公钥基础设施证书策略和证书运行框架》，主要由以下几部分组成：

（1）概括性描述

（2）信息发布与信息管理

（3）身份标识与鉴别

（4）证书生命周期操作要求

（5）认证机构设施、管理和操作控制

（6）认证系统技术安全控制

（7）证书、证书吊销列表和在线证书状态协议

（8）认证机构审计和其他评估

（9）法律责任和其他业务条款

陕西 CA 认证体系内的实体以及陕西 CA 数字证书持有者，必须完整地理解和执行陕西 CA 电子认证业务规则所规定的条款，承担相应的责任和义务。

该业务规则适用于电子认证服务。

1.1.2 陕西省数字证书认证中心

陕西省数字证书认证中心（简称陕西 CA，英文名 Shaanxi Digital Certificate Authority， 英文简称 SNCA）是依法设立的权威第三方认证机构，2005 年 8 月 19 日，获得全国首批由中华人民共和国信息产业部颁发的电子认证服务许可证。

陕西 CA 的主要业务内容包括：

（1）制作、签发、管理数字证书；

（2）对签发的数字证书的真实性进行验证；

（3）提供数字证书目录查询服务；

（4）其他经主管部门核准办理的业务；

（5）为政务部门提供数字证书统计、查询、下载等支持服务，以及与电子政务系统的数字证书应用集成支持服务；

（6）提供数字证书相关培训；

（7)实现证书基于移动终端的应用，使用户可以在手机端直接进行实名认证、证书申请、扫码登录、扫码签名，以及直接进入相关应用系统进行单点登录等功能应用

利用陕西 CA 签发的数字证书以及相关 PKI 技术可以实现以下功能：

（1）能够确认数据电文签署人的身份；

（2）能够保证数据电文在传递、接收和储存过程中的完整性；

（3）能够避免系统被侵入或者人为破坏以及数据电文被篡改；

（4）能够保证网络信息的安全加密、解密。

1.2 文档名称与标识

1.2.1 文档名称

本文档名称:《陕西 CA 电子认证业务规则》。(陕西 CA CPS)，版本编号为 4.0。

本电子认证业务规则在陕西 CA 的网站上予以发布：http://www.snca.com.cn。

1.2.2 标识

“陕西 CA”是陕西省数字证书认证中心股份有限公司的缩写。

1.3 电子认证活动参与者

本文中所包含的电子认证活动参与者有：电子认证服务机构、注册机构、订户、依赖方以及其它参与者，下面将分别进行描述。

1.3.1 电子认证服务机构

电子认证服务机构 CA（Certification Authority）承担证书签发、更新、吊销、密钥管理、证书查询、证书黑名单（又称证书吊销列表或 CRL）发布、政策制定等工作。

陕西 CA 是依法设立的权威的第三方电子认证服务机构。

1.3.2 注册机构（Registration Authority）

注册机构 RA(Registration Authority)负责订户证书的申请受理、审批和管理，直接面向证书订户，并负责在订户和 CA 之间传递证书管理信息。

CA 可以授权下属机构或委托外部机构作为注册机构，但必须陕西 CA 与合作机构签署协议，合作机构可成为陕西 CA 的注册机构，并遵照陕西 CA 的管理办法开展数字证书业务。

1.3.3 依赖方

依赖方是指信赖于证书所证明的基础信任关系并依此进行业务活动的实体。

1.3.4 订户

订户是指向 CA 机构申请数字证书的实体。

需要明确的是，证书订户与证书主体是两个不同的概念。“证书订户”是指向陕西 CA 申请证书的实体，通常为个人或机构；“证书主体”是指与证书信息

绑定的实体,服务器证书中的“证书主体”通常是指受信任的服务器或用于确保与某一机构安全通信的其它设施。证书订户需要承担相应的责任与义务,而证书主体则是证书所要证明的可信赖方。

1.3.5 其他参与者

其他参与者指为 CA 证书服务体系提供相关服务的其他实体。

1.4 证书应用

1.4.1 适合的证书应用

陕西 CA 签发的证书按照应用安全级别和应用场景分成五大类证书。

通用证书适合应用在企业信息化、电子政务和电子商务等领域,用于证明订户在电子化环境中所进行的身份认证和电子签名以及数据加密等服务。证书类型包括:自然人证书和机构证书。

自然人证书,包括个人用户证书,用于区分、标识、鉴别个人身份的场景,适用于个人身份认证和电子签名,以及数据加密等服务。

机构证书,包括机构单位证书和机构法人证书,用于需要区分、标识、鉴别机构身份的场景,适用于机构身份认证和电子签名,以及数据加密等服务。

具体如下表:

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。
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。

设备证书包括各种设备证书和域名证书，用于标识各种设备身份，实现设备身份认证以及交互数据的加解密，保证传输数据的完整性和安全性等。

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）。

手机盾证书是基于密钥分割的软件密码模块产生的证书，适合应用在移动互联网、云服务和传统业务等各领域，用于证明订户在移动化和云服务环境中所进行的身份认证与电子签名。

云证书是由云端密码设备产生的证书，由订户自主掌控，适合应用在移动互联网、云服务和传统业务等各领域，用于证明订户在移动化和云服务环境中所进行的身份认证与电子签名。

事件证书是一种适合对即时业务和特定场景业务签名认证的一次性数字证书，脱离场景该证书就不能使用。适合应用在企业信息化、电子政务和电子商务等领域，用于证明业务场景中所进行的电子签名行为。事件证书只用于一次性事件型电子签名场合。

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。

1.5 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，陕西CA制定本电子认证业务规则（CPS），并指定专门的机构—陕西CA运营策略委员会作为策略的管理机构。

陕西CA运营策略委员会，作为陕西CA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CPS，并作为CPS实施检查监督的决定机构。

陕西CA运营管理部作为CPS的工作机构，负责起草CPS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

陕西CA将对电子认证服务规则进行严格的版本控制，并由陕西CA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股份有限公司运营管理部

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 CPS 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》，陕西CA根据规范要求，制定本电子认证业务规则（CPS），并提交工业和信息化部备案。陕西CA运营策略委员会作为策略管理机构，是CPS符合策略的决定结构。

陕西CA保证制定和发布的CPS，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。

陕西CA运营策略委员会根据法律法规和本CPS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陕西CA、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CPS的工作部门，保证陕西CA认证服务体系的运行符合本CPS的要求。

1.5.4 电子认证业务规则的发布

电子认证业务规则的发布方式包括：

陕西 CA 网站发布，网站地址：http://www.snca.com.cn

纸介质发布：

联系人：陕西省数字证书认证中心股份有限公司运营管理部

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

1.5.5 电子认证业务规则的变更

陕西 CA 有权对 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，在规定的时间内向工业和信息化部进行备案。

在本 CPS 做出任何变动之前，陕西 CA 运营策略委员会将对运营管理部提供变更建议报告进行研究，最终做出变更决定。

1.5.6 CPS 批准程序

陕西 CA 的 CPS 由运营管理部起草拟定后，提交陕西 CA 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 CPS 进行修改，由运营管理部提交修改建议报告，提交陕西 CA 运营策略委员会批准。

1.5.7 CPS 发布

在 CPS 修改审批之后，由运营管理部在陕西 CA 网站 http://www.snca.com.cn 上公布变更后的 CPS。对本 CPS 所做的修改，将于陕西 CA 发布之日起立即生效。所进行的修改将取代以往 CPS 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，陕西 CA 在公布 CPS 后向工业和信息化部备案。

1.6 定义和缩写

1.6.1 陕西 CA

陕西省数字证书认证中心股份有限公司

1.6.2 定义

（1）公钥基础设施（PKI）：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）电子认证服务机构（CA）：受用户信任，负责创建和分配公钥证书的权威机构。

（3）注册机构（RA）：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）。

（4）数字证书（Digital Certificate）：也称公钥证书，由电子认证服务机构（CA）签名的包含公开密钥拥有者信 息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

（5）证书撤销列表（CRL）：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，也称黑名单服务。

（6）CA 注销列表（ARL）

一个经电子认证服务机构数字签名的列表，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。

（7）证书策略（CP，Certificate Policy）：是关于电子认证服务机构制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。

（8）电子认证业务规则（CPS）：关于电子认证服务机构在证书签发、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。

（9）私钥（Private key）：非对称密码算法中只能由拥有者使用的不公开密钥。

（10）公钥(Public key)：非对称密码算法中可以公开的密钥。

（11）唯一甄别名(DN ，Distinguished Name)：在数字证书的主体名称域中，用来唯一标识用户的 X.509 名称。此域需要填写反映用户真实身份的、具有实际意义的、与法律不冲突的内容。

（12）身份标识（ID）

应用中的身份标识号码，也称为序列号或账号，是某个应用中相对唯一的编码，在应用中相当于是一种“身份标识”，身份标识号一般是不变的，至于用什么来标识该“身份标识”，则由证书应用机构自己制定的规则来确定。

1.6.3 缩略语

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

本 CA 机构的信息库面向订户及依赖方提供信息服务，提供的信息服务包括

但不限于以下内容：LDAP、OCSP、CPS、CP 及陕西 CA 不定期发布的信息，其中 OCSP 以接口形式提供，OCSP、LDAP 访问地址：

OCSP 地址:117.32.132.74 port 49520

LDAP 地址:117.32.132.74 port 49500

2.1.1 认证信息的发布

证书状态可以通过 CA 机构的 OCSP 和 CRL 获得，《电子认证业务规则》发布在公司的网站上，供相关方下载、查阅。公司网址：www.snca.com.cn

2.2 发布的时间或频率

本CA机构的CPS按照1.5.7所述的批准流程，一经发布到公司网站，即时生效。

2.3 信息库访问控制

对于公开发布的CP、CPS和CA证书等公开信息，陕西CA允许公众自行通过网站进行查询和访问。

3 身份标识与鉴别

3.1 命名

3.1.1 名称类型

根据实体的类型不同，陕西 CA 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

陕西CA签发的最终订户证书的命名具有通常理解的语义，用它可以确定证书使用者的身份，同时根据证书应用范围和协议确定证书名称，以方便证书应用系统使用者使用。

陕西CA证书主体甄别名属性

属性	值
Country(C)	国家
Organazation(O)	组织、机构
Organization Unit(OU)	组织机构 陕西CA证书中可以包含多个OU属性 （1）组织部门名 （2）组织身份证明文件号 （3）一个引用依赖方协议的声明，该协议明确了使用证书的条款
State or Province(S)	省
Locality(L)	市
Common Name(CN)	通用名 域名或IP（服务器证书） 个人名称（个人证书、代码签名证书） 单位名称（单位证书、代码签名证书）

3.1.3 订户的匿名或伪名

陕西 CA 中心不允许订户使用匿名或假名。

3.1.4 理解不同名称形式的规则

DN 的命名规则由陕西 CA 定义，详见本 CPS 7.1.4 的说明。

3.1.5 名称的唯一性

在陕西CA所签发的数字证书中，用DN （Distinguished Name）项来唯一标识用户的证书名称。用户申请证书时，证书系统会自动对其唯一性进行审核。如果不能通过唯一性审核，证书系统将拒绝签发证书。

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

证书类别	证明拥有私钥的方法
通用证书	通过证书请求中所包含的数字签名来证明证书申请人持有与注册公钥对应的私钥。 在陕西 CA 证书服务体系中，私钥在用户端生成，证书请求信息中包含用私钥进行的数字签名，CA 用其对应的公钥来验证这个签名。 陕西 CA 要求证书申请人妥善保管自己的私钥，因此，证书申请人视作其私钥的唯一持有者。
设备证书	通过证书请求中所包含的数字签名来证明证书申请人持有与注册公钥对应的私钥。
手机盾证书	通过证书请求中所包含的数字签名来证明证书申请人持有与注册公钥对应的私钥。 在手机盾证书服务体系中，私钥在订户终端和服务云端共同计算生成，基于密钥分割的软件密码模块，证书请求信息中包含用私钥进行的数字签名，CA 用订户终端和签名服务云端共同计算生成的公钥来验证这个签名，视作申请人为其私钥的拥有者。
云证书	通过证书请求中所包含的数字签名来证明证书申请人持有与注册公钥对应的私钥。 用户移动终端和云服务端的密码设备协同产生，用户移动终端和云服务端各自加密保存部分密钥因子
事件证书	通过证书请求中所包含的数字签名来证明证书申请人持有与注册公钥对应的私钥。 本 CA 机构在签发证书前，系统将自动使用订户的公钥验证其私钥签名的有效性和申请数据的完整性，以此来判断证书使用者拥有私钥。

3.2.2 组织机构身份的鉴别

对于组织身份的鉴别,CA 机构或授权的注册机构需要验证组织的合法证件。证书申请人需持营业执照（或组织机构代码证、社会团体登记证、事业单位登记证）等有效证件，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 CA 机构或授权的注册机构提交域名证明文件。

身份鉴别可通过现场鉴别或在线鉴别。所有证书类型的身份鉴别都遵循本规则。

现场鉴别方式：

用户需携带数字证书申请表、营业执照（副本）原件及复印件（或组织机构代码证、社会团体登记证、事业单位登记证等）、经办人身份证原件及复印件、经办人授权证明（法人授权书或在申请表加盖公章），客服人员需要核对营业执照及经办人身份证原件。

在线鉴别方式：用户在线填写组织身份信息及法人信息，提交营业执照（副本）复印件、授权证明、经办人身份证复印件等，系统自动通过工商库、手机运营商库验证法人信息的真实性，并通过给法人手机发送证书办理的短信通知以确保法人的真实意愿；针对经办人信息通过微信刷脸认证或手机实名认证+手机动态验证码验证经办人信息的真实性。用户提交资料、身份验证通过之后，系统自动生成 PDF 申请表由经办人完成在线签署，以确保经办人的真实意愿并留存申请表电子版文件。

审核通过后进行批准申请或拒绝申请的操作。CA 机构或注册机构将妥善保存用户提交的申请资料及电子材料。

3.2.3 个人身份的鉴别

个人身份的鉴别可以使用有效的身份证件，包括但不限于：身份证、港澳台居民身份证、户口簿、护照、军官证等。

个人或授权的代办人需持上述个人或代办人有效身份证件和授权，到CA机构或授权的注册机构提交数字证书申请表和上述有效身份证件的复印件等申请资

料。个人身份的鉴别除采用受理点现场鉴别外，可通过在线电子化的方式进行鉴别。CA机构或授权的注册机构通过公安库、运营商库、银联库、刷脸认证、手机动态验证码几种手段的结合使用来进行身份核验。

CA机构或授权的注册机构按照CA审核流程对申请资料的原件、复印件或电子材料真实性进行审核，在线鉴别采用有效的自动化审核方式。审核通过后进行批准申请或拒绝申请的操作。CA机构或注册机构将妥善保存用户的申请资料及电子材料。

3.2.4 没有验证的订户信息

无。

3.2.5 授权确认

代表个人：在 CA 机构的数字证书申请表上写明代办人的身份信息并签名确认后，则证明本人对代办人的授权。

代表组织：组织授予经办人的委托授权书或组织在 CA 机构的数字证书申请表上或经办人身份证复印件上加盖单位公章后，则证明本组织对经办人的授权确认。

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。

陕西 CA 将根据业务需要，在遵循本《电子认证业务规则》的各项控制要求的基础上，与 CA 的证书服务体系中未涉及的其他电子认证服务机构建立交叉认证关系。但交叉认证并不表示本 CA 机构批准了或赋予了其他 CA 中心或电子认证服务机构的权力。

3.3 密钥更新请求的标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

订户在证书有效期内且证书未被撤销的情况下提出密钥更新请求，视为常规密钥更新请求。

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。

除事件证书外，所有证书在常规密钥更新中，都是通过使用订户当前有效私钥对包含新公钥的密钥更新请求进行签名，CA 机构使用订户原有公钥验证确认签名来进行订户身份标识和鉴别。

事件证书只适用于一次性签名事件，没有证书密钥更新服务。

3.3.2 吊销后密钥更新的标识与鉴别

订户在证书吊销后申请密钥更新时，按照初始证书申请流程重新申请。

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。

订户通过认证机构吊销时，鉴别过程如下：

订户通过一定的方式，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。

如果是因为订户没有履行本《证书策略》、《陕西CA电子认证业务规则》《数字证书用户协议》所规定的义务，由陕西CA机构或授权的注册机构申请吊销订户的证书时， 不需要对订户身份进行标识和鉴别。

4 证书生命周期操作要求

4.1 证书申请

证书的申请可以采用两种方式：现场面对面申请及在线自助申请。

4.1.1 证书申请实体

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，可向陕西 CA 的注册机构提出证书申请。

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 证书申请过程与责任

订户按照本《电子认证服务规则》所规定的要求，通过现场面对面或在线方式提交证书申请，包括相关的身份证明材料。CA 机构或注册机构应明确告知证书用户所需承担的相关责任和义务，订户表达申请证书的意愿后，CA 机构或注册机构依据身份鉴别规范对订户的身份进行鉴别，并决定是否受理申请。

订户需要提交的资料及鉴别方式参照本文档 3.2。

申请过程中各方责任为：

订户要按照陕西 CA《证书策略》和《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。

陕西 CA 和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。在线申请信息通过权威第三方提供的服务进行一致性查验。

根据《中华人民共和国电子签名法》的规定，证书申请人未向 CA 机构提供真实、完整和准确的信息，或者有其他过错，给 CA 机构或电子签名依赖方造成损失的，应承担相应的法律责任和经济赔偿。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

CA机构或授权的注册机构按照本《电子认证业务规则》所规定的身份鉴别流程对申请人的身份进行识别与鉴别。具体的鉴别流程详见§ 3.2初始身份确认。

4.2.2 证书申请批准和拒绝

注册机构完成对证书用户申请的鉴定，并在申请者同意了证书使用应履行的责任后，予以批准申请，发放证书。如果鉴证未通过或用户拒绝履行应尽的责任，则会拒绝申请。被拒绝的证书申请者可随后再次提出申请。

4.2.3 处理证书申请的时间

在申请者提交的资料齐全且符合要求的情况下，处理证书申请的时间不超过5个工作日。

4.3 证书签发

4.3.1 证书签发中注册机构和电子认证服务机构的行为

注册机构审核申请用户的身份和资料的真实性，批准申请或拒绝申请，并用安全方式将用户证书 DN 发送到陕西 CA 中心签发系统。

认证服务机构对提交得用户 DN 信息以及公钥按照 X.509 证书格式生成证书，发送到 RA 处，将签发成功的证书发给用户。

4.3.2 电子认证服务机构和注册机构对订户的通告

为用户制证后将用户证书直接发放给用户，并将用户的公钥证书发布到主从目录上，以供用户在线查询下载公钥证书。同时，可以通过在线方式实现对证书

撤销列表（CRL）的查询。

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、准确的身份信息经注册机构审核通过，并同意《数字证书用户协议》的约定，申领到证书后即视为订户已经接受此证书。

4.4.2 电子认证服务机构对证书的发布

陕西CA中心在证书签发完成后，将数字证书通过LDAP目录服务将证书发布到http://www.snca.com.cn上，用户可在其上查询下载数字证书。

4.4.3 电子认证服务机构对其他实体的通告

陕西CA系统提供对证书在线状态查询协议的支持，证书成功下载后，证书是否可以信任，用户可以通过标准的证书状态查询接口来获取证书有效性的检查结果。对于陕西CA签发的证书，陕西CA不主动通告其他实体。

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 CPS1.4 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《数字证书用户协议》及 CPS 和 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。

当证书到期或被吊销之后，用户必须停止使用其私钥和证书。

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

4.6.1 证书更新的情形

证书更新指在不改变证书中订户的公钥或其他任何信息的情况下,为订户签发一张新证书,陕西 CA 在证书到期,除事件证书不提供证书更新外,其余都提供证书更新服务。证书到期进行更新服务,可以使用相同的密钥对。

4.6.2 请求证书更新的实体

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。

4.6.3 证书更新请求的处理

证书更新业务提供现场及远程在线办理两种方式。

对于证书更新请求,陕西CA会进行以下验证操作:

（1）更新申请对应的原证书存在并且为陕西CA签发；

（2）用原证书的公钥对更新申请的签名进行验证；

（3)注册机构对申请订户的身份进行查验与鉴别，鉴别要求同本CPS中3.2节描述；

（4）陕西CA注册机构先注销旧证书后，再为证书订户发放更新后的新证书。

4.6.4 颁发新证书时对订户的通告

证书更新完成后，面对面更新的，当面提交给订户，网上在线自助处理时，系统会有提示更新成功或下载成功信息。

订户向注册机构提出更新申请时，注册机构在审核订户身份后，无论是拒绝还是批准订户的更新申请，均有义务告知订户申请结果。

4.6.5 构成接受更新证书的行为

当订户向注册机构提出证书更新请求，并提供真实、准确的身份信息经注册机构审核通过，注册机构将更新后的证书交还给订户，即视为订户接受更新证书的行为。

4.6.6 电子认证服务机构对更新证书的发布

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。

4.6.7 电子认证服务机构对其他实体的通告

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，订户可以申请证书密钥更新。

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。

4.7.1 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。

事件证书私钥在使用过一次后即销毁，不提供证书密钥更新服务。

4.7.2 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。

4.7.3 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，注册机构进行密钥更新。

4.7.4 颁发新证书时对订户的通告

证书更新完成后，面对面更新的，当面提交给订户，网上在线自助处理时，

系统会有提示更新成功或下载成功信息。

订户向注册机构提出密钥更新申请时，注册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。

4.7.5 构成接受密钥更新证书的行为

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

4.7.6 电子认证服务机构对密钥更新证书的发布

同本文档4.6.6。

4.7.7 电子认证服务机构对其他实体的通告

同本文档4.6.7。

4.8 证书变更

4.8.1 证书变更的情形

指改变证书中的订户公钥之外的信息而签发新证书的情形，如用户 DN 信息改变，造成证书改变。证书变更是申请重新签发一张证书，对原证书进行吊销处理。

事件证书仅用于业务场景的一次性的电子签名，不提供证书变更服务。

4.8.2 请求证书变更的实体

合法的陕西CA的证书用户。

4.8.3 证书变更请求的处理

（1）终端用户可提出变更申请、审核、签发。

（2）由RA管理员进行变更处理。

其流程与原始证书签发流程相同，证书有效期将为证书变更时间到原证书到期时间。

4.8.4 颁发新证书时对订户的通告

同本文档4.6.4。

4.8.5 构成接受变更证书的行为

同本文档4.6.5

4.8.6 电子认证服务机构对变更证书的发布

同本文档 4.6.6。

4.8.7 电子认证服务机构对其他实体的通告

同本文档4.6.7。

4.9 证书补办

4.9.1 证书补办的情形

Ukey 证书用户在证书丢失之后，需要尽快到现场进行补办；手机盾证书用户在手机丢失、更换手机之后，需要进行证书补办；云证书根据安全级别要求可与手机硬件绑定，在手机更换或丢失之后也涉及证书补办；事件证书不涉及证书补办。

4.9.2 请求证书补办的实体

证书订户、证书订户的授权代表或证书对应实体的拥有者（比如服务器证书的拥有者）可以要求补办证书。

4.9.3 证书补办请求的处理

订户提出证书补办请求之后，陕西 CA 需要审核补办申请对应的原证书存在并且为陕西 CA 签发；同时对申请订户的身份进行查验与鉴别，鉴别要求同本 CPS 中 3.2 节描述；审核通过之后，陕西 CA 将注销旧证书，再为证书订户发放更新后的新证书。

4.9.4 颁发新证书时对订户的通告

同本文档4.6.4。

4.9.5 构成接受补办证书的行为

同本文档 4.6.5。

4.9.6 电子认证服务机构对补办证书的发布

同本文档 4.6.6。

4.9.7 电子认证服务机构对其他实体的通告

同本文档4.6.7。

4.10 证书吊销和挂起

4.10.1 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）陕西 CA 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，由注册机构审核通过后吊销证书的情形；被动吊销是指当注册机构或 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。

事件证书仅用于业务场景的一次性的电子签名，证书私钥在使用过一次后即销毁，不提供证书吊销服务。

4.10.2 请求证书吊销的实体

在符合本 CPS4.10.1 所述的情形下，请求证书吊销的实体与本 CPS4.1.1 证书申请实体相同。

另外，注册机构或陕西CA也可以在本CPS4.10.1所述的情形下主动吊销订户的证书。

4.10.3 吊销请求的流程

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，向注册机构或关联过新应用的注册机构提出吊销证书请求。

2）接到吊销申请的注册机构，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）注册机构在验证吊销申请后吊销证书。

4）陕西 CA 及时将证书吊销信息发布到陕西 CA 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。

4.10.4 吊销请求宽限期

当订户一旦发现出现CPS&4.10.1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。

4.10.5 电子认证服务机构处理吊销请求的时限

陕西 CA 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。

4.10.6 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。

4.10.7 CRL 发布频率

陕西CA的CRL发布周期为24小时。但在特殊紧急情况下可以立即签发CRL。

4.10.8 CRL 发布的最大滞后时间

一个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。

4.10.9 在线的吊销/状态查询的可用性

陕西CA提供在线的吊销/状态查询，该服务7X24小时可用。

4.10.10 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。

4.10.11 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。

4.10.12 因私钥损害而造成的证书吊销

发现私钥损害的证书应立即注销证书。

4.10.13 证书挂起的情形

陕西CA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。

事件证书不提供挂起服务。

4.10.14 请求证书挂起的实体

所有合法的陕西CA证书订户或者其代理人、陕西CA及其授权的注册机构、法院及其他司法部门等有权提出证书挂起请求。

4.10.15 挂起请求的处理

陕西CA或注册机构在接到证书订户的挂起请求之后，对订户身份进行鉴别，鉴别通过之后，对所申请的证书进行挂起操作，挂起用户证书后，陕西CA或其注册机构将通过发送E-MAIL邮件或邮寄等方式通知用户证书被挂起。用户证书被挂起后，用户必须在证书有效期到期前恢复证书，否则陕西CA或其注册机构有权自行注销证书。对此造成的任何后果，陕西CA不负任何责任。

4.10.16 挂起的期限限制

挂起的时间不得超过证书的实际有效时间。

4.11 证书状态服务

陕西 CA 通过网站、OCSP、LDAP 提供证书状态服务。

4.11.1 操作特征

陕西CA以网络服务的形式提供证书状态查询。网站通过80端口采用HTTP协议发布CRL。OCSP反映证书的当前状态。证书目录LDAP符合LDAP V3协议发布CRL列表。

4.11.2 服务可用性

陕西CA的OCSP、CRL 提供7*24 小时服务。

4.11.3 可选特征

无。

4.12 订购结束

当证书到期或证书被吊销则认证机构、注册机构与订户关系结束。

4.13 密钥生成、备份与恢复

4.13.1 密钥生成、备份与恢复的策略与行为

通用证书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，手机盾证书由基于密钥分割的软件密码模块生成；云证书签名密钥对由服务器端密码机生成。

加密证书的密钥对在 KMC 区内由加密机产生，然后存放到 KMC 中的密钥库中供 CA 系统索取使用，KMC 中的密钥库采用热备方式存储。陕西 CA 依据国家密码

管理部门的相关规定，对加密证书密钥进行集中管理。

密钥恢复只针对加密密钥，签名密钥不提供密钥恢复。加密证书密钥恢复是严格受控过程，只有在以下情况才允许进行密钥恢复：

（1）证书持有人提出申请；

（2）国家司法机构因执法的需要。

4.13.2 会话密钥封装和恢复策略与行为

会话密钥是指用户在建立加密通道时临时生成的加密密钥，该密钥由应用环境来产生使用，陕西CA不对其进行保存和恢复。

5 认证机构设施、管理和操作控制

5.1 物理控制

系统的物理安全和环境安全是整个陕西CA系统安全的基础，它包括基础设施的安全处理、周边环境的监控、区域访问控制、设备安全及灾难预防等。为把陕西CA系统的危险减至最低限度，陕西CA选择设施的适当位置时，充分考虑了水灾、地震、电磁干扰与辐射、犯罪活动以及工业事故等的威胁。

陕西CA系统中的基础设施包括设备及所在机房，对这些设施进行了严格的管理，对系统的访问进行了严格控制，并需要经过授权和进行监控，还装有电子出入控制系统、防侵入系统、机械组合锁等装置。

陕西CA认证机构的物理场地满足以下安全要求并最有效地控制风险：

- 防止物理非法进入

  五层合理的物理结构及完善的安全管理体系。

- 防止未经过授权的物理访问

  确保未经过授权人员不得访问陕西 CA 机构内的受限区域。

- 维持 CA 服务的完整性、可用性

  保障 CA 服务的系统、设施不受到破坏，保证认证服务不被中断。

5.1.1 场地位置与建筑

陕西CA建立了符合标准的电子认证基础设施。安全区内墙六面全部用钢板焊接，屏蔽效果良好，具有防物理侵入、防电子泄露等高安全性能。

陕西CA认证业务的运营场地位于西安市高新技术产业开发区高新三路9号信息港大厦7楼。其运营场地概况如下：

整体建筑由能够阻止物理穿透的材料建成。操作区域及以上区域的墙壁，在其双层饰面之间，采用钢板夹层。操作区域只设置一个大门作为常规入口。操作区域及以上区域均没有窗口。

5.1.2 物理访问

陕西CA系统内各个房间之间利用隔墙进行保护，中心各区均装有防盗门。

陕西CA共设了五个物理安全层来满足认证业务的特定安全要求。

第一层为陕西CA的办公区。

第二层为公共区。办公区向内就是公共区，它是陕西CA操作区入口之外的区域，是进入操作区前各项准备工作的缓冲区域。

第三层为操作区。该区包括DMZ非军事区和RA注册系统操作区。进入操作区的所有授权人员均要通过门禁检查才能进入，非授权人员需要进行登记后才可在相应人员的陪同下进入。

第四层为安全区。该层包括CA签发系统和KMC密钥管理中心。需进行三人（含三人）以上指纹和密码验证身份后才可进入，并有进、出电子记录。

第五层为最安全区。该层为KMC密钥管理中心内的托管中心，进入时要进行三人（含三人）以上指纹和密码识别身份验证，进入托管中心需由专人使用门禁磁卡及钥匙才可开启大门。

以上各层均设有监控录像进行监控。

5.1.3 电力与空调

陕西 CA 中心执行连续运转的所有硬件机房，都配备了高品质的空调系统，

确保所有设备在正常温度、湿度下稳定运行。

电力供给则使用三路供电措施，包括：市电、UPS不间断电源及发电机供电，确保了CA机房用电的安全可靠。

5.1.4 水患防治

陕西CA 的主机房位于大楼的顶层以防止可能出现的地面水患，机房顶部也进行了可靠的防漏水处理，并有完善的排水系统，可完全杜绝水患或将水患的可能控制在最小。

5.1.5 火灾防护

陕西CA设有消防室，配备有JB-QB-GST200/96型火灾报警控制联动系统，根据机房内的各处温感探测器来自动监控火情和启动灭火装置，电器系统完全符合电子数据处理设备的防火标准。机房每个区还备有独立的干粉灭火器，可做为主消防器械的补充，保证了机房出现的火情能被及时发现和控制。为确保楼内基础设施及人员的生命财产安全，陕西CA还制定了火灾处理应急方案，以便发生火灾时能快速高效地扑灭，控制火情，尽量减少因火灾造成的损失。

防火系统建设的标准和规范：

建筑设计防火规范 GBJ16-87

火灾自动报警系统设计规范 GB50116-98

电子计算机房设计规范 GB50174-93

5.1.6 介质存储

陕西CA的存储介质主要包括硬盘、移动硬盘、光盘等，储存的内容主要包括：软件以及归档、备份等数据信息，这些介质保存在安全设施中，只允许授权访问。

5.1.7 废物处理

废弃纸介质用碎纸机粉碎处理，其他介质以不可恢复原则进行相应的销毁处理。对于硬件设备必须清空处理后方可搬出中心机房。

5.1.8 异地备份

为了提高灾难恢复的时间和质量及安全信息的保密性，对关键系统数据、审计日志数据和其它敏感信息进行日常备份，并保存在陕西CA建筑物以外的安全处。

5.2 程序控制

5.2.1 可信角色

陕西CA的可信人员包括：

- 首席安全官员
- 主用户
- 其他管理员（主要包括系统管理员、安全官员、审计人员、网络管理员、加密机管理员）

对于可信任角色，系统规定其权限，对于任务，系统规定参加的角色和人数。

系统管理员具有完成所有功能的权利，并负责管理操作员的建立和口令。系统管理员设置两名，他们的口令绝对保密，身份认证的方式也必须很严格。对系统管理员的操作进行日志记录，以进行审计跟踪。

系统操作员的权限受到限制，只能执行一般的操作，不能建立用户，无权改变系统设置。

在进入系统时，必须通过权限设置或身份认证。审核员对操作员的操作进行审核。系统对系统操作员的操作进行日志记录，以进行审计跟踪。

5.2.2 每项任务需要的人数

陕西 CA 的各项任务都具有严格的策略和控制程序，各岗位人员具有明确的职责。陕西 CA 从安全角度出发，严禁单人进入机房，严禁单人操作。

- 鉴证和签发证书时，要求至少2名可信人员参与
- 访问CA机房进行业务工作时，至少应有3名可信人员参与
- 访问密钥管理中心机房进行业务工作时，至少应有3名可信人员参与

- 系统管理员设置 2 名

5.2.3 每个角色的识别与鉴别

对于物理访问控制，要通过门禁磁卡、指纹识别来鉴别不同的人员，并确定相应的权限。

对于RA、CA、KMC各区安全管理员进行与证书有关的业务管理工作时，需用与管理员对应的用户名/口令方式及数字证书进行身份及权限识别。

5.2.4 需要职责分割的角色

各区管理员有明确的具体角色，以区分任务和责任，如：安全管理员、主用户以及其他管理员等。

5.3 人员控制

5.3.1 资格、经历和无过失要求

（1）在陕西CA工作的人员，必须具备可信、认真负责的特点，其所受的教育、培训及工作经历应足够胜任公司交给的工作。

（2）陕西CA系统操作管理人员必须具备认证系统的相关经验，熟悉PKI基本知识；熟悉CA证书的产生、签发、更新、密钥更新等业务知识；熟悉相关硬件设备的使用及一般性故障的处理；具备系统维护的经验及网络安全经验。对于陕西CA的所有人员应保证没有违法记录。

（3）陕西CA对CA运行管理人员的背景、资历、经验等情况都进行必要的核实和审查，具备认证操作的实务经验和系统管理运营经验。

5.3.2 背景审查程序

陕西CA对应聘CA运行管理人员背景的审查程序为：

（1）系统管理员、操作员和审核员和核心岗位员工应提供如下资料：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。

（2）人力资源专员通过电话、信函、网络、走访、调阅档案等形式对其提供的材料的真实性进行鉴定。

（3）行政部撰写背景审查报告，经主管领导批准后方可上岗。

5.3.3 培训要求

陕西 CA 对员工进行以下内容培训：

（1）电子认证服务行业基本知识培训；

（2）电子《中华人民共和国电子签名法》及《电子认证服务管理办法》等相关文件的培训；

（3）陕西CA认证系统运营培训；

（4）陕西CA认证系统使用软件的培训；

（5）操作人员业务流程及规范培训；

（6）企业内部全面品质管理培训；

（7）对所有员工进行不定期的安全意识教育和培训，增加责任感。

5.3.4 再培训周期和要求

根据陕西CA策略调整、系统更新、业务增加，陕西CA对员工要进行再培训，以适应新的变化。

员工每年至少进行1到2次技能培训及相关知识培训。

对于系统升级、新系统的使用、策略的变化、PKI/CA和密码技术的进步等，根据公司实际情况安排相应的培训。

5.3.5 工作岗位轮换周期和顺序

（1）根据通用业务对小范围岗位进行轮换，达到通用业务大家都能够满足上岗的要求。

（2）陕西CA运维人员和负责系统设计、开发的人员承担不同的职责，双方的岗位互相分离，为保证安全，后者不能成为前者，即实行开发人员和运维人员分离的原则。

5.3.6 未授权行为的处罚

如陕西 CA 员工被怀疑或进行了未授权操作，陕西 CA 证实后立即中止该员工本职岗位工作，根据情节严重程度，采用批评教育、调换岗位、辞退等方式处理。如造成公司重大损失的，陕西 CA 可提请司法机关处理等措施。

5.3.7 独立合约人的要求

陕西CA如因人力不足或特殊需要，聘请专业的第三方服务人员参与系统维护、设备维护等，除了必须签署工作内容的保密协议外，该服务人员必须在陕西CA专人全程监督和陪同下从事相关工作，同时要进行必要的知识培训和安全规范培训，使其严格遵守陕西CA的业务管理规范。

5.3.8 提供给员工的文档

陕西CA提供给员工的文档包括：

陕西省CA运营管理规范及流程

陕西省CA质量体系文件

陕西CA体系机构培训文档

陕西CA PKI基础知识培训文档

公司制度汇编

知识产权保密协议

劳动合同书

试用期合同

应用软件系统操作说明书

各岗位日常操作手册

陕西CA 电子认证业务规则

系统恢复操作手册、灾难恢复方案等

5.4 审计日志程序

陕西CA的审计日志由安全管理部交于档案室统一保存，备份介质存放在陕西CA档案室，存放期不少于3年。

5.4.1 记录事件的类型

陕西CA必须记录与运行系统相关的事件。这些记录，无论是手写、书面或电子文档形式，必须包含事件日期、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注销的信息，如申请表、协议、身份资料和其他相关信息等。

（2）认证系统密钥的生成、变化等记录。

（3）认证系统自身密钥对的生成、内置、变更等成功和失败的记录。

（4）认证系统日常运作产生的日志记录文件。

（5）进出陕西CA 控制区域内的表格、安全令牌进出敏感区域的记录、机房工作日志、系统日常维护记录、监控录像等。

（6）系统软硬件设备上线、更换、下线等的记录。

（7）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。

（8）陕西CA还要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。

5.4.2 处理日志的周期

每季进行一次审计跟踪处理(检查违反政策及其它重大事件)。

对于物理设施的访问日志，每周进行一次检查、处理。

在异常事件发生后或审计日志已满时，要立即处理。

5.4.3 审计日志的保存期限

与证书相关的审计日志，在证书失效后至少保存十年。

5.4.4 审计日志的保护

将审计日志按时间和序号存贮到安全介质中，并由专人负责管理，严格禁止未授权的访问、阅读、修改和删除等操作。

5.4.5 审计日志备份程序

系统日常运行审计文档由管理员每周进行一次归档(每周五进行)。所有文档包括最新的审记跟踪文档需储存在磁盘中并存放在安全的文档库内。

5.4.6 审计收集系统

陕西CA 的审计收集系统涉及的对象包括：

（1）证书管理、受理和用户服务系统

（2）证书签发系统

（3）证书目录系统

（4）备份恢复系统

（5）访问控制系统（包括防火墙、入侵防御系统）

（6）网站系统

陕西CA 采用手工的方式，进行上述系统日志的收集和审查，以保证系统安全运行的需要。

5.4.7 对导致事件实体的通告

在认证系统的运行出现影响安全控制措施的时候，必须通知安全管理人员，并采取有关的应对措施。如果严重影响到系统的运行，导致无法提供正常的证书服务，陕西CA将会通过网站和其它方式向用户进行通告。

在陕西CA进行审查中发现的攻击现象，陕西CA将记录攻击者的行为，在法律许可的范围内追溯攻击者，陕西CA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。

5.4.8 脆弱性评估

陕西CA 每年至少会进行二次系统安全性评估，其中包括从内部和外部对系统可能面临的威胁进行评估。根据评估结果，和系统日志的日常审计和监督实施，及时调整和系统运行密切相关的安全控制措施，以便将系统运作的风险降到最低。

5.5 记录归档

5.5.1 归档记录的类型

陕西 CA 对下列信息进行归档：

（1）证书申请信息；

（2）审计记录；

（3）监控录像；

（4）系统操作服务记录。

5.5.2 归档记录的保存期限

对 CA 证书和密钥生命周期内的管理事件的归档，其保留期限不少于 CA 证书和密钥生命周期；

（1）监控录像保留期限不少于6个月；

（2）系统服务操作记录以及审计记录保留期限不低于3年；

（3）订户证书以及相关信息的归档保留期限不少于证书失效后5年；

（4）CA证书和密钥的归档在CA证书和密钥生命周期之外，再保留5年。

5.5.3 归档文件的保护

为保证归档文件的安全，将归档文件存贮到安全介质中，指定人员安全保管，定期查询登记日志，归档文件不得更改，没有授权的人员无法访问。为防止介质老化，应定期对数据的可用性进行检查。

5.5.4 归档文件的备份程序

陕西 CA 对归档文件定期进行备份，备份文件将被放在异地进行保存。

5.5.5 记录的时间戳要求

陕西CA对每项记录都有时间记录，但这些时间没有采用时间戳技术。

5.5.6 档案收集系统

陕西CA具有专门的电子归档文档的存放系统，归档收集由人工和自动两种方式，归档收集系统由内部管理控制。

5.5.7 获得和检验归档信息的程序

定期检查归档数据的可用性和完整性。

5.6 电子认证服务机构密钥更替

陕西 CA 数字证书认证中心在对 CA 密钥更新时通过签发三个证书来实现 CA 密钥更替。

使用 CA 新的签名私钥对 CA 旧的公钥签名的证书：这是一个自签发的 CA 证书，它是使用新 CA 签名私钥对旧的 CA 验证公钥签名的证书。这使得用新 CA 签名密钥签发的证书用户能够验证由旧签名密钥签发的证书。该证书的合法期限从旧的公/私钥对产生时起到旧的公钥密钥对作废为止。

用旧的私钥对新的公钥签名的证书：它是用旧 CA 的签名私钥对新 CA 的公钥签名的证书。这使得用旧 CA 签名密钥签发的证书用户能够验证由新签名密钥签发的证书。该证书的合法期限从新的公/私钥对产生时起至所有 CA 用户都安全获得了新的 CA 公钥为止（至少到旧的公钥作废为止）。

用新的私钥对新的公钥签名的证书：这是自签发的 CA 新的根证书。这使得用新 CA 签名私钥创建的用户能够相互验证对方的证书而无需验证内部交叉认证链，该交叉认证链由一个旧的自签发 CA 证书链的起始。该证书的合法期限从新

的公/私钥对产生时起至 CA 再次更新公/私对证书制定的作废为止。

5.7 损害与灾难恢复

在出现异常或灾难情况时，为了能够在最短的时间内重新恢复认证系统的运行，陕西CA制订可靠的损害和灾难恢复计划。

5.7.1 事故和损害处理流程

陕西CA遭到攻击，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现象或因不可抗力造成的灾难，陕西CA将按照灾难恢复计划实施恢复。

5.7.2 计算资源、软件和/或数据的损坏

陕西 CA 对业务系统及其他重要系统的资源、软件和数据进行了备份，并制定了相应的应急处理流程。当系统的资源、软件和数据损坏时，要在 24 小时内恢复。

5.7.3 实体私钥损害处理程序

陕西 CA 的根私钥出现损毁、遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，陕西 CA 应该：

（1）立即向电子认证服务管理办公室和其他政府主管部门汇报，通过网站和其它公共媒体对订户进行通告，采取措施保证用户利益不受损失。

（2）立即吊销所有已经被签发的证书，更新CRL 和OCSP 信息，供证书订户和依赖方查询。同时陕西CA 立即生成新的密钥对，并自签发新的根证书。

（3）新的根证书签发以后，按照本CPS 关于证书签发的规定，重新签发下级证书和下级操作子CA 证书。

（4）陕西CA 新的根证书签发以后，将会立即通过陕西CA 信息库、目录服务器、HTTP 等方式进行发布。

当证书订户发现实体证书私钥损害时，订户必须立即停止使用其私钥，并立

即向陕西CA申请吊销其证书，或者立即通过传真、电子邮件的方式通知陕西CA或其注册机构吊销其证书。

当天陕西CA或其注册机构发现证书订户的实体私钥受到损害时，陕西CA或注册机构将立即吊销证书，并通知证书订户，订户必须立即停止使用其私钥。

5.7.4 灾难后的业务连续性能力

陕西CA在遭遇本节5.7.1、5.7.2和5.7.3中描述的灾难后，将立即起动灾难恢复机制，首先恢复在线证书状态查询和CRL列表下载的能力，其次恢复证书的制作能力，以保证陕西CA各种订户的业务需求。一般性的故障将在1个小时内恢复，较大的故障一般也将在24小时之内恢复各项业务的正常运行。

5.8 电子认证服务机构或注册机构的终止

将会严格按照《中华人民共和国电子签名法》中第二十三条和《电子认证服务管理办法》第四章的要求和说明去执行。

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

CA 系统和 RA 系统的密钥对是在加密机内部产生，加密机具有国家密码主管部门的相应资质。在生成 CA 密钥对时，CA 机构按照加密机密钥管理制度， 执行详细的操作流程控制计划，选定并授权 3 个密钥管理员，密钥管理员凭借智能 IC 卡对密钥进行控制。

通用证书的签名密钥对由订户的密码设备（如智能 USB KEY 或智能 IC 卡等）生成，加密密钥对由密钥管理中心生成。

手机盾证书的签名密钥由基于密钥分割的软件密码模块生成。

云证书的签名密钥由服务器端密码机生成，加密密钥对由密钥管理中心生

成，密码机具有国家密码主管部门的相应资质。

6.1.2 私钥传送给订户

通用证书订户的签名密钥对由自己的密码设备生成并保管。

事件型证书的签名密钥对由签名密码设备生成并保管。

手机盾证书签名密钥对由基于密钥分割的软件密码模块生成，通过安全通道协商传输。

云证书：签名密钥对由服务器端密码机生成，加密存储在云服务器数据库中。

证书的加密密钥对由密钥管理中心产生，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

注册机构通过安全软件把公钥通过安全通道发给陕西CA。

6.1.4 电子认证服务机构公钥传送给依赖方

陕西CA的公钥通过如下方式传递给依赖方：

（1）依赖方访问陕西CA的网站，下载根证书。

（2）依赖方访问陕西CA的目录系统获取根证书。

（3）陕西CA、注册机构或合作伙伴通过签名电子邮件将CA的根证书传输给依赖方。

6.1.5 密钥的长度

陕西CA用户签名密钥对的长度是 RSA算法：1024位或2048位，SM2算法：256位

陕西CA用户加密密钥对的长度是 RSA算法：1024位或2048位，SM2算法：256位

6.1.6 公钥参数的生成和质量检查

陕西CA系统的密钥中公钥由CA系统软件从加密机中取出，符合国家密码管理部门的要求。

6.1.7 密钥使用目的

密钥的用途在证书的“密钥用途”域中有定义，主要分为加密、解密、签名和验证几种用途。

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

陕西 CA 使用国家密码管理部门认可的密码设备产生 CA 密钥对，陕西 CA 也使用密码硬件设备来存储密钥对。

在密码硬件设备的初始化、上线、销毁等生命周期内，陕西 CA 有相应的策略来保障硬件密码设备的安全。

陕西 CA 密码设备遵循多人在场、多人控制的原则。

6.2.2 私钥多人控制（m 选 n）

为保证系统运营安全，对CA的各类私钥操作都采取3 of 5的安全口令管理机制，即五个管理员有三个以上到场，输入三个以上的管理员口令，方可执行相应的操作。

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。

通用证书对应的签名私钥由自己保管，密钥管理中心不负责托管。手机盾证书的签名私钥由订户终端和签名服务云端协同计算产生并分别保管；云签证书签名私钥加密存储在云服务器数据库中。

密钥管理中心严格保证订户密钥对的安全，密钥以密文形式保存，密钥库具有最高安全级别，禁止外界非法访问。密钥管理中心严格保证订户密钥对的安全，密钥以密文形式保存，密钥库具 有最高安全级别，禁止外界非法访问。

6.2.4 私钥备份

作为灾难恢复的一项措施，需要进行密钥备份。陕西CA 采用密码设备以及密钥备份卡进行密钥备份，这些备份存储在本地以及异地。在备份密钥时，必须由密钥管理员使用加密IC 卡，同时至少有两名管理员在场，启动密钥管理程序，执行密钥备份指令才能完成。

6.2.5 私钥归档

当陕西CA的CA密钥对超过使用期或因其他原因终止使用后，这些CA密钥对将归档保存至少5 年。归档CA密钥对保存在CPS6.2.1所述的硬件密码模块中。对归档私钥到了归档保存期，将按CPS6.2.10销毁。

6.2.6 私钥导入、导出密码模块

陕西CA的密钥对在硬件模块上生成、保存和使用。为实施灾难备份或恢复，需要对CA密钥进行导入或导出，当导出CA密钥时，需要至少两名管理员在场，并进行身份验证。导出的密钥以密文的形式存放。当导入CA密钥时也至少需要两名管理员在场，并进行身份认证。

6.2.7 私钥在密码模块的存储

陕西CA的私钥在密码模块中以密文的形式存在。

6.2.8 激活私钥的方法

CA私钥：具有激活私钥权限的管理员使用含有自己的身份的加密IC卡登录，启动密钥管理程序，进行激活私钥的操作，需要多管理员同时在场。

订户私钥：通过PIN码激活。

6.2.9 解除私钥激活状态的方法

关闭密码模块设备、停止私钥服务应用等。

6.2.10 销毁私钥的方法

陕西 CA 的私钥，不再使用并且不再需要保存时，为避免丢失或非授权使用需要销毁私钥，在归档期结束后需销毁时需有多名管理员在场安全彻底销毁。

订户私钥，在确信无需保存时，可以通过删除或初始化来销毁私钥。

6.2.11 密码模块的评估

陕西 CA 使用的密码模块，是经国家密码管理部门认可、批准的。

密码模块的评估由国家密码管理部门进行。

6.3 密钥对管理的其它方面

6.3.1 公钥归档

陕西CA对生命周期结束后的公钥进行归档，归档证书存放在系统数据库中。

6.3.2 证书操作期和密钥对使用期限

订户证书的有效期与密钥对有效期一致，根据合同设定有效期，有效期不能超过陕西 CA 根证有效期。

为了保证在证书有效期内签名的信息可以验证，公钥的使用期限可以在证书的有效期限以外，直到私钥受到损害或密钥对存在被破解的风险发生。当私钥受到损害或密钥对被破解后，签名证书的公钥仅仅在技术层面上来验证数字签名，这时这种验证在法律上不一定有效。

6.4 激活数据

6.4.1 激活数据的产生和安装

陕西 CA 私钥的激活数据由硬件加密机内部产生，并分割保存在 5 个备份密钥卡中，需通过专门的读卡设备和软件读取。

对于订户的私钥，激活数据就是私钥保护密码，是由用户自己产生并且需要符合一定的安全策略，例如至少8 位字节长、需要在密码中同时具有大小写字符和数字等。

6.4.2 激活数据的保护

保存有陕西 CA 私钥的激活数据的 5 个密钥备份卡，由 5 个不同的可信人员持有，分别存在个人负责的保密柜中。

对于陕西CA的订户的私钥激活数据，用户需要进行妥善保护不要泄露给其他人，如果因为激活数据丢失造成的私钥被盗用进行操作的情况，将视同私钥主人用私钥进行操作。

6.4.3 激活数据的其他方面

陕西CA的密钥激活数据在传送时，应保证激活数据不被窃取、篡改或非授权使用；在销毁时，应确保激活数据被彻底销毁。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

陕西CA 的系统运行环境按功能划分安全区，并实行访问权限控制。核心系统和其它系统隔离，采用防火墙和入侵检测保证安全。并实行：

系统安全配置，关闭不必要的服务与端口。

操作系统必须安装最新的补丁程序，由专人负责最新补丁的安装。

生产系统每台机器均由专人负责，严格上机操作程序，口令逐级管理，逐级授权。

各人负责各自权限范围内的操作。

日志和操作记录的审计制度。

数据备份和恢复机制。

6.5.2 计算机安全评估

陕西 CA 对计算机的安全要求如下：

支持多异型机联机、能进行联机事务处理和批处理，支持多用户、多任务和批处理。

操作系统具有 C2 级安全级别，具有自主访问控制。

具有很好的容错处理能力，能提供各种安全保密处理。

支持多种通信协议。

支持系统的扩展与本地升级。

6.6 生命周期技术控制

6.6.1 系统开发控制

在系统的设计和开发中，陕西 CA 注意在安全开发环境中严格按照软件工程的要求进行开发控制，保证系统的安全性和可靠性。

6.6.2 安全管理控制

陕西CA通过已制定的安全策略、管理制度以及操作流程对CA系统进行安全管理控制。

6.6.3 生命期的安全控制

陕西CA的CA认证系统在系统设计过程中充分进行了安全性考虑，在正式使用前通过了国家有关部门的系统安全性审查。

6.7 网络的安全控制

在陕西 CA 的网络系统中，把整个网络划分为四个区：公共区、DMZ、操作区和安全区。各安全层次之间采用不同类型的防火墙，每个安全层次在一个子网上，安全策略不尽相同， 使得网络系统具备很强的防范能力。

在采用多层防火墙技术增加系统的安全性的同时，我们还选用了入侵检测设备等，这些产品可以从多方面对网络系统进行监测和分析，能够及时发现入侵者并及时报警，同时还能够采取一定的补救措施。

6.8 时间戳

时间戳系统提供的时间戳服务在技术实现上严格遵循国际标准时间戳协议（RFC3161），采用标准的时间戳请求、时间戳应答以及时间戳编码格式，时间源采用国家授时中心提供的标准时间。

7 证书、证书吊销列表和在线证书状态协议

7.1 证书

陕西 CA 签发的证书符合 X.509 V3 格式。遵循 RFC3280 标准。

7.1.1 版本号

陕西CA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。

7.1.2 证书扩展项

CA 证书扩展项除使用 IETF RFC 3280 中定义的证书扩展项，还支持私有扩展项。

CA 采用的 IETF RFC 3280 中定义的证书扩展项：

•颁发机构密钥标识符 Authority Key Identifier

•主体密钥标识符 Subject Key Identifier

•密钥用法 Key Usage

•扩展密钥用途 Extended Key Usage

•私有密钥使用期 Private Key Usage Period

•主体可选替换名称 Subject Alternative Name

•基本限制 Basic Constraints

•证书撤销列表分发点 CRL Distribution Points

私有扩展项可支持以下类型:

•个人身份证号码 Identify Card Number

•企业营业执照(统一社会信息代码)IC Registration Number

•企业组织机构代码 Organization Code

•企业税号 Taxation Number

7.1.3 算法对象标识符

陕西CA签发的证书按照RFC3280标准,用sha1RSA或SM2算法签名。

7.1.4 名称形式

陕西 CA 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。

7.1.5 名称限制

陕西CA签发的证书，其名称须严格按照7.1.4的规则来定义。

7.1.6 证书策略对象标识符

见陕西 CA 证书策略第 1.2 节。

7.1.7 策略限制扩展项的用法

未使用本扩展域。

7.1.8 策略限定符的语法和语义

未使用本扩展域。

7.1.9 关键证书策略扩展项的处理规则

未使用证书策略扩展项。

7.2 CRL

7.2.1 版本号

陕西CA使用的CRL符合X.500 标准。

7.2.2 CRL 和 CRL 条目扩展项

CRL 数据定义:

(1) 版本 (Version)

含义:显示CRL 的版本号。

(2) 签名 (Signature)

含义: 签发CRL 的CA 的签名。

(3) 算法标识 (algorithmIdentifier)

含义:定义签发CRL 所使用的算法。

(4) CRL 的签发者 (Issuer)

含义:指明签发CRL 的CA 的甄别名。

(5) CRL 发布时间 (thisUpdate)

(6) 预计下一个CRL 更新时间(next update)

(7) 吊销证书信息目录(revoked certificates)

(8) CRL 扩展 (CRL Extension)

- CA 的公钥标识(AuthorityKeyIdentifier)
- CRL 号 (CRL Number)

7.3 在线证书状态协议

7.3.1 版本号

陕西CA 可以提供支持RFC2560(X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP)的OCSP 服务。

版本号：1.0

7.3.2 OCSP 扩展项

暂无

8 认证机构审计和其它评估

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）陕西CA 按照国家主管部门的要求、国家相关标准和本CPS 的规定进行运营和服务，按照陕西CA 制订的内部评估和审计规范，每年至少定期执行一次内部的评估审核，包括对陕西CA、陕西CA 授权的发证机构和其他关联机构的评估审核。陕西CA 认证体系的关联机构，包括RA、RAT 以及其他陕西CA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，并接受陕西CA对其所有的流程和操作进行审计，检验其是否符合本CPS 和与之相关的陕西CA在授权协议规定的、或者其它公示过的运营服务政策的规定。陕西CA对关联机构的评估，一般一年进行一次。评估人员由陕西CA安全管理委员会根据要求指派并备案。评估人员必须熟悉陕西CA的规范和运营服务的相关知识，了解保证安全的基本知识，按照陕西CA的规范、协议提供服务等情况，独立、公正地对关联单位作出评估结论。

陕西CA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。陕西CA 的关联实体，被评估的次数一般情况下为一年一次。

8.1.1 评估者的资质

（1）陕西CA 无条件接收国家主管部门的评估。对陕西CA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，陕西CA评估人员应具备PKI和CA系统基本知识，熟悉行业规范，具有行业相关知识或者具有国家评估审计人员相应资质。评估小组的成员可以由公司各相关部门的代表组成。

8.2 评估者与被评估者的关系

（1）外部评估者(信息产业主管部门或者其委托的其他机构)和陕西CA之间是独立的关系，没有任何的业务、财务往来，或者其它任何利害关系足以影响评估的客观性，评估者应以独立、公正、客观的态度对陕西CA进行评估。

（2）陕西CA的内部评估者，独立于与被评估的对象所在的部门。

8.3 评估内容

（1）陕西CA按照信息产业主管部门依法提出的评估要求和规范，接受其任何内容的评估。

（2）陕西CA内部评估审核的内容包括：

- 是否制订和公布CPS
- 是否按照CPS来制订相关的操作规范和运作协议
- 是否按照CPS及相关操作规范和运作协议开展业务
- 服务的完整性：密钥和证书生命周期的安全管理、证书吊销的操作、业务系统的安全操作、业务操作规范审查
- 物理和环境安全控制：信息安全管理、人员的安全控制、建筑设施的安全控制、软硬件设备和存储介质的安全控制、系统和网络的安全控制、系统开发和维护的安全控制、灾难恢复和备份系统的管理、审计和归档的安全管理等。

8.4 对问题与不足采取的措施

（1）信息产业主管部门评估完成后，陕西CA必须根据评估的结果检查缺失和不足，根据其提出的整改要求，提交修改和预防措施以及整改计划书，并接受其对整改计划的审查，以及对整改情况的再次评估。

（2）陕西CA 完成内部评估后，评估人员需要列出所有问题项目的详细清单，由评估人员和被评估对象共同讨论有关问题，并将结果书面通知陕西CA运营策略委员会和被评估者，进行后续处理。

（3）被评估对象必须根据评估的结果检查缺失和不足，提交修改和预防措施以及整改计划书，并接受评估者对整改计划的审查，以及对整改情况的再次评估。

8.5 评估结果的传达与发布

（1）信息产业主管机构在完成评估后，按照法律法规的要求对评估结果进行处理。

（2）陕西 CA 的内部评估结果在与被评估对象的相关人员进行讨论确定后，将其视为机密资料进行处理，只有被评估对象和评估人员以及陕西 CA 运营策略委员会可以了解。非经陕西 CA 安全管理委员会的批准或者被评估对象的授权，评估人员不能泄露给任何其他无关的第三方知晓。

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

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。

9.1.2 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。

9.1.3 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。

9.1.4 其它服务费用

陕西 CA 保留收取其他服务费的权利。

9.1.5 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

9.2.1 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。

9.2.2 其他资产

无。

9.2.3 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。

9.3 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。

9.3.1 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。

9.3.2 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。

9.3.3 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

9.4.1 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。

9.4.2 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。

9.4.3 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。

9.4.4 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。

9.4.6 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。

9.4.7 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。

9.4.8 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。

9.5 陈述与担保

9.5.1 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。

（11）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。

9.5.2 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。

9.5.3 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。

9.5.4 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。

9.5.5 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。

9.6 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。

9.7 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。

9.8 赔偿

9.8.1 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。

9.8.2 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。

9.9 有效期限与终止

9.9.1 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。

9.9.2 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。

9.9.3 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。

9.10 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。

9.11 修订

9.11.1 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。

9.11.2 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。

9.11.3 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。

9.12 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。

9.13 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。

9.14 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。

9.15 一般条款

9.15.1 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。

9.15.2 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。

9.15.3 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。

9.15.4 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。

9.15.5 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。

9.15.6 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。